Demo Investigation

Endpoints

Hostname	First Timestamp	Last Timestamp	Events
SCRANTON.dmevals.local	5/1/2020 10:55:56 PM	5/2/2020 4:18:37 AM	136
NASHUA.dmevals.local	5/1/2020 11:10:23 PM	5/1/2020 11:17:52 PM	58
UTICA.dmevals.local	5/2/2020 3:55:06 AM	5/2/2020 4:21:21 AM	112
NEWYORK.dmevals.local	5/2/2020 4:02:44 AM	5/2/2020 4:17:35 AM	9

Investigation Summary

An investigation based on the https://github.com/OTRF/detection-hackathon-apt29 dataset. Investigation and endpoint summaries are generated by a large language model (LLM) from the Investigation events, comments and Micro-Technique evidence.

Generated with: gpt-3.5-turbo 16,384 context

Introduction:
The incident response investigation was conducted to analyze and understand a series of sophisticated cyber intrusions across multiple endpoints within the organization's network. The purpose was to identify the scope and impact of the attacks, assess the potential risks posed to the organization, and recommend mitigation strategies to enhance cybersecurity defenses. The incidents highlighted in the investigation signify a significant threat to the organization's data security and operational continuity.

Summary of Findings:
The forensic timeline summaries revealed a pattern of coordinated attacks across the endpoints, indicating the presence of a persistent and sophisticated threat actor. The attackers employed various techniques such as command and control activities, defense evasion tactics, lateral movement through remote services, execution via PowerShell, credential access through OS credential dumping, and attempts to establish persistence through registry modifications and autostart mechanisms. These actions suggest a targeted effort to gain unauthorized access, escalate privileges, and potentially exfiltrate sensitive data from the organization's network.

Root Cause Analysis:
The root cause of the incidents can be attributed to vulnerabilities in the organization's cybersecurity defenses, including inadequate endpoint protection, weak password policies, and insufficient monitoring of network traffic. Misconfