Carbon Black.

Global Threat Report
The Year of the Next-Gen Cyberattack

While Cryptomining, Fileless Attacks, Ransomware and Commodity Malware Are Still Causing Havoc, a New Breed of Cyberattacks (Fueled by Geopolitical Tension) is Emerging

JANUARY 2019

Executive Summary

In 2016, fileless attacks such as PowerWare and the alleged hack against the Democratic National Committee (DNC) stole sensitive information and global headlines. In 2017, WannaCry, NotPetya and BadRabbit demonstrated ransomware's global ubiquity.

Then, as we kicked off 2018, the Spectre and Meltdown vulnerabilities offered an ominous start to a year that many thought would be marred by high-profile, global-scale cyberattacks.

In some respects, the prognosticators were correct. Billions of personal records were stolen in 2018, unearthed in breaches that successfully targeted household names in government, technology, healthcare, travel and hospitality. Compounding the problem has been increased geopolitical tension between western democracies and countries like Russia, China and North Korea.

While 2016 may have been "The Year of the Fileless Attack" and 2017 may have been "The Year of Ransomware," 2018 was, in many respects, "The Year of the Next-Gen Cyberattack."

Modern cyberattacks appear to increasingly be fueled by geopolitical tension and reveal how clever attackers have become in evolving to remain undetected — using techniques such as lateral movement, island hopping and counter incident response to stay invisible. According to Carbon Black's threat research, we believe 2019 promises to be a year where endpoint visibility becomes more paramount than ever as attackers continue to evolve and global tensions increase.

To better understand the current attack landscape as we head into 2019, the Carbon Black Threat Analysis Unit (TAU) researched the current state of cyberattacks across the Carbon Black customer base and in conjunction with our incident response (IR) partners to produce all of the content enclosed in this report.

2018 WAS, IN MANY RESPECTS,
"THE YEAR OF THE NEXT-GEN CYBERATTACK."

Carbon Black.

Key Report Stats

1. The **average endpoint protected by Carbon Black was targeted by two cyberattacks per month** throughout 2018

2. Carbon Black customers, in aggregate, are seeing **approximately 1 million attempted cyberattacks per day**

3. The **top five industries targeted by cyberattacks in 2018**, according to Carbon Black's global threat data, were: Computers/Electronics, Healthcare, Business Services, Internet/Software and Manufacturing

4. **Global governments saw increased cyberattacks** in 2018 stemming from Russia, China and North Korea

5. As 2018 came to a close, **CB TAU saw several cyberattacks targeting global governments** that included indicators of compromise attributable to North Korea

6. Approximately **$1.8 billion of cryptocurrency-related thefts** occurred in 2018

7. The top ransomware variant seen in 2018 was **Kryptik**

8. The **top industries targeted by ransomware** in 2018 were: Manufacturing, Business Services, Retail, Government and Computers/Electronics

9. The **top commodity malware family seen in 2018 was Emotet**, a banking trojan targeting financial information

10. The **top industries targeted by commodity malware in 2018** were: Computers/Electronics, Manufacturing, Business Services, Software/Internet and Healthcare

11. Nearly 60% of attacks now involve **lateral movement**

12. Half of incident response engagements now involve instances of **counter incident response**

13. Half of cyberattacks today use the victim primarily for **island hopping**

14. IR firms are encountering **destructive attacks during 32% of investigations**

By the Numbers: Cyberattack Trends of 2018

The average endpoint protected by Carbon Black was targeted by two cyberattacks per month throughout 2018. At this rate, an organization with 10,000 endpoints is estimated to see more than 660 attempted cyberattacks per day. Across the Carbon Black customer footprint (totaling approximately 15,000,000 global endpoints) this means there are, on average, 1 million attempted cyberattacks per day.

