McAfee
An Intel Company

JACKPOT! MONEY LAUNDERING THROUGH ONLINE GAMBLING

McAfee Labs
White Paper

ABOUT McAFEE LABS

McAfee Labs is the world's leading source for threat research, threat intelligence, and cybersecurity thought leadership. With data from millions of sensors across key threats vectors—file, web, message, and network—McAfee Labs delivers real-time threat intelligence, critical analysis, and expert thinking to improve protection and reduce risks.

www.mcafee.com/us/mcafee-labs.aspx

INTRODUCTION

The same basic money-laundering model used during Prohibition is applied today by the modern cyberthief.

The ingenuity of criminals never ceases to amaze us. Whether it's the things they steal or the way they steal them, creativity reigns. That cleverness also flows to converting their ill-gotten gains into "clean" money.

Modern money laundering is said to have started during Prohibition in the United States, when the proceeds from illegal alcohol sales needed to be converted into cash flowing from a legitimate business. They took advantage of common, large cash-flow businesses with anonymous, difficult-to-trace transactions—taxi services, restaurants, laundries, foreign currency exchanges come to mind—and many seemingly legitimate fortunes were built as a result. Indeed, several prominent American families trace their financial success to the sale of alcohol during Prohibition.

That same basic money-laundering model—taking advantage of accessible, high-volume businesses with anonymous, difficult-to-trace transactions—is applied today by the modern cyberthief.

In this report, we highlight one such example: the use of online gambling sites to launder dirty money. Like criminals during Prohibition, cyberthieves employing this method depend on anonymity, access, and the river of money that typically flows through an online gambling site. We hope you enjoy the read.

Vincent Weafer, Senior Vice President, McAfee Labs

Follow McAfee Labs

CONTENTS

JACKPOT! MONEY LAUNDERING THROUGH ONLINE GAMBLING
McAfee Labs White Paper

This white paper was written by:

Charles McFarland

François Paget

Raj Samani

EXECUTIVE SUMMARY 4

GROWTH OF ONLINE GAMBLING 5

Growth of licenced online gambling sites 6

Growth of unlicenced online gambling sites 8

Money laundering though online gambling sites 8

BENEFITS OF MONEY LAUNDERING THROUGH ONLINE GAMBLING 10

Anonymity 10

Access 10

Ancillary services 12

Word of caution 13

ADDRESSING THE ISSUE 14

CONCLUSION 15

ABOUT THE AUTHORS 15

EXECUTIVE SUMMARY

Each of the four major online segments (sports betting, poker, casino, and bingo) will continue to grow, reaching approximately €31.2 billion (US$43.0 billion) by 2015, implying a compound annual growth rate of approximately 7.3%.

Cybercrime stories often focus on the unfortunate victim or speculate on the vulnerability exploited in the attack, with rumors and conjecture plastered across social and other media. These two elements of an attack are often interesting, but they tell only a part of the story. The development of the attack, including researching the target, and the development of weapons and infrastructure are rarely discussed; yet they form essential elements of the crime. We looked at these components, or rather at the outsourcing of these components, in our publication *Cybercrime Exposed: Cybercrime-as-a-Service*.[1]

While *Cybercrime Exposed* focused on the initial stages of an attack, this report focuses on the final stage, as cybercriminals launder their proceeds to avoid detection by law enforcement agencies. Criminals use a variety of methods to conceal money, such as merchandise laundering and secret banking, but this report focuses on the most prominent method—online gambling. This method is unlikely to surprise anyone; physical gambling locations have been used for money laundering for some time. Further, the ease with which players (including criminals) can use online gambling operators makes them a considerably more attractive proposition than their physical counterparts. According to one source, "each of the four major online segments (sports betting, poker, casino, and bingo) will continue to grow, reaching approximately €31.2 billion (US$43.0 billion) by 2015, implying a compound annual growth rate of approximately 7.3%."[2]

In addition to the ease of use online gambling sites offer, players enjoy greater anonymity with cryptocurrencies as a transaction method. We discussed the use of virtual money in our recent report *Digital Laundry: An analysis of online currencies, and their use in cybercrime*.[3] Transacting with Bitcoin and other virtual money is gaining popularity in online casinos. If we include the number of ancillary services, such as laundering tools, to the availability and anonymity of online casinos, then their attractiveness for experienced and would-be criminals becomes very clear.

