WHITEPAPER

Combating the Top Five Cyberattacks with Managed Detection and Response

Cybercriminals have rapidly acquired new cyber weapons and modified the ways they launch cyberattacks. Weapons and attack capabilities that were previously only observed in large-scale nation-state operations are now falling into the hands of the masses. Today's attackers are more sophisticated, and capable of exploiting weaknesses at previously unseen speed and scale.

Data breaches and major attacks, therefore, remain common occurrences despite innovative advances in security products and solutions in recent years. As cybercriminals continue to adapt and evolve, understanding what it really takes to respond to attacks–and secure all sensitive data–is now paramount for businesses of all sizes.

This whitepaper walks through the top five attacks most commonly observed in the AWN CyberSOC™ service by our security experts who support hundreds of Arctic Wolf customers. We (1) provide some background on the nature of each attack type; (2) highlight the tactics, techniques, and procedures (TTPs) commonly used by threat actors; (3) discuss the early detection strategies adopted by Arctic Wolf security engineers; and (4) describe what steps need to be taken to contain and remediate these cyberattacks.

Even though cybersecurity technology has become increasingly sophisticated, what stands out is the consistency of the nature of the attacks over the years. For example, phishing remains the number one method of spreading malware and stealing credentials. Despite spending $100 billion or more in cybersecurity, companies are no safer than they were 10 years ago.

This highlights the need for a new approach to cybersecurity, one that is based on detection and response, and not prevention. The approach also must protect against multiple attack vectors and be adaptive to defend against new variants or changes in attackers' strategy. Large companies achieve this with a 24x7 security operations center (SOC), but every company needs to create a cybersecurity strategy that includes the capabilities delivered by a world-class SOC.

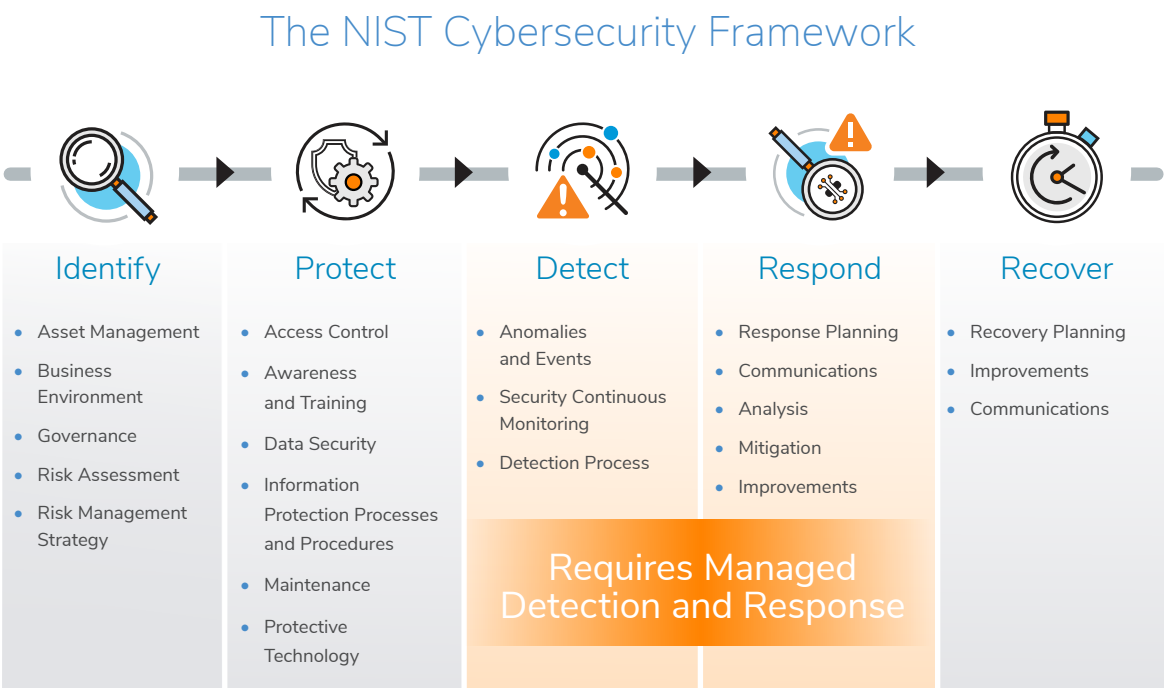
- Businesses of all sizes are now targets–not just large enterprises
- The biggest threats of today–such as ransomware and phishing–have been around for years
- Most businesses still take 214 days to detect a security breach and another 77 days to respond to and contain it[1]
- Everything from hospital patient records to company secrets to social security numbers and personal banking information is at risk
- Prevention-based approaches are now inadequate; Detection and response is the future for effective security