2

ATTEMPTED CYBERATTACKS PER MONTH TARGETING CB PROTECTED ENDPOINTS

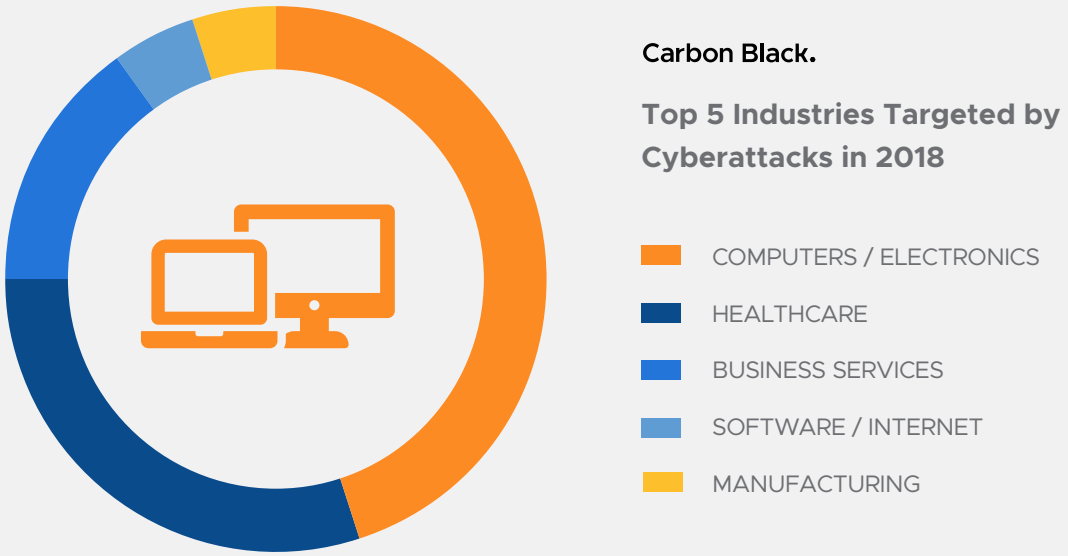
660+

ATTEMPTED CYBERATTACKS A 10,000-ENDPOINT ENTERPRISE SEES PER DAY

1M

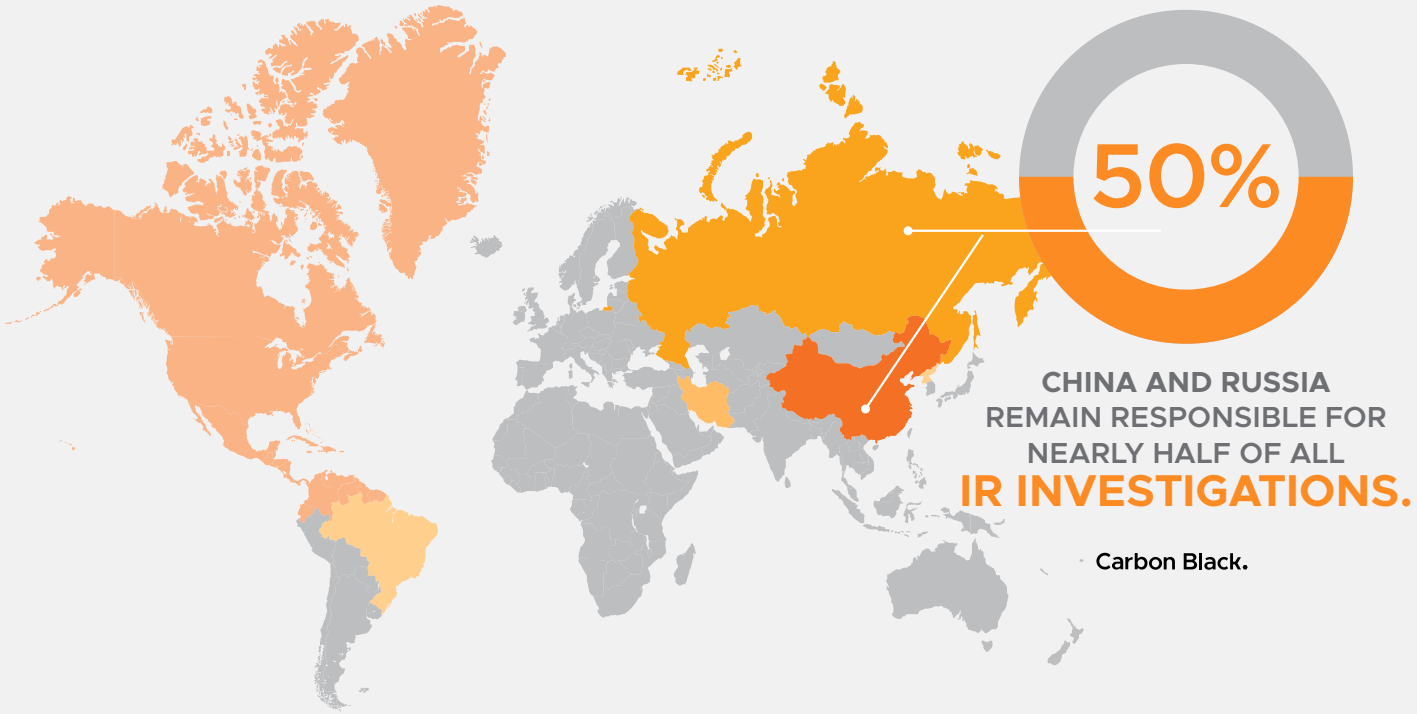
ATTEMPTED CYBERATTACKS ACROSS THE CB CUSTOMER FOOTPRINT PER DAY

The top five industries targeted by cyberattacks in 2018, according to Carbon Black's global threat data were: Computers/Electronics, Healthcare, Business Services, Software/Internet and Manufacturing



Nation-State Cyberattacks Take Center Stage

As 2018 came to a close, China and Russia were responsible for nearly half of all cyberattacks. Of 113 investigations our IR partners conducted in the third quarter, 47 stemmed from those two countries alone.



