CYBER INTRUSION SERVICES CASEBOOK 2016
CONTENTS

FOREWORD ................................................................. 02

EXECUTIVE SUMMARY .................................................. 03

KEY TRENDS ............................................................... 04

CASE STUDIES AND RECOMMENDATIONS ..................... 06

FALCON OVERWATCH: REVEALING THE LATEST ADVERSARY TRADECRAFT ........................................ 22

ABOUT CROWDSTRIKE ..................................................... 25
The year 2016 marked several notable milestones – not only for CrowdStrike, but the entire cybersecurity arena. We’ve seen unparalleled attacks on government agencies, critical infrastructure operating systems, and Fortune 500 companies spanning all industries and many countries. These attackers are not only becoming smarter, they’re also becoming more patient than ever – infiltrating a system, spending months performing undetected reconnaissance, and striking at the perfect (or to the victim – the most imperfect) time possible.

My primary mission as an FBI executive with oversight for the Cyber Program was to detect digital threats, identify the actors posing those threats, and to mitigate them to protect national assets and intellectual property. In my unique position now as both President of Services and Chief Security Officer at CrowdStrike, I have the responsibility to ensure that corporate security infrastructure can stand up to these attackers – in many cases, the same adversaries I became so familiar with while in the government. These nation-state actors and organized cyber-criminal enterprises are well funded, well trained, and have a very specific target in mind: disrupting and dismantling your organization.

The 2016 CrowdStrike Cyber Instrusion Services Casebook examines several incident response and remediation cases we’ve worked over the past year, some very high-profile. It discusses trends we’ve identified and emphasizes the need for proactive and real-time monitoring services to establish an effective cybersecurity posture. This report also underscores that our unique combination of forensic experts and a vast threat intelligence network, coupled with our flagship endpoint protection platform, are key to expeditious and successful incident response and remediation.

Shawn Henry
CrowdStrike, CSO and President of Services
Despite increased spending on cybersecurity in 2016, CrowdStrike Services saw targeted intrusions continue as sustained and ever-present challenges for organizations across both the private sector and government-related organizations, such as the Democratic National Committee (DNC). Moreover, the tactics and methods adversaries use display an absolute brazenness and determination to penetrate client environments and safeguards regardless of attackers’ motivations.

The content of this report draws upon CrowdStrike’s incident response team’s daily work: these stories “from the trenches” not only offer insights into the real-life attacks perpetrated against large organizations across various industries, but also detail how our team works effectively with clients to identify and eject attackers.

Extensive experience helping clients respond quickly and effectively to stop breaches reveals information that security professionals — from CISOs to SOC managers — can leverage to inform their own response planning, and defend against similar attacks in the future. To this end, the report also provides recommendations for proactive steps organizations can take to improve their success rate in preventing, detecting and responding to these attacks.
Surveying the data points across the many cases CrowdStrike Services worked during the past 12 months revealed three key trends. In-depth case studies illustrating each trend follow in this casebook.

**TREND 1: Attackers are Increasingly Using Anti-Forensic Tools to Cover Their Tracks**

Attackers are taking greater steps to hide their activities from traditional investigative tools and methodologies. This trend highlights the need for organizations to employ investigative digital forensics experience combined with the real-time monitoring and detection capabilities that an endpoint detection and response (EDR) solution provides. Specific anti-forensic tools common to cases CrowdStrike worked include Sdelete, log clearing, timestamp alteration and data encryption.

- **SDelete** is a command line utility that offers a number of options. In any given use, it allows for deleting one or more files and/or directories, or cleansing the free space on a logical disk.

- **Log clearing**, as the name implies, is a method of removing the recording of system events that would allow a security team to backtrack what may have caused a security incident. In a Windows environment, for example, log clearing could be used to erase security logs that record each event as defined by the audit policies set by an organization’s IT department.

- **Timestamp alteration** helps attacker tools better blend with existing files on the system to which they are copied. By changing timestamps, an attacker aims to defeat timeline analysis conducted around the time of known attack activity and help reduce timestamp anomalies when tools are placed in operating system folders.