As we have stated in our recent publications, traditional crime is evolving. According to the US Federal Bureau of Investigation Bank Crime reports, bank robberies in 2011 fell to 5,014, from 5,546 in 2010.[4] Cybercrime is becoming the new theater for the 21st-century criminal. This report details one particular element of this evolution—money laundering through online gambling.

Getting paid—and getting away with it—remains the ultimate goal of cybercriminals.

Tweet about this report

Follow McAfee Labs

"Online casinos are vulnerable to a wide variety of criminal schemes. For example, criminals may participate in games with exclusively criminal players, exchanging money to launder proceeds; or a criminal might intentionally lose a game to a public official in order to effect a bribe payment."[5]

Virtual currencies, electronic banking, online gambling, and online auctions now feature heavily in money laundering techniques.

Follow McAfee Labs

GROWTH OF ONLINE GAMBLING

The quote at left is part of an assessment the FBI sent in September 2013 to Congressman Bill Young of Florida, in response to his letter to the FBI. This level of concern is reflected by law enforcement agencies across the world. According to the Europol Serious and Organised Crime Threat Assessment 2013, "virtual currencies, electronic banking, online gambling, and online auctions now feature heavily in money laundering techniques."[6]

Perhaps the rise of criminal activities within online gambling should not be a surprise, nor should their popularity. From the onset of online gambling in the mid-1990s, its growth has been nothing short of staggering, and it is forecasted to continue growing. The increase in online revenues appears to compensate for the decline in physical site–based revenues. This claim is supported by Microsoft's 2011 publication *Casino Insights and Trends*.[7]

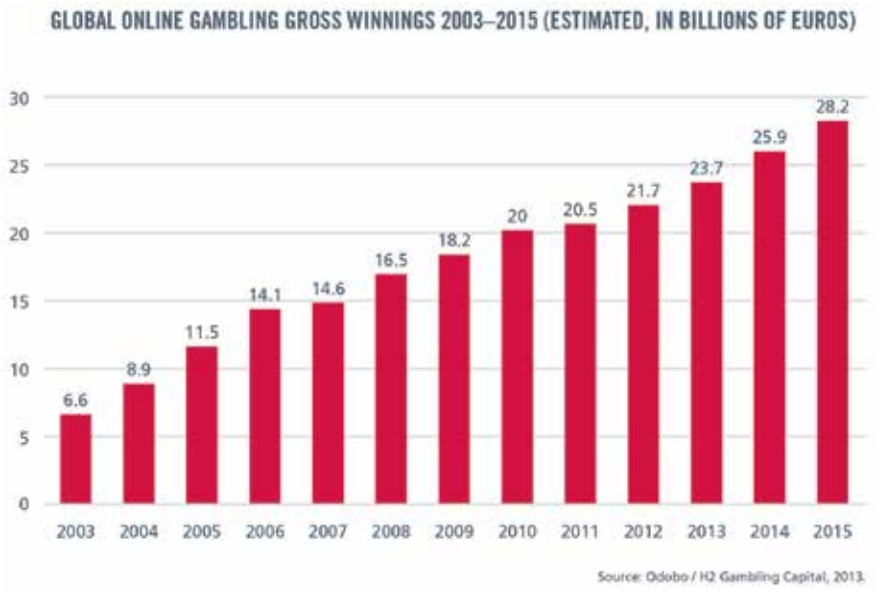

Figure 1. Gross winnings (stakes minus prizes) from online gambling, both actual and projected.

