Secureworks®
A Dell Technologies Company

EXECUTIVE SUMMARY

2017

State of Cybercrime Executive Summary

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

Introduction

Although the global financial toll of cybercrime is difficult to quantify, in the United States alone, internet crime in 2016 led to reported losses in excess of $1.3 billion, according to the FBI.

Organized cybercrime operates like a business, seeking to maximize profits and minimize risk. To be successful, criminals require a variety of tools, specialist skills and techniques. One place cybercriminals go to obtain these resources is the internet underground, also referred to as the dark web, darknet or the deep web. In these forums, digital storefronts and chat rooms cybercriminals form alliances, trade malware and tactics, and buy and sell stolen data. Secureworks monitors and studies this activity to anticipate future threats and to create defenses that protect our clients.

This underground market is thriving, but it only provides part of the picture. Professional cybercriminals running global, high turnover operations take care to hide their activities from anyone who might be watching. Like more traditional organized criminal groups, they avoid communication channels such as online forums and chat rooms which they know could be subject to monitoring by researchers and law enforcement agencies. Consequently, a complete view of the cybercrime landscape cannot be achieved with 'dark web' threat intelligence alone. That knowledge must be combined with what we learn through the technical tracking of more sophisticated cybercriminals, wherein our researchers observe their efforts to compromise organizations, as they happen.

Secureworks, a Dell Technologies company, has been tracking cybercrime activity for more than 10 years, collecting vast amounts of data on criminals, their operations and their money-making schemes.

As Secureworks monitors security events across hundreds of thousands of devices and endpoints within 4,400 client environments in 59 countries, researchers in Secureworks' Counter Threat Unit™ (CTU) collect and examine cybercriminals' toolsets, tactics and procedures around the clock, 365 days a year.

This executive summary of Secureworks' annual 2017 State of Cybercrime Report presents CSOs, CISOs and security executives a high-level overview of the cybercrime landscape and trends observed primarily from mid-2016 through mid-2017. (Download the full report at https://www.secureworks.com/dell-2017-state-of-cybercrime). Readers will gain valuable information on major cyber threats currently plaguing companies and individuals and rare insight into the behaviors and organizational structure of some of the most proficient criminal groups on the internet.

Secureworks offers the findings in this report to help all organizations better protect themselves from current and emerging cyber threats, making us all collectively smarter and exponentially safer.

Secureworks offers the findings in this report to help all organizations better protect themselves from current and emerging cyber threats, making us all collectively smarter and exponentially safer.

Snapshot of Key Findings

Based on careful observation of the cybercrime landscape and trends from mid-2016 to mid-2017, the Secureworks Counter Threat Unit (CTU) identified 11 key findings that span the risk of cyber threats, the complexity of the online criminal landscape, and the market economics of online crime.

1. **Business email compromise (BEC) and business email spoofing (BES**) schemes continue to grow, evolve and target small, medium and large businesses. Between January 2015 and December 2016, there was a 2,370 percent increase in identified exposed losses, according to the FBI.

2. **Ransomware** threats thrive and new variants are created as they deliver to cybercriminals a high return on their investments. In 2016, CTU researchers saw 200 new ransomware variants, a 122 percent increase from the previous year.

3. **Banking malware** can be custom-made to target specific institutions and carry out specific attacks. Often financial malware is capable of stealing personal identifiable information as well as banking credentials.

4. **Mobile malware** can steal personal and financial data, and can spy on users.

5. **Organized cybercrime syndicates** operate like full-time businesses but avoid online cybercrime forums to hide their activities.

6. **Cybercrime groups depend on individuals** with highly-specialized, diverse skills to create finely-tuned attack systems.

7. **The line between nation-state cyber activity and cybercrime** is often blurred as organized crime groups are afforded a degree of patronage.

8. **Money mules are still in vogue,** but cybercriminals diversify their cash-out operations by taking Bitcoin payments.

9. **Personal information** remains a popular commodity, with tested and verified credit card data being sold for as little as $10 per record. “Fullz,” which contains all the personal data needed to open up new lines of credit in a person’s name, can also be purchased for as low as $10.

10. **Malware-as-a-Service and spam botnets** are so affordable (at $200 per million messages) that nearly anyone can become a cybercriminal.

