Secureworks®

REPORT

2017

State of Cybercrime

Exposing the threats, techniques and markets that fuel the economy of cybercriminals

Contents

Foreword 3

Introduction 4

Key Findings 5

Cybercrime

1. Business Email Compromise 7
2. Ransomware 9
3. Banking Malware 12
4. Mobile Malware 20

Criminal Landscape

5. Organized Cybercrime 22
6. Diverse Roles 23
7. Gap Between Criminality and Nation-States 25
8. Money Muling 27

Online Crime — A Market Economy

9. Commodities 30
10. Spam Botnet Usage 34
11. Exploit Kit Activity Decline 37

Conclusion 39

Glossary of Terms 40

About Secureworks 41

© 2017 Secureworks, Inc. All rights reserved.

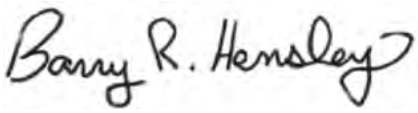
Secureworks®

Foreword

Secureworks has been tracking cybercrime activity for more than 10 years and, as we monitor this activity to protect our clients, we collect a large amount of data on both the criminals and their infrastructure and systems. This annual report presents an overview of the cybercrime landscape and trends we observed primarily from the period of mid-2016 to May 2017, in addition to a handful of other trends ranging from 2015 to 2016.

The unique and valuable intelligence shared in this report stems from the visibility gained from our thousands of clients, the machine learning and automation from our industry-leading Counter Threat Platform™, and the actionable insights from our team of elite Counter Threat Unit™ (CTU) researchers, analysts and consultants. We call this the Network Effect, and it is the unparalleled power and protection of this Network Effect which enables us to prevent security breaches, detect malicious activity in real time, respond rapidly and predict emerging threats.

Secureworks' goal in publicly sharing this report's findings is to help all organizations better protect themselves from current and emerging cyber threats; to help make them become Collectively Smarter. Exponentially Safer.™ When you can outsmart and outwit adversaries, when you can get in front of the threat, when you can anticipate, defend, predict and secure your organization, and when you can freely focus on growing and improving your organization, it's a beautiful thing. We hope that you enjoy reading.



Barry Hensley
Chief Threat Intelligence Officer for Secureworks

© 2017 Secureworks, Inc. All rights reserved.

Introduction

Day-to-day commerce increasingly relies on an interconnected web of digital processes and systems that goes largely unseen and is scarcely understood by most of the people depending on it. Exploiting this interconnectivity, and the lack of knowledge surrounding it, has turned into a big business for cybercriminals, whose nefarious Internet activities wreak financial havoc every year on companies and consumers alike. The global financial toll of cybercrime is difficult to quantify, but in the United States, the FBI reported that Internet crime led to losses in excess of $1.3 billion USD in 2016.

One way cybercriminals obtain the resources and connections they need to engage in their activities is through the Internet underground or "dark web." Definitions of the Internet underground may vary, but to Secureworks, it means the collection of Internet forums, digital shop fronts and chat rooms that cybercriminals use to form alliances, trade tools and techniques, and sell compromised data that can include banking details, personally identifiable information and other content.

It is clear, however, that the full extent of cybercrime is not visible solely through this window. Organized criminality is conducted by closed groups who have no need to advertise their intentions on Internet underground forums. Such criminals may use these forums to obtain specific tools and services, but they will conduct much of their activity away from view.

As a result, while underground forums may be a useful source of intelligence to understand some aspects of online criminality, they provide only one perspective. It is only through coupling this with directed, technical monitoring and analysis of cybercriminal toolsets that we can attempt to complete the picture.

Through these methods of collection, Secureworks CTU researchers have identified a number of ways in which cybercrime continues to present a significant risk to organizations and individuals alike, both through targeted, bespoke attacks and malware obtained on the Internet underground. As cybercrime continues to prove undeniably lucrative, it has given rise to a diverse range of threat actors, including organized cybercrime syndicates, nation-states and lone actors, with a spectrum of capabilities. This cybercrime economy is not a stagnant market — CTU researchers have found that it adapts to changes in the environment, as cybersecurity technology improves and law enforcement takes action against known threats.

To fully understand the extent of the online criminal economy, Secureworks CTU researchers blend visibility into both open and hidden criminal forums with an extensive technical monitoring capability. Analysis of activity around botnets, spam, Internet attack traffic and our massive global network of sensors reveal how changes in techniques, trends and patterns of attack are invisible to those relying solely on forum monitoring.

© 2017 Secureworks, Inc. All rights reserved.

Key Findings

From May 2016 to May 2017, Secureworks CTU researchers identified the following 11 key findings based on their observations.

Cybercrime continues to present a significant risk to individuals and organizations

1 Business email compromise (BEC) and business email spoofing (BES) accounted for $5 billion USD in losses globally, between October 2013 and December 2016. Victim's losses, related to BEC and BES schemes, increased by 2,370 percent between January 2015 and December 2016, according to figures released by the FBI.

2 Ransomware is a growing threat, and continues to offer cybercriminals a high return on investment; in 2016 alone, CTU researchers saw 200 new ransomware variants, a 122 percent increase from the year before.

3 Banking malware can be bespoke, designed to target specific institutions with a specific purpose. Often the financial malware is capable of stealing all manner of personal information, as well as banking credentials from victims.

4 Mobile malware is a significant threat and will continue to grow, with information theft and spying capabilities becoming widely available.

The online criminal landscape is complex and composed of actors with a diverse range of capabilities

5 Organized cybercrime operates like a business, perpetrated by a small number of groups who take great care not to expose their activities in online forums.

6 Within the ecosystem, there are a range of diverse roles, which are either filled from inside criminal groups or "outsourced" for efficiency.

© 2017 Secureworks, Inc. All rights reserved.

7	The perceived gap between criminality and nation-states, in terms of both actors and capabilities, will continue to shrink.
8	Money muling continues to be an integral component of the online cybercriminal landscape, although threat actors continue to diversify their cash out operations.

Online crime is a market economy

9	Personal information remains a popular commodity, with tested and verified credit card data available in some cases for as little as between $10 and $20 USD, and "fullz," or highly-detailed personal information records, are also offered for as low as $10 USD.
10	Malware-as-a-Service and the affordability of spam botnets ($200 USD per million messages) provide cybercriminals with a low barrier of entry.
11	The market adapts to changes in the environment. For example, technical improvements as well as law enforcement takedown operations have significantly impacted exploit kit usage.

© 2017 Secureworks, Inc. All rights reserved.

Cybercrime continues to present a significant risk to individuals and organizations

1

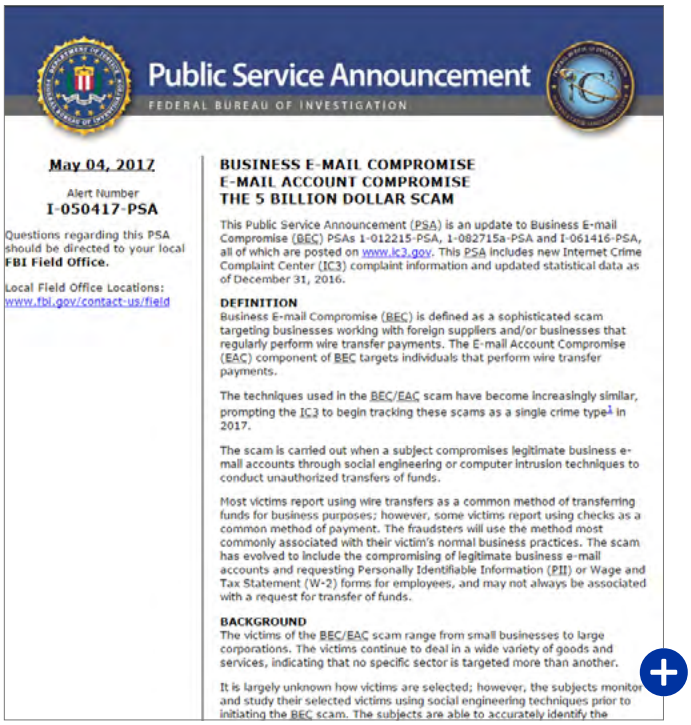
Business email compromise (BEC) and business email spoofing (BES) accounted for $5 billion USD in losses globally, between October 2013 and December 2016. Victim's losses, related to BEC and BES schemes, increased by 2,370 percent between January 2015 and December 2016, according to figures released by the FBI.

As security awareness grows, especially among companies and their employees, it becomes more challenging for cybercriminals to trick victims into conducting fraudulent transactions, downloading malware or compromising sensitive data. This becomes substantially easier if threat actors can make employees believe their request is coming from a trusted colleague or boss.

Business email spoofing (BES) and business email compromise (BEC) have become increasingly popular techniques used by threat actors to defraud victim organizations. With business email spoofing, or BES, cybercriminals send emails to employees who have access to company funds through an email account closely resembling that of a company executive. The "executive" requests the employee to authorize a money transfer to a particular account, which of course is actually owned by the cybercriminal. Although these attempts are often successful, as employees feel pressured to comply with their superior's demands and the emails usually introduce some form of time pressure, larger transactions may fall under more scrutiny and checks, causing the activity to be detected.

An alternative to business email spoofing is business email compromise, or BEC. Here, threat actors actually compromise the computer, email account or email server of the victim organization in order to intercept and alter or initiate business transactions, including direct payments on behalf of the victim organization with the money destined to financial accounts they control.

In May 2017, the FBI revealed that victims' losses related to BEC and BES schemes increased by 2,370 percent between January 2015 and December 2016 (see **FIGURE 1**). Further, they revealed that these schemes accounted for more than $5 billion USD in reported losses globally between October 2013 and December 2016.



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

May 04, 2017

Alert Number
I-050417-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office.**

Local Field Office Locations:
www.fbi.gov/contact-us/field

BUSINESS E-MAIL COMPROMISE
E-MAIL ACCOUNT COMPROMISE
THE 5 BILLION DOLLAR SCAM

This Public Service Announcement (PSA) is an update to Business E-mail Compromise (BEC) PSAs 1-012215-PSA, 1-082715a-PSA and I-061416-PSA, all of which are posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center (IC3) complaint information and updated statistical data as of December 31, 2016.

DEFINITION
Business E-mail Compromise (BEC) is defined as a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The E-mail Account Compromise (EAC) component of BEC targets individuals that perform wire transfer payments.

The techniques used in the BEC/EAC scam have become increasingly similar, prompting the IC3 to begin tracking these scams as a single crime type[1] in 2017.

The scam is carried out when a subject compromises legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

Most victims report using wire transfers as a common method of transferring funds for business purposes; however, some victims report using checks as a common method of payment. The fraudsters will use the method most commonly associated with their victim's normal business practices. The scam has evolved to include the compromising of legitimate business e-mail accounts and requesting Personally Identifiable Information (PII) or Wage and Tax Statement (W-2) forms for employees, and may not always be associated with a request for transfer of funds.

BACKGROUND
The victims of the BEC/EAC scam range from small businesses to large corporations. The victims continue to deal in a wide variety of goods and services, indicating that no specific sector is targeted more than another.

It is largely unknown how victims are selected; however, the subjects monitor and study their selected victims using social engineering techniques prior to initiating the BEC scam. The subjects are able to accurately identify the

FIGURE 1: *Business E-mail Compromise: The 5 Billion Dollar Scam (Source: FBI)*

Secureworks CTU researchers assess that these schemes will likely continue to grow in popularity due to their low barrier to entry and high payout potential.

© 2017 Secureworks, Inc. All rights reserved.

CASE STUDY

GOLD SKYLINE

In 2016, CTU researchers tracked the activities of a criminal threat group, likely of Nigerian origin, dubbed by the CTU team as GOLD SKYLINE (also referred to as "Wire-Wire Group 1").

The CTU discovered that this group had successfully compromised email accounts of several non-client organizations by using commodity Remote Access Trojans (RATs). The group then used their access to monitor each organization's communications regarding business transactions.

Whenever payment details were relayed to the payer via an invoice, GOLD SKYLINE would use their access to alter the destination bank account details and route payments to their own account.

In one particularly unfortunate case identified by CTU researchers, a U.S. chemical company unknowingly wired $400,000 to a bank account controlled by GOLD SKYLINE.

© 2017 Secureworks, Inc. All rights reserved.

2

Ransomware is a growing threat, and continues to offer criminals a high return on investment; in 2016 alone, CTU researchers saw 200 new ransomware variants, a 122 percent increase from the year before.

Over the past year, ransomware activity has dramatically increased across the world as cybercriminals have realized its relative simplicity of use and virtual untraceability. Secureworks CTU researchers observed nearly 200 new, named ransomware variants in 2016, up from 90 the year prior (see **FIGURE 2**).

CTU researchers observed nearly 200 new, named ransomware variants in 2016, up from 90 the year prior.

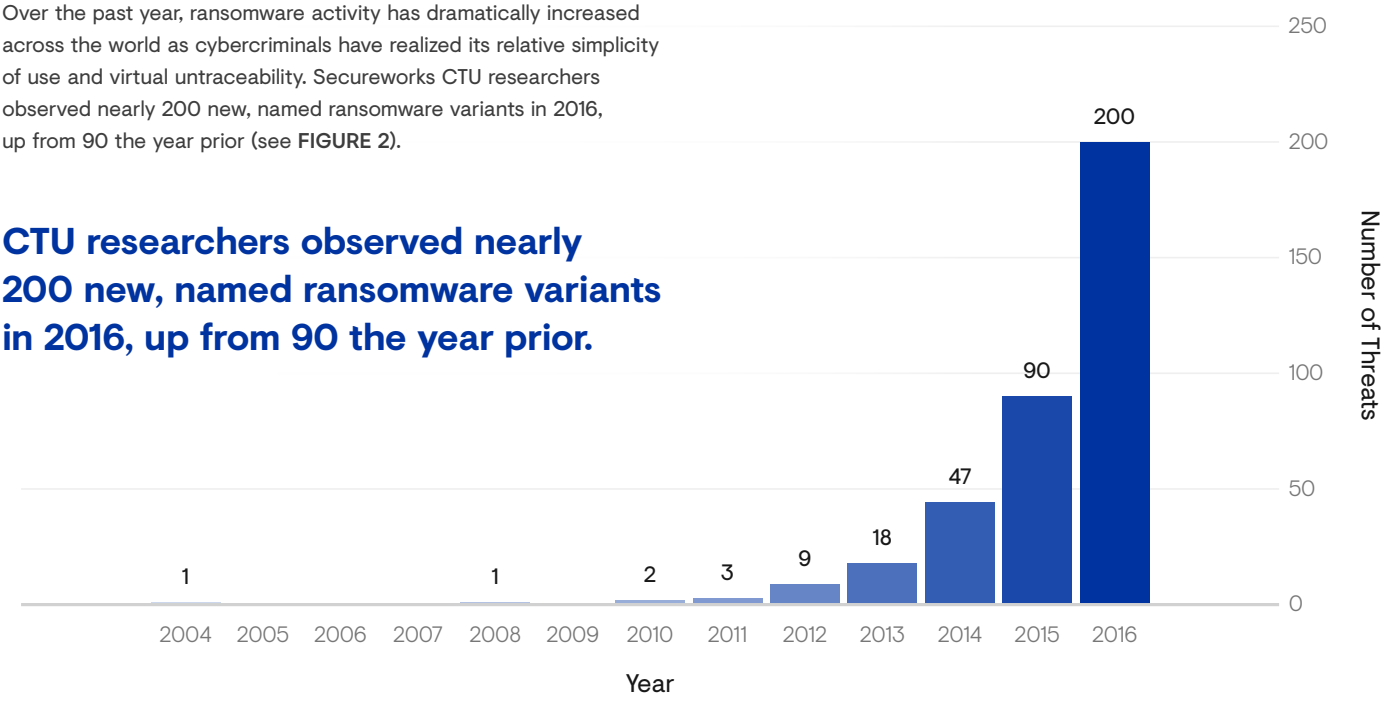


FIGURE 2: *Number of new ransomware threats per year*

Types of Ransomware

New ransomware variants generally fall into three categories:

Well-designed

Operators establish reliable distribution methods, for example spam or exploit kits and/or vibrant affiliate programs. Much like legitimate software, this ransomware typically goes through multiple release iterations.

Poorly designed

Under-resourced and/or low-skilled operators attempt but are unable to establish long-term distribution.

Rebranded

Operators generate this from kits they acquire through underground vendors or open source offerings. Each variant may have its own name or encrypted file extension, but it will function exactly like other variants developed from the same kit.

© 2017 Secureworks, Inc. All rights reserved.

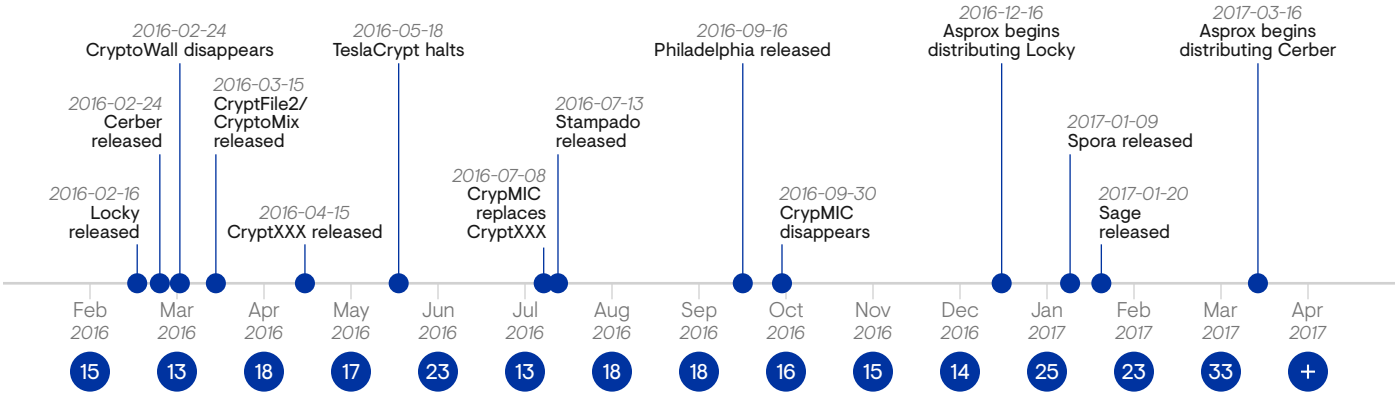


FIGURE 3: *Ransomware timeline*

The departure of several venerable ransomware families during 2016 made the year one of upheaval. After two years as the largest ransomware family by distribution, CryptoWall was withdrawn in February 2016. Shortly after in May 2016, TeslaCrypt abruptly released decryption keys for the latest variants and ceased operation.

However, they were soon replaced by the emergence of two new major families, Cerber and Locky. Cerber is sold openly through an affiliate program on semi-exclusive underground forums and became a popular replacement for CryptoWall affiliates, when that ransomware was withdrawn. Locky was the ransomware of choice for two of the larger operators of the Bugat v5 or Dridex banking botnets and added additional affiliates throughout 2016.

Both families of ransomware have been observed being distributed by the Asprox spam botnet. Asprox continued to distribute a JavaScript-based ransomware, frequently detected as "Nemucod," during the year. Asprox largely targets the U.S. with "missed overnight package" spam lures. In December 2016, Asprox's operators began distributing Locky, and in early 2017, they began distributing Cerber (see **FIGURE 3**). The Troldesh (Shade) ransomware is available as a kit, and it continued to be used to target Russia and the United Kingdom, with smaller campaigns targeting Japan. Finally, TorrentLocker, a ransomware family that emerged in 2013, continued distribution in modest volumes.

© 2017 Secureworks, Inc. All rights reserved.

An example of an openly sold "kit" ransomware is 'Stampado' (see **FIGURE 4**). In July 2016, a threat actor using the handle "The_Rainmaker" began selling the Stampado ransomware on an underground forum, advertising it as easy to use with a price of $39 USD. Stampado includes a "Russian Roulette" feature that deletes a random file from the victim's computers every six hours if the ransom is not paid.

Stampado had numerous shortcomings, including a design flaw allowing file decryption without payment. The same threat actor later began selling an updated version with the new name Philadelphia, substantially increasing the asking price from $39 to $389 USD (see **FIGURE 5**).

Arguably, the most well-known ransomware attack to date was the May 2017 large-scale campaign delivering the WCry ransomware (also known as WannaCry or WanaCryptor), which attempted to spread via a Windows Server Message Block (SMB) worm to other vulnerable systems. The worm leveraged an exploit disclosed by an online group known as Shadow Brokers who, in March 2017, released tools and other information it claims originated from the U.S. National Security Agency (NSA). Even though the WCry ransomware outbreak was contained fairly quickly after a kill switch was discovered in its code, it had a significant impact on a number of organizations which were using legacy systems or ones that had not been patched against the vulnerability it used to spread, including a number of systems within the U.K.'s National Health Service.

WCry may have been the most public ransomware outbreak to date, but it is not an isolated event. Ransomware attacks have been rife in 2016 and 2017, due in part to the malware's widespread availability and success at turning a profit for cybercriminals. The NotPetya attack of mid-2017, while not really focused on the extortion element common to other ransomware campaigns, showed that organizations continue to be vulnerable to such attacks.

FIGURE 4: *Stampado sales post*

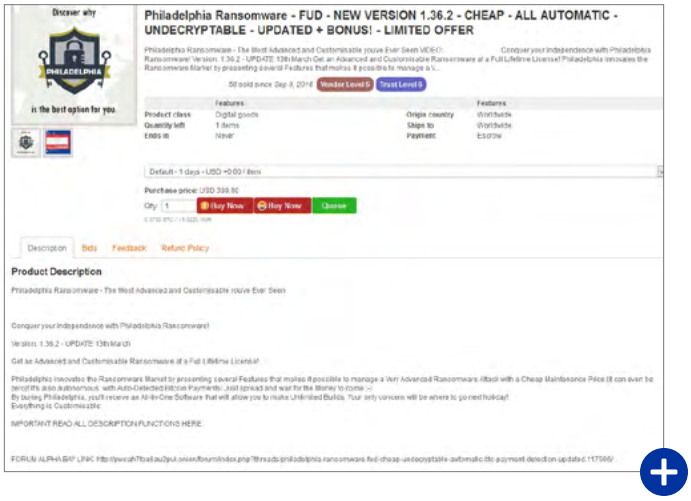


FIGURE 5: *Ransomware sales post*

© 2017 Secureworks, Inc. All rights reserved.

3

Banking malware can be bespoke, designed to target specific institutions with a specific purpose.

Banking trojans and banking malware are hallmarks of organized cybercriminal groups, who use them to facilitate large-scale fraud across the globe. These attacks range from highly-targeted intrusion activities mounted against high-value targets to massive banking trojan botnets which provide a good return on investment through achieving mass distribution.

Secureworks reverse engineers malware so as to gain an understanding of the malicious software's capability, communication mechanisms and supporting infrastructure. We also automatically retrieve and decrypt the various targeting configurations that show which financial organizations and other entities in which countries are having their customers' credentials targeted.

Secureworks' reference datasets on banking trojan configurations provide a continuous picture of targeting from 2008 to the present day. Analysis of targets in these configurations shows a focus that might be expected, such as online banking and money transfer websites. However, some less obvious targeting was also observed, for example, payroll processing portals .

A representation of the various banking trojans, giving the relative number of configurations analyzed between April 2016 and April 2017, is in **FIGURE 6**.

Each of these banking trojans can tell their own and often unique story. In this section, we take a look at the CTU team's aperture into Trickbot and Gozi ISFB banking malware.

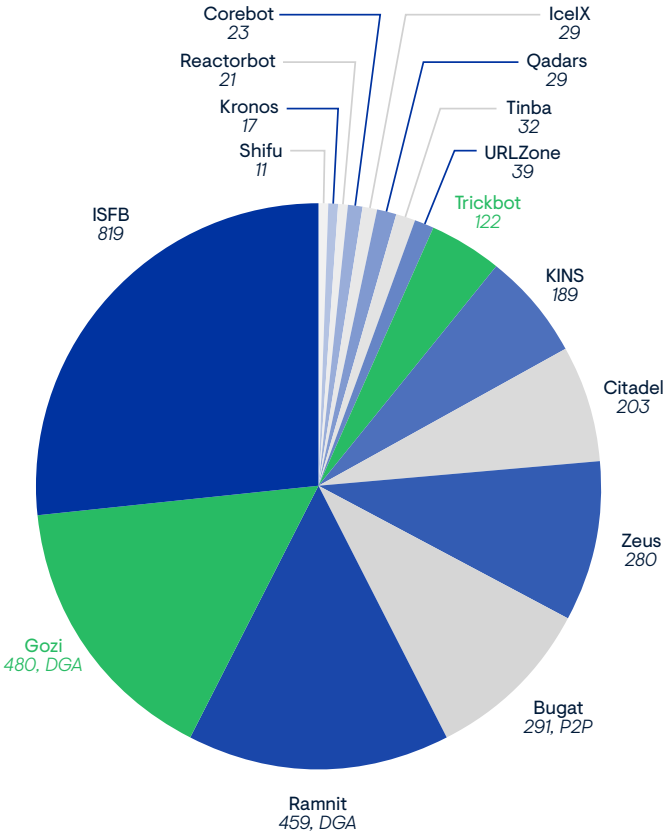


FIGURE 6: *Unique banking trojan configurations extracted April 2016 – April 2017*

© 2017 Secureworks, Inc. All rights reserved.