"Within the next three-year period, it is predicted that the market will grow by almost 30%, to a value of €28.24 billion (US$38.95 billion)," says H2 Gambling Capital, a market research firm that focuses on the value and volume of activity within the global gambling industry.[8] This growth can be attributed to a change in consumer habits, and to the United States finally opening its doors to regulated online gambling. This rise is graphically depicted in Figures 1 and 2, taken from H2's report *There's Nothing Virtual About the Opportunity in Real-Money Gambling*.[8]

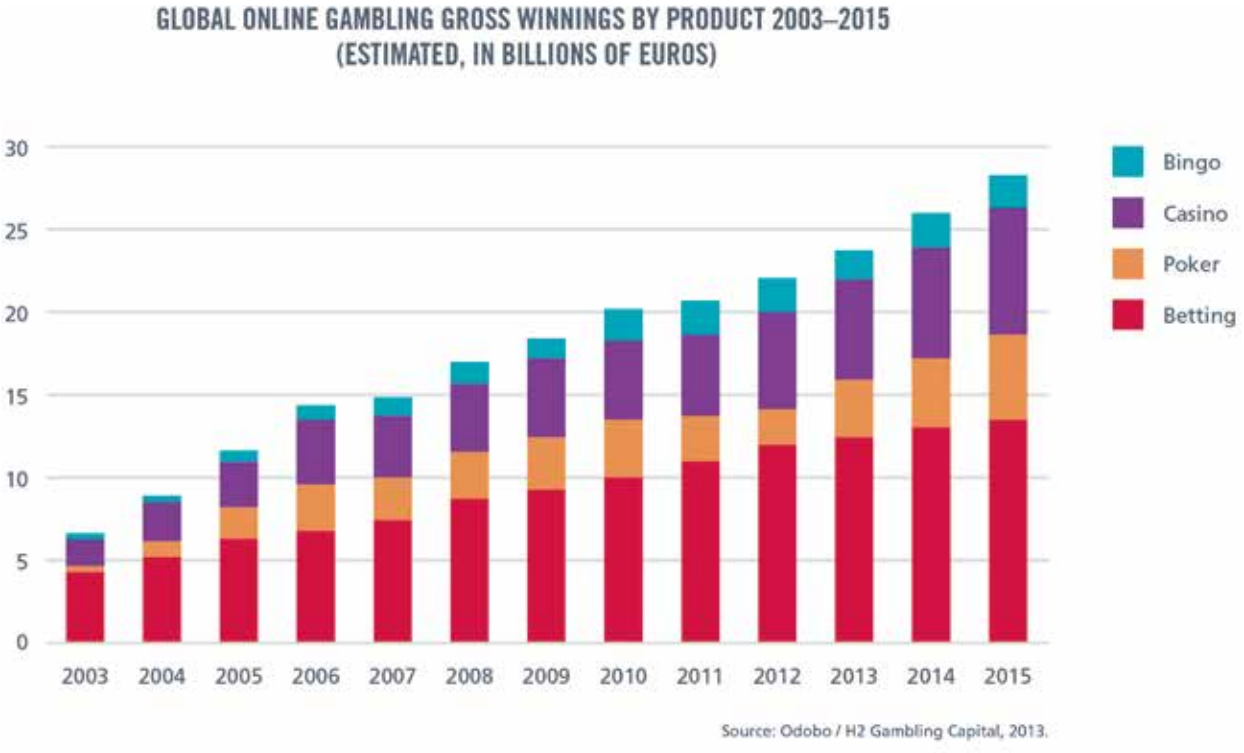

Figure 2. Gross winnings by products.

The products in Figure 2 show the four leading categories that make up the online gambling industry. Although the majority of revenue has come from sports betting, H2 sees the greatest growth in online poker (predicted to show a compound annual growth rate of 14.4%) and casinos (10.9%), respectively. Poker and casinos offer opportunities for money laundering.