11. **Cybercrime adapts quickly** to evade new security technologies. To stay resilient, companies should continuously assess risk, test vulnerabilities, and mature their cybersecurity programs relative to their unique threat landscape.

The Findings

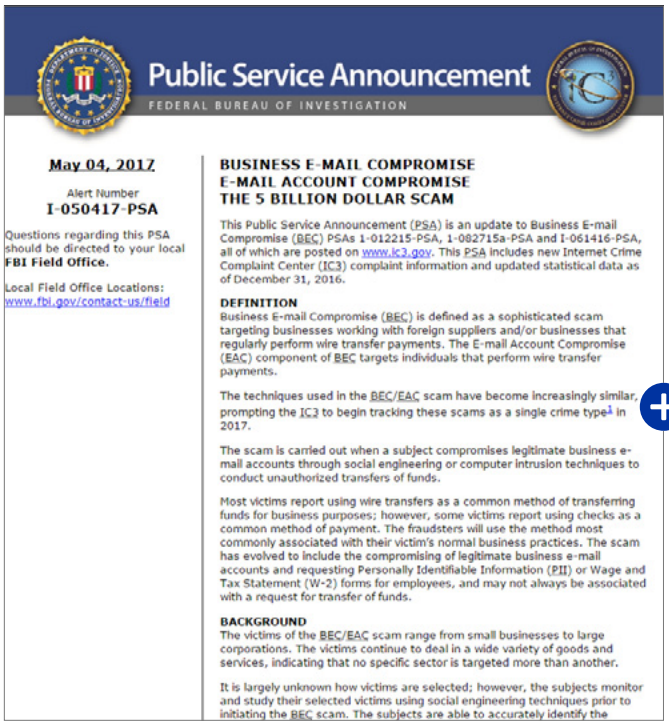
Cyber threats continue to pose a significant risk to organizations' revenue and reputation, as well as personal privacy.

1. Business email spoofing and business email compromise help cybercriminals overcome increased security awareness.

Business email spoofing (BES) and business email compromise (BEC) are popular techniques that cost organizations across the globe $5 billion USD between October 2013 and December 2016, according to the FBI (see **FIGURE 1**). BES is the creation of a forged email message that pretends to come from the account of a senior company executive and demands that an urgent payment be made to a bank account controlled by the criminal actor. Many BES scams target employees within the accounting department who are authorized to make money transfers on behalf of the company. By exploiting the implied authority of the spoofed executive and imposing some form of pressure such as an arbitrary deadline, the threat actor hopes the target will comply. Unfortunately, receivers often do comply with the sender's request and transfer funds to an account that belongs to a cybercriminal.

To fool their target recipients, attackers can use either a spoofed 'from' email address or one that closely resembles it. For example, the company CFO's email might be mike@acme.com, but the spoofed email sent to another company employee may read mike@aceme.com, just close enough to trick someone who is not paying close attention. Alternatively, to send an email that actually displays the CFO's true email address — mike@acme.com – attackers may alter some of the information that displays in the email header, including the sender's name, email address, recipient's name, date and subject. This method is almost as simple as writing someone else's return address on an envelope.

Business Email Compromise (BEC) is a social engineering scheme in which threat actors gain access to the email account of someone involved in processing sales transactions on behalf of the business. In this way, the criminal is able to intercept emails between the two parties. When a vendor sends an email with an attached invoice, the threat actor alters the payment instructions so that payment is made to a bank account controlled by the criminal.



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)*

2. Ransomware activity continues to increase because attacks are profitable.

Through 2016 and into 2017, ransomware activity has dramatically increased across the world as cybercriminals have learned that it offers a high return on investment, is relatively easy to use, and is difficult to investigate. CTU researchers observed nearly 200 new, named ransomware variants in 2016, up from 90 the previous year (see **FIGURE 2**). In May 2017, the WCry (also known as WannaCry or WanaCryptor) ransomware had a significant impact on a number of organizations who had not patched their systems, including a number of hospitals within the UK National Health Service. Unable to access their files, many hospitals reportedly were forced to cancel routine procedures, close emergency rooms, and shut down wards.

