Secureworks®

ANNUAL REPORT

2018 State of Cybercrime

The Deep, Dark Truth Behind the Underground Hacker Economy

Introduction

It's common in the cybersecurity world to say the Internet is like an iceberg. The open Internet most people use on a daily basis is only the visible tip. Beneath the surface, hidden from public view, is a vast and mysterious "dark web" where criminals interact in forums and marketplaces with relative impunity.

In truth, the dark web is not an open playground for criminals. The primarily low- and mid-level criminals who use the dark web do so at great risk of being discovered by the large number of law enforcement and security researchers who also frequent those underground channels.

For this reason, the most sophisticated and capable criminal gangs steer clear of the dark web where possible. Instead, they operate in the depths beneath the iceberg, practicing rigorous operational security and working diligently to avoid the unwelcome attention of international law enforcement. They may sell goods and services on the dark web, but they will not use it as a forum to discuss their activities or build business relationships.

It is these sophisticated criminals, operating deep in the trenches, who develop and sell the ransomware- and malware-as-a-service deployed by nation-states and cybercriminals alike. They are the sophisticated threat groups who steal millions of dollars in one day by penetrating banking networks and disabling anti-fraud controls in order to perform near-simultaneous cash withdrawals from ATMs all over the world. They are the well-organized gangs defrauding buyers to the tune of hundreds of thousands or even millions of dollars by inserting themselves into the middle of large business transactions or real estate purchases.

Secureworks Counter Threat Unit® (CTU®) researchers have spent the last 16 years tracking, monitoring and, where possible, disrupting the activities of these sophisticated criminal elements. Experience shows that these actors are responsible for the vast majority of actual losses associated with cybercrime. As such, they invest heavily in their operations and actively manage down any associated risks. Moreover, they display a depth of technical competence and tradecraft that is equal to, if not better than the nation-state-sponsored advanced persistent threats that often grab headlines.

To understand their risk, organizations must understand the true threats that lie beneath the dark web and between the lines. Only with the right telemetry, analytics and expertise can those threats be exposed, understood and anticipated. Through insights gained from incident response, client telemetry and research activity, CTU researchers have developed capabilities that combine dark web monitoring and client brand surveillance with automated technical tracking of cybercriminal toolsets to provide a holistic view of the threat these actors pose. These insights, in turn, drive the protections and advice Secureworks provides to clients.

Why protecting against known threats isn't enough

Cybersecurity can be a cat-and-mouse game – cybercriminals launch an attack, cybersecurity teams discover and defend against it, and the cybercriminals then evolve their tools and techniques so that they can continue to be successful.

Relying on a strategy of protecting against "known threats" means cybercriminals always have the upper hand.

Secureworks CTU researchers use sophisticated capabilities to understand not just threat actor tools and associated indicators, but also their tactics, techniques and procedures. By analyzing their behavior over time, researchers and analysts can track cybercriminals' moves as they make them, enabling clients to build defenses that anticipate evolving threats and continue to protect their organizations.

Executive Summary & Key Findings

From July 2017 through June 2018, Secureworks CTU researchers analyzed incident response outcomes and conducted original research to gain insight into threat activity and behavior across 4,400 companies. The team identified the following key findings:

A steady level of "background noise" from low-level criminality is impacting businesses around the world and should not be ignored.

_01 **Cryptocurrency mining remains an extremely popular way for criminals to monetize access to infected computers.** In 2017, at least one in three organizations experienced cryptocurrency mining activity on their network. These infections represent unauthorized access to the network and can affect critical business functions.

_02 **There has been no significant decrease in the volume of ransomware, banking malware, point-of-sale (POS) memory scrapers or other threats available for purchase on underground forums.** CTU researchers tracked the emergence of 257 new ransomware families from July 2017 through June 2018, including GandCrab, which was the most prevalent ransomware threat in the first half of 2018 and continues to harm unprepared businesses.

_03 **Unscrupulous hosting providers help cybercriminals stay below the radar by offering them access to anonymized servers and Internet access.** Malicious forums advertise the ability to control anonymous hosted computers, known as Virtual Private Servers (VPS), and other dedicated hosting services for between $10 and $300 USD. Criminals leverage these services for a wide range of scams, counterfeit goods and other criminality. However, these openly advertised hosting services typically aren't the ones used to host command and control servers for malware that hits corporate IT networks.

_04 **Spam remains the leading means by which criminals deliver malware.** Infections via web exploit kits continued to drop precipitously as browser vendors improved security and the use of technologies like Flash and Java declined.

Data and unauthorized access continue to have a value in underground marketplaces, which means criminals will continue to pursue them.

_05 **Personally identifiable information (PII), including full biographic dossiers, payment card data and other bulk data sets, are regularly offered for sale in underground forums.** Actual purchase prices are difficult to determine, but point-in-time observations have identified advertised prices as low as $10 to $25 for "fullz," or comprehensive dossiers.

_06 **Criminals also use forums to sell access to compromised systems and organizations.** Advertised prices range from 50 cents to $400 for RDP access, and roughly $1,000 to $20,000 for broader access to a compromised organization, depending on the type of system or organization, the level of access offered and the geographic location of the asset.

A small subset of professional criminal actors are responsible for the bulk of cybercrime-related damage, employing tools and techniques as sophisticated as most nation-state threat actors.

_07 **Business email compromise (BEC) and email account compromise (EAC) have accounted for $12.5 billion in financial losses between October 2013 and May 2018, according to figures released by the FBI.** While the operations are relatively simple in form, these attacks have been incredibly well executed on a large scale by highly organized groups of criminal actors with a Central-to-West African nexus.

_08 **Sophisticated criminal gangs have combined advanced social engineering and network intrusion techniques with POS malware to generate millions of dollars of revenue through stolen payment card data.**

_09 **Criminals have conducted "global cashout" and ATM jackpotting operations by coordinating sophisticated network intrusions alongside near-simultaneous physical tactics across dozens of countries, resulting in millions of dollars of losses.**

_10 **A relatively small number of banking malware operations continues to evolve and dominate the global landscape.** These malware families, closely controlled by small groups of professional operators from Eastern Europe, have evolved to target new sources of wealth, such as cryptocurrency exchanges and online retailers.

_11 **The threat actors who developed SamsamCrypt and BitPaymer, the two most impactful ransomware threats observed by CTU researchers during the reporting period, have retained them for their exclusive and targeted use versus selling them as a service.**

_12 **The boundary between nation-state and cybercriminal actors continues to blur, as cybercriminals use tools and techniques that were once thought to be the sole preserve of nation-state threats. Similarly, nation-states are using criminal networks and tools to help achieve their own objectives.**

KEY FINDING #1

A steady level of "background noise" from low-level criminality is impacting businesses around the world.

Cybercrime is ubiquitous, and it represents a robust market economy. Goods and services are readily available for sale, and the technical barrier of entry is low for many types of unsophisticated criminal activity. This means that virtually anyone can become a cybercriminal and everyone is a potential target.

_01

Cryptocurrency mining remains an extremely popular way for criminals to monetize access to infected computers.

Despite Bitcoin and Monero losing well over half their value since January 2018 (see **FIGURE 1**), mining still provides a considerable return on investment. For some in the criminal community, mining is also less morally objectionable and less likely to draw law enforcement intervention than other types of attacks, as evidenced by the fact that some forums support mining but have banned the sale of more destructive threats, such as ransomware.

Contrary to suggestions that cryptocurrency mining is on the decline, network security events for cryptocurrency mining activity across Secureworks iSensor® Intrusion Detection Systems show mining attacks remain popular among criminals (see **FIGURE 2**).

CTU researchers looked at network traffic going from a large number of organizations to mining pools, domains that allow computers mining cryptocurrencies to work together to increase their likelihood of earning a reward. This research concluded that *at least* one in three organizations experienced some kind of cryptocurrency mining on their network in 2017 (see **FIGURE 3**), and that, in some cases, mining infections remained untreated for *more than a year*.

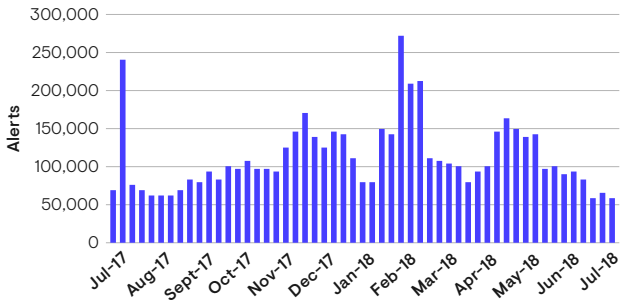


FIGURE 2: *Network security alerts for cryptocurrency mining network signatures. (Source: Secureworks)*

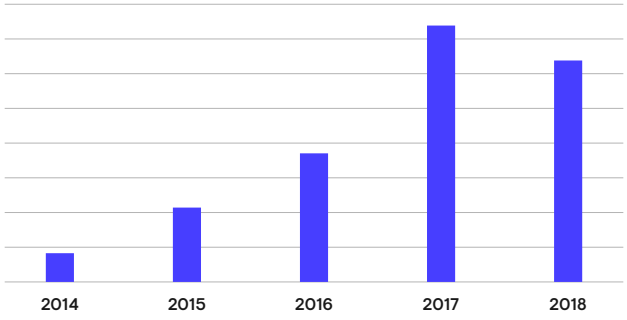


FIGURE 3: *Cryptocurrency mining activity on unique organizations per year. (Source: Secureworks)*

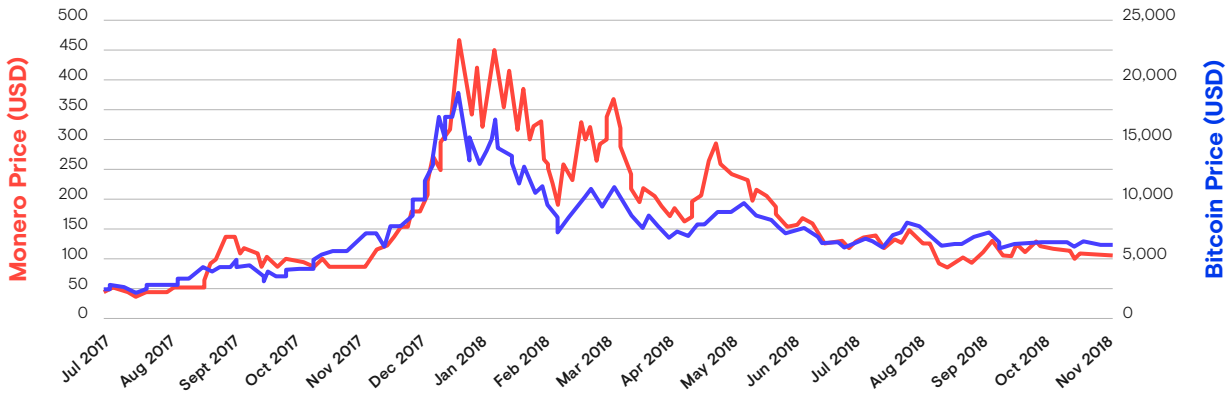


FIGURE 1: *Bitcoin and Monero prices, June 2017 to November 2018. (Source: coinmarketcap.com)*

Secureworks®

A number of very popular cryptocurrency miners are available for free from public code repositories. However, criminal actors on underground forums offer miners for sale that they claim are difficult to detect and may also include persistence mechanisms and other capabilities associated with more traditional malware (see **FIGURE 4)**. These tools present an extremely low barrier to entry for minimally sophisticated threat actors to monetize infected systems.

Recognizing that profitability comes from scale, resourceful criminal groups use underground forums to sell access to networks of infected computers around the world for the specific purpose of mining cryptocurrency. Botnets, such as the Smominru botnet, have reportedly generated millions of dollars in revenue for their controllers.

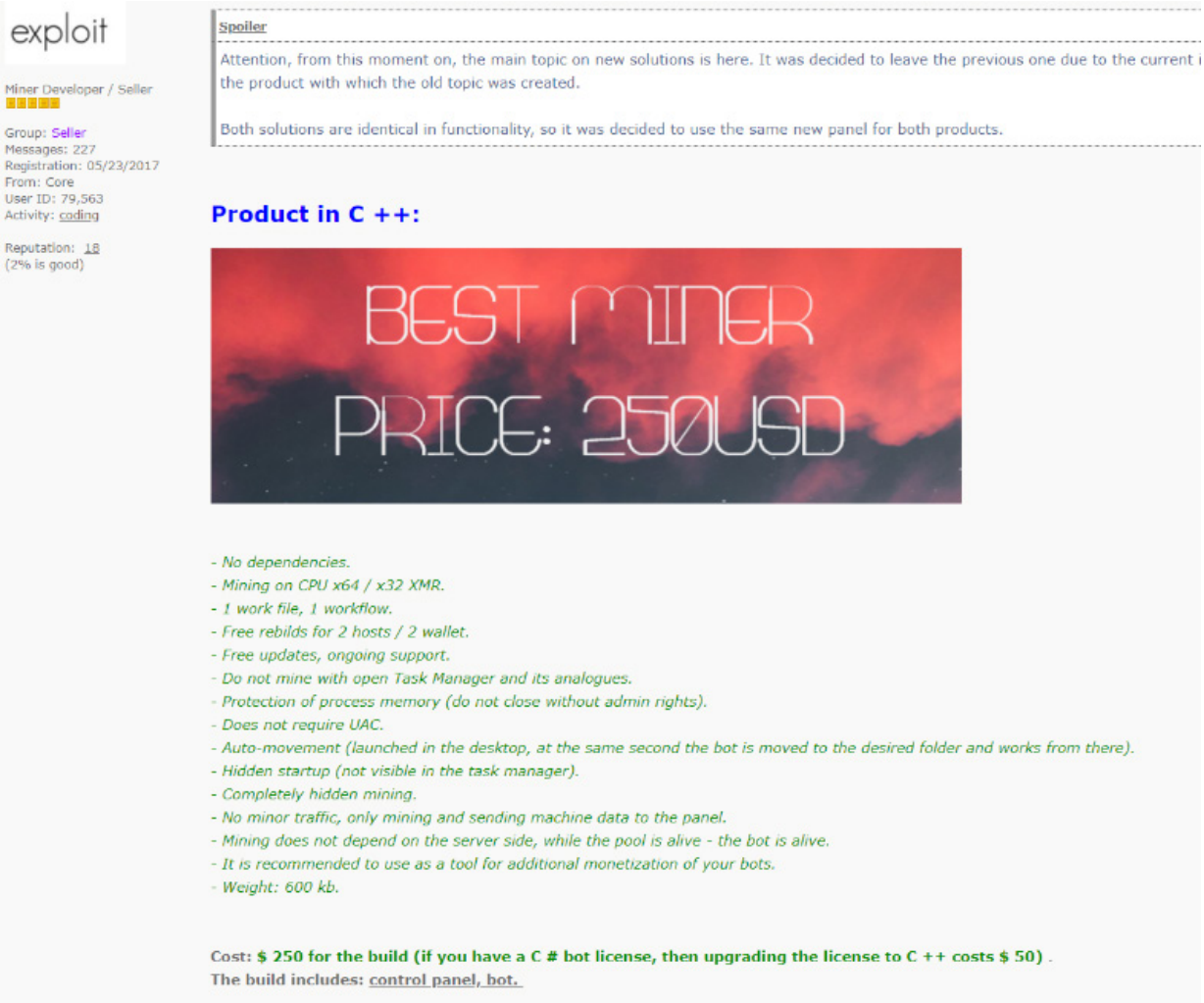


FIGURE 4: *Cryptocurrency miner "for sale" post.*

_02

There has been no significant decrease in the volume of ransomware, banking malware, point-of-sale (POS) memory scrapers or other threats available for purchase on underground forums.

Criminal actors continue to advertise banking malware, POS malware and ransomware on underground forums. Furthermore, there is no evidence that ransomware has been displaced by other capabilities such as cryptocurrency mining, and targeted ransomware attacks continue to be a worrying trend.

Advertised malware, such as the PandaZeus banking Trojan (see **FIGURE 5**), is widely distributed and is having a noticeable impact.

The growth of traditional file-encrypting ransomware did slow in 2017 due to numerous factors including the following:

- The retreat of several large cybercriminal groups that were previously consistent in distributing high-volume ransomware spam campaigns
- The reduced availability of mature, turnkey ransomware kits available for purchase or use through affiliate programs
- The sudden and dramatic rise of cryptocurrency prices, which made mining an appealing means of monetizing compromised systems and may have dis-incentivized the use of ransomware for some.

FIGURE 5: *PandaZeus malware builders for sale by alkipper, a broker of banking malware including KINS. (Source: Online forum)*

Secureworks

However, CTU researchers continue to track the emergence of new ransomware families and variants and see no evidence to support speculation that cryptocurrency mining is replacing this threat completely. Between July 2017 and July 2018, no less than 257 new and distinct ransomware families were observed.

For the most part, ransomware targeting remains indiscriminate, and these new families are unsophisticated and have not been particularly successful. There are some exceptions, however; familiar families like Locky and Cerber have been replaced by new market leaders such as GandCrab, a popular ransomware-as-a-service that releases regular updates and feature additions (see **FIGURE 6**).

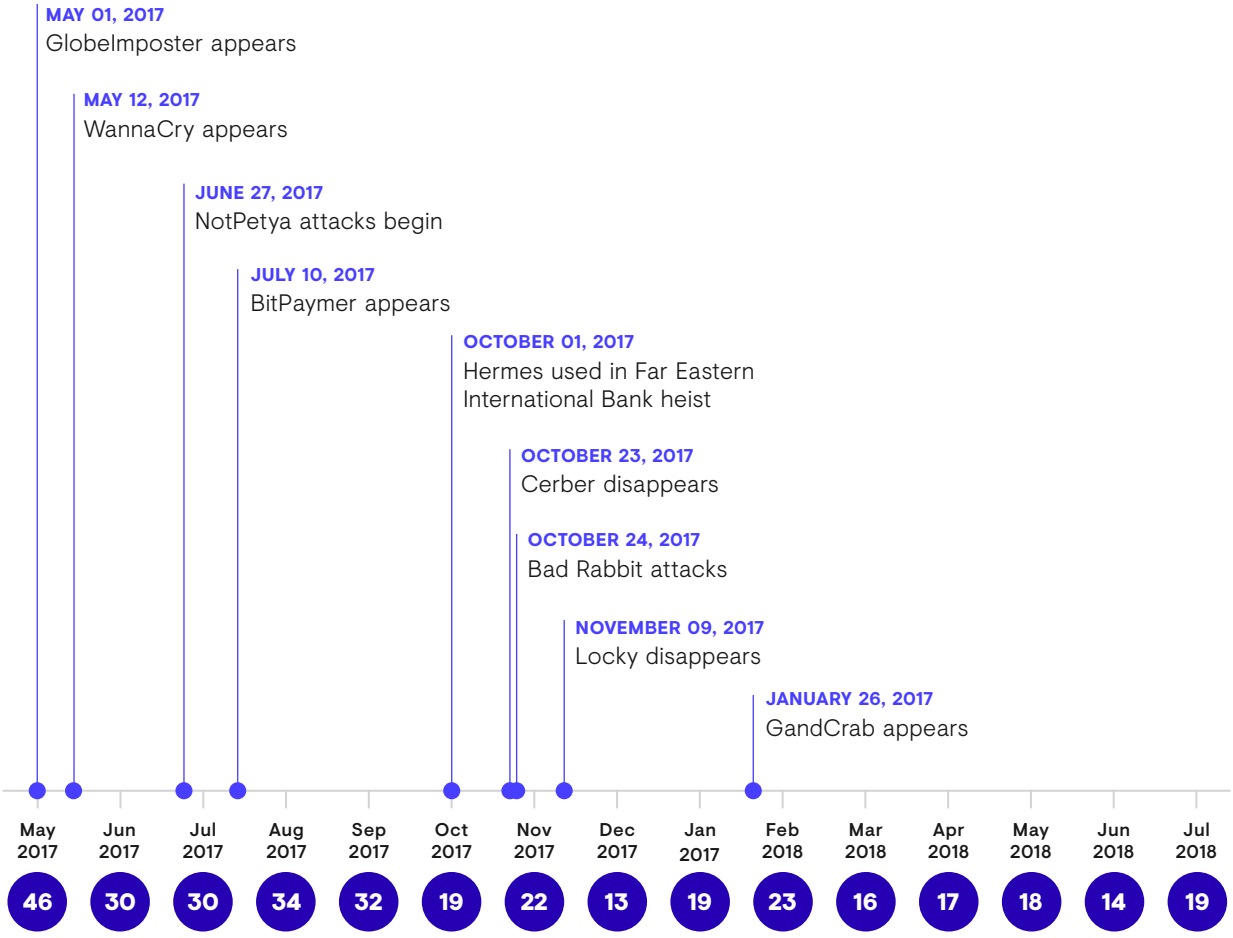


FIGURE 6: *Total new ransomware samples with notable events highlighted. (Source: Secureworks)*

GandCrab

The growing popularity of ransomware-as-a-service

In January 2018, CTU researchers identified a new piece of ransomware called Gandcrab being distributed by the RIG and Grandsoft exploit kits, offered for sale on Russian-language underground forums. The developers promoted Gandcrab's usability and the minimal effort required of criminal customers to deploy it (see **FIGURE 7**), and they even offered a partner program in which the developers received 30–40 percent of any resulting revenue from successful attacks.

In June 2018, Gandcrab was delivered in phishing campaigns by emails containing Word documents with malicious macros (see **FIGURE 8**).

Gandcrab version 4, which appeared around August 2018, supported additional languages over version 3, including English, German, Italian, Spanish, French, Korean, Japanese and Chinese. As with the Gandcrab version 3 campaign, the ransom amount was $1,200 worth of Bitcoin or Dash cryptocurrency (see **FIGURE 9**).

FIGURE 7: *GandCrab "for sale" post.*

FIGURE 8: *Phishing email. The attachment contains a malicious macro that downloads the Gandcrab ransomware. (Source: Secureworks)*

FIGURE 9: *Gandcrab version 4 ransom note. (Source: Secureworks)*

_03

Unscrupulous hosting providers help cybercriminals stay below the radar by offering them access to anonymized servers and Internet access.

Law enforcement can track down cybercriminals by following the breadcrumbs created when criminals use personal details to register phishing or command and control domains with legitimate hosting companies or by identifying the IP addresses criminals use to access their targets and other services. To reduce this risk, the cybercriminal underground has given rise to a number of hosting providers who take a relaxed view on ethics, do not implement and enforce rigorous terms and conditions on their services, and do not respond willingly to requests from law enforcement for information about their customers.

CTU researchers identified more than a dozen hosting providers advertising infrastructure services in forums. However, analysis of client telemetry shows that these hosting services typically appear in the context of various scams, spam runs, mass scanning and other low-level criminality, not as malware command and control infrastructure for the more sophisticated criminal actors. The sophisticated groups and openly malicious hosting providers prefer to use closed communication channels, such as Jabber chats, to trade their infrastructure.

Hosting services – advertised price: $100-300/month

- Sometimes known as “bullet-proof hosters,” these entities specialize in turning a blind eye to their customers’ behavior. In some cases, the provider may even advertise that they will resist requests from law enforcement or other agencies to identify their customers.
- The services advertised for sale range from simple virtualized private networks (VPNs) through virtualized private servers (VPSes) to dedicated hardware, nicknamed “dedic” hosting.
- In 2018, very few of the providers who host major criminal operations are advertising their services on open forums, however they still offer services via direct messages to malicious criminal actors or through established trust relationships.

CASE STUDY:

Brazzzers

Brazzzers (not to be confused with the pornography site conglomerate) is a hosting provider selling “Fast Flux” services.

Fast Flux is a domain name system (DNS) resolution technique whereby a domain resolves to a constantly changing list of IP addresses to avoid IP-based blocking. On investigation, it became clear to CTU researchers that Brazzzers was actually re-selling hosts from other service providers who typically had very few or no terms and conditions associated with them. One example was the hosting provider “PE Gornostay Mikhailo Ivanovich.” Hosting names that contain “PE” are for “private entities” in Russia and Ukraine. These types of registrants are frequently associated with less-respectable hosting providers.

The vast majority of IP addresses associated with PE Gornostay Mikhailo Ivanovich have been associated with either tech support scams, malicious scanning or malware activity. Between June 2017 and July 2018, there were more than 25,000 intrusion detection system (IDS) events associated with IPs assigned to PE Gornostay Mikhailo Ivanovich across the Secureworks client base. The majority of these events represented wide-scale scanning or other low-level activity but also included activity that would be considered a breach of acceptable terms and conditions for most legitimate service providers: alerts relating to attempted SQL injection, FTP login attempts, and outbound HTTP requests to suspicious domains. While this evidence demonstrates the ability for cybercriminals to keep a low profile, none of the activity originating from this hosting provider against Secureworks clients was associated with operations that CTU researchers identify as typical of sophisticated cybercriminal actors.

25,000

IDS events between June 2017 and July 2018 associated with PE Gornostay Mikhailo Ivanovich

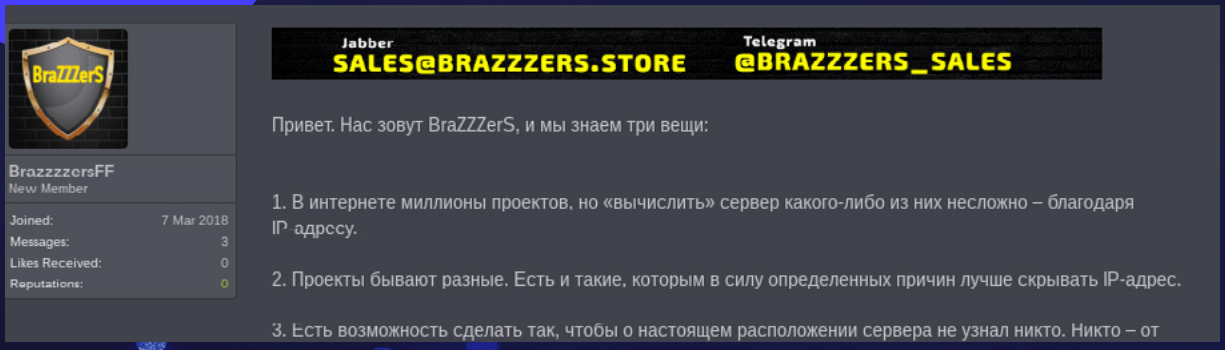


FIGURE 10: *Brazzzers Store Fast Flux hosting. (Source: Online forum)*

_04

Spam remains the leading means through which criminals deliver malware.

Spam remains the leading means of delivering malware into targeted networks. However, the number of massive, million-bot-strong spam botnets available for rent continues to decline. Cutwail, the elder statesman of such botnets, has been on a continuous decline since Operation Tovar in May 2014, which saw the demise of Cutwail's largest customer, Gameover Zeus (see **FIGURE 11**).

Cutwail, Necurs, Phorpiex, Onliner, Lethic and other botnets remain available for rent by well-connected and moneyed cybercriminals. However, operators of large botnets increasingly have begun insourcing spam operations with custom malware rather than relying on outsourced spam botnets. The Chanitor operators deliver their campaigns with Send Safe, Trickbot with RelayMTA and Emotet with a custom spam module.

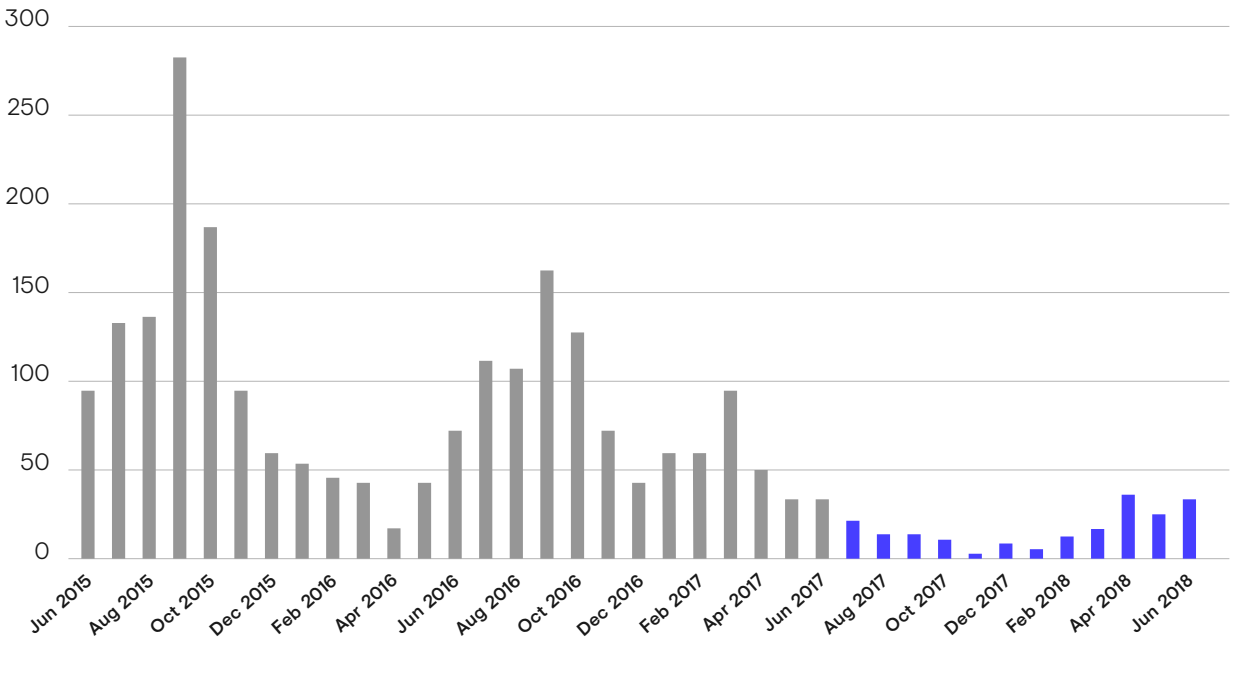


FIGURE 11: *Unique Cutwail botnet templates per month from June 2015 to July 2018. (Source: Secureworks)*

KEY FINDING #2

Data and unauthorized access continue to have a value in underground marketplaces, which means criminals will continue to pursue them.

Massive customer data breaches have become common in recent years. For cybercriminals around the world, data continues to represent a treasure trove of opportunities for financial gain.

_05

Personally identifiable information (PII), including full biographic dossiers, payment card data and other bulk data sets, are regularly offered for sale in underground forums.

Advertised sale prices for full biographic information, called "fullz," and other personal data is a poor indicator of their value without also knowing the quality of the data and the price that someone was actually willing to pay for it. Snapshot observations of that kind also do not necessarily provide evidence of market trends. They do, however, give an indication of what the seller thinks the market will bear at that point in time.

Between July 2017 and July 2018, CTU researchers observed fullz for sale for between $10 and $25 and verified credit card information for sale for between $12 and $70, depending on the type of card (see **FIGURE 12**).

Some of this data was undoubtedly stolen by sophisticated cybercriminals with the intention of monetizing intrusions targeting POS terminals or consumer online banking.

Service	Bin	Type	Refund	Country & Mark	Dumped In	Price	Qty
Track 1+2 Code 201	556750 No Pin	Mastercard Corporate Fleet Card	Yes	USA Credit	USA, MN	$48.4	1
Track 2 Code 201	527516 No Pin	Mastercard Standard	Yes	USA Debit	USA, PA	$12.45	2
Track 2 Code 201	514344 No Pin	Mastercard Standard	Yes	USA Debit	USA, MA	$13.2	1
Track 2 Code 201	481588 No Pin	Visa Business	Yes	USA Debit	USA, PA	$27.3	1
Track 1+2 Code 201	556963 No Pin	Mastercard Corporate Fleet Card	Yes	USA Credit	USA, SC	$50	1
Track 2 Code 201	474487 No Pin	Visa Platinum	Yes	USA Debit	USA, AL	$17.22	3
Track 2 Code 201	427538 No Pin	Visa Classic	Yes	USA Debit	USA, MA	$19.95	1
Track 2 Code 201	435545 No Pin	Visa Platinum	No	USA Debit	USA, SC	$18.66	1
Track 2 Code 201	400344 No Pin	Visa Platinum	Yes	USA Credit	USA, NY	$19.32	2
Track 1+2 Code 201	553258 No Pin	Mastercard Corporate Fleet Card	Yes	USA Credit	USA, SC	$65.6	1

FIGURE 12: *Verified card details for sale.*

_06

Criminals also use forums to sell access to compromised systems and organizations.

Criminals have been quick to realize the inherent value of access to data or compromised systems, particularly where it can be used to facilitate fraud or some other kind of illicit activity. Threat actors covet direct access to servers that receive high volumes of visitors (who can then be targeted) and to compromised systems that hold potentially sensitive information. Advertised prices for these assets can be as low as 50 cents for a single RDP, used by criminals as a catch-all term for a remotely accessible host, and up to $20,000 for direct access to a compromised environment.

Typically, RDPs are one-off compromised hosts, often in a data center but sometimes on an individual's home computer. The most famous RDP market is xdedic. Xdedic was founded in 2014 and subsequently migrated to a Tor-only site. The more-sophisticated RDP vendors install malware running as a persistent service on the compromised host, which provides access to a full graphical user interface (GUI) for their customers through OpenVNC or FreeRDP. The less-sophisticated vendors may simply provide credentials to use Microsoft's remote desktop protocol or secure socket shell (SSH). The customer who purchases access to the host has free access to anything on the host or that the host has access to. Frequently, hosts sold as an RDP will not provide access to other systems within a corporate organization.

When a criminal actor determines it has obtained broader access to a corporate organization, it will often raise the price of access and advertise this access appropriately. Between July 2017 and July 2018, CTU researchers observed advertised prices for direct access to compromised organizations in the thousands of dollars. These ranged from a common advertised price of around $1,500 all the way up to a (probably over-priced) $20,000 in one case.

The Value of Data as a Global Commodity

In order to be profitable, global underground forums for stolen data must continue to promote a diverse range of criminal products and services, retain a large enough user base and avoid too much attention from law enforcement investigators or security researchers. Otherwise, they risk losing their users to other forums and ultimately failing.

Cost of Chinese Cybercrime

Sources cited in research soon to be published by the Dutch National High Tech Crime Unit (NHTCU) assess that Chinese cybercrime, predominantly focused on Chinese victims, cost the Chinese economy $28.4 million USD in 2016.

The Chinese underground, as a whole, has its own very distinct culture, but the NHTCU analysis describes a situation with parallels to criminality elsewhere in the world. Banking credentials (differentiated between Chinese and non-Chinese bank accounts) are offered for sale; in one case, analysts found that one week of access to a leaked-data search engine was being sold for the equivalent of $4.50. Other goods and services offered for sale included access to compromised botnets (僵尸网络, or jiāngshī wǎngluò), the malware used to generate additional nodes in these botnets (木马作者, mùmǎ zuòzhě) and exploits.

KEY FINDING #3

A small subset of professional criminal actors are responsible for the bulk of cybercrime-related damage, employing tools and techniques as sophisticated as most nation-state threat actors.

"Commodity" cybercrime is a threat that organizations should take seriously. However, the reality is that a significant proportion of the profits from cybercrime go to a relatively small number of threat actors and organized criminal groups who operate outside of accessible forums on the dark web.

The technical capabilities and levels of operational security employed by these groups are on a par with or better than a large proportion of the nation-state threat actors that CTU researchers investigate. The close-knit nature of these criminal actors makes them complicated to track via underground forums. Instead, advanced technical tracking capabilities provide the best insights into their malicious activities.

_07

Business email compromise (BEC) and email account compromise (EAC) have accounted for $12.5 billion in financial losses between October 2013 and May 2018, according to figures released by the FBI.

In July 2018, the FBI reported that BEC and EAC had generated total exposed dollar losses of more than $12.5 billion from October 2013–May 2018. A whopping $7.2 billion of these losses happened between December 2016 and May 2018. Fraud enabled through EAC is lucrative for criminals and is, therefore, a threat for anyone involved in lengthy and high-value transactions, such as business procurement processes or private real estate purchases.

CTU researchers have gained unique insight into the methodology used by sophisticated criminal gangs such as GOLD GALLEON to defraud victims (see **FIGURE 13**).

01 Attacker scans the seller's email account(s)- for high-value transactions in the preorder phase (i.e., a buyer has asked for a quote).

02 Attacker sets up a redirect rule in the seller's email to hijack future emails from the buyer.

03 Buyer sends a purchase order (PO) to the seller, and the PO is redirected to the attacker.

04 Attacker "clones" the buyer's email (using a similar but misspelled domain) and forwards the PO to seller, establishing a man-in-the-middle (MITM) compromise.

05 Seller replies to "buyer" (the cloned email address controlled by attacker) with an invoice containing payment instructions.

06 Attacker modifies the bank payment destination in the invoice and forwards the modified invoice to the buyer.

07 Buyer wires money to attacker-controlled bank account.

08 Seller's email is compromised by phishing or malware.

FIGURE 13: *Typical BEC process. (Source: Secureworks)*

Gaining access to one of the email accounts involved in a transaction is essential to the successful execution of a fraud enabled by BEC. Commercial off-the-shelf malware such as the Predator Pain Trojan, iSpySoft Infostealer or HawkEye Keyloggger are commonly used. This malware is disguised using commercial "crypters," such as Cyber Seal, to avoid detection by anti-virus software. Alternatively, phishing emails trick users into disclosing their login credentials, which can then be used to log in to Internet-accessible email accounts.

The organized criminal groups conducting this form of fraud have built up their experience in launching effective social engineering techniques. It is very difficult for busy individuals involved in processing the sorts of transactions that are typically targeted to spot the deception at the point where it occurs.

Preventing criminals from gaining access in the first place is critical. The most effective defense tactics include multi-factor authentication on Internet-accessible email accounts, user awareness education on phishing, endpoint controls to detect malware running on machines, and log monitoring to detect anomalous login activity on accounts.

Even with those measures in place, organizations should assume that at some point they will be successfully targeted. Some of the additional defense tactics Secureworks has seen used to thwart BEC attacks include robust controls around financial payments being sent to new accounts or those with modified account details, as well as "out-of-band" techniques such as phone calls or written correspondence, where authorizers communicate that the financial details provided at the start of the transaction process will not change.

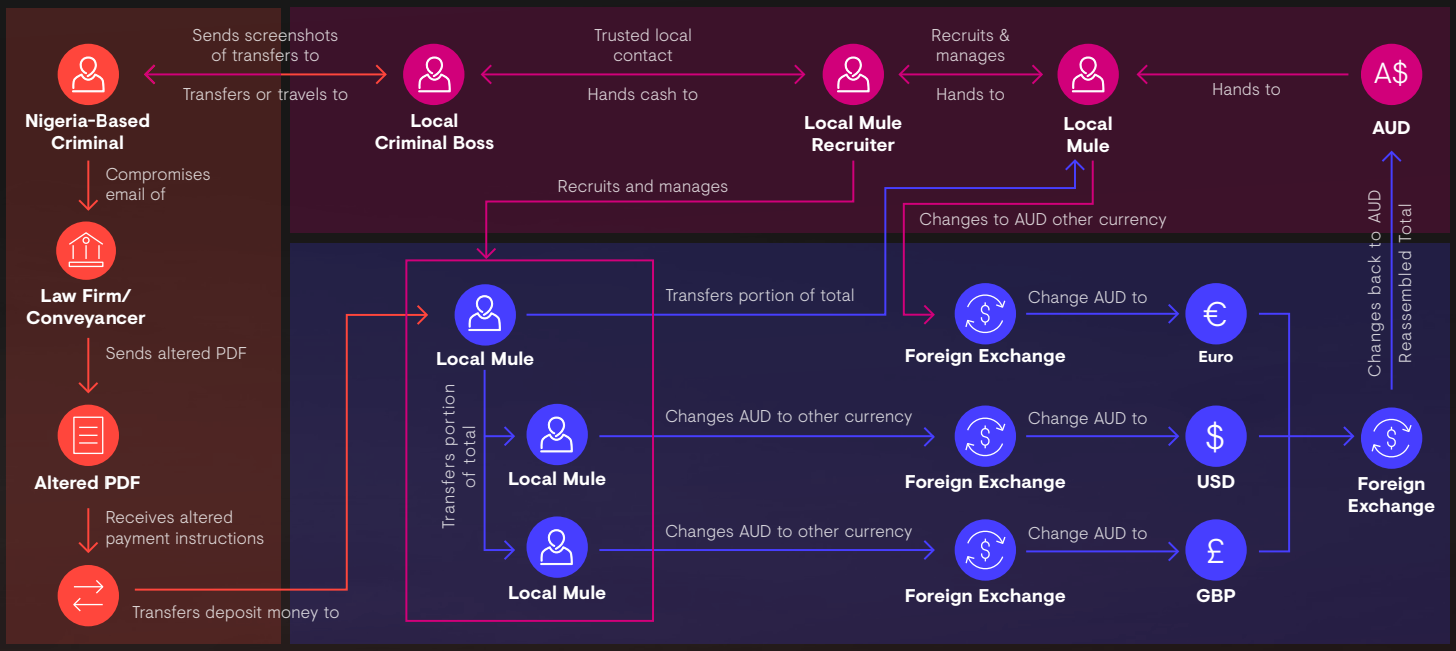
CASE STUDY:

GOLD MILTON

Coordinated and sophisticated tactics fuel email account compromise.

Purchasing real estate involves one-off, high-value transactions between parties who may not know each other particularly well. This provides an ideal opportunity for EAC-enabled fraud. CTU researchers have assessed GOLD MILTON to be a Nigeria-based group tracked by Secureworks that has extensively targeted real estate agents and law firms in Australia. Trusted members of the group have been sent from Nigeria to Australia in order to coordinate their nefarious activities, and networks of local money mules have been established to withdraw the proceeds of their crimes, which are then sent back to Nigeria as physical cash, transferred electronically via international money transfer services or as cryptocurrency, or converted to physical goods (see **FIGURE 14**).

FIGURE 14: *GOLD MILTON's operating methodology. (Source: Secureworks)*



Stage 01

A Nigeria-based criminal compromises the Outlook Web Access of various real estate agents and/or law firms involved in conveyancing or some other aspect of property deals. The criminal alters the standard payment instruction PDF just before it is sent to customers or vendors, using the real estate deal schedule on the victim's OWA calendar to determine when the PDF should go out. The victim receives the PDF with altered payment instructions and dutifully transfers the deposit to a local mule's account, which is often a business account set up with false documents to enable it to receive and send larger amounts per transaction than a retail account. The Nigeria-based criminal then uses WhatsApp to send photos or screenshots to both the local criminal boss and local mule recruiter showing the transaction amount and destination account.

Stage 02

The local mule takes stolen funds and either physically or digitally splits the total amount among the other mules in the syndicate. Each mule then takes or transfers their portion of the funds to a different foreign currency exchange business and converts the cash to Euro, GBP and/or USD.

These funds are then "reconstituted" into AUD through transactions at yet another foreign currency exchange or multiple exchanges.

Stage 03

A mule then hands these funds to the local Nigerian mule recruiter, who then takes out everyone's cut of the money and hands the remainder to the local Nigerian criminal boss through a number of possible methods:

- Loaded onto gift cards and mailed to Nigeria
- Placed with traveling mules, who fly back to Nigeria
- Used to buy electronics, which are mailed back
- Remitted via Western Union, etc.
- Used to buy jewelry and expensive watches that are then simply worn on flights out of Australia
- Used to buy bitcoin

_08

Sophisticated criminal gangs have combined advanced social engineering and network intrusion techniques with POS malware to generate millions of dollars of revenue through stolen payment card data.

On August 1, 2018, the U.S. Department of Justice (DoJ) announced the arrest of three Ukrainian nationals who are allegedly members of a sophisticated cybercrime group tracked by CTU researchers as GOLD NIAGARA and also known as FIN7. The DoJ indicted this group for network intrusions in 47 states that resulted in the theft of more than 15 million card details from 3,600 business locations. In reality, while the arrests were notable and occurred several months before the DoJ indictment, GOLD NIAGARA remains a highly active and dangerous threat.

The market for selling credit card details on underground forums incentivizes criminals to target POS terminals, where credit card details can be extracted from the memory of the running device by using specialized malware. In January 2018, CTU researchers observed the source code for Katrina v3.0 POS malware available for sale for $350, with assurances that it works on systems from Windows XP to Windows 10.

In 2015, liability for counterfeit fraud shifted to either the merchant or the bank, whichever has not adopted chip technology. However, slow adoption in the United States in particular has meant that there are a number of sophisticated groups conducting network intrusions and stealing millions of card details from POS terminals.

Cybercriminals are also clever about monetizing card data even after the theft has been discovered, and credit card dump sites such as JokerStash have come under more scrutiny as a possible way for sophisticated criminals to do just that. Common Point of Purchase (CPP) notifications are sent to retail locations after financial institutions have determined that cards with fraudulent charges were previously used at the same location. In cases where CPP notifications have been issued, CTU researchers are aware of instances where threat actors dumped cards in bulk on JokerStash after news of a compromise became public. The evidence suggests that the criminal sellers were intent on extracting every last bit of value (see **FIGURE 15**).

Over the last five years, CTU researchers have observed significant improvements in the tooling and capability of groups like GOLD NIAGARA and GOLD FRANKLIN involved in the theft of financial card data using POS malware. Organizations processing data of this kind are advised to stay vigilant against these targeted attacks.

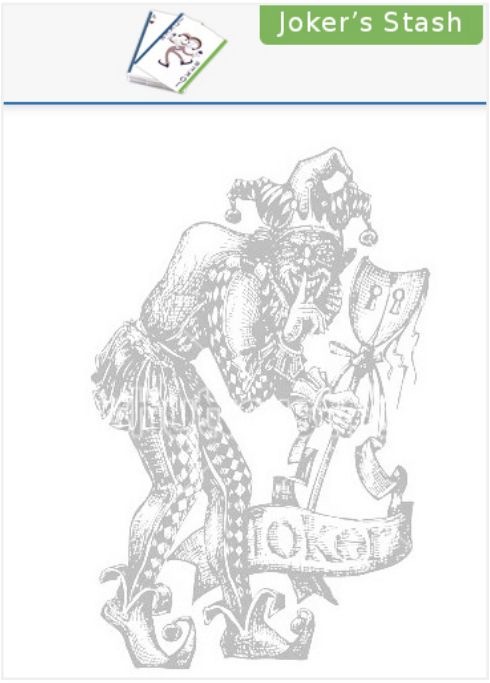


FIGURE 15: *JokerStash credit card dump site. (Source: Secureworks)*

CASE STUDY:

GOLD NIAGARA

Capabilities of POS threat groups differ, but competency is a shared trait — Part 1.

Active since: At least 2015

Impact and scale: DoJ indictment states 15 million credit card records from 6,500 individual POS terminals.

Signature tools and techniques used: A variety of backdoors written in VBS, JScript, JavaScript and more. Also, Cobalt Strike, Carbanak, Meterpreter and a number of POS malware variants, such as SuperSoft.

Monetization of activity: Sale of card details through underground forums, notably JokerStash.

Capability development over time: GOLD NIAGARA is extremely competent. They have demonstrated advanced social engineering techniques to gain initial access. In one case, the spear phishing email sent by the group to a target claimed that a group who had dined at the restaurant the previous evening had been struck down with food poisoning. It included an attached document that the sender claimed was an outline for proposed legal action. This kind of lure would be incredibly difficult for any restaurant manager to ignore (see **FIGURE 16**).

Active POS Threat: Gold Niagara

Simple methods. Simple tools. Anything but simple adversary.

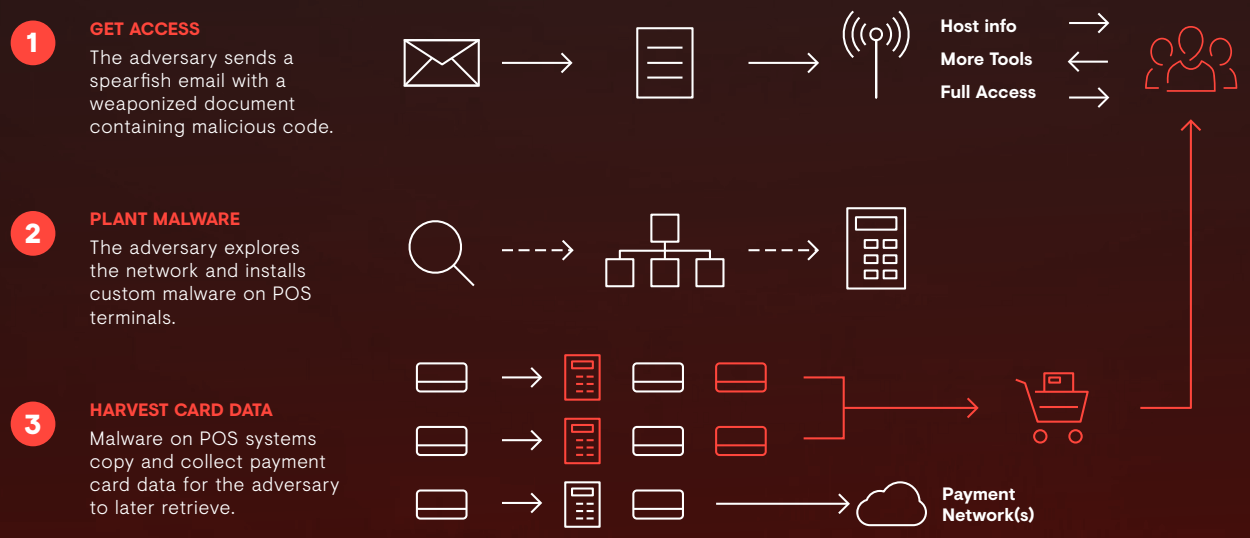


FIGURE 16: *GOLD NIAGARA operating methodology. (Source: Secureworks)*

CASE STUDY:

GOLD FRANKLIN

Capabilities of POS threat groups differ, but competency is a shared trait — Part 2.

Active since: At least 2015

Impact and scale: GOLD FRANKLIN is one of the most disruptive financial threats that Secureworks analysts tracked between 2014 and 2018. FrameworkPOS has been deployed to thousands of POS terminals, and CTU researchers have counted tens of millions of stolen credit cards.

Signature tools and techniques used: Framework POS malware. (The same author also likely created MozartPOS, although Secureworks CTU researchers have no evidence connecting MozartPOS to GOLD FRANKLIN). The group also uses a number of open source exploitation and remote access tools including Metasploit, Mimikatz, PowerSploit and LogMeIn.

Monetization of activity: Sale to underground forums for re-sale.

Capability development over time: When the group was first observed in 2012, it made basic operational mistakes such as misconfiguring services and failing to overcome basic security controls. It has now eradicated those mistakes and demonstrated an ability to remain undetected and steal payment card information from victim networks over a period of months (see **FIGURE 17**).

Active POS Threat: Gold Franklin

Exploiting relationships.

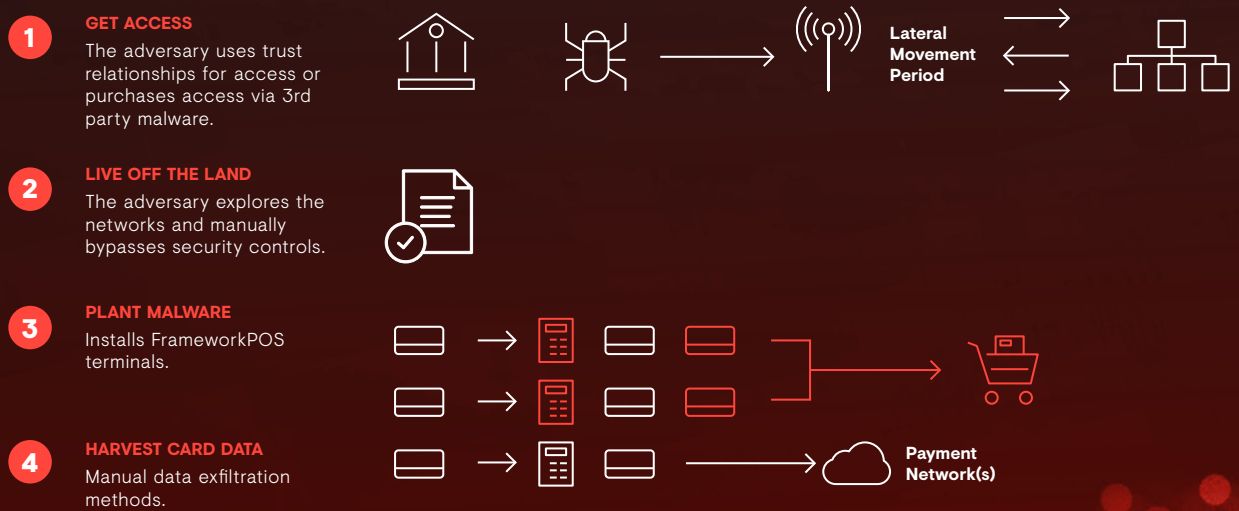


FIGURE 17: *GOLD FRANKLIN operating methodology. (Source: Secureworks)*

_09

Criminals have conducted "global cashout" and ATM jackpotting operations by coordinating sophisticated network intrusions alongside near-simultaneous physical action across dozens of countries, resulting in millions of dollars of losses.

On August 11, 2018 criminals withdrew $13 million USD from accounts resident at Cosmos Bank, the second-largest cooperative bank in India. The withdrawals were made via 14,849 individual transactions in just over two hours from ATMs in 28 countries. Two days later, the criminals made three transactions through one of Cosmos Bank's Society for Worldwide Interbank Financial Telecommunication (SWIFT) terminals to transfer a further $1.9 million USD to a bank account located in Hong Kong.

These kinds of "cashout operations" involve extremely complex logistics and, as such, are typically the purview of well-organized criminal and government-backed criminal actors. The perpetrators need to first gain access to the bank network and remain there undetected for a sufficient period of time in order to gain a detailed understanding of the anti-fraud controls and processes they need to subvert so that they can freely withdraw funds. In parallel, they need to be able to recruit and control a large network of "cashers," often spread across dozens of countries, who are responsible for conducting near-simultaneous physical withdrawals of the stolen money.

The high levels of technical competence and organization required mean that global cashout operations are relatively rare, but highly lucrative (see **FIGURE 18**).

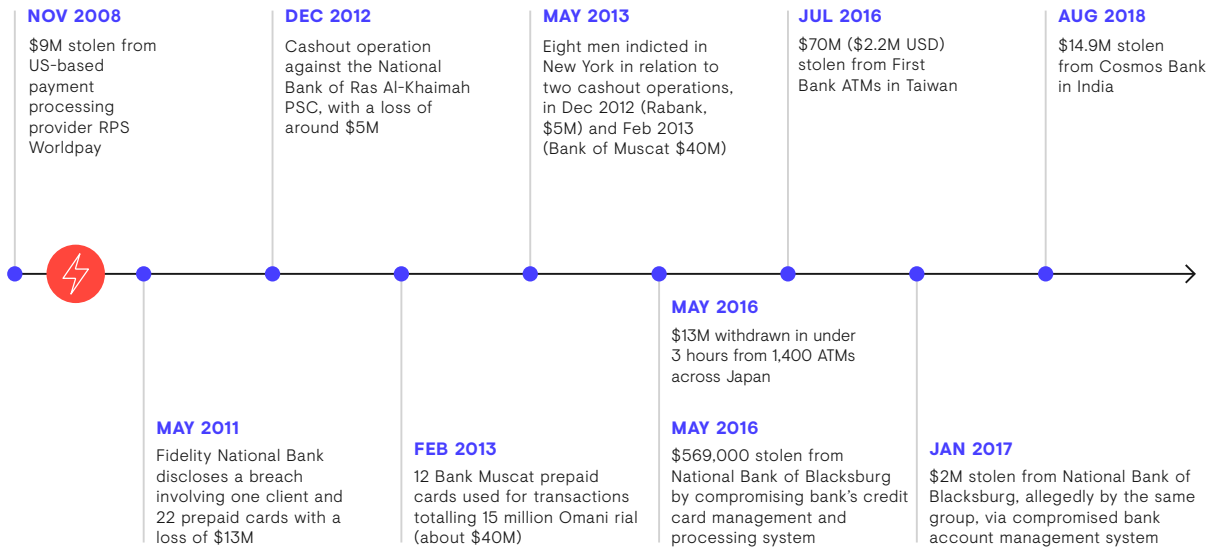


FIGURE 18: *Notable unlimited cashout operations over the years. (Source: Secureworks)*

CASE STUDY:

GOLD KINGSWOOD

Fake companies lend legitimacy to phishing campaigns.

In January 2018, CTU researchers observed phishing activity using malware dubbed SpicyOmelette, a full-functioned JavaScript RAT, and Sonemone, a credential theft tool. Both of these tools are provided as malware-as-a-service to the GOLD KINGSWOOD threat actor group.

The phishing campaign used a recruitment theme. Both the SpicyOmelette RAT and the Sonemone tool were signed using code-signing certificates purportedly issued by companies called DapsOne LTD and Auxira Ltd, probably to add further legitimacy in case of any superficial checks of the files and to avoid detection based on file reputation. Both companies were registered in the United Kingdom in August 2017 using addresses associated with businesses that provide mail-forwarding services for organizations without a permanent or fixed address. At the time this campaign was identified in May 2018, neither company had a website, phone numbers or any other publicly available information, and CTU researchers believe they may have been set up solely to add legitimacy to the malware. The effort it took to create these front companies offers a glimpse into the sophistication of the tools used by GOLD KINGSWOOD and other criminal groups.

Other criminal groups have targeted ATM infrastructure directly. In March 2018, Europol arrested "Denis K," a Ukrainian national and alleged malware developer, in Spain for his part in a series of thefts since 2013 that Europol estimated had cost €1 billion to banks in more than 40 countries. Spain's Interior Ministry reported at the time that Denis K had personally accumulated about 15,000 bitcoins (roughly $120 million USD, at the time it was reported) from this activity.

Denis K is associated with a criminal threat group CTU researchers track as GOLD KINGSWOOD, also referred to as Cobalt gang. They are highly capable and resilient; CTU researchers observed a phishing campaign linked to GOLD KINGSWOOD on March 7, the day after Denis K was arrested in Spain, indicating that the arrest did not cause a halt in operations, at least in the short term.

Active since at least 2016, GOLD KINGSWOOD initially focused on Russian banks but subsequently expanded to target financial institutions around the world. The group has also been observed targeting organizations in credit card processing and other fund-transfer areas of financial services. Their ultimate objective when targeting banks is to illegally withdraw funds by one of three methods: ATM jackpotting, causing ATMs to spit out money to local cashers; artificially increasing the balance on selected accounts and then withdrawing the money from those accounts; or transferring funds electronically to alternative, criminal-controlled accounts.

_10

A relatively small number of banking malware operations continues to evolve and dominate the global threat landscape.

A small list of cybercrime malware is making the greatest impact, including — but not exclusively limited to — the malware families described in this section. In some cases, they make money for their owners through an affiliate business model; in others, by using highly targeted methods to extort large sums of money from victims. What characterizes these variants is the tight control the malware developers exhibit and the malware's ability to evolve to remain effective against new targets and new defensive techniques.

Emotet: A Prolific Downloader

Emotet has been the most prevalent threat observed across the Secureworks client base since late 2017. It evolved from the Bugat banking Trojan in 2010 to an advanced banking Trojan in 2014 to a malware distribution framework in 2018. The Emotet downloader is distributed by a phishing kit as a loader alongside malicious Word documents and uses compromised web servers for the first level of command and control infrastructure contacted by the malware. It has been observed to download a range of secondary payloads (see **FIGURE 19**), including Server Message Block (SMB) modules that propagate through compromised networks using a hardcoded list of popular passwords and tools to steal credentials and enumerate mail contacts. The goal is likely to launch additional spam and standalone banking Trojans such as PandaZeus.

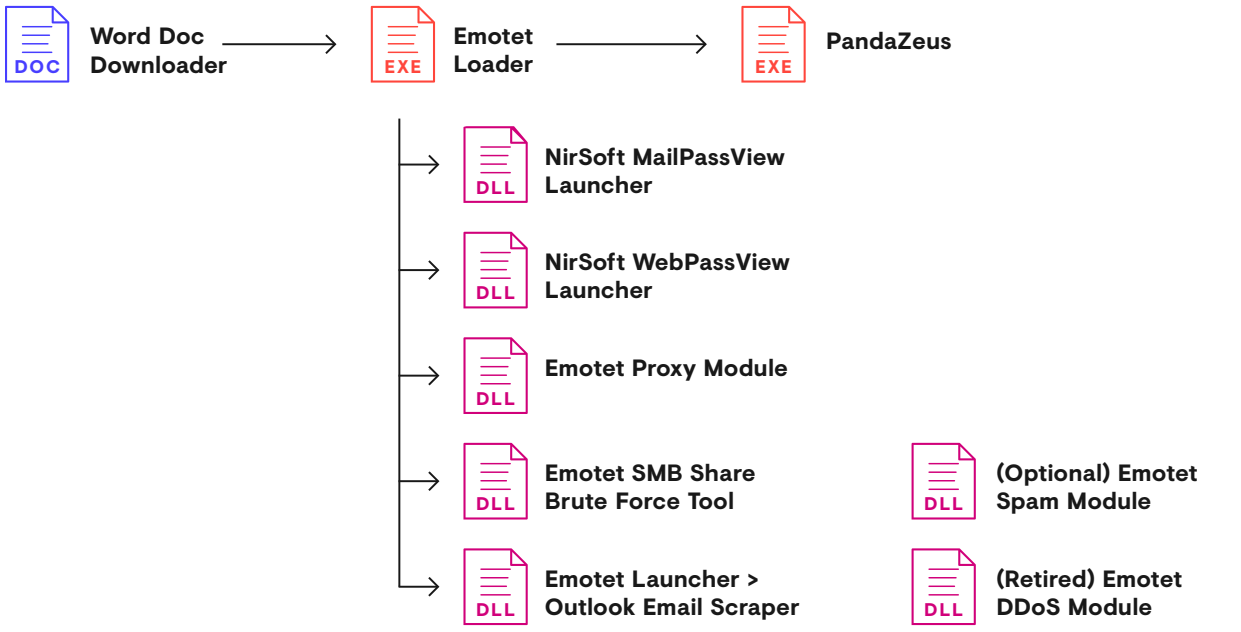


FIGURE 19: *Modules and payloads in a standard Emotet loader session. (Source: Secureworks)*

Secureworks

TrickBot: Targeted and Incorporating New Types of Wealth

In 2017, TrickBot remained a top threat targeting financial institutions and their customers. Trickbot is operated by a core group of threat actors who lease the use of the botnet to individuals and other groups. During the period of analysis for this report, TrickBot added more than 400 organizations across the globe to its target set (see **FIGURE 20**). These targets were mostly in North America and Europe, largely absent from South America, Asia and Africa, and completely absent in Russia and other Commonwealth of Independent States nations.

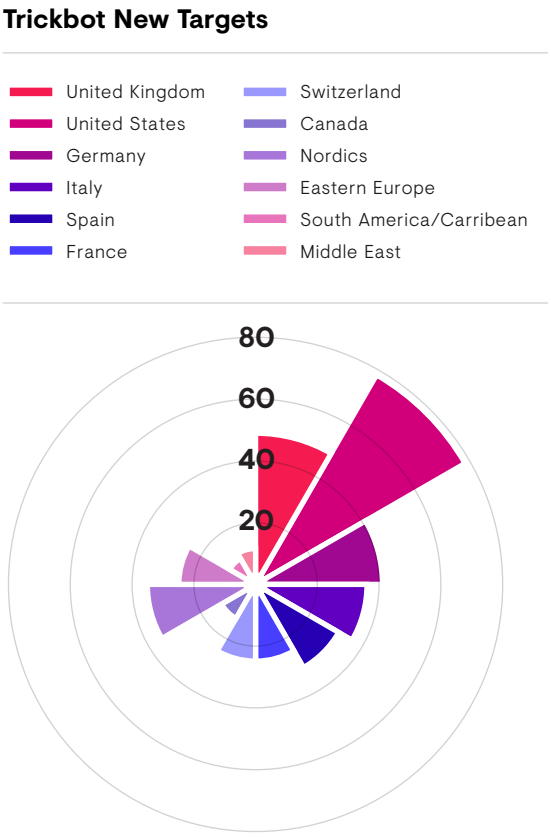


FIGURE 20: *Geographic distribution of TrickBot targets added July 2017 to July 2018. (Source: Secureworks)*

The overwhelming majority of these targets were financial institutions, including organizations involved in commercial and retail banking, wealth management, securities brokerage and money transmission (see **FIGURE 21**). The targeting, however, continued to expand to include retailers, cryptocurrency exchanges, a customer relation management (CRM) firm, career recruitment platforms and payroll processors.

