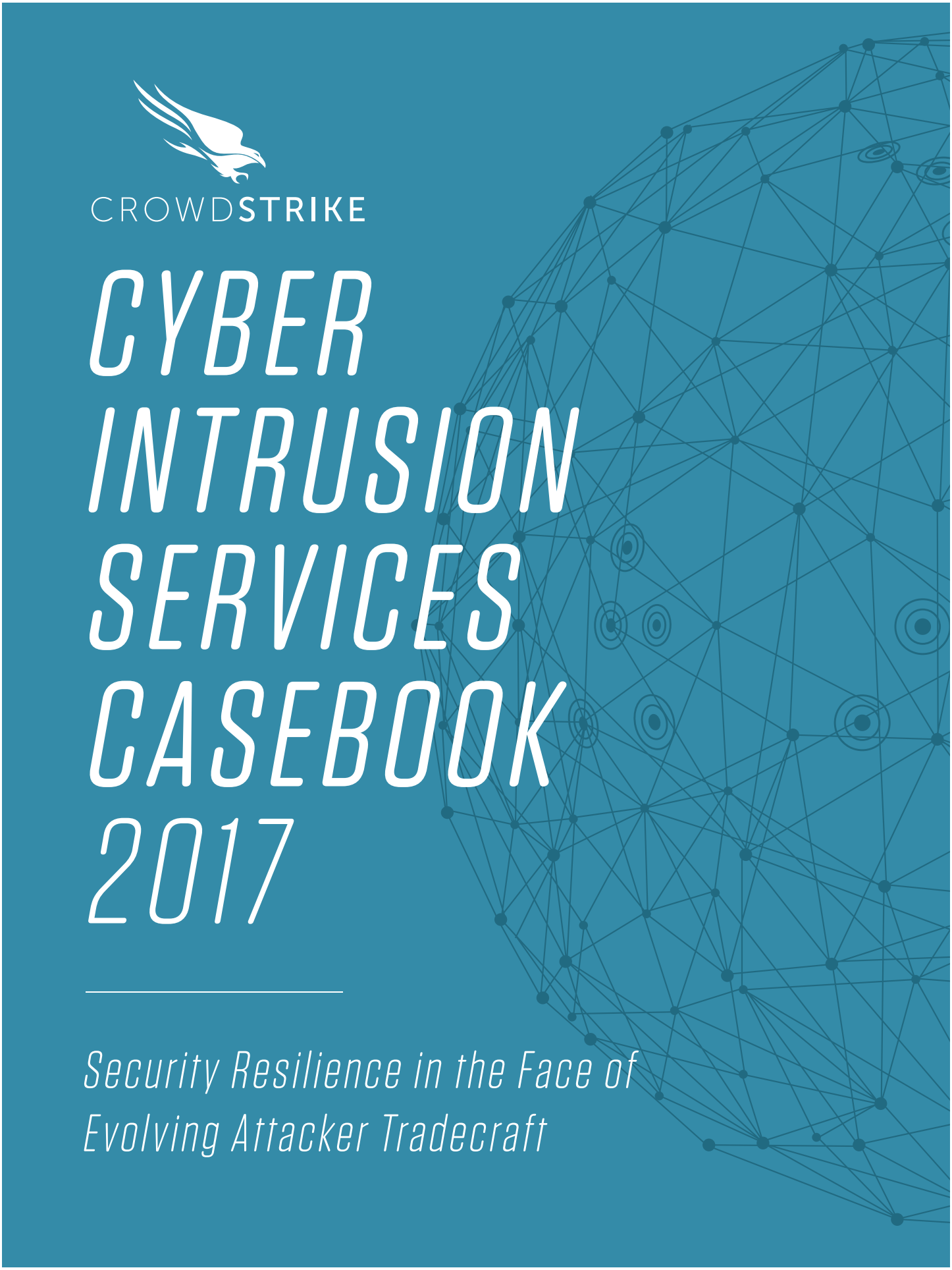


CROWDSTRIKE

CYBER INTRUSION SERVICES CASEBOOK 2017

Security Resilience in the Face of Evolving Attacker Tradecraft

CONTENTS

FOREWORD

Cyberattacks — and the resulting breaches — are a fact of life now. The impact left in the wake of a successful intrusion can be massive when customer data or other confidential information is stolen, exposed, changed, or deleted. It's an inescapable certainty: Where valuable digital assets exist, aggressive threat actors follow.

These actors continuously develop and adopt new means to achieve their objectives, from the destructive NotPetya malware using stealth propagation techniques, to ransomware extortion, to the use of valid operating system processes to exploit the network. Likewise, security stakeholders from CISOs to incident responders to the board of directors must evolve their security planning to ensure resilience in the face of an attack. This document provides guideposts to further you along that path.

Drawn from real-life client engagements, the annual **CrowdStrike® Cyber Intrusion Services Casebook** provides valuable insights into ever-evolving attacker tactics, techniques and procedures (TTPs). It also reveals the strategies the CrowdStrike Services team devised to effectively and quickly investigate and remove threats from victims' networks. Additionally, the report reveals emerging trends observed in attack behaviors, including the preferred tactics used by threat actors to gain entry to the targeted environment.

Based on CrowdStrike Services' extensive experience in the field, this casebook provides key takeaways that can inform both executive stakeholders and security professionals how to respond to intrusions more effectively. Most importantly, it offers recommendations that organizations can implement proactively — right now — to improve their ability to prevent, detect and respond to attacks. The threat is real, the risk is high, and CrowdStrike Services stands shoulder-to-shoulder with our clients to secure their data and their infrastructure: "One Team, One Fight."