The CTU believes ransomware will continue to grow in popularity because attackers can earn good money from this illicit activity. For example, the CTU observed the Philadelphia ransomware — an updated version of the Stampado Ransomware kit — for sale on the underground for $389 USD, while on average, between $500 and $1,000 USD is demanded from one ransomware victim (see **FIGURE 3**). This potential return on investment, combined with the difficulty in identifying the perpetrator behind a ransomware attack, makes ransomware attractive to online criminals.

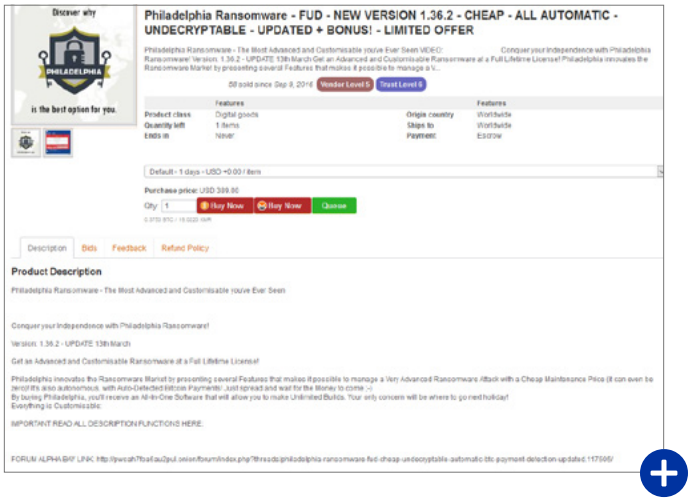


FIGURE 3: *Ransomware sales post*

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

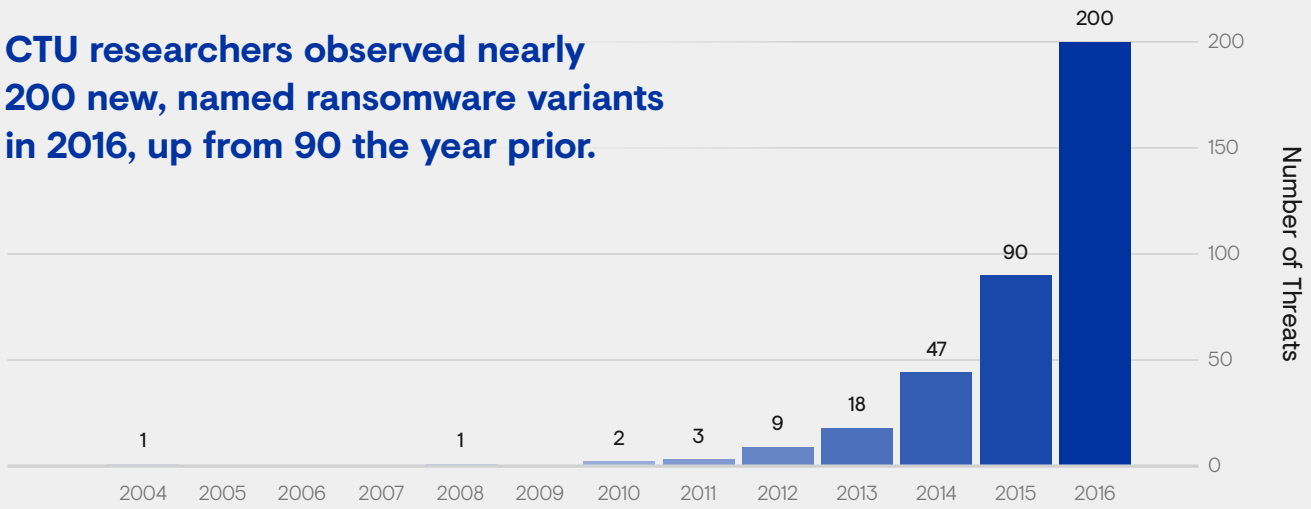


FIGURE 2: *Number of new ransomware threats per year*

3. Banking malware can be bespoke.

Organized cybercriminal groups use banking malware to facilitate large-scale fraud across the globe. These attacks range from highly-targeted intrusion activities, mounted against specific, high-value targets (e.g. wealth management companies, boutique private banks, payroll processing companies and the business banking arms of large retail banks) to commodity banking botnet attacks that are less customized but target large numbers of consumer bank accounts across the globe.

