CrowdStrike Products

CROWDSTRIKE

THE EVOLUTION OF RANSOMWARE: HOW TO PROTECT ORGANIZATIONS FROM NEW TRENDS AND METHODS

There's no question that ransomware is a growing threat. High-profile attacks that crippled multiple U.S. cities, including Baltimore, Maryland, and Park City, Utah, made headlines in 2019. However, those attacks reflect only the public side of a much larger cybercriminal industry that is constantly innovating its capabilities. In fact, ransomware is one of the fastest growing threats in cybersecurity, with damages predicted to build to **$20 billion globally by 2021, up from "only" $345 million in 2015**.

This paper explains the evolution of ransomware by breaking down the new trends in online extortion threats, and provides prescriptive advice on how to protect and secure your organization against such an attack.

EVOLUTION OF RANSOMWARE AND CURRENT TRENDS

AN OLD SCHEME

Even though ransomware has been in the headlines consistently over the past five years or so, the idea of taking users' files or computers hostage by encrypting files, hindering system access or other methods — and then demanding a ransom to return them — is quite old. In the late 1980s, criminals were already holding computers or files hostage in exchange for cash sent via the postal service. One of the first ransomware viruses ever documented was the AIDS trojan (PC Cyborg Virus) that was released via floppy disk in 1989. Victims needed to send $189 to a P.O. box in Panama to restore access to their systems, even though it was a simple virus that utilized **symmetric cryptography**.

MONETIZATION

Despite its long history, ransomware attacks were still not that widespread well into the 2000s — probably due to difficulties with payment collection. However, the emergence of cryptocurrencies, such as Bitcoin in 2010, changed all that. By providing an easy and untraceable method for receiving payment from victims, virtual currencies created the opportunity for ransomware to become a lucrative business.

EASIER BUT STILL CUMBERSOME

eCrime — a broad category of malicious activity that includes all types of cybercrime attacks, including malware, banking trojans, ransomware, mineware (cryptojacking) and crimeware — seized the monetization opportunity that Bitcoin created. This resulted in a substantial proliferation of ransomware beginning in 2012. However, this ransomware business model is still imperfect, because while Bitcoin payments are easy transactions for criminals to use, they are not always so easy for their non-tech-savvy targets to navigate. To ensure payment, some criminals have gone so far as to open call centers to provide technical support and help victims sign up for Bitcoin — but this takes time and costs money.

CASE STUDY: ROBBINHOOD MALWARE DEVASTATES THE CITY OF BALTIMORE

In May 2019, the city of Baltimore, Maryland, suffered a severely damaging attack from ransomware called "RobbinHood." It cost the city at least **$18.2 M** in lost or delayed revenue, in addition to the direct costs required to restore systems. The attack shut down the city's credit card payment system and halted the property market by disabling municipal processes for collecting property taxes, real estate fees and fines.

RobbinHood is a new strain of ransomware that emerged in April 2019. It operates by shutting down an organization's signature-based antivirus (AV) and backup services that would prohibit its encryption. RobbinHood does this by issuing the following "sc. exe stop" command: `cmd.exe /c sc.exe stop AVP /y` (AVP stands for AntiVirus Program and represents the generic name for AV software). This action is followed by a series of other intrusive commands and measures. Once executed, the ransomware blocks 181 Windows services associated with AV, mail servers and other software that could prevent file encryption. This is an example of "living off the land," which consists of using tools already present on the system to perform malicious tasks such as persistence, privilege escalation and defense evasion. These tactics shut down defenses and allow attackers to stealthily infiltrate endpoints.

BIG GAME HUNTING

To optimize their efforts, eCrime operators decided to pivot from the "spray and pray" style of attacks that were dominating the ransomware space and focus on "big game hunting" (BGH). BGH combines ransomware with the tactics, techniques and procedures (TTPs) common in targeted attacks aimed at larger organizations. Rather than launching large numbers of ransomware attacks against small targets, the goal of BGH is to focus efforts on fewer victims that can yield a greater financial payoff — one that is worth the criminals' time and effort.

This transition has been so pronounced that BGH was recognized as one of the most prominent trends affecting the eCrime ecosystem in the **CrowdStrike® 2020 Global Threat Report**. Recent eCrime statistics show that while the volume of ransomware attacks has decreased, the sophistication of these attacks has increased substantially.

