Secureworks®

2019

Incident Response Insights Report

A Case for Mastering Security Fundamentals

Contents

03 Executive Summary and Key Findings

05 About the Report

06 Trends Viewed Through the Lens of Incident Response
"Why would they want to target OUR network?"

17 Post-compromise Native Tool Use in 2018
"It's probably nothing... our sysadmins use those tools."

19 The Case for Improving Visibility
"That server was decommissioned months ago."

22 Third-party Risks Realized
"It came from the national CSIRT, but we didn't know whether to trust them."

24 Business Change and Risk Implications
"We've had a lot of change in our environment over the last few years."

27 Key Recommendations

29 Conclusion

© 2019 SecureWorks, Inc. All rights reserved.

Secureworks®

Executive Summary

Each year, Secureworks® analysts create this report to bring together their findings from over a thousand incident response engagements throughout the year. The lens of incident response provides a unique window into the sharp end of information security. This visibility helps to identify how organizations could improve their ability to prevent, detect, and respond to the threats they face, and helps to track significant changes in attack methods.

What Can Organizations Do Better?

When compiling findings from 2018 incident response data, Secureworks analysts were struck by a sense of déjà vu when evaluating what organizations could have done better. Year after year, the same issues and security gaps are blighting organizations' ability to identify and respond to threats:

- Gaps in basic security controls and organizations' visibility of their own environments continue to allow threat actors to gain access and entrench themselves.
- Security implications of adopting new technologies or major changes to networks are not consistently addressed, creating longer-term problems for many organizations.
- Suppliers and third parties can be compromised if they provide an easier path to the ultimate target than a direct attack, and organizations continue to struggle to find the balance between trust and oversight over third-party access.

Aren't New Threats Leading to New Recommendations?

The incidents observed by Secureworks analysts in 2018 revealed a year of evolution rather than revolution in attack methods. In previous years, government-sponsored, criminal, and hacktivist groups each had a distinct way of operating. For example, government-sponsored actors often invested time and resources into developing their own malware to use in highly targeted attacks, whereas financially motivated criminals used indiscriminate and broader-scale tactics. These groups' methods rarely overlapped.

In 2018, those same groups often used overlapping tactics, such as leveraging unauthorized access to systems within a network to carry out attacks, implementing "living off the land" techniques, and making extensive use of publicly available malware, services, and exploits. Their philosophy appears to be "why waste time and money building new tools and methods when existing tools continue to work?"

Secureworks analysts identified the following highlights from incident response engagements in 2018:

Business email fraud, ransomware, digital currency mining (also known as cryptomining), and banking trojan activities constituted over 60% of the total attack methods.

Ransomware attacks tended to be more serious in impact than in previous years, with threat actors increasingly trying to gain access to entire networks to deploy payloads across a large number of systems.

Government-sponsored actors continued to target organizations for various strategic objectives, but capability across groups continues to diverge. Many groups conduct entire intrusions using publicly available tools and techniques, whereas others adopt increasingly sophisticated approaches to gain access to systems.

Putting highly sophisticated threats aside, the general homogenization of the threat landscape is an indication that the threat actors are collectively maturing toward behaviors that take advantage of the systemic defensive gaps organizations leave open year after year. These are the behaviors that offer threat actors the best chances of success.

How Should Organizations Address These Security Gaps?

This report describes how organizations were compromised and impacted in 2018, as well as tactical lessons that victims learned to improve how they can prevent, detect, and respond to these threats. Too often, the implementation of fundamental security principles and processes ends up being the difference between a run-of-the-mill detection and resolution versus a more impactful and costly incident. Organizations should refocus on those all-important security basics and consider how their own security controls, visibility, and response processes would stack up in these real-world incident scenarios.

© 2019 SecureWorks, Inc. All rights reserved.

About the Report

In 2018, Secureworks conducted more than a thousand incident response engagements that totaled more than 40,000 professional incident response hours. More than 120 terabytes of investigative data were collected. Secureworks analyzes this data to help organizations plan for, detect, respond to, and recover from cybersecurity incidents.

The engagements analyzed for this report included accredited emergency and proactive services across the full range of industry sectors and around the globe. Emergency services involved live response to ongoing situations. They ranged from analyzing malicious files and doing forensic analysis of a single system, to comprehensive and coordinated evictions of advanced threats that had been lurking within large networks for years.

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

The Secureworks Incident Response Insights Report 2019 examines how threat actors exploited those gaps in real-life situations and provides takeaway lessons for improvement.

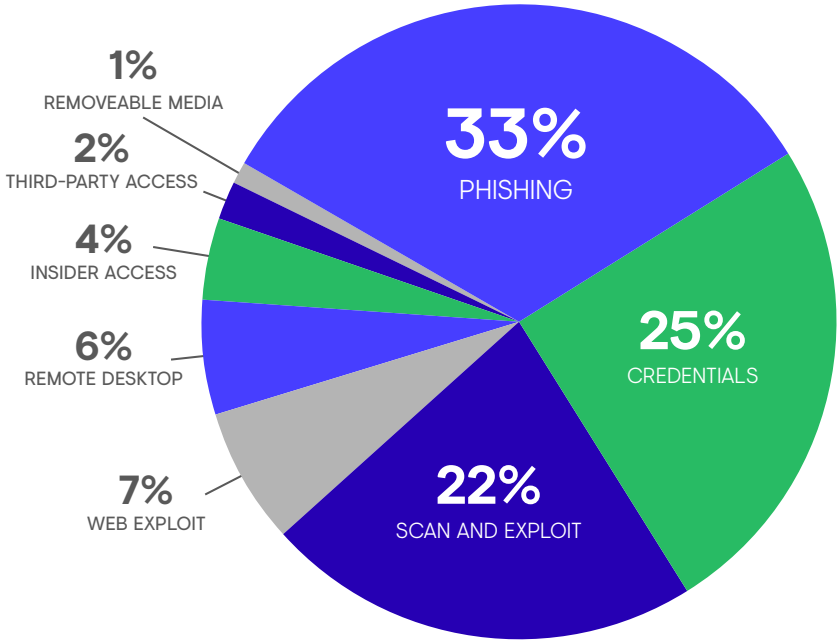


FIGURE 1: *Initial access vectors for intrusions in 2018 suggest that people and process rigor is just as important to cybersecurity posture as technology rigor. (Source: Secureworks)*

© 2019 SecureWorks, Inc. All rights reserved.

Trends Viewed Through the Lens of Incident Response

"Why would they want to target OUR network?"

At the beginning of an incident response engagement, Secureworks analysts often encounter baffled organizations seeking to understand what has happened to them and sometimes asking "why would someone want to target OUR network?" The answer to that question depends on what assets they have. Every organization has something of value to threat actors, such as money, intellectual property, computing resources, and personally identifiable information (PII). Financially motived criminals try to make money however they can: using systems to mine cryptocurrency they can sell, encrypting files and demanding ransom, gaining access to bank accounts to steal money, or stealing personal or credit card data that they can sell. Some government-sponsored actors seek sensitive intellectual property to bolster their own economy; others may want to disrupt or destroy organizations for political purposes.

Continuing the trend from previous years, financially motivated attacks dominated the activity observed during 2018 incident response engagements. Business email fraud, ransomware, digital currency mining (also known as cryptomining), and banking trojan activities represented more than 70% of the Secureworks incident engagements performed in 2018.