A botnet is a network of computers that are under the control of an attacker or an attack group. Users don't realize that their computers have become infected with malware and are responding to commands issued by attackers. This unauthorized access can be used to send malicious spam to infect more users, or to steal users' banking login credentials by manipulating their web browser session.

In contrast to widely-disseminated attacks, customized, targeted attacks can be carried out by sophisticated organized criminal groups who develop bespoke malware and spend considerable time and resources compromising and then understanding their high-value target.

In fact, security experts saw organized criminal groups pull off several large-scale ATM "jackpotting" attacks. With this style attack, the cybercriminals infect the ATMs across a bank's network with malware that is designed to remotely trigger the ATMs to dispense all of its cash, right into the hands of the individuals, known as money mules, recruited by the criminal gang to collect and move their stolen profits. These attacks are called "jackpotting" because money is spat out from an ATM in a similar manner as coins are spat out from jackpot slot machines. In one such attack, which was reported to have involved the theft of millions of dollars from ATMs in Europe, the former Soviet Union and Malaysia, a sophisticated threat group dubbed GOLD KINGSWOOD by the CTU and commonly known as "Cobalt," got their initial foothold into the targeted bank's network by sending bank employees spearphishing emails (see **FIGURE 4**). These emails were rigged to appear as if they came from the bank's ATM manufacturer. The emails contained a malicious attachment that reportedly infected the employee's computer, allowing the attackers to move laterally across the bank's internal network to reach the workstation or server that controls the ATM fleet.

FIGURE 4: *Cobalt gang headline*

4. Mobile malware poses a significant threat to both information and privacy.

On the dark web, CTU researchers have observed numerous instances of cybercriminals selling mobile ransomware that they claim will encrypt files on an Android phone, demand payment for decryption, and spy on all functions of the phone (see **FIGURE 5**). Cyber attackers are spreading the mobile malware to users by sending them text messages that contain a link and purportedly come from the recipient's cell phone company. When the receiver clicks on the link, malware surreptitiously is downloaded.

Secureworks CTU researchers predict mobile malware, and ransomware in particular, will proliferate, depriving users of access to their contacts, photos and data (See **FIGURE 6**). Both information theft and spying capabilities are predicted to become more widely available.

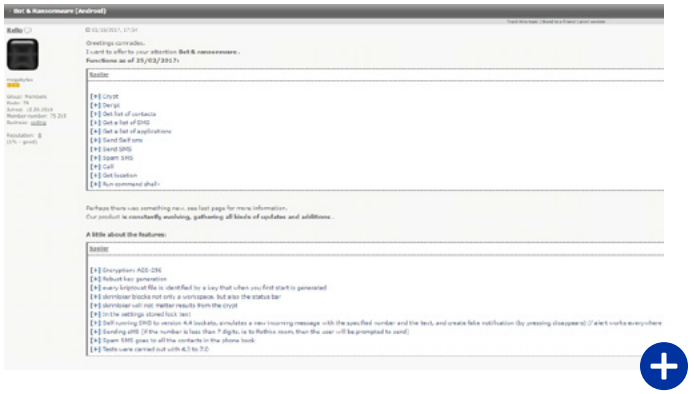


FIGURE 5: *Android bot sales post*

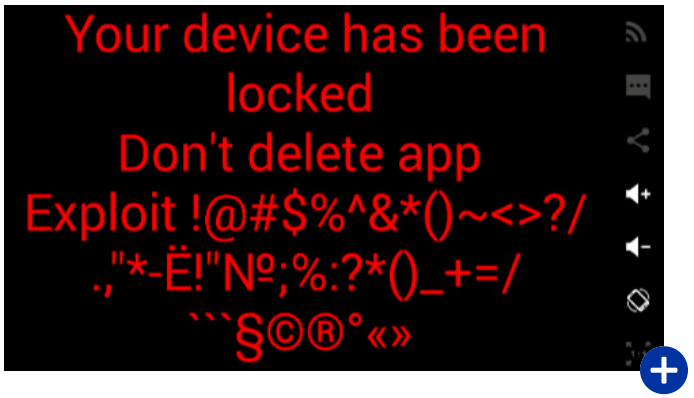


FIGURE 6: *Android ransomware lock screen in development*

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

5. Organized cybercrime operates like a private business.

Cybercriminals use internet forums and chat rooms to form alliances, to trade tools and techniques, and to sell compromised data, such as credit card data and personally identifiable information. However, organized cybercrime gangs operate more like traditional businesses and refrain from exposing their activities in online forums where they may be spotted by global law enforcement. Cybergangs outsource jobs and employ full-time professionals who serve in different roles. Some cybercrime groups are affiliated with nation states and work on behalf of the government.

