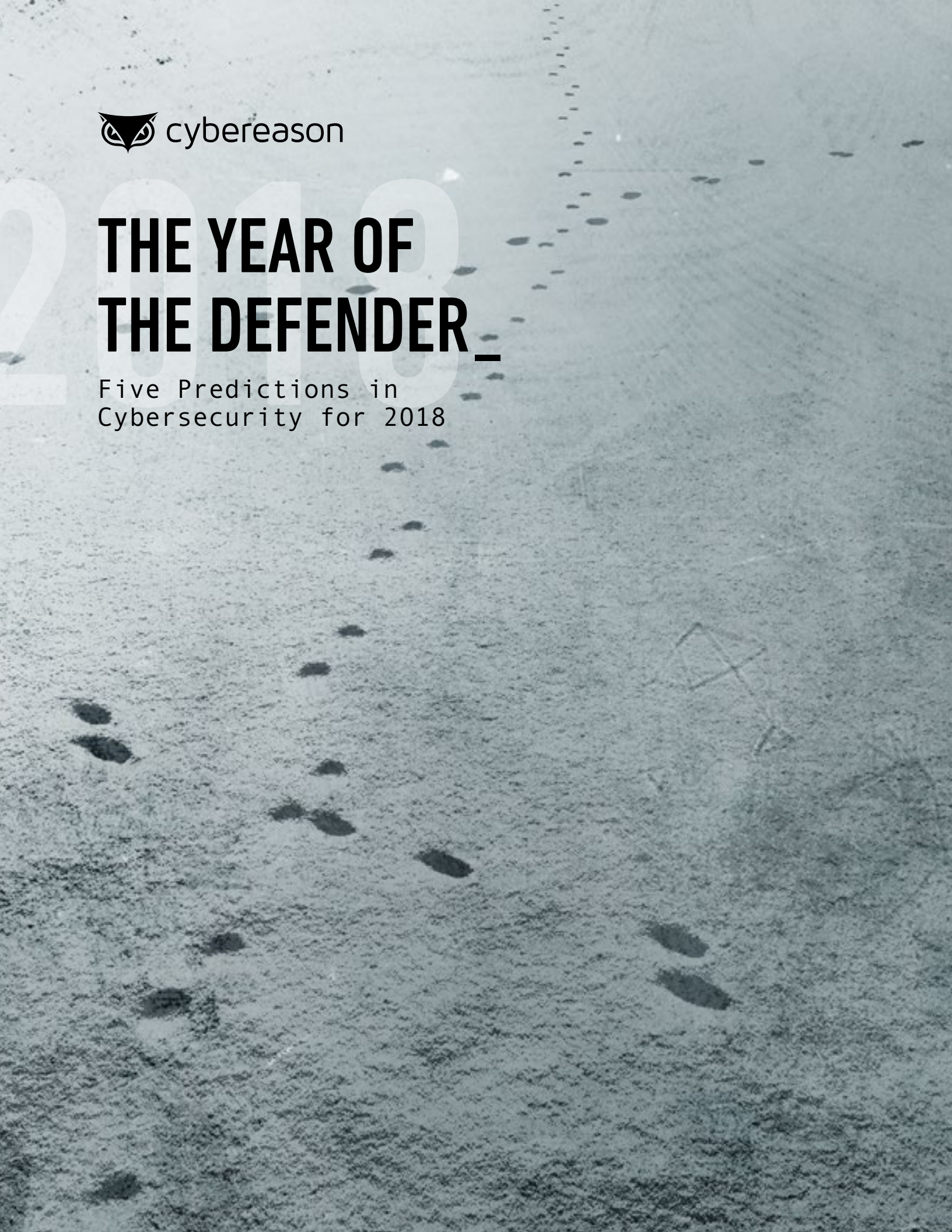

cybereason
2018
THE YEAR OF
THE DEFENDER_
Five Predictions in
Cybersecurity for 2018

FIVE TRENDS IN 2018_

WHAT DOES 2018 HOLD IN STORE FOR THE DEFENDERS?