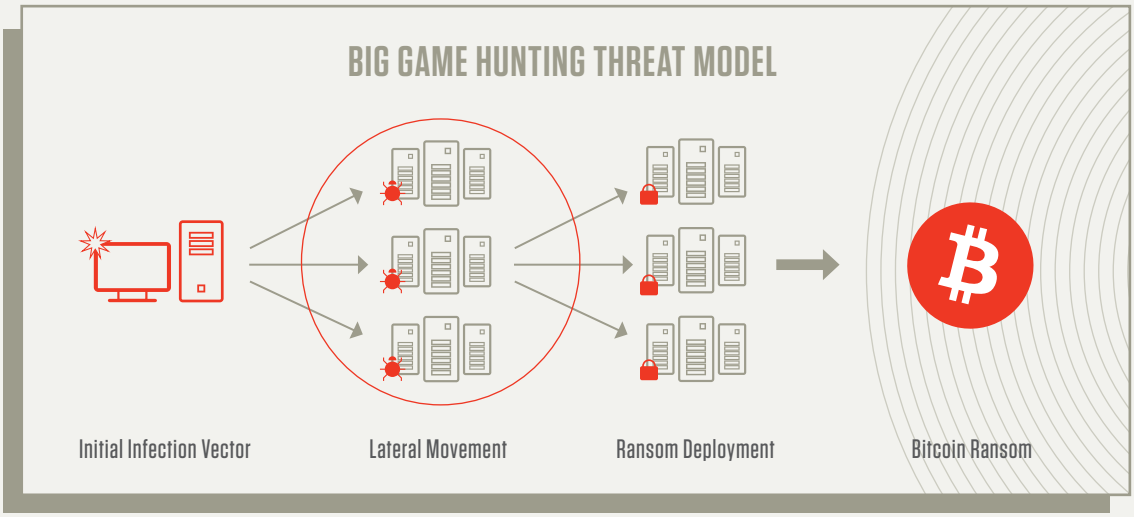


Figure 1. Adversary groups are targeting enterprise organizations in BGH attacks that garner huge payoffs.

THE ACTORS BEHIND RANSOMWARE ATTACKS

CrowdStrike® Intelligence monitors the eCrime ecosystem by tracking eCrime organizations, independent threat actors, and their relationships. For example, the creator of Samas (aka Sam Sam) was identified as a threat actor named BOSS SPIDER; INDRIK SPIDER was credited with the creation of Dridex; and WIZARD SPIDER, also known as the Russia-based operator of the TrickBot banking malware — which in the past had focused primarily on wire fraud — was identified as the group that created Ryuk. These groups have been observed propagating ransomware attacks that are part of the BGH trend and raking in huge profits through targeted attacks that reap big rewards. For instance, since its initial appearance in 2016 until its last known activity toward the end of 2018, BOSS SPIDER has taken in more than $6.7 million USD. Since WIZARD SPIDER's initial appearance in August 2018, this threat actor group is estimated to have netted over 695.80 Bitcoin across 51 transactions, with an approximate value of $3.6 million USD.

CrowdStrike has also observed that threat actors have started working together to facilitate targeted attacks.

MORE SOPHISTICATION AND BLURRED LINES

Just like any software developer, eCrime groups are constantly striving to improve and upgrade their ransomware with new functionality. WIZARD SPIDER, for example, has added many new capabilities to Ryuk and removed useless and obsolete functionality from the code. This group also added new enumeration modules that are downloaded onto victim systems to locate credentials and perform lateral movement within the victim's environment — with the objective of gaining access to the domain controller. Successfully gaining such access allows WIZARD SPIDER to deploy Ryuk ransomware throughout the victim's environment.

To complicate things, a trend observed in 2018 that continues today is the blurring of lines between nation-state and eCrime ransomware campaigns. Whether the ransomware code is stolen or willingly shared between nation-state actors and cybercriminals remains unclear, but CrowdStrike has observed both types of adversaries using similar malware, such as Ryuk, either for immediate financial gain or to create a distraction designed to obscure the origin of a nation-state attack.

