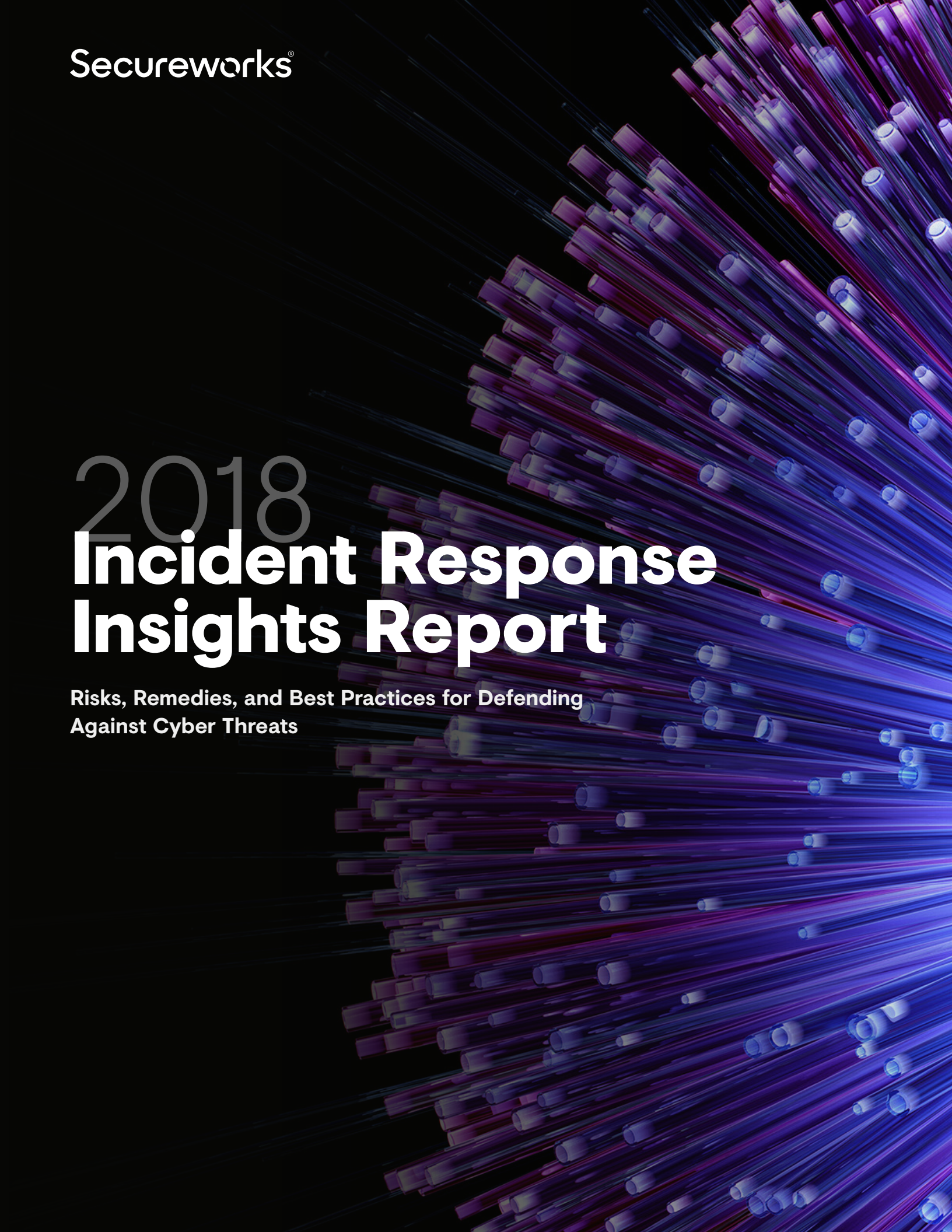
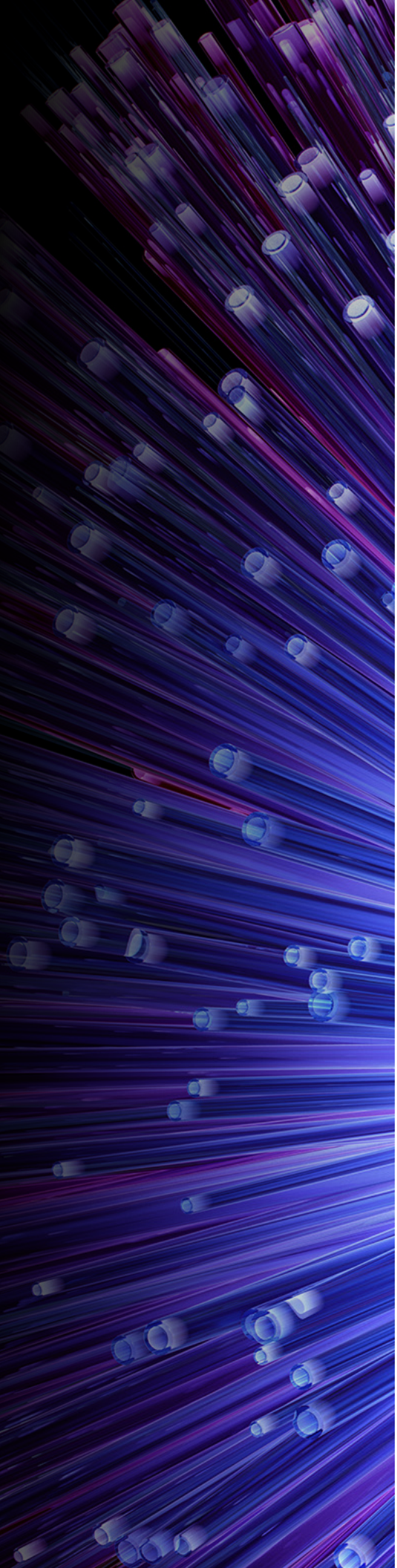
Secureworks®



2018

Incident Response Insights Report

Risks, Remedies, and Best Practices for Defending Against Cyber Threats



Contents

Secureworks®

Executive Summary

You don't have to look hard to find examples of major cybersecurity breaches in 2017 that created significant damage or disruption for the organizations involved. Indeed, news of these incidents has become commonplace. All too often, companies are learning in the hardest way possible – when an incident happens – how they could have been better prepared or responded more effectively.

In 2017, Secureworks'® Incident Responders helped hundreds of organizations navigate through complex and high-risk incidents. Our investigation, engagement, and insight into these actual breaches, plus our visibility across 250 billion log events every day, affords a deep understanding of the ever-shifting threat landscape – and how companies are defending themselves against these threats. This report shares best practices and valuable lessons learned over the past year from these real-world incidents.

Our 2017 incident analysis reveals the following:

1

Many organizations are overlooking fundamental security practices and hygiene, leaving gaps that are being exploited by online adversaries.

More than 80% of the recommendations Secureworks made to organizations after an incident included security fundamentals (such as patching, user account management, implementing multi-factor authentication, and disabling unused protocols).

2

In many organizations, a general lack of visibility of their own environments allowed threat actors to go about their business largely undetected.

50% of companies had insufficient endpoint or network visibility. On average, targeted threats remained undetected in networks for 380 days.

3

Organizations need to mature their incident planning in order to respond more effectively and defend faster against a variety of threat types. Specifically, they need to test and exercise their plans – which can familiarize network defenders with their roles and smooth out response processes, ensuring that the right data and logs are easily available to incident responders, for example.

In 70% of incidents Secureworks identified deficiencies in access to or quality of logs, which slowed response efforts.

"Rather than adopting proactive security services simply to 'check a box,' embrace them as a way to mature security capabilities."