1. Ponemon Institute's Global 2017 Cost of a Data Breach Study

Detection and Response: Required for an Effective Cybersecurity Strategy

The National Institute of Standards and Technology (NIST) Cybersecurity Framework is a risk-based approach to managing cybersecurity risk and defines a set of cybersecurity activities and desired outcomes. The core of the framework consists of five concurrent and continuous functions: Identify, Protect, Detect, Respond, and Recover.

A common approach to IT security is to invest heavily in cybersecurity protection measures, or the "Protect" function in the NIST framework. Businesses typically deploy several perimeter and endpoint security products with the assumption that they are then secure. Unfortunately, implementing only a subset of the functions within the framework has proven to be insufficient.



Statistics highlight how, despite deploying various protective point products, businesses still struggle with detecting and responding to cyberattacks. Based on The Ponemon Institute's research from 2017, companies took an average of 214 days to detect data breaches and 77 days to contain and respond to them.

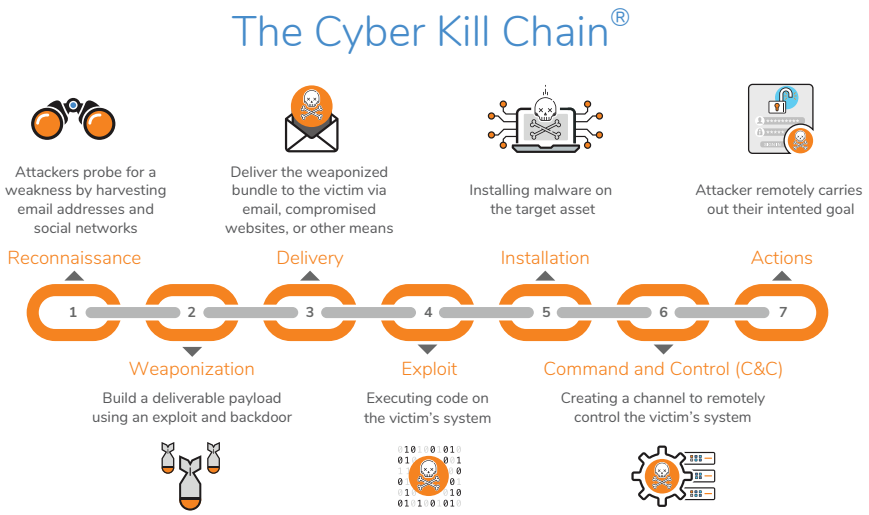
In the aftermath of most data breaches, IT teams find that attacks usually don't look like attacks at all, except in hindsight. Detection strategies depend on aggregating and correlating logs from critical components in an organization's network. Event log data and alerts from these sources need to then be normalized and analyzed thoroughly, with the aid of customized rules written by trained security experts. Detecting patterns of anomalous activity that may be indicators of compromise, therefore, requires the deep analysis of several critical log sources, including:

- Firewalls
- IDS/IPS
- Endpoint security (EPP, Antivirus)
- Active Directory
- Email security gateways
- SaaS applications
- Cloud workloads

Timely detection and response requires the in-depth analysis of log data from the above sources. And, as stated earlier, it also requires creating the customized rules and logic applicable to each environment.

Top Five Attack Vectors

In the following sections, we discuss the top five cyberattacks Arctic Wolf experts observe "in the wild." The attacks are described in the context of the Cyber Kill Chain from Lockheed Martin, an industry standard for outlining the various stages of any targeted cyberattack.



