CROWDSTRIKE

CYBER INTRUSION SERVICES CASEBOOK 2018

STORIES FROM THE FRONT LINES OF INCIDENT RESPONSE IN 2018 AND INSIGHTS THAT MATTER FOR 2019

CONTENTS

FOREWORD

Shawn Henry
CrowdStrike, CSO
and President of Services

In 2017, the cybersecurity world saw a rise in destructive attacks unlike any we've experienced before. Adversary groups don't observe geographic or industry boundaries, criminal groups have learned to work together to increase their effectiveness, and these malicious actors continue to innovate to achieve their geopolitical or financially-motivated objectives. The impact of these developments is that cybersecurity can no longer be considered an IT problem. It is a business problem.

Just a few of the challenges addressed by the CrowdStrike's Services team in 2018 included: helping with midterm election security; exposing persistent eCrime actors and nation-state adversaries; helping Fortune 500 enterprises and government agencies recover from complex ransomware outbreaks; identifying active attackers in government organizations and critical systems; and addressing vulnerabilities in supply chains.

And we've advocated for better cybersecurity for all, preaching the "1-10-60" rule that defines metrics for accountability and readiness, and briefing boards of directors and C-suites on the criticality of making cybersecurity a top priority.

In 2018, our global Services team focused resources, intelligence and technology to detect and disrupt future attacks. We've analyzed the massive amounts of security data collected from every engagement this year and we've gained new insights into what challenges organizations face and how they can better prepare for the next wave of threats.

This casebook presents some of the findings and recommendations we've made in key engagements across a representative sample of the work we performed last year. We dig into:

- Emerging and notable trends
- Examples of ill-prepared organizations and the devastating effects of the breaches they suffered
- Essential recommendations to prevent companies from becoming another statistic of poor security planning and execution

This casebook also underscores the expertise of our team and the important work we're doing at CrowdStrike® Services. As you read the case studies, you will see that CrowdStrike stands shoulder-to-shoulder with our clients as we work together to stop adversaries and repair damage. But this casebook is not just for CrowdStrike clients — we want everyone to become better prepared to overcome their adversaries in 2019.

EXECUTIVE SUMMARY

A common thread among the incident response (IR) cases handled by the CrowdStrike Services team this year was the resourcefulness and sophistication of today's adversaries. Adversaries are relentless in their search for gaps in organizations' IT infrastructure, both on-premises and in the cloud, and the case studies and statistics included in this report provide vivid examples of their ill-intentioned ingenuity. Organizations should realize:

- **eCrime actors are employing more creative tactics and techniques in their quest to monetize attacks.** There is no slowdown in attacker innovation and the brazenness of eCrime actors. Business email compromises (BECs) figured heavily this year: We encountered examples of attackers moving beyond simply reading emails, as in a typical BEC, to actually being able to watch the email being written and sent.

- **Attackers strike quickly and deeply, yet they are willing to be patient to achieve their objectives.** They get in fast and "breakout" quickly. Nation-state attackers are particularly persistent, demonstrating remarkable patience and resourcefulness as they search for high-value data in the targeted organization.

- **Commodity malware is often a precursor to a disruptive attack.** Access gained with commodity malware is increasingly sold to other bad actors, who use it to deploy ransomware, steal intellectual property, or engage in cryptomining, fraud, and extortion.

- **Attackers continue to hide in plain sight, masquerading as legitimate users.** The fastest and most damaging attacks continue to be those where attackers masquerade as legitimate users. These often occur when user credentials are uncontrolled, misconfigured, or bypassed. Once access is gained, the organization is left completely exposed.

This year's Cyber Intrusion Services Casebook shines a light on how quickly attackers can gain access to your organization. As CrowdStrike previously reported in its 2018 Global Threat Report, an intruder only needs one hour and 58 minutes on average to jump from the machine initially compromised to begin moving laterally through the network. This short breakout time is critical to the success of an attack, and the case studies included in this report drive home the need for speed when containing an intruder and stopping a breach.

Organizations should strive to meet the time objective of the 1-10-60 rule — on average, take no more than one minute to detect a threat, 10 minutes to investigate it, and 60 minutes to remediate it. Organizations that can operate at this level will dramatically improve their chances of staying ahead of the adversary and stopping a potential breach from occurring.

The 1-10-60 rule is a challenging benchmark that requires speed and experience, and to achieve it, organizations will need to adopt next-generation solutions, such as the CrowdStrike Falcon® platform, and leverage strategic advisory services. These steps will deliver the visibility and operational expertise necessary to stop breaches before adversaries can take control of your entire network.

A UNIQUE PERSPECTIVE

CrowdStrike Global Threat Report

Global cyber threat intelligence and insights from the Falcon platform and OverWatch

Cyber Intrusion Services Casebook

Insights from reactive incident response engagements involving CrowdStrike Services

Falcon OverWatch Report

Insights gained from proactive threat hunting conducted in customer environments where Falcon is deployed

CrowdStrike provides a unique perspective when assessing the state of cyber threats. These distinct vantage points are represented in three annual publications, each highlighting the contributions and assessments of individual CrowdStrike teams: insights drawn from the analysis of the CrowdStrike Falcon Intelligence™ team are presented in the Global Threat Report; observations from the Falcon OverWatch™ team as they hunt adversaries are presented in the Mid-Year OverWatch Report; and finally, the real-world experience gained from the Services team responding to incidents and breaches is documented in this **Cyber Intrusion Services Casebook.** This comprehensive and holistic view of the threat landscape allows CrowdStrike to provide specific guidance on the actions organizations can take to improve their security postures.

This Casebook report drills down into the findings from the Services team, drawn from the work it carried out in incident response engagements over the past 12 months. The findings presented here contribute to CrowdStrike's larger body of knowledge and offer unique insights and perspective on the ever-evolving cyber threat landscape.

KEY FINDINGS

The data points provided in this section are the result of information CrowdStrike Services has collected in its incident response, compromise assessments and strategic advisory engagements over the past 12 months. The anecdotal nature of this report affords a different perspective from the findings outlined in other CrowdStrike reports produced by the Falcon OverWatch and Falcon Intelligence teams, which may include data and insight derived from numerous sources, including the 1 trillion security events that the Falcon platform collects each week.

ATTACK REPORTING

Discussions of cybersecurity typically trend toward doom and gloom, but this year's findings also offer some good news: Organizations are continuing to improve their ability to self-detect breaches.

2017
68%

2018
75%

This year, 75 percent of organizations that engaged CrowdStrike for incident response were able to internally detect a breach. That's a 7 percent increase over last year. CrowdStrike attributes this improvement to organizations making a greater effort to mature their security operations and postures. Maturity levels are being enhanced by investments in resources to detect attacks, including endpoint detection and response tools (EDR), threat intelligence, proactive managed hunting and managed remediation services.

But while more organizations were able to self-detect breaches, those detections were not always timely. The ability to quickly detect an intrusion is the foundation of rapid response and remediation, which, in turn, lessens the potential impact of a breach on an organization and its customers and partners. When intruders are not detected promptly, they can wreak havoc at their leisure. In fact, the average attacker dwell time, as reported, was 85 days based on the engagements that CrowdStrike Services was involved in.

This is comparable to the 86-day span revealed in last year's report and suggests that little progress has been made in detection speeds. Clearly, there is considerable room for improvement. Boards of directors, executive management, and the public at large are all rightly concerned that organizations take days, weeks or even months to detect attacks. CrowdStrike recommends that, on average, detection can and should occur within one minute — in accordance with the 1-10-60 rule — and it is committed to helping organizations reach that crucial benchmark.

While speedy detection and response are critical to ensuring that a compromise does not lead to a significant breach, the case studies included in this report illustrate that prevention is equally important, if not more. Commodity malware attacks, spear-phishing campaigns and compromised credentials can often be a precursor to targeting sensitive IP (intellectual property) and PII (personally identifiable information), launching business/operational disruption campaigns, or even attempts to defraud a company via wire transfers. By leveraging best-of-breed endpoint detection, such as the CrowdStrike Falcon platform and monitoring tools that scale and include advanced artificial intelligence (AI) capabilities, organizations can detect the initial signs of a breach before any real damage occurs.