Shawn Henry
CrowdStrike CSO and President of Services

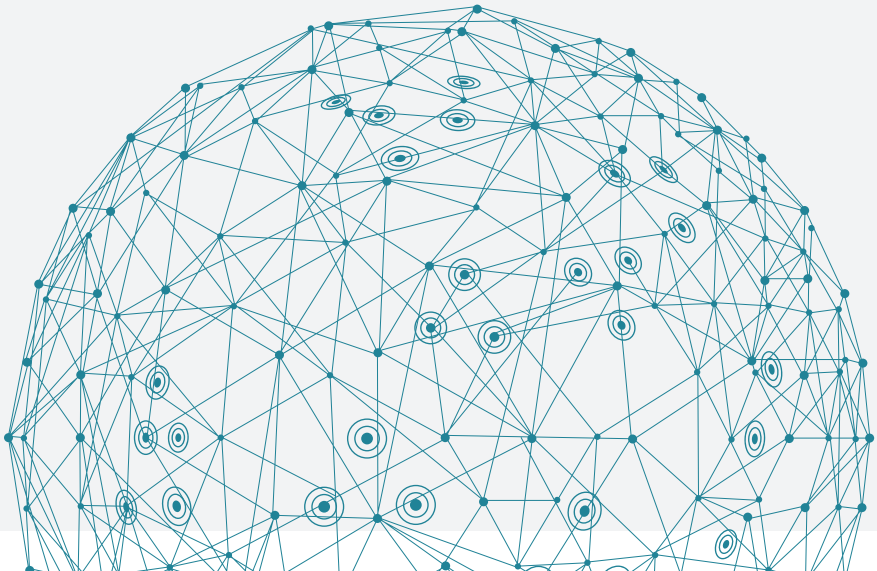
EXECUTIVE SUMMARY

Several key trends emerged from the incident response (IR) cases the CrowdStrike Services team handled on behalf of clients this past year. The team's case summaries and statistics show vividly how resourceful and relentless sophisticated attackers can be as they continually look for gaps in clients' IT infrastructure. Organizations should realize:

1) The lines between nation-state sponsored attack groups and eCrime threat actors continue to blur.

2) Self-propagation techniques have added a new twist to ransomware attacks and their ability to paralyze clients' operations.

These trends make it clear that any organization relying primarily on traditional security measures and tools, such as signature-based antivirus or firewalls, will not be able to detect or fend off determined, sophisticated threat actors. As attackers become more brazen and their attack techniques continue to evolve, organizations must likewise evolve their security strategies to proactively prepare for the next attack.



KEY FINDINGS

Surveying the data points across the many cases CrowdStrike Services worked on the past twelve months revealed the following statistics and key trends. In-depth case studies illustrating each trend follow in this casebook.

Organizations continue to improve their ability to self-detect breaches

The ability to detect an incident soon after it occurs is critical: Of the clients CrowdStrike Services worked with during the past year, 68 percent were able to internally detect a breach — this was an 11 percent increase over the prior year. It reflects organizations' overall efforts to continue maturing their security postures while investing in security tools and resources to detect attacks, including endpoint detection and response (EDR) tools such as CrowdStrike Falcon Insight™.

The average attacker dwell time is 86 days

This statistic reflects the number of days between the first evidence of a compromise and its initial detection. The longer an attacker can dwell in the environment, the more opportunity he has to find, exfiltrate or destroy valuable data or disrupt business operations. In some outlier cases, the team saw dwell times as high as 800 to 1,000 days, but these were exceptions and not the norm. Regardless of dwell time duration, automated systems may eventually detect an intrusion, but by the time human staff is alerted and aware it's often too late: the attackers must be stopped before they can achieve their objectives.

The most prevalent attack objectives

Of the incident response cases where the CrowdStrike team identified a breach type, those listed below were the most prevalent:

- **Intellectual Property (IP) theft**
- **Monetary loss**
- **Personally identifiable information (PII) theft**
- **Ransom or extortion**

The most common attack vectors

Across the IR cases the team handled, the list below shows the most prevalent means by which attackers first gain a foothold in the environment:

Web server, web application, web shell exploits or file uploaders:	37%
Remote access (examples: RDP, VPN):	23%
Supply chain compromise:	12%
Social engineering, phishing, spear phishing:	11%
Cloud-based service exploits, attacks against externally accessible email portals or other unauthorized access:	11%
Reconnaissance only or other:	6%