Growth of licensed online gambling sites

When we talk about "licensed" online gambling, we refer to those gambling websites that have a jurisdictional license to conduct activities. As of November 2013 there were approximately 104 international jurisdictions that regulated a total of 2,734 Internet gambling sites (for 867 gambling-site owners) in at least one form of wagering, according to Casino City,[9] an independent directory and information service. Some of those jurisdictions are depicted in the following table.

NUMBER OF REGULATED ONLINE GAMBLING WEBSITES					
Jurisdictions	March 2008	May 2009	July 2010	January 2011	November 2013
Alderney	54	66	96	98	120
Antigua and Barbuda	142	77	78	65	50
Costa Rica	244	220	226	185	181
Cyprus	22	32	45	47	120
Gibraltar	172	216	255	262	312
Isle of Man	10	15	26	38	79
Italy	1	57	59	60	230
Kahnawake (Mohawk Territory, Canada)	324	251	216	181	120
Netherlands Antilles	320	271	312	280	456
United Kingdom	107	92	99	108	103

Source: Casino City.

Table 1: Licensed gambling sites are regulated by a wide variety of countries.

Figure 3: A partial list of rogue sites according to Casino City.

In Table 1 we see that the number of licensed sites is very fluid. Consequently, the numbers presented in this report may have changed by the time you read this. For example, of the 2,734 licensed gambling sites cited, 47 are already deemed "rogue" and not trustworthy according to Casino City. (See Figure 3.) Given such volatility, it is no surprise that online players are warned to "play at their own risk."

For every licensed online gambling site, there could be up to nine unlicensed online gambling sites.

Growth of unlicensed online gambling sites

Although a large proportion of gamblers comply within local laws and use licensed gambling services (and contribute to these impressive growth figures), a significant percentage are engaged in gambling at unlicensed websites. Examples of unlicensed online gambling vary but can include bingo, poker, betting, and other casino games.

In fact, the number of licensed gambling websites is simply a drop in the ocean compared with sites that are unlicensed (and subsequently illegal in some jurisdictions). In October 2011, one count of unlicensed websites reached 25,000.[10] With dozens of unlicensed gambling sites being created every day, it is likely this number has increased significantly.

Money laundering through online gambling sites

Let's turn our attention to money laundering through online gambling sites: The recent study *Online Gambling as a Game Changer to Money Laundering?* suggests three compelling reasons that explain why online gambling sites are so appealing to money launderers:[11]

- Gambling involves a huge volume of transactions and cash flows, which are necessary to disguise money laundering.
- Gambling does not involve a physical product (such as paper currency), making it much more complicated to track the flow of money and prove real vs. virtual turnover.
- Gambling winnings are tax free in many jurisdictions.

These advantages offer the would-be money launderer real motivation to use online gambling sites. The advantages may also include a decreased likelihood of detection as well as lower costs associated with laundering funds. Money launderers can generally use online gambling sites in two scenarios:

- When an illegal transaction occurs, the proceeds can be laundered by betting them and receiving the payouts as gambling winnings. The ability to transfer small funds into "legal gambling wins" is aided by the offshore nature of many services and vastly reduces the detection rate by law enforcement. The reduced detection rate lowers the cost of laundering as the number of potential fines decreases.
- Using gambling as a payment tool for illegal transactions, such as paying off gambling wins as cash for illegal goods. By conducting a player-to-player transfer to send funds to the account of the seller of the illegal goods, the seller is can claim the funds as tax-free gambling winnings.[12]

Follow McAfee Labs

Key differences between licensed and unlicensed gambling sites:

- Licensed gambling sites generally require adherence to anti-money-laundering legislation.
- Licensed gambling sites are usually audited by a supervisory authority.
- Licensed gambling sites sometimes require players to deposit funds through institutions subject to anti-money-laundering requirements.