Jeffrey Carpenter, Senior Director, Secureworks' Incident Response Consulting Practice

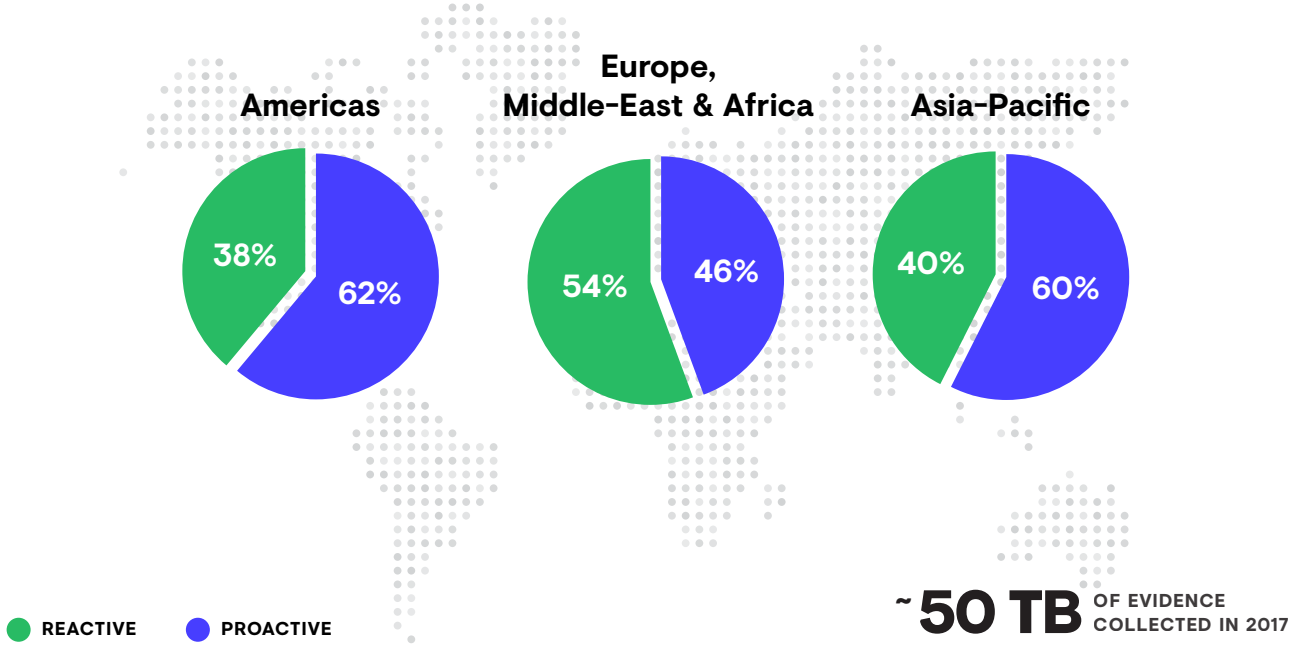


FIGURE 1: *Profile of response services provided globally by Secureworks in 2017.*

About This Report

Throughout the course of 2017, the Secureworks Incident Response team and Secureworks Counter Threat Unit™ (CTU™) conducted 996 incident response engagements, including both accredited reactive and proactive services, across the full range of industry sectors. In all, clients received tens of thousands of hours of leading incident response services that helped them plan for, detect, respond to, and recover from cybersecurity incidents of all types.

Secureworks' reactive incident response services, involving live response to ongoing situations, came in all shapes and sizes – from analyzing malicious files and forensic analysis of a single system, to comprehensive and coordinated eviction of advanced threats that had been lurking within large networks for years.

In addition, proactive services helped organizations plan for incidents (Incident Response Planning), rehearse the plan (Table Top Exercising or Workshops), proactively hunt for threats (Targeted Threat Hunting), or find evidence of compromise within networks.

The recommendations delivered in this report are based on the sum total of observations made by Secureworks during emergency incident response and threat hunting engagements, as well as the trends observed during proactive threat hunting, tabletop exercises and risk assessments.

Learning from Incident Response Outcomes in 2017

A Global Profile of the Threats

Secureworks incident responders encountered a wide range of threats in 2017 in three notable categories: financially-motivated criminals, nation-state sponsored threat actors, and insiders. The majority of incidents were attributed to the criminal category (83%), and Figure 2 highlights the diversity of these typically high volume schemes. Although Nation-state sponsored and insider threat categories represented a smaller percentage, they often had a higher impact on their target.

Top 3 industry verticals most impacted by nation-state sponsored threats 2017

Manufacturing

Technology Provider

Government

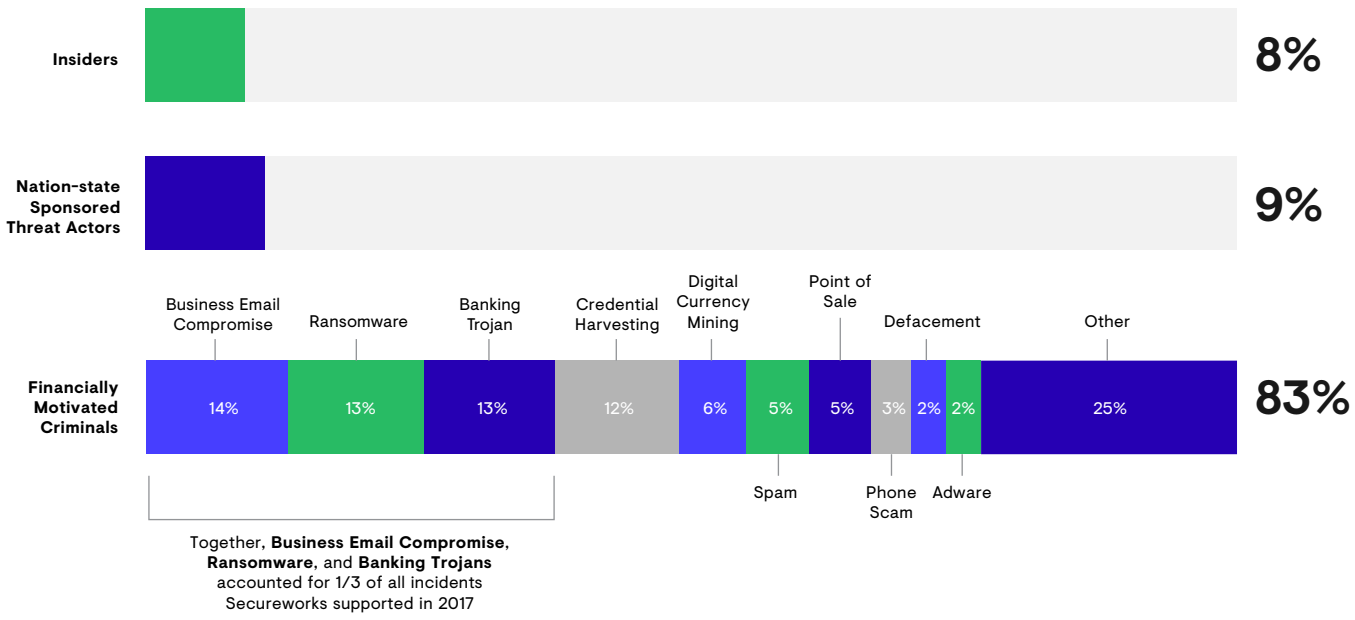


FIGURE 2: *Profile of threat categories and classes observed during incident response engagements in 2017.*

Within the criminal category, three threat classes in particular -- Business Email Compromise (BEC), Ransomware and Banking Trojans -- accounted for 1/3 of all incidents. These threats are prolific, and all organizations should remain vigilant.

Business Email Compromise (BEC) incidents – where criminals intercept and change financial details to re-route money into bank accounts under their control – continue to generate startling sums for criminals (Secureworks State of Cybercrime Report, 2017). Figures released by the FBI in 2017 suggest global losses of more than $5 billion over a three-year period. BEC represented 14% of financially-motivated criminal incidents supported by Secureworks in 2017 (see Figure 2), and it is expected to be a constant feature of the criminal landscape for the foreseeable future.

Ransomware went mainstream. WCry (also known as WannaCry) spread globally, and familiar variants like SamSam and Locky kept incident responders busy. WannaCry's key feature was speed, SamSam actors used compromised systems to deploy their ransomware, and a variety of other ransomware payloads were spread using indiscriminate methods like spam emails. While the attack methods varied, the business impact was consistent: key systems became unavailable, affecting business continuity or worse (see Figure 4).

Flawed assumptions like "we have backups so we shouldn't worry," "all ransomware threats are the same," and "we can always just pay the ransom" can be dangerous. In a high-pressure situation, organizations should already have rehearsed their options and know the practical realities of paying or not, including the possibility that data may not be returned.

Banking trojans delivered through massive criminal botnets, while no longer the dominant presence in the criminal threat landscape, remained common in the 2017 cyber threat landscape.

In other threat categories:

Nation-state threats were more diverse in 2017 than ever before. Approximately 9% of Secureworks incident response engagements involved evicting nation-state threats from targeted networks, but they were often the most time consuming to resolve.

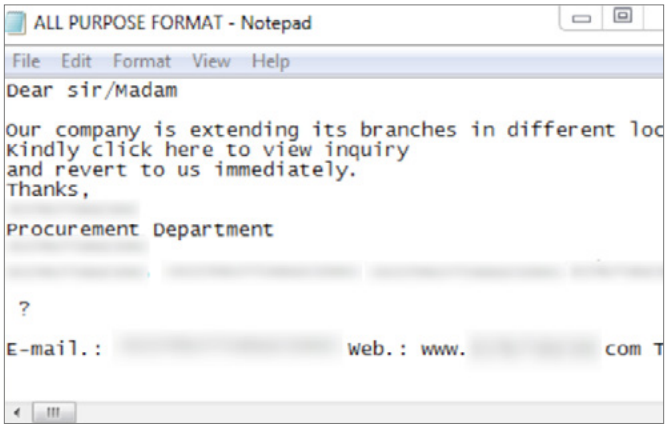


FIGURE 3: *A Business Email Compromise threat actor composes a phishing email. (Source: Secureworks)*

FIGURE 4: *Desktop background that appeared when WCry ransomware successfully executed. (Source: Secureworks)*

Due to the often entrenched nature of these adversaries – plus the necessity to fully understand the extent of the threat actor's capability and access – the average time it took to evict was 500% greater than when responding to other non-targeted threats.

The top three verticals most impacted by targeted threats in 2017 were manufacturing, technology providers and government institutions. Cyber attacks sponsored by nation-states continued to compromise manufacturing and technology organizations in 2017, primarily in pursuit of intellectual property (such as product designs and blueprints), as well as targeting government networks for political secrets (including PII data). In 2017, Secureworks CTU researchers observed BRONZE UNION, a threat group of Chinese origin, targeting defense, security, and political intelligence from organizations in the aerospace, government, defense, technology, and manufacturing verticals.

In 2017, the average time to evict advanced threats was 500% greater than the time to evict non-targeted threats.

```
C:\windows\temp\alg.exe a -m5 -v2000m -hp
[PASSWORD} -inurl -r " [DESTINATION] .rar" "\\[FILE
PATH] \Projects\ [SENSITIVE PROJECT FOLDER]"
```

FIGURE 5: *BRONZE UNION prepare sensitive technology data for exfiltration. (Source: Secureworks)*

Targeted threats often seek to cover their tracks

```
C:\Windows\Explorer.EXE
    "C:\Windows\system32\cmd.exe"
        REG DELETE "HKCU\Software\Microsoft\Terminal Server Client" /F
```

FIGURE 6: *Secureworks Advanced Endpoint Threat Detection (AETD) Red Cloak™ catches Iran-based threat group, COBALT TRINITY covering its tracks by deleting a registry key containing information about the group's lateral movement activities. (Source: Secureworks)*

Behind the Scenes: What Is AETD Red Cloak™?

As referenced in Figure 6, Advanced Endpoint Threat Detection (AETD) leverages Secureworks' proprietary Red Cloak™ Endpoint Detection and Response (EDR) technology, developed by the Secureworks Counter Threat Unit (CTU) team and the company's threat hunters. AETD and AETD Elite with Active Threat Hunting provide endpoint visibility to identify threats that evade antivirus and other threat prevention technologies, even advanced threats and those that use little or no malware. Red Cloak leverages extensive, detailed insights into how adversaries operate—intelligence harnessed from actual threat hunts and incidents over the years.

How Attackers Gained Entry

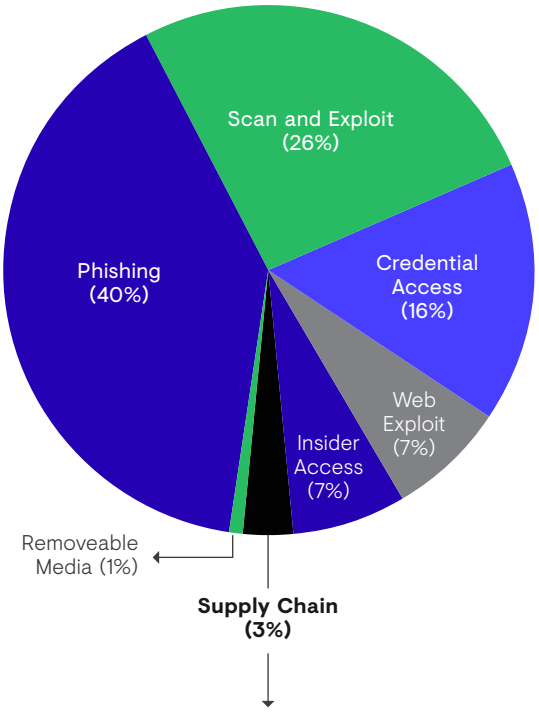
Phishing continues to be the delivery method of choice for the majority of attacks, whether targeted or opportunistic. Some 40% of incidents started with a phishing email designed to deliver malware or steal account passwords. Phishing continues to be an effective way of luring people into opening attachments and links that deploy malicious software. A combination of user education and security controls (such as automated malware sandboxing) continues to be the best method for reducing phishing risks – but there's still a long way to go. According to Secureworks' 2018 Security Leaders Survey, 42% of respondents said malware sandboxing was a component of their company's incident response program today.

Supply chain attacks represented some of the highest risk incidents in 2017. While representing just a small portion of total attack methods (3%), they were typically associated with high-impact, targeted threats.

During some of these events, the adversaries were able to insert malware into updates for legitimate software. In the past 12 months, trojanized updates were used to carry out the high-scale NotPetya disruptive attacks (via MeDoc software) and espionage (using Netsarang, and CCleaner). Trojanized software updates greatly improved the threat actors' odds of entering networks undetected in these cases, and there's no reason to assume that these methods won't continue into 2018.

Web exploits accounted for 7% of incidents, as they tested organizations' ability to patch, harden, and monitor their systems for both high volume and targeted exploit attempts.

Scan and exploit represented 23% of total attack methods. Threats of all types continue to exploit vulnerable internet-facing systems and services – from password guessing attacks on vulnerable internet-facing services, to placing discreet webshells on vulnerable servers.



Supply Chain Access: Not To Be Underestimated

Access via the supply chain, while representing a smaller percentage of total methods used by attackers, was typically associated with high-impact, targeted threats.

FIGURE 7: *Methods of access observed during incident response in 2017.*

Top 5 Recommendations Made in 2017

Here's a summary of the most frequent recommendations Secureworks made to organizations during 2017 engagements:

Implement or Enhance Logging
Too often, incident responders are unable to piece together what happened because logs were not available or did not contain the right information.

Adopt Multi-Factor Authentication (MFA)
Networks and services that are accessed remotely by users cannot be protected by a user name and password alone. Sooner or later, public-facing accounts without MFA will be compromised.

Manage User Account Privileges
Attackers routinely exploit redundant accounts or accounts with unnecessary access rights to obtain more privileges in a compromised network. They often target administrative access on end user systems to gain an initial foothold.

Integrate Endpoint Security Capabilities
A consolidated view of suspicious behaviors and events on endpoint systems is a powerful tool for detecting and responding to a threat after a compromise. Such endpoint visibility is crucial in understanding the nature of an ongoing intrusion.

Develop or Practice Incident Response Planning
Responding to incidents effectively is difficult without the right preparation. Organizations are more resilient when tried and tested response plans are in place.

Taken together, the lessons learned across incident response engagements throughout 2017 are a reminder that tackling **network security fundamentals** is still a major issue for organizations of all shapes and sizes; detection and response are too often hampered by inadequate logging and **visibility** into the environment; and a lack of **planning and practice** is impeding organizations from remediating effectively to minimize operational and business risks.

The Stakes Are High for Network Security Fundamentals

Once threats gain access to a network, they routinely capitalize on shared or legacy user accounts or accounts with unnecessarily high privileges to get a foothold and move within the network.

Applying The Lessons for a Stronger Defense

Success Starts with Fundamentals

Patch, Patch, and Patch Again

Patching lapses were a consistent theme in 2017 response engagements. While patching guidance and best practices are plentiful, the practicalities of applying patches to all affected assets, as soon as they become available, is rarely a straightforward exercise. Patching is often de-prioritized due to concerns about business continuity, for example. However, there is compelling evidence for getting it done. A significant proportion of the incidents Secureworks investigated traced back to a vulnerability being exploited where the vendor had already issued a patch.

WannaCry: a Wakeup Call

WCry (also known as WannaCry) was the event in 2017 that truly mainstreamed the debate about patching. In May, WannaCry exploited a security hole in a Windows protocol that allows file and printer sharing (called SMBv1). WannaCry quickly made headlines as the ransomware spread around the world, facilitated by a wormable exploit that spread self-replicating malware from system to system.

Back in March, almost two months before WannaCry hit, Microsoft had released a patch for those vulnerabilities. Then in April, a group called Shadow Brokers released an existing exploit for that vulnerability on the Internet (see Figure 8). When WannaCry hit in May, it quickly became apparent how many organizations had not applied Microsoft's patch, as a large number of high-profile organizations were badly affected. Those who applied the patch were protected.

WannaCry was a reminder that the difficulty and cost of patching a vulnerability must always be considered in the context of how seriously the organization could be impacted if that vulnerability were to be exploited by a cyber threat. Long-term reputation and revenue are at stake.

FIGURE 8: *Timeline of 2017 WCry outbreak. (Source: Secureworks)*

Prioritize patching efforts with intelligence.

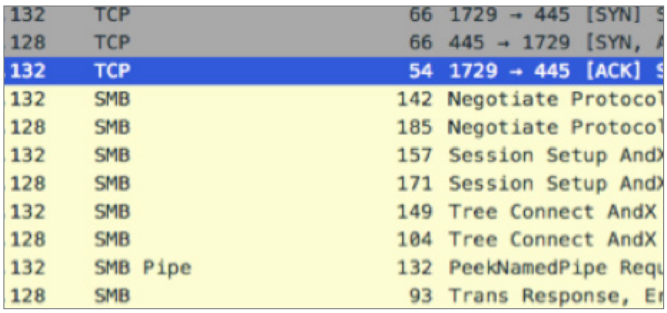
One of the difficulties of running an effective patching program is that a vulnerability is only a problem if threat actor intent and capability exists to exploit it. Knowing which ones are urgent, because they're being actively exploited or because of the potential impact, can be a challenge.

A solid grasp of the threat landscape can help. Trusted threat intelligence suppliers, alongside the vibrant online cybersecurity community, can act as useful signposts for vulnerabilities that genuinely require urgent patching. One great example was the intelligence community's quick recognition of the combined risk posed by Microsoft's recommended patch and exploits released by the Shadow Brokers group both before and after the patch release. Knowing what vulnerabilities pose the most risk can aid better prioritization and management decisions, and ultimately reduce costs and risk.

Implement compensating controls when you can't patch.

If you can't patch because of the potential disruption to business operations or fear of breaking critical dependencies, it's essential to adopt alternative compensating controls. Regarding the WannaCry outbreak, for instance (see Figure 9), organizations could have disabled the SMBv1 protocol on network segments that didn't use it, creating a short-term alternative control for the Microsoft patch.

Even with compensating controls in place, it is still essential to have hygiene policies and network architecture in place for prevention, along with monitored endpoint and network security applications for faster detection.



132	TCP	66	1729 → 445 [SYN] S
128	TCP	66	445 → 1729 [SYN, A
132	TCP	54	1729 → 445 [ACK] S
132	SMB	142	Negotiate Protocol
128	SMB	185	Negotiate Protocol
132	SMB	157	Session Setup AndX
128	SMB	171	Session Setup AndX
132	SMB	149	Tree Connect AndX
128	SMB	104	Tree Connect AndX
132	SMB Pipe	132	PeekNamedPipe Requ
128	SMB	93	Trans Response, Er

FIGURE 9: *WCry used a worming component that exploited the SMBv1 vulnerability. (Source: Secureworks)*

"The idea that attacks are leveraging zero-day vulnerabilities which defenders are powerless to prevent is a myth. In almost every case where software vulnerabilities were exploited to gain access to a network or system, the vendor had released security patches for those vulnerabilities months beforehand."

Don Smith, Senior Director, Secureworks Counter Threat Unit (CTU) Operations & Analysis

Hygiene Highlight: Maintaining Anti-Virus Signatures

Secureworks incident responders continued to find WCry ransomware artifacts in engagements in late 2017, where only the existence of the "kill switch" domain prevented the ransomware from executing. Secureworks also identified examples where the same SMBv1 exploits had been successfully used to deploy cryptocurrency mining software, rather than the ransomware component used by WCry. These investigations highlight the importance of maintaining anti-virus signatures: in one of the incidents, anti-virus failed to identify the WCry malware because the signature pack had not been updated for several years.

The Three P's of Protection

Secureworks 2017 Incident Response investigations provided a valuable reminder of how important it is to prioritize the basics above all else, even in a comprehensive program with the latest technologies. A program can only be effective if people, process, and technologies are working in concert to defend against cyber threats. Three of the basics that frequently make the difference between a high and low impact incident are:

- **Partitioning** or segregating your network
- Reducing user **privileges**
- Understanding and hardening your **perimeter**

While easy to comprehend, these basics are often difficult to implement. The consequences of ignoring them become crystal clear, however, when looking back across a year of experience from the trenches.

Partitioning

Partitioning, or network segmentation, can include geographical segmentation, user role segmentation, and segmentation of sensitive systems – in all cases, only allowing users to connect to systems where a business reason exists. This prevents malware from having free rein on the network.

During the high-profile NotPetya destructive attacks, partitioning proved to be the difference between limited or extensive business impact. At approximately 10:30 on June 27, the NotPetya destructive attacks began tearing through organizations across the globe, rendering systems inoperable.

The spread was aggressive. For example, Secureworks has seen cases where vast proportions of organizations' networks have been destroyed within minutes of the initial infection, and the entire organization brought to standstill within a couple of hours (see Figure 11).

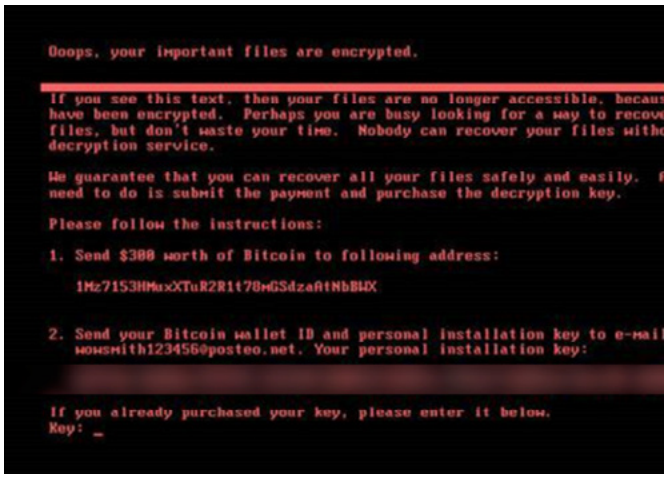


FIGURE 10: *"Ransom note" delivered after a NotPetya compromise. (Source: Secureworks)*

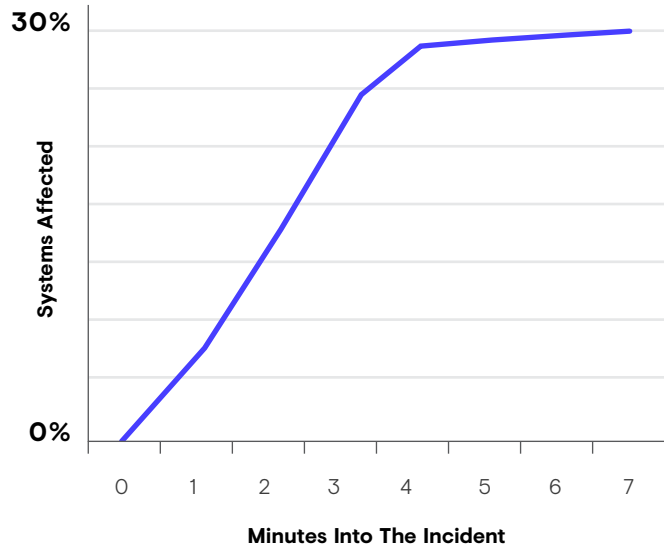


FIGURE 11: *Rapid spread of NotPetya, destroying a third of one organization's systems in 2 minutes. (Source: Secureworks)*

NotPetya masqueraded as a ransomware attack, but subsequently appeared to be a high-collateral, destructive attack targeting entities within Ukraine. The software update service deploying the Ukrainian accounting software MEDoc was compromised to deliver NotPetya instead of the latest software update. Thousands of organizations were hit, and Secureworks was asked to assist with the incident response in a number of cases. Some clients were brought to a complete standstill – the vast majority of their IT estates destroyed and normal business operations ceased, costing many millions of dollars. Other organizations were in better shape, with the attack contained to their Ukraine-based systems.

The deciding factor between limited impact and all-out devastation was related to how the malware spread. NotPetya harvested credentials from memory as one way of spreading. Some of the credentials it gathered had full administrative privileges, and a network with less segmentation would have allowed those user accounts to connect to almost every other system on the global network. Where organizations had effective privilege management in place, as well as internal firewalls creating network segments that default-deny connections to other systems, it was much easier to contain the malware spread.

Privileges

User permissions also tend to be crucial when preventing initial malware infections; if a user can't install new programs without prior authorization — a control known as application whitelisting — then it becomes much harder for malware to gain a foothold on the system. 2017 witnessed the re-emergence of Shamoon attacks in the Middle East designed to cripple business operations. Shamoon was first observed in an attack against Saudi Aramco in 2012; but in late 2016 and early 2017, up to 30 organizations were targeted in a new wave of attacks (see Figure 12).

The Curious Case of Mia Ash

The importance of managing user privileges was painfully clear when our incident responders saw firsthand the sophisticated techniques employed by COBALT GYPSY, the Iran-based threat group believed to be behind the Shamoon attacks. When generic phishing and subsequent targeted spear-phishing attempts aimed at employees didn't work, the group launched one of the most sophisticated social engineering campaigns ever witnessed by Secureworks.

They created a fake persona – a London-based photographer named Mia Ash – to "befriend" an employee at the target organization via LinkedIn. After weeks of conversation, she eventually sent him an email containing a malicious attachment and asked him to open it on his work computer. Even though the user tried to open the attachment, it did not run because the employer restricted user permissions sufficiently. This case highlights the importance that limiting user permissions (such as privilege restrictions and application whitelisting) can play in preventing highly targeted and persistent attacks.

FIGURE 12: *Fake Mia Ash LinkedIn profile. (Source: LinkedIn)*

Perimeter

Finally, protecting the perimeter has always been a staple of the security industry. While cloud services increasingly blurred network boundaries, an escalating number of incidents also demonstrated how easily traditional (non-cloud) perimeter weaknesses can be exploited.

Know what is facing the internet. In 2017, a number of Secureworks customers experienced SamSam ransomware incidents, where the threat actor gained access by identifying Remote Desktop Protocol (RDP) services that did not use two-factor authentication or lock accounts after multiple authentication failures. With only a single sign-in to block their path, the threat group was able to successfully brute-force these services, guess passwords, and use the subsequent access to deploy SamSam and propagate it throughout the network (see Figure 13). Secureworks has observed the SamSam threat actor (nicknamed GOLD LOWELL) attempting as many as 500,000 RDP login events that went unnoticed before the actor managed to gain access.

Another example is the WannaCry campaign, which used vulnerable SMB public facing services to propagate. In most cases, there should be no reason for SMB traffic to be allowed from the network out onto the internet, or SMB traffic from the internet into the network.

Incidents that traverse cloud infrastructure are generally becoming more common, challenging companies to think more broadly about their perimeters. While these incidents are rarely exclusive to cloud infrastructure and typically involve local systems and processes, they illustrate the potential security challenges associated with cloud deployments and highlight some meaningful risk mitigation strategies.

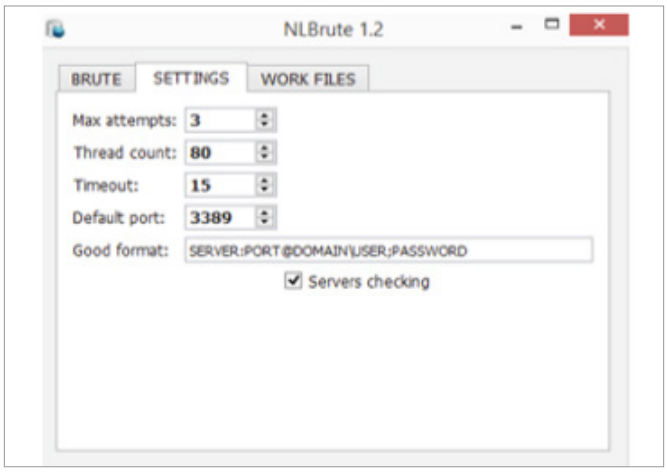


FIGURE 13: *Screenshot of the brute force tool used during SamSam intrusions. (Source: Secureworks)*

Controls to protect your on-premise perimeter:

- Know what ports and services you have facing the internet.
- Reduce and remove these where possible.
- Patch when required.
- Improve visibility at the endpoint.
- Use appropriate access management controls such as two-factor authentication and password lockout policies.

In 2017 our incident responders investigated a compromise of an account in a cloud storage environment. They determined that the security policy configuration on an affected system left it open to brute-force attempts. The password guessing continued for at least a month, leading to multiple accounts being compromised and enabling the threat actor to create multiple other local accounts on the system.

In a separate incident, access to credentials for an organization's cloud environment led to multiple accounts being compromised. A threat actor used these accounts to create new cloud instances, create and delete access keys, and alter passwords and password policies in the organization's cloud environment.

In the first example, the threat actor exploited vulnerabilities created by configuration issues, emphasizing the importance of effective configuration management and testing. Monitoring for account lockouts and brute-force attempts also would have helped mitigate the activity. In both incidents, the impact would have been limited if the organizations had controls to prevent malicious user account creation or permission changes, and used multi-factor authentication (MFA) on internet-facing applications.

"We are routinely encountering incidents where threats are getting access to networks through internet facing services that only require a single password to gain access."

Jeffrey Carpenter, Senior Director, Secureworks' Incident Response Consulting Practice

Controls for cloud services

Focus on extensions of existing on-premise security controls

- Ensure effective access control. This safeguard is essential and should include multi-factor authentication (MFA) for all public-facing access. Administrator access should ideally use MFA and IP whitelisting from the corporate address space.
- Ensure that configurations adapt as systems are added and removed. Many will elastically open firewall rules to systems when they're created, but not remove them when they're deleted. Secureworks has seen incidents where threat actors have leveraged this configuration hole to remove sensitive data from the environment by naming systems they own with a previously-used corporate system name.
- Regularly review and monitor user permissions, privileged activity, and configurations.
- Implement threat intelligence-led monitoring of available logs, endpoints, and network activity, where possible.

Your Best Intel Source: Visibility Into Your Environment

See More, But Focus on What Matters

One of the first steps in any threat hunt or in-depth incident response investigation is to deploy endpoint agents that help responders see more, giving them immediate, broad, and deep visibility into suspicious activity on hosts. That insight quickly helps you understand the risk you are carrying.

Visibility is a good thing, but you also need enough context to interpret what you're seeing and use it to your advantage. In most cases, the initial deployment will identify a range of opportunistic trojans, adware, and other malware in your environment. Triaging all those alerts and working out which ones are important can take time and may distract incident responders from the task at hand. Ideally, organizations will have a handle on commodity threats in advance so that incident responders don't have to deal with a high volume of commodity infections and can focus their time on issues specific to the incident at hand.

In one lengthy threat hunting project, AETD Red Cloak identified commodity or opportunistic threats on 46% of the total hosts to which it had been deployed. In a different investigation, where the initial threat hunt was in response to data theft by a nation-state actor, malicious activity was identified on 23% of hosts. Only a small proportion of that activity was related to the targeted intrusion (see Figure 14), but it was difficult for the in-house security team to focus on that more serious activity because of the general hygiene conditions highlighted through the deployment of Red Cloak.

Serious Threats Can Hide In the Noise of High Volume Commodity Infections

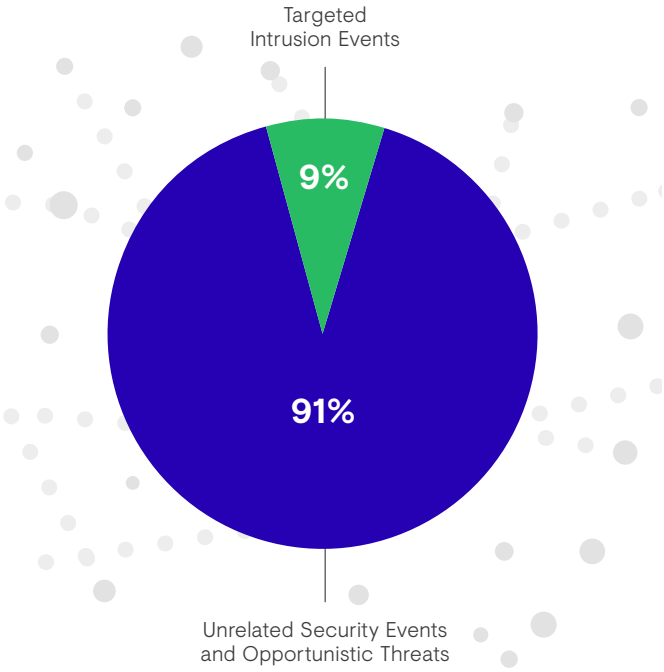


FIGURE 14: *Results of a threat hunting engagement deployed to investigate data theft discovers high volume of unrelated malicious activity. (Source: Secureworks)*

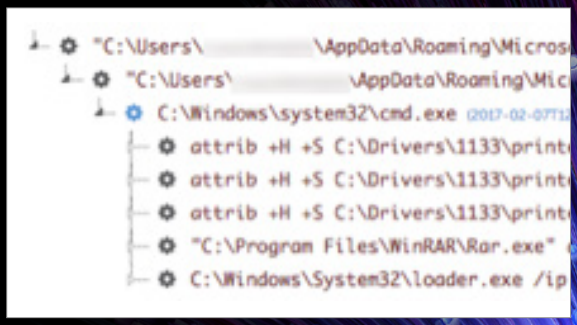
Triaging the findings of an incident response investigation is much easier if you can tell the difference between what's malicious and what is internal research activity or security testing.

Commodity threats within your environment most likely means you have gaps in existing prevention and detection controls. Getting visibility and a good understanding of what normal activity in the environment looks like can go a long way towards addressing this challenge. It also increases the chances of spotting sophisticated threats earlier or, at the very least, ensuring that once they're spotted, the incident response effort is faster, reducing the overall risk to the organization.

In Secureworks 2018 Security Leaders Survey, 43% of respondents said that regular threat hunting activities were part of their incident response program.

As an illustration of the power of endpoint agents, Secureworks AETD Red Cloak endpoint agent detected an active intrusion and theft of tens of gigabytes of data that occurred on the day of a proactive threat hunting engagement, prompting a major incident response engagement. Had this activity not been found, the impact would have been even worse, with even more data loss and the threat actor entrenching to enable long-term data theft.

The Value of Threat Hunting



AETD Red Cloak detecting exfiltration preparation. (Source: Secureworks)

Foresight Is Better Than Hindsight

Incident response is technically complex work that happens amid business pressure to rapidly contain or evict the threat. So the challenge becomes exponentially greater when an organization has not done the groundwork in advance to ensure that all relevant logs are being captured appropriately and to fully document its environment. There are also many cases where the visibility existed to detect a threat long before the incident, but because the key information was not monitored, it went unnoticed.

Finding the missing pieces is a challenge when there's no history

Figure 15 shows the various reasons why the root cause of incidents went undetected, leaving organizations without concrete evidence on which to base future priorities and investment. In 42% of these unresolved cases, a lack of logging and visibility was the problem. A further 38% of cases had sufficient logging, but the logs didn't go back far enough to allow a full historical analysis. The more logging that's in place, configured in a way that enables security incidents to be understood, the greater the chance of successfully identifying the root cause of an incident and defending better in the future.

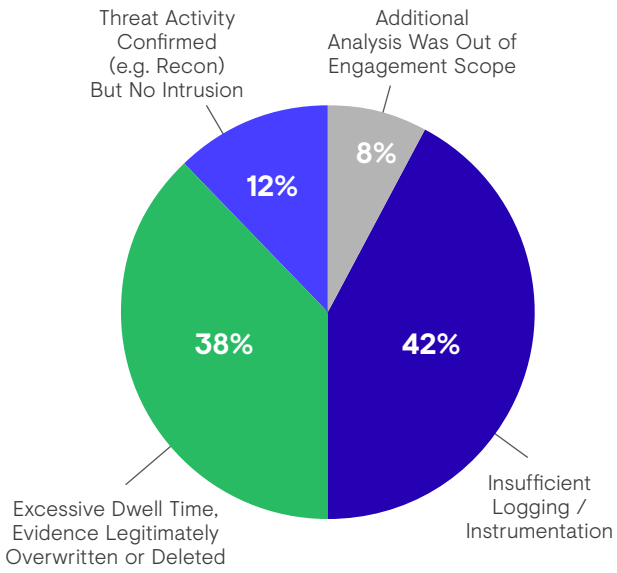


FIGURE 15: *Reasons why incident root cause remained unidentified in a group of 2017 incidents.*

All logs are NOT created equal

Assess log quality. During several cases in 2017, incident responders encountered systems that, while configured to retain logs for several months, did not contain useful information for the investigation, such as login and logoff events. Thus, the act of logging is not enough. In addition to making sure that systems are writing and retaining logs, it's also important to ensure they're configured to log the type of information that will allow network defenders and responders to piece together what happened. Forensic readiness includes ensuring that logging best practices are applied in all the right places before an incident occurs.

"The majority of incidents tend to have log analysis at their core, with effort spent trawling through logs from various sources to understand what happened and when."

Jeffrey Carpenter, Senior Director, Secureworks' Incident Response Consulting Practice

Determine log availability. In one ransomware incident in 2017, an organization noticed files had been encrypted on as many as 27 systems. A forensic investigation was launched to remediate the infections and identify the root cause. When the investigation started, it became clear that all affected systems were only configured to log for 2 hours, so all relevant logs relating to the malware infection had been overwritten.

Leverage the visibility you *do* have

Much of the malicious activity discovered during incident response engagements could have been prevented had alerts been identified and acted on in a timely manner. Here's an example of how much risk can remain undiscovered — even with good security tools — when people and process aren't working in concert with them: after discovering artifacts from an intrusion on a public-facing system, Secureworks carried out a targeted threat hunt and discovered a number of problems, including 41 compromised or threat actor-created user accounts, tools used to maintain access to the environment, reconnaissance tools, crypto-currency mining software, web application scanners, and other malicious tools. In many of these instances, antivirus or Windows security tools identified and logged the malicious tools but were not configured to block or quarantine them. As no person or process was reviewing the alerts, they went unnoticed for several months.

Organizations should ensure that threat detection logs are regularly monitored. This could be manually, through configuration (e.g., tools configured to send email alerts to an administrator) or through partnering with a Managed Security Services provider to monitor infrastructure for threats.

"If you have logs, make sure you are monitoring them... especially if you are thinking about investing in another technology that generates more logs."

Don Smith, Senior Director, Secureworks CTU Operations & Analysis

Preparation and Response

Eviction and Threat Re-entry: End the "Whack-a-Mole" Game

Breached organizations are naturally eager to remove attackers from their network as quickly as possible. However, hands-on experience informs a different approach. When highly-skilled adversaries have targeted a network, they'll typically have invested time and effort to maintain their access over a long period; therefore, it is unlikely that they will simply walk away once evicted. Instead, they will probably develop alternative routes for entry that may be difficult to spot in the first few hours and days of a response effort.

Failed eviction efforts can notify the attackers that they've been discovered and can make a thorough eviction more complex to carry out. That's why experienced incident responders take a long-term approach to understanding an adversary's behavior, capability, and intent over time before evicting a targeted threat. Let's examine a few case studies to see how adversaries try to maintain their access in the face of an eviction.

1. Expect more compromised credentials than meets the eye

In one example, Secureworks assisted an organization that had been compromised by an advanced China-based threat group, BRONZE RIVERSIDE (also known as APT10). Evidence of the threat actor's presence was identified on large number of systems because multiple remote user accounts were being abused. Initially, responders blocked domains, removed malware, and limited the number of password resets. Almost immediately, the adversary reverted to other user accounts that the impacted organization wasn't aware had been compromised (see Figure 16).

Without a full understanding of the adversary's access to compromised credentials in the network, initial attempts to evict are likely to fail. Secureworks incident responders typically advocate a period of enhanced instrumentation and monitoring to understand the adversary's methods, access, and likely response prior to any eviction of a targeted threat.

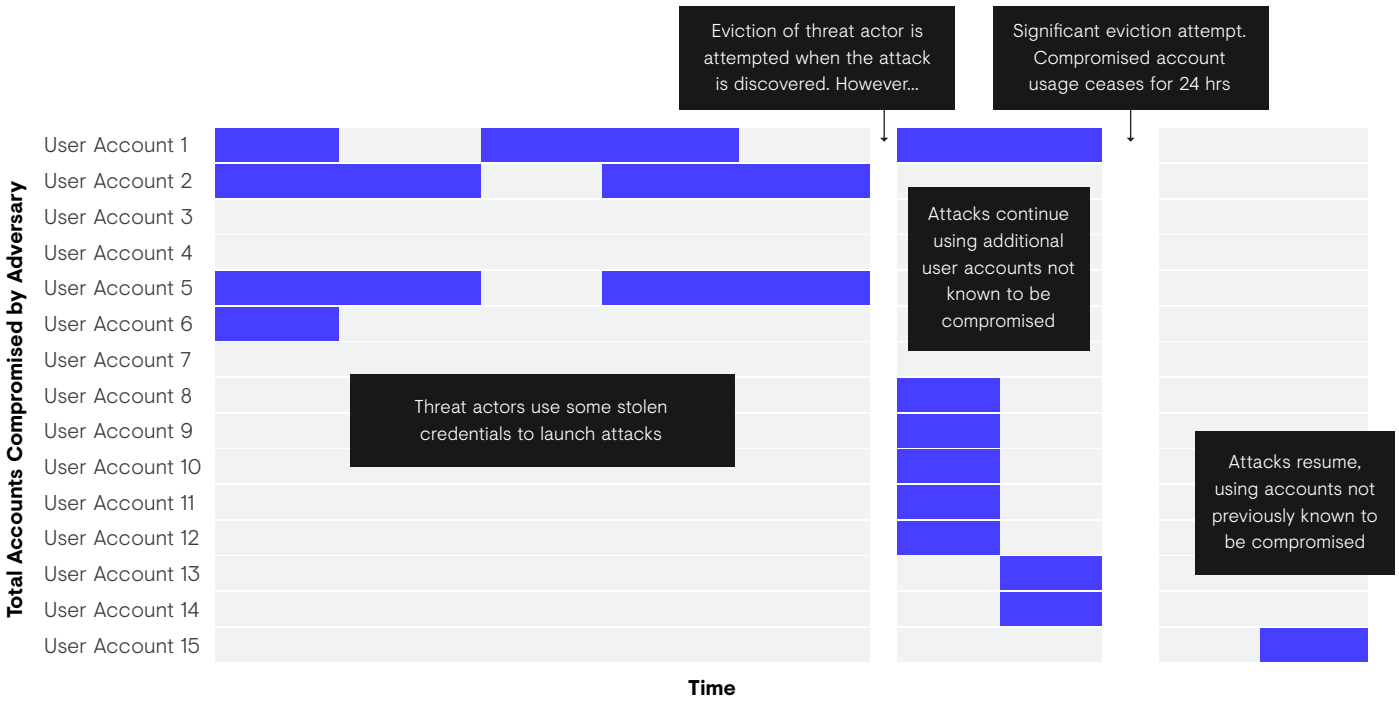


FIGURE 16: *Compromised account use by adversary over time. (Source: Secureworks)*