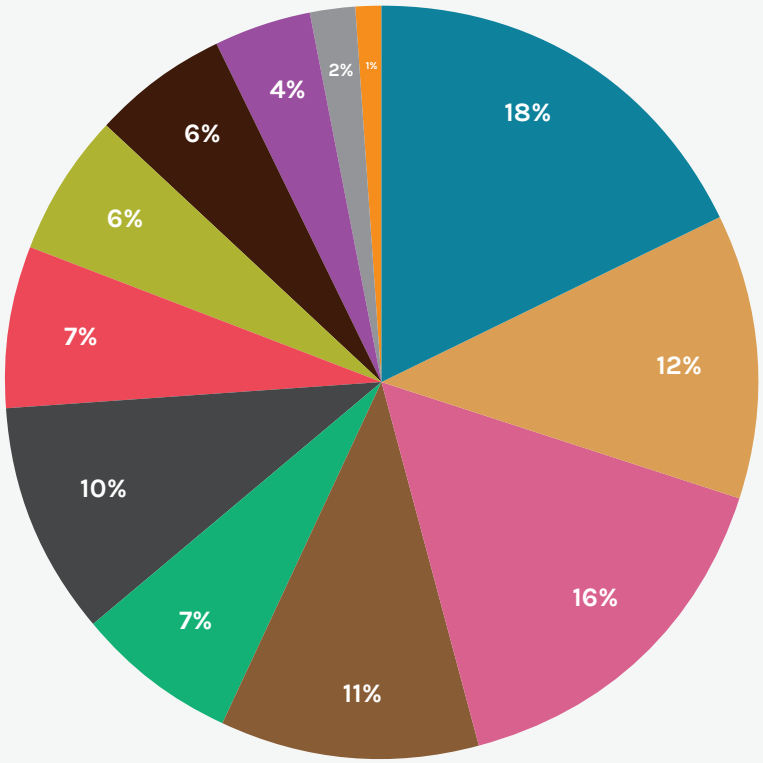
Malware-free attacks made up the majority of attacks — 66 percent

CrowdStrike defines malware-free attacks as those where the initial tactic did not result in a file or file fragment being written to disk. Examples include attacks where code executes from memory or where stolen credentials are leveraged for remote logins. Attackers can also exploit inherent weaknesses in the client IT infrastructure — these present intrusion opportunities for attackers who don't want to leave traces of their trespassing. Fileless attack examples include:

- **Using remote tools like RDP or VPN with compromised credentials**
- **Executing code from memory**
- **Conducting exploits by leveraging inherent weakness in a client's IT stack (e.g., an Apache Struts vulnerability that allows malignant XML to be fed to a Struts server)**
- **Using spear phishing and social engineering to gather credentials**

Industry representation across CrowdStrike IR engagements

The organizations CrowdStrike Services works with vary in size and represent a wide range of industry sectors. However, the conclusions from the data are clear: No organization is immune to cyber intrusions and all must prepare to defend against the next attack.



18%	Retail	12%	Healthcare	16%	Information Technology
11%	Legal	7%	Non-profit/Think Tank	10%	Finance
7%	Conglomerate	6%	Manufacturing	6%	Travel/Hospitality
4%	Entertainment	2%	Insurance	1%	Professional Services

KEY TRENDS

Surveying the data points across the many cases CrowdStrike Services worked the past year revealed two key trends, summarized below. At the end of the summary, each key trend is illustrated by in-depth case studies that include recommendations that may help inform your organization's security strategy.

TREND 1: *The lines between nation-state sponsored attack groups and eCrime threat actors continue to blur.*

CrowdStrike Services cases reveal that eCrime groups increasingly leverage the same tactics and methods used by nation-state actors. These include fileless malware and "living off the land" techniques involving processes native to the Windows operating system, such as PowerShell and WMI (Windows Management Instrumentation). Many also employ anti-forensics tools and methods in an effort to erase signs of their presence and increase dwell time. Brute-force attacks on RDP (remote desktop protocol) servers are also prevalent in these cases.

TREND 2: *Self-propagation techniques have added a new twist to ransomware and destructive attacks and their ability to paralyze clients' operations.*

This year saw ransomware and destructive malware make headlines across the globe. Previously, an infection generally required some sort of user intervention. Now CrowdStrike investigations are seeing malware variants that employ techniques designed to spread once a system is infected. Victim organizations worldwide experienced the repercussions of failing to keep critical systems up to date and relying on ineffective legacy security technologies.

CASE STUDIES AND RECOMMENDATIONS

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

CASE STUDY 01

01

THE CLIENT

A commercial services organization was targeted by an adversary who distributed the SamSam variant of ransomware to systems in the victim's environment. Like other strains, SamSam encrypts files and demands a ransom for a decryption key to unlock the victim's data. This infection had already occurred prior to the CrowdStrike Services engagement.

SITUATIONAL ANALYSIS

Although the client paid the ransom prior to CrowdStrike's involvement, the client sought assistance with preventing the ransomware from spreading to additional systems, and with determining the original point of entry by the attackers.

The SamSam ransomware variant is most commonly associated with xDedic, a Russian-operated darknet forum launched in 2014 that facilitates the buying and selling of crimeware as well as compromised credentials used for accessing RDP servers across government, corporate and university networks. Once a buyer has purchased access to a compromised server via xDedic, the threat actor typically performs fraudulent activities such as ransomware deployment and Bitcoin mining, or uses the compromised hosts as a staging area to mount attacks on other networks.

Since 2016, the CrowdStrike Falcon Intelligence™ team has tracked multiple instances of xDedic tools in use on compromised hosts, including the xDedic RDP Patch, SCClient, SysScan, mustupdate.bat and del.bat.

The criminal operators of SamSam have continued to distribute the threat at a steady pace and in a targeted manner that has allowed them to operate while staying out of the headlines, unlike other ransomware threats such as Locky and Cerber. As with the compromised RDP servers xDedic deals in, previous victims have included organizations in the education, healthcare, government and commercial sectors.

ATTACK TOOLS: AUTOMATED RANSOMWARE AND STICKY KEYS

CrowdStrike confirmed that the malware within the client environment was a variant of the SamSam (aka "Samas") ransomware commonly associated with xDedic. Although designed to automatically encrypt files on a victim's network, SamSam does not provide the attacker with the ability to access, acquire or exfiltrate data from the network.