6. Cybercrime roles can be highly specialized and diverse.

On the dark web, cybercriminal enterprises seek skilled job candidates for a variety of positions and pay people based on their skills and demand (see Criminal Actors and Responsibilities on pp. 11-12). A variety of experts are needed to create well-oiled cyberattack systems which include malware writers, cybercriminal recruiters and money mules who either knowingly or unknowingly help criminal groups launder money.

7. The line between nation-state cyber activity and cybercrime Is blurring.

Members of organized crime groups cooperate and communicate in closed channels. 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.

8. Money mules are still in vogue, but virtual currency helps threat actors diversify.

Cybercrime is about making money, but transferring the money directly into a hacker's bank account would lead authorities directly to the criminal. So instead of putting the money directly into their own accounts, threat actors move the money around a few times to make the electronic trail harder to follow. To stealthily move money, attackers hire money mules. A money mule transports stolen money on behalf of a thief. Money mules are often individuals who have answered a "work from home" ad, are unaware of the scheme taking place, and believe they are simply processing payments for a business based overseas (see **FIGURE 7**).

A typical financial transfer using a money mule looks something like this: the mule receives the stolen funds directly into his personal bank account, he keeps a portion that was promised by his "employer," and then he transfers the balance to his employer's business account, which is typically overseas. From there, that money is often transferred again and again to bank accounts that may be quickly emptied or closed, making the stolen funds extremely difficult to trace.

To reduce costs, some criminals might choose to receive payments in virtual currencies such as Bitcoin, to remove the need of paying a money mule network. This is particularly true when it comes to ransomware campaigns.

FIGURE 7: *Seeking Polish mules*

Online crime is a market economy.

9. Personal information remains a popular commodity.

Credit card data and personally identifiable information (PII) can be purchased on the dark web for as little as $10 per record (See **FIGURE 8**). The most popular PII is referred to as "Fullz," a record that contains a person's full name, address, phone number and social security number, as well as other financial, geographical and biographical information on a victim. This comprehensive data record can help cybercriminals open new credit card accounts, create fake passports and commit medical fraud using the victim's health insurance card data. Fullz records are often obtained by collating data garnered from databases of businesses that have been breached or by piecing together data obtained from malware that mines vast databases.

10. Malware-as-a-service and spam botnets provide a low barrier to entry.

Cybercriminals with little technical knowledge can purchase information-stealing malware for just a few hundred dollars. On the dark web, cybercriminals have been selling information-stealing malware for as little as $300. (See **FIGURE 9**). Sellers claim that the malware features a web-based control panel to help attackers remotely administer the machines they infect, scrapes the victim system's memory for credit card data, and steals passwords to online stores.

Cybercriminals can also purchase "Spam-as-a-Service" from attackers who control large botnets and will spread spam for as little as $200 per one million emails. The spam is often used to peddle counterfeit goods, pharmaceuticals and other fraudulent scams that prompt users to enter their credit card information or banking credentials.

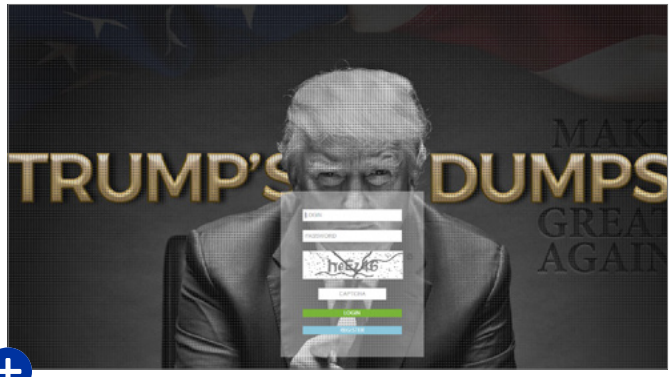


FIGURE 8: *Trump's Dumps offers cards from the U.S., Japan, South Korea and other countries for between $10 and $20 USD each, with refunds offered in case of a "bad card" that has been blocked by the bank already and cannot be used for fraud.*