ATTACK OBJECTIVES

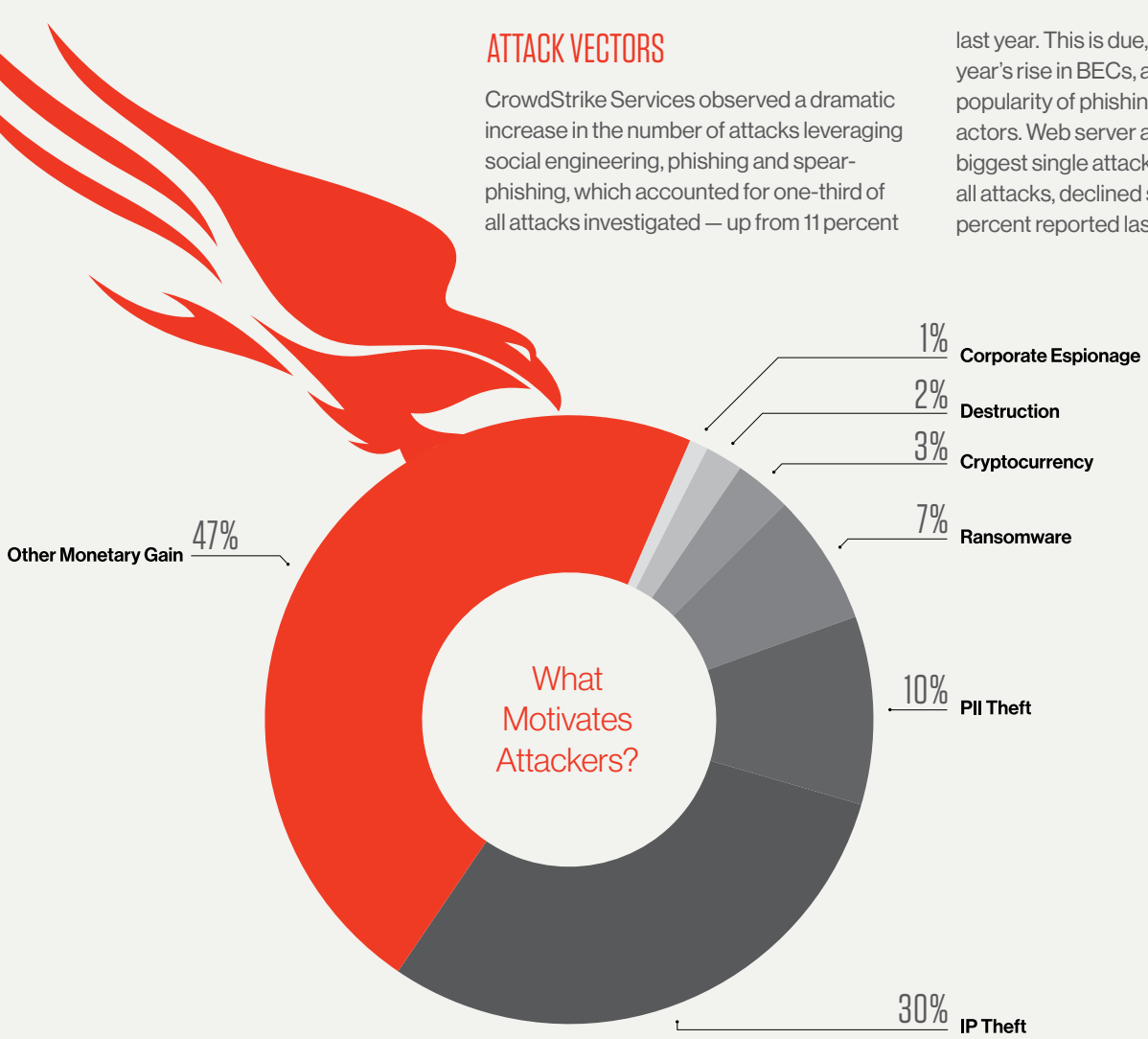
Over the last year the most prevalent attack objectives the CrowdStrike Services team responded to were motivated by monetary gain. Organizations should not be surprised that the second most common objective was intellectual property (IP) theft, as this malicious activity is well-known among industry leaders. Just over 12 percent of the cases involved attacks that were destructive in nature, or related to cryptocurrency or ransomware motives.

75%

This year, 75 percent of organizations that engaged CrowdStrike for incident response were able to internally detect a breach.

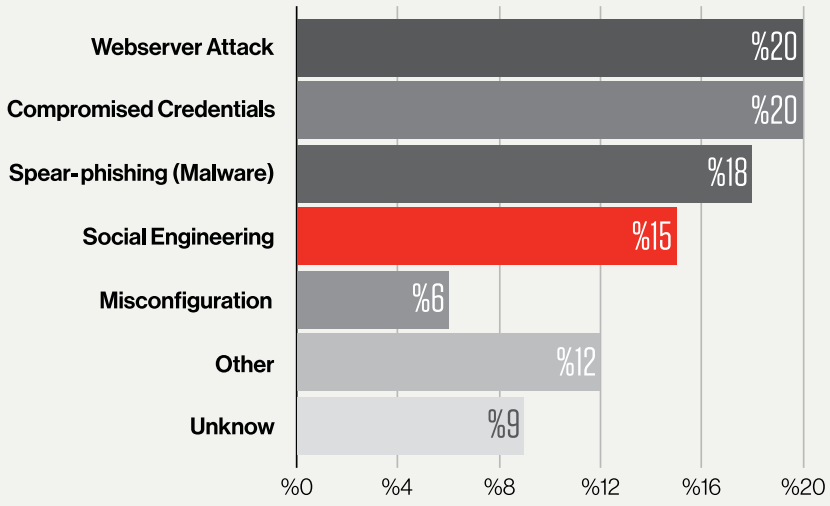
ATTACK VECTORS

CrowdStrike Services observed a dramatic increase in the number of attacks leveraging social engineering, phishing and spear-phishing, which accounted for one-third of all attacks investigated — up from 11 percent last year. This is due, in no small part, to this year's rise in BECs, along with the continued popularity of phishing among nation-state actors. Web server attacks, although still the biggest single attack vector at 19.7 percent of all attacks, declined significantly from the 37 percent reported last year.

