TechTarget | Custom Media
EBOOK

Cybercrime's Most Wanted: Guide to Protection

The Changing Nature of Attacks

Cybercrime has rapidly evolved, and not for the better. What began in the 1990s as innocent pranks designed to uncover holes in Windows servers and other platforms soon led to hacker Kevin Mitnick causing millions of dollars in malicious damages, landing him in prison for half a decade and raising the awareness of cybersecurity enough to jump-start a multimillion-dollar antivirus industry. Then came the script kiddies, unskilled hackers who used malicious code written by others to wreak havoc, often just for bragging rights. If only that were still the case.

The 21st century has seen a dramatic shift from casual hacking to true cybercrime. According to Verizon's 2018 Data Breach Investigations Report,[1] half of all breaches last year were conducted by organized criminals, the overwhelming majority of whom belong to organized crime rings. The report found that 76% of breaches were motivated by financial gain, whether the goal was to steal intellectual property, embezzle cash, seize cryptocurrencies like Bitcoin or hold an organization's data for ransom by encrypting it in place, thus rendering it unusable to the organization or person attacked.

The resulting increase in the cost of cybercrime has been profound. Recently, the Center for Strategic and International Studies estimated that cybercrime in 2017 cost somewhere between $445 billion and $608 billion worldwide, an increase of more than $100 million over the lowest estimates in 2014.[2] The rise of ransomware has been a growing part of

JUNIPER NETWORKS

[1] "2018 Data Breach Investigations Report," Verizon, 2018

[2] "Global Cost of Cybercrime Exceeded $600 Billion in 2017, Report Estimates," SecurityIntelligence, Feb. 23, 2018

that cost, with Cybercrime Magazine estimating that $5 billion was spent on ransomware payments in 2017, up 1,500% in just two years.[3]

The situation is expected to only worsen. And these organized, highly coordinated attacks—of all kinds—can create far more damage in reputation and goodwill if you're not prepared for them.

Preventing such damage is the purpose behind this e-book. What follows is a lineup of today's most wanted cybercriminals, as well as a course of action to help you protect yourself, your data, your reputation, and your enterprise.

Impacts on the Enterprise

Thanks to the ubiquity and anonymity of the Internet, it's difficult to know where every cyberattack is coming from. Attacks can be instigated from organized gangs in Iran, Russia, China or the United States, and executed by a virtual army of computers in a botnet, unwittingly providing bandwidth and opportunity for malware written half the world away. Furthermore, the emergence of cryptocurrency further distances attackers from law enforcement, by using blockchain technology to isolate those paying ransom from the payees' accounts and the world's traditional financial institutions.

To help ensure the safety of enterprise data and resources, a strong line of defense is needed. And since business today is increasingly conducted on mobile devices at all hours of the day, the network security perimeter now extends beyond an organization's four walls to virtually every corner of the planet. With the number of attacks increasing, and the attack surface continually expanding, legacy antimalware protection models are no longer sufficient to meet the challenge. To keep ahead of this worldwide crime wave, new protection models—powered by advanced threat protection—are now required, and organizations that do not adapt will certainly find themselves falling prey to cybercrime or ransomware.

To thwart the advancing threats, businesses need to adopt a security posture that utilizes both intelligence and automation to augment the work human security analysts are being barraged with.

The Lineup: Organized Crime Gangs

Let's start by looking at the FBI's "Most Wanted" list, where you will find a page dedicated to those most wanted for cybercrime.[4] Topping this list recently were:

- **The Iranian Mabna Hackers,** a private Iranian government contractor group that gained access to and stole data from universities, federal and state agencies, private companies and others in dozens of countries around the world, selling the data to Iranian universities and the Iranian government itself.
- **The Jabberzeus Subjects,** a group of Russian and Ukrainian hackers that created the so-called Zeus attack, which, if inadvertently installed, can capture bank account numbers, passwords, personal identification numbers and other information necessary to log into online banking accounts, enabling the group to coordinate unauthorized transfers of funds from victims' accounts.
- **The Iranian DDoS Attacks,** another organized crime ring of Iranian nationals, employed by private security companies ITSecTeam and Mersad, that for years conducted coordinated distributed denial-of-service (DDoS) attacks on U.S.-based financial organizations and other businesses.