Cybersecurity dominated the news cycle in 2017. Every few weeks there were headlines about viral ransomware, global destructive wipers posing as ransomware, leaks of spy tools from U.S. intelligence agencies and breaches at major companies. And while there are still a few weeks remaining in 2017, we're crossing our fingers and hoping that we're done with cybermeltdowns for the year.

What does 2018 hold in store for the defenders? Unfortunately, more of the same security drama, according to Cybereason's researchers and analysts. Specifically, they identified the following as some of the bigger security trends in the new year:

01. SUPPLY CHAIN ATTACKS INCREASE & REMAIN UNDERREPORTED
02. DESTRUCTIVE ATTACKS DO NOT LET UP
03. THE LINE BLURS BETWEEN APT ACTORS & CYBERCRIMINALS
04. FILELESS MALWARE ATTACKS BECOME UBIQUITOUS

Defenders will always face challenges as we attempt to protect our organizations, and no one likes end-of-the-year security reports that are all doom and gloom. And the more our researchers and analysts talked about what to expect in 2018, the more there was a cause to believe that the situation could actually improve for the good guys and gals next year. There was a bit of optimism peppered among their talk of ransomware, wipers, APTs (advanced persistent threats) and other security nasties. Organizations, they said, are finally understanding that cybersecurity really matters and encompasses more than buying antivirus software or setting up firewalls. The entire company needs to toe the line and adopt a security mindset. And this leads to the final prediction for 2018:

05. 2018: THE YEAR OF THE DEFENDER

Let this snapshot of 2017's biggest cyberincidents (illustrated on the following page) be a reminder of just how crazy things have been this year. Like all predictions, the weeks ahead will determine their accuracy. But whatever the new year holds, here's hoping that defenders are truly empowered in 2018.

2017 IN REVIEW_

MAR 2017

VAULT 7, HACKING TOOLS LEAK

Thousands of documents detailing various CIA cyberwarfare and electronic surveillance activities

RIVER CITY MEDIA, DATA BREACH

1.37 billion email addresses revealed and exposed illegal spam operation

APR 2017

THE SHADOWBROKERS DUMP, HACKING TOOLS LEAK

Contains tools and exploits of unpatched vulnerabilities

M.E.DOC, SUPPLY CHAIN

Ukrainian accounting software widely used for tax purposes. Main infection vector of NotPetya

OPERATION CLOUD HOPPER, SUPPLY CHAIN

Targeted IT MSPs in order to stealthly hack their clients' networks

MAY 2017

ONELOGIN, DATA BREACH

Customer data was compromised during this time, including the ability to decrypt encrypted data

WANNACRY, RANSOMWARE

Ransom.Wannacry is a worm that spreads by exploiting a vulnerability in Windows' implementation of SMB

JUN 2017

INDUSTROYER / CRASH OVERIDE, DESTRUCTIVE ATTACK

An attack on Ukraine's power grid that deprived part of Kiev of power for an hour*

NOTPETYA, DESTRUCTIVE ATTACK

Worm, used The ShadowBrokers exploits; Wiper disguised as a ransomware

DEEP ROOT ANALYTICS, DATA BREACH

Exposed names, dates of birth, home addresses, phone numbers, and voter registration details

INDIAN AADHAAR INITIATIVE, DATA BREACH

135 million records & 100 million bank accounts revealed

JUL 2017

HBO, DATA BREACH

Breach of servers and release of unpublished episodes, sensitive information and Twitter account takeover

AUG 2017

CCLEANER, SUPPLY CHAIN

Maintenance utility. A second-stage payload targeted high-profile technology companies

SHADOWPAD, SUPPLY CHAIN

NetSarang's products are installed on servers and workstations belonging to system admins

SEP 2017

EQUIFAX, DATA BREACH

145.5 million records of US citizens stolen

OCT 2017

NOV 2017

UBER, DATA BREACH

Uber disclosed they hid year-old hack that exposed data of 57m people, paid hackers $100k to keep quiet

VAULT 8, HACKING TOOLS LEAK

First leak of source code, more are expected

PARADISE PAPERS, DATA BREACH

Bermuda-based offshore law firm Appleby hacked, 13.4 million files leaked to a German newspaper

DEC 2017

*Attack took place in Dec 2016 and was published in June 2017

CHAIN, CHAIN, (SUPPLY) CHAIN ATTACKS_

The world witnessed several supply chain attacks in 2017, including Kingslayer, CloudHopper, CCleaner, ShadowPad, PyPi and M.E.Doc. Reports of these attacks are likely to increase in 2018 as new players enter the hacking game and gain capabilities that were once exclusive to APT-league players (see page 9 for our prediction on what next year will bring APT actors).

A supply chain attack aims to damage an organization by targeting less secure elements in the supply network. Exploiting a service provider's supply chain, data supply chain or traditional manufacturer supply chain has been seen in a litany of major data breaches in the past few years. In all of these attacks, the victim is not the ultimate target of the attack, but rather a stepping stone to other networks. There are a few common formats to a supply chain attack:

- Compromising service providers in order to gain access to their customers' systems, networks and data.
- Targeting the development infrastructure or the build/update servers of trusted applications, and introducing backdoors into the digitally signed code. Hacking the distribution points of software and software updates.
- Abusing open-source software code, knowing that it is broadly leveraged in different applications.

A VARIETY OF SUPPLY CHAIN TARGETS

Most of the supply chain attacks that occurred in 2017 targeted software aimed at IT administrators and software developers, with the exception of M.E.Doc, which backdoored accounting software used for tax filing in the Ukraine.

Targeting software used by IT and development teams is a classic attack approach. These groups often have higher administrative rights and access to secure assets, making them ideal targets. Definitely expect to see an increase in this type of supply chain attack.

But we'll also see an increase in M.E.Doc-type of attacks that compromise software that's used by other departments in an organization, like HR, marketing and accounting, and perhaps other unsuspecting business functions. This is particularly true for attackers who are looking to compromise organizations in a specific geography or in a certain industry. Any business that uses a specific, dominant platform or software is at risk for becoming an attacker choke point.

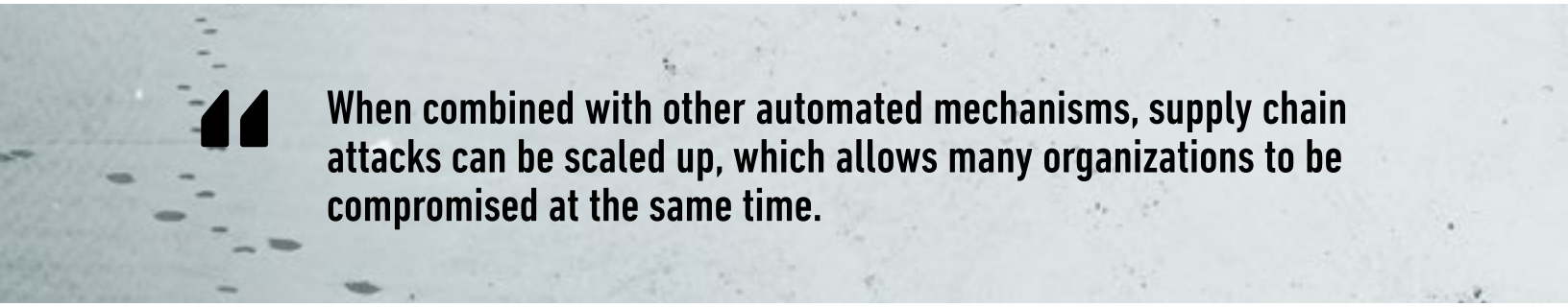
SUPPLY CHAIN ATTACKS OFFER A LUCRATIVE BUSINESS MODEL

Supply chain attacks are increasing because of their economies of scale. The past few years have been filled with massive data breaches that have flooded the underground markets with personal identifiable information, credit card numbers and bank account details. The supply of data now exceeds the demand, bringing down the value of this information. Attack campaigns are operated like a business and like any business that hopes to stay afloat, each campaign has to yield a profit, have low operational costs and a high ROI.

Supply chain attacks, such as M.E.Doc or CCleaner, enable hacking at scale: the attackers build a hacking operation that targets one organization, and through it are able to gain an initial foothold and further compromise hundreds and sometimes thousands of organizations. When combined with other automated mechanisms, these operations can be scaled up, which allows many organizations to be compromised at the same time. This powerful shift helps drive the economics in favor of the attacker.

Plus, supply chain attacks are the gift that continues to give: as long as they are not revealed, they provide ongoing access to new targets without investing in a new toolset. Compared to other common infection mechanisms like spear phishing and compromising passwords, the impact of a supply chain attack is widespread and continuous.

In some ways, improving enterprise security has helped foster supply chain attacks. With defenders cutting off easy routes to infections, attackers have become even more creative in how they attack enterprises. They see supply chain attacks as an easy way to infiltrate soft targets (especially if the company has limited security awareness and few security practices), commandeer their customers and surreptitiously install malware on their machines. Additionally, attacking trusted applications, contractors and suppliers provides adversaries with a stealthy way to compromise hard-to-reach targets, like defense contractors.



> **When combined with other automated mechanisms, supply chain attacks can be scaled up, which allows many organizations to be compromised at the same time.**

While the number of supply chain attacks will continue to grow, we expect detection to lag, especially in cases when the target provides products or services to a specific country or industry. Since most supply chain attacks include adding a backdoor to legitimate, certified software, they are rarely detected by an organization's security tools. And don't expect the software vendor that's being targeted to detect the attack. The security teams at these companies usually don't anticipate that their software would be targeted during the development stage, a point not lost on attackers.

Even if a compromised vendor discovered an attack, they could be reluctant to disclose it, fearing that their reputation would be damaged. They're likely to quietly fix the problem and leave the compromised customers unknowingly exposed. A better option (and one that we prefer and hope companies follow) is to immediately report the compromise despite the potentially painful consequences.

> **Compared to other common infection mechanisms like spear phishing and compromising passwords, the impact of a supply chain attack is widespread and continuous.**

A FEW STEPS YOU CAN TAKE NOW TO MITIGATE THESE RISKS

- Follow best security practices, monitor vendor access to internal data and networks, establish boundaries and adhere to these boundaries strictly
- Log and monitor any external vendor access, be knowledgeable of third-party providers' incident response and disaster recovery plans
- Decrease your attack surface by limiting users' ability to install third party software on machines, primarily freeware.

HIGHWAY TO THE DESTRUCTIVE ZONE_

In 2018, destructive attacks (those that look to wipe out data on a computer instead of holding it for ransom) will only get worse. The general trend, especially since 2010, has been an increase in attacks that were carried out using relatively simple, but capable, destructive malware.

June's NotPetya attack exemplifies this type of attack. While initial reports classified NotPetya as ransomware, it was later determined that the program's behavior more closely matched a master boot record (MBR) wiper, which is a very basic technique. But this very basic attack had a devastating effect that went beyond re-imaging machines and restoring data from backups: companies lost an estimated $1.2 billion in combined quarterly and yearly revenue as a result of NotPetya.

CHEAP, SIMPLE AND DESTRUCTIVE

As more actors become emboldened by the lack of consequences for conducting cyberattacks, we are going to see an increase in destructive cyberattacks next year. Most of them will show a level sophistication that's good enough to get the job done, and rely on basic tools to cause severe damage. Ultimately, cheap, dirty and effective is all any actor needs to play in this arena, a realization that many are having. For the private sector this means an increased risk of being hit by unsophisticated, yet destructive attacks.

> As more actors become emboldened by the lack of consequences for conducting cyberattacks, we are going to see an increase in destructive attacks next year.

DESTRUCTION IN DISGUISE

Along with an uptick in destructive attacks, 2018 will yield an increase in destructive malware that masquerade as ransomware. Like peanut butter and jelly or Thelma and Louise, the two go together. Take ransomware and remove its ability to decrypt files, and you have yourself a wiper. This was the case with NotPetya. Initially, the malware was labelled as ransomware. That assessment was soon amended and NotPetya is now considered a wiper.

While these types of attack may not prove rewarding for financially motivated adversaries, they're very effective at causing disruption. Disruption is an especially appealing tactic for nation-states and less sophisticated attackers who care less about profit and more about conveying a message or covering a hacking operation's forensic evidence. Cybereason researchers saw this firsthand while investigating an attack in which the ONI ransomware was used as a wiper to cover up an elaborate hacking operation.

Even though the majority of cyberincidents are still motivated by espionage or criminal activity, more destructive attacks fueled by masquerading tools, especially by nation-state actors, will be an alarming and growing trend in 2018. They're a perfect way for novice attackers to show their chops. And they provide nation-states with a developing cybersecurity program a low-cost, easy way to flex their offensive muscle. Don't be surprised if regional disputes start including destructive cyberattacks.

A FEW STEPS YOU CAN TAKE NOW TO MINIMIZE THESE RISKS

- **Create an effective data backup system:** The majority of these attacks are currently focused on destroying data and preventing access to drives. The difference between a few hours of down time and losing significant business information is dependent on how often data is backed up and the ease of restoration.
- **Develop a patch management process:** The patching process can be complex, depending on your organization's infrastructure and overall security posture. But, organizations should have a robust vulnerability management program in place to stay ahead of the curve.
- **Zero-trust environments and network segmentation:** Make the hacker's job harder by reducing their access and requiring multiple actions to have a desired effect limits their ability to wipe out an entire network. By segmenting networks and reducing the amount of inherent trust, hackers must trade time for completeness when attempting to attack a system. Segmentation will also help prevent worms and other malicious code that self propagates from affecting the entire organization.

THE APT ACTORS: GOING FROM FINE DINING TO FAST FOOD_

Advanced, targeted attacks have traditionally been associated with nation-state players, earning the countries behind these campaigns the moniker APT actors. Examples of APTs include Stuxnet, which took down Iran's nuclear program, and Hydraq, which was used in the Operation Aurora campaign that targeted Google and other U.S. companies in 2009.

But in the last few years, the lines have blurred between the attack capabilities of nation-state players and those of the lower-level cybercriminals groups. Techniques and tools that were once used by a few APT actors have been adopted by dozens of other threat actors, including freelance groups hired by government agencies and organized criminals who are using complex hacking operations to collect intelligence, steal intellectual property, pilfer sensitive financial data and even siphon cash from banks.

TWO REASONS BEHIND THIS DEVELOPMENT

THE COMMODITIZATION OF ADVANCED TOOLSETS

The Shadow Brokers and Vault 8 leaks, for example, included the source code for high-end tools allegedly developed by the NSA and the CIA respectively, making these tools readily available for everyone. Additionally, underground markets in the Dark Web offer sophisticated tools that are easy to use and customize along with complementary hacking services. This enables attackers with limited budgets, the technical knowledge, and the operational experience required to successfully enter the game. There are also more online resources for hackers to use, including free or open-source blackhat tools like RATs (Remote Access Tools), keyloggers and wipers, or sophisticated pentesting toolkits such as Metasploit and Cobalt Strike.

PUBLIC DISCLOSURE OF ATTACK TECHNIQUES

The attack capability knowledge of the three-letter government agencies is now readily available on the Internet. This is mostly the result of the Vault 7 leaks, which exposed the TTPs (tactics, techniques and procedures) of the CIA, including technical user manuals that contain ideas, operational concepts and methods.

On the topic of public disclosure, there's an ethical debate around if the research security companies release helps adversaries. On the one hand, discussing new threats and techniques helps the security community learn and keeps organizations safe. On the other, it provides the bad guys with information on how to improve their tactics.

THE BREAKING POINT FOR ATTACK ATTRIBUTION

The combined result of both of these developments is that smaller actors have access to the same assets as the big players. With this shift, 2018 will be the breaking point for attack attribution, as the security community's ability to effectively track groups based on tools and techniques decreases. When both nation-state actors and more common actors are using the same tools, the security community's ability to attribute attacks to real-world organizations or military units is severely hindered.