- **Data encryption** is often employed by adversaries during the objectives and exfiltration stages of an attack. As an example, encrypted archives are commonly used to obscure the source of stolen data and frustrate attempts at conducting damage assessments.

▼ See supporting Case Studies 1 and 2 beginning on page 06
**TREND 2:** Third-Party Trust Relationships Introduce Significant Risk to the Enterprise

Any organization with a distributed business model needs to assess security processes in place at field offices to prevent unauthorized access. The franchise model, for example, is highly susceptible to intrusions since enterprise security is dependent on both the IT systems in place and the security practices (or lack thereof) at the franchisee level of operations.

In several cases, our team identified credit card data theft due to compromises at the franchisee level of operations. These compromises also negatively impacted the corporate networks of the “parent” company. Examples of tactics that exploit poor security processes and user authentication management include:

- **Compromised** remote desktop software credentials to remotely access other hosts
- **Point of sale (POS)** malware introduced in various ways

**TREND 3:** Malware-Free Intrusions are Now the Norm as Attackers Increasingly Use Trusted System Processes to Execute Exploits

Any exploit that utilizes a trusted Windows system process will almost certainly evade traditional endpoint security measures. This includes both PowerShell and Windows Management Instrumentation (WMI), among others. Increasingly, our team sees threat actors using virtually no malware in their attacks as they rely more and more on such trusted processes. Utilizing an endpoint protection platform such as CrowdStrike Falcon, which is designed to be effective against both malware-based and malware-free attacks, our team was able to quickly identify a wide variety of malicious activities. Combined with implementing more stringent IT management practices, the team prevented numerous entry attempts by attackers using this approach. Specifically, these attackers utilize the following methods, among others:

- **Using PowerShell** as a “staging” tool to execute other scripts to compromise a system
- **Using WMI** to install backdoors for persistence, which allows the adversary to launch malicious code automatically after a specified period of system uptime or according to a specific schedule
- **Some commodity malware** is also sophisticated enough to propagate through network shares and, via polymorphism, change hashes so they slip by traditional anti-malware endpoint detection systems

All three trends underscore the necessity of having a security plan that is revised and tested regularly to surface weakness that would allow these tactics to persist and compromise an environment. The following cases illustrate these trends in-depth.

▼ See supporting Case Studies 1, 2 and 3 beginning on page 06
CASE STUDY #1

Democratic National Committee

Of the cases covered in this report, this is the only one with client attribution. Clients turn to CrowdStrike Services for our team’s deep expertise in digital forensics, incident response and remediation. But perhaps the most important reason they come to us is simply this:

Trust.

Our clients trust that CrowdStrike will keep their confidential information private. This means we operate under strict confidentiality rules with our customers, and we jealously guard their identities.

However, in this rare case, the Democratic National Committee (DNC) asked CrowdStrike to share publicly information about the adversary tradecraft so that other organizations can benefit from this information and protect themselves more effectively.
SITUATIONAL ANALYSIS

The DNC, the formal governing body for the U.S. Democratic Party, called CrowdStrike at the end of April 2016 to perform a compromise assessment on their corporate network and determine if any breaches had taken place. CrowdStrike immediately deployed our Falcon Host next-generation endpoint security technology across the corporate environment, which rapidly picked up adversary activity on a number of systems within the network, triggering the transition into an incident response engagement. CrowdStrike Services deployed resources to determine the full scope of the incident, monitor for ongoing attacker activity, and support the DNC’s remediation efforts.

CrowdStrike’s primary objectives in this engagement were to:

- Identify the nature and scope of the compromise
- Determine whether data was exfiltrated from the DNC environment and the extent of any exfiltration discovered
- Plan and assist in implementation of the remediation of the DNC environment and eliminate the adversary from the corporate network

ORDER OF EVENTS

- During its investigation, CrowdStrike identified evidence of intrusions by two separate Russian state-sponsored actors - COZY BEAR and FANCY BEAR.
- Through forensic analysis, CrowdStrike identified evidence of data staging shortly after the initial intrusion by FANCY BEAR, in preparation for data exfiltration.
- Remediation efforts to improve visibility, harden the environment, and remove the adversaries were conducted in early June 2016.