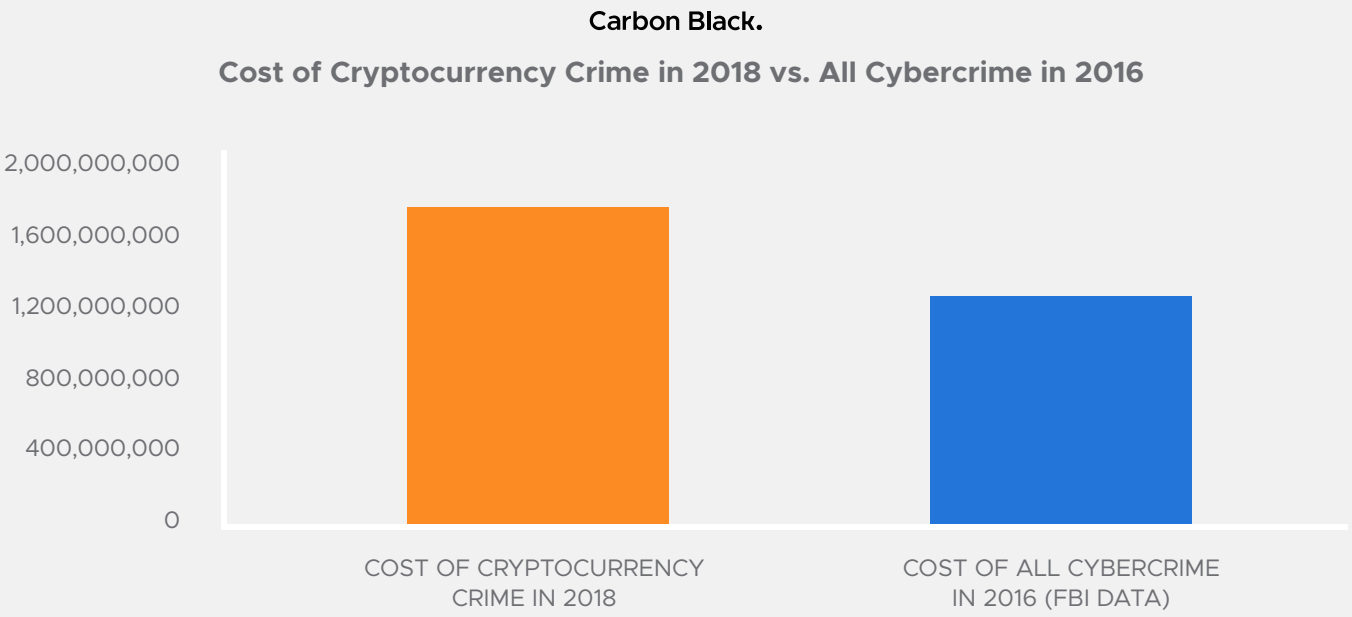
Not to be outdone, North Korea made a splash toward the end of 2018. According to CB TAU data, fileless attacks against global governments in Q4 included indicators of compromise reported as nation-state attributable to North Korea, commonly referred to as HARDRAIN by U.S. government partners, Department of Homeland Security and the FBI.

Of the identified fileless attacks, variants of the malware Graftor were uniquely identified as the fileless payload. The **FBI has high confidence** that Graftor variants are used by North Korean cyber operations, also referenced as HIDDEN COBRA, to maintain presence on victim networks and to further network exploitation.

Cryptocurrency Attacks

Approximately $1.8 billion of cryptocurrency-related thefts occurred in 2018. To determine this number, we evaluated open-source reporting and dark web marketplaces to identify and quantify the largest threats posed from cryptocurrency-related crimes. During this process, we found almost $1.8 billion in losses throughout 2018.

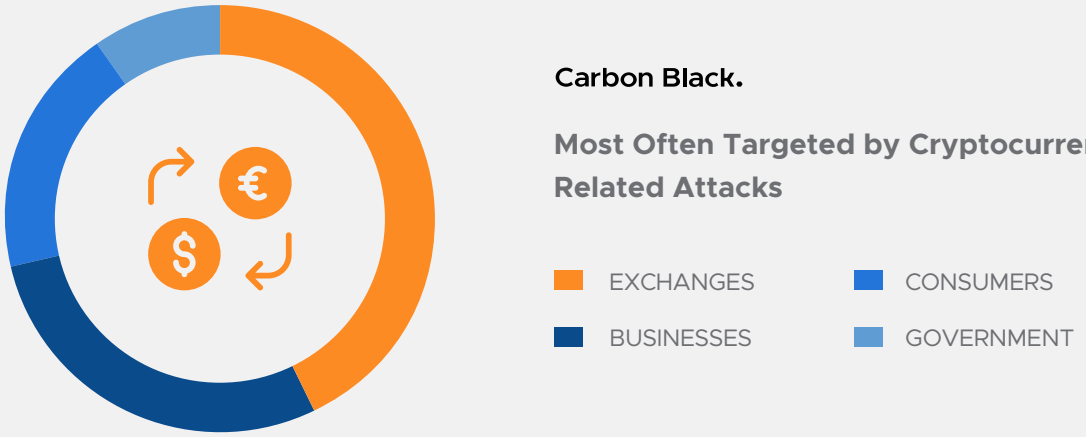
To quantify this figure and put in perspective how far cybercrime has evolved in two years, we looked at the data from the United States FBI's Internet Crime Complaint Center (IC3), which reported $1.3 billion in victim losses from total internet crime for all of 2016.



Of the identified attacks, cryptocurrency exchanges are the most vulnerable target for cybercriminals. Attacks on these exchanges account for just over 27% of all reported incidents. These exchanges represent prime targets for cryptocurrency theft, fraud and harvesting of user information for follow-on targeting by these same criminals.

Although bitcoin is still the lead cryptocurrency for legitimate cyber transactions, cybercriminals are moving to alternative and more profitable currencies, such as Monero, popularized by major retailers and online services, like Fortnite. As a result, Monero is now used in 44% of all attacks.