The process associated with money movement within online gambling platforms is shown in Figure 4. We see in particular the various options regarding deposit and withdrawal methods. Although the graphical depiction is an oversimplification, the number of options available demonstrates that would-be money launderers have many opportunities to obfuscate money flows through online gambling sites, and ultimately make the task for law enforcement more difficult.

There's a key difference between licensed and unlicensed gambling sites and the likelihood of their reporting financial intelligence to law enforcement. Licensed operators require players to transmit deposits and withdrawals via licensed banks, for example. The MoneyVAL report "The use of online gambling for money laundering and the financing of terrorism purposes" makes the point:[13]

> "Licensed online gambling operators generally fall within the scope of the national Anti-Money Laundering/Countering the Funding of Terrorism legislation and are therefore subject to Customer Due Diligence, record-keeping and reporting requirements. Supervision for AML/CFT purposes is either conducted by the Financial Intelligence Unit or else by the financial/gambling supervisory authority of the country concerned."

There is great debate regarding the level of oversight by licensed operators. Although that oversight is likely to decrease the risk of money laundering, the following risks clearly exist, according to the report:

- "Unlicensed online gambling sites do not require players to deposit funds through licensed financial institutions that are subject to adequate AML/CFT requirements."
- "Not all jurisdictions that license online gambling require online gambling operators to ensure that players deposit funds solely through licensed financial institutions that are subject to adequate AML/CFT requirements."

Further, alternate payment methods such as intermediaries, virtual currencies, and pre-paid cards for both licensed and unlicensed operators are likely to result in less scrutiny into deposits and withdrawals, and ultimately increase the risk of money laundering.

Figure 4: Steps for online gambling deposits and withdrawals.

Follow McAfee Labs

BENEFITS OF MONEY LAUNDERING THROUGH ONLINE GAMBLING

There are many benefits to using online gambling platforms for money laundering. The most compelling are anonymity, access, and ancillary services.

Anonymity

In our report *Digital Laundry* we suggested that the benefit of using virtual currencies for criminal purposes is the level of anonymity afforded to participants. This same benefit holds for those using online gambling sites.

As depicted in Figure 5, certain providers are explicit about the level of anonymity that online players enjoy.

This example not only rejects the need for personal information when using the online platform, but also cites Bitcoin as another layer to reinforce the level of anonymity afforded to players.

In spite of the claims of Bitcoin adherents, however, using online gambling platforms does not guarantee anonymity. Further resources are becoming available to offer online players even greater obfuscation to hide their true identities. In particular, some platforms leverage the TOR network for additional anonymity, as depicted in Figure 6.

TOR is free software that allows users to achieve online anonymity. By directing Internet traffic through a series of relays, users can conceal their locations and usage from surveillance, thus defeating any attempt to monitor online activities.

Online gambling sites on TOR, however, will never be as popular as those operating on the "visible" web. This is due to the technical limitations of many users, complexity, and the proliferation of scams by anonymous users.

Figure 6: The TOR network offers additional anonymity to online gamblers and criminals.

Access

TOR is an approach to achieving anonymity. But anonymity is not the only concern: Users may also have trouble with access. One access mechanism is the use of a proxy server, which can make a connection appear as if it comes from another location or country. Proxy servers could help bypass restrictions that licensed sites have in place to block players from countries where the site owner does not have a proper license.

Figure 5: Anonymity is a chief benefit of online gambling.

Follow McAfee Labs

The availability of player anonymity and location-hiding services simplifies the technical obstacles money launderers face.

Another mechanism, which solves both the problems of anonymity and access, is a virtual private network (VPN), which offers the additional benefit of encrypting the traffic from the peering eyes of Internet service providers (ISPs) or law enforcement. Certain providers give users a multitude of VPN connections—for example, torguard.net advertises 300 servers across 23 countries.