The investigation by CrowdStrike revealed not only the use of SamSam ransomware, but also:

- **Evidence of RDP and network logon brute-force attacks**
- **Evidence of TTPs connected to the xDedic Russian criminal hacking group**
- **A handful of compromised privileged accounts**
- **Sticky Keys used as a persistence mechanism**

Sticky Keys, a Windows Ease of Access feature, enables keyboard shortcuts such as typing capital letters without pressing more than one key at a time. It can be easily executed from the Windows logon screen and runs with system-level privileges. If an attacker is able to replace the Sticky Keys binary or one of the other Ease of Access binaries, he can gain system-level access without needing to authenticate. A logon via this method also leaves no log records.

Although not a recommended practice, many system administrators use Sticky Keys to retrieve forgotten passwords so they can log into a server: This is most likely the avenue the attacker pursued for his brute-force attacks to gain RDP login credentials.

INVESTIGATION AND ANALYSIS

CrowdStrike worked with the client to deploy the CrowdStrike Falcon® endpoint monitoring agent on several thousand hosts, and the Falcon Forensics Collector (FFC), a tool used to collect drive snapshots for digital forensics, on over 40 hosts within the network. Additionally, the team used a variety of industry standard tools and procedures to conduct forensic analysis.

CrowdStrike's analysis included identifying the root cause of the intrusion that led to the deployment of SamSam ransomware within the client's network. Evidence of brute-force attacks on an RDP server showed it to be the most likely initial infection vector. CrowdStrike also helped identify the persistence mechanism used by the ransomware, allowing the team to prevent it from continued propagation within the customer's network.

The services team used several tactics to determine the extent of the compromise, in addition to hunting for previously unidentified malicious activity in the forensic data. The team looked for evidence of program execution, persistence mechanisms and other artifacts of malicious activity. CrowdStrike also leveraged a known list of indicators to initiate its analysis.

CrowdStrike's comprehensive analysis included examining the following:

- **Forensic artifacts commonly used in IR investigations**
- **Known malicious indicators in each image, including file names and MD5 hashes of malicious software**
- **System registry hives**
- **Artifacts indicating process execution of malicious and benign software**

The analysts also manually reviewed the forensic data looking for other indicators not included above. CrowdStrike determined that an attacker accessed systems within the client environment to create user accounts and to deploy and execute ransomware and batch scripts. Investigators also determined that the attacker's goal was to secure more RDP server logins to sell to other cybercriminal threat actors.

KEY RECOMMENDATIONS

Enforce Network Level Authentication (NLA) for RDP sessions:

Any server that is public-facing on the internet and accessible via RDP should be configured to require NLA for RDP sessions. This would require successfully authenticating prior to receiving the Windows logon screen.

Implement two-factor authentication (2FA) to prevent unauthorized access:

2FA requires users to provide a one-time generated token on a separate device after entering login credentials.

CASE STUDY 02

02

MANUFACTURER SEEKS GUIDANCE TO HARDEN E-COMMERCE WEB SERVER AND DATABASE

THE CLIENT

A manufacturer asked CrowdStrike to conduct investigative forensic analysis on the systems associated with its e-commerce website, provide security recommendations to prevent further access by an attacker, and improve the website's overall security posture.

SITUATIONAL ANALYSIS

When clients are able to detect and remediate an attack on their own, they still often rely on CrowdStrike's expertise in digital forensics, especially when they need to file a cyber insurance claim in the event of a successful attack. Other times, clients seek guidance simply to gain knowledge that can help fortify their security posture and stop the next attack.

In this engagement, CrowdStrike was tasked with investigating and confirming a threat actor's methods and providing recommendations to prevent a future attack.

CrowdStrike learned that in the attacker's attempt to steal and exfiltrate credit card data, network access was gained via a vulnerability in a widely used e-commerce application installed on the client's web server.

ATTACKER TACTICS AND TECHNIQUES

The attacker executed arbitrary image file uploads to the e-commerce web application and injected code into the web server. The attacker uploaded six images, each containing appended PHP code. Of the six uploaded image files discovered, three were unique. Overall, the images included three unique web shells of varying sophistication and functionality.

For example, the first image uploaded contained an encrypted PAS web shell. The web shell requires a password to decrypt and gain access to the web shell functionality. PAS web shell variant capabilities can include command line functionality, SQL database manipulation, file upload/download capabilities and remote shell callouts.

The database server that supported the client's e-commerce web server was compromised due to malicious JavaScript tags the attacker inserted into web page code tables. Those JavaScript tags were designed to execute code that captures and sends credit card information to an external website. The malicious JavaScript code used for credit card theft was hosted on an external server referenced by the JavaScript tags and would only execute in a customer's browser.

INVESTIGATION AND ANALYSIS

CrowdStrike conducted forensic analysis during the investigation to gain a comprehensive understanding of the compromise, reveal attacker activity and identify data exposure. During the process, CrowdStrike analyzed two web server images, one running the e-commerce web application and another hosting the corresponding database server.