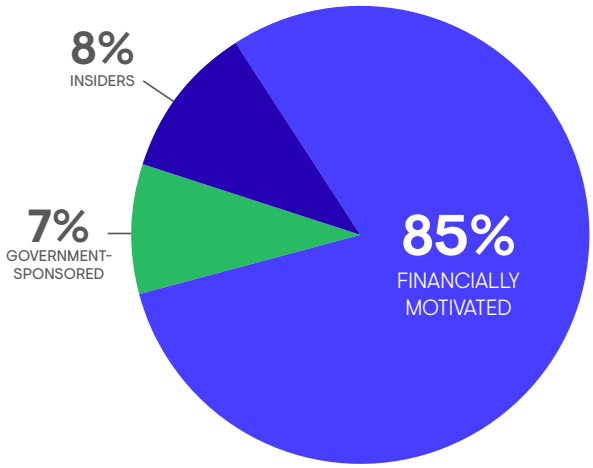


FIGURE 2. *Threat categories 2018. (Source: Secureworks)*

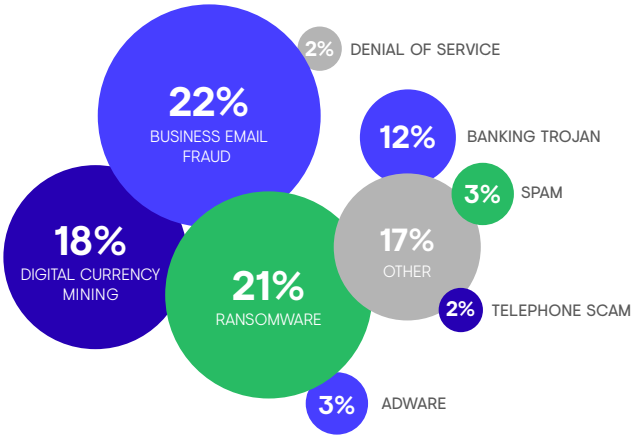


FIGURE 3. *Financially motivated criminals observed during incident response engagements in 2018. (Source: Secureworks)*

© 2019 SecureWorks, Inc. All rights reserved.

Business Email Fraud

Business email fraud encompasses business email compromise (BEC) and business email spoofing (BES). These incidents are a growing part of financially motivated attacks and tend to have two victims. One victim is the owner of an email account that is compromised, perhaps by stealing their password and using the credentials to access Outlook on Office 365. Their mailbox is monitored for opportunities to persuade a colleague to transfer money to the threat actor's bank account. This colleague, who may be in the same organization or may be in a role such as customer or supplier, becomes the second victim.

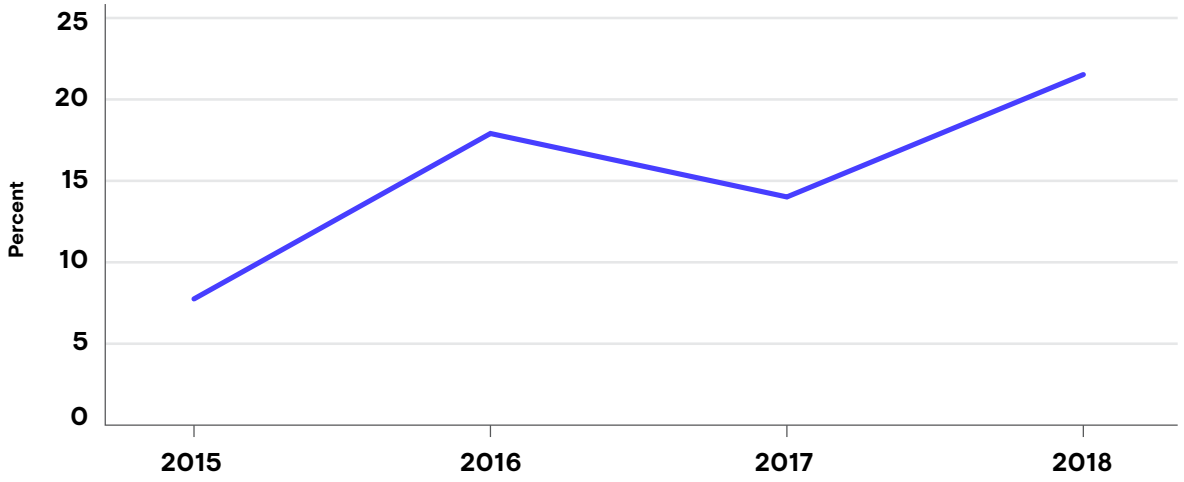


FIGURE 4: *Business email fraud as a % of total financially-motivated incidents 2015-2018. (Source: Secureworks)*

Business email fraud campaigns tend to leverage publicly available tools or native functionality such as mail forwarding rules, and execution does not require sophisticated technical capabilities. Secureworks analysts have observed these threat actors adapting their activities to improve their success rate. In one case, the threat actors monitored emails containing travel itineraries and timed their fraud activity while one of the victims was on a flight. This behavior ensured that the second victim in communication with the threat actor could not verify whether the request was legitimate. As a result, the threat actors successfully stole more than $1 million USD.

© 2019 SecureWorks, Inc. All rights reserved.

INCIDENT ANALYSIS

Business Email Fraud Targets Executives

Routine business email fraud typically involves the compromise of an email account owned by a small to medium-sized business and the theft of a few thousand dollars. In 2018, Secureworks analysts observed evidence of threat actors increasingly targeting large transactions, including two instances involving seven-figure sums.

In one of these incidents, email credentials were stolen after several users followed a link in a voicemail-themed phishing email. The following day email accounts of multiple executives were accessed by criminal threat actors, and used to conduct a fraud attempt. Specifically, an email from the CEO to a business unit's chief financial officer (CFO) requested approval and quick processing of an attached invoice for approximately $1 million USD to "avoid overdue taxes." The CFO then forwarded the email to two employees to process the wire transfer and respond with confirmation that the payment had been made (see **FIGURE 5**).

Discovery

User vigilance led to suspicion of the request and the organization's rapid response prevented the transfer of illicit funds.

Lessons Learned

Because business email fraud leverages legitimate corporate services (e.g., remote email accounts) and social engineering, traditional security and detection tools have limited ability to detect these threats. Implementing multi-factor authentication (MFA) on Internet-facing webmail accounts, developing response procedures for business email fraud incidents, and identifying alternate communication channels if corporate email is compromised can help organizations prevent and effectively respond to this type of activity. Training users to identify suspicious changes or behaviors during a transaction and having a clear process for reporting possible incidents are useful approaches to mitigating these risks.

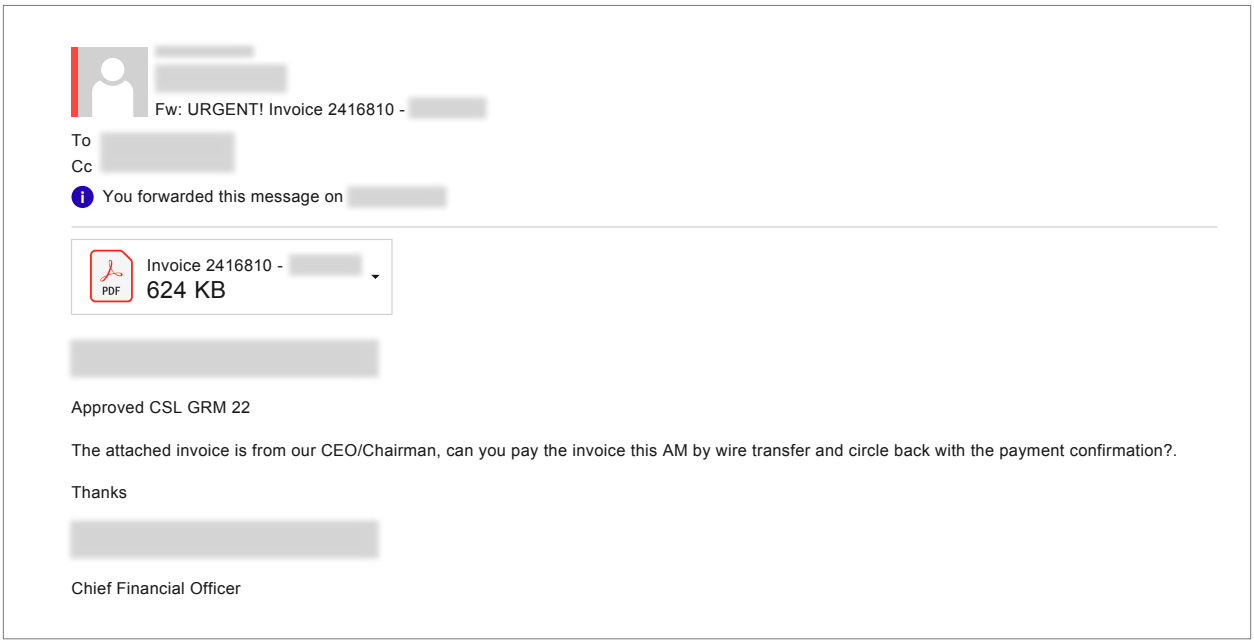


FIGURE 5: *Email requesting processing of fraudulent request. (Source: Secureworks)*

© 2019 SecureWorks, Inc. All rights reserved.