2. Assume that the adversary has contingency plans too!

Threat actors typically set up multiple back doors into compromised networks to ensure that casual discovery and remediation of one entry point does not jeopardize the threat actor's overall operation. In one case in 2017, the affected organization put effort and expense into rebuilding systems after they were compromised by an adversary using malware to access the network (see Figure 17). After a few weeks, the threat actor returned via a different route – a compromised legacy remote access system – and re-deployed malware in the network.

Examples like this underscore the need to first identify all access points, including remote access tools and webshells. Only then can you launch a single, coordinated effort to deny the adversary all access, while also investing resources wisely.

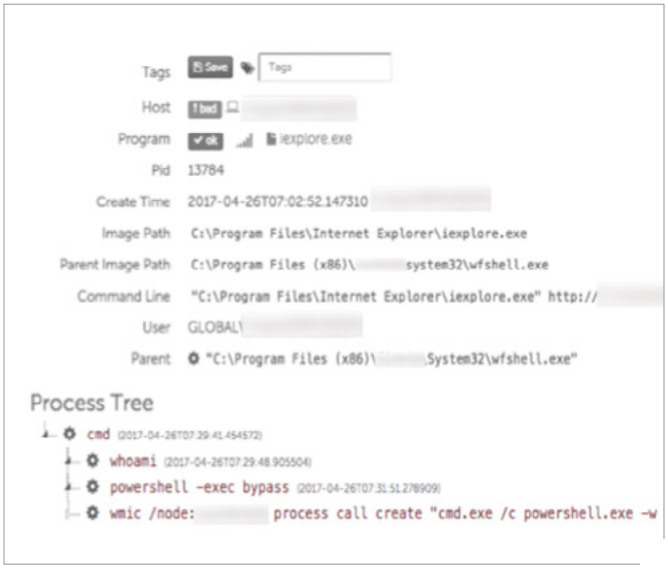


FIGURE 17: *Stolen credentials enable malware to be re-installed after eviction. [This adapted process tree shown in Secureworks AETD Red Cloak illustrates a Powershell command that was used to download malware onto a system after re-entry via compromised accounts for a remote access system]. (Source: Secureworks)*

3. Watching the watcher cuts both ways

The landscape of an incident response situation can change dramatically when the adversaries become aware that they're being evicted. During one incident last year, a threat actor attempted to re-enter the network with the same accounts and malware it had previously used. As soon as the adversary realized its method had been discovered and blocked, it changed its approach entirely and leveraged a compromised third-party network to connect to the victim's environment instead. In another case, an adversary switched to using a compromised website to temporarily stage tools that it could retrieve and use later in a re-entry attempt.

During this type of incident, Secureworks analysts advocate a range of measures (including establishing secure "out-of-band" communication channels) to limit the risks associated with an adversary gaining insight into response activities.

FIGURE 18: *Advanced Endpoint Threat Detection (AETD) Red Cloak alerts a client to webshell activity. (Source: Secureworks)*

4. Seek advice when the dust has settled

Once a determined threat actor has been evicted, response teams can provide network defenders with advice and support to improve their chances of being able to continuously mitigate and resist these threats in the future. One organization had experienced multiple compromises by several targeted threat groups during a three-year period. The recommendation was for the organization to increase its visibility of network and endpoint activity in an effort commensurate with the level of targeted threat the organization was facing. This approach enabled the organization to later detect and mitigate a multi-pronged re-entry attempt involving multiple spearphishing and webshell deployment attempts (see Figure 18).

Responding to high impact incidents can be stressful and time-consuming, especially when a determined and skilled adversary is involved. These four examples demonstrate why it's important to understand the extent of your adversary's access, intent, and capability before acting. They also illustrate the value of crafting scenario-based incident plans in advance.

"Understanding the adversary's intent before taking action is often the key to preventing re-entry. Red Cloak is a valuable component of a targeted threat hunting program because the intelligence driving it models actual threat actor behavior."

Barry R. Hensley, Senior Vice President and Chief Threat Intelligence Officer, Secureworks

Exercise Is Essential for Speed and Stamina

Technical actions are just a small part of the overall effort when organizations respond to a significant incident. Security leaders and executives alike will want to know: How and when are internal employees, the Board, regulators, customers and business partners informed? What is the legal view on the organization's liability? Who is responsible for maintaining critical business functions if the IT network suddenly becomes unavailable? Who briefs the press office, what position should the organization take in response to media inquiries, and which senior executives have received media training to conduct press briefings? These are questions to consider before a crisis hits.

Cybersecurity incidents involve business risk and are not simply IT issues. Given the potential impact on business availability, revenue, and reputation, it's crucial that stakeholders from across the organization come together and work as effectively as possible. Cybersecurity incident response is therefore as much a proactive business function as a reactive one. Yet, in the Secureworks 2018 Security Leaders Survey, 71% of respondents say the focus of their company's incident response capabilities fall into a reactive category – either "responding to threats as they happen" or "meeting compliance mandates" (see Figure 19).

71% of respondents say the focus of their company's incident response capabilities fall into a reactive category.

The development of processes and procedures in advance can ensure that the people involved in an incident understand their own roles and those of their colleagues especially when working across disparate business functions. One way organizations can strengthen that collaboration is with is a tabletop exercise.

Tabletop exercises are discussion sessions that put an organization's incident response planning and process through its paces. The discussions bring together technical and business leaders to evaluate incident management, recovery, and business continuity in the face of different cybersecurity-events. The goal is to test established plans, enhance the ability to respond to unanticipated events, and – most importantly – to ensure everyone is on the same wavelength during the response.

Focus of Incident Response Capabilities at Respondent Companies

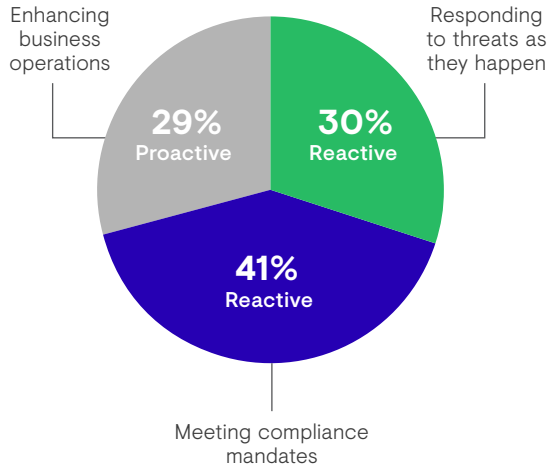


FIGURE 19: *Source: Secureworks 2018 Security Leaders Survey*

Anatomy of a tabletop exercise

Secureworks typically presents a client's incident management team with a scenario designed to test both technical and business processes. The life-like incident may involve, for example, a customer database with international privacy issues, foreign contractors, and complex regulatory frameworks. The team addresses technical, legal, and business challenges along the path to remediation as the incident unfolds.

Team members — from the C-level executives and HR, to marketing and technical staff — typically engage in fierce discussions with a range of excellent suggestions as they mull over the potential consequences of their actions in a highly-charged but safe environment. Secureworks encourages a regimen of exercises to give a large number of stakeholders across the organization an opportunity to hone their familiarity with incident response processes and build relationships with other stakeholders in advance of an incident. By incorporating "lessons learned" workshops throughout the lifecycle of an exercise regimen, observations are captured and follow-on actions are defined and assigned for action.

Customization of scenarios can include the utilization of "functional" exercise injects (providing emulated technical artifacts for analysis); escalation events to ensure top leadership gets involved; and the expansion to a Full Spectrum Incident Response Exercise that utilizes Secureworks' Red Team tactics to carry out real-time emulated adversary actions in the client environment.