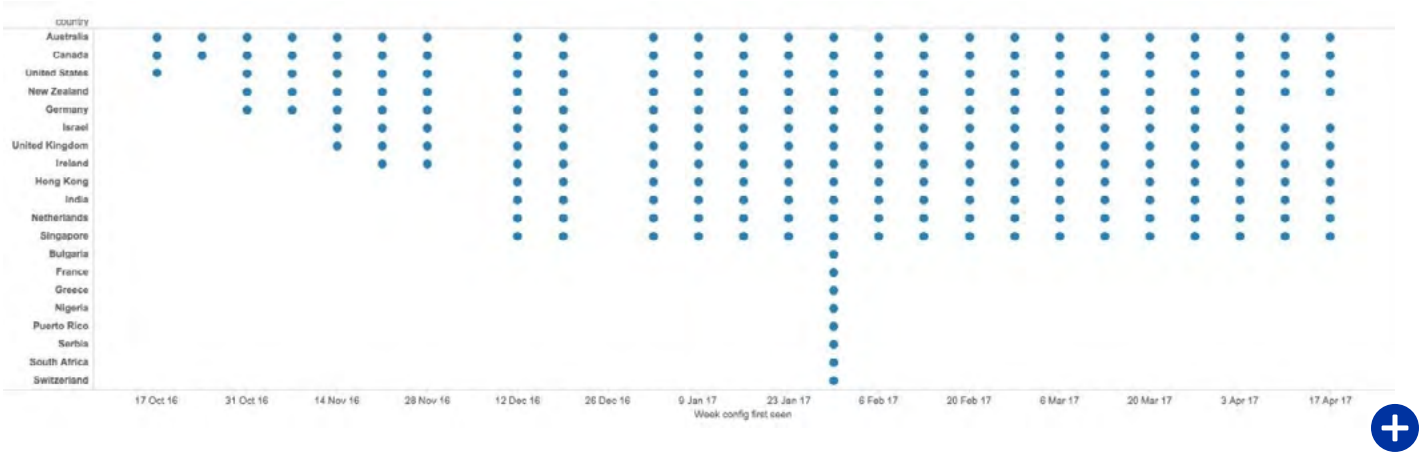


FIGURE 7: *Trickbot targeting from October 2016 to April 2017 (Source: Secureworks)*

Trickbot, a bespoke banking malware that first appeared in August 2016, is controlled by a small group of operators and is unavailable in underground or public forums. Secureworks is able to identify the individual institutions and countries being targeted by regularly interacting with command and control servers to obtain and decrypt targeting configurations. In the case of Trickbot, Secureworks CTU researchers observed threat actors conducting what appeared to be a successful test deployment targeting bank customer credentials in only Australia, Canada and the United States, before expanding targeting to 12 countries around the world. Notably, the malware structure, list of targets and TTPs of Trickbot's operators are markedly similar to those of Dyre (see **FIGURE 7**).

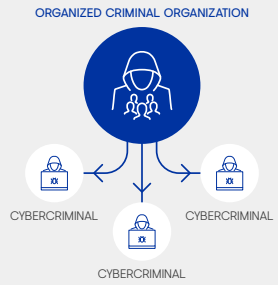
Trickbot's initial targeting of Australian banks during the "testing phase" mirrors the initial targeting behind the malware variant known as "Zloader" or "SSLZeus" that appeared in mid-2016 and spread to target bank customers globally. The initial targeting of Australian institutions may be due to the robust nature of the various malware and fraud detection and prevention mechanisms employed by Australian banks, making Australia a popular testing ground for the effectiveness of banking malware and its resultant fraud.

© 2017 Secureworks, Inc. All rights reserved.

DIAGRAM 1A: Steps, Tools and Threat Actors Involved in Online Banking Fraud

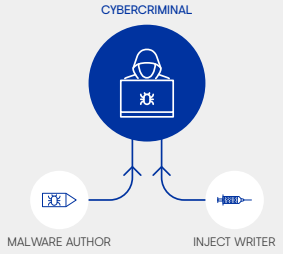
Organized criminal organizations engage in online banking fraud as one means of generating income.

1



A member of an **organized criminal organization** initiates or expands its online banking fraud operations.

2

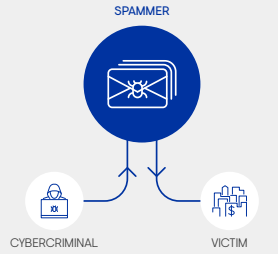


The banking **cybercriminal** coordinates the online banking fraud operation, hiring malware authors and web inject writers.

Malware authors design malicious software that will infect the computers of the victims and steal the victims' banking credentials. These credentials will be used to steal money from the victims' online accounts.

Web **inject writers** design specialized software code (inject code), which is loaded into the malicious banking malware. It is designed to mimic and to interact with the websites of specific banks. As the victims log into their bank's website, the web injects can alter payment instructions, circumvent two-factor authentication and mask unauthorized transactions from online statements.

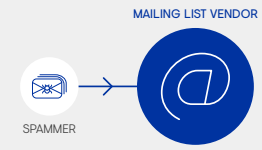
3



The banking cybercriminal pays a **spammer** to send their malware, laced with custom web inject code, as spam to potential victims.

© 2017 Secureworks, Inc. All rights reserved.

4

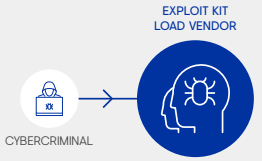


The spammer pays a **mailing list vendor** for a list of target email addresses to send the malicious spam out to.

5

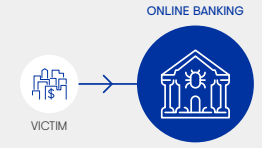
The spammer uses a spam-sending botnet to distribute the malware out to the **victims** via a phishing message. The message is designed to trick the victim into clicking on a malicious file attachment or link (the malicious file is often disguised as a receipt for an overnight delivery, a tax bill or a speeding ticket).

6



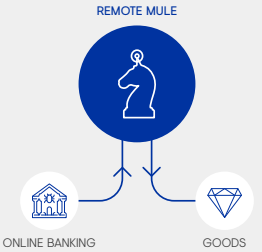
The banking cybercriminal also pays an **exploit kit load vendor,** a cybercriminal who has compromised a number of legitimate websites and installed malicious attack tools (commonly known as "exploit kits"), onto the compromised websites. The links in the spam emails direct the victim to browse to the infected websites, and if the victim's browser is vulnerable to the any of the attacks tools hosted on the site, the malware and custom web injects are downloaded onto the victim's computer.

7



When the victim logs onto their bank's website and conducts an **online banking** session, the cybercriminals can use the banking malware and web injects to spy on the banking transactions, steal the victim's usernames and passwords and alter payments being made by the victim.

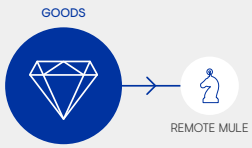
8



Using the malware, the banking cybercriminal can then transfer funds from the victim's bank account to a fraudulently-controlled bank account, located in the same country as the victim's bank account. These accounts are known as "**remote mule** accounts." Stolen funds are also often used by the remote mules to purchase high-value goods online, such as electronics, expensive fashion accessories, toys, essentially all manner of high-end goods.

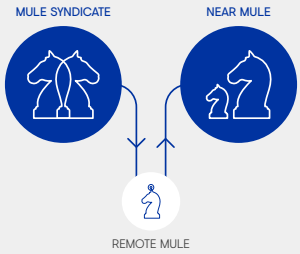
© 2017 Secureworks, Inc. All rights reserved.

9



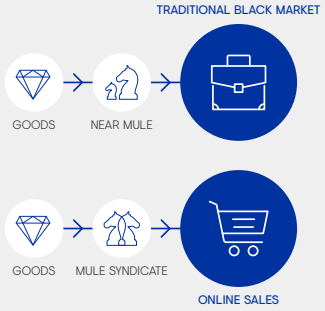
These fraudulently-purchased high-value **goods** are often sent to a remote "pack and send" or "goods remailing" mules who will take care of shipping the goods to the required destination.

10



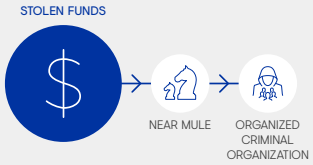
The organized criminal organization pays the **mule syndicate,** who in turn instructs the remote mule to send the stolen money and high-value goods on to a **"near mule."** A near mule typically operates in a country located close in proximity to the mule syndicate and is more trusted and is often a knowing part of the criminal operation, as opposed to the remote mule who may not know that he or she is part of a criminal operation and merely thinks they have signed up for a work-from-home job.

11



The near mule then transfers the goods to a **traditional black market** for sale. In addition, members of the mule syndicate will put the high-value goods up for sale on online retail and auction sites (Gumtree, eBay, etc.)

12



The resulting **funds** from the sale of the goods and the stolen cash are sent to the near mule. These funds are then funneled to the organized criminal organization.

© 2017 Secureworks, Inc. All rights reserved.

DIAGRAM 1B: Big Picture of Online Banking Fraud

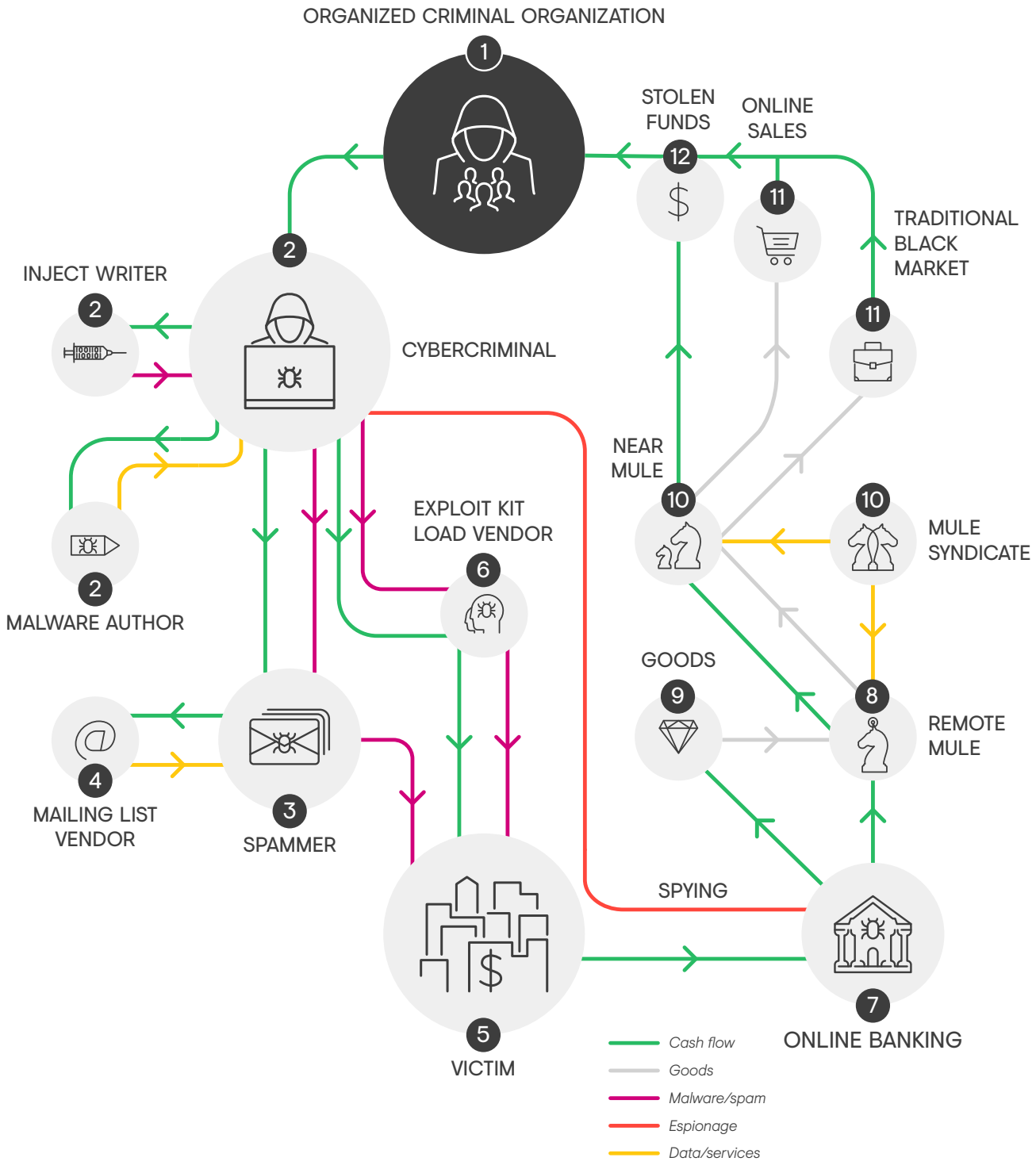


DIAGRAM 1B: (Source: Secureworks)

© 2017 Secureworks, Inc. All rights reserved.