Also populating this list are nation-state actors, including:

- **Sun Kailiang,** one of five members of the People's Republic of China's People's Liberation Army, indicted for conspiring to penetrate the computer networks of six American companies while they were engaged in negotiations or joint ventures or pursuing legal actions with or against state-owned enterprises in China. They used their illegal access

[3] "Global Ransomware Damage Costs Predicted to Exceed $5 Billion in 2017," Cybercrime Magazine, May 18, 2017

[4] See the FBI's current "Cyber's Most Wanted" list.

to steal proprietary information including emails and trade secrets related to nuclear plant designs.

- **Igor Anatolyevich Sushchin,** a member of the Russian Federal Security Service, who worked with fellow FSB officers to penetrate major webmail and Internet hosting companies in the United States "for the purpose of commercial advantage and private financial gain."

There are other ways to categorize cybercriminals, whether organized or lone actors. Here are a few of the most notable and their raison d'etre:

The Datanapper: The perpetrator of today's fastest growing cybercrime uses a variety of techniques to plant malware on your systems that encrypts all your files, offering to give you the decryption token in exchange for a large amount of bitcoin. Motivation: Cold, hard cash.

The Hothead: Perhaps a disgruntled employee or a customer incensed by some perceived slight, the hothead wants to do as much damage as possible to your systems, data and network. These actors are motivated by powerful emotions, like Terry Childs, an IT employee of the city of San Francisco who locked every user out of the city network before turning in his ID.

The Insider: Usually also a Hothead, this cybercriminal has a big benefit: a head start from within the enterprise they are targeting, on the wrong side of the firewall. Motivators of note include intellectual property (IP), which can then be sold to competitors; embezzlement of cold, hard cash; or revenge, as in the Childs case cited above.

The Hacktivist: Several of these bad actors have ended up on the FBI's Most Wanted cybercriminal list. Whether driven by loyalty to state, today's increasingly partisan politics at home or religious differences, these cybercriminals think their belief system—whatever it may be—is better than yours. Their methods include DDoS attacks, IP theft, and exposure of your internal emails, as in the notorious Sony hack, widely believed to be in retaliation for the release of a movie that unfavorably characterized North Korea's leader.

The Proud Citizen: Those in this subset of the politicos work for a state-sponsored organization, or the state itself, with the simple goal of inflicting damage any way they can. Most active nation-state actors include Iran, Russia, China and North Korea.

The Millennial Hacker: Although these actors seem to be steadily decreasing in volume over the past decades, that may just be due to the increase in all the other categories above. However, there are still merry pranksters who sabotage systems "just because they can."

Protection Plans

- One of the most effective strategies organizations can take is to adopt an advanced threat protection (ATP) solution that incorporates machine learning and automation to help root out malware before payloads can detonate and wreak havoc network wide. Why are these types of software so important? As threats become increasingly sophisticated, they can evade traditional detection tools and strategies, evidenced by the emergence of advanced persistent threats (APTs), which can remain unnoticed for weeks or months.

  The problem is multidimensional. First is the sheer volume, with more than 250,000 new malicious programs registered every day. And malware evolves, as demonstrated by Stuxnet, which evolved to avoid detection by signature-based cybersecurity software. Sandboxing—creating a virtual environment that appears like production to "fool" the payload into detonating—has become less effective as malware writers adopt the same tools as sandbox developers. The big problem is the lack of scalability of human input: There aren't enough skilled analyst to go around, and the ones in the field don't have enough time to retrain systems to intercept evolving malware.

  Enter machine learning. ML, a style of artificial intelligence that learns relationships from analyzing very large data sets, empowers new AATPsolutions by learning correlations through the observation of patterns in the network traffic. This enables the AATPto combine data gathered from internal sandboxes with behavior logs from hundreds of millions of file objects. It learns to categorize objects simply by correlating analytics with the ever-evolving models.

Automation is also a critical component, given the speed at which malware can spread coupled with the lack of cybersecurity talent throughout organizations. A recent report by the Ponemon Institute looked at the ways automation reduces the costs and risks associated with cybersecurity and found that organizations can save an average of more than $2.3 million a year while strengthening their security posture by using cyberautomation.[5] The benefits can be rapid and dramatic, with respondents indicating that more than half of all cyberexploits or the containment of malware can be handled without any human intervention.

- Every organization should create, maintain and update their business continuity and disaster recovery plans, including offsite replication of any business-critical data or application. In the event a ransomware payload does successfully detonate in a production environment, the easiest way to avoid paying an exorbitant ransom—and perhaps discourage the bad actors—is by failing over to a known good instance without being adversely affected at all.
- Patch management should be assiduously followed, as operating systems, applications, network components and of course antivirus, antimalware and AATPsoftware that are out of date can thwart other efforts to keep infrastructure and networks secure. When reviewing patch management, ensure that endpoints are considered, especially for an increasingly mobile workforce that relies on iOS, Android and Windows devices—and often, all three at once.
- Identity and access management is often the way in for bad actors, especially for former employees, temps and contractors who hold a grudge against the enterprise. When employees (or guests) no longer need access or are terminated, loss of access should be immediately propagated throughout the network to block illicit entry before it happens.
- All software should be restricted from executing from temporary folders or zip decompression, a tactic that is often used to mask malware during detonation.
- One of the most dreaded IT tasks—backup—is still critical, but more important, enterprises must test their restore capability on a regular basis. A recent survey of 1,000 organizations found that a quarter of backups failed to work properly, with 12% reporting a corrupted backup.[6]
- Last but certainly not least, training and awareness—for all employees, not just IT—can make the difference between failure and success for any cybersecurity program. The IBM X-Force Threat Intelligence Index 2018 found that human error in the form of basic misjudgments such as storing intellectual property on an insecure personal device, falling for phishing emails or misconfiguring cloud servers led to more than two-thirds of all records compromised in 2017.[7]

Taking these steps can have a profound impact on stopping IP theft, improving resistance to ransomware and stopping malicious attacks either before they reach the network or in their tracks when they do.

[5] "Reducing Cybersecurity Costs & Risk Through Automation Technologies," Ponemon Institute, November 2017

[6] "World Backup Day 2017: Even with Backups, Users Still Lose Data," SC Media, March 31, 2017

[7] See the IBM X-Force Threat Intelligence Index 2018

Getting Started

An ATP solution can go a long way toward improving an enterprise's security posture. Here are a few considerations when evaluating ATP offerings:

- Mind the gap: Reducing the time between the introduction of new malware and its detection from weeks to hours or minutes can have the greatest impact on the spread of malware like WannaCry.
- Get smart: Machine learning will identify correlations between known malware, known false positives and payloads under consideration. ATP with machine learning built in will adapt in step with malware evolution.
- Sweat the small stuff: ATP solutions should have the ability to recognize minor behavior patterns that rules-based systems can't detect and thus catch mutations earlier and with more precision.
- Precision matters: Reducing the number of false positives and negatives that need to be reviewed by humans is critical. Lowering the signal-to-noise ratio means more time to react to real issues when they occur.
- Go global: ATP that brings a global network of shared knowledge to assist in training machine language models helps improve the effectiveness of malware detection worldwide. With machine learning, the more data, the better the outcome.
- Single pane, less pain: The ability for ATP to ingest feeds from third-party sources in the enterprise—i.e., other security products—enables the delivery of a "single pane of glass" timeline that displays all threat data across the entire environment, whether on premises or in the cloud.
- Turn data to action: Knowing there's a problem is good. Having actionable intelligence about where an attack exists in the threat life cycle is better. Automatically remediating is best.

The time to act? Now.

With the number of threats increasing daily, and threats mutating and evolving in an effort to avoid detection, cybersecurity professionals have a heavy load already. And as cybercriminals—and their attacks—become more sophisticated, the need for a higher level of threat prevention and remediation is apparent.

Since cybercriminals are already integrating artificial intelligence, machine learning and automation into their attacks, enterprises must take the same stance, using the computing horsepower at their disposal to eliminate the redundant and unnecessary work that can be handled automatically on their behalf. Fortunately, there are tools today to help.

About Juniper

Since its founding over 20 years ago, Juniper has been committed to bringing simplicity to networking, including the security and safety of information that flows through the network.

That is why Juniper introduced the Juniper Advanced Threat Prevention Appliance (JATP), which works with the security products you already have to improve productivity of both analysts and responders.

JATP can detect advanced malware in 30 seconds, fueled by threat behavior analytics and machine learning. It integrates seamlessly with existing security architecture and provides unmatched protection against advanced threats targeting your organization. It is the only solution certified by ICSA Labs to provide 100% detection of advanced threats.

JATP combines advanced threat detection with consolidated security analytics across all infrastructure and offers one-touch threat mitigation to streamline security and SecOps. With JATP, you protect on-premises and cloud-based assets, email and data, and gain a deeper insight into compromised users and endpoints.

To find out more, visit Juniper at **https://www.juniper.net/us/en/products-services/security/advanced-threat-prevention-appliance/**