Of note, TAU has seen instances where ransomware attackers first looked specifically for cryptocurrency wallets in an attempt to target them. If no wallet was located, the attacker proceeded with a traditional ransomware attack. This follows the trend of many businesses preparing for ransomware attacks by preemptively purchasing cryptocurrency and keeping it in a secure location.



TAU Analysis: Monero Cryptomining Campaign

In June 2018, CB ThreatSight, Carbon Black's managed alert monitoring and triage service, analyzed a RETADUP worm that leverages AutoIt to launch a Monero cryptomining campaign. While monitoring a customer's environment, the CB ThreatSight team discovered a series of unusual alerts. Further investigation of the suspect processes revealed these alerts were related to an attacker leveraging the open-source Monero framework to launch a cryptomining campaign.

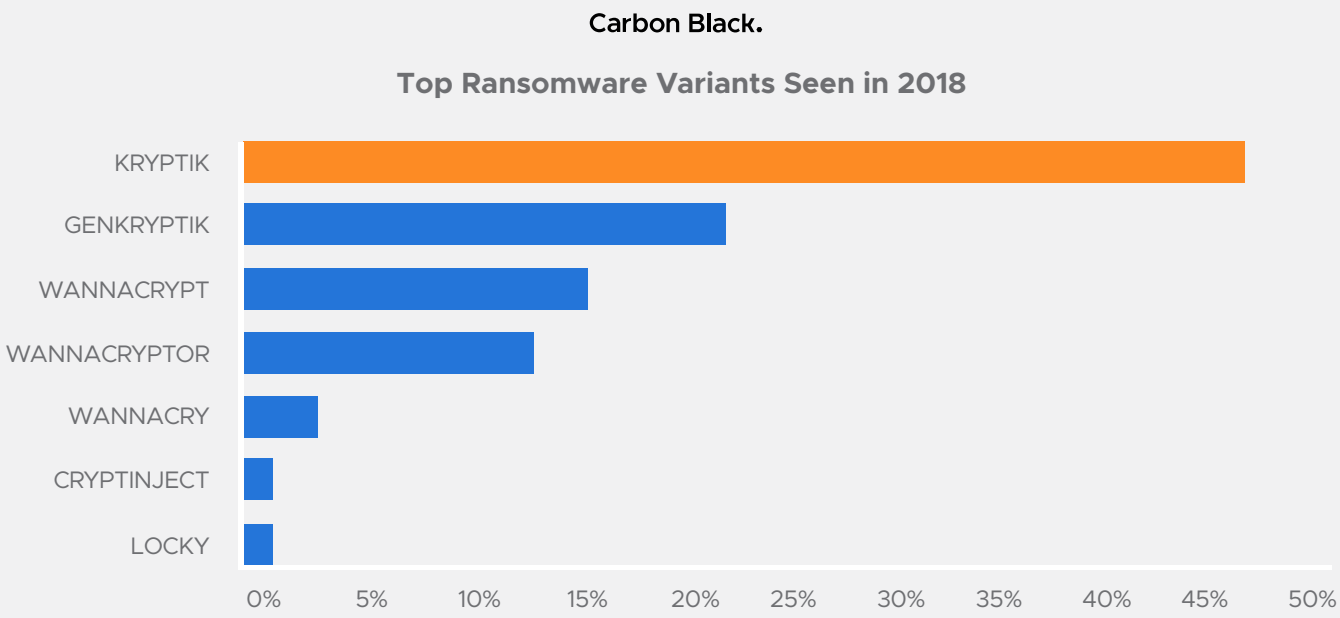
This variant of the RETADUP worm uses AutoHotKey, an off-the-shelf keyboard macro tool, to script its infection and propagation actions. The worm is polymorphic by nature and is difficult to block based on file hash or name. The worm gathers its mining tools by injecting into notepad and completing its tasks, causing notepad to make network connections to its C2 servers.

In this campaign, the C2 will attempt to deliver a payload containing an AutoIT (another macro tool) script for mining. This tool will try to connect to a mining pool and start mining Monero coin.

For a full technical write-up of the campaign, **click here.**

Ransomware

The top ransomware variants seen in 2018 were: Kryptik, GenKryptik, WannaCryptor, WannaCrypt, WannaCry, CryptInject and Locky.