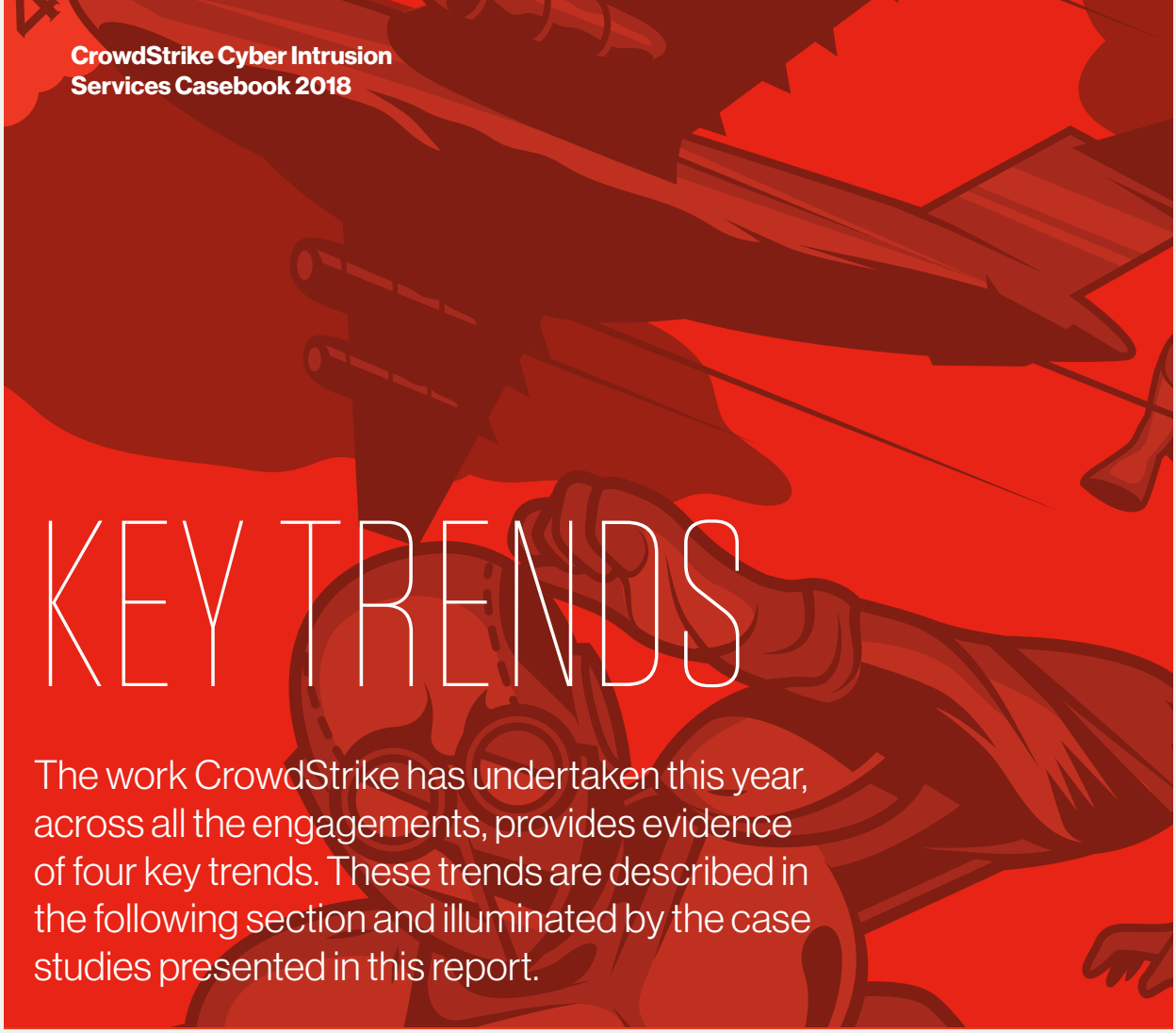


Social engineering, phishing and spear-phishing, accounted for one-third of all attacks

How Do Attackers Gain Access?



CrowdStrike Services continued to see regular use of PowerShell or Windows Management Instrumentation (WMI) in cases this year. The malicious use of legitimate systems tools creates a significant challenge for organizations, which may struggle to identify when a tool is being used properly and when it is being used as a weapon. The right security tools, such as the CrowdStrike Falcon platform, can detect the difference and close down these threats.



KEY TRENDS

The work CrowdStrike has undertaken this year, across all the engagements, provides evidence of four key trends. These trends are described in the following section and illuminated by the case studies presented in this report.

TREND #1: ECRIME ACTORS ARE EMPLOYING MORE CREATIVE TACTICS AND TECHNIQUES IN THEIR QUEST TO MONETIZE ATTACKS.

There is no slowdown in attacker innovation and the brazenness of eCrime actors. CrowdStrike encountered attackers gaining more power and insight into the systems of their victims through the use of remote access tools that deliver real-time monitoring capabilities. This has enabled attackers to move beyond reading emails, as in a typical BEC, to being able to watch the email being written and sent.

The eCrime ecosystem is also evolving. Actors and tools that used to operate discretely now show evidence of working in coordination. For example, the Services team has seen instances where Dridex, the malware usually associated with the adversary group tracked by CrowdStrike Falcon Intelligence as INDRIK SPIDER, is used in conjunction with the FakeUpdates campaign or FrameworkPOS to deliver Dridex. Previously, the FakeUpdates are types of malware associated with other criminal groups.

TREND #2: ATTACKERS STRIKE QUICKLY AND DEEPLY, AND THEY ARE WILLING TO BE PATIENT TO ACHIEVE THEIR OBJECTIVES.

Adversaries typically get in fast and "breakout" quickly. Nation-state attackers are particularly persistent, demonstrating patience and resourcefulness as they search for high-value data in the targeted organization.

As in previous years, misplaced trust and confidence in legacy tools offered opportunities for attackers to dwell in environments for extended periods of time. This is particularly true of sophisticated nation-state actors.

Incomplete and ineffective IR engagements can compound this problem. The CrowdStrike Services team worked on a number of cases where organizations thought their incidents were resolved by previous IR vendors, only for CrowdStrike to discover the attacker was still present or had re-entered the environment almost immediately.

This illustrates why security needs to be holistic. Running incident response on a single system does not tell the whole story of what's happening in the environment; it only

The team worked on multiple engagements this year where simple misconfiguration and misunderstanding of access controls allowed attackers to gain access to an organization through its cloud services vendor.

tells the story of what's happening on that lone system. High-value data is increasingly being stored in cloud-based file-sharing systems and services that have effective and robust security tools; however, they need to be configured properly, and their logging functions must be monitored with vigilance.

The CrowdStrike IR team frequently sees data owners who move their data to the cloud with the expectation that their cloud services vendors will provide security controls, but they have no way of knowing if the vendors have properly configured and applied those security controls. The team worked on multiple engagements this year where simple misconfiguration and misunderstanding of access controls allowed attackers to gain access to an organization through its cloud services vendor.

TREND #3: COMMODITY MALWARE IS OFTEN A PRECURSOR TO A DISRUPTIVE ATTACK.

You can't let your guard down—access gained with commodity malware is increasingly sold to other bad actors, who then use it to deploy ransomware, steal intellectual property, or engage in cryptomining, fraud and extortion.

An organization's susceptibility to commodity malware is also an indicator of the effectiveness of their entire security strategy: If their systems can be compromised with commodity malware, then what could a more sophisticated attacker do?

Last year's report spotlighted the rise of malware variants that employed techniques designed to first infect one system, and then spread to any systems connected with it. This was the case in several notable ransomware attacks. This year, CrowdStrike observed the use of bot networks to aid the initial delivery and subsequent spread of infections.

In a further twist, the CrowdStrike team frequently saw attackers using a malware family called TrickBot to gain access and control systems, only to hand off that access and control to other adversary groups who then attempted extortion attacks. This veritable "den of thieves" was even observed targeting some small to mid-sized organizations.

TREND #4: ATTACKERS CONTINUE TO HIDE IN PLAIN SIGHT, MASQUERADING AS LEGITIMATE USERS.

The fastest and most effective attacks continue to be those where attackers masquerade as legitimate users. These often occur when user credentials are uncontrolled, misconfigured or bypassed, and once access is gained, the organization is left completely exposed. Attackers that are able to gain and maintain access to legitimate credentials can acquire tremendous insight into an organization.

eCrime actors use credential-stuffing and BECs, while nation-state actors tend to use legitimate credentials for direct email and virtual private network (VPN) access. These tactics are a growing problem across a multitude of industries, and organizations of all sizes. Use of single-sign-on (SSO) and multi-factor authentication (MFA) are logical approaches to bolstering and protecting credentials. However, engagements CrowdStrike Services was involved in this year have shown that misconfigured and uncontrolled use of these controls can hinder rather than help, and leave organizations with a false sense of protection.

CASE STUDIES & RECOM-MENDATIONS

Seeing how others have successfully responded to attacks can help you understand how you can improve your own defenses. These anonymized case studies provide insight into how CrowdStrike Services helped real organizations deal with the risks, threats, and actual attacks that have become an ongoing reality of doing business in today's global digital environment.

CASE STUDY #1

A CLEAN LAPTOP LEFT, A DIRTY LAPTOP CAME BACK: AN INTERESTING DRIVE-BY TECHNIQUE

THE CLIENT

An apparel manufacturer with a global presence, including retail locations, was caught up in a malware campaign that compromised its entire EU (European Union) presence.

SITUATIONAL ANALYSIS

One weekend, an employee of the manufacturer brought their laptop to a coffee shop. They used the laptop, which was protected by traditional antivirus software, to visit a website belonging to one of the manufacturer's partners. That site was compromised with FakeUpdates, a campaign affecting thousands of Joomla and WordPress sites, which ultimately led to a Dridex malware infection, and PowerShell Empire installation on the laptop. When the employee returned to work the next Monday, the infected laptop served as the entry point for the adversary to compromise the corporate network.

This situation highlights the risks presented by laptops and endpoint security that only works on the corporate network. Systems that were safe at the end of the workday may be infected by the next morning.

A cloud-based security product that's "always on" would have notified this manufacturer of the compromise in real time, and the adversary could have been stopped before connecting to the corporate network and allowing its entire EU region operations to be compromised.

INVESTIGATION AND ANALYSIS

CrowdStrike Services began its analysis by deploying the Falcon platform throughout the environment to gain real-time protection and visibility on the endpoints, and then used Falcon Forensics Collector, a tool created by CrowdStrike, to collect historical information from endpoints in order to triage and scope incidents quickly. Real-time data, in conjunction with artifacts the adversary had left on the system, were used to understand what had occurred, identify key systems and pinpoint compromised users.

The CrowdStrike investigation included forensic hard-drive analysis of three systems and historical artifact collection from a few thousand additional endpoints. The investigation also identified a misconfiguration in Active Directory that placed all domain users in the local administrators' group for systems within the EU. This misconfiguration alone did not allow for the attack to succeed, but it certainly helped the adversary compromise the environment quickly and completely.