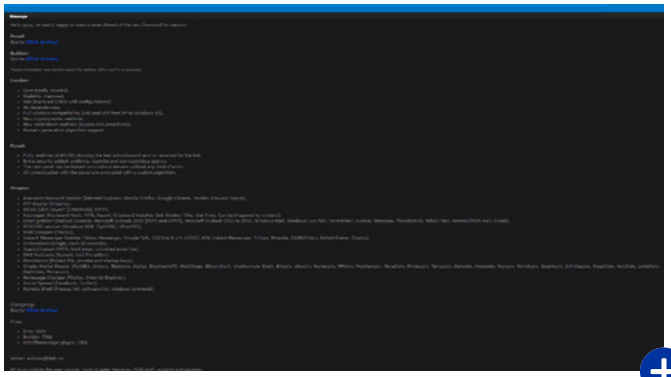


FIGURE 9: *DiamondFox sales advertisement*

11. The cybercrime market adapts quickly to evade new security technology and techniques.

As law enforcement and security professionals discover new defenses, cybercriminals consistently develop new offensive techniques. For years cybercriminals used exploit toolkits as a preferred way to attack computers. These kits automate the exploitation of vulnerabilities in users' web browsers and third-party software such as Adobe Flash Player. But in 2016, law enforcement disruption operations against several exploit kit operations and security enhancements for popular web browsers reduced the effectiveness of exploit kits. CTU researchers observed a shift towards a different method of attack: malvertising, or malicious advertising.

Malvertising involves injecting malicious code into ads, including popup ads, banner ads, and links to news stories. This code can be executed without user interaction; without even clicking on anything on the page, users can be directed to download malware. This threat can occur on any website that carries advertisements, and a number of high-profile sites have been affected by this type of attack.

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.

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.

Conclusion

The cybercriminal world continues to develop creative ways to target victims and abscond with funds.

Individuals and organizations need to understand the inner workings of the cybercriminal world, be aware of the threats targeting them and know how to prevent them.

Cybercriminals can be goal-driven and patient. They often have a singular focus and have the time and technical resources to identify and target prospective victims. Both organized and forum-based criminals work constantly to find innovative and efficient ways to steal information and money with the lowest risk of disruption and arrest. To stay one step ahead of threats detailed in this report, your best bet is to increase your awareness of online criminal threats, techniques and markets.

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.

Security Recommendations

for Defending Against Current and Emerging Cyber Threats

1

Engage cybersecurity early as you embark on digital transformation and strategic growth initiatives. Cybersecurity deserves the same continuous attention in our enterprise risk portfolio as financial, regulatory or geopolitical risk. Managed security solutions can scale quickly to support and enable your growing digital footprint in traditional networks, off-premise and in the Cloud.

2

Improve your security posture culturally as well as technically. Successful cyber attacks via email compromise and email spoofing accounted for $5b USD in losses globally from 2013-2016, and victims' losses increased by 2,370% between January 2015 and December 2016. We're vulnerable wherever our employees live and work, so investing in a culture of security training and day-to-day vigilance has never been more important. This also goes for executives who are a significant target of advanced attacks to steal mission-critical intellectual property.

3

Invest in protection, not just prevention. The risk is better managed when the organization's approach to security is not dependent on the latest product or service, but rather when a security program operates across four critical and distinct components that work in concert to help you take the right action:

- **Prevent** - stop the known threats with tools and processes that inspect content.
- **Detect** – recognize and validate potential threats when they bypass defenses.
- **Respond** – quickly identify, contain and eradicate by leveraging a blend of automated capabilities (essential to execute at the speed of the threat) overseen by human experts with experience in threat behavior.
- **Predict** – visibility across the enterprise and its user endpoints, coupled with threat intelligence, testing and vulnerability management, can be leveraged to get a step ahead of the threats and support the organization's transformation initiatives -- from operating in the Cloud to international expansion.

As organizations pursue a unified approach to security, their environments become less attractive to cybercriminals who will always seek the greenest pastures for a better return on investment.

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.™

Secureworks is a Dell Technologies company.

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
+61 1800 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

NETHERLANDS
Transformatorweg 38-72, 1014
AK Amsterdam,
+31 20 674 5500

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