Leveraging a deployment of CrowdStrike Falcon, the CrowdStrike Services team found two sophisticated attackers with a nexus to the Russian Federation, both utilizing anti-forensics techniques and tools in an attempt to cover their tracks.
COZY BEAR

The sophisticated Russian-state sponsored threat actor COZY BEAR was observed by CrowdStrike operating elsewhere as early as 2014. This actor has many other names in the information security community, including APT-29, Office Monkeys, CozyCar, and CozyDuke. Unlike many of the dozens of individual nation-state actors that the CrowdStrike Falcon Intelligence team monitors, COZY BEAR tends to cast a wide net, sending out thousands of phishing emails to a broad set of targets. This is notable, as most nation-state attackers tracked by CrowdStrike prefer to conduct more focused operations against smaller sets of targets.

COZY BEAR is flexible and changes tool sets frequently. The actor’s implants have included those designated as SeaDaddy, MiniDionis, and AdobeARM RAT. In terms of post-exploitation operations, COZY BEAR is aggressive, using the latest components of the target operating system to hide from antivirus and host-based security tools.

FANCY BEAR

The Russian nation-state adversary group known as FANCY BEAR has been observed by CrowdStrike operating in many organizations since the mid-2000s and represents a constant threat to a wide variety of organizations around the globe. The adversary targets aerospace, defense, energy, government, media, and dissidents, using a sophisticated and cross-platform implant.

FANCY BEAR’s code has been observed targeting conventional computers and mobile devices. To attack their victims, they typically employ both phishing messages and credential harvesting using spoofed websites.

This threat actor has demonstrated the ability to run multiple and extensive intrusion operations concurrently. At the time the DNC intrusion was occurring, this actor was involved in extensive operations targeting European military organizations.

This threat actor has been observed targeting victims in multiple sectors across the globe. Because of its extensive operations against defense ministries and other military victims, FANCY BEAR’s profile closely mirrors the strategic interests of the Russian government, and may indicate affiliation to the Main Intelligence Department or GRU, Russia’s premier military intelligence service.
This adversary has dedicated considerable time to developing a primary implant known as X-Agent, and also leverages proprietary tools and droppers such as X-Tunnel, WinIDS, Foozer and DownRange. Their main implant has been ported across multiple operating systems for targeting conventional computers as well as mobile devices. This group is also known for registering domains that closely resemble domains of legitimate organizations they plan to target, to establish phishing sites that spoof the look and feel of the victim’s web-based email services, with the intention of harvesting their credentials. FANCY BEAR has also been linked publicly to intrusions into the German Bundestag and France’s TV5 Monde TV station in April 2015.

The initial infection vector COZY BEAR utilized is unknown and was not revealed through the course of CrowdStrike’s forensic investigation. However, CrowdStrike’s threat intelligence indicates that the DNC breach could be the residual result of a large-scale phishing campaign orchestrated by this threat actor in Summer 2015. This was likely the means used to trick DNC employees into downloading the initial payload, or stage one of a two-stage implant. By the time CrowdStrike Services was called in to investigate, COZY BEAR had moved onto executing stage two of their implant, which was a WMI backdoor. This was one of two mechanisms they used to maintain network persistence.

The other backdoor utility COZY BEAR utilized was the well-known SeaDaddy implant, developed in the Python scripting language and compiled with py2exe. Their second means of maintaining access was through a PowerShell bootstrap implant. This implant is a modular framework that initially gives the attacker only rudimentary access to the system. But when directed, the implant can install modules by interacting with the Windows Management Instrumentation (WMI) database. This allowed the adversary to launch malicious code automatically after a specified period of system uptime or on a specific schedule. The PowerShell backdoor is simple yet powerful. It consists of a single obfuscated command that sets it to run persistently.

As is the norm for any nation-state adversary, once inside the victim’s environment the attackers attempted to escalate their access and maintain their foothold in the network as they acted on their objectives.
FANCY BEAR used different tradecraft, deploying X-Agent malware with capabilities to do remote command execution, file transmission and keylogging. It was executed via rundll32 commands. In addition, FANCY BEAR’s X-Tunnel network tunneling tool, which facilitates connections to environments that are hidden from the public with Network Address Translation (NAT), was used to also execute remote commands. Both tools were deployed via RemCom, an open-source replacement for PsExec available from GitHub. They also engaged in a number of anti-forensic analysis measures, such as periodic event log clearing and resetting timestamps of files. X-Agent and X-Tunnel files are compiled as either executables or dynamic link libraries. Both implants are fully featured modular frameworks that give an attacker the ability to upload, download, and execute additional modules. Additionally, in some variants, the adversary can use a secure shell capability to establish a connection or exfiltrate data. Both malware variants have been associated with FANCY BEAR during previous CrowdStrike Services client engagements.

Once the attackers have domain or administrative credentials, they can perform actions on remote machines, allowing for further lateral movement in the network.

ATTACKER MOTIVATION

Based on the data exfiltrated from the DNC, one of FANCY BEAR’s goals appears to have been to collect opposition research the DNC’s research staff had gathered on President Elect (then Republican primary candidate) Donald Trump and other Republican (GOP) presidential candidates. By the time CrowdStrike started incident response work, this threat actor had already stolen data from the network.

One of COZY BEAR’s objectives appears to have been the collection of communications intelligence by targeting servers facilitating email and VOIP communications.

Falcon OverWatch, CrowdStrike’s 24/7 managed hunting team, assisted in the incident response. The OverWatch team saw attacker activity as it occurred with “over the shoulder” observation of “hands on keyboard” as command line activity occurred. This real-time information provided the CrowdStrike Services team with additional indicators of compromise to examine, which in turn helped reveal what the attackers were trying to accomplish.
The CrowdStrike Services team’s forensics work revealed that once COZY BEAR carried out its two-stage intrusion, the adversary then leveraged Sdelete to clean up the stage-one backdoor and downloader, of which our team saw evidence in ShimCache. ShimCache (or AppCompatCache) is used by the Windows Operating System to identify application compatibility issues. This registry key holds the full file path and last modified timestamp of files executed. Based on CrowdStrike’s experience and the names of these files, FANCY BEAR appears to have performed credential dumping, reconnaissance, remote command execution, exfiltration staging, keylogging and lateral movement when accessing a key shared drive within the DNC network.

CrowdStrike’s approach to remediation included advising the DNC IT team to re-image a large number of systems within the DNC environment and to create a new domain. Additionally, new security controls were put in place to harden the environment from reinfection and ensure the confidentiality, integrity, and availability of DNC services and operations. The DNC team had also deployed CrowdStrike’s Falcon Host endpoint technology in support of this effort, putting continuous monitoring and prevention capabilities in place on DNC endpoints.
The DNC example suggests several steps any organization can take to lock down its network environment and prevent unauthorized access by sophisticated adversaries. These recommendations include:

- Focus on credential management and require both two-factor authentication (2FA) at time of logon and re-authentication at regular intervals such as every four or 12 hours.

- Deploy real-time visibility, detection and prevention abilities that a next-generation AV and EDR solution such as Falcon Host provides, to prevent processes such as the use of SeaDaddy, X-Agent and X-Tunnel backdoors.

- Fight spear phishing campaigns, which target all organizations, using technology such as email and URL filtering, in addition to training employees to spot and report malicious emails.

- Ensure that C-level executives continually review, modify and re-approve contracts with third-party IT vendors and ensure that those contracts provision for immediate breach notice to the organization and implementation of sufficient security controls on the network.