CrowdStrike attributes this attack to INDRIK SPIDER, the adversary usually associated with Dridex. Prior to this incident CrowdStrike had not associated INDRIK SPIDER with the FakeUpdates campaign.

ATTACK TOOLS

That partner site was compromised with FakeUpdates, and the user's browser was sent through a redirection path that led to what appeared to be a legitimate software update-themed page. There, the user's system was fingerprinted through an obfuscated JavaScript file downloaded from a cloud-based file transfer service, which then led to the download and launch of a malicious Flash-Player-themed executable.

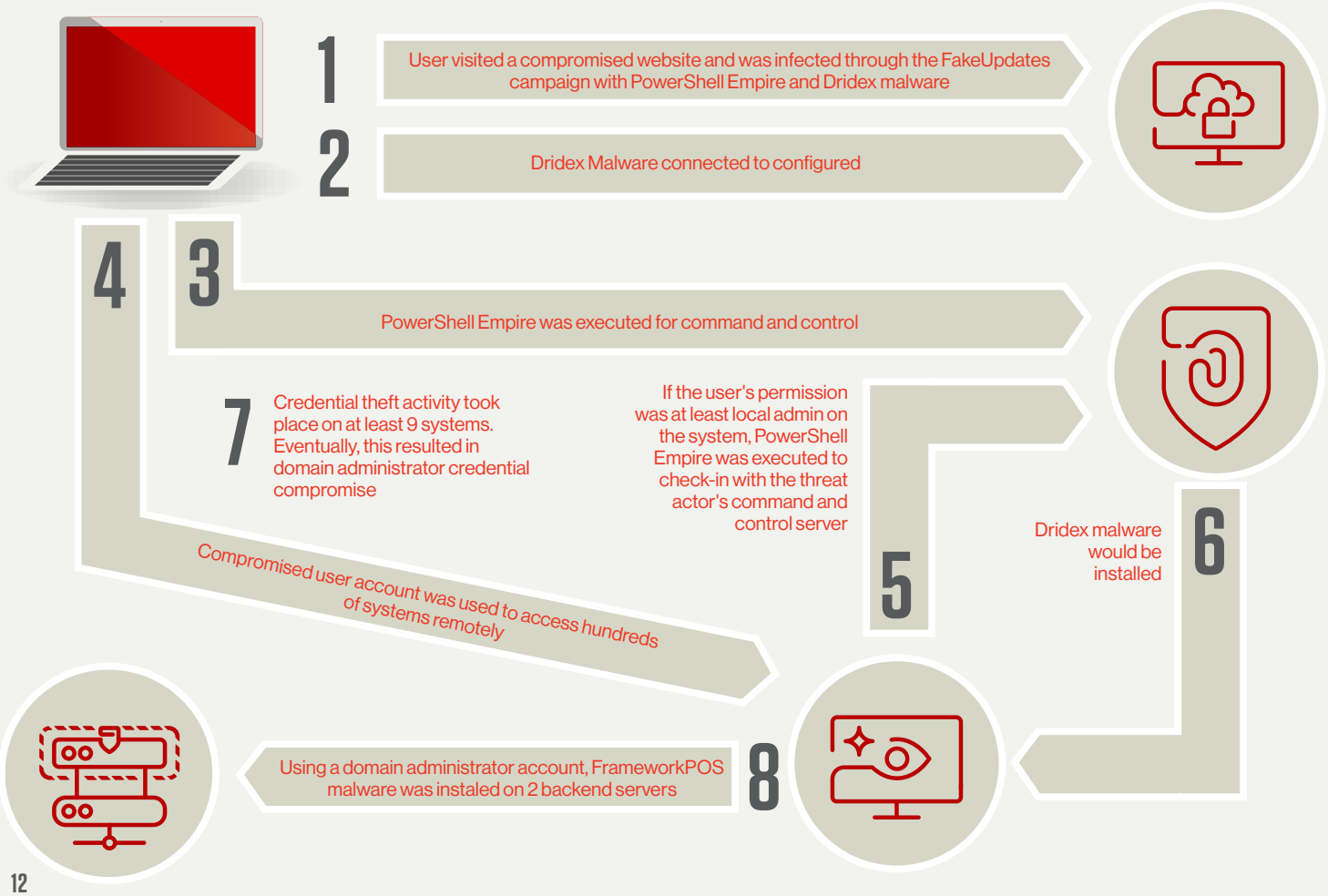
The malicious executable was not recovered during analysis, but the end result was a Dridex malware infection and a PowerShell Empire installation. Dridex is a notorious banking trojan designed to capture banking credentials from web browsing sessions. It is capable of taking screenshots, capturing POST data, redirecting URL requests and injecting code into most modern web browsers. PowerShell Empire is a freely available, post-exploitation framework that can run PowerShell modules and is known to have impressive capabilities.

When the employee whose system was the source of the initial compromise returned to work and connected their laptop to the corporate network, the adversary used PowerShell Empire to quickly pivot to many dozens of systems, using the compromised user's permissions to gain access. When the adversary encountered a server, they executed Mimikatz, a credential theft utility, to gather additional privileged account credentials. Using these newly-acquired credentials, the adversary group eventually gained access to a domain controller and retail store backend server. They installed FrameworkPoS on the retail store server with the objective of stealing credit card data.

HOW THE TOOLS FIT INTO THE MITRE ATT&CK FRAMEWORK

Tactics	Techniques
Initial Access	Drive-By Compromise
Execution	User Execution, PowerShell, Scheduled Task
Persistence	Change Default File Association, DLL Search Order Hijacking, Registry Run Keys / Startup Folder, Valid Accounts
Privilege Escalation	Bypass User Access Control, DLL Search Order Hijacking, Process Injection, Valid Accounts
Defense Evasion	Bypass User Access Control, DLL Search Order Hijacking, Deobfuscate/Decode Files or Information, Process Injection, Scripting
Credential Access	Credential Dumping
Discovery	Remote System Discovery, System Information Discovery
Lateral Movement	Remote Desktop Protocol
Collection	Automated Collection, Data Staged, Man in the Browser
Exfiltration	Exfiltration Over Command and Control Channel
Command and Control	Commonly Used Port

ATTACK LIFECYCLE



KEY RECOMMENDATIONS

- **Implement a cloud-based EDR tool**
  EDR tools provide visibility into the file system, processes, logs and other aspects of a host, and alert on behavior that indicates the host has been improperly accessed. A cloud-based EDR tool, such as CrowdStrike Falcon Insight™, provides protection across every system anywhere in the world, not just on the corporate network.
- **Perform a global password reset**
  Any time an adversary gains access to a domain controller, whether or not evidence suggests they stole the Active Directory database, it is prudent to conduct a password reset. This involves resetting local and domain users and also any service accounts and contractors.
- **Change corporate and personal banking credentials**
  When dealing with a banking trojan such as Dridex, it is important to change the credentials for all banking accounts, regardless of whether evidence indicates the account was compromised. This is a best practice to protect both the company and its employees.
- **Conduct an Active Directory configuration review**
  The adversary abused a misconfiguration within the company's Active Directory that provided unnecessary privileges, globally, to all users within the EU domain. While likely not the sole source of the attack, this misconfiguration certainly played a role in increasing the speed and spread of the attack. CrowdStrike recommended that the customer perform a deep review of their Active Directory configurations across the entire global enterprise.
- **Standardize logging time zones**
  Global enterprises have systems distributed around the world, and events are recorded in each system with log files timestamped locally. When an incident occurs, incident response teams need to collate the events to create a timeline. That takes much longer when each timestamp has to be converted to a standard time zone, such as UTC, before sense can be made of the events. All too often, this small but crucial configuration is overlooked, leading to problems and subsequent delays in discovering new information and correlating events.
- **Segregate accounts**
  End users should not be given administrator privileges on their local systems. CrowdStrike recommends one account for administration of servers, one for workstation administration, and one for domain controllers. No account should be able to access a system that is not within the same category; for example, the account used to administer domain controllers cannot be used to access workstations or servers. Also, adding one-time passwords, or passwords that expire after short periods of time for these accounts goes a long way in decreasing the ability of the adversary to use the accounts.

CASE STUDY #2

THERE'S NO SUCH THING AS "A LITTLE" SECURE

THE CLIENT

A small government contractor was fully compliant with federal requirements, but that didn't protect them from a long-term compromise by suspected nation-state actors.