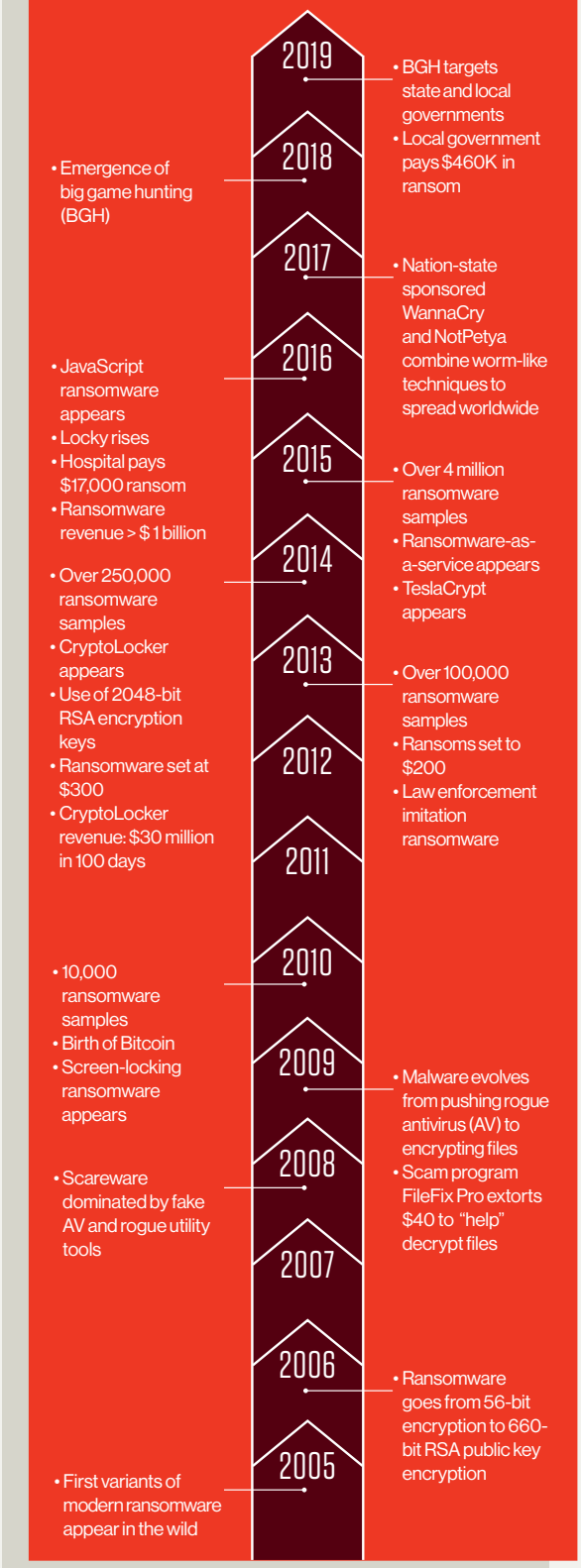
HOW RANSOMWARE WORKS

There are many points of entry for ransomware, with phishing emails and website pop-ups among the most common vectors. Another entry route involves using exploit kits that take advantage of specific vulnerabilities.

DARK PSYCHOLOGY: COMBINING BUSINESS SAVVY WITH RUTHLESS SOCIAL ENGINEERING

Technology and human nature are two sides of the same coin when it comes to ransomware attacks. In one case observed by CrowdStrike, a CEO's email was spoofed and the attacker used social engineering to trick employees into clicking a link in a fake email from the executive. To succeed, this attack required methodical research into the company's management, its employees and the industry. As BGH attacks increase, social engineering is becoming a more intensive presence in phishing attacks. Social media also plays a huge role, not only enabling attackers to discover information on potential victims but also as a conduit for deploying malware.

THE EVOLUTION OF MODERN RANSOMWARE



WEBSITE POP-UPS AND EXPLOIT KITS: A DAMAGING COMBINATION

Website pop-ups and exploit kits can be used together to propagate ransomware that allows attackers to create "Trojan pop-ups" or advertisements containing hidden malicious code. If users click on one of them, they are surreptitiously redirected to the exploit kit's landing page. There, a component of the exploit kit will discreetly scan the machine for vulnerabilities that the attacker can then exploit. If the exploit kit is successful, it sends a ransomware payload to infect the host. Exploit kits are popular with eCrime organizations due to their automated nature. In addition, exploits are an efficient fileless technique, as they can be injected directly into memory without requiring anything to be written to disk, making them undetectable by traditional antivirus software. Exploits kits are also proliferating among less sophisticated attackers, because they do not require a great deal of technical know-how to deploy. With a modest investment on the darknet, virtually anyone can get into the online ransom business.

FILELESS ATTACKS: RANSOMWARE WITHOUT RANSOMWARE

Fileless ransomware techniques are increasing. These are attacks in which the initial tactic does not result in an executable file written to the disk. Fileless ransomware uses pre-installed operating system tools, such as PowerShell or WMI, to allow the attacker to perform tasks without requiring a malicious executable file to be run on the compromised system. This technique is popular because fileless attacks are able to bypass most legacy AV solutions.

For a detailed explanation of how fileless ransomware works, download the **CrowdStrike fileless ransomware infographic.**

RANSOMWARE-AS-A-SERVICE (RAAS)

Because cybercriminals are always looking for ways to optimize their operations and generate more profits, they have been inspired by the SaaS (software-as-a-service) model to create a RaaS (ransomware-as-a-service) model. RaaS providers offer all of the attack components needed to run ransomware campaigns — from malicious code to results dashboards. Some even include a customer service department, putting ransomware within the reach of non-technically savvy criminals. In addition, the subscription cost is usually covered as a portion of the proceeds from the campaign — making this a cost-efficient model for cybercriminals to adopt.