Once the exercise is complete, a detailed report should highlight key findings, along with any readiness gaps and recommendations to improve security posture. The highest performing organizations tend to host full-team tabletop exercises at least once a year. Smaller groups looking to work on specific processes and procedures should aim to practice at least quarterly. As skill sets grow, some businesses have integrated exercising as part of a larger crisis management exercise program in their organization. Ultimately, some form of tabletop exercise is an essential step in getting an organization to the next level of cybersecurity maturity and crisis management preparedness.

While an encouraging 56% of respondents say they now involve business leaders in incident response exercises, the remaining 44% are only including the security team or don't conduct exercises at all. This leaves a gap between the IT response and the business response, increasing the risk of miscommunication, negative media, lack of confidence, and more.

(Source: Secureworks Security Leaders Survey 2018)

Hallmarks of A Mature Incident Response Program

Understanding the situation quickly can be the difference between success and failure during an incident. Preparing and exercising incident response plans; knowing your threat landscape intimately; being able to prioritize the alerts that matter; having access to the right time-sensitive artifacts such as logs; and having the patience and visibility to assess threat actor behavior, capability and intent before taking action: these are all hallmarks of an organization that has matured its incident response and overall cybersecurity posture.

Failing to prepare is preparing to fail. However building blueprints for various scenarios, defining roles for key stakeholders, and setting clear recovery objectives will not only create a framework for swift and efficient response, but will also ensure that best practices are integrated as the organization builds response maturity. Part of that maturity involves the ability to retrieve time-sensitive response evidence (including creating forensic disk images, collecting RAM, and protecting collected data in transit).

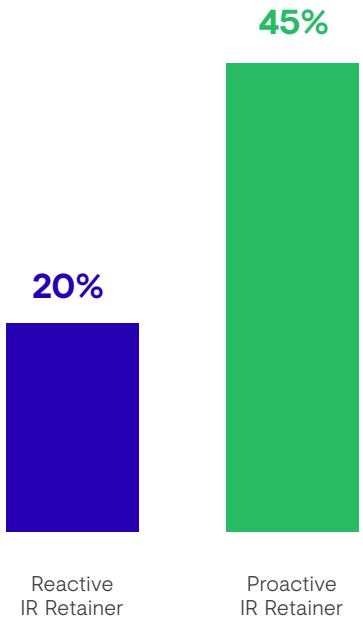


FIGURE 20: *Types of IR retainers in place at respondents' organizations. (Source: Secureworks 2018 Security Leaders Survey)*

Skills availability is key. In-house capabilities vary, so availability of skills should be reviewed regularly. Training can help increase in-house responder skills, and incident management retainers from vendors can provide necessary forensics and overflow response capacity in the event of significant incidents.

When Secureworks surveyed security and IT executives in 2018, only 20% of respondents had retainers in place for reactive incident response versus 45% of respondents with retainers in place for proactive services (see Figure 20). The commitment to proactive services is commendable, but no company is immune to a breach. All organizations should have access to both proactive and emergency capabilities.

Although regulatory requirements for incident planning and preparation are an important tool for ensuring sector resilience, Secureworks encourages organizations to move past the check-the-box approach when adopting proactive services. The best results are achieved when organizations incorporate these initiatives as part of a comprehensive program of capability development.

In 2017, more than a third of Secureworks' proactive response activity involved either developing or reviewing a network defender's Cybersecurity Incident Response Plans (CIRP)

Scanning the Horizon: What to Expect in 2018

Danish physicist Nils Bohr famously said: *"Prediction is very difficult, especially if it's about the future."* Relevant visibility, experience, and analysis, however, can be leveraged to identify meaningful trends in threat behavior and defensive readiness. Based on insights about the threats that are creating the biggest problems for organizations and also the lessons that businesses are learning from these incidents. Secureworks predicts four key threat trends for the near future:

"Living off the land" will continue to provide the most useful tools to adversaries.

Living off the land (or adversaries using tools that are already present on the network to carry out their actions) remains the approach of choice for most targeted attackers once access to a network has been gained. By using tools already on targeted systems, attackers avoid the risk of importing their own tools and minimize the chances of detection. Organizations that are successfully tackling targeted threats in their environments are the ones that can spot and act on anomalous use of native functionalities – such as WMI, Powershell, and Psexec – and consistently detect attackers using legitimate remote services.

All targeted network compromises we observed in 2017 involved living off the land to some degree, and Secureworks has no reason to believe this will change as we progress into 2018. Think of it from the adversary's point of view: *why go through the risk of bringing malware and intrusion tools onto a network when you can use stolen credentials and legitimate native functionality to access the network, move laterally, discover systems or data of interest, and prepare files for exfiltration?*

Publicly available tools will be increasingly leveraged in targeted attacks.

It's a misconception that highly capable criminal and nation-state adversaries always use the scariest new tools and that organizations need to buy the shiniest new detection tool in response. Rather than invest time and resources into developing malware and infrastructure, some advanced threat groups are increasingly gravitating towards freely available tools and services to conduct their operations. Entire intrusions are being conducted using freely available webshells (e.g., C99, and AspxSpy), remote access tools (e.g., NanoCore and NetWire), and online services (e.g., popular code sharing sites being used for C2 and file sharing sites used for malware delivery). For an adversary, it's a no-brainer: *why go to the effort of developing a capability when it's freely available online, especially when it makes our operations more difficult to track and attribute.*

"We're seeing more and more examples of advanced threat actors opting to use public or freely available tools and services across their intrusions. It makes their operations easier to get off the ground and can make their methods more difficult to track and attribute."

Don Smith, Senior Director, Secureworks CTU Operations & Analysis

The adversary's "speed to exploitation" will continue to put pressure on security teams when vulnerabilities are published.

2017 was littered with examples in which security researchers and hardware and software developers disclosed major vulnerabilities, only to see them subsequently weaponized by a variety of adversaries such as SMB v1 (CVE-2017-0143) and Apache Struts Vulnerability (CVE-2017-5638). Unfortunately there's no sign of change in 2018. When vulnerabilities are announced, the race is on to evaluate exposure, test, and deploy before adversaries start to exploit those vulnerabilities at high volume, or with great impact, or both. High-impact intrusions featuring threat actors who took advantage of vulnerable systems months after public disclosure were relatively common in 2017.

Security fundamentals will remain important and too often overlooked.

Dealing with the fundamentals of network security will continue to be just as important in 2018 as it was in 2017. Secureworks has the highest confidence in that prediction, because we say it every year. Most significant network compromises have involved threat actors taking advantage of basic gaps in security to some degree, be it unchecked user privileges, lack of network segregation, or insufficient perimeter controls. The truth is that we rarely see organizations walking away after incident response thinking "if only we had that fancy piece of technology." Security technologies are essential, but they're only effective when complemented by good security hygiene.

Conclusion

The laundry list of security breaches in 2017 confirms that organizations have good reason to improve their incident response rigor in two forms: proactive planning for better resilience, and adequate capabilities for responding to threats effectively when an incident is underway. Secureworks' extensive real-world experience reveals that success is largely tied to three important factors:

- A rededication to fundamental security practices
- Increased visibility into the organization and its vulnerabilities
- A sophisticated and proactive approach to planning, testing, and exercises designed to heighten both awareness and response skills around security threats.

By its nature, the lens of incident response provides a pessimistic view of the security world, so it is important not to lose sight of the positive steps that many organizations are taking to minimize risk to their data and networks. Organizations that make a conscious effort to improve incident response planning, preparation, hunting, and skills availability will be better prepared to prevent, detect, and respond to the complex array of threats that continue to challenge organizations across the globe in 2018.

About Secureworks

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world. We combine visibility from thousands of clients, aggregate and analyze 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.™

Corporate Headquarters

1 Concourse Pkwy NE #500
Atlanta, GA 30328
1.877.838.7947
secureworks.com

Asia Pacific

AUSTRALIA
Building 3, 14 Aquatic Drive
Frenchs Forest, Sydney NSW
Australia 2086
1800 737 817
secureworks.com.au

JAPAN
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
81-(44)556-4300
secureworks.jp

Incident Response Hotline

USA AND CANADA TOLL-FREE:
+1 877-884-1110

INTERNATIONAL:
+1 770-870-6343

irservices@secureworks.com

Europe & Middle East

FRANCE
8 avenue du Stade de France
93218 Saint Denis Cedex
+33 1 80 60 20 00
secureworks.fr

GERMANY
Main Airport Center,
Unterschweinstiege 10
60549 Frankfurt am Main
069/9792-0
secureworks.de

NETHERLANDS
Transformatorweg 38-72, 1014
AK Amsterdam,
+31 20 674 5500

UNITED KINGDOM
UK House, 180 Oxford St
London W1D 1NN
+44(0)203 907 6280
secureworks.co.uk

1 Tanfield
Canonmills
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040
secureworks.co.uk

UNITED ARAB EMIRATES
Building 15, Dubai Internet City
Dubai, UAE PO Box 500111
00971 4 420 7000