SITUATIONAL ANALYSIS

When CrowdStrike Services was called in to investigate a compromise by potential nation-state actors, it wasn't the first vendor on the scene. Over the years, this company had engaged multiple security vendors to perform incident response activities, for a subset of its environment, to fix specific problems, but they'd never examined the entire enterprise.

CrowdStrike applied its comprehensive methodology and found a problem that had persisted for over two years, affecting many more systems than originally considered. The adversary had escaped the notice of preceding security providers and managed to maintain persistent access to the network the entire time.

Security has to be holistic, encompassing every facet of an organization's environment to ensure persistence cannot be maintained by bad actors. The longer adversaries can dwell inside systems, the more damage they can do. Comprehensive visibility across the network is the only way to prevent this. Running incident response on a single system only ensures the security of that one system; the rest of the network may be infected, but no one will know because nobody looked. Visibility across the network is the only way to prevent long dwell times.

INVESTIGATION AND ANALYSIS

The initial point of entry was unable to be identified since this incident had begun years before CrowdStrike was engaged, but evidence suggested it was a web server vulnerability. How the adversary stayed inside is uncertain. They installed numerous backdoors and remote shells across the environment. They used legitimate credentials to move throughout the environment unnoticed, and compromised the Active Directory database to steal the hash associated with the KRBTGT account. From there, they were able to bypass standard access controls by creating forged tickets. The forged tickets would grant them access, with or without a legitimate user account, until the password for KRBTGT was changed at least twice. This is called a "Golden Ticket" attack.

Initially, two systems were thought to be compromised. However, when the Falcon Forensics Collector was deployed across the majority of the network, CrowdStrike observed that many other systems had been compromised, as well. The Services team was able to track a majority of the adversary's activity because the client was logging process creations on its domain controllers. They also had robust server backups, so the team was able to go back through the history and pull system artifacts from two years ago. These are things the Services team wishes everybody would do.

While logs are useful to investigators who come in after a compromise is suspected, they're more useful when security teams monitor them to stop contemporary attacks. This company logged everything, but they weren't looking at those logs. If they had been, they would have noticed that the adversary had compromised the password hash and was using it to create Golden Tickets. The malicious command literally had the word "Golden" in the command line.

The adversary was looking for email content belonging to the company's executives, as well as confidential data about government contracts on Exchange and file servers. They usually conducted these searches in the middle of the night and during U.S. government holidays, when security and IT teams are more likely to be short-staffed, and alerts are less likely to attract attention. For instance, CrowdStrike saw they had gained access to mailboxes at 11 p.m. on Thanksgiving. This is a tactic that has been attributed to Chinese actors for at least a dozen years.

CrowdStrike applied its comprehensive methodology and found a problem that had persisted for over two years, affecting many more systems than originally considered.

As with many organizations whose business is dependent on government contracts, compliance is king in this company. If the government said a particular control was good enough, they implemented it and moved on. They were fully compliant, but in the end, suspected nation-state actors were able to infest their systems for years. CrowdStrike sees this often and unfortunately, checklist compliance does not equal security.

ATTACK TOOLS

The threat actors leveraged a custom build of Mimikatz to compromise credentials and craft forged Kerberos tickets. Through Windows event logs, CrowdStrike was able to identify that not only had the threat actor obtained plaintext passwords for multiple users, but also had obtained the password hash for the KRBTGT account.

In addition, the adversary used "DLL search order hijacking" to compromise an antivirus executable. This particular executable was created by the threat actor on the target systems. While the file on disk was legitimate, it was used to execute malicious code. The adversary accomplished this by placing a specially crafted file in the "search order" for the executable. When the binary was executed, it searched for the libraries it needed to function and loaded the adversary's code into memory. This allowed the adversary to avoid detection by traditional signature-based technologies, as the malicious activity would only be observed at run-time.

They used a lot of commonly available tools for system administration, including PSExec, PowerShell, and scheduled tasks. These tools, like Active Directory Explorer, were employed to gather information about the domain, such as user and system names. CrowdStrike also observed the use of WinRAR, an archiving utility that was thought to have been used for archiving email mailboxes for exfiltration.

A unique tool that this adversary used was a legitimate cloud file transfer service. They removed data from the customer's network and moved it directly to their own account with the file transfer service. Because this particular service is in wide use among enterprises, most businesses will not block access to it.

HOW THE TOOLS FIT INTO THE MITRE ATT&CK FRAMEWORK

Tactic	Technique
Persistence	Scheduled Tasks
Privilege Escalation	Golden Ticket, Plaintext Passwords in Log Data
Defense Evasion	DLL Search Order Hijacking
Credential Access	Mimikatz
Lateral Movement	PSExec, Powershell, Pass the Hash
Exfiltration	WinRaR

KEY RECOMMENDATIONS

- **If you log it, review it**
  Ensure that you set up a formal process with respect to how you review and manage logs. Sometimes, logs are turned off as a result of compliance efforts and space requirements; be aware of that possibility and implement controls to prevent it.
- **Patch everything**
  Make sure everything is patched and a vulnerability management program is in place. Maintain a software inventory and regularly review patches available for the environment as part of the patch program.
- **Execute a holistic investigation**
  In the long run, performing a comprehensive investigation the first time, throughout your entire environment, can save a lot of time and effort down the road. If you scope an investigation to a limited set of systems, you risk allowing the attackers to maintain persistence, lying dormant for some time before becoming active again at a later date.a

CASE STUDY #3

MONETIZE OR DIE: THE ADVERSARY THAT CAME BACK AND SWAPPED TACTICS

THE CLIENT

An insurance company did the right thing by keeping good backups, but the attack didn't end when they refused to pay a ransom — the attacker switched to cryptomining.

SITUATIONAL ANALYSIS

Good backups put this company in a position of power when they were hit with a ransomware attack. They didn't have to pay the adversary because they didn't need them to decrypt its data: they just restored the assets and got back to business. After the recovery, the company asked CrowdStrike to find out how they were attacked.

The ransomware used, HC7/Gotya, was written in the Python scripting language and compiled into an executable to run on a Windows system without Python being installed. Using two open source tools, unpy2exe and decompyle6, CrowdStrike was able to reverse engineer this ransomware binary back to its original source code.

At first, the CrowdStrike Services team thought it was dealing with a typical ransomware investigation. The team's analysis continued by attempting to identify the initial intrusion vector and deployment methods used to distribute the ransomware.

In these investigations, CrowdStrike deploys the Falcon sensor to monitor the customer's systems for unauthorized activity. The CrowdStrike Falcon OverWatch™ team monitors and hunts through the Falcon data around the clock for the duration of the investigation. In this case, OverWatch notified the Services team of new hands-on-keyboard activity — the adversary was attempting to monetize their access by deploying cryptomining software called XMRig. CrowdStrike Services shifted its focus to stopping and preventing further access in this second-wave attack, which would have continued to impact the company's business if the team had not been alerted in time to shut the doors. Falcon was able to proactively block the cryptomining activity, so no damage was done. By providing expertise to the customer's security team, CrowdStrike was instrumental in eradicating the adversary from the environment completely in just under six hours.

INVESTIGATION AND ANALYSIS

CrowdStrike identified the initial infection vector as an exposed web server vulnerable to CVE 2017-7269, a vulnerability in Microsoft Internet Information Services 6.0 servers. When weblogs for this server were reviewed, the vulnerability was positively identified, based on the specific PROPFIND requests being made.

The adversary attempted to use an EternalBlue (MS17-010) scanner to search for unpatched systems within the network. This, however, was blocked by the security tools the company had already deployed. To get around the block, the adversary used Mimikatz to harvest credentials and PSExec to move laterally using legitimate accounts in order to deploy the ransomware to targeted systems.

When the company did not pay the ransom and recovered using its backups, the adversary used their predominant access-persistence mechanism. This mechanism resides within the WMI repository via permanent event subscriptions.

There are three elements necessary to create a fully functioning permanent event subscription: an event filter, an event consumer and a filter-to-consumer binding.

- The event filter is a WQL (Windows Query Language) query that provides the parameters on how and when an action is to be performed.
- The event consumer is the action to be executed when the parameters of the event filter are met.
- The filter-to-consumer binding identifies the association between the event filter and event consumer.

WMI permanent event subscription can be easily queried using PowerShell, and malicious permanent event subscriptions stand out, usually due to a large base64 encoded PowerShell blob existing in the event consumer.

By providing expertise to the customer's security team, CrowdStrike was instrumental in eradicating the adversary from the environment completely in just under six hours.

The script below and a target list of systems located in a hosts.txt file, can be used by defenders to identify this activity across the environment.

```
$Computers = Get-Content hosts.txt
$Cred = Get-Credential
$CommonArgs = @{
       Namespace = 'root\subscription'
       ComputerName = $Computers
       Credential = $Cred
       }
Get-WmiObject @CommonArgs -Class '__
EventFilter'
Get-WmiObject @CommonArgs -Class '__
EventConsumer'
Get-WmiObject @CommonArgs -Class '__
FilterToConsumerBinding'
```

This was of particular interest because this method of persistence was used exclusively by nation-state actors as recently as two years ago. Seeing it here is evidence that some methods are trickling down to less sophisticated actors.

The persistence mechanism downloaded code on a scheduled basis, enabling the adversary to pass commands to the targeted system through PowerShell Reflective Injection. Credential harvesting occurred through injection into the LSASS (Local Security Authority Subsystem Service) process and used the completely in-memory version of Mimikatz. With the stolen credentials, the adversary could pivot to systems of interest and establish a secondary access method by instantiating an SSH tunnel with the tool Plink.

The adversary used this secondary access to deploy a batch script to interfere with antivirus software, download XMRig and create a service with the Non-Sucking Service Manager (NSSM), so that XMRig would continue to execute after a reboot.

The Services team worked with the company to enable Falcon preventions and deployed network and hash blocks to prevent further adversary activity and eliminate them from the environment. At that point, there was nothing the adversary could do.

Less than six hours passed between the moment CrowdStrike discovered hands-on keyboard activity until the adversary was eradicated from the systems, and they haven't been able to get back in.

ATTACK TOOLS

The adversary leveraged different variants of the same ransomware, all written in Python and compiled into an executable, likely through use of the py2exe tool. A result of this method is that the Python interpreter, the required Python libraries, the code, and any pertinent data are all packaged together, resulting in a large binary.

When the adversary returned to the environment after their failed extortion attempt, they used all open source tools, including:

- NSSM, a utility used to install and configure persistent services
- MS17-010 (EternalBlue) vulnerability scanner
- PSExec, a tool used to execute applications on a remote system with appropriate credentials
- Plink, a tool used to establish a secondary access method

Tscon, a tool that allows for RDP session hijacking
A variant of XMRig, a Monero cryptocurrency miner that leverages a system's CPUs to perform mining operations
Key artifacts of this investigation were contained in the Windows Event logs. These included RDP session hijacking attempts, as well as related XMRig services that were instantiated. Querying the WMI repository for permanent event subscriptions was a critical next step in identifying the adversary's main source of persistence. Lastly, identification of the initial infection vector occurred after CrowdStrike traced the first ransomware compromise to a vulnerable web server and reviewed the weblogs for successful exploits of the CVE 2017-7269 vulnerability.

HOW THE TOOLS FIT INTO THE MITRE ATT&CK FRAMEWORK

Tactics	Techniques
Initial Access	Exploit Public-Facing Application
Execution	PowerShell, Scripting, Graphical User Interface, WMI
Persistence	WMI, Event Subscription, New Service, Redundant Access
Credential Access	Credential Dumping
Discovery	Account Discovery
Lateral Movement	Windows Admin Shares, Remote Desktop Protocol
Command and Control	Commonly-Used Port, Standard Application Layer Protocol, Remote Access Tools, Fallback Channels

CrowdStrike constantly sees organizations compromised because they haven't upgraded to supported operating systems. The savings gained by stretching the life of an outdated system are not worth the risks.

KEY RECOMMENDATIONS

- **Develop a post-recovery strategy**
  Recovery is not the last step in remediating a ransomware attack. The adversary may have planted backdoors or other surprises in the environment. Organizations need to know how the adversary got in before they can be sure they were successfully ejected.
- **Upgrade operating systems**
  This is not the only company leveraging end-of-life systems, such as Windows XP and Server 2003. CrowdStrike constantly sees organizations compromised because they haven't upgraded to supported operating systems. The savings gained by stretching the life of an outdated system are not worth the risks.
- **Upgrade to PowerShell V5 and remove previous versions**
  Logging in this version is so robust that security teams can see commands being executed in real time. If companies would update PowerShell to version 5 across the enterprise, their own security teams could see what is happening and respond right away. Also, removing previous versions of PowerShell in the enterprise will aid in preventing downgrade attacks. Updating PowerShell takes a conscious effort, but it's worth it.
- **Leverage MFA for all users and Privileged Access Management tools**
  Make it as difficult as possible for adversaries to get access to and leverage both user and admin credentials from outside your network. Once they have those, they can do whatever they want in the environment. In addition to MFA, a more robust privilege access management process will limit the damage adversaries can do if they get in.

CASE STUDY #4

AN EMPLOYEE SATISFACTION SURVEY WAS A FRONT FOR A PAYROLL HEIST

THE CLIENT

A retailer in the U.S. was targeted by a phishing scam that led to an attempt at a large-scale payroll theft, culminating in arrests.

SITUATIONAL ANALYSIS

This company noticed suspicious activity on the account of one of its C-level executives. The company identified the original phishing email, which was an invitation from an external company to participate in an employee survey. The executive didn't think an employee satisfaction survey had been authorized, so they went to the survey page to check it out.

Subsequently, a group of users that reported to the executive received a similar email. This one came from the executive's email account. Trusting the credibility of a link sent by one of their executive officers, many employees complied with the request and visited the page to take the survey. Employees who had not completed the survey were sent a reminder from the executive's account, and more people went to the page.

The retailer had recently outsourced its payroll functions to a third-party payment solutions provider. CrowdStrike noticed that password resets for the payroll portal were being requested and informed the company. CrowdStrike caught the fraud just a few days before payroll was issued, but if it had not been discovered, the loss would have exceeded $1,000,000.

The company engaged CrowdStrike Services to help them understand the implications of the attack and find out if it had impacted their systems more than they had already determined.

INVESTIGATION AND ANALYSIS

The executive originally phished didn't enter any credentials into the page, but that wasn't necessary. Simply visiting the page gave the adversary a chance to grab the hash of their credentials by leveraging a web browser vulnerability that allowed a website to request username and password hash from a users system. The adversary then cracked the hash to get into the SSO system and leveraged all the privileges belonging to the executive.

The CrowdStrike Services team believes the adversary explored the executive's email in search of anything they could monetize. They found their opportunity when they happened upon the news that the company was outsourcing its payroll.

The Services team examined Microsoft Outlook at a granular level and saw many logins from unauthorized IPs. The team was able to put together a chain of "who sent what to whom," which revealed password resets and email deletions. Among the deletions were a lot of messages from the third-party payroll service. Adversaries often delete emails that might expose their malicious activities, so this seemed significant.

The adversary had requested password resets to the third-party payment portal for some of the employees, and then intercepted the reset messages before legitimate account owners could see them. Once inside the payment portal, the adversary redirected the employees' paychecks to an online bank that provides the ability to send money anywhere in the world from an account via gift cards. CrowdStrike has observed other BEC cases that involved SSO credential theft, but those cases involved only an internal portal. This is the first time the team has seen an adversary bold enough to use a third-party portal as part of an attack. Clearly, they were confident in their ability to intercept communications between the third-party portal and employees with legitimate accounts.

CrowdStrike noticed that password resets for the payroll portal were being requested and informed the company. CrowdStrike caught the fraud just a few days before payroll was issued, but if it had not been discovered, the loss would have exceeded $1,000,000.

The Services team discovered that the survey page used as bait had been hosted on an unmonitored website operated by a small library located in the US. The code was buried deep on the web server, but when attempts were made to retrieve the files to find more evidence, it was too late. The library had found the page first and wiped the file.

CrowdStrike, with the permission of the customer, conveyed essential details of the case to the FBI. Using this information and information about other CrowdStrike cases involving the same adversary, the FBI was able to arrest the group that was using this particular set of TTPs.