#1 Ransomware and Other Types of Malware Attacks

Background:

Ransomware is a type of malware that either threatens to block access to a victim's data, publish it, or destroy it unless a ransom is paid. Ransomware typically blocks data access by encrypting the victim's data, rendering it inaccessible, and then demands a ransom in the form of digital cryptocurrencies before the victim is allowed to decrypt the data. In most extortion attacks of this nature, recovering the locked data without the attacker-provided decryption keys is impossible. Also, because perpetrators use crypto-currencies to meet ransom demands, tracing and prosecuting them is extremely difficult.

Attacker TTPs:

The most common techniques attackers use to deliver weaponized payloads include malicious emails with attachments, or physical media, such as infected USB devices. Most of these methods require some form of human interaction or activity to lead to infection, such as opening an email attachment or inserting a infected USB device into their endpoints. More advanced techniques, such as supply chain interdiction in the form of poisoned software update packages, are becoming increasingly common. An unsuspecting victim might download what appears to be a routine software update, yet turns out to be malicious software. For example, infections of Nyetya appeared on several systems running a legitimate updater for the M.E. Doc document management software.

Finally, advanced cybercriminals use another pivot attack tactic, which goes after watering hole domains. These attacks compromise the infrastructure assets of trusted organizations to ultimately reach the intended targets. While these "watering holes," or otherwise trustworthy websites that the intended targets are known to visit, may host

Among the most notorious ransomware attacks from 2017 were the WannaCry, NotPetya and BadRabbit cryptoworms. The propagation of WannaCry, which infected 300,000 machines worldwide, depended on attackers exploiting Microsoft Windows vulnerabilities in the SMB protocol. In March 2018, the city of Atlanta was attacked using the SamSam ransomware strain, temporarily disrupting city operations. As of late April 2018, the City of Atlanta incurred close to $3M in total incident response expenses, as a consequence of this single attack.

legitimate content, threat actors often alter the JavaScript or PHP to request content from IP addresses they control. After doing so, these websites then contain or reference malicious files that may infect an endpoint.

Detection Strategies:

If the attacker delivers ransomware or malicious software to a victim's endpoint, the alerts and event log data from the antivirus (AV) or endpoint protection platform (EPP) installed on the endpoint often help with early detection. These solutions are deployed as tamper-proof endpoint agents and use a variety of methods, including real-time file scanning using signatures, heuristics and sandboxing. Arctic Wolf Concierge Security Engineers (CSEs) detect attackers based on the analysis of cross-correlated alerts, including those from the AV or EPPs.

If the attacker makes it past your endpoint security defenses, the command-and-control (C2) traffic between the infected endpoint and the malicious actor's server can be detected by analyzing event logs from firewalls or continuous network monitoring devices, such as the Arctic Wolf on-premises network sensor. In many cases, Arctic Wolf CSEs used signature-based approaches to detect suspicious patterns in web traffic in the form of DNS queries made to resolve domains such as "server454.xswet-alr7.ru" that may be known to dangerous. Such an observation is typically indicative of a breached endpoint.

Containment and Remediation Action:

Upon carefully evaluating the indicators of compromise, and determining that the customer needs to be engaged, the Arctic Wolf CSE notifies the customer's IT team based on the established incident response (IR) plan. The containment action for ransomware and malware attacks involves isolating the infected endpoint before the malware can achieve lateral movement, and attack other network drives to which the infected endpoint has access.

The remediation action, once the endpoint has been isolated, is to reimage and re-provision the device back to the original user. This is done once the files affected by the compromise have been appropriately scanned, cleaned, and restored from the organization's information backups.

Finally, the CSE helps lead a security review that determines if other machines were compromised, ensures that permanent blocks are configured in perimeter security devices, and also helps analyze the EPP solution to ensure that future occurrences of the malware are blocked or prevented.

> ***Real World Example**–Upon detecting suspicious C2 traffic at a credit union in Michigan, the Arctic Wolf CSE moved quickly to help isolate the infected endpoint before the threat actors could move laterally, preventing severe disruption to the credit union's operations, such as posting direct deposits or clearing transfers. The infection was determined to be related to the WannaCry epidemic. In response, the CSE then provided the credit union's IT staff with guidance on how to update their endpoint security policies and perimeter defenses, including disabling all versions of the Server Message Block (SMB) protocol at the network boundary, ensuring that future attempts by attackers could be blocked.*