Ransomware

Although Secureworks analysts responded to fewer ransomware engagements than in previous years, the incidents observed in 2018 tended to be more serious as they increasingly leveraged post-intrusion methods to deliver ransomware from within the network after some form of network compromise. Often, this approach involves the threat actor deploying semi-automated scripts to disable security controls and then deploying the ransomware payloads. This approach is significantly more effective than other approaches, with the average number of impacted hosts per incident increasing from 1.8 to 114.3 when post-intrusion methods were used (see **FIGURE 6**).

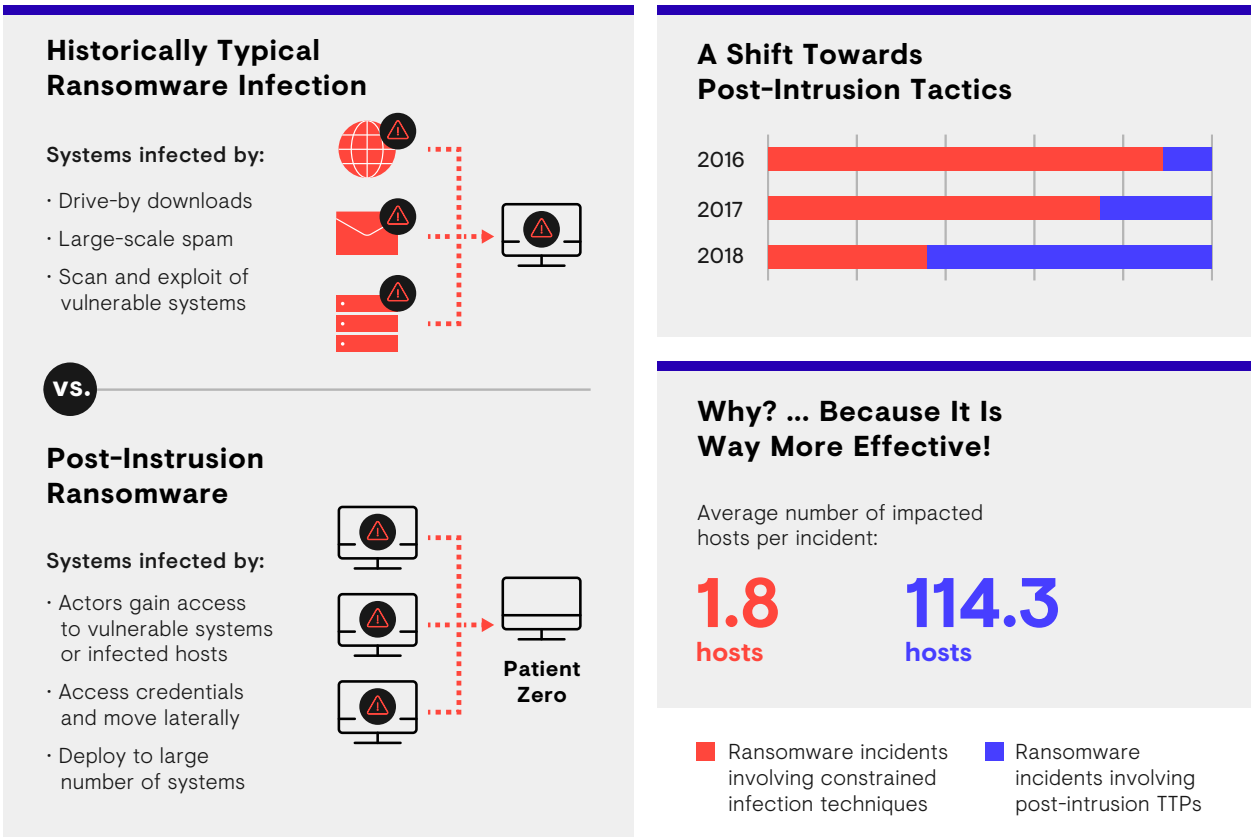


FIGURE 6: *A snapshot of the ransomware threat landscape shift from 2016 to 2018. (Source: Secureworks)*

© 2019 SecureWorks, Inc. All rights reserved.

This approach to ransomware deployment was typified with network breaches involving SamsamCrypt ransomware and incidents involving BitPaymer and Ryuk, in which the ransomware deployments took a significant disruptive toll. This trend has shown no sign of abating in 2019, with Ryuk and LockerGoga ransomware severely impacting manufacturing and engineering organizations.

Secureworks analysts also observed an evolution of the ransomware model. Engagements in 2018 involved fewer new ransomware types compared to prior years, but existing families like GandCrab were available to threat actors as ransomware-as-a-service.

!

Emotet and TrickBot should no longer be considered just indiscriminate threats, and any evidence of these infections should trigger full incident response procedures to assess the scale of the threat within the environment. In addition, organizations should not underestimate the value of maintaining backups that are stored in a manner that minimizes the risk of being encrypted.

INCIDENT ANALYSIS

Ryuk Runs Rampant

In late 2018, Secureworks analysts assisted several organizations with widespread and highly damaging Ryuk incidents. In the majority of these incidents, TrickBot malware was installed using a prior Emotet infection. TrickBot quickly spread throughout the network environment by leveraging system administration accounts that used the same credentials.

In one incident, the threat actor was able to use TrickBot's VNC module across the network as an ingress point. The threat actor then used Remote Desktop Protocol (RDP) to connect to the domain controller and distribute Ryuk ransomware across the corporate network (see **FIGURE 7**).

Discovery

Network defenders discovered the widespread TrickBot infection. While the organization was in the process of remediating these infections, the threat actors started to distribute Ryuk. This post-intrusion ransomware caused a vast proportion of the organization's network to become encrypted and rendered unusable.

Lessons Learned

The use of tools such as Emotet and TrickBot to conduct a penetrative network intrusion and subsequently distribute ransomware should prompt organizations to rethink their assumptions about the severity of these types of infection.

© 2019 SecureWorks, Inc. All rights reserved.

Ryuk Ransomare Deployed After TrickBot Compromise in 2018

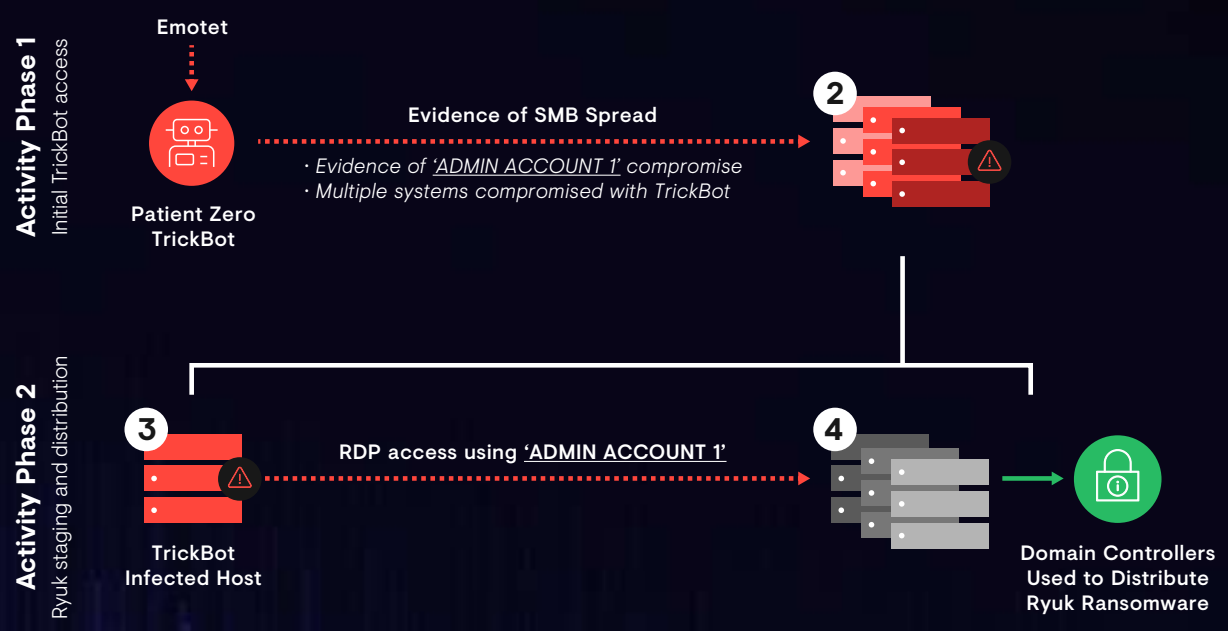


FIGURE 7: *(Source: Secureworks)*

Digital Currency Mining

Despite cryptocurrency values dropping significantly from heights reached in December 2017, malicious digital currency mining activity outpaced banking trojans in terms of volume of incidents that Secureworks responded to in 2018. Secureworks analysts cross-referenced their 2018 incident response findings with visibility across thousands of client environments around the world and found that cryptocurrency mining impacted more than a third of all Secureworks clients in the last 18 months.