HOW THE TOOLS FIT INTO THE MITRE ATT&CK FRAMEWORK

Tactic	Techniques
Initial Access	Phishing
Execution	Login to Customer Email System
Credential Access	Hash Capture / Cracking
Discovery	Recon of Compromised Email Boxes
Lateral Movement	Reset of External HR Portal Passwords
Exfiltration	Limited to Email Data

KEY RECOMMENDATIONS

- **Implement MFA**
  The CrowdStrike Services team has seen many incidents that could have been prevented by ensuring the use of MFA. Everyone should use it, particularly if you are using popular cloud-based systems for email, payroll, human resources and much more. Systems that are widely used by businesses are popular with adversaries, and even the most security-aware users can be socially engineered.
- **Monitor cloud infrastructure**
  People buy cloud services and believe they are secure and that the cloud services provider is taking care of them. But often, this is not the case and every business should take responsibility for its own infrastructure. Pay for the extra reports the provider offers and take the same precautions you would if the infrastructure was on-premises. In this case, the data and reports had been purchased, but they were not reviewed. If the customer had known to look, they would have seen that IPs from Nigeria were logging into their accounts. This BEC didn't have to go undiscovered for four weeks.
- **Put a rules-based firewall in front of your single sign-on**
  Set up rules to block IPs coming from suspicious domains before they can get into the network. If this customer had utilized a rules-based firewall, the adversary never would have seen the payroll portal, let alone accessed it.
- **Preserve evidence such as suspicious emails**
  Any organization that comes across a suspicious email should save it offline, for review by a qualified investigator, such as a CrowdStrike — or contact your local FBI Cyber Crime representative.

CASE STUDY #5

FINTECH COMPANY'S MULTI-FACTOR AUTHENTICATION FAILS AND A PHISHER WALKS RIGHT IN

THE CLIENT

A global fintech provider of innovative lending products was doing everything right to control access to its network, but one mistake left them open to a BEC.

SITUATIONAL ANALYSIS

This company realized something was wrong when thousands of emails were sent to their employees by an internal user. The email's subject line mentioned a shared document, and the attached PDF directed recipients to a linked web page that asked them to submit their login details.

An unauthorized third party had gained access to the internal user's credentials and used them to phish the entire organization. Shortly after the first user was compromised, three more followed. These compromises happened despite the fact that the company was using a best-of-breed SSO product in conjunction with a separate MFA service.

CrowdStrike did not discover any fraud. Rather, the adversary seemed to be in search of more credentials, which is characteristic of adversaries that conduct BECs. However, this adversary only had access to stolen credentials for about eight days, so there's a chance they hadn't had time to target a user with the authority to make financial decisions before CrowdStrike stopped them.

INVESTIGATION AND ANALYSIS

CrowdStrike discovered that the SSO product was configured in such a way that MFA was not enforced. This error is common enough that the SSO vendor's documentation specifically states that misconfiguration will disable MFA.

The system was supposed to work as follows: A user who tried to log in to Office 365 would be automatically directed to the authentication systems belonging to the SSO and MFA providers. Once the user provided legitimate credentials, they would be directed back to Office 365. However, because of the misconfiguration, users bypassed the SSO/MFA system and were sent directly to Office 365. Office 365 offers a built-in MFA feature, but it was not turned on because the company was relying on its third-party software to handle that function. In addition, some employees were using outdated email protocols and applications that do not support the modern authentication their SSO and MFA products need in order to work properly. Instead of implicitly denying the unauthorized user, the systems allowed entry.

The adversary may have known this was a way to get around authentication denials, or they may have just stumbled on this company's misconfiguration. The CrowdStrike Services team often sees adversaries connect with Office 365 in search of mailbox content, but their goal is usually to exfiltrate a copy of the mailbox content. They can't get that through a web browser, so they try a legacy protocol like IMAP or POP that does not support MFA. That may be how the adversary entered this system.

The SSO product provided internal logging, which CrowdStrike used to review all the company's email accounts, as well as their Office 365 activity. The Services team looked for malicious logins characterized by several factors, such as sign-ins from suspect locations like Nigeria, impossible travel scenarios, or the use of IP addresses belonging to IP anonymizers such as VPN providers.

The CrowdStrike Services team has seen many incidents that could have been prevented by ensuring the use of MFA.

CrowdStrike also looked for specific mailbox settings, such as rules set by users to forward or delete messages. Adversaries typically change these settings when they launch a phishing campaign in order to hide their activity from the legitimate user. Changes to the SMTP forwarding settings were also checked, because adversaries leverage them to send all inbound mail to inboxes they control.

This company had an email filtering system that performed URL rewrite in its corporate environment, but this product had a hard time scanning attachments. The original phishing email most likely slipped through these defenses because the malicious links were in the attachment, not the body of the message. The other three compromises would not have been caught by the email filtering system because they were sent by internal users, and therefore would not pass through the filtering system at all. Most companies don't check content originating from and staying within the network.

ATTACK TOOLS

No exploits or tools were used to conduct this campaign. It was a classic BEC that relied on social engineering and human error. However, CrowdStrike analyzed many key artifacts, including:

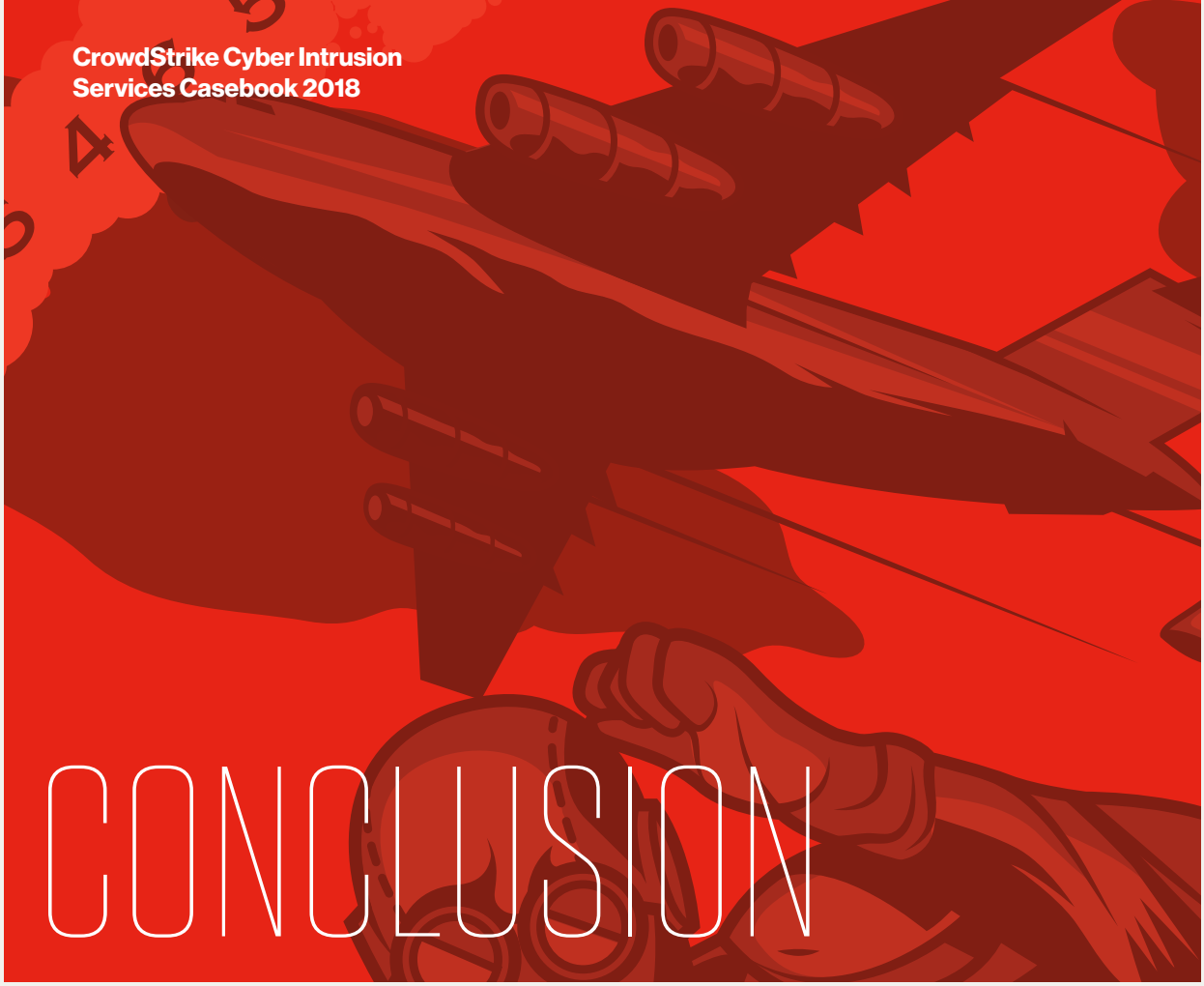
- SSO logs
- Azure Active Directory sign-in logs
- Unified Audit Log (UAL) logs
- Azure Active Directory Identity Protection alerts
- Email forwarding rules, SMTP forwarding and user delegates
- Phishing emails
- Mailbox content