An example of this type is a famous RaaS called "Hermes," which was first distributed in 2017 and sold on darknet forums for $300 USD. A Hermes purchaser typically received a build supporting two email addresses, a decryptor and a unique RSA key pair. Other eCrime groups using Hermes attacks began popping up once its success was established.

Another example is PINCHY SPIDER, a RaaS operation and criminal group that was first observed in 2018*. Operating on a 60-40 profit split with its customers, the adversary group increased the pace of its releases to provide updated versions every two weeks. This acceleration in the development cycle is linked to the fact that the adversary group had to frequently morph its code to prevent security vendors from blocking it.

* CrowdStrike 2019 Global Threat Report

NOTEWORTHY STRAINS OF RANSOMWARE

BitPaymer: Targets enterprise organizations using the Dridex loader module to gain an initial foothold in the victim's network

Dridex: A strain of banking malware that leverages macros in Microsoft Office to infect systems

Hermes: RaaS first distributed in 2017 — in mid-August 2018, a modified version of Hermes, dubbed Ryuk, started appearing in a public malware repository

KeRanger: First ransomware targeting Mac OS X, was also able to encrypt Time Machine backup files

Petya: Encrypts the master file table (MFT) to make the entire system inaccessible

PowerWare: Encrypts hostage files through "fileless" infection

Ransom32: Written in Javascript, making it suitable for cross-platform infection on Mac and Linux systems

Ryuk: Similar to Samas and BitPaymer because it targets enterprise organizations and uses PowerShell — PsExec is used to push out its binary

Samas: Leverages vulnerable JBOSS systems to spread across a network and even attack backup files on the network — targets large organizations per BGH

WannaCry: Ransomware worm that takes advantage of the Microsoft Windows exploit EternalBlue — encrypts using the AES cipher

HOW TO PROTECT AGAINST RANSOMWARE

PRACTICAL STEPS

Backups are a good defense but must be protected as well, as they often are the first thing attackers prohibit or try to destroy in an environment. Making sure backups are secure and can be accessed separately, even in a compromised environment, is a standard precautionary measure.

In September 2019, the **U.S. Department of Homeland Security** published an article outlining additional measures organizations should take to handle the threat of ransomware. The article provides advice on how to protect against ransomware, prepare for a potential incident, and recover from an attack, and where to find help. It includes practical recommendations ranging from keeping systems patched and up to date, to training end users and creating and executing an incident response plan.

USING THE MITRE ATT&CK FRAMEWORK TO ASSESS READINESS

The **MITRE ATT&CK® framework** is a comprehensive matrix that inventories and classifies the techniques and tactics used by adversaries. It includes ransomware-specific techniques under a category called "**Impact**." The information it provides allows security teams to see how they might be attacked, reflect on their abilities to detect and stop such techniques, and plan for optimal protection.

THE CROWDSTRIKE APPROACH

Because ransomware creators constantly shift their techniques, the CrowdStrike Falcon® next-generation endpoint protection platform uses an array of complementary prevention and detection methods, including the following:

- **Machine learning** for the prevention of both known and previously unknown or "zero-day" ransomware without requiring updates
- **Exploit blocking** to stop the execution and spread of ransomware via unpatched vulnerabilities
- **Indicators of attack (IOAs)** to identify and block additional ransomware behaviors and protect against fileless and new categories of ransomware
- **Automated threat analysis** to immediately obtain all of the details about the ransomware found, including origin, attribution, similar families and IOCs (indicators of compromise)

The CrowdStrike Falcon endpoint protection platform also maps to the MITRE ATT&CK framework with alerts in the Falcon platform. This allows security teams to quickly and clearly understand what is happening on their endpoints if an attack occurs — including the stage of the attack and any known adversary group that is linked to it.

INDICATORS OF ATTACK: A UNIQUE AND EFFICIENT WAY TO THWART FILELESS MALWARE

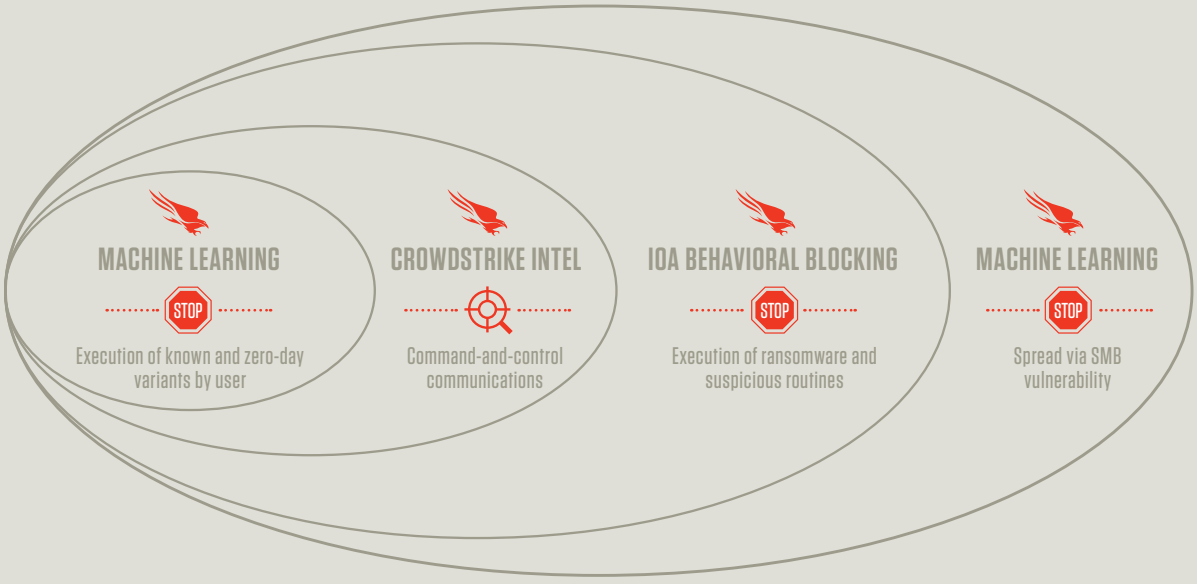
Fileless ransomware is extremely difficult to detect using signature-based methods, sandboxing or even machine learning-based analysis. CrowdStrike has developed a more effective approach using IOAs to identify and block additional unknown ransomware and other types of attacks. IOAs look for early warning signs that an attack may be underway — signs can include code execution, attempts at being stealthy and lateral movement, to name a few. By identifying the execution of these activities in real time, including their sequence and dependencies, IOA technology can recognize them as early indicators that reveal the true intentions and goals of an attacker.

IOAs also provide a reliable way to prevent ransomware from deleting backups. This gives users the ability to restore encrypted files, even if the file encryption began before the ransomware was stopped. This ability for IOAs to monitor, detect and stop the effects of what ransomware is attempting to achieve allows attacks to be stopped before any damage is done. In fact, the IOA approach is so effective and resilient against ransomware iterations that a single IOA can cover numerous variants and versions of multiple ransomware families, including new ones as they are released in the wild.

CASE STUDY: CROWDSTRIKE PROTECTS AGAINST WANNACRY RANSOMWARE

The CrowdStrike Falcon platform's multilayered prevention capabilities stopped WannaCry ransomware from encrypting files and spreading. Due to its ability to proliferate on its own, WannaCry caused a significant number of infections from a campaign that began on May 12, 2017. The speed at which WannaCry can propagate throughout an organization makes it a potentially devastating strain of ransomware. Once WannaCry is on a network, it leverages a vulnerability in the Windows file-sharing protocol Server Message Block (SMB) to move through the organization. After it is executed on a target system, it is only a matter of seconds before files on the second system become encrypted, followed quickly by the ransom note. CrowdStrike Falcon not only protected systems against the initial infection of WannaCry, it also prevented the spread of WannaCry within protected environments. In addition, CrowdStrike Intelligence was able to identify new variants quickly, and the knowledge gained was instantly integrated into the Falcon platform to provide additional layers of protection.

FALCON ENDPOINT PROTECTION AGAINST **WANNACRY**



FULL PROTECTION FROM DAY ONE

CONCLUSION

As headlines continue to remind us, ransomware remains a significant threat from cybercriminals and nation-state actors that are constantly working to increase their malicious capabilities. CrowdStrike is committed to defending against ransomware by evolving and innovating its security technology to stay a step ahead of even the most determined adversaries.

As this paper makes clear, it requires a combination of elements to adequately protect your organization. This includes taking practical steps to align your organization with sound security practices, and also deploying the innovative, cloud-native, next-generation prevention and detection technology provided by the CrowdStrike Falcon platform.

ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: **We stop breaches.**

Speak to a representative to learn more about how CrowdStrike can help you protect your environment:

Phone: 1.888.512.8906

Email: sales@crowdstrike.com Web: www.crowdstrike.com