The digital forensics investigators leveraged several tactics to hunt for known and previously unknown malicious activity in the forensic images. To reach this goal, CrowdStrike analyzed various artifacts, including:

- **Command history**
- **MySQL history**
- **Remote connections**
- **Web access logs**
- **System logs**
- **Scheduled cron jobs**
- **Filesystem metadata**
- **Malicious scripts**
- **Users and privileges**
- **E-commerce web app logs**

Analysis by the CrowdStrike team determined that even though the attacker had access to both the web server and the underlying database, the compromised database did not contain customer credit card data. In addition, the client's network was architected so credit card data was not stored on the impacted web server.

However, the attacker did have access to customer identification information, including names, physical addresses, email addresses and phone numbers. Based on forensic analysis, CrowdStrike determined that the attacker acted within a matter of days.

KEY RECOMMENDATIONS

CrowdStrike provided the client with recommendations, much of it focusing on hardening and improving the resilience of the client's e-commerce web application implementation and its supporting database. The recommendations included:

Improve vulnerability patch management:

Applying vendor-supplied patches to commercial web applications can shore up known vulnerabilities. When encountering an unknown vulnerability, inform the software vendor so it can work to address the issue and provide a patch. If using an old or unsupported version, upgrade to a supported application that will be patched and updated by the vendor as new security vulnerabilities are discovered.

Institute File Integrity Monitoring (FIM):

This assists with future identification of maliciously altered files. Simple FIM can be implemented by creating an MD5 hash of core files and comparing the known-good stored hashes with the current hash of a file. Additionally, there are several open-source and commercial FIM products that can perform this function in a more automated fashion.

Implement an endpoint detection and response (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. Implementing a tool such as CrowdStrike Falcon Insight EDR increases the chances of detecting attacker activity within the network, and accelerates your ability to respond when suspicious activity occurs. Because log and core system files are critical to the integrity of the system, there is overlap between FIM and EDR tools. However, the additional monitoring of events and processes provided by an EDR tool is vital to host security.

Rebuild compromised e-commerce web servers and databases:

Rebuilding this system ensures any backdoors or malicious code that may have been placed on the system by the threat actor are removed.

Reset passwords for compromised systems:

Reset all account passwords on the web servers and databases. Additionally, clients should utilize a "least privilege" principle for all accounts on their web servers and databases. This ensures that only users with a critical business or application need have administrative access.

Enable database logging for both transactions and slow queries:

- **Transactions:** Transaction logs record actions taken on the database associated with a user and timestamp. These are valuable from both an auditing and investigation perspective, and should be reviewed to determine if any suspicious queries are performed.

- **Slow queries:** These logs record any queries that are taking more than the average amount of time to complete. These are valuable from both an auditing and investigation perspective, and should be reviewed to identify any suspicious queries that take an unusually long time to complete.

Perform web application penetration testing:

This should be performed on at least a biannual basis to ensure that a web application is patched and secure. The testing should be conducted by a third party with the goal of identifying any unpatched vulnerabilities on the web application or the system running the web application.

Perform database and webroot review:

The attacker placed malicious code inside both the database and the web server webroot directory that attempted to identify and send payment card information out of the client environment. Establishing a clean baseline database image ensures these systems are free of malicious code or suspicious data.

CASE STUDY 03

03

RETAILER'S POINT-OF-SALE SYSTEM COMPROMISED BY A FILELESS ATTACK

THE CLIENT

CrowdStrike Services is often engaged by clients to perform compromise assessments to determine if an attacker has gained entry. In this engagement for a large retailer, CrowdStrike found an attacker present in the client's environment and pivoted to IR mode to identify the attacker.

SITUATIONAL ANALYSIS

While conducting a compromise assessment to determine the status of the client environment, the CrowdStrike team uncovered a suspicious forensic artifact: an anomalous process that had executed out of a system drive, but on just two systems. FFC picked up this process as it occurred and long before the client environment was examined.

The team traced the process back to a suspicious service where PowerShell was used to push out a memory-only Metasploit implant. Tracing backward, it became apparent that this PowerShell code stub had been pushed to all point-of-sale (POS) systems on the client's network of more than 14,000 systems and 160 controllers. Further review of the implant revealed it to be RAM-scraping malware.

The attacker implemented the attack in two stages that compromised hosts within the client's credit card processing systems. Subsequent intrusions occurred after the adversary lost access and returned by dropping malware via a spear-phishing campaign. The key attack method utilized Windows Services to execute code in a lightweight manner that did not alert users or leave artifacts, except for event log and registry entries. The attacker also started and stopped Windows Services remotely.

ATTACK TACTICS AND TECHNIQUES

The first evidence of compromise of card-processing POS endpoints occurred over several days as the FrameworkPOS malware launched scripts that ran on two POS hosts. The same script ran three times at 30- to 40-minute intervals in the previously identified hosts and several additional POS hosts over two days. Additionally, the attacker performed Active Directory information collection from a separate host. A day later, the same POS hosts executed the launching script again.

The next month, another host showed signs of compromise for the first time, via installation of a PowerShell implant that injected a simple backdoor into the running powershell.exe process. This host was identified as an "orchestration system," one of the few points where the client's corporate and franchise domains were bridged. This appeared to be the attacker's favored staging point, and for 12 days, over 14,000 hosts in the client network had the launching script installed from this host.