In summary, the casework CrowdStrike Services provided on behalf of the DNC shows how effective intelligence and investigative capabilities, coupled with the near-instant visibility provided by a next-generation endpoint protection platform such as CrowdStrike Falcon, can detect sophisticated anti-forensics methods for fast and effective remediation.
A travel hospitality vendor with annual gross revenues in the billions of dollars retained CrowdStrike Services to investigate an internally-detected cyber intrusion. The client conducts business in a franchise model, with field locations accessing the corporate network for various legitimate business functions. In this case, the attack vector was network misconfigurations at the franchise level.

THE PRIMARY OBJECTIVES OF THIS ENGAGEMENT WERE:

- Identify the nature and scope of the compromise
- Ensure that the client’s sensitive data did not leave the environment
At a high level, CrowdStrike Services saw "brute-forcing" of credentials at the franchise level, which the attacker then leveraged to move to the corporate network. Although the attacker utilized several different credential dumping tools, they refrained from extensive use of valid credentials.

Upon obtaining legitimate user credentials, the attacker exploited "dual-homed" systems and misconfigured network devices to move laterally from the franchise systems to the corporate network. A dual-homed system contains two network cards, connecting to both the local network and the internal corporate network. In multiple instances, CrowdStrike’s Falcon OverWatch team observed the attacker pivoting from the franchise environment to the corporate network where Falcon Host endpoint technology was deployed.

Once inside the client network, the attacker initially dumped credentials and used a tool to harvest network and routing information to enumerate, or see which hosts were located where on specific network segments.

The threat actor’s motivation was simple: steal credit card data. CrowdStrike was not able to ascertain what the attacker did with this data, but our team did confirm the data was dumped.

Using a local administrator account, the threat actor deployed Windows Credentials Editor (WCE) in a scripted manner within two days of entering the environment. They then looked to see if POS malware was already installed and also sought IP and routing information so they could traverse from one system to new parts of the network.

In this respect, the use of CrowdStrike Falcon endpoint protection provided a major benefit: the CrowdStrike Services team was afforded significant visibility across the environment, allowing them to quickly cut off access shortly after the adversary gained entry to a host. In this way, the team was able to stay ahead of the attacker and keep them constantly on the run from system to system.

Although the client was a CrowdStrike customer, they had not yet deployed CrowdStrike Falcon at their data centers. This was one of the reasons the client called on the CrowdStrike Services team to provide extra assistance in ridding themselves of the attacker.
ADVERSARY TACTICS AND ANTI FORENSICS METHODS

CrowdStrike identified two different families of POS malware in use to collect credit card data:

- **RawPOS**
- **MalumPOS**

CrowdStrike discovered the use of malicious software by analyzing the Application Compatibility key entries, Prefetch, and file system artifacts $MFT, Journal Entry, and the UsnJrnl file. In all, the threat actors used over three dozen different varieties of malware and unknown malicious software to act on their objective. These tools included remote administrative tools, credential dumpers, secure deletion software, and memory-scraping malware.

The two POS data dumpers were installed as a service, or at system level, on the POS terminal itself, which then sends the data for validation to a POS gateway. For POS systems that read card track data into memory, POS malware was used to scan memory looking for the track data. Once found, the card track data was stored to a file and persistently run as more card data was stored in memory.

MalumPOS is a malware variant that dumps the track data to a file on disk for later retrieval. The variants of MalumPOS and RawPOS can go undetected by traditional antivirus endpoint systems because the attackers can easily change the hashes or signatures that traditional AV tools rely on to identify known malicious files.

Despite these limitations, several credential dumping tools were identified and quarantined by the antivirus installed on hosts within the client environment. This may explain why the attacker tried so many different credential dumpers.

To remove their tools as well, the threat actors used Sdelete, a secure removal tool that can be scripted. CrowdStrike's forensics revealed data remnants left behind. While their efforts were somewhat hampered by the attacker's use of sdelete, the CrowdStrike team was able to decipher data stored around it.
With the near-real-time visibility CrowdStrike Falcon provides, CrowdStrike Services tracked the attacker activity and stopped them from taking further action. The client’s security team was very diligent in assisting during the investigation and response period. Using CrowdStrike Falcon, both teams were able to observe attacker groups troubleshooting their methods of entry and pinging older hosts in the network that they had previously compromised.