How the Tools Fit into the MITRE ATT&CK Framework

Tactics	Techniques
Initial Access	Spear-Phishing Attachment
Persistence	Account Delegation
Defense Evasion	Inbox Rules, Email Deletion, Masquerading
Discovery	Recon of Compromised Email Boxes
Collection	Email Collection
Exfiltration	Legacy Protocols (e.g., IMAP/POP3)

KEY RECOMMENDATIONS

- **Implement MFA Correctly**
  The CrowdStrike Services team has seen many incidents that could have been prevented by ensuring the use of MFA. Everyone should use it, particularly if you are using popular cloud-based systems for email, payroll, human resources and much more. Systems that are widely used by businesses are popular with adversaries and even the most security-aware users can be socially engineered.
- **Disable unused legacy mail protocols**
  IMAP and POP are prone to attacks as they do not support MFA. Disable them in favor of a protocol that supports modern authentication, such as MAPI.
- **Utilize native document APIs supported by Microsoft**
  Microsoft has an extensive set of APIs and reports that will enable an organization to pull events out of Office 365 and send them to their SIEM for processing. CrowdStrike advises any business that has been targeted by a BEC to do this.
- **Require user and executive security awareness training**
  Regular security awareness training won't stop the occasional human error, but it will help prevent mistakes caused by ignorance. Make mandatory training a regular occurrence.



CONCLUSION

Adversaries and tools vary widely, but these case studies reveal some common defenses that every security stakeholder should put in place as they continually evaluate their staffs, processes and technologies for security resilience:

- **Implement MFA to ensure individuals' authentication and validation is addressed as a high priority.** Attackers are focused on gaining access to credentials. Proper implementation of MFA is both a powerful and practical step to neutralizing their efforts.

- **Expand the focus and scope of log monitoring to better track adversaries and attacks.** Attention and capabilities must move beyond traditional logging sources to include application-level logging and monitoring.

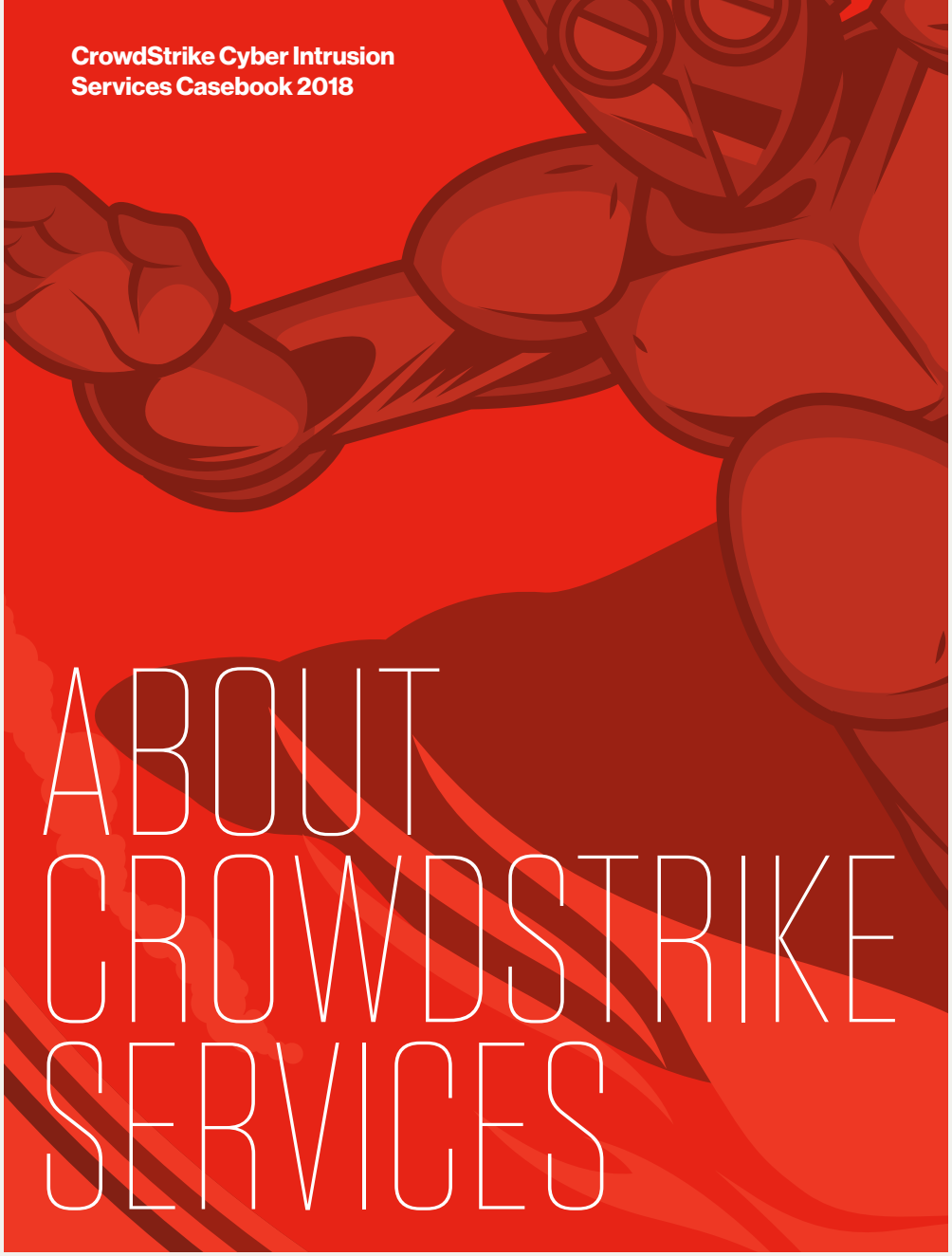
- **Ensure vulnerabilities are patched quickly and effectively.** CrowdStrike Services provided this same guidance in last year's Casebook, and the advice remains as important now as it was then. Adversaries leverage both known and newly discovered weaknesses in key IT systems. When vendors release patches to address vulnerabilities, ensure those patches are applied properly.

- **Review cloud application security controls.** Organizations need to thoughtfully assess their cloud infrastructure and applications so they can determine if appropriate levels of security and governance are implemented.

Preparing for the next attack is an integral part of managing risk, but attackers are innovative and technology is changing at a faster pace than ever. How do you prepare for the unknown?

The unknown is manageable when you implement the best practices defined above, and have access to the right expertise when you need it. Rapid detection of threats, seamless classification and understanding of risk, and speedy remediation are essential ingredients in mitigating the damaging effects of a breach.

The experts at CrowdStrike Services can help you identify potential unknowns, fix the gaps in your people, processes, and tools, and, ultimately, fortify your organization's cyber resilience. No one can predict the future, but CrowdStrike can help you be prepared for it.



ABOUT CROWDSTRIKE SERVICES

CrowdStrike Services equips organizations with the protection and expertise they need to defend against and respond to security incidents. Leveraging CrowdStrike's world-class threat intelligence and next-generation endpoint protection platform, the CrowdStrike Services incident response (IR) team helps customers around the world identify, track and block attackers in near real time. This unique approach allows CrowdStrike to stop unauthorized access faster, so customers can resume normal operations sooner. CrowdStrike also offers proactive services so organizations can improve their ability to anticipate threats, prepare their networks and ultimately, prevent damage from cyberattacks.

EXPERIENCED A BREACH?
Call +1 855.276.9347
www.crowdstrike.com/services

ABOUT CROWDSTRIKE

CrowdStrike is the leader in cloud-delivered endpoint protection. Leveraging artificial intelligence (AI), the CrowdStrike Falcon platform offers instant visibility and protection across the enterprise and prevents attacks on endpoints on or off the network. CrowdStrike Falcon deploys in minutes to deliver actionable intelligence and real-time protection from Day One. It seamlessly unifies next-generation AV with best-in-class endpoint detection and response, backed by 24/7 managed hunting. Its cloud infrastructure and single-agent architecture take away complexity and add scalability, manageability, and speed.

CrowdStrike Falcon protects customers against all cyber attack types, using sophisticated signatureless AI and Indicator-of-Attack (IOA) based threat prevention to stop known and unknown threats in real time. Powered by the CrowdStrike Threat Graph™, Falcon instantly correlates 1 trillion security events a week from across the globe to immediately prevent and detect threats.

There's much more to the story of how Falcon has redefined endpoint protection, but there's only one thing to remember about CrowdStrike: We stop breaches.