Secureworks also tracks the targeting and distribution methods of Gozi ISFB, progeny of the Gozi malware first discovered by Secureworks in 2007. Unlike Trickbot, numerous threat actors deploy Gozi ISFB by using leaked versions of the malware source code or by purchasing the commercially supported and updated version from underground vendors. Interestingly, fewer groups leveraged this malware in 2016 than previous years, but it was used to perpetrate higher-value fraud, including repeated attempts against the same "big five" banks in Japan (see **FIGURE 8**).

For comparison, Secureworks analyzed the UK and Australian targets of Gozi ISFB and Trickbot over the last year. In both countries, Trickbot demonstrated a greater diversity of targeting. In addition to the major retail financial institutions, many smaller financial institutions — often serving a single region or municipality — were included. Furthermore, an Australian wealth management company and superannuation management provider and several small boutique UK private banks were included. These are attractive targets as their customers are wealthy and the funds are often not "checked on" by the customers as often as retail banking accounts. Trickbot also targeted an Australian funds transfer company, capable of moving money internationally. Its inclusion in the target list is likely motivated by a desire to abuse the service to move illicitly-obtained funds out of the country (see **FIGURE 9**).

Malware targeting is diverse and not limited to major banks. Wealth management companies and their high-net-worth customers are also targeted, as are payroll processing portals.

In contrast, Gozi ISFB's targeting is frequently narrower and focused on the larger retail banks. However, it is often the business banking arms of these institutions that are targeted for credential theft, as these accounts are likely to have high balances, high daily transfer limits and direct access to international funds transfers from their Internet banking website. They offer the potential for far greater criminal reward from a single fraudulent transaction than a similar fraud against a personal (retail) banking account.

FIGURE 8: *Gozi ISFB global targeting*

New Target	Goal
Recruitment sites	Recruit mules
Social network credentials	Exploit accounts and facilitate trust-based attacks
Webmail and ISP account credentials	Facilitate trust-based attacks leveraging the user's detailed correspondence history
Payroll processors	Perpetrate payment diversion or harvest PII
Account credentials of banking software creators and mobile app security developers	Future-proof their tools by better understanding targeted platforms

FIGURE 9: *While tools such as Gozi ISFB and Trickbot are predominantly used to target financial institutions, CTU researchers have seen other types of targets in their configuration files.*

© 2017 Secureworks, Inc. All rights reserved.

What's better for cybercriminals than having control over compromised debit or ATM cards? How about controlling the ATMs themselves?

Over the past year, we have seen organized criminal groups pull off several large-scale ATM jackpotting attacks, essentially infecting the ATMs across a bank's network with malware and remotely triggering them to issue millions of dollars of cash, right into the hands of their money mules. The beauty of ATM jackpotting attacks is that the money is dispensed without the need for a card or transaction. However, these high-dollar heists are not for rookies. They are carried out by extremely sophisticated organized criminal groups who develop bespoke malware and spend considerable time and resources compromising and then understanding the targeted banking network. One prime example is a massive bank heist which made news headlines in July and August of 2016.

The incident involved a cybercrime group dubbed "GOLD KINGSWOOD" by the CTU team and also referred to by some researchers as "Cobalt" (see **FIGURE 10**). GOLD KINGSWOOD successfully compromised a large number of ATMs around Europe and Asia and stole millions of dollars. Conducting these attacks required the group to leverage and coordinate not only jackpotting malware, but detailed knowledge of each bank's ATM refill schedule and an extensive ring of money mules tasked with picking up the cash at specified times.

Although Secureworks has observed specific malware for sale on the underground that claims to be able to "jackpot" an ATM (asking price $10,000 USD), even if the malware is functional, CTU researchers assess that large-scale attacks such as these will remain the purview of more sophisticated groups, who operate in private, away from underground forums, and who possess the significant technical and human resources required to pull off these major heists (see **FIGURE 11**).

FIGURE 10: *Cobalt gang headline*

FIGURE 11: *ATM malware sales post*

© 2017 Secureworks, Inc. All rights reserved.

4 Mobile malware is a significant threat and will continue to grow.

Mobile ransomware is of increasing concern. Large-scale attacks could be devastating to individual and corporate phone communications, while small-scale spyware infections would offer all manner of personal information to attackers.

Mobile devices have not been immune to the growing threat of ransomware. In fact, Secureworks CTU researchers have identified several instances of malware for sale that are advertised as being capable of spying on all functions of an Android phone, encrypting files on the device and demanding payment. The functionality detailed in **FIGURE 12** is a common feature set and is delivered via a malicious Android package kit (APK) file. This particular malware was seen advertised for around $1,000 USD on Russian-speaking forums.

Clearly, this is a less-targeted and smaller-value approach than targeting companies with ransomware, but it may also be easier to succeed, as individuals are unlikely to have the security knowledge and resources that organizations have to defend against these threats. When coupled with the rise of SMS phishing and advanced exploit kits, Secureworks CTU researchers predict that we could see a spate of attacks focused on encrypting Android phones and tablets, leaving users with no access to contacts, photos or the myriad of important "personal" functions provided by these ubiquitous devices (see **FIGURE 13**).

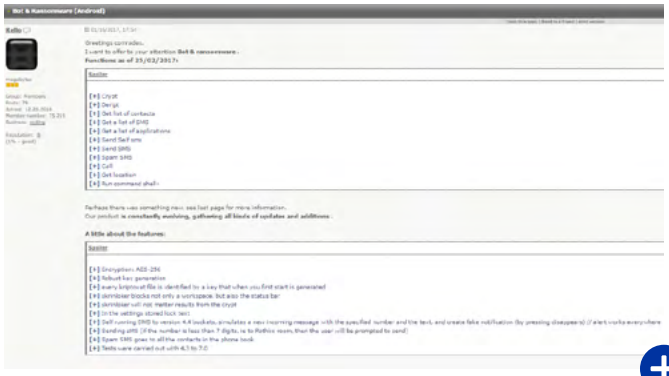


FIGURE 12: *Android bot sales post*

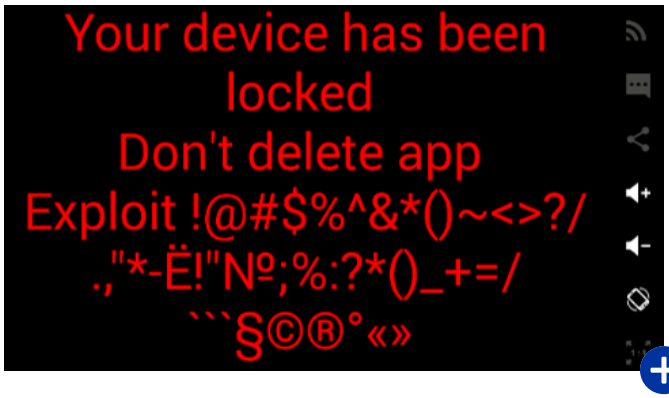


FIGURE 13: *Android ransomware lock screen in development*

© 2017 Secureworks, Inc. All rights reserved.

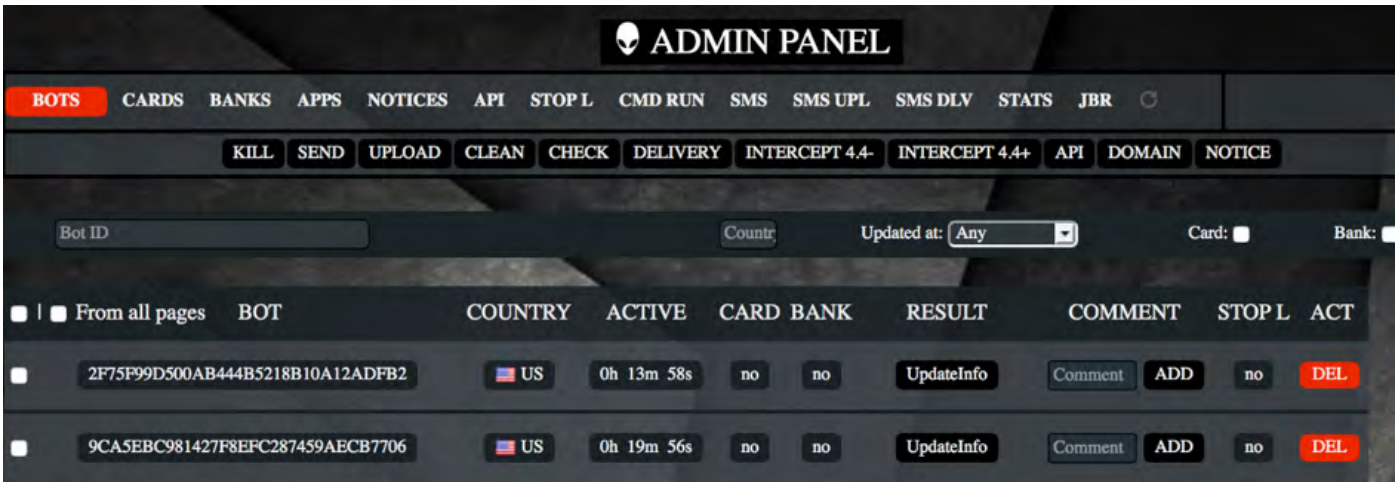


FIGURE 14: *Marcher admin panel (Source: Securify)*

Cybercriminals also continue to develop banking malware for Android devices. One such piece of malware is called "Marcher," or "Exobot," which is a banking malware and spyware combination targeting Android. This malware is being distributed through SMS spam messages purporting to be from the recipient's telephone company. Victims are lured into following a link that then downloads a malicious Android application file.

Once installed, Marcher has full access to the victim's Android device, stealing mobile banking credentials and harvesting credit card numbers where possible. Cybercriminals can control Marcher through SMS messages sent to the handset and hidden from the victim's view (see **FIGURE 14**).

CTU researchers assess that Marcher is being used by an organized, experienced threat actor or organized cybercriminal group due to its level of sophistication, the rapid, sustained distribution of the malware, and the increasing financial losses that victims are experiencing. The team expects to see an increase in the use of mobile malware, thanks to the success of Marcher and the increasing ease of obtaining and using such tools.

© 2017 Secureworks, Inc. All rights reserved.

The online criminal landscape is complex and composed of actors with a diverse range of capabilities

5

Organized cybercrime operates like a business, perpetrated by a small number of groups who take care not to expose their activities in online forums.

It is true that the Internet forums and chat rooms of the underground are used by criminals to form alliances, trade tools and techniques, and sell compromised data, such as banking details, personally identifiable information and other content. However, it is a misconception to think that this describes the totality of the cybercrime landscape.

The most sophisticated and damaging cybercrime is conducted by well-seasoned and "traditional" organized criminals. Lucrative online criminality is run like a business, controlled by organized crime groups who are focused on minimizing risk and maximizing profit. Such groups have considerable reach, will often be active in other areas of more traditional criminality, and when necessary, will employ the services of other professional criminals who specialize in certain areas, such as moving money or goods around the world. These organized criminals carry out their crimes in closed groups. They have no need to advertise their intentions on Internet forums, and take great care to maintain secrecy and minimize their profile to reduce the risk of disruption by global law enforcement.

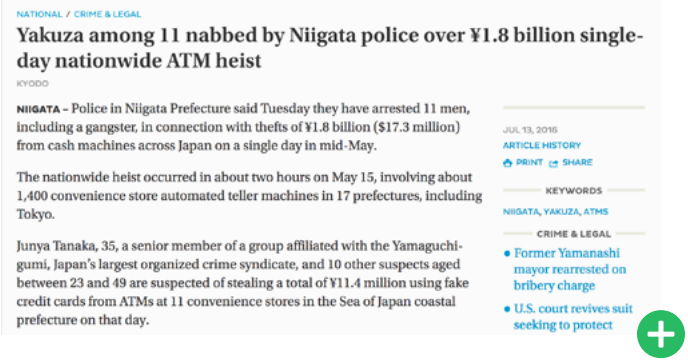
For many criminal groups, online criminality simply presents another means of generating or maximizing revenue. One prime example of a criminal group which adopted cybercrime as another method of bringing in money is the very traditional Japanese organized crime ("Yakuza") group known as the "Yamaguchi-gumi." In May 2016, a senior member of the Yamaguchi-gumi organized crime group was arrested in connection with the theft of ¥11.4 million from ATMs across Japan, as noted in **FIGURE 15**. The highly-organized and well-coordinated theft used blank ATM cards, which they overwrote with stolen card data from a South African bank. The cards were then used to make cash withdrawals at more than 1,400 ATMs across Japan in a three-hour period between 5 a.m. and 8 a.m.

These organized criminals employ good operational security and tradecraft in order to avoid attracting the attention of law enforcement. They obfuscate their communications and make their endeavors even harder to track and attribute than some of the lower-level online criminals.

Meanwhile, other organized crime groups have developed cybercrime as their main focus. However, they continue to operate along the lines of more traditional organized criminal enterprises.