The popular practice of implanting false flags to throw off analysts also makes attribution extremely hard. Both APT actors and other groups are forging compile times, operating off hours (like on holidays), implanting foreign language or unique cultural evidences into pdb strings and re-registering the old command-and-control domains of other adversaries. And considering that the evidence used to attribute attacks can be tampered with, figuring out who's behind an attack is an almost impossible task.

And APT actors are making attribution even more complicated (believe it or not). As the advanced tools they once used become commodity programs, they're turning to generic ones, particularly in sensitive operations. While these programs aren't terribly slick, they're effective at getting the job done. And, most importantly, they're used by many other threat actors. For security researchers, this makes figuring out whether a nation-state or a hacking group is behind an attack nearly impossible since all the actors are using the same tools.

A COUPLE OF STEPS YOU CAN TAKE NOW TO MINIMIZE THESE RISKS

- **Remediate through a firehose:** Unfortunately with this trend, a security operations center (SOC) can no longer ignore low-priority, commodity malware. The ubiquity of this malware and the fact that it's commonly ignored by security teams is precisely why attackers are looking to use it in their campaigns. Use batch scripts and automated remediation tools to remove commodity malware, which prevent security professionals from becoming overwhelmed with work and potentially missing more advanced threats.
- **Follow the movement:** If the endpoint is where attacks originate, lateral movement into other parts of the network can help defenders determine the difference between adware and targeted attacks. Organizations should reinforce their ability to observe, trigger on and remediate lateral movement attempts. This will help ensure that the SOC is only focusing on capable hackers rather than every piece of spam or adware that a user clicks.

FILELESS ATTACKS ARE THE NEW NORMAL_

Fileless malware attacks, also called memory-based or living-off-the-land attacks were initially used by nation-state actors. While there's been a lot of buzz around this tactic more recently, it's been around for awhile. You're hearing more about it now because in recent years this technique has found its way into the toolkits of more common cybercriminals as they rely less on traditional toolkits to carry out their attacks.

FIRST, A BRIEF HISTORY ON THIS THREAT

Fileless malware is malicious code that exists in memory and not on the target's hard drive. The code is injected into a running process, such as explorer.exe, and then used for the exploit. Instead of using malware to deliver a malicious payload, adversaries use PowerShell, Windows Management Instrumentation (WMI) and other administration tools built into Windows.

HOW COMMON ARE FILELESS ATTACKS?

According to the *SANS 2017 Threat Landscape Survey*, one-third of organizations surveyed reported facing fileless attacks in 2017. Cybereason researchers have also seen evidence that adversaries are very keen on using fileless malware attacks. For example, in a large-scale attack targeting a global conglomerate based in Asia, Cybereason researchers discovered that a fileless PowerShell-based infrastructure built by the adversary was critical to the operation. This infrastructure, which used customized PowerShell payloads taken from known offensive frameworks such as Cobalt Strike, PowerSploit and Nishang, was so key to the operation that the attackers diligently worked to restore it after the customer took measures to shut it down.

Here's another example showing the prevalence of fileless malware attacks. In one month in 2017, the Cybereason Security Services Team was involved in investigating half a dozen instances of rogue PowerShell exploitation in customer environments. Many of these cases turned out to be malicious use of PowerShell by attackers. The story behind the handful of other cases was more interesting. In those instances, Cybereason discovered that the customers' red teams were conducting penetration testing and had incorporated fileless malware attacks into their exercises. Once red teams incorporate an attack tactic into their exercises, it's a clear validation that the technique is frequently used.

WHAT'S BEHIND THE ATTACKERS' INTEREST IN FILELESS MALWARE ATTACKS

To start, fileless malware attacks leverage tools that are native to Windows, making them effective and stealthy, since most security programs can't detect malicious use of PowerShell and WMI. And since there's no malware signature for antivirus software to detect (remember, there's no payload file to infect a system), those programs are ineffective at flagging these attacks.

The more defenders focus on signature-based detections, the more attackers will utilize stealthier payloads, such as obfuscating commands or using various processes to host the PowerShell engine. An example of such attack is reflectively loading PowerShell Empire DLL into a legitimate process.

Adversaries are also turning to fileless malware attacks since there are numerous readily-available tools and ready-to-use scripts that make creating PowerShell payloads particularly easy. To be clear, these tools aren't malicious by nature. They are tools shared by the information security community that offer a tremendous opportunity for red teams (and adversaries) to quickly create PowerShell payloads and evade detection. We're looking at you, Empire, Metasploit, Cobalt Strike and PowerSploit, just to name a few.

SO, WHY ARE WE PREDICTING THAT FILELESS MALWARE ATTACKS WILL BE UBIQUITOUS IN 2018? LET'S REVIEW.

- » There are a ton of free tools and free scripts that can be abused to create PowerShell payloads.
- » Very few security tools are able to detect malicious PowerShell. Scripting languages are notoriously flexible, making them easy to obfuscate.
- » Since PowerShell is as ubiquitous as Windows OS, these tactics are very effective, especially as malware droppers.
- » The security community is seeing more and more of these attacks and there's no reason to believe they'll decrease in frequency next year. When attackers find a technique that works, they to tend to use it even more (look at their fondness for ransomware).

A FEW STEPS YOU CAN TAKE NOW TO MINIMIZE THESE RISKS

- » Upgrade to PowerShell 5, require PowerShell signing, and explore the option of activating new Windows features to mitigate PowerShell downgrade attacks.
- » Implement and stick with a patch management process. A no-brainer, yet a vital best practice to protect against any of the number of malware delivery methods associated with fileless malware attacks
- » Restrict unnecessary scripting languages, limit user access to WMI
- » Implement endpoint security solutions with active monitoring. By analyzing behaviors against baselines, changes in usual patterns will result in prompt investigation of suspicious activity.

2018: THE YEAR OF THE DEFENDER?_

Every year seems to be "the year of" something in cybersecurity, whether it's "the year of the ransomware reign" or "the year of the retail hack." We decided to deem 2018 as the Year of the Defender. Too optimistic, you say? Here's our reasoning:

» Organizations have made small, yet meaningful strides around reducing the number of days to identify and contain a breach, according to the Ponemon Institute's 2017 Cost of Data Breach study. In 2017, organizations took an average of approximately 191 days to identify a breach, down from 201 in 2016. Meanwhile, containing a data breach took 66 days, compared to 70 days.

» Fileless malware attacks, particularly those attacks that leverage PowerShell and WMI are here to stay. The good news, though, is that in light of these attacks, they have prompted a change in detection capabilities and solutions. The hype cycle around fileless malware attacks has risen to a point where it is finally on every security team's and organization's agendas. We believe that there is no better time to improve the way teams handle these attacks. A combination of tools and teams share of mind to this problem will help, and we're optimistic – 2018 is a good year to see this shift happening.

» Next year, companies around the world will truly get aboard the cybersecurity train (Choo! Choo!) thanks to the General Data Protection Regulation (GDPR), a new E.U. regulation that governs how businesses protect the data and privacy of E.U. citizens. While the GDPR is an E.U. measure, its implications are global. All companies, regardless of whether they're located in the E.U. or not, must comply with the GDPR if they handle the data of E.U. citizens. Noncompliance results in major fines being levied against a company, a situation that any company undoubtedly wants to avoid. Complying with the GDPR forces them to plan in order to comply with it, making cybersecurity an issue for the entire C-suite.

» If security wasn't already a board-level topic of discussion in 2016, damaging attacks like NotPetya undoubtedly made it one in 2017. During earnings calls, C-suite executives from global corporations discussed how NotPetya impacted quarterly and yearly revenue. While losing money is never something to celebrate, NotPetya made the importance of effective cybersecurity a board-level topic once and for all. And with boards paying more attention to cybersecurity in 2018, their support will further empower the defender.

Learn more about Cybereason