Attack Name:
Ransomware

Attacker TTPs:
Malicious email attachments, infected USB memory devices, poisoned software updates, watering hole domains

Detection Strategies:
Delivery Stage: endpoint
AV and EPP

C2 Stage: AWN sensor continuous monitoring

Where the Kill Chain Is Broken:

Delivery

Command and Control

Containment Action:
Isolate infected host(s)

Remediation Action:
Reimage, re-provision infected host(s), restore backups

Security Review:
Update FW and EPP configurations

#2 Password Phishing Attacks

Background:

Phishing attacks are carried out to obtain sensitive information such as usernames, passwords, social security numbers or credit card numbers. Attackers typically operate under the guise of a trustworthy entity, such as a website for a bank, or the login page for an email or messaging service.

Attacker TTPs:

Social engineering is the most common attack technique used for password phishing. It involves luring unsuspecting users into clicking links in emails that bring them to a landing page with the look and feel of a legitimate page with which they may be familiar. However, these URLs point to locations maintained by the threat actors. They may indeed look like valid domains, for example, arctlcw0lf[dot]com, or they may take advantage of the obfuscation in shortened URLs, for example, bitly[dot]com/seemingly-harmless-random-string. Once victims click on the malicious URL and make it to the landing page, they proceed to enter their legitimate domain credentials, giving them away.

Another type of phishing, called spear-phishing, is an attack that specifically targets a particular victim. For example, attackers use email attachments to deliver specially-crafted malicious files. When the victim opens the file, a request is sent to authenticate the client with a remote (attacker-managed) server, sending over the victim's credential hash. The attackers can typically use trivial password-cracking techniques to obtain the plain text password from the credential hash, especially when outdated hashing algorithms such as MD4 or MD5 are used.

Detection Strategies:

In most cases, the first line of defense when it comes to phishing attacks are alerts and event log data from email security solutions that offer real-time analysis of URLs in emails, email attachments, and web objects. Access to threat intelligence feeds is critical to ensure that malicious URLs, for example, are accurately detected and alerts are appropriately signaled. Detection at this stage breaks the cyber kill chain either at the "Delivery" or the "Exploitation" stage of the attack, depending on whether the victim has opened a malicious attachment or clicked a malicious link, or if the CSE detects the attempt upon email delivery, based on the analysis of logs from email security solutions.

Sometimes, an email security solution may not flag the embedded malicious URL or attachment before the victim interacts with it, in which case "call-back" traffic (the traffic sent back to a the C2 server where the credentials may be sent in the clear) can be detected. This detection strategy involves continuously monitoring outbound host communications over multiple protocols in real-time to determine if the traffic is indicative of an infected host. For example, from the previous case involving the malicious .docx file that was used to capture credentials, C2 connections are often made through a connection over SMB using TCP ports 445 or 339. Note that the phished credentials in these attacks could either be part of the victim organization's Active Directory (AD) network or belong to one of the SaaS applications that are in use.

A massive phishing attack targeted Google Docs users in 2017. Potential victims received seemingly legitimate invitations to view a Google Docs file. When unsuspecting users clicked through, they arrived at a login screen almost indistinguishable from the real Google Docs page. Around a million users are estimated to have been affected worldwide.

Attack Name:

Phishing

Attacker TTPs:

Social engineering; malicious emails with specially crafted attachments

Detection Strategies:

Delivery/Exploitation Stage: Email security solutions

C2 Stage: FW continuous monitoring, AD activity monitoring

Where the Kill Chain Is Broken:

Delivery

Exploitation

Command and Control

Containment and Remediation Action:
Upon carefully evaluating the indicators of compromise, and determining that the customer needs to be engaged, the CSE notifies the customer's IT team based on the established incident response (IR) plan. The containment action for phishing attacks involves isolating the infected endpoint once it is determined it contains malicious software installed by the attackers. This quarantine occurs so that this malicious code is unable to achieve lateral movement. In addition, the user account associated with the AD or SaaS application is usually disabled immediately to prevent potential data exfiltration attempts or fraudulent activities.

The remediation action, once the endpoint is isolated, is to reimage and re-provision the device back to the original user, and also take appropriate account-provisioning actions for the impacted AD or SaaS account.

Finally, the CSE helps conduct a security review to ensure that the appropriate controls such as two-factor authentication (2FA) are employed where possible. The CSE assists in ensuring that permanent blocks, on ports, IP addresses, and protocols, are configured in the firewall, and also helps analyze the email security solution so that future occurrences of the same type of phishing attempt are blocked or prevented. To conclude, CSEs provide ongoing awareness training and users learn best practices for safe web browsing and dealing with suspicious emails.

> ***Real-World Example**–After correlating alerts and event log data from email security appliances with suspicious C2 traffic on the network of a hospital system in Pennsylvania, an Arctic Wolf CSE concluded that a malicious .docx email attachment was opened by an unsuspecting hospital admin, which compromised their credentials. The CSE provided specific guidance to isolate the infected endpoint and disable the impacted user's account, disallowing lateral movement and preventing the compromise of the personal health information (PHI) associated with the hospital's patients, including all patient records. The CSE then helped re-configure network boundary devices, and instructed the hospital's IT staff on how to update their email security solutions so that future attacks could be prevented.*

#3 PUP Adware

Background:
A potentially unwanted program (PUP), sometimes referred to as a potentially unwanted application (PUA), is a type of malware that an end-user usually perceives as unwanted. PUP malware is known to severely weaken an infected endpoint's security and dramatically compromise the user's privacy. PUPs typically display intrusive, annoying advertising and can track a user's Internet usage in order to sell information to advertisers. In certain cases, PUPs even rack up texting charges for a user by exploiting premium SMS services. PUPs may also surreptitiously monitor keystrokes, scan files on the infected endpoint's hard drive, and even access local browser cookies.

Attacker TTPs:
Setting a victim up for a "drive-by download" is the most common attack technique used by threat actors employing PUPs. Such malicious downloads occur even in cases where a user has provided authorization but did so without understanding the consequences of installing the application. This includes, for example, counterfeit executable files, ActiveX components for Internet Explorer, or Java applets that add rich content

Containment Action:
Isolate infected host(s), disable impacted AD/SaaS account(s)

Remediation Action:
Reimage, re-provision infected host(s). Re-provision AD/SaaS account(s)

Security Review:
Implement 2FA controls. Update FW and EPP configs

In September 2017, security researchers at Cisco revealed that the ubiquitous computer cleanup tool, CCleaner, had been compromised by cybercriminals for more than a month. The updates that users were downloading from CCleaner had been poisoned with a malware backdoor. The incident exposed millions of computers and highlighted the threat of software supply chain attacks. At the RSA security conference in San Francisco in April 2018, representatives from CCleaner's parent company, Avast, explained how criminals were able to launch this attack, which ultimately led to 2.27 million downloads of the corrupt CCleaner version.

to web pages. In other cases, the downloads happen without the user's knowledge when visiting a website or clicking on a seemingly harmless pop-up window. In many examples, the user may actually intend to close a pop-up window to dismiss an ad but enable a PUP download while doing so. Many attackers also exploit vulnerabilities in browser plugins to run malicious software without the victim's knowledge.

Attackers may also leverage poisoned software updates and other supply chain attacks to deliver PUPs. This was the technique in the widespread campaign that used the adware-removal tool CCleaner to surreptitiously distribute PUPs. In more advanced attacks, the PUPs install a root certificate on a victim's device, which allows hackers to intercept private data such as banking details without a browser giving security warnings. In most cases, when PUPs are bundled with other programs, there is also no clear opt-out method for the user to disallow the PUP's installation.

Detection Strategies:

Endpoint antivirus (AV) solutions are typically the first line of defense for detecting PUPs. Based on the in-depth analysis of logs and alerts from AV solutions, Arctic Wolf CSEs are able to detect the presence of PUPs on an endpoint soon after the drive-by download completes and malware is installed.

Endpoint AV solutions can help detect several known varieties of PUPs, including files that use runtime packers. Runtime packers decrease the size of executable files without requiring an external unpacker. Such files aren't generally considered malicious, but runtime packers are widely used with PUP files since they can enable known malware types to go undetected. Applications that are used to sniff, filter, or manipulate network traffic, RATs (remote access trojans), keyloggers, and known malicious Javascript or ActiveX scripts are also flagged by endpoint AV solutions as they may indicate the presence of a PUP.