In February 2018, TrickBot added a "spreader" module that uses the Mimikatz tool to recover Windows credentials that are then used to copy and execute the malware throughout a compromised network using the SMB protocol. Coupled with the "worm" module released in July 2017 that implements the ETERNALBLUE exploit, this new development enabled single infections to turn into widespread outbreaks affecting hundreds or thousands of endpoints within an organization. Even in cases where financial fraud did not occur, the disruption of business operations and the cost of large-scale remediation had enormous costs.

In April 2018, CTU researchers began to observe a new module distributed to a smaller selection of victims. This module placed the PowerShell Empire post-exploitation framework on infected machines. Doing so gave the TrickBot threat actors interactive access to the compromised network and allowed the perpetration of more targeted operations.

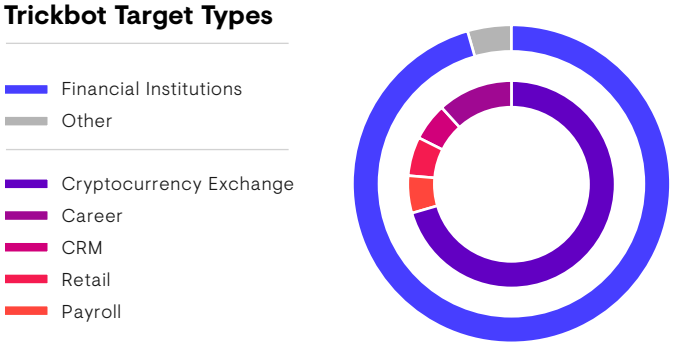


FIGURE 21: *Types of TrickBot targets added July 2017 to July 2018. (Source: Secureworks)*

_11

The threat actors who developed SamsamCrypt and BitPaymer, the two most impactful ransomware threats observed by CTU researchers during the reporting period, have retained them for their exclusive and targeted use versus selling them as a service.

In terms of scope and scale of incidents, the most damaging ransomware attacks investigated by CTU researchers have been attributed to SamsamCrypt and BitPaymer. These ransomware families, which are used exclusively by their respective operators, are carefully deployed by seasoned operators in a manner that maximizes damage to — and sometimes results in the complete destruction of — the victim's IT network.

The SamsamCrypt ransomware, which CTU researchers have associated exclusively with the GOLD LOWELL threat group since it first appeared in late 2015, is deployed to business-critical assets manually. It is introduced into victims' networks through weak network perimeter access points, such as poorly secured Windows servers with RDP enabled.

BitPaymer is ransomware used by the operators of Bugat v5, also known as Dridex, in targeted attacks first observed in July 2017. After obtaining access to the environment, the Bugat v5 operators move laterally through the environment with tools such as PsExec and RDP, and might choose to deploy BitPaymer. CTU researchers assess that the same developer(s) who created Emotet and Bugat v5 also created BitPaymer. BitPaymer operations have earned the crew millions of dollars through Bitcoin payments. The criminal actors responsible may have transitioned to monetization via ransomware as financial institutions have become better at identifying fraudulent high-value transfers from compromised business accounts. The same threat actors have been observed stealing documents from compromised organizations before encrypting hosts with BitPaymer.

GOLD LOWELL

In analyzing the GOLD LOWELL threat group's activities since 2015, CTU researchers identified a new breed of ransomware threat. Rather than indiscriminately delivering ransomware via phishing email or "drive-by" downloads from compromised websites, GOLD LOWELL deliberately delivers ransomware to critical assets from inside a compromised network.

GOLD LOWELL is opportunistic in the sense that victims are identified based on publicly accessible vulnerabilities or poorly secured Internet-facing servers. However, once a target has been identified, the threat group's behavior is extremely targeted. Because of the systematic way in which it operates, GOLD LOWELL has caused extensive damage, amounting to millions of dollars in either remediation costs or paid ransoms.

_12

The boundary between nation-state and cybercriminal actors continues to blur, as cybercriminals continue to use tools and techniques that were once thought to be the sole preserve of nation-state threats. Similarly, nation-states are using criminal networks and tools to help achieve their own objectives.

In March 2018, a threat actor likely associated with the Iranian government used access that had previously been leveraged for espionage to deploy a cryptocurrency miner across the environment. CTU researchers have also observed other government-backed espionage groups deploying cryptocurrency miners within compromised networks.

In August 2018, CTU researchers assessed with moderate confidence that a campaign using GandCrab version 4 to target South Korean users and cryptocurrency wallets was part of a broader pattern of cyber attacks by the Democratic People's Republic of Korea against the South Korean population and infrastructure.

These examples, along with the various examples of advanced tradecraft demonstrated by criminal actors throughout this report, show how the line between cybercrime and nation-state threats is and has been blurred for a number of years. This will come as no surprise to anyone who tracks the advanced criminal actors discussed in this report. The notion that nation-state-sponsored advanced persistent threats (APTs) are dimensionally different from cybercrime is fundamentally flawed; CTU researchers' analysis shows that advanced criminal actors operate in the same way government threat actors do, and in many cases the tools and techniques they employ are even more advanced.

Conclusion

Any meaningful analysis of the cybercrime landscape needs to take account of the underground forums and marketplaces, because the interactions that occur there drive high-volume, low- to mid-level criminality. However, it only provides part of the picture.

The other, more harmful aspect of the criminal underworld are the highly organized, resourceful and capable criminal actors who operate anonymously below the proverbial iceberg and are responsible for the overwhelming majority of losses associated with cybercrime. Sophisticated social engineering, detailed reconnaissance, advanced and highly obfuscated malware and targeted network intrusions are all techniques more commonly attributed to the nation-state APT actors who often grab the headlines. But the reality is that both criminals and government teams will employ techniques and tools adequate for achieving their objectives. For organized criminal groups, the sheer scale of their operations means that there is a high chance that malware and command and control infrastructure will eventually be detected and identified. Criminals will adjust to that challenge by investing up front and making continuous improvements in order to ensure those operations continue to be effective. By necessity, they use sophisticated techniques that are often more advanced than the majority of the nation-state groups tracked by CTU researchers.

The observations of CTU researchers over the last 12 months show that the threat from cybercrime is adaptive and constantly evolving. To stay ahead of it, it is imperative that organizations develop a holistic understanding of the landscape and how it relates to them, and tailor their security controls to address both opportunistic and more highly targeted cybercriminal threats.

Glossary of Terms

Advanced persistent threats (APTs) — targeted activity from a single adversary attempting to gain access to a network in pursuit of a specific objective. Most often APT intrusions are focused on theft of data, but in some cases it may be to disrupt or sabotage a target.

ATM jackpotting — a technique designed to steal money from an ATM without using a credit or debit card. Malware designed for this purpose is referred to as "jackpot malware."

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.

Botnet — a network of computers compromised with malicious software and controlled as a group.

Bulletproof hosting (or hosters) — Computing resources that may be rented with terms of services that are permissive to semi-legal and illegal activity, and are resistant to abuse complaints.

Business email compromise (BEC) — 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 (BES) — sending spoofed email from an external account imitating a company executive or employee authorizing a fraudulent transaction to the criminal.

Casher — a person involved in a fraud scheme, whose job is to withdraw cash from ATMs using stolen credit cards.

Commodity cybercrime — cybercriminal attacks launched on a large scale, often using exploit kits, ransomware or other malware purchased on the dark web.

Crypter — a type of software that can encrypt, obfuscate and manipulate malware to bypass security programs by presenting itself as a harmless program until it gets installed.

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.

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.

Drive-by download — the unintentional download of malicious code to your computer or mobile device that leaves you open to a cyberattack.

Email account compromise (EAC) — similar to business email compromise but affecting any email account, not just those associated with the business.

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.

Hosters — providers of online hosting services.

Jabber chats — discussions taking place over the instant messaging tool Jabber.

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

Malware-as-a-service — allows criminals to gain access to malware capabilities that 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.

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 that is unauthorized and possibly illegal, by sending an email designed to trick the recipient into disclosing information. Spear phishing is highly targeted phishing activity.

Ransomware — a type of malware that prevents 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 that is unauthorized.

Server Message Block (SMB) — an application-layer network protocol mainly used for providing shared access to files, printers, and serial ports and miscellaneous communications between nodes on a network.

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

Spreader — Malware built for the purpose of spreading additional copies of itself or other malware.

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

TOR — free software for enabling anonymous communication. Tor directs Internet traffic through a free, worldwide, volunteer overlay network consisting of more than 7,000 relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis.

Secureworks®

About Secureworks

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world. We close gaps in security layers with a Defense in Concert that combines visibility from thousands of clients and aggregates and analyzes data from any source, anywhere, to 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.™
www.secureworks.com

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
+49 069 9792 0
www.dellsecureworks.de

NETHERLANDS
Transformatorweg 38-72,
1014 AK Amsterdam,
+31 20 475 2026

UNITED KINGDOM
One Creechurch Place,
1 Creechurch Ln,
London EC3A 5AY
+44 0 131 260 3040
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