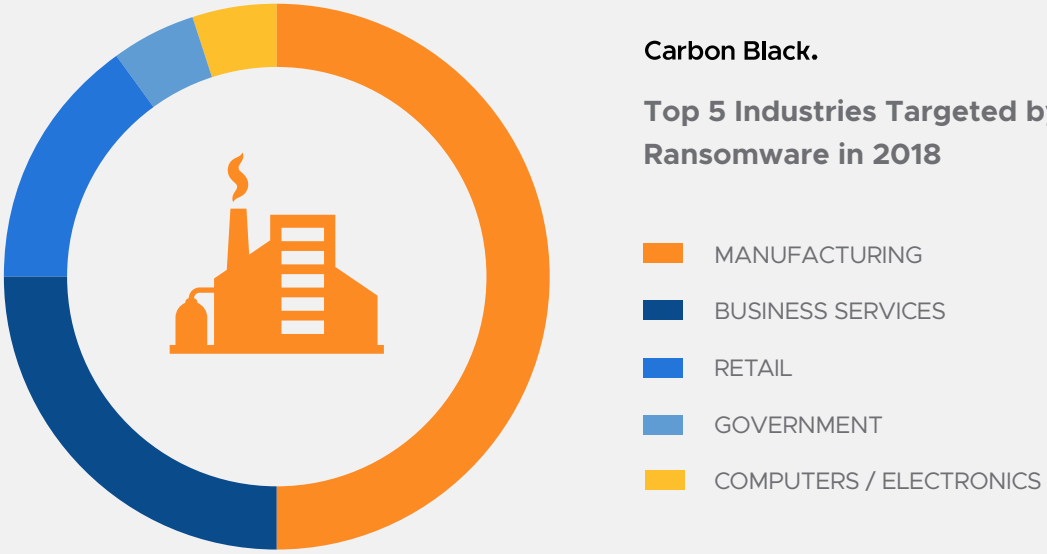
About Kryptik

The Kryptik trojan attempts to target victim machines via nefarious installers. It then attempts to acquire admin rights to make registry modifications, allowing it to execute each time a Windows machine boots. The Kryptik trojan can be very persistent and, without the appropriate visibility, can be difficult to detect as it attempts to delete its executable file after running.

As noted by a threat profile from the New Jersey Cybersecurity and Communications Integration Cell (NJCCIC): "[The Kryptik trojan] queries the Windows registry for the .ini or .dat file paths. It also queries registry subkeys for the actual host, username, and password related to the specific FTP client application. Kryptik searches the registry, querying for both ftpIniName and InstallDir that hold the wcx_ftp.ini file. The trojan can recover many common FTP clients, email clients, file browsers, and file manager programs. Kryptik also can update itself and remotely download new versions."

Kryptik was among the infections found in the notorious attack targeting the Ukrainian power grid in late 2015.

The top industries targeted by ransomware in 2018 were: Manufacturing, Business Services, Retail, Government and Computers/Electronics.



TAU Analysis: Ransomware Leveraging Open-Source Tools

In June 2018, an organization contacted Carbon Black TAU about a ransomware attack they were investigating. TAU team members worked with the firm investigating the incident. After the initial analysis was completed, it became apparent that this network had been compromised prior to the ransomware attack.

Artifacts indicated that, as far back as October 2017, unknown actors were leveraging Remote Desktop Protocol to connect to a system from an IP originating from Russia. However, the majority of the activity related to this attack started one week prior to the ransomware attack and focused on a second system on the network. There were a series of RDP connections over a seven-day period, with little other malicious-related activity. It was surmised this activity was from the attackers testing their access via compromised credentials on a daily basis prior to selling or leveraging the compromised system.

On the day of the ransomware attack, one last RDP connection was initiated from Russia, approximately 20 minutes later a RDP connection from Sweden was made to a system on the network. After the connection

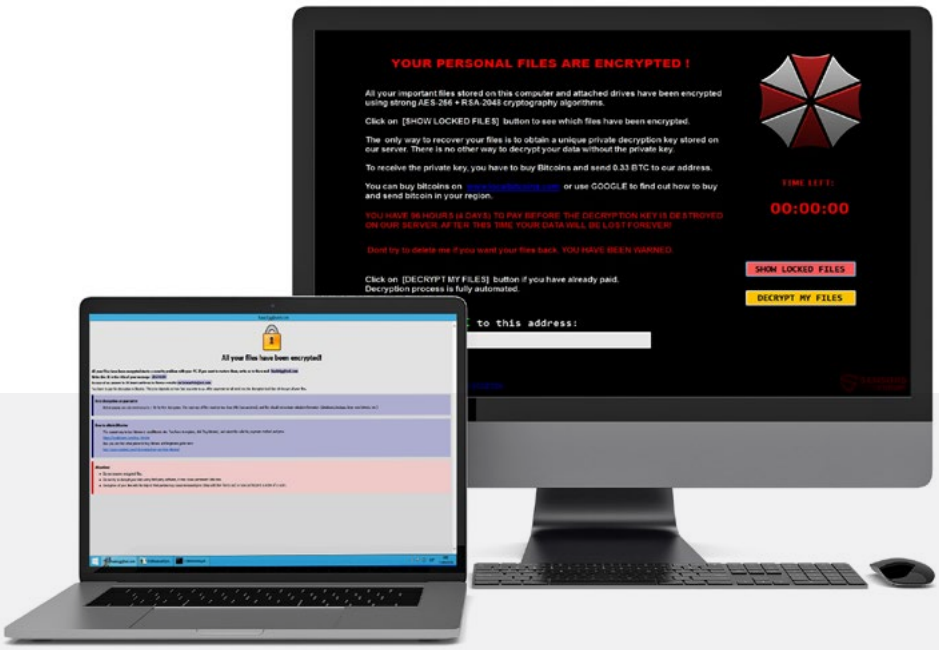
was established — approximately 30 seconds later — the attacker began downloading several files onto the system. Within minutes, the attacker commenced their reconnaissance and ransomware attack.

It should be noted that this attack scenario has become very common over the last 12 to 18 months, and continues to be successful and profitable for groups selling access to compromised systems, as well as attackers leveraging the ransomware portion.