A number of VPN providers offer their customers the ability to hide their IP addresses and appear to come from a particular city. Some are already advertising VPN servers located in New Jersey and many other cities in the world. Although there is no suggestion that connections are being blocked from outside the state, this particular example demonstrates that the marketplace to bypass restrictions already exists (as iPlayer users in the United States can testify). The costs will vary but could be as low as US$20 per month. These services can be merely a single layer upon additional layers of obfuscation to mask one's identity.

The availability of such services simplifies the technical obstacles money launderers face in bypassing restrictions, or in hiding their identities. These workarounds make a mockery of geographic restrictions placed upon online gambling services. On November 26, 2013, for example, a report claimed that the state of New Jersey expanded the boundaries of its gambling to allow online players, but with the following restriction: "To take part, you will have to be within the state and at least 21 years old."[14]

```
-----------------------------------------------:
                                               :
 Running A Successful + Profitable             :
 Gambling Ring                                 :
 By CandyMan                                   :
                                               :
-----------------------------------------------:


DISCLAIMER: THE FOLLOWING INFORMATION IS OFFERED
FOR INFORMATIONAL, EDUCATIONAL, AND ENTERTAINMENT
PURPOSES ONLY. THE PROCEDURES CONTAINED BELOW
ARE ILLEGAL. ANY USER OF THESE PROCEDURES TAKES
ALL RESPONSIBILITY FROM ANY HARM OR LEGAL ACTION
THAT MAY ARISE.


WARNING:
========
Opening a gamble ring can be VERY profitable, but
you will face 2 problems: 1.)The Organized Crime
will not like others cutting into to this very
profitable and illegal business, they may hurt
you badly, or you may be among the many others
who were given cement shoes and thrown in the
river or lake! 2.)You face the problem of being
busted for illegal gambling and lots of fines,
legal costs, and jail time.

WHAT YOU NEED TO BE
===================

You are going to need to be a bad ass, because you
will need to collect the bets from people who lost
and are not paying you. You will have to instill
fear in them and bust a couple of there bones. If
you have problems doing this you can always hire
someone to work under you to do this dirty work.
You will still have to be tough fucker to kick
some ass if some of the people that work under
you if they begin to steal money or try to open
their own gambling ring. You also need to break
apart any competition that you may have.
```

Figure 7: Advice for running a gambling ring.

Follow McAfee Labs

Ancillary services

With the advent of many online gambling sites, we have witnessed a multitude of ancillary services that can assist would-be gamblers in obfuscating their funds from prying eyes. Some of these money-laundering tools are depicted in Figures 8 and 9.

Figure 8: One site for Bitcoin use and money laundering.

The information in Figure 8 can be used to obfuscate the origins of Bitcoin transactions. These "mixers" claim to offer anonymity, as depicted in Figure 9.

Figure 9: Another site offering Bitcoin services.

Follow McAfee Labs

In addition to mixers, alternate services allow potential customers to anonymously acquire virtual currencies. In *Digital Laundry* we wrote about the introduction of anti–money-laundering controls within formal exchanges. The Financial Crimes Enforcement Network (FinCEN) has sent letters to Bitcoin-related businesses requiring them to comply with federal money-transmission laws.[15] Subsequent to the letters and other actions, a number of businesses suspended trading and others registered with FinCEN, resulting in customers receiving requests for more information to prove their identity. In May 2013, for example, a report[16] claimed that Mt. Gox (the now bankrupt Bitcoin exchange) would request customers looking to deposit or withdraw currencies to show government-issued identifying documents and a utility bill. Mt. Gox placed this statement on its website:

> "The Bitcoin market continues to evolve, as do regulations and conditions of compliance for Mt. Gox to continue bringing secure services to our customers. It's our responsibility to provide a trusted and legal exchange, and that includes making sure that we are operating within strict anti-money laundering rules and preventing other malicious activity."

These requirements do not provide the level of anonymity that some of those purchasing virtual currencies on FinCEN-registered exchanges desire, leading to the advent of services as depicted in Figure 10.