In November 2016, after four years of coordinated efforts by multiple countries, five key members of the cybercriminal syndicate behind the "Avalanche" network were tracked down in Ukraine and arrested. The Avalanche network had been active since 2009 facilitating phishing attacks, DDoS attacks, malware distribution and cross-border money movement. Officials estimate the platform was responsible for hundreds of millions of dollars in fraudulent activity and victims of malware infections attributed to the Avalanche network were identified in over 180 countries.

However, according to Ukrainian news outlets, the gang's alleged ringleader, Gennady Kapkanov, attempted to resist arrest by firing his assault rifle at Ukrainian officers, before ultimately being overcome and taken into custody. Despite this violent attempt at evading arrest and the evidence of his involvement in Avalanche, a Ukrainian judge released him on a technicality. Ukrainian authorities subsequently lost track of Kapkanov, making it unclear whether he will face any consequences at all.



NATIONAL / CRIME & LEGAL

Yakuza among 11 nabbed by Niigata police over ¥1.8 billion single-day nationwide ATM heist

KYODO

NIIGATA – Police in Niigata Prefecture said Tuesday they have arrested 11 men, including a gangster, in connection with thefts of ¥1.8 billion ($17.3 million) from cash machines across Japan on a single day in mid-May.

The nationwide heist occurred in about two hours on May 15, involving about 1,400 convenience store automated teller machines in 17 prefectures, including Tokyo.

Junya Tanaka, 35, a senior member of a group affiliated with the Yamaguchi-gumi, Japan's largest organized crime syndicate, and 10 other suspects aged between 23 and 49 are suspected of stealing a total of ¥11.4 million using fake credit cards from ATMs at 11 convenience stores in the Sea of Japan coastal prefecture on that day.

JUL 13, 2016
ARTICLE HISTORY
PRINT SHARE

KEYWORDS
NIIGATA, YAKUZA, ATMS

CRIME & LEGAL
- Former Yamanashi mayor rearrested on bribery charge
- U.S. court revives suit seeking to protect

FIGURE 15: *Yakuza headline (Source: Japan Times)*

© 2017 Secureworks, Inc. All rights reserved.

6

Within the ecosystem, there are a range of diverse roles.

As with any business, attracting and retaining the right talent is important for organized cybercriminal enterprises. This need has created an underground job market requiring a diverse range of skills, which derive compensation based on their availability and demand. Here is a list of several of the principal cybercrime actors.

Criminal Actors and Responsibilities

"Traditional" Organized Cybercriminals

These criminals work for sophisticated, organized crime groups, and focus on cybercrime. The top online crime groups run a strict business, and the group leaders seek out experts to work in the various parts of their operation. They are totally focused on minimizing risk and maximizing profit, thus you will never see them conducting business out in the open on Internet forums.

Money Mules

These are often unwitting people who receive the stolen monies or goods, and then transfer them out of their country and ultimately into the hands of the criminal, often via a local or "nearside" mule who is trusted by the criminal.

Malware Author/Writer

The malware author/writer codes the malicious software that will be used to infect the computer of the unwitting victims and steal (among other things) their banking credentials, which are then used to steal their money.

Inject Writer

The inject writer codes the specific pieces of individual code (known as "injects") that are loaded into the malware in order to mimic and interact with the websites of specific banks, as victims log in to their online banking site and carry out their normal banking. Injects are the most important part of this type of banking malware, as a well-written inject can alter payment instructions, use social engineering tricks to circumvent two-factor authentication and mask unauthorized transactions from online statements, leaving victims almost helpless to detect or stop the theft themselves without calling their bank or relying on paper statements.

Exploit Kit Load Vendor

Exploit kit load vendors will use their collection of often legitimate websites that have been hacked to include malicious attack tools called "exploit kits," and they will attempt to force the victim's web browser to download and install the malware that the cybercriminal pays them to distribute. Cybercriminals will pay exploit kit load vendors per number of victims that their malware is installed on using the exploit kits.

© 2017 Secureworks, Inc. All rights reserved.

Network and System Administrators

Network and system administrators support the organization's botnet-related revenue streams (DDoS, spam distribution, malware deployment) by "bot herding," gaining control over a large number of distributed computing resources. They maintain command and control and other infrastructure for ransomware campaigns, banking trojans and exploit kits.

Data Processing Specialists

These data processing specialists triage large amounts of data that the organization collects, including information on compromised devices, stolen bank details and other personal information. They are also tasked with identifying the value in this data and producing the output in a sellable format.

Network Exploitation Specialists

These specialists are responsible for deploying and using tools to maintain undetected access within a victim's network over a long period of time. This may require innovative problem solving, and the development of new tools and solutions to achieve their objectives.

Service Providers

Service providers support smaller organizations on a contract basis. Responsibilities vary by service type.

Bulletproof Hosting — Resisting attempts by local law enforcement to investigate customer organizations.

Counter Anti-Virus (CAV) — Reviewing malware to ensure that existing anti-virus technologies will not detect it.

Cybercriminal Recruitment

Some cybercriminal role recruitment takes place on the Internet underground, with a significant proportion of forum posts advertising for people with certain skillsets or connections. However, organized cybercriminal groups often avoid advertising or accepting positions on underground forums. Once a certain level of sophistication and experience is reached, threat actors are more likely to work with people they already know and trust.

© 2017 Secureworks, Inc. All rights reserved.

7

The perceived gap between criminality and nation-states, in terms of both actors and capabilities, will continue to shrink.

As mentioned above, members of organized crime groups cooperate and communicate in closed channels, and in some cases these groups occupy the same office space. In countries like Russia, where the line between nation-state cyber activity and cybercrime has long been blurred, organized crime groups are afforded a degree of patronage that likely includes some protection of operational infrastructure.

Indeed, lines may even be blurred further. Evgeniy Bogachev, a long-time resident on the FBI's most wanted list, created a sub-network from his infamous Gameover Zeus botnet that was dedicated exclusively to espionage. Gaining insight into highly-organized and sophisticated online criminal activity is impossible to achieve if one solely monitors underground forums. Secureworks researchers have a long history of working with international law enforcement agencies and industry partners on high-level, anti-malware operations which aim to stifle criminal success, garner valuable insight into the murky world of cybercrime and protect the world from these digital threats.

© 2017 Secureworks, Inc. All rights reserved.

CASE STUDY

North Korea associated with the theft of $81 million USD from the Bangladesh central bank

A stark example of how the line between nation-state cyber activity and cybercrime has blurred is exemplified by the activities of a cyber threat group, dubbed Nickel Gladstone by CTU researchers and popularly known as Lazarus Group. Between 2015 and 2017, NICKEL GLADSTONE targeted several large banking networks in an apparent attempt to steal funds. In January 2016, the group compromised the network of the Bangladesh central bank and attempted to conduct fraudulent SWIFT transactions.

The attackers appear to have had extensive awareness of the SWIFT transfer processes, based on the malware they developed to hide their fraudulent transactions from the Bangladesh central bank employees. Their familiarity with the system is also evidenced by the fact that they were able to customize their tools to the victim's environment during the intrusion.

Approximately $81 million USD was reportedly transferred to, and later liquidated from, accounts used by the NICKEL GLADSTONE group. The stolen funds were later transferred through casinos in the Philippines, in what appears to be a sophisticated money-laundering operation.

Secureworks CTU researchers have also found evidence that NICKEL GLADSTONE attempted to defraud accounts owned by a commercial bank in Vietnam, and in late 2016, used Strategic Web Compromises (SWC) of financial websites in Poland and Mexico to deliver malware to specific global organizations.

CTU researchers have identified several technical links between this group's activity and cyber capabilities strongly associated with the North Korean government. The apparent nation-state involvement in cyber-enabled criminal activity represents a notable shift in the threat landscape.

CTU researchers assess with moderate confidence that the NICKEL GLADSTONE group poses an ongoing and credible threat to global banking networks.

© 2017 Secureworks, Inc. All rights reserved.

8

Money muling continues to be an integral component of the online criminal landscape, although criminals continue to diversify their cash out operations.

Most cybercrime is perpetrated in an effort to make money, so cybercriminals have to be able to turn stolen financial data, such as online banking credentials and credit card details, into physical cash or goods. This step is often risky, so experienced criminals minimize their own risks by using "money mules" to do this work. Mules are either knowing or unknowing accomplices who receive the stolen funds or high-value goods, and then transfer them on through a distribution chain out of their country and eventually into the hands of the cybercriminal.

Cybercriminal groups may advertise for money mule positions on the Internet underground, as seen in **FIGURE 16**, and sometimes other threat actors will volunteer to open a bank account and receive stolen funds in exchange for a percentage of those funds or a flat fee, as seen in **FIGURE 17.** In this way, cybercriminals who are not as technically capable can fill a niche by offering a different service.

However, the proverb that "there's no honor among thieves" is often at the forefront of a criminal's mind when engaging mules on forums, as these forums often feature "trust rating" systems and specific message boards dedicated to grievances and outing so called "rippers" — individuals who have been deemed untrustworthy. More sophisticated and experienced organized criminal groups will make use of the services of specific mule recruitment groups that specialize in recruiting, grooming and organizing unwitting members of the public, rather than using other criminals to receive the initial stolen funds.

To this end, CTU researchers have found that mule recruitment campaigns often use phrases such as "work-from-home," "accounts payable," "financial controller" or "reshipping specialist" to mislead potential mules into thinking they are applying for an above-board work-from-home job. Applicants are told the job responsibilities entail receiving money or high-value goods and forwarding those funds or goods to a third party, keeping around five percent of the total amount as their salary. Cybercriminals go so far as to utilize employment application forms, contracts and over-the-phone interviews to make the job appear even more legitimate. The CTU research team has also identified cybercriminals purchasing or using malware to steal credentials for job recruitment websites in order to find job-hungry candidates to contact and hopefully recruit.

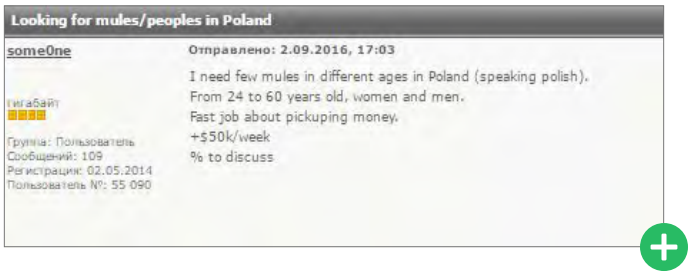


FIGURE 16: *Seeking Polish mules*

FIGURE 17: *Offering money transfer*

To gain more insight into how money mules are recruited, see **DIAGRAM 2** >

© 2017 Secureworks, Inc. All rights reserved.

DIAGRAM 2: Money Mule Recruitment Process

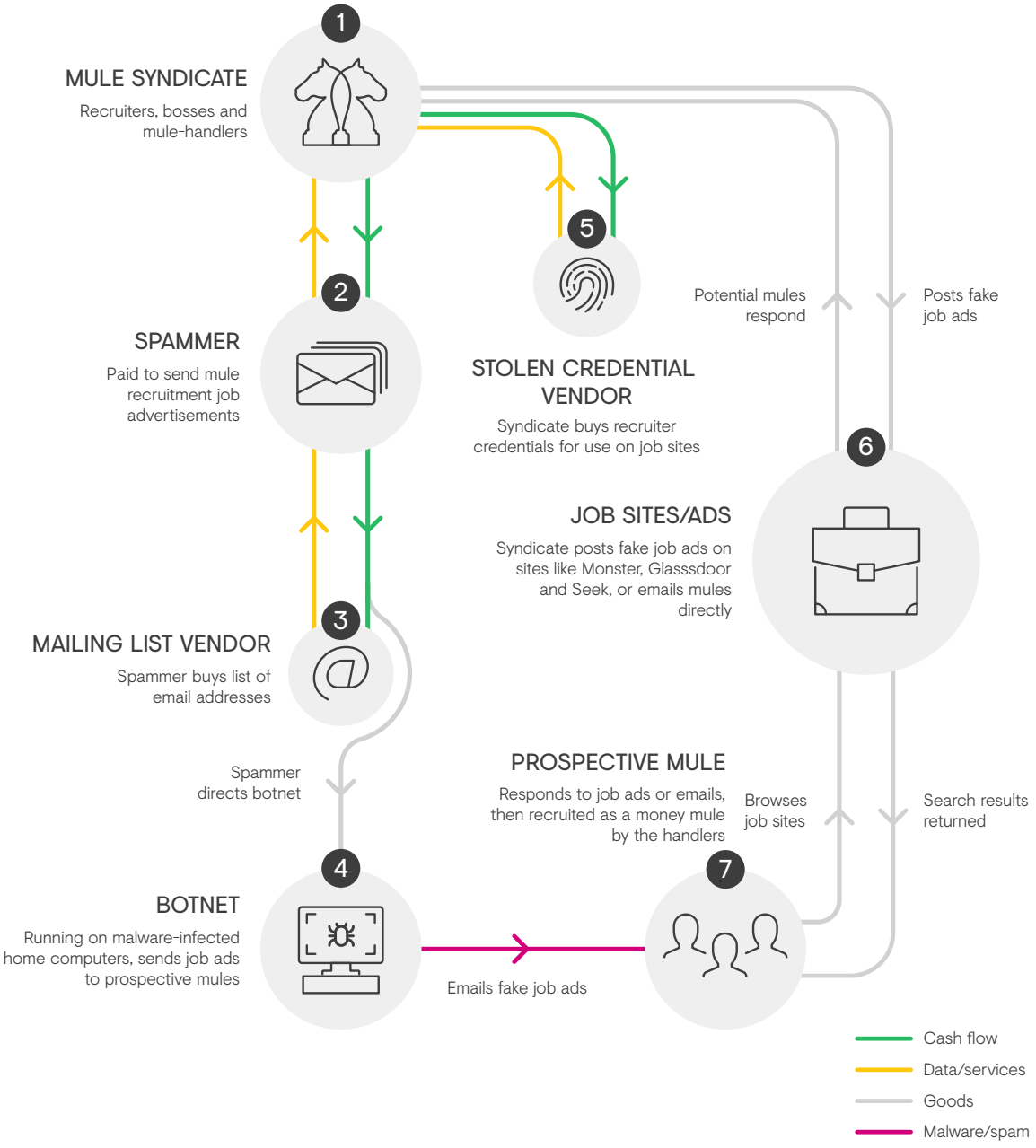


DIAGRAM 2: (Source: Secureworks)

© 2017 Secureworks, Inc. All rights reserved.