Each time the attacker took action, the client security team cut off access and prevented the attacker from taking further malicious action. The remediation effort was ongoing over several days as the overriding goal was to continuously stop the threat actor from taking further action and ultimately, to prevent data exfiltration.

In this case, an engaged and responsive client, combined with CrowdStrike’s endpoint technology and consulting expertise, were successful in identifying and expelling one of several threat actors that had targeted the client. This client had experienced several compromises during the prior three years, but with CrowdStrike’s help was able to eject the attacker within eight days of beginning the engagement.

Marrying the real-time detection and prevention abilities of CrowdStrike Falcon with CrowdStrike’s other digital forensics capabilities allowed for fast identification and remediation. Without a real-time next-generation AV and EDR solution such as Falcon Host, identifying the attack methods would have been practically impossible.

The franchise model allows for keeping IT resources separate from other business resources. But a centralized approach to IT systems and network management allows for tighter controls to enforce security policies that strengthen an organization’s overall security posture.

However, ultimately the corporate and franchise legal entities are separate. This creates a legal and operational conundrum that is perhaps unique to the franchise business model.

Organizations with extended partner networks, particularly those using the franchise business model with POS systems to collect customer credit card data, can take the following steps to prevent a similar situation from occurring to them:
• Understand your network: know every device and system that ties into your network from the franchise or field office level and completely understand and document your network topology.

• Franchise licenses should be written so the corporate stakeholder retains the rights to conduct complete digital forensics and investigations within the franchisee's network. In some franchise businesses, the corporate "parent" must stop where the corporate network ends and the franchise network begins. This can severely limit their ability to prevent breaches of sensitive data.

• Ensure that the internal security team has visibility into how firewall rules are determined and implemented throughout the environment. These rules should be stringent and reviewed frequently by the IT team — and if available, the security team also should be involved in determining firewall rules between the corporate and franchise networks.

• Utilize a POS system that tokenizes the tracked data so the full credit card number is not being sent all at once. In such systems, if an attacker does gain access to a large dump of credit card data, only a certain number of the cards will be valid due to the tokenization.

• Utilize a newer POS system that requires chip-based transactions.

• From payment gateway to POS, ensure data is encrypted on the wire — not all POS systems are up-to-date in this area. Also, beware of using outdated POS analytics tools.

• Set up processes to ensure only authorized personnel can access POS terminals and equipment: attackers with physical access to the systems can attach hardware via USB sticks that contain malware, penetration tools and other malicious files to gain network access. This restricted access is vitally important at the franchise level of operations.
A large conglomerate that serves the energy industry called on CrowdStrike to remediate a Pinkslipbot malware outbreak, and to investigate and determine the root cause. A leader in their sector, this client realizes annual gross revenues in the tens of billions of dollars.

THE PRIMARY OBJECTIVES OF THIS ENGAGEMENT WERE:
- Identify the nature and scope of the compromise
- Monitor the client network and systems

To accomplish these objectives, CrowdStrike performed triage and forensic analysis of the known-infected systems. Next, CrowdStrike focused on defining the scope of the compromise as well as monitoring the network and system-level activity to detect any future malicious activity.
Prior to CrowdStrike starting the investigation, the client’s internal security team had taken steps to block known Command and Control activity. Additionally, the client had engaged its anti-malware endpoint protection vendor to help identify and detect the Pinkslipbot infection through anti-malware technical support and analysis. CrowdStrike utilized information provided by the client to initiate the investigation.

Pinkslipbot (AKA Qakbot, Akbot, Qbot) is a known malware that has existed since 2007. It is essentially a keystroke logger that steals data. Attackers use it to look for credit card data and as soon as it achieves elevated privileges, it runs through administrator shares.