Word of caution

Gambling platforms, and especially unlicensed gambling sites, may seem enticing due to the level of anonymity they offer, but their propensity to not pay causes significant concern to money launderers. Clone websites are in operation, and customers may not be aware of potential scams. "The Hidden BetCoin" and "Tor BetCoin," for example, are identical with the exception of the warning presented in Figure 10.

Figure 10: A warning of clone gambling websites within the TOR network.

In addition to seeing warnings, money launderers posing as gamers face challenges getting paid from some underground gambling sites. Discussions on forums show multiple users complaining of not having their winnings paid into their Bitcoin wallets, with comments such as "I bet. Was paid 1x, but I have approx – 12 wins that have not paid out."

Follow McAfee Labs

Greater collaboration between law enforcement agencies to target unlicensed gambling sites is required, particularly with those that operate outside the visible Internet.

ADDRESSING THE ISSUE

Given the growing and ever-changing landscape of online gambling players and enablers, those working to apprehend cybercriminals must have a variety of skills and perspectives into this extensive money-laundering infrastructure. These actors must be able to leverage cross-sector/border and public-private partnerships, combining the capabilities of law enforcement, ISPs, Internet security companies, independent monitoring organizations, academia, and the financial institutions ultimately in receipt of suspicious fund transfers.

The work undertaken at Europol's European Cybercrime Centre is a good example of how strong global collaboration efforts with other agencies and the private sector can help address this growing threat.[17] These efforts include:

- **Data fusion:** The gathering and processing of information on cybercrime, and maintaining technical expertise for law enforcement in all member states.
- **Operations:** Providing member states with the technical, analytical, and forensic expertise required to conduct cybercrime investigations.
- **Local/global partnerships:** Facilitating law enforcement cooperation with partners within and outside the member community, and coordinating complex transnational cases in close collaboration with organizations such as Interpol, Eurojust (EU agency for judicial cooperation), European Union Cybercrime Taskforce, and European Cybercrime Training and Education Group.
- **Strategy:** Producing threat assessments, including trend analyses and forecasts as well as new developments on cybercriminal activity and functional processes.
- **Training and awareness:** Collaborating closely with organizations such as police academies to develop training activities and generally raise cybercrime awareness among trainees, as well as informing and building capacity among law enforcement officials, judges, and prosecutors.
- **Research and development:** Developing forensic tools to enable member states to more effectively detect and prosecute cybercriminals.

Although the legal framework can define the requirements for licensed operators, greater collaboration between law enforcement agencies to target unlicensed sites is required, particularly with those that operate outside the visible Internet (such as those that operate on TOR). Only with a strong online law enforcement capability can we prevent cybercriminals from getting paid and getting away with it. The work undertaken at the European Cybercrime Centre is a good example of how strong global collaboration efforts with other agencies and the private sector can help tackle this growing threat.

Follow McAfee Labs

CONCLUSION

Online gambling sites—licensed and unlicensed—are growing in popularity. More games, more access, and more transaction methods are resulting in greater opportunities for would-be criminals to hide their illicit gains from the prying eyes of global law enforcement agencies.

Without a means to cash out, the volume of cybercrime would decrease. However, the anonymous online money-laundering marketplace today is growing rapidly with the volume of attacks. Although requiring licenses for gambling operators is an important approach, this step does nothing to halt the tide of unlicensed operators.

ABOUT THE AUTHORS

Charles McFarland is a senior MTIS research engineer at McAfee in North America. He has been in the security industry for eight years, primarily focused on encryption technologies, data analysis, and cybercrime. McFarland operates in the McAfee Threat Intelligence Service, building analysis tools for threat and vulnerability data as well as providing data correlation. He has worked on intelligence gathering applications using AI technologies such as NLP and is a member of the Association for the Advancement of Artificial Intelligence. You can follow Charles McFarland on Twitter at http://twitter.com/CGMcFarland.