For cybercrime groups intent on stealing large dollar amounts, they might also purchase complete documentation for legitimate business banking accounts and associated documentation, as seen advertised in **FIGURE 18** for $2,200 USD. These accounts are typically authorized to receive and transfer more funds per transaction than individual personal accounts, making it easier to transfer large amounts of money in a short period of time. Cybercriminals' favorite options are accounts whose banks or countries of residence are known to be slow in returning funds identified as stolen, giving the attackers extra time to move the funds to another account, often in another country.

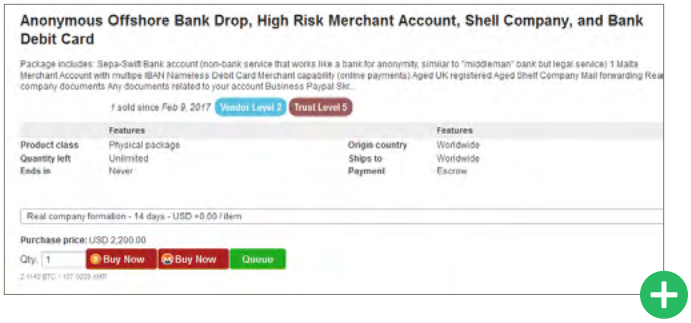


FIGURE 18: *Full money transfer service*

Bitcoin laundering using tumbling, mixing and coin laundering

As previously mentioned, money muling continues to be a key component for many online criminal enterprises. However, the use of virtual currency and its every increasing popularity has given cybercriminals additional options for their cashing out operations.

In fact, one reason ransomware activity has dramatically increased across the world is the ease with which ransom payments can be made in Bitcoin. By accepting victim payments in Bitcoin, criminals can reduce the need for money mules, lowering overhead and risk, particularly when the Bitcoin is "cleaned" through services like "tumbling," "mixing" and "coin laundering."

These services have given criminal users of Bitcoin an additional layer of protection from identification, mixing funds obtained from crime with "clean" funds in order to obfuscate the source and break the trail to the end user. Numerous third parties advertise these services, and they are often only accessible through TOR.

© 2017 Secureworks, Inc. All rights reserved.

Online crime is a market economy

9

Personal information remains a popular commodity, with tested and verified credit card data available in some cases for as little as between $10 and $20 USD, and "fullz," or highly-detailed personal information records, also offered for as low as $10 USD.

Since the day consumers began making purchases on the Internet, credit card data has been a popular target for cybercriminals. Credit card sales are ubiquitous on the Internet underground, with stolen card data from across the world being offered at fractions of a USD for unverified bulk orders. But as retailers and financial institutions have collectively improved their ability to mitigate credit card breaches and their consequences to the victims, it is no longer the cybercriminals' goal to simply get their hands on bulk, unverified credit card data.

Like anyone else, cybercriminals prefer to know what they are getting for their money. Tested and verified high-balance cards from around the world may be offered for between $10 and $20 USD a piece (see **FIGURE 19**). This is a small price to pay, considering the potential gain attackers can extort from unsuspecting victims.

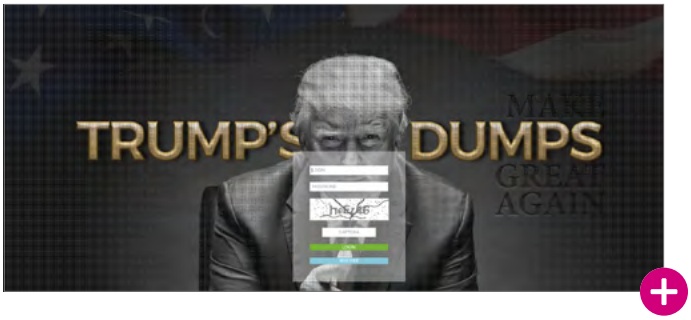


FIGURE 19: *Trump's Dumps offers cards from the U.S., Japan, South Korea and other countries for between $10 and $20 USD each, with refunds offered in case of a "bad card" that has been blocked by the bank already and cannot be used for fraud.*

© 2017 Secureworks, Inc. All rights reserved.

According to CTU researchers, to make this process more efficient, sellers often use Automated Vending Carts (AVCs), which are similar to the shopping carts used by legitimate online retailers. AVCs allow a customer to create an account with the seller and buy specific card details through an automated system. AVCs used to be run by lower-level cybercriminals who sold credit card data they purchased cheaply from other threat actors. However, these unverified cards often proved to be worthless, as many of them had already been used by the attacker who originally acquired them or by another criminal, as credit card details can at times pass through several sets of hands on their way to the AVC vendor. Another situation witnessed by the CTU researchers is where the card data is sold to multiple criminals at the same time and thereafter cancelled by the victim.

Recently, CTU researchers have seen AVCs increasingly offer large numbers of pre-verified card details, along with more personal information about the real owners of the cards, providing a more quality "product" for purchasers. Many AVCs offer full or partial refunds if the purchased cards are not usable or have a low credit balance.

Today's AVCs accept digital currencies such as Bitcoin for payment, and allow the buyer to select cards according to their Bank Identification Number (BIN), name and address/location of the credit card owner or the card's available balance, as seen in **FIGURES 20** and 21. These details can help the buyer evade detection when making fraudulent purchases with the card. In addition to purchasing card data, criminals can also purchase ready-to-clone magnetic strip data for writing to a blank card.

In order to make a purchase, the buyer applies filters and the AVC returns a list of available cards that match the buyer's requirements. The purchaser then selects the cards they want, sometimes also entering a desired quantity, and as long as there are sufficient funds in the buyer's account, the AVC "vends" the cards by displaying the full details on the screen for copying or downloading.

FOUND: 98574

BIN	Base	Country	State	City	ZIP	Name	Card	Level	Type	Tracks	Code	Bank	Price $
3791836	no refund 20.03_KR201_95%	KR					AMERICAN EXPRESS		C	TR2	201		9.5
4980129	no refund 16.03_JAPAN_TR2_95%	JP					VISA	classic	C	TR2	201		12.5
4670085	no refund 20.03_KR201_95%	KR					VISA	classic	C	TR2	201		12.5
4980013	no refund 16.03_JAPAN_TR2_95%	JP					VISA	classic	C	TR2	201		12.5
4784311	refund available 03.04.US_95%	US	MA	Berlin	01503		VISA	classic	C	TR2	201		10
4518424	no refund 20.03_KR201_95%	KR					VISA	classic	C	TR2	201		12.5
4635060	refund available 08.03.MIX_TR1TR2_95%	US	MA				VISA	prepaid	D	TR1+TR2	121		9.5
4400667	refund available 08.03.MIX_TR1TR2_95%	US	MA	Berlin	01503		VISA	signature	C	TR1+TR2	201		9.5
4313076	refund available 08.03.MIX_TR1TR2_95%	US	MA				VISA	signature	C	TR1+TR2	201		9.5
4682712	refund available 08.03.MIX_TR1TR2_95%	US	MA				VISA	prepaid	D	TR1+TR2	101		9.5
4842242	refund available 08.03.MIX_TR1TR2_95%	US	MA	Berlin	01503		VISA	prepaid	D	TR1+TR2	121		9.5
5310701	no refund 20.03_KR201_95%	KR					MASTERCARD	gold	C	TR2	201		20
4868960	refund available 08.03.MIX_TR1TR2_95%	US	MA	Berlin	01503		VISA	platinum	C	TR1+TR2	201		12.5
4868960	refund available 08.03.MIX_TR1TR2_95%	US	MA	Berlin	01503		VISA	platinum	C	TR1+TR2	201		12.5
4670085	no refund 20.03_KR201_95%	KR					VISA	classic	C	TR2	201		12.5
4518425	no refund 20.03_KR201_95%	KR					VISA	classic	C	TR2	201		12.5
4330280	no refund 20.03_KR201_95%	KR					VISA	platinum	C	TR2	201		16.5
4028570	no refund 20.03_KR201_95%	KR					VISA	classic	C	TR2	201		

FIGURE 20: *AVC card sales*

Bin	Type	Country	Bank name	Level	Brand	Name	Expire	City	Zip	Address
454742	DEBIT	UNITED KINGDOM		CLASSIC	VISA		2019/10	–	SG8 0QR	
454313	DEBIT	UNITED KINGDOM		CLASSIC	VISA		2020/11	–	35508	
371783	CREDIT	UNITED KINGDOM		PLATINUM	AMERICAN EXPRESS		2022/02	–	WD6 3RH	
446292	DEBIT	UNITED KINGDOM		CLASSIC	VISA		2018/05	–	EH53JR	
465844	DEBIT	UNITED KINGDOM		CLASSIC	VISA		2018/02	–	DT3 4BG	
475128	DEBIT	UNITED KINGDOM		CLASSIC	VISA		2018/11	–	NL7 9GL	
475129	DEBIT	UNITED KINGDOM		CLASSIC	VISA		2020/02	–	M130rk	
379196	CREDIT	UNITED KINGDOM		–	AMERICAN EXPRESS		2019/06	–	GU22 0NS	
557366	DEBIT	UNITED KINGDOM	–	–	MASTERCARD	–	2019/05	–	wa16 7lq	
446238	DEBIT	UNITED KINGDOM		CLASSIC	VISA		2018/10	–	S72GQ	
454742	DEBIT	UNITED KINGDOM		CLASSIC	VISA		2020/04	–	RM12 4TY	
529932	CREDIT	UNITED KINGDOM		STANDARD	MASTERCARD		2017/11	–	CR2 8LH	
371783	CREDIT	UNITED KINGDOM		PLATINUM	AMERICAN EXPRESS		2019/03	–	–	–
456735	DEBIT	UNITED KINGDOM		CLASSIC	VISA	I	2020/11	–	SE4 2BQ	
475130	DEBIT	UNITED KINGDOM		CLASSIC	VISA		2019/10	–	TW9 4BZ	
465942	DEBIT	UNITED KINGDOM		CLASSIC	VISA		2018/01	–	s63 8ns	
454313	DEBIT	UNITED KINGDOM		CLASSIC	VISA		2018/04	–	NG19 9AN	
446274	DEBIT	UNITED KINGDOM		CLASSIC	VISA		2019/02	–	ss71lf	
454638	CREDIT	UNITED KINGDOM		CLASSIC	VISA		2019/09	–	Dt3 6pb	
454638	CREDIT	UNITED KINGDOM		CLASSIC	VISA		2017/05	–	GL7 5HN	
529930	CREDIT	UNITED KINGDOM		STANDARD	MASTERCARD		2019/04	–	DY3 1HJ	
456726	DEBIT	UNITED KINGDOM		CLASSIC	VISA		2018/08	–	B49 6RD	
374614	CREDIT	UNITED KINGDOM		PREMIUM PLUS	AMERICAN EXPRESS		2019/05	–	LE8 0NA	

FIGURE 21: *UKDumps offers UK cards with the physical address associated with the person who owns the card $9 – 11 USD each and offers no refunds.*

The way in which stolen credit card is sold and monetized by criminals is further illustrated in **DIAGRAM 3** >

© 2017 Secureworks, Inc. All rights reserved.