Traditionally, campaigns like this have targeted small to mid-size utility or energy companies, municipalities and hospitals. In this latest variant, a ransomware family referred to as Dharma or Crysis is being leveraged.

These types of campaigns continue to grow in popularity, and can typically be detected before attackers cause any damage or encrypt data. Unsurprisingly, attackers are continuing to leverage open source or freely available programs to assist them in their network reconnaissance and preparations before launching the ransomware portion of their attacks. Files that were used in this attack revealed a repository containing numerous tools that were leveraged by the attacker. These tools highlight how attackers are utilizing off-the-shelf programs to conduct network reconnaissance and install secondary backdoors.

For a full technical write-up on this ransomware attack, **click here.**



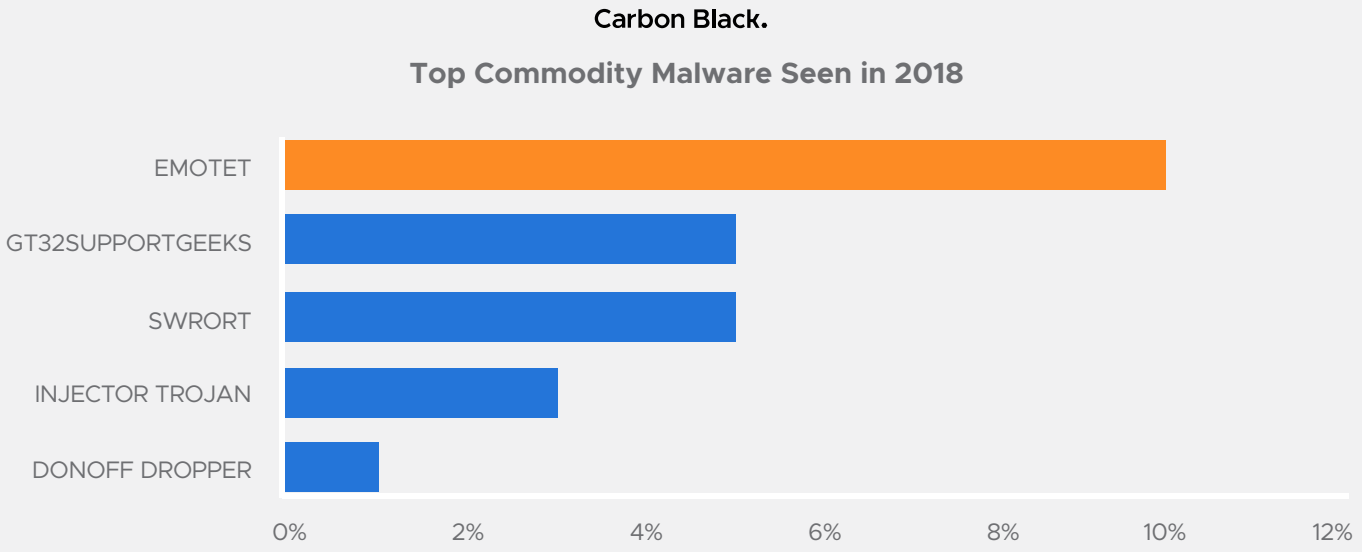
Carbon Black.

RANSOMWARE ATTACKS LEVERAGING OPEN-SOURCE TOOLS

HAVE BECOME COMMON OVER THE LAST 12 TO 18 MONTHS.

Commodity Malware

The top commodity malware families seen in 2018 were: Emotet, GT32SupportGeeks, Swrort, Injector Trojan and Donoff dropper.



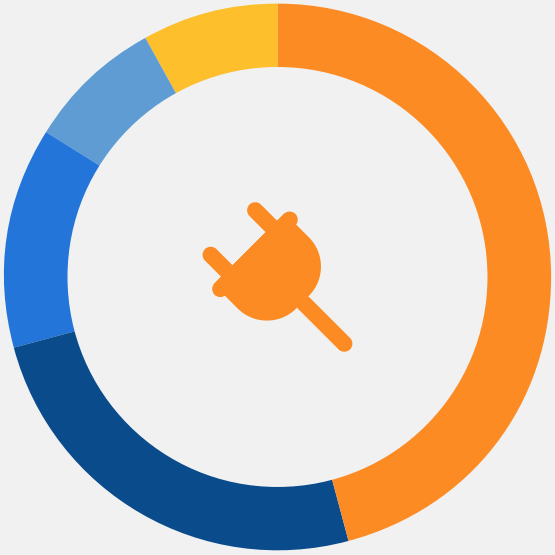
TAU Analysis: Emotet Leverages Microsoft Office Word Docs, PowerShell to Deliver Malware

Emotet is a family of banking malware, which has been around since at least 2014. Attackers continue to leverage variants of Emotet and are becoming increasingly shrewd in the techniques they employ to deliver the malware onto an infected system. In the spring of 2018, Carbon Black's TAU and other researchers observed the adaptation to existing methods leveraging PowerShell, where attackers were encrypting the URLs of the C2s used to host the second stage payload.