Pinkslipbot is often delivered by exploit kits and will move through organizations by exploiting network shares. The malware also contains a dictionary of common passwords to be used against administrator accounts. Pinkslipbot is delivered primarily via drive-by downloads through exploit kits such as RIG and Sweet Orange, as well as through removable USB drives and network shares.

Pinkslipbot attempts to disable web reputation-based anti-malware products from Intel Security, AVG, and Symantec by hooking DNS APIs and returning invalid IP addresses for domains used by these vendors to detect the malware. The bot is equipped with other counter-anti-malware features, such as the ability to set folder permissions to read-only status to prevent signature updates, as well as a DNS spoofing mechanism that returns invalid IP addresses for any A-queries for websites related to anti-malware products.

The client’s internal IT team attempted to contain the malware outbreak on their own, but they did not understand how it operated in totality. In the meantime, the malware evaded the traditional endpoint anti-malware software installed on their hosts.
IDENTIFYING NEW INDICATORS OF COMPROMISE

Using CrowdStrike Falcon, our team found and provided new attack indicators to the client’s anti-malware vendor, which in turn created new signatures for detection and removal.

The anti-malware vendor, a large and well-known traditional endpoint security provider, did provide the client with some level of remediation, but it was not complete without visibility into the polymorphism aspects of the Pinkslipbot malware.

CrowdStrike did not see signs of “hands-on keyboard” activity. The CrowdStrike team’s conclusion was that the client was not explicitly targeted by the attacker, but instead its employees were unknowingly victims of a drive-by malware campaign and were infected upon visiting a compromised website. Subsequently, all the client’s compromised systems were herded into the attacker’s botnet.

REMEDIATION

Until CrowdStrike Services could fully contain the malware outbreak, CrowdStrike Falcon provided the necessary visibility to find machines that didn’t have any antivirus or anti-malware protection installed. If a new Pinkslipbot variant infected the client hosts with new hashes, Falcon Host would block them and stop further compromises in the client environment.

Additionally, Falcon identified several rounds of polymorphism exhibited by the malware: each time it changed, analysts were able to use recorded endpoint data to identify new signatures. CrowdStrike provided new indicators of compromise for updated signatures used for containment. In addition, the malware had scheduled updates, so CrowdStrike would see spikes in infection after those updates occurred.

In total, over 500 hosts were remediated in under two weeks. As CrowdStrike provided valuable recommendations and indicators, the malware was contained with updated anti-malware signatures.
The key findings and recommendations based on this case study fall into two categories, policy and technology:

**Policy Recommendations:**
- Restrict privileged account logins based on roles: employees had admin-level credentials, which enabled the infection to spread to other systems on the network.
- Harden workstations by ensuring endpoint protection is installed on all hosts, not just a majority or subset of total hosts.

**Technology Recommendations:**
- Improve host visibility with a next-generation AV and EDR solution such as CrowdStrike Falcon, and consider implementing proactive 24/7 adversary hunting, such as that offered by Falcon OverWatch, to augment internal security team activities.
- Implement log aggregation and storage: if there is no record of an event happening, it’s nearly impossible to backtrack and analyze inciting incidents or processes.
- Implement Network Traffic Alerting and Collection: understand what is "crossing the wire" and be alerted when specific types of data are transmitted, as well as tracking source and destination IPs.

CrowdStrike Services equips organizations with the protection and expertise they need to defend against and respond to security incidents. Leveraging the primary components of the CrowdStrike Falcon™ platform — Falcon next-generation endpoint protection, Falcon Intelligence threat intelligence gathering and reporting operations, and the 24/7 Falcon OverWatch proactive threat hunting team — the CrowdStrike Services incident response team helps customers around the world identify, track and block attackers in real time. This unique approach allows CrowdStrike to stop unauthorized access faster and prevent further breaches, 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 stop breaches.
 Unlike traditional security vendors, the primary components of the CrowdStrike Falcon Platform -- Falcon Host, Falcon Intelligence, Falcon OverWatch and CrowdStrike Services -- do not exist in silos: each product and service works harmoniously, empowering each other to provide customers immediate value and protection.