DIAGRAM 3: Steps and Threat Actors Involved in Monetizing Stolen Credit Card Data

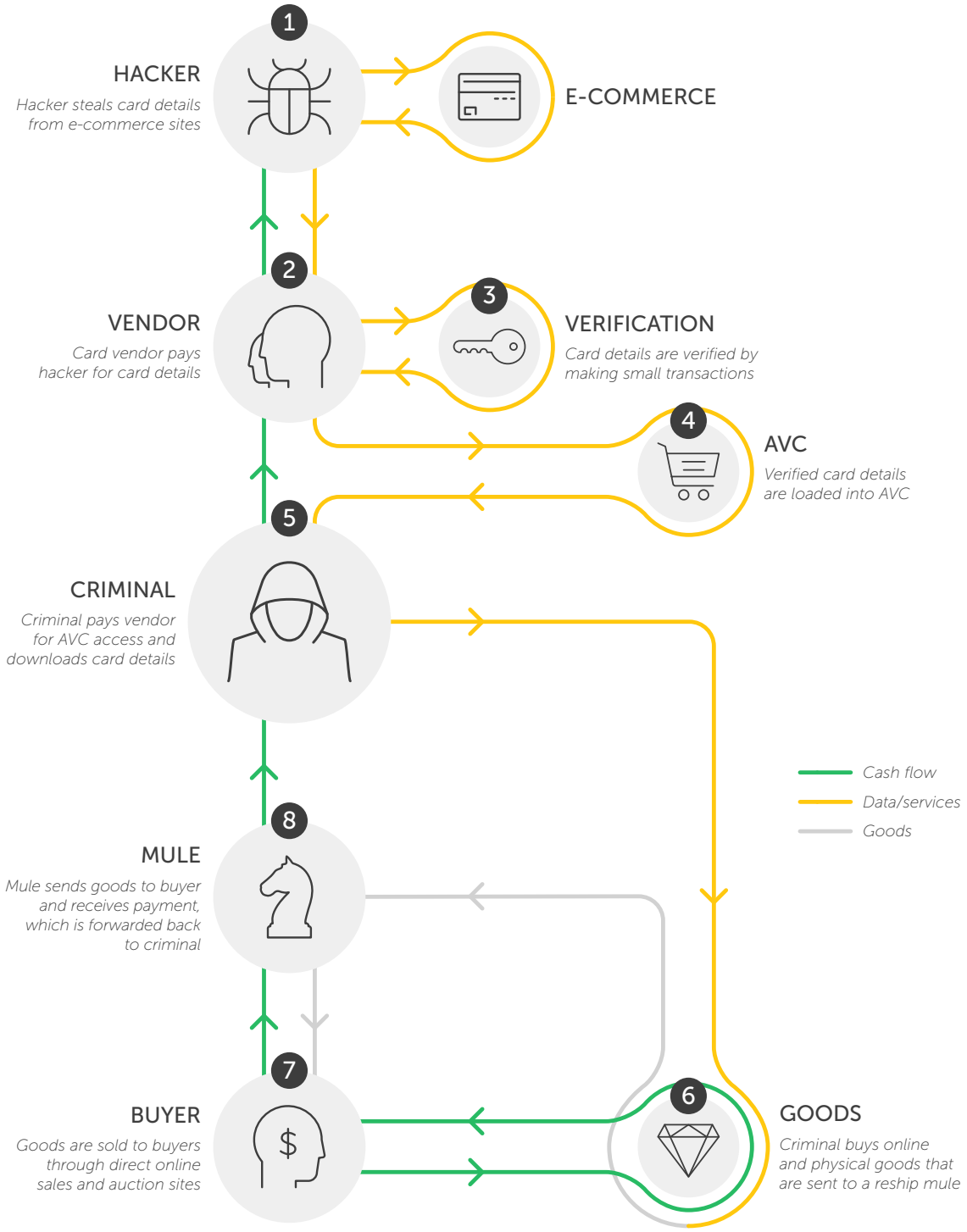


DIAGRAM 3: (Source: Secureworks)

© 2017 Secureworks, Inc. All rights reserved.

Fullz

Sometimes cybercriminals are after more than an individual's credit card data. They often go after "fullz," or full sets of personally identifiable information (PII) about individual victims.

Fullz are dossiers that provide enough financial, geographic and biographical information on a victim to facilitate identity theft or other impersonation-based fraud. Depending on the vendor, country and inclusion of other premium information like passport scans, fullz typically cost around $10 USD as seen in **FIGURES 22** and **23**.

Once a criminal possesses one of these full dossiers, there are numerous methods by which he or she can make money. With enough information, threat actors can convincingly pose as the victim both online and over the phone, as they possess even the answers to "secret questions." Often, impersonation is only detectable by biometric controls.

There are a number of ways cybercriminals obtain fullz. Some are collated from the hacked databases of businesses that have failed to properly encrypt customer or staff PII. Similarly, they may be pieced together by mining vast databases of data stolen using malware. Other fullz are obtained more directly using spearphishing or malware specifically designed to obtain PII. These "fresh fullz" are the most valuable, as they contain up-to-the-minute information on the target.

FIGURE 22: *Fullz product descriptions*

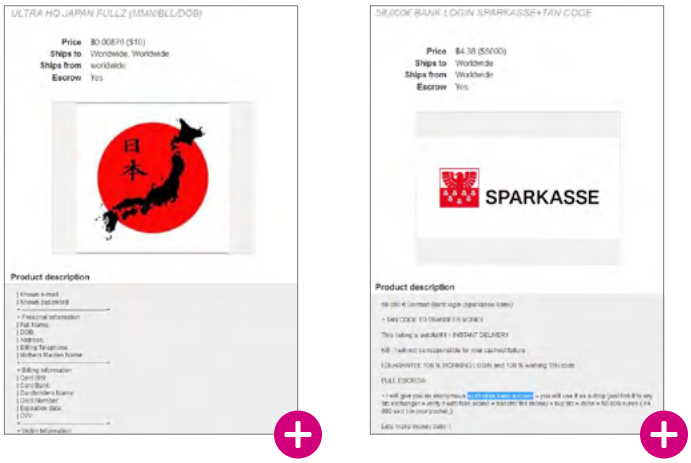


FIGURE 23: *Fullz product descriptions*

© 2017 Secureworks, Inc. All rights reserved.

10

Malware-as-a-Service and the affordability of spam botnets (as low as $200 USD per million messages) provide criminals with a low barrier of entry.

The Internet underground is thriving with ready-to-purchase malware. In underground forums, inexperienced or less-skilled cybercriminals are able to purchase information-stealing malware for reasonably low prices, typically in the form of pre-compiled binaries or premium builder kits that enable attackers to custom-configure their own binaries.

CTU researchers saw sellers promoting DiamondFox, a fully-featured information-stealing malware, for prices ranging from $300 to $700 USD as outlined in **FIGURE 24**. DiamondFox's advertising suggests it comes with a web-based control panel to help attackers administrate the machines they infect, and is able to perform tasks including: scrape the victim system's memory for credit card data, launch DDoS attacks, send spam, allow remote control of the victim's computer and steal browser passwords from the content of web forms as victims browse or buy things online.

The feature set of DiamondFox is fairly comprehensive and many different malware families make use of this type of functionality, but other families may have different "licensing" or "per feature costs." The CTU research team also saw other malware for sale, including "smokebot," which advertised a price-per-module sales approach, as seen in **FIGURE 25**.

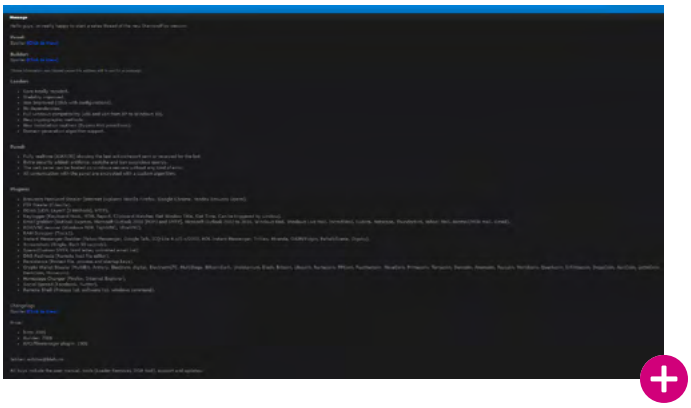


FIGURE 24: *DiamondFox sales advertisement*

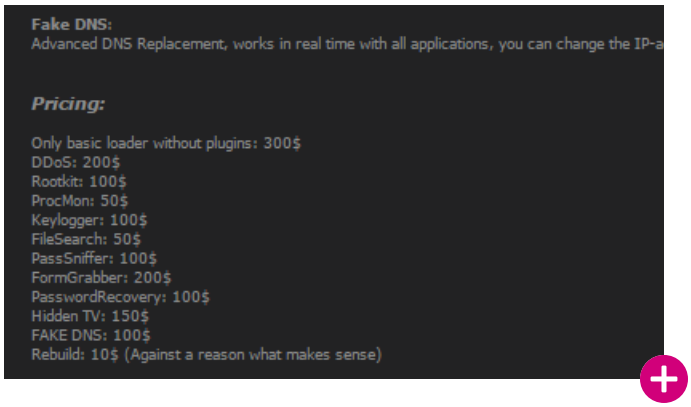


FIGURE 25: *Smokebot sales advertisement*

© 2017 Secureworks, Inc. All rights reserved.

Spam Botnets

Spam is a classic tool that continues to evolve. It remains the most commonly used method for the distribution of all manner of cybercriminal wares. It is used, among other types of scams, for romance scams, fraud facilitation, and the sale of counterfeit goods and pharmaceuticals. Today, cybercriminals can tap into large botnets to increase the spread of their spam exponentially, a product that can be thought of as "Spam-as-a-Service."

The CTU research team observed one large spam botnet known as "Kelihos" charging as little as $200 USD per million emails sent for pharmaceutical and counterfeit goods-type messages, while mule recruitment campaigns may cost $300 USD per million emails sent and phishing messages may run as much as $500 USD per million. Those prices seem to reflect the relative risk the spammer and their network are taking, as malicious phishing emails draw more attention from authorities and security researchers than pharmaceutical spam. In 2017, Russian native Peter "Severa" Levashov was arrested in Spain as the alleged creator and administrator of Kelihos.

CTU researchers observed that pharmaceutical spam messages were generally sent on weekends and malware-containing spam messages were sent during the working week, regardless of the country being targeted.

In the Internet underground, massive email lists are also readily available and have been observed by CTU researchers to cost as little as $1 USD per million email addresses, as seen in **FIGURE 26**. Accounts identified as active, sell at a higher premium, and prices may also vary based on location, seller and other factors. For example, language- or region-specific emails that can be used in more targeted campaigns may cost more, with one vendor offering a French-only email list at $40 USD for 500,000 addresses.

The CTU research team monitors several of the largest spam botnets, including Cutwail, a botnet that has existed since 2007. Over the last five years, CTU researchers have seen over 250 million unique email addresses in spam runs sent through Cutwail alone.

However, over the past year, the team has observed Cutwail conducting fewer campaigns than usual, with 1,076 unique spam templates observed in May 2016–2017, compared to 3,785 the year prior and 8,236 the year before that (see **FIGURE 27**). The team assesses that this decrease may be related to the takedowns of the "Gameover Zeus" network and the arrest of many members of the "Dyre" cybercriminal group, both of which were major customers of Cutwail. Still, Cutwail remains a potent spam threat that is responsible for millions of spam messages every month around the globe.

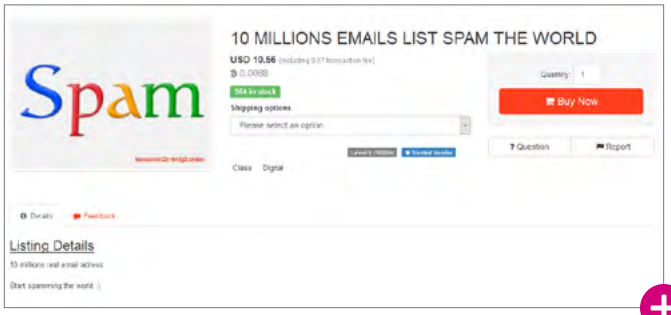


FIGURE 26: *Email list for sale*

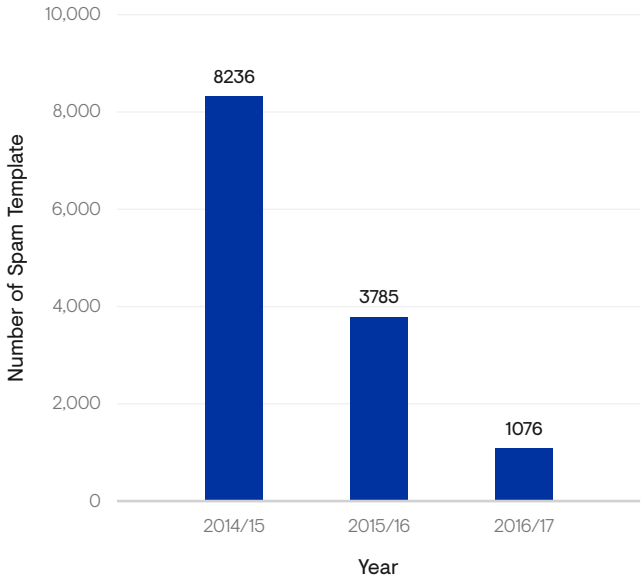


FIGURE 27: *Number of Cutwail spam templates*

© 2017 Secureworks, Inc. All rights reserved.