In 2018, Carbon Black observed a spike in this type of technique being detected across customers' utilizing their managed hunting services. This attack has been observed as originating from phishing campaigns that are leveraging Microsoft Office Word documents with obfuscated VBScripts using PowerShell and the ConvertTo-SecureString cmdlet, which in the later stages is used to decrypt the C2(s) and associated logic. This represented an evolution of current macro attack techniques, where these types of cmdlets are not typically associated with phishing campaigns.

For a full technical breakdown of Emotet, **click here.**

The top industries targeted by commodity malware in 2018 were: Computers/Electronics, Manufacturing, Business Services, Software/Internet and Healthcare.



Carbon Black.

Top 5 Industries Targeted by Commodity Malware in 2018

- COMPUTERS / ELECTRONICS
- MANUFACTURING
- BUSINESS SERVICES
- SOFTWARE / INTERNET
- HEALTHCARE

TAU Analysis: ROKRAT Malware

ROKRAT (also referred to as DOGcall) is a family of malware that has been used by attackers originating from North Korea. The family continues to evolve and adopt techniques from other families also used by the same attack group. The ROKRAT core payload is typically deployed by a loader, which has also been observed dropping additional families. In 2018, CB TAU monitored the use of this and related families. ROKRAT provides attackers with numerous capabilities to introduce additional tools and malware onto a network, exfiltrate data, harvest credentials, as well as capture screenshots of the victim system. The latest variants of ROKRAT use internet cloud solutions such as pCloud, Dropbox and Yandex as a command and control (C2) channel.

However, earlier variants (that utilize the same loader) used hard-coded URLs, which were primarily hosted by Korea telecoms. These variants shared the same loader and had functionality (system information gathering and OS profiling) that overlapped with ROKRAT, yet their primary function was to download a second stage malware masquerading as a jpg image file. As previously reported, these payload variants were typically observed being used in conjunction with carrier files, such as word processing documents.

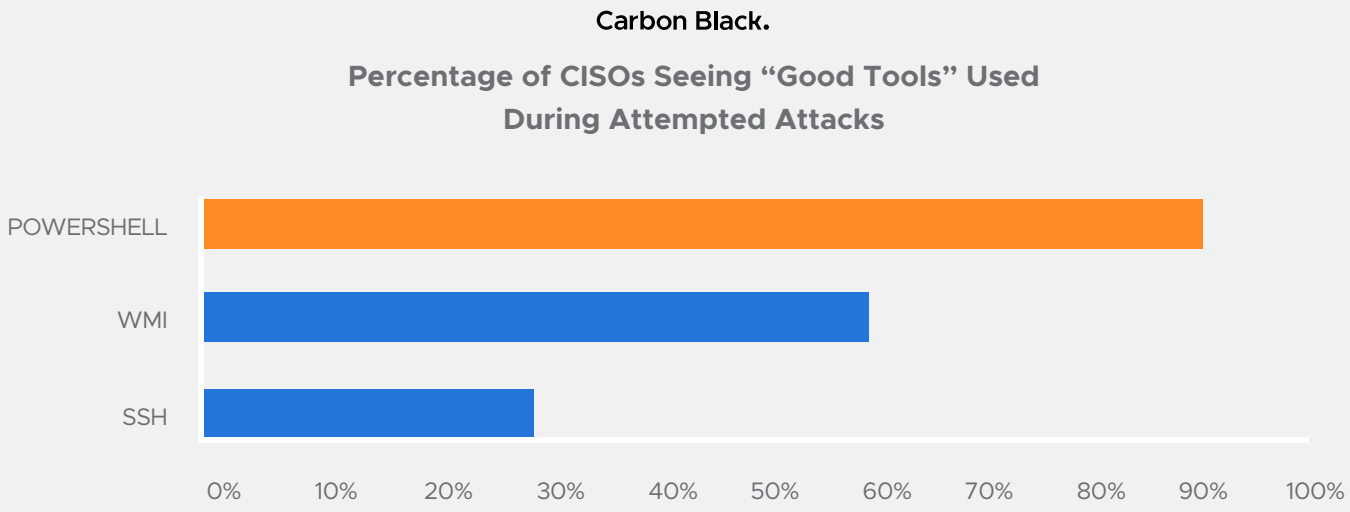
For a full technical write-up on ROKRAT, **click here**.

Emerging Cyberattack Trends Heading into 2019

Increased Prevalence of Lateral Movement

Nearly 60% of attacks now involve lateral movement, which means attackers aren't just going after one component of an organization. They're getting in, moving around and seeking more targets as they go.

Cybercriminals are continuing to hide in plain sight and move laterally leveraging non-malware / fileless attack methods. PowerShell, Windows Management Instrumentation (WMI) and Secure File Transfer Protocol (SSH) were the top three legitimate applications attackers were leveraging in 2018, according to data gathered from Carbon Black's IR partners.