INCIDENT ANALYSIS

Cryptocurrency Mining on the Side

Cryptocurrency mining-related infections are not exclusive to financially motivated threat actors. During a targeted intrusion, Secureworks analysts identified that the threat actor had used persistent access facilitated by Meterpreter installations to run cryptocurrency miners on a large number of compromised hosts. Access that was primarily used for espionage objectives can easily be used to deploy tools like a cryptocurrency miner. The goal could be to generate revenue, financially support malware campaigns, or act as a decoy to distract responders from other espionage activities.

Host	✓ok
Process	(not available)
Query Time	2018 -
Query Type	A
Query Name	xmr.pool.minergate.com
RDATA	136.243.88.145 Netflows with this address

FIGURE 8. *DNS lookup for a cryptocurrency mining pool. (Source: Secureworks)*

Discovery

The DNS record in Figure 8 for a cryptocurrency mining pool was identified on systems previously used for espionage. It was detected by Secureworks' Advanced Endpoint Threat Detection service.

Lessons Learned

The lines between threat categories can be blurred. Having sufficient visibility and situational awareness of the environment is crucial when evaluating whether threat behaviors are linked. If there is any indication that multiple strands of threat activity may be linked, it is important that organizations take the time to understand the threat they are facing rather than embarking on a game of whack-a-mole.

!

While the immediate impact of most cryptocurrency mining compromises is more limited than other threats, organizations should take the time to investigate and understand how the cryptocurrency miners ended up on a system. Their presence may be due to unauthorized network access and could be indicative of a more serious intrusion or gap in security controls.

© 2019 SecureWorks, Inc. All rights reserved.

Banking Trojans

Though Secureworks analysts responded to fewer incidents involving banking trojans in 2018 compared to previous years, these incidents remained a consistent presence. Banking trojans such as Emotet and TrickBot continued to represent a notable proportion of financially motivated attacks in 2018. The malware families continue to evolve significantly to increase their capability and change the nature of the threat.

Emotet, for example, added several new modules. One module is a spreader that uses a list of the most common passwords to guess credentials and spread the malware throughout the network, and another gathers and exfiltrates Outlook mailbox files. These kinds of changes can elevate an Emotet incident from a low-risk single-machine banking trojan infection to a network-wide compromise of a business's sensitive information. It is no longer sufficient to just quarantine an Emotet infection and move on.

In 2018, tools that have historically been synonymous with banking credential theft were increasingly leveraged to enable network access for alternative motives. As a consequence, the terms 'banking trojan' and 'commodity threats' potentially disguise the severity of threat posed by these infections. Any evidence of these malware types existing within an environment for a long period of time warrants a full and thorough investigation.

INCIDENT ANALYSIS

Banking Trojan Infection Enables Theft of $50,000 From Employee

Emotet was one of the most prolific malware families impacting Secureworks clients in 2018. It is delivered via spam emails with lures such as unpaid invoices, missed parcels, and electronic greeting cards. During a 2018 incident, an employee at an organization lost approximately $50,000 USD in personal funds as a result of an Emotet infection in their employer's environment.

A lack of password-complexity and multi-factor authentication (MFA) within the organization enabled Emotet to spread to thousands of endpoints in the network using hard-coded passwords contained in Emotet's spreader module. When the victim accessed their personal online bank account on their work system, their credentials were stolen and subsequently used to defraud their personal bank account.

Discovery

This activity was discovered when the victim reported that funds had been siphoned from their personal bank account.

Lessons Learned

This example provides a strong case for network hygiene (i.e., rapid detection and remediation of commodity malware) and highlights how complex passwords could have limited the spread of infection. In this case, personal Internet activity on a corporate system was targeted. A clear policy that defines acceptable personal use of corporate systems is a foundation for managing these risks.

Rule	EmotetMutexAndEvent
Host	
Color	| bad
Label	Emotet Event
Detected	2018 -

FIGURE 9. *Example of an Emotet infection detected with Secureworks' Advanced Endpoint Threat Detection. (Source: Secureworks)*

© 2019 SecureWorks, Inc. All rights reserved.

Insider Threat

Insider threats accounted for 8% of the total incidents Secureworks analysts responded to in 2018. These incidents ranged from suspicions of data theft and irregularities during joiners, movers, leavers (JML) processes, to incidents with significant operational and reputational risks.

INCIDENT ANALYSIS

Who's Watching the Watchers?

During an insider threat incident in 2018, a domain administrator with elevated network privileges used their access to install a suite of unapproved tools. The administrator was able to remotely access systems using the NoMachine remote desktop tool (see **FIGURE 10**) and recover user credentials from the local system (Power Memory). The insider also accessed email and human resources accounts belonging to other employees.

As a result of the insider's actions, the affected organization suffered a serious system outage. Although there was significant evidence of malicious activity, some of the logs necessary to fully understand the extent of the damage were not available to Secureworks analysts.

FIGURE 10. *NoMachine remote desktop tool. (Source: NoMachine.com)*

Discovery

The organization discovered the activity when one of the unapproved files caused an outage of a business-critical system.

Lessons Learned

This incident highlighted the need to have appropriate checks and balances on activity involving privileged access, including activity logging, protection of logs against tampering, and third-party activity monitoring. For extremely sensitive configurations, organizations may want to consider the concept of the two-person rule.

© 2019 SecureWorks, Inc. All rights reserved.

Targeted Intrusions

Targeted activity from government-sponsored actors comprised 7% of incident response engagements in 2018. Secureworks analysts remediated targeted intrusions in a range of industries, including manufacturing, academic, political, business services, healthcare, heavy industry, utility, and legal organizations. Many targeted threat groups have increasingly adopted publicly available tools and techniques to carry out their intrusions. This approach requires fewer development resources and makes operations more difficult to attribute. Secureworks analysts regularly observed entire intrusions being carried out using publicly acquired web shells and remote access capabilities (e.g., Trochilus, QuasarRAT, PupyRAT, the TeamViewer desktop-sharing tool) from public sources for initial access.

INCIDENT ANALYSIS

Surgically Targeted Intrusions

In 2018, targeted threat actors continued to minimize activity in environments to reduce the chances of being detected. In one incident, Secureworks analysts determined that despite having access to a network for over a week, the threat actors accessed only two hosts to conduct what appeared to be highly targeted data exfiltration. The behaviors were common to most targeted attacks: initial access leveraged credentials that appeared to have been acquired in a previous incident; additional credentials were stolen and a web shell was installed for persistence; file listings were generated; and then a subset of files on those lists were stolen.

Discovery

The initial entry was detected by Secureworks' Advanced Endpoint Threat Detection service.

Lessons Learned

When threat actors operate slowly and carefully, detective controls to identify suspicious behaviors are critical. This detection is most easily done on the endpoint, but all critical servers and as many other systems as possible must be instrumented to look for this kind of activity. Perimeter controls still have value to detect entry into and exit from the environment, but threat actors are likely to be careful to blend in with normal network traffic.