Mobile Spam

A growing trend in spamming is the use of SMS and mobile messaging. Using "text to SMS gateways," cybercriminals are able to mass distribute phishing messages containing links that lead to fraudulent messages prompting the user to enter financial data, such as credit card information or banking credentials. Alternatively, these messages may include links to download Android applications that purport to be legitimate applications, but are actually criminal malware, such as Android ransomware and spyware.

CTU researchers have observed activity surrounding SMS spamming on the underground market, including an advertisement for a SMS spamming tutorial for sale at $650 USD, as seen in **FIGURE 28**.

Mobile messaging spam is likely to be more effective at duping users than traditional spam methods because users may be less aware that SMS can be used as an attack vector. It is not unusual for consumers to receive SMS messages from their banks for the purposes of authentication, so they may not sense they are being scammed. Furthermore, mobile devices currently do not employ the same level of technical protection as desktop or laptop computers, making phishing links more likely to reach victims and malicious code more likely to execute successfully.

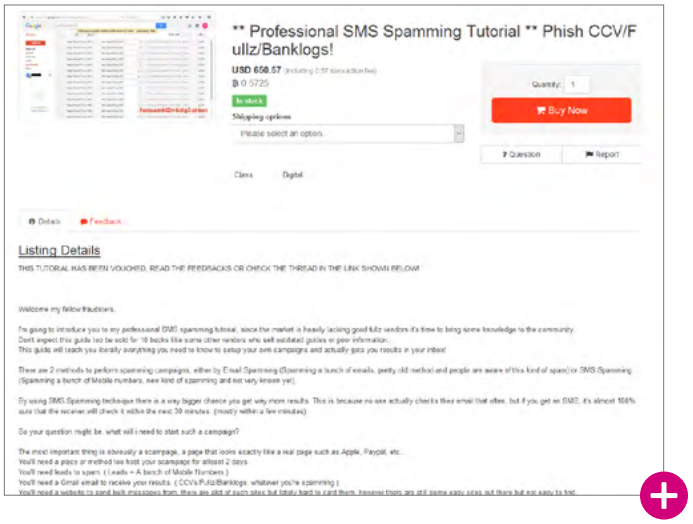


FIGURE 28: *SMS spam tutorial sale post*

© 2017 Secureworks, Inc. All rights reserved.

11

The market adapts to changes in the environment; for example, technical improvements as well as law enforcement takedown operations have significantly impacted exploit kit usage.

Exploit kits were once a lucrative tool for cybercriminals, offering an ongoing way to exploit a browser or browser plugin on a victim's computer to force the download and execution of malware.

Better security and fewer browser exploits are forcing exploit kit designers to shift tactics, changing the game.

CTU researchers have noticed a general decline in exploit kit activity since September 2016, as well as a marked decline in the success of exploit kit installation attempts — the proportion of computers infected with malware after visiting an exploit kit — which has fallen to less than 10 percent. Some attribute the decline in activity to the takedown of the popular Nuclear, Angler and Neutrino exploit kits over the course of 2016; however, CTU researchers believe there are additional factors at work. Over the past year, there have been fewer-than-normal disclosed browser and third-party plugin vulnerabilities for criminals to exploit. In addition, newer operating systems carry more attack mitigations, so as older, vulnerable computers are replaced, it is natural to see a decrease in exploit kit activity and installation. This decline in exploit activity is illustrated in **FIGURES 29** and **30**.

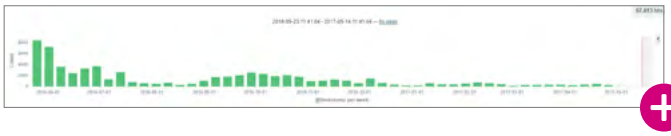


FIGURE 29: *Looking at the data generated from Secureworks' clients, this decline in observed exploit kit attacks is easily visible.*

FIGURE 30: *Exploit kit activity tracked by CTU researchers from September 2016 – April 2017. Note the activity on the Neutrino, Rig, Rig VIP (a Rig variant) and Sundown exploit kits, where a browser exploit was used.*

© 2017 Secureworks, Inc. All rights reserved.

Exploit kit operating models are not as successful as they once were. CTU researchers have observed that the successful install rate — the proportion of computers infected with malware after visiting an exploit kit — is now generally under 10 percent.

However, cybercriminals have not abandoned exploit kits entirely, and are trying new approaches to increase their odds of successful attacks. One approach they have adopted is a hybrid model that leverages social engineering techniques in combination with the exploit kit, for example prompting the victim to download a browser font package, which is really a malware payload in disguise.

There are two service models for exploit kits: a hosted service (see **FIGURE 31** as an example) and an installation package for the buyer to host themselves.

Exploit kits are marketed on the Internet underground on closed, invitation-only forums or directly to known exploit kit users and developers. The operators of new kits often try to build a subscriber base before going live and offer discounts for early adopters. Kits are also advertised, via spam messages, on the Jabber messaging system, targeting known exploit kit users.

Campaigns can be geographically specific and distribute payloads by region. For example, Secureworks has observed an exploit kit delivering banking malware only to victims in a particular country. The malware configuration also only targets banks in that country. Secureworks has also observed an exploit kit declining to attack vulnerable systems at a specific time, only for it to exploit the same system later. It may be that exploit kit operators configure malware distribution at intervals to make tracking them more difficult.

CTU researchers have also observed a slight shift towards malware being dropped via “malvertising” campaigns, instead of relying on traditional exploit kits. With malvertising, the threat actors focus on compromising advertising networks by adding malicious scripts to target users of popular websites.

FIGURE 31: *Nebula Exploit kit for sale; Note subscription on a pay-per-period basis*

© 2017 Secureworks, Inc. All rights reserved.

Conclusion

It is clear that the cybercriminal world, including the Internet underground, is alive and well, with both creative developments in the way in which victims are being targeted by cybercriminals and the ways in which they are carrying out their nefarious activities.

Whether you are an individual or an organization, it is useful to understand the inner workings of the cybercriminal world and to be aware of the threats targeting you, your money and your information.

Cybercriminals can be goal-driven and patient, and they often have a singular focus, plenty of time and access to vast, modern technical resources. Both organized and forum-based criminals are working constantly to find innovative and efficient ways to steal information and money with the lowest risk to their personal freedom. If we wish to stay "one step ahead" of the threats detailed in this report, awareness of online criminal threats, techniques and markets is our best defense.

Authors

This report was authored by the Secureworks Counter Threat Unit (CTU). With more than 70 of the world's most highly-regarded security researchers, Secureworks' distinguished CTU research team is one of the key assets which sets Secureworks apart. Secureworks' researchers analyze threat data across our global client base and actively monitor the cyber threat landscape to provide a globalized view of emerging threats, zero-day vulnerabilities, and the evolving tactics, techniques and procedures (TTP) of advanced threat actors. The CTU research team's primary objective is to protect our clients' information and operations from today's most advanced security threats, by applying its research and cyber threat intelligence into all aspects of our security solutions.

© 2017 Secureworks, Inc. All rights reserved.

Glossary of Terms

419 Scam (Phishing) — also known as a "Nigerian scam," where the sender requests, usually via email, help in facilitating the transfer of a substantial sum of money. Often the victim is required to provide some form of advanced payment, in order to enable the transaction or secure their commission.

Automated Vending Carts (AVCs) — similar to the shopping carts used by legitimate online retailers, allowing a customer to create an account with the seller and buy specific card details through an automated system.

Banking Trojan — malware used to gain confidential information about customers and clients of online banking and payment systems.

Bitcoin — a type of digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank.

Bulletproof Hosting — rent servers to individuals or groups engaged in criminal activity and offer a degree of protection against law enforcement investigations into their clients.

Business Email Compromise — hijacking an email account or an email server to intercept or initiate business transactions, and direct payments to financial accounts owned by the criminal.

Business Email Spoofing — sending spoofed email from an external account imitating a company executive or employee authorizing a fraudulent transaction to the criminal.

Crime-as-a-Service — the idea that the different components required for effective cybercrime can be assembled on a task or project basis using traditional outsourcing concepts.

Counter Anti-Virus (CAV) — allows malware developers or owners to submit samples to discreet online sandboxes and receive an indication as to whether existing anti-virus technologies will detect their malware.

Cybercrime — sometimes referred to as online crime or internet crime. At its broadest, it can be defined as all crime perpetrated with or involving a computer. This report takes that broad definition, but the focus of the analysis is on financially motivated cybercrime rather than other types of criminal activity, such as child exploitation.

DDoS — Distributed Denial of Services

Drop Services — also known as "drops." Services which help criminals (including but not exclusively cybercriminals) transfer money.

Exploit Kit — a toolkit used by cybercriminals to exploit vulnerabilities in systems or devices. Most commonly, exploit kits target internet browsers by compromising websites to re-direct users to malicious sites, which then attempt to exploit their browser to gain some level of access to their device.

Fullz — full sets of identifying information. Dossiers that provide enough financial, location and biographical details on a victim to facilitate identity theft or other impersonation-based frauds.

Internet 'Underground' (Dark Web) — the Internet forums and chat rooms that criminals use to form alliances, trade tools and techniques, and sell compromised data that can include banking details, personally identifiable information and other content.

Jackpotting — a technique designed to steal money from an Automated Teller Machine (ATM) without using a credit or debit card. Malware designed for this purpose is referred to as "jackpot malware."

Malware — code which is written to perform some form of unauthorised action, often resulting in harm. Includes computer viruses, worms and Trojans.

Malware-as-a-Service — allows criminals to gain access to malware capabilities which are sold and maintained by an individual or group. Designed, much like other –as-a-Service models, to introduce efficiencies in terms of scaled support, and to lower the technical barrier of entry for engaging in criminal activity.

Mobile Malware — malware designed specifically to attack mobile devices (usually mobile phones).

Money Mule — a person involved in the movement of stolen funds or goods from the victim to the criminal perpetrator. Often an unwitting participant.

Operations Security — also referred to as Operational Security or 'OpSec'. In this context, measures taken by cybercriminals to avoid detection or, if detected, prevent law enforcement from being able to develop an evidential case for directly attributing to specific individuals.

Organized Criminal Group — a group of individuals with an identified hierarchy or comparable structure, engaged in significant criminal activity, usually for financial gain.

Phishing — an attempt to gather information from an individual or organization in a way which is unauthorized and possibly illegal, by sending an email which is designed to trick the recipient into disclosing information. Spear phishing is highly-targeted phishing activity.

Romance Scam (Phishing) — a confidence trick involving feigned romantic intentions towards a victim, gaining their affection and then exploiting their goodwill to commit fraud.

Ransomware — a type of malware that prevent or limits users from accessing their system or files. Normally employed by cybercriminals to extort victims.

Remote Access Trojan — malware that allows another (remote) computer to gain access to the machine on which the malware is running, in a way which is unauthorized.

Spam — unsolicited email messages sent to a group of recipients.

SWIFT (Society for Worldwide Interbank Financial Telecommunication) — a messaging network that financial institutions use to securely transmit information and instructions through a standardized system of codes.

Tumbling — also referred to as mixing. Services which mix funds obtained from cybercrime with "clean" funds in order to obfuscate the source and break the trail to the end users.

© 2017 Secureworks, Inc. All rights reserved.

About Secureworks

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that keeps organizations safe in a digitally connected world. We combine visibility from thousands of clients, artificial intelligence and automation from our industry-leading Secureworks Counter Threat Platform™, and actionable insights from our team of elite researchers and analysts to create a powerful network effect that provides increasingly strong protection for our clients. By aggregating and analyzing data from any source, anywhere, we prevent security breaches, detect malicious activity in real time, respond rapidly and predict emerging threats. We offer our clients a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

1 Concourse Pkwy NE #500
Atlanta, GA 30328
1.877.838.7947
www.secureworks.com

Asia Pacific

AUSTRALIA
Building 3, 14 Aquatic Drive
Frenchs Forest, Sydney NSW
Australia 2086
1.800.737.817
www.secureworks.com.au

JAPAN
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
81-(44)556-4300
www.secureworks.jp

Europe & Middle East

FRANCE
8 avenue du Stade de France
93218 Saint Denis Cedex
+33 1 80 60 20 00
www.secureworks.fr

GERMANY
Main Airport Center, Unterschweinstiege 10
60549 Frankfurt am Main
069/9792-0
www.dellsecureworks.de

UNITED KINGDOM
UK House, 180 Oxford St
London W1D 1NN
+44(0)207 892 1000
www.secureworks.co.uk

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040
www.secureworks.co.uk

UNITED ARAB EMIRATES
Building 15, Dubai Internet City
Dubai, UAE PO Box 500111
00971 4 420 7000

© 2017 Secureworks, Inc. All rights reserved.

Secureworks®