CrowdStrike then discovered strings matching the format recorded by the FrameworkPOS malware in an unallocated space on the orchestration system. As these files were completely unallocated, no metadata was available to determine when the files were created, modified or ultimately deleted. This data was provided to the organization so it could match the recovered data with transaction information and determine when this data was recorded. It is important to note that the captured data did not originate on this host; the decoded data contained the hostnames of the various POS and controller hosts in the client environment where the capture did occur. This means that at some point prior to deletion, the attacker:

- **Copied the captured data from the endpoints to the orchestration host**
- **Subsequently deleted this data**

NON-MALWARE TECHNIQUE USED TO VALIDATE DATA DUMPS

To confirm the length of their credit card dump files, the threat actor used cgwin.exe, a word count utility, to determine the length of a data dump file by counting characters, words and lines.

The attacker also leveraged RemoteExec, an open-source Windows utility, to execute commands remotely on hosts. Similar to PSExec, RemoteExec only requires the appropriate credentials to run commands remotely. AdFind was used for Active Directory enumeration, while 7-Zip was used to make archives of the Active Directory data.

KEY RECOMMENDATIONS

- ### *Implement end-to-end encryption to secure all POS transactions:*

  End-to-end encryption of transactional data prevents the immediate exploitation of stolen payment card data: In this case, the amount of card data compromised and the economic damage to the client was minimized.

Ensure log archives are created, and make use of them as necessary:

Centralized logging was in place, but may not have been set up or used properly. Disk space issues were prevalent, and days of event logs went missing, so CrowdStrike could not track adversary movement on those days.

Train the staff to avoid spear phishing, but know that such training won't totally prevent it:

This is especially true at any organization where the staff must read and receive emails from senders outside the organization.

Log full PowerShell commands:

This can be done by using a group policy to turn on logging for PowerShell and capture the full command line input.

Upgrade to PowerShell v5 +:

Microsoft greatly improved the logging capabilities with PowerShell by enabling script block logging and auditing. Script block auditing captures the full command or contents of the script — including who executed it and when it occurred — and it is helpful in piecing together actionable PowerShell activity.

Don't rely on traditional antivirus-only endpoint offerings:

The implants were strictly PowerShell-based, and when executed would not have been detected by traditional signature-based antivirus offerings. A solution such as Falcon Insight EDR can detect implants that utilize PowerShell.

CASE STUDY 04

04

SELF-PROPAGATING DESTRUCTIVE MALWARE DELIVERED VIA SUPPLY CHAIN ATTACK

THE CLIENT

The company was infected by NotPetya in June 2017, as were many other organizations around the world. From a geopolitical context, this client was ensnared in a campaign against organizations doing business in Ukraine.

SITUATIONAL ANALYSIS

NotPeya has been covered extensively in the media since the initial widescale attack on June 27, 2017. CrowdStrike has shared its research findings with the wider security community and encourages you to read the blog entries about NotPetya at www.crowdstrike.com/blog.

In this engagement, the client determined that a subset of its computer systems had been infected by the malware, based on a review of data in its log management system and reports from its employees. As soon as the client became aware of the situation, it took measures to contain the incident and assess the extent of the impact on its network. Part of those measures included engaging CrowdStrike.

The CrowdStrike Services team was tasked with determining the type of malware, the initial infection vector, the propagation methods used by the malware, and the scope and impact of the incident.

Containment steps the client took within an hour of learning of the attack included:

- **Disabling network connectivity for nearly all systems, including systems that were not compromised by the malware**
- **Iteratively disabling DNS, DHCP, various communication ports and other access and connectivity points**
- **Powering down impacted systems**

INVESTIGATION AND ANALYSIS

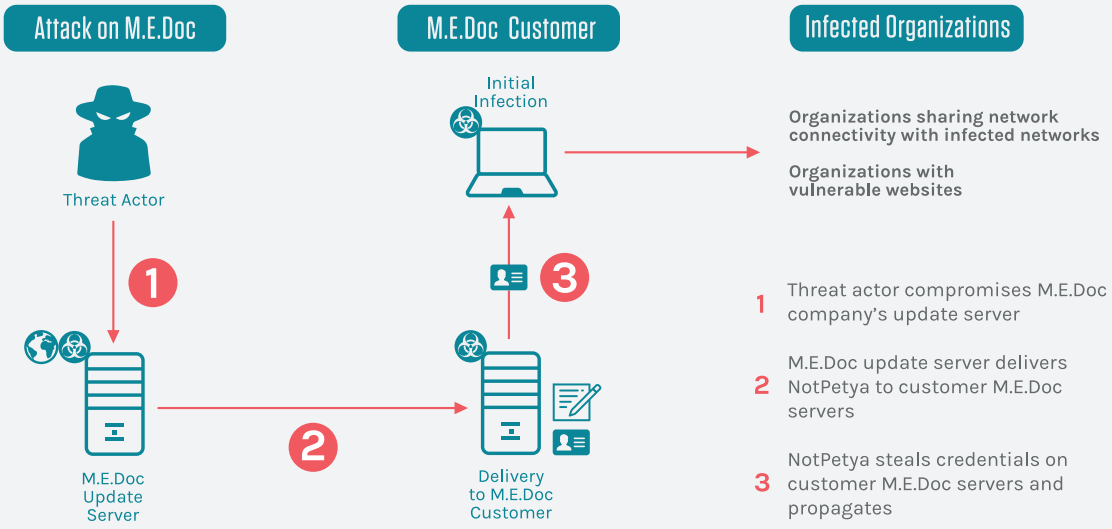
CrowdStrike reviewed relevant forensic system images and client-provided documents, conducted employee interviews, and performed analysis of data with the CrowdStrike Falcon platform, as well as the FFC data. CrowdStrike worked with the client to deploy the Falcon platform throughout the client environment to more than 14,000 workstations, 4,000 servers and 150 domain controllers, providing near real-time visibility into the IT environment.