!

While Secureworks analysts observed a significant proportion of targeted threat groups gravitating toward freely or publicly available malware, this doesn't tell the whole story. Some targeted threat groups are diligently focused on developing custom malware tools and adopting more sophisticated approaches to malware delivery.

© 2019 SecureWorks, Inc. All rights reserved.

INCIDENT ANALYSIS

Man-on-the-side (MotS) Technique Used to Deliver Remote Access Tool

During a targeted intrusion in 2018, a user requested an installer from what appeared to be a valid Adobe Flash download URL. However, the size of the data download was larger than the file that was saved to disk, suggesting that malicious content may have been served alongside the legitimate installer using the "man-on-the-side" (MotS) technique (see **FIGURE 11**). The trojanized installer seemed to have self-modified shortly after execution to remove all but minute traces of the malicious content, leaving only a legitimate Adobe Flash installer binary on disk. Analysis of the malicious content suggested a link to the likely Russia-based IRON LIBERTY threat group (also known as Energetic Bear or Dragonfly), which has targeted global energy, nuclear, and defense organizations since at least 2010.

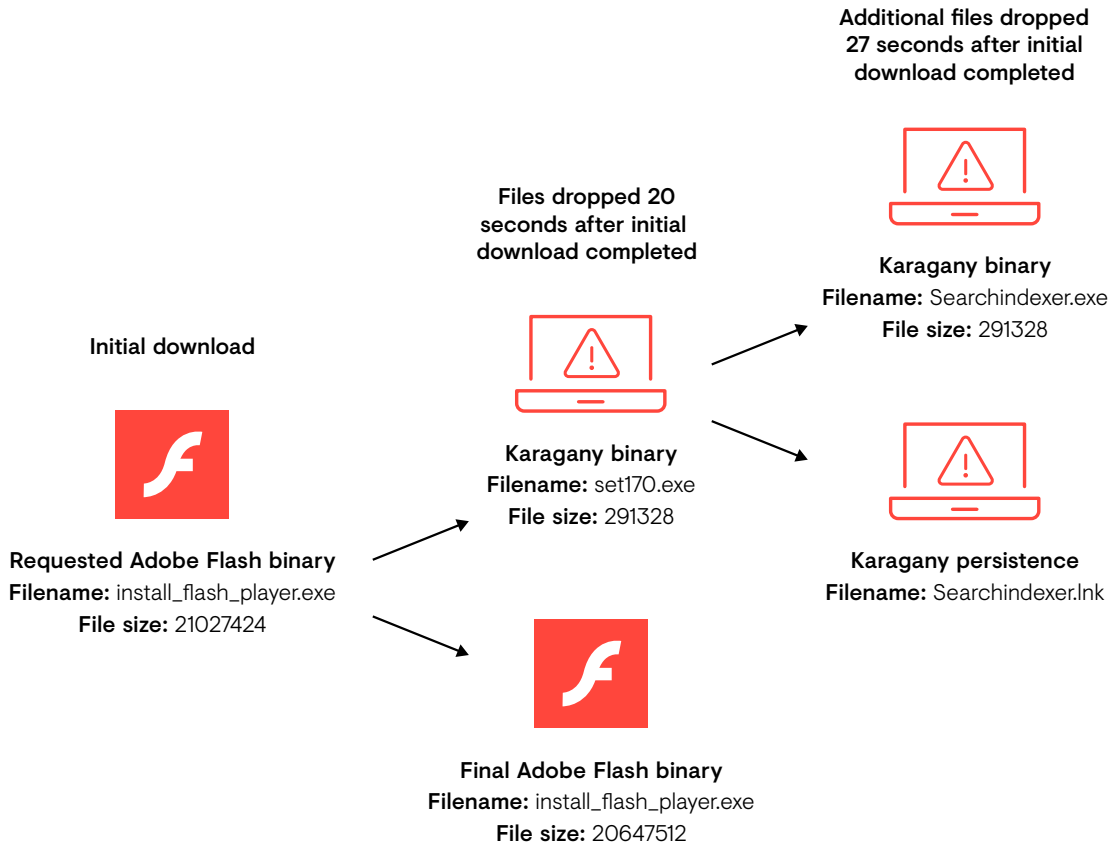


FIGURE 11: *Discrepancy between the requested and delivered Flash installers. (Source: Secureworks)*

© 2019 SecureWorks, Inc. All rights reserved.

Post-Compromise Native Tool Use in 2018

"It's probably nothing... our sysadmins use those tools."

Following many network compromises Secureworks analysts observed in 2018, the threat actors leveraged tools, services, and credentials native to the compromised environment to achieve their objectives. This activity is also known as "living off the land." Figure 12 lists the native Windows tools that Secureworks analysts observed targeted threat actors leveraging in 2018. The open-source LOLBAS repository also includes living off the land binaries (LOLBINS) and scripts (LOLScripts) that are typically used by threat actors.

arp	at	BITSAdmin	cacls / icacls	call
cd	chcp	CMD	cmdkey	copy
CSC	Csvde	del	dir	DSGet
DSQuery	find	findstr	hostname	ipconfig
klist	move	mstsc	nbtstat	net
Netsh	netstat	nltest	Notepad	nslookup
ping	PowerShell	query session	quser / query user	reg add
reg import	reg query	reg save	REGEDIT	route
Sc	schtasks	sqlcmd	start	systeminfo
taskkill	tasklist	time	TYPE	Vssadmin
whoami	winrs	winword	wmic	wevutil

FIGURE 12: *Native Windows tools and functionality observed in 2018, including Microsoft SQL and Windows Server tools. (Source: Secureworks)*

© 2019 SecureWorks, Inc. All rights reserved.

Much of the functionality from the most commonly observed tools applies to the following phases of an intrusion:

- discovery (e.g., net, ping, quser, whoami)
- defensive evasion (e.g., del, taskkill)
- lateral movement (e.g., net, schtasks)
- collection (e.g., findstr)

Activity associated with the 'net' tool represented nearly half of all native Windows tool use events during incidents observed in 2018. This command-line tool enables a threat actor to perform a range of network functions, including discovering system attributes (e.g., host, user, and group enumeration) and connecting to other networked devices. Figure 13 shows that 'net use' and 'net user' commands accounted for more than three-quarters of 'net' activity observed in 2018. Targeted threat actors typically used 'net use' command structures similar to the following to connect to other systems in a compromised environment:

```
net use \<internal IP address>
<password> </user:domain name\
username>
```

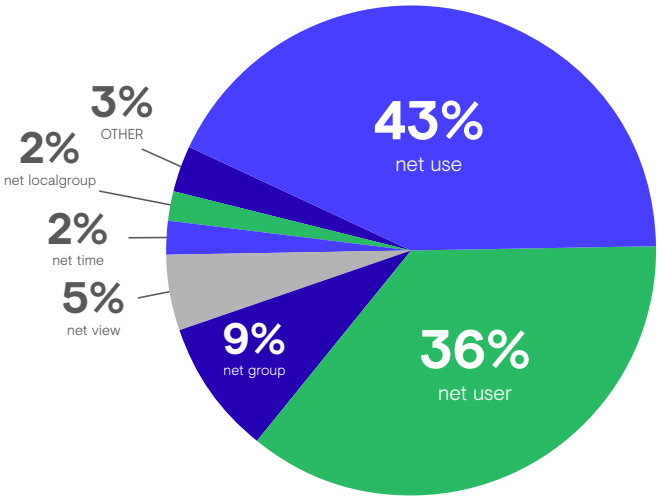


FIGURE 13: *Net commands used by targeted threat actors in 2018. (Source: Secureworks)*

Secureworks analysts recommend that organizations implement a risk-based approach that considers these living off the land methods alongside the organization's operational needs, assets, and vulnerabilities. Minimizing opportunities for threat actors to gain a foothold on systems is the first step to mitigating these risks. Secureworks analysts also recommend actively monitoring security controls to ensure proper functionality and managing user privileges to limit tool access to appropriate users, which should include implementing least privilege and separation of privileges.

Ultimately, identifying suspicious use of native and legitimate tools starts with visibility and understanding how they are typically used in an environment. From this position, organizations are better able to actively monitor for suspicious behavior linked to these tools.