In many cases, unfortunately, the endpoint antivirus solution is unable to appropriately flag the PUP, especially when the malware does not fit any known profile. In such cases, the firewall appliance or an on-premises network sensor detects any suspicious connections made with remote C2 servers or scammer networks that the threat actors run to manage large-scale attacks.

Containment and Remediation Action:

After thoroughly evaluating the indicators of compromise, and determining that the customer needs to be engaged, the Arctic Wolf CSE notifies the customer's IT team based on the established incident response plan. The containment action in cases of PUP malware is to first quarantine and isolate the infected endpoints before the malware can achieve lateral movement and infect other devices.

The remediation action once the endpoint has been isolated is to run an in-depth adware/malware removal tool to ensure that all detected PUPs are appropriately deleted permanently from the device. In certain extreme cases, the CSE also recommends reimaging and re-provisioning the endpoint before returning it to the original user.

Attack Name:
PUP adware

Attacker TTPs:
Drive-by downloads, browser vulnerabilities, poisoned software updates, social engineering

Detection Strategies:
Delivery Stage: Endpoint AV
C2 Stage: AWN sensor continuous monitoring

Where the Kill Chain Is Broken:

Delivery

Command and Control

Containment Action:
Isolate infected host

Remediation Action:
Run adware removal tool Reimage, re-provision infected host(s) if necessary

Security Review:
Update FW and endpoint AV configurations, End-user coaching

Finally, the CSE also engages in a comprehensive security review with the customer's IT representatives to ensure that the email security defenses, endpoint AV solutions, and perimeter defenses are appropriately updated, and that the recently discovered PUPs are blocked or prevented in the future.

Real-World Example–After detecting suspicious scammer C2 traffic on the network of a law firm in Texas, the Arctic Wolf CSE determined what endpoints were infected and alerted the law firm's IT staff to isolate them immediately, preventing serious loss of sensitive client data. The CSE then provided guidance on updating the firm's endpoint AV solution and reviewed perimeter defenses to ensure that permanent blocks are configured for all the appropriate ports, IP addresses and protocols associated with the scammer network's infrastructure. The CSE also helped with awareness training to make certain that the firm's attorneys and staff received the appropriate coaching necessary as far as best practices for safe web browsing and handling suspicious emails.

#4 Brute-Force Login Attacks

Background:

Brute-force login attacks consist of threat actors systematically attempting password or passphrase combinations in hopes of eventually guessing correct combinations and accessing restricted resources protected by the passwords.

Attacker TTPs:

Attackers typically use brute-force attacker tools, automated password crackers, and "dictionary attack" tools to hack longer passwords that have a larger set of possible values. Brute-force mechanisms, that attempt to guess passwords at the rate of a billion guesses per second, are specifically damaging when the attempt is made to penetrate a backend enterprise system. However, as the number of characters increases, a billion guesses per second might still not be practical enough to complete the attack successfully.

This is where a "dictionary" attack can be more effective, where attackers make guesses using words in a dictionary, instead of attempting all possible combinations. Attackers often further "mutate" the words, based on common things users might do to passwords, for example, "bru13F0rce".

Detection Strategies:

In-depth analysis of AD and SaaS application login activity logs are the primary methods used to detect brute-force login attacks. Authentication data logs are critical in several security and compliance operations issues that most admins contend with. However, working with authentication data logs is quite complex and may require analyzing terabytes of data over a very short time period. Arctic Wolf CSEs are able to write custom detection rules and understand when data shows activity indicative of an attack.

Repeated failed authentications against restricted systems or other secure assets in a specified period of time, for example, is generally observed to be a brute-force attack. Accounts showing a high number of failed login attempts before a successful one are also potential victims of a brute-force attack.

Brute force attackers are typically motivated financially and may be organized crime actors. Based on Verizon's research, more than a third of point-of-sale (POS) intrusions employed brute force to compromise POS systems.

Attack Name:

Brute-force

Attacker TTPs:

Automated password cracker tools, dictionary attacks

Detection Strategies:

Delivery Stage: AD and SaaS login activity

Exploitation Stage: AD and SaaS login activity

Where the Kill Chain Is Broken:

Delivery

Exploitation

Aided by advanced machine learning techniques, Arctic Wolf CSEs can analyze vast troves of data from AD and SaaS log sources to detect anomalous login activity indicative of brute-force attacks. A vast majority of these attacks are detected either when failed login attempts are noticed, or after unusual activity is detected around a compromised account. In the former case, we break the kill chain in the "Delivery" stage of the attack, while it happens in the "Exploitation" stage of the attack in the latter example.

Containment and Remediation Action:

The containment action for brute-force attacks first involves disabling the impacted user account associated with the AD or SaaS application. This is normally done immediately after a compromise to prevent potential data exfiltration attempts or fraudulent activities.

The remediation action requires re-provisioning the AD and/or SaaS application accounts for impacted users, and also reimaging their endpoints when there is reason to believe malicious software may have been installed by the attacker.

Finally, the Arctic Wolf CSE helps conduct a security review to make certain appropriate controls are established to block or prevent similar attacks in the future. Among the most common changes made from a security perspective are ensuring that user accounts are locked out after a designated number of failed login attempts. Based on the specific customer's environment and user characteristics, the CSE provides guidance on this implementation. Further security measures may include enforcing time delays before successive login attempts.

The CSE oversees customer enactment of reCAPTCHA challenge-response tests to prevent attackers from submitting login attempts using the rapid-guessing techniques discussed earlier. reCAPTCHA is a newer CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) mechanism. In some special cases, if certain IP addresses are observed to exceed a high threshold of invalid logins, they are flagged as malicious and the CSE may recommend updating perimeter defenses with policies to restrict or block associated traffic.

The CSE also lends guidance from a security awareness perspective, to ensure that end-users and admins receive the appropriate coaching for security best practices, which includes using secure password managers and enforcing stricter rules around password complexity requirements.

> ***Real-World Example**–After noticing suspicious Active Directory user login activity based on customized logic the Arctic Wolf CSE had written for a hospitality and hotel management group in New Jersey, the CSE determined that several accounts were compromised from a brute-force attack. The CSE immediately informed the group's IT team to disable the impacted accounts. As the detection logic was triggered on anomalous multi-geo activity and repeated login failures, the CSE was able to detect the attackers very early and prevent serious data exfiltration attempts that could have compromised the personal information of their staff, guests and partners. The CSE then participated in an in-depth security review and provided guidance on policy updates and password management.*

Containment Action:
Disable impacted AD/SaaS account(s), Isolate infected host(s), if necessary.

Remediation Action:
Re-provision AD/SaaS account(s). Reimage infected host(s), if necessary

Security Review:
Update authentication policy, implement reCAPTCHA, update FWs

5 Attacks on Unpatched Servers and Infrastructure

Background:

These attacks are specifically designed to exploit weaknesses and vulnerabilities in servers and other Internet-facing infrastructure that admins or users may be unaware of or have overlooked. In a vast majority of such attacks, patches were already publicly announced and made available to fix the vulnerabilities. Increasingly, however, attackers move faster than victims to exploit these vulnerabilities, allowing them to initially compromise exposed Internet-facing devices and then attempt lateral movement. Some of the most notorious examples of attacks based on unpatched devices include the WannaCry malware epidemic and the Equifax data breach.

Attacker TTPs:

The first step attackers take is to determine vulnerabilities in a specific target, or if there are known vulnerabilities in random systems. The attacker then launches the attack based on the discovered vulnerabilities.

One of the most common techniques involves using scanning tools and web crawling software to run automated reconnaissance missions. These illicit forays check web applications for vulnerabilities such as buffer overflows, cross-site scripting (XSS), SQL injections, debugging backdoors, and misconfigurations to exploit. In the Equifax data breach example, and many others, the attackers exploited a vulnerability that should have been patched. In fact, the Apache Struts vulnerability (CVE-2017-5638) had a patch available in March 2017. Using simple scanning techniques, cybercriminals determined that Equifax was running a vulnerable version of Apache Struts and launched their attack in May, a full two months after the patch was released.

Detection Strategies:

The most important detection method involves running vulnerability scanning tools, especially in critical Internet-facing infrastructure devices. Vulnerability scanning tools are also employed for system hardening and alerting when vulnerable, unpatched systems are detected. Network sensors may also detect anomalous requests coming in to Internet-facing entities, which may indicate attackers probing the system. Detection using sensors or vulnerability scanners breaks the cyber kill chain at or before the initial "Reconnaissance" stage of the attack.