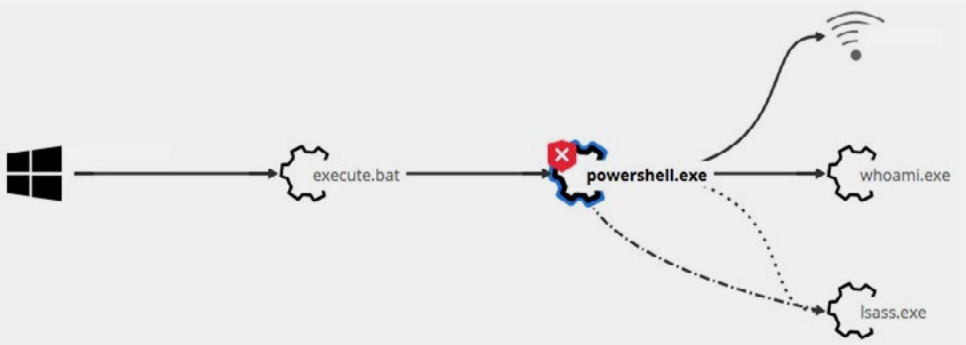


TAU Analysis: Using Trusted Microsoft Applications for Malicious Behavior

In August 2018, an attack leveraging cmd.exe and PowerShell was investigated by CB ThreatSight analysts. The initial investigation discovered that a batch file was executed on the targeted system. This batch file then invoked PowerShell with a base64 encoded command. Decoding the command revealed a series of PowerShell cmdlets which were utilized to download and decrypt a second stage payload. The first stage of base64 decoded command appears to be a payload created by a popular PowerShell Framework, like PowerShell Empire.

The second stage payload also leveraged legitimate Microsoft applications to complete the series of malicious events. Our investigation concluded that this was an internal pentest being conducted; however, the tactics leveraged represent commonly used and effective techniques that are observed in the wild. In the latter stages, we observed a WMIC bypass technique, dubbed "squiblytwo." All of these processes used are trusted Microsoft applications which are commonly abused by an attacker to perform malicious behavior, in an attempt to avoid detection. This is where an understanding of what is normal behavior for these trusted applications becomes paramount in order to quickly detect outlying activity.

For the full technical write-up from TAU on this attack, **click here**.



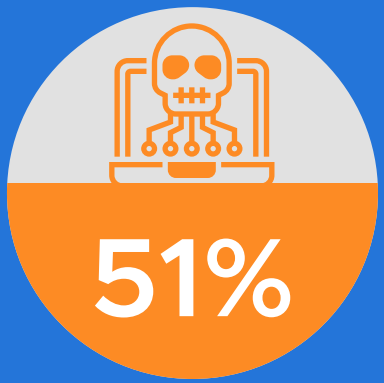
Counter Incident Response

Half of incident response engagements now involve instances of counter incident response, another concerning sign that attackers have become increasingly sophisticated and are initiating longer-term campaigns — as well as a clear signal that incident response must get stealthier.

51% OF IR PROFESSIONALS SEE

COUNTER INCIDENT RESPONSE DURING IR ENGAGEMENTS

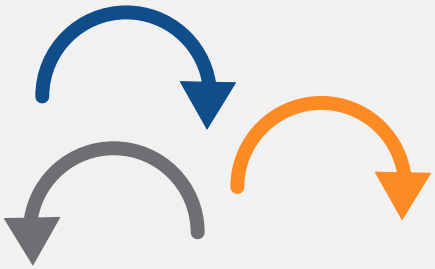
Carbon Black.



Island Hopping

Half of cyberattacks today use the victim primarily for island hopping. In these campaigns, attackers first target an organization's affiliates, often smaller companies with immature security postures. This means that your data is not only at risk, but so is the data at every point in your supply chain, including that of your customers and partners.

50% OF IR FIRMS
HAVE ENCOUNTERED AN
ATTACK LEVERAGING
ISLAND HOPPING



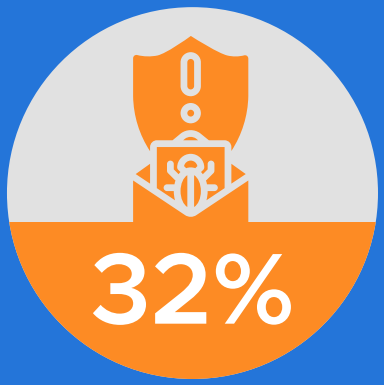
Carbon Black.

Destructive Attacks

As nation-state cyberattackers become more sophisticated and powerful, their attacks become increasingly destructive — our respondents said victims experienced such attacks 32% of the time. One IR professional recounts firsthand experience: "We've seen a lot of destructive actions from Iran and North Korea lately, where they've effectively wiped machines they suspect of being forensically analyzed."

DURING 32% OF INVESTIGATIONS
IR FIRMS ARE ENCOUNTERING DESTRUCTIVE ATTACKS.

Carbon Black.



About Carbon Black

Carbon Black (NASDAQ: CBLK) is a leading provider of next-generation endpoint security delivered via the cloud. Leveraging its big data and analytics cloud platform – the CB Predictive Security Cloud – Carbon Black consolidates prevention, detection, response, threat hunting and managed services into a single platform with a single agent and single console, making it easier for organizations to consolidate security stacks and achieve better protection. As a cybersecurity innovator, Carbon Black has pioneered multiple endpoint security categories, including application control, endpoint detection and response (EDR), and next-generation antivirus (NGAV) enabling customers to defend against the most advanced threats. More than 4,600 global customers, including one-third of the Fortune 100, trust Carbon Black to keep their organizations safe.

Carbon Black.

1100 Winter Street
Waltham, MA 02451
P: 617.393.7400
F: 617.393.7499

carbonblack.com