© 2019 SecureWorks, Inc. All rights reserved.

The Case for Improving Visibility

"That server was decommissioned months ago."

Increased logging and increased endpoint visibility were the second and third-most frequent recommendations to organizations following incidents in 2018.

While organizations should be vigilant to the external threats they are most likely to encounter, visibility also includes the organization's view of its own environment. Organizations cannot build an effective information assurance program or determine appropriate security controls without understanding their environment. How can an organization protect assets it does not know about?

This process starts with keeping accurate inventories for hardware and authorized software in a configuration management database (CMDB). While complex platforms exist to manage this process, something as simple as an assets spreadsheet is a good start. User permissions should be limited where possible to prevent users from installing unauthorized software.

Incident response can also be severely disadvantaged when a victim organization's understanding of its network topography is out of step with reality. Secureworks analysts have supported incidents where threat actors have a better understanding of the environment than the network owners. For example, in 2018 Secureworks analysts observed the COBALT DEWEY targeted threat group (also known as APT35) extending its access within a compromised business services organization by leveraging a previously decommissioned domain controller. Secureworks analysts have encountered other examples of threat actors leveraging ingress points that network defenders believed to be disabled. When a threat actor can leverage systems or services that are assumed to be out of commission, network defenders and responders will be at a severe disadvantage.

Once an organization knows its systems and software, effective monitoring tools can help find anomalies. Secureworks' Advanced Endpoint Threat Detection provides visibility of user and system activity during an intrusion but also has rules to detect the presence of unwanted software such as adware or peer-to-peer applications. It also identifies connections between systems, which may identify systems that were previously undetected. When effective endpoint detection is first deployed in an organization's environment, it often creates large numbers of alerts for previously unknown unauthorized software on hosts. Responding to these alerts can be time-consuming and inconvenient, but it is an important way to minimize the attack surface of the organization's network environment.

Secureworks analysts consistently find that many organizations have insufficient network, endpoint, and log visibility, which limits the ability to detect threats they are facing. A lack of processes and appropriate technologies can hinder organizations' situational awareness of their own networks, risks, and security gaps. Organizations should continue to invest in maintaining and developing their understanding of their own networks and the threats they face to help successfully tackle complex information security challenges that inevitably arise during an incident. With an informed view of its assets, organizations can confidently maintain and update systems. By optimizing log completeness and log retention, organizations ensure that they have sufficient forensic readiness.

© 2019 SecureWorks, Inc. All rights reserved.

Logging supports the monitoring and auditing of security controls.

Secureworks analysts recommend that organizations log as much information as possible across their environment for completeness of visibility. Network defenders should adopt technologies and processes to analyze and filter logs so that a small number of high-priority events require manual review. It is also important that organizations consider the types of information being logged to ensure that data relevant to understanding the full extent of any security event is captured and accessible to incident responders.

When determining what logs to capture, organizations should understand why the information is significant and how it could be used in an investigation. For example, logging failed access attempts can reveal what actions did not work for the threat actor, but that data should be compared to successful attempts in order to establish normal behavior for a specific user.

Organizations should also use logging as a tool to validate and monitor their security controls. Additional considerations need to be made around where logs are stored and how long they are retained.

Targeted Threats Can Make Themselves At Home When Visibility is Lacking

Secureworks analysts were able to determine the dwell time, which is the time between threat actor entry and detection, for a subset of incidents in 2018. On average, opportunistic threat actors resided in an environment for 73 days, compared to 221 days for targeted threat actors. Although these numbers are slightly lower than prior years, the metric indicates that significant gaps in detection capability still exist in many organizations.

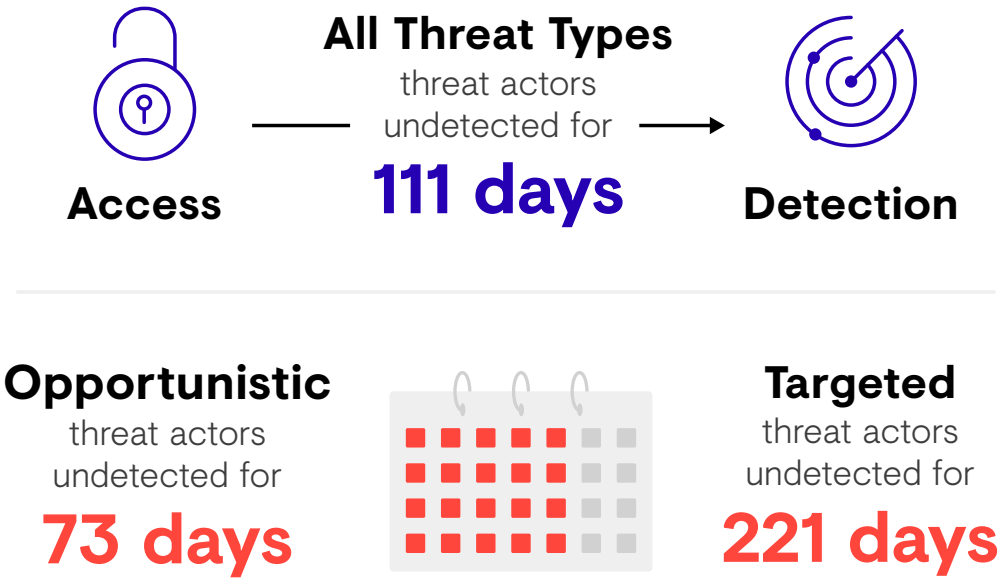


FIGURE 14. *Average Dwell Time for Threats in 2018. (Source: Secureworks)*

© 2019 SecureWorks, Inc. All rights reserved.

Third-Party Risks Realized

"It came from the national CSIRT, but we didn't know whether to trust them."

Managing third-party risks can be a challenge. Part of mitigating these risks depends on the level of trust placed in the security arrangements of organizations in the supply chain. Some suppliers have robust tools and processes to secure both their own and customers' interests, but others may operate differently when it comes to security.

As an illustration, in 2018 Secureworks analysts supported a small manufacturer that is part of the supply chain for several larger critical national infrastructure organizations. The manufacturer received a notification from a national computer security incident response team (CSIRT) about a potential compromise but took no action because it did not recognize the significance of the notification. Eventually, Secureworks analysts were engaged to investigate the reported intrusion and concluded that the threat actor targeted the manufacturer to gain access to information about its customers and possibly to target customers using compromised email accounts.

One of the primary functions of many national CSIRTs and law enforcement agencies is to contact organizations that have been identified as possible victims of a network intrusion. Organizations that do not regularly deal with national agencies could view infrequent notifications as unfamiliar or suspicious, especially if there is limited context. Organizations should validate the credentials of anyone providing these notifications as a matter of course, but legitimate government notifications are typically credible and merit a thorough investigation.