François Paget is a senior researcher and one of the founding members of McAfee Labs. He has identified and analyzed new threats, and has created countersteps to detect and eliminate them. Today, Paget conducts a variety of forecast studies and performs technological monitoring for McAfee and its clients. He focuses particularly on the various aspects of organized cybercrime and the malicious use of the Internet for geopolitical purposes. Paget is active in various partnership actions with French and international authorities involved in fighting cybercrime. You can follow François Paget on Twitter at http://twitter.com/FPaget. http://blogs.mcafee.com/author/Francois-Paget.

Raj Samani is vice president and CTO, Europe, Middle East, and Africa for McAfee. He is an active member of the information security industry through his involvement with numerous initiatives to improve the awareness and application of security in business and society. Samani has worked across numerous public sector organizations in many cybersecurity and research-orientated working groups across Europe. He is the author of the recently released Syngress book *Applied Cyber Security and the Smart Grid*. Samani is currently the Cloud Security Alliance's strategic advisor for EMEA and is also on the advisory council for the Infosecurity Europe show, *Infosecurity Magazine*, an expert on both searchsecurity.co.uk and the Infosec portal, and regular columnist for *Computer Weekly*. You can follow Raj Samani on Twitter at http://twitter.com/Raj_Samani.

Tweet about this report

Follow McAfee Labs

ABOUT McAFEE

McAfee, part of Intel Security and a wholly owned subsidiary of Intel Corporation (NASDAQ: INTC), empowers businesses, the public sector, and home users to safely experience the benefits of the Internet. The company delivers proactive and proven security solutions and services for systems, networks, and mobile devices around the world. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique global threat intelligence network, McAfee is relentlessly focused on keeping its customers safe.

http://www.mcafee.com

1 http://www.mcafee.com/us/resources/white-papers/wp-cybercrime-exposed.pdf

2 http://www.bwinparty.com/AboutUs/OurMarkets/The%20online%20gaming%20market.aspx

3 http://www.mcafee.com/us/resources/white-papers/wp-digital-laundry.pdf

4 http://www.fbi.gov/about-us/investigate/vc_majorthefts/bankrobbery

5 http://stopinternetgambling.com/wp-content/uploads/2014/01/FBI_Online-Gambling_Response-to-Congressman-Young_093013.pdf

6 https://www.europol.europa.eu/sites/default/files/publications/socta2013.pdf

7 http://advertising.microsoft.com/uk/WWDocs/User/en-uk/ForAdvertisers/Gambling.%20Casinos.May2011_External.pdf

8 http://odo.bo/h2report. "There's Nothing Virtual About the Opportunity in Real-Money Gambling," 2013, Odobo / H2 Gambling Capital.

9 http://online.casinocity.com/

10 http://www.igaming-monaco.com/resources/press/etude_2_addiction_gb__light_.pdf

11 http://www.wiso.uni-hamburg.de/fileadmin/bwl/rechtderwirtschaft/institut/Ingo_Fiedler/Online_Gambling_as_a_Game_Changer_to_Money_Laundering_01.pdf

12 http://www.wiso.uni-hamburg.de/fileadmin/bwl/rechtderwirtschaft/institut/Ingo_Fiedler/Online_Gambling_as_a_Game_Changer_to_Money_Laundering_01.pdf

13 http://www.coe.int/t/dghl/monitoring/moneyval/Typologies/MONEYVAL%282013%299_Onlinegambling.pdf

14 http://www.nj.com/njvoices/index.ssf/2013/11/internet_gambling_atlanti_city.html

15 http://www.coindesk.com/fincen-sends-warning-letters-unregistered-bitcoin-businesses/

16 http://www.forbes.com/sites/andygreenberg/2013/05/30/not-so-anonymous-bitcoin-exchange-mt-gox-tightens-identity-requirement/

17 https://www.europol.europa.eu/ec3

61057wp_jackpot_0414_fnl_PAIR