If attackers evade the vulnerability scanning tools and compromise one of the exposed devices, the CSE can detect any suspicious connections made with remote C2 servers run by the threat actors to manage large-scale attacks.

Containment and Remediation Action:

The first containment action is to determine the severity of any detected vulnerability. This step usually requires careful analysis, especially when there are multiple detected vulnerabilities and decisions of prioritization occur. The Arctic Wolf CSE then guides a response based on their understanding of the attacker landscape to ensure patching is conducted in the least disruptive way. In the case of very severe vulnerabilities, impacted entities may be isolated and shut down or configured to operate with limited functionality, leading to downtimes. This isolation activity could involve multiple impacted entities if there is evidence that more than one Internet-facing server, for example, is compromised.

In the Equifax data breach case, the exploited Apache Struts vulnerability had a patch released in early March 2017. The attack began two-and-a-half months later, in mid-May, and was not detected by Equifax until July 29th. The hack was revealed to the public on September 7th. The total damages from this security lapse are estimated to be over $600M.

Attack Name:
Unpatched servers and infrastructure

Attacker TTPs:
Scanning tools, web crawling software

Detection Strategies:
Recon Stage: Periodic vulnerability scanning

C2 Stage: AWN continuous monitoring

Where the Kill Chain Is Broken:

Reconnaissance

Command and Control

Containment Action:
Determine severity of identified vulnerability. Isolate, shut down, or restrict impacted system(s)

Remediation Action:
Prioritize and plan for patching. Patch and restore services

Security Review:
Update vulnerability scanning and patching policies FW and EPP configurations

The remediation activities start with patching the impacted entities based on their assigned priorities, ensuring minimal impact to end users and business operations. Once the patches have been tested and work as expected, the impacted systems are brought back online and any disrupted services restored.

The Arctic Wolf CSE also helps conduct an in-depth security review to make certain that appropriate patching policies and processes are in place for operating systems and network devices, such as switches and routers, web servers, databases, firewalls, and other critical infrastructure. This may result in updating policies concerning how often vulnerability scanning tools are run. Since each situation is unique, careful analysis is required to decide how patches should be prioritized for known vulnerabilities, taking into consideration end-user impact and operational downtime.

> **Real-World Example**–*Arctic Wolf CSEs identified the infamous Apache Struts vulnerabilities in Internet-facing infrastructure devices on an Oregon retail business's network. The CSEs then assisted with system hardening, so that all critical patches were applied in a timely manner. These steps prevented large-scale attacks against the retail business and helped them avoid millions of dollars in remediation costs, especially from compromised data of their customers and suppliers.*

The Arctic Wolf Difference

Enabling your employees, customers, and partners with advanced IT systems, while simultaneously securing business operations and sensitive information can be a daunting task. Small and midsize enterprises (SMEs) typically address this problem by deploying a variety of perimeter security devices, endpoint AV solutions, and maybe even a SIEM. This approach has consistently proven to be ineffective, as businesses continue to struggle with attacks and data breaches.

A security operations center (SOC) is critical to continuously monitor data centers and servers, user login activity, SaaS applications, cloud workloads, managed laptops and other endpoints, and email systems. A SOC enables IT to correlate events across multiple, disparate systems, and extract actionable intelligence to aid effective threat detection and response. Unfortunately, the cost of operating and staffing a fully-operational SOC is well beyond the budget of most SMEs. This is where Arctic Wolf's managed detection and response (MDR) solution can help.

Arctic Wolf's AWN CyberSOC™ is a turnkey SOC-as-a-service that comes with 24x7 security expert coverage, detailed processes and support for incident response, and our proprietary cloud-based SIEM technology at a predictable annual subscription. AWN CyberSOC extends your IT team or augments your security team with our customized experience and expertise in combating sophisticated cybercriminals. Arctic Wolf ensures your business remains protected even as attackers continue to evolve.

ARCTIC WOLF Layer 7 Data Solutions

AICPA SOC

SOC2 Type II Certified

Contact us
arcticwolf.com
1.888.272.8429
info@arcticwolf.com