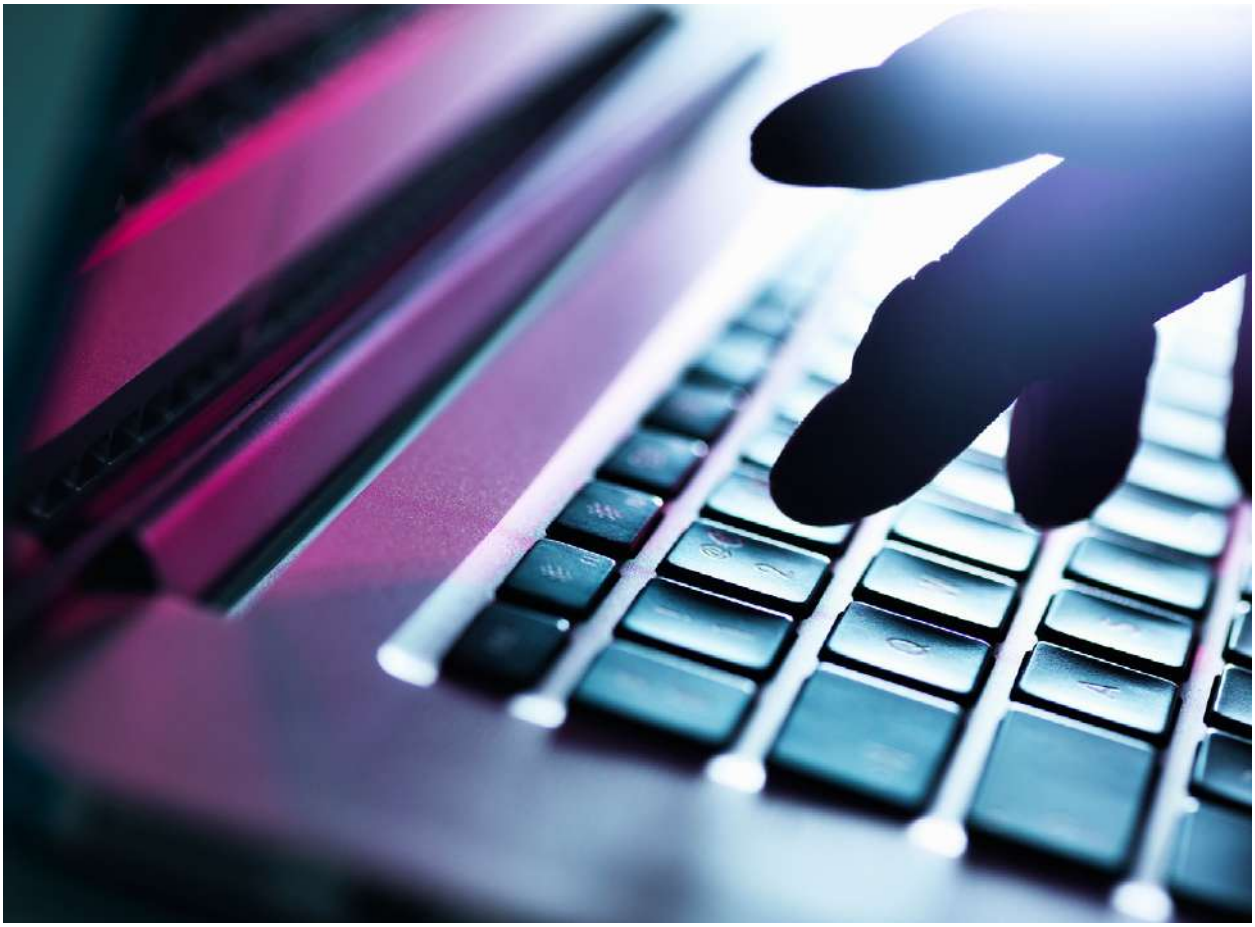
Despite the notification, the victim did not appreciate the severity of the intrusion until a full threat hunt was carried out. Secureworks analysts focused on cost-effective and realistic security control improvements that would clean up known malicious activity, reduce the attack surface, and ultimately help rebuild trust with customers.

This case emphasizes the importance of conducting due diligence with key suppliers to understand their security and response capabilities. Threat actors target weak links in supply chains and will leverage trust relationships to pivot from one compromised organization to another. Having an awareness of these risks can ultimately be used to determine how an organization should interact with suppliers, what information should be shared, and the necessity for compensating controls around any shared connectivity.

© 2019 SecureWorks, Inc. All rights reserved.

Throughout 2018, Secureworks analysts observed sophisticated threat groups preying on supply chain organizations as a means of gaining access to the organization's customers. Examples include a March 2019 disclosure of hardware supplier Asus discovering a compromised update server, and the December 2018 indictment of two BRONZE RIVERSIDE (also known as APT10) operators who compromised IT service providers to ultimately access the networks of these businesses' customers. In addition to targeting IT service and hardware providers, Secureworks analysts observed evidence of sophisticated threat groups compromising third-party communications systems and software providers to access the suppliers' clients.

Managing risks from third parties is challenging but similar to other security risks. Third-party risks can be managed but not eliminated. Relationships between organizations are based on trust, and time needs to be spent establishing the right level of trust. That balance should include validating the security posture of the most trusted organizations and implementing stringent security controls on the least trusted organizations. Compromises in the supply chain are a high-profile part of today's information security challenges. Secureworks has observed that when organizations have a proportionate understanding of the risk, they tend to invest in the correct level of visibility and response capabilities to manage the risk of third party related compromises.



© 2019 SecureWorks, Inc. All rights reserved.

Business Change and Risk Implications

"We've had a lot of change in our environment over the last few years."

Security risks are not static. Discounting the evolving threat landscape, organizations' networks and topologies are continuously shifting. During 2018, Secureworks analysts observed ample evidence of these factors playing a significant role during incidents.

Mergers and acquisitions (M&A) are a classic case of change, where it is imperative that both sides of the process have assessed and understand the cybersecurity implications of joining their IT assets. Pre-existing threats can spread to other systems added to the network. In one case observed in 2018, the IRON LIBERTY threat group (also known as Energetic Bear, Dragonfly, and Crouching Yeti) had compromised one organization and was able to gain access to another organization after an acquisition. The threat actors operated in the environment for over a year, using a combination of custom tools and open-source virtual private network (VPN) software to avoid detection and steal significant volumes of intellectual property.

Organizations on both sides of an acquisition should assess the risks of their counterpart's security programs, including third-party access, detection and response capabilities, vulnerability management, testing and architecture arrangements, general security hygiene, and security history. Before integrating infrastructure, organizations should consider proactive threat hunting and architecture reviews where elevated risk exists.

Checklist for determining cybersecurity risk during mergers and acquisitions

Both organizations should review the following aspects of the other party's environment:

- Proactive threat hunting results, if available
- Third-party relationships and security requirements
- Detection and response capabilities
- Vulnerability management and testing results
- Network and systems architecture
- General security hygiene
- Security and breach history

© 2019 SecureWorks, Inc. All rights reserved.

```
Command Line:        "cmd" /c cd /d "c:$Recycle.Bin\"&PowerShell.exe
                     -ExecutionPolicy Bypass -File          .ps1 >p.log&echo
                     [S]&cd&echo [E]
```

FIGURE 15. *Execution of PowerShell script from Recycle Bin. (Source: Secureworks)*

In one incident in 2018, an organization conducted a proactive threat hunt to search for evidence of threat activity in the network of an organization it was acquiring. Secureworks analysts identified several types of threat activity, including a targeted intrusion on one of the acquired organization's Microsoft Exchange mail servers. The threat actor leveraged system access and native tools (ping, whoami, ver, net view) to understand the environment, retrieve directory listings from other systems in the network (dir), and execute a malicious PowerShell script from the initial system's Recycle Bin folder (see **FIGURE 15**).

This example highlights that proactive steps such as risk assessments and threat hunts can help identify and remediate security gaps and malicious activity before threats are introduced to the other environments associated with the M&A arrangement.

The broad adoption of cloud services represents another common area of IT change. Cloud services can be convenient and affordable, and in some cases hosting data with well-resourced, trusted third parties can offer security benefits as well.