The team also deployed FFC across business units on both Windows and Linux systems, providing the team with visibility into past events within the company environment.

CrowdStrike also analyzed the malware, identifying it as NotPetya. The NotPetya malware originated as a Trojan embedded in an update to the M.E.Doc software, accounting software used to interact with Ukrainian tax systems and created by Intellect Service, a Ukraine-based company.

M.E.Doc leverages an automatic update function to download specially formatted executables from the software developer's web server. A threat actor infiltrated the update process and maintained access during the spring of 2017. Several update executables on the developer's servers contained components with backdoor code. This update enabled an attacker to push malware onto the systems of M.E.Doc users, as shown in the following diagram.

NotPetya Outbreak Initial Infection



The NotPetya malware self-propagated leveraging PsExec, WMI and Server Message Block (SMB) vulnerabilities. Technical review of client firewall configurations confirmed the ability for the malware to propagate via these three mechanisms.

CrowdStrike used several techniques to hunt for malicious activity within the data collected. The analysts looked for evidence of program execution, persistence mechanisms, items that appear infrequently, and other artifacts of malicious activity. Utilizing these methods, the team sought to identify previously unknown malicious or suspicious files across the analyzed hosts in the client's environment.

NotPetya Outbreak Propagation

Step 1: Malware drops DoublePulsar and extracts credentials via Mimikatz

Step 2: Malware attempts to gather a list of known systems and IP addresses

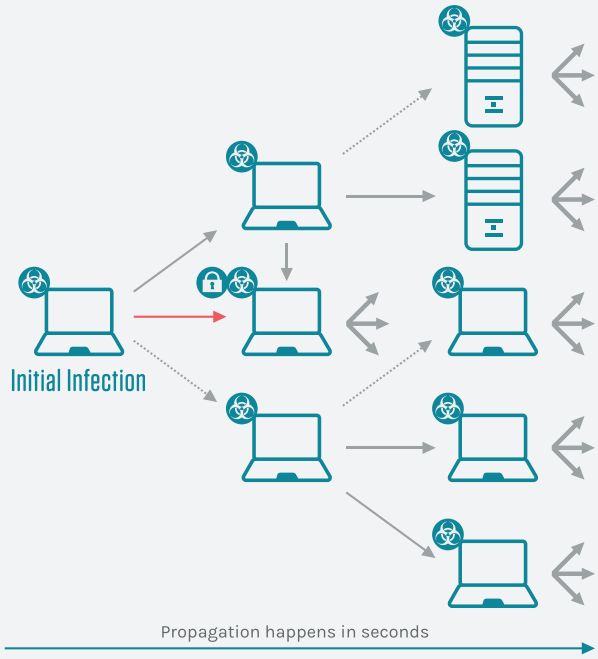
Step 3: Malware attempts to propagate using credentials

Step 4: If credentials fail, malware attempts CVE-2017-0144 (EternalBlue & EternalRomance) exploits

Step 5: Systems encrypt 65 specific file extensions and reboot themselves

Legend

- **Unsuccessful login or exploitation**
- **Successful login**
- **Unsuccessful login, successful exploitation**



As for the scope and impact of the attack, CrowdStrike confirmed that more than half of the client's systems were impacted by NotPetya and that the malware compromised several hundred sets of credentials.

The various system and log data CrowdStrike analyzed to investigate attacker activity revealed the following indicators of compromise:

Indicators:

- **Creation of pefc.dat and dllhost.dat files**
- **Scheduled task to shutdown the system and/or execution of shutdown.exe**
- **Successful/unsuccessful logon by a compromised user account during the event**
- **Windows Security Event Log being cleared during the event**
- **AV alerts**
- **Operating system installation date after the event**

KEY OBSERVATIONS

The technical and strategic successes of the client in successfully limiting the impact of the NotPetya attack were due mainly to the client's network architecture. Additionally, CrowdStrike made several observations related to process and technology that are germane to improving the client's overall information security posture. These observations were drawn with reference to the SANS Institute's 20 Critical Security Controls.

The particular observations listed below collectively illustrate the state of the environment as it existed during the time of the incident. The categories of observations below describe where opportunities for security enhancements were found:

Account management and access control:

In some instances, IT departments grant user accounts more permissions than necessary to accomplish the tasks germane to each user's job function. In doing so, IT staff increase the attack surface that adversaries can leverage to gain a further foothold into the network. CrowdStrike recommends implementing improved access controls over corporate applications by providing unique credentials to each user who requires access. Additionally, shared accounts should be restricted. Lastly, the client's IT staff should avoid the use of the local administrator account on Windows, the root account on Mac, and the root account on Linux for daily tasks not requiring elevated privileges.

System hardening:

Similar to the provisioning of user accounts, granting users high levels of access and privilege on systems often is seen as conducive to creating an agile, nimble computing environment. However, this may have unintended consequences. Advanced attackers know how to use privileges to move laterally through a network and establish a strong foothold within the environment. The client should work toward the prevention of users operating as administrators on their local machines, and research the many applications that allow privilege management of workstations. Such strategies allow users to have the necessary freedom to work while still providing balanced security that can help mitigate targeted attacks.