The CrowdStrike Services team works very closely with the Falcon OverWatch team during incident response investigations. CrowdStrike’s Falcon OverWatch team delivers around-the-clock insight with powerful adversary hunting capabilities to keep our customers’ assets safe. This 24/7 global operation center is staffed by an elite group of cyber intrusion detection analysts and investigators, all dedicated to continuously hunting for adversary activity and malware in our customers’ environments.

When OverWatch discovers new adversary tactics, techniques and procedures (TTPs) in a client environment, CrowdStrike Services security consultants use that information to further their investigations during an incident response engagement. Below are a few specific examples of adversary tradecraft Falcon OverWatch uncovered during the past twelve months to help our customers stop breaches.
PowerShell, a built-in Windows scripting language, can be leveraged as an infection vector, downloading implants, launching implants, hosting implants, and dumping credentials. Although CrowdStrike teams have seen it in the wild for years, the OverWatch team now very frequently observes evidence of PowerShell and other “living-off-the-land” tool usage by adversaries attempting to bypass traditional security technologies and fly under the radar.

- **PowerShell Used for Loading DLL Implants via Rundll32**
  In one example, the team detected a spear phishing campaign where a ZIP file was opened and a shortcut file executed, launching PowerShell with a base64-encoded command line. It proceeded to write and launch a decoy document, write a malicious PE file and load it via rundll32. Hands-on-keyboard commands then followed beneath the rundll32-loaded implant.

- **Malicious PowerShell script hidden in legitimate admin script**
  In this tactic, the attackers add a line to an otherwise benign VBScript used during Windows logon process, launching a malicious PowerShell script that steals credentials. This enables the adversary to continuously collect credentials from the environment in a surreptitious manner.

Falcon Host visibility into this attack activity
• **Use of Microsoft OneDrive for Covert Data Exfiltration**
  On a number of occasions, the OverWatch team observed use of the "net use \\docs.live.net@SSL" command to mount adversary-controlled Microsoft OneDrive account shares and then issue copy commands to exfiltrate data out of the environment via SSL.

• **WMI + Powershell + Meterpreter**
  In this attack method, the adversaries use WMI (Windows Management Instrumentation) to launch a PowerShell process that downloads a Meterpreter payload. This payload is hosted by a PowerShell process, which then issues attacker commands. WMI is the Microsoft implementation of Web-Based Enterprise Management (WBEM), which is an industry initiative to develop a standard technology for accessing management information in an enterprise environment.

These are just some examples of the Falcon OverWatch team uncovering new adversary tradecraft as they actively hunt adversaries to protect customer environments. For further information on CrowdStrike Falcon OverWatch, please see the white paper "Proactive Hunting: The Last Line of Defense Against the 'Mega Breach’" at www.crowdstrike.com.
CrowdStrike is the leader in cloud delivered next-generation endpoint protection. CrowdStrike’s core technology, the CrowdStrike Falcon™ platform, stops breaches by preventing and responding to all types of attacks – both malware and malware-free. CrowdStrike has revolutionized endpoint protection by being the first and only company to unify three crucial elements: next-generation antivirus, endpoint detection and response (EDR), and a 24/7 managed hunting service – uniquely delivered via the cloud in a single lightweight sensor. Falcon uses the patent-pending CrowdStrike Threat Graph™ to analyze and correlate billions of events in real time, providing complete protection and five-second visibility across all endpoints. The company leads in threat prevention with its potent combination of signatureless machine learning and behavioral-based analytics. Many of the world’s largest organizations put their trust in CrowdStrike, including three of the 10 largest global companies by revenue, five of the 10 largest financial institutions, three of the top 10 healthcare providers, and three of the top 10 energy companies. CrowdStrike Falcon is currently deployed in more than 176 countries.

EXPERIENCED A BREACH?
Call 855.276.9347 or email services@crowdstrike.com