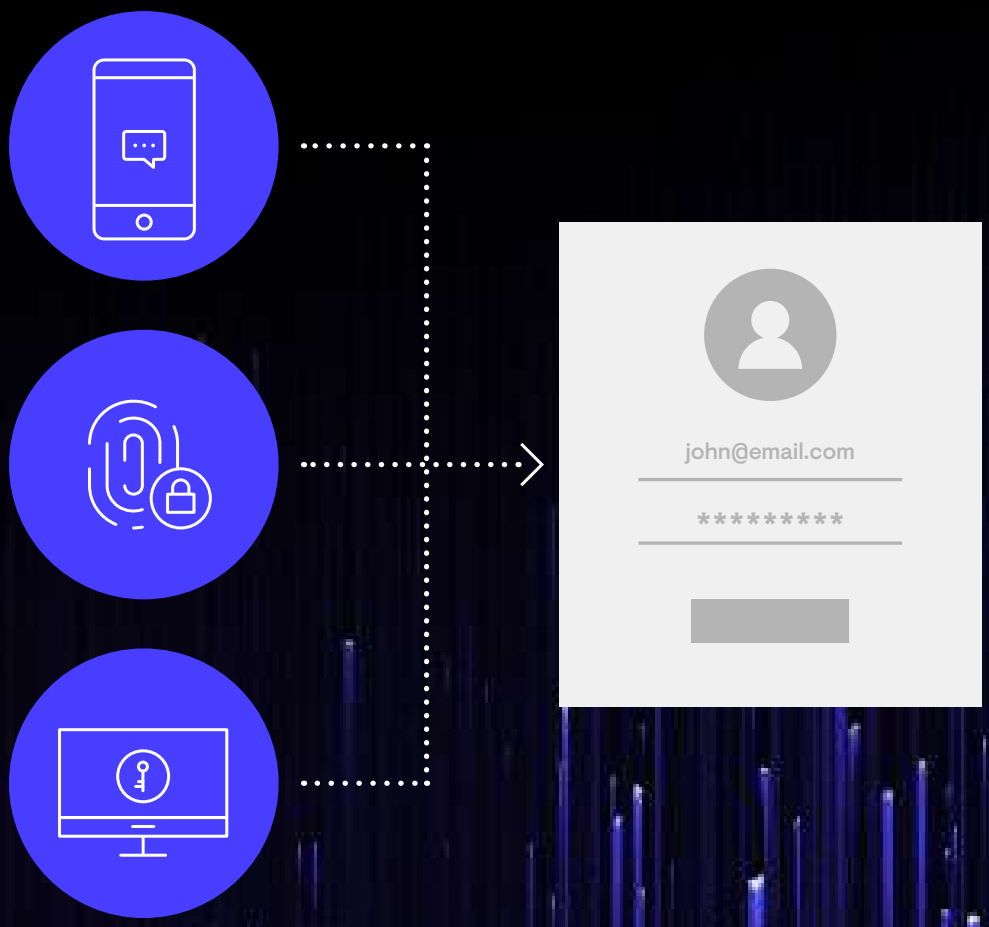
However, these services must be implemented with a strong emphasis on security. In several engagements in 2018, Secureworks analysts investigated stolen passwords for single sign-on (SSO) or cloud solutions exploited by threat actors. Additionally, numerous organizations adopted Office365 in their environments but had not correctly implemented logging, which created a challenge for responders when phishing or valid credentials were the initial access vector for an incident.

Many commodity malware families such as Emotet have integrated common password lists in payloads to expand the sphere of compromise. Additionally, threat groups like COBALT DICKENS target specific user accounts on single authentication systems with commonly used passwords like "Spring2017!" using a technique called password spraying. The implementation of these solutions needs to be secure, use multi-factor authentication (MFA), and be consistently applied to all Internet-facing services. Without these controls it is only a matter of time before accounts are compromised.

© 2019 SecureWorks, Inc. All rights reserved.

We Need to Talk About MFA.

Threat actors who steal credentials via social engineering and other tactics can easily compromise systems that are only protected by a single factor such as a password. Multi-factor authentication (MFA), which relies on something a user knows (e.g., a password) plus at least one other factor such as something the user has (e.g., a token) or a particular attribute (e.g., where the user is), complicates access. The complexity increases the burden for the threat actor to gain additional knowledge to use the stolen credentials.



Key Recommendations to Improve an Organization's Security Posture

The recommendations Secureworks analysts provided during incident response engagements in 2018 did not change significantly from previous years. Threat actors continue to leverage and coalesce around tactics that they know will work, because organizations still struggle to tackle the basics of cybersecurity. Organizations should focus on several key themes to improve their security posture.

1. Choose a Framework

It is easy for organizations to examine incidents and their ensuing root cause analyses in isolation and develop point-in-time solutions to address the issues. But building a security program around an existing industry standard framework ensures that the organization addresses many of the security gaps, and not just the systems that have already been compromised. While there are a number of frameworks to choose from, the practical and pragmatic CIS Controls framework includes straightforward guidance for defenders. Most of Secureworks analysts' recommendations are found in this framework, yet many of the controls the framework classes as basic appear to be beyond the reach of many organizations according to incident response data from the last year.

2. Implement MFA

The most common and effective recommendation Secureworks analysts provide is to implement MFA on all externally facing services. Every service available on the Internet, including cloud applications such as Office 365/Outlook, external VPNs, and SSO pages, should require users to provide a one-time password (OTP) in addition to their regular password. The OTP can be generated from a physical token or a software app. Though deprecated by some standards, an OTP via SMS message to the user's phone is better than a single factor. This rule should apply to all users, especially senior managers and suppliers/vendors that need access to the organization's systems. This security control prevents a threat actor from stealing or guessing a user's password and then using it to gain access to the organization's systems. This is one of the most common tactics used by threat actors and also one of the most difficult to detect.

3. Increase Visibility

Incident response efforts are often hampered by a lack of visibility in the environment. This condition may be due to a lack of historical logs that allows network defenders to forensically piece together what happened, or it may be due to a lack of appropriate tools to monitor for ongoing threat actor activity. Organizations should check that log policies are configured to log useful data for an appropriate amount of time. Endpoint monitoring tools are essential for detecting suspicious activity in the environment after other controls have been evaded.

© 2019 SecureWorks, Inc. All rights reserved.

The move to the cloud has affected many organizations' visibility, as logs are in a different location than they used to be, are not as detailed or configurable, or are not as readily available. Most large cloud providers offer their own way of retrieving appropriate audit logs, so ensuring that this functionality is identified and leveraged is an important part of any cloud migration. Organizations that anticipate and specify their logging requirements during service procurement tend to fare better in incident response situations than those that consider logging requirements after a malicious event occurs.

4. Conduct Preparedness Exercises: Cyberattacks Do Not Occur in a Bubble

Cybersecurity technology solutions cannot address all cybersecurity risks. Business email fraud is a good example of how people and processes play a starring role in either increasing or reducing risk.

In the business email fraud incident described earlier in this report, where the threat actor used a compromised email account (victim 1) to send a fraudulent invoice, and the recipient (victim 2) unknowingly paid it to the threat actor, technological solutions would not have been sufficient. Security controls such as MFA could protect victim 1, but protecting victim 2 requires an effective financial governance process. Organizations should establish a process that involves multiple approvals for transactions, out-of-band confirmation of changes to bank account details, and no regular exceptions for "urgent" requests from senior management.

5. Using Exercises to Understand and Improve Security Posture

Table-top exercises can benefit organizations at different stages. In some cases, the scenarios and subsequent discussions can help participants understand their environment. Involving stakeholders from Legal, Public Relations, and other groups across the organization provides insight about what data is and is not important and why. In other cases, the scenarios can validate participants' understanding of their environment, test the effectiveness of established processes, identify security gaps, and give participants an opportunity to practice before a "real world event."

Common Gaps Identified Through Incident Response Tabletop Exercises

- Misalignment of playbooks (e.g., internal CERT and Executive Crisis Team)
- Lack of communication plan within the incident response plan
- Inability to determine what data is or is not important, and why
- Unclear roles and responsibilities
- Employee susceptibility to social engineering
- Gaps in basic hygiene

!

Involving the whole business in incident response processes and preparedness can ensure a coordinated effort to mitigate attacks. It can also identify gaps in processes and procedures. Using tabletop exercises to test the incident response plan is one of most effective steps organizations can take toward breach preparedness. For a true assessment of readiness, all stakeholders should be included in those exercises.

© 2019 SecureWorks, Inc. All rights reserved.

Conclusion

The recommendations Secureworks analysts made in the aftermath of more than a thousand incident response engagements over the past year were very similar to recommendations in 2017 and 2018: organizations need to improve processes and execution on cybersecurity hygiene.

It can be easy to lose sight of security fundamentals as an organization's complexity increases, but the recommendations in this report are widely accepted as best practices for a reason: they work. If an organization does not have situational awareness of its environment, network defenders will likely struggle to resolve complex challenges that inevitably arise during an incident.

Constantly changing IT environments, corporate priorities, and relationships with third parties continue to create cybersecurity challenges year after year. To reduce risk exposure, organizations should close the gaps they can control and make the company less of a target.

The next best step on an organization's cybersecurity journey may be to take a step back and reassess its ability to execute the fundamentals.

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 customers, 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 customers 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

UNITED KINGDOM:
0808-234-1203

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