Critical asset identification:

The client organization comprises a variety of business units that retain a wide range of intellectual property. Such potentially high-value targets may require additional security controls. The client should make a determination of which business units and intellectual property, if lost or damaged, would harm the organization's reputation or cause business disruptions. This may include identifying where that data resides, including the specific departments within the company.

Patch management:

Patching of applications and operating systems is a significant step in reducing the attack surface of computing assets within an organization. Implementing solutions to provide a centralized patch management system that encompasses as many applications as possible within one product will address vulnerabilities as soon as a patch is issued by a software vendor. It also allows for easier maintainability of the patching system, as well as a more complete reporting and audit location.

Network visibility:

Malware commonly uses DNS to resolve domain names to the desired command and control servers. Gaining visibility into the domains being resolved on the network can lead to the identification of other compromised hosts and improve overall understanding of the size of the compromise. DNS servers should log all resolution requests to a centralized platform, and those logs should have attacker-owned domain names queried against them to reveal evidence of compromise. The client was encouraged to invest in packet capture and analysis systems, as attackers have moved to encrypting their communications over standard ports.

Disaster recovery and business continuity plans:

In an environment as complex and dynamic as this client's, constructing a disaster recovery plan is no small undertaking. As a safeguard against natural and man-made disasters, it is important to consider backing up sensitive data to an offsite location.

Additionally, plans for these types of events will help to bring the business back online as quickly as possible. These plans may focus on virtual business work streams such as engineering, sales and customer service, as well as physical business work streams, e.g., the engineering and production areas. Backing up important data in a dedicated offsite location can prevent the loss of intellectual property should an organization experience the total loss of a production facility.

CONCLUSION

The above cases share several common traits that security stakeholders in any organization should be mindful of as they continually evaluate the staff, processes and technology they've put in place for security resilience:

- ## *Threat actors have many attack vectors to exploit in their quest to penetrate a target environment:*

  Defending against the variety of tactics attackers can leverage to penetrate your defenses requires a multi-faceted approach to security planning and strategy. There is no single "magic bullet" that will stop determined adversaries.

- ## *Resiliency in the face of ever-changing attacker tactics requires new means to detect and prevent attacks:*

  Traditional signature-based antivirus endpoint offerings will not stop advanced intrusion methods, many of which are now fileless and execute from memory or utilize known system processes.

- ## *Ensure vulnerabilities are patched quickly and effectively:*

  Threat actors leverage weaknesses in key IT systems, both those known and newly discovered — when vendors release patches to address vulnerabilities, ensure those patches are applied properly.

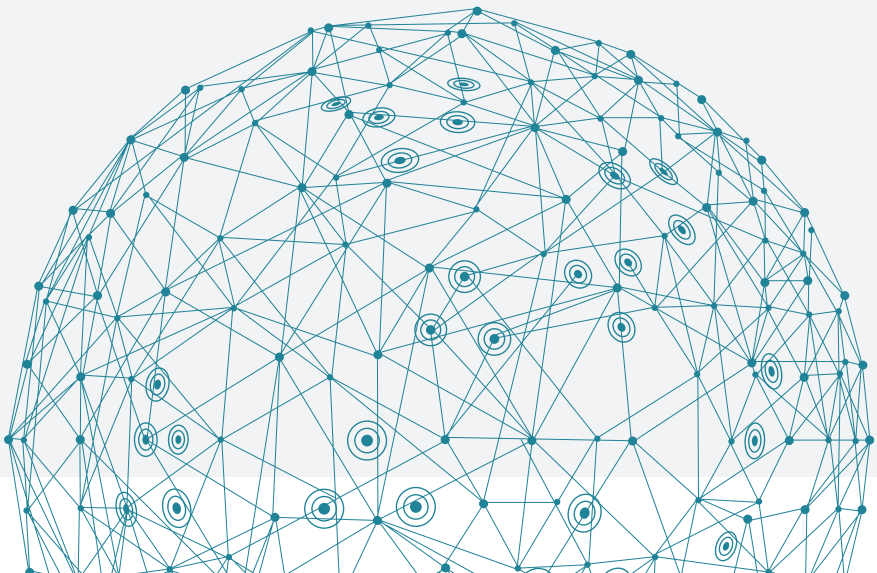
- ## *Account management and access control remain critical pieces of an overall security posture:*

  Know what resources user accounts can access, what permissions they possess and prevent unauthorized network and application access with two-factor authentication.

Preparing to deal with the next attack is an integral part of managing risk. Security professionals' knowledge can be deep and wide, but can never be comprehensive enough to encompass every unknown facing their organizations. We encourage you to learn more about how the experts of CrowdStrike Services can help identify potential unknowns and other gaps in your people, tools and processes and to ultimately fortify your organization's cyber resilience.

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 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.



ABOUT CROWDSTRIKE

CrowdStrike® is the leader in cloud-delivered endpoint protection. The CrowdStrike Falcon® platform offers instant visibility and protection across the enterprise and prevents attacks on endpoints on or off the network. The CrowdStrike Falcon platform deploys in minutes to deliver actionable intelligence and real-time protection from Day One. Falcon 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 cyberattack types, using sophisticated signatureless artificial intelligence/machine learning and indicator-of-attack (IOA) -based threat prevention to stop known and unknown threats in real time. Powered by the CrowdStrike Threat Graph™ database, Falcon instantly correlates over 70 billion security events 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.

EXPERIENCED A BREACH?

Call 855.276.9347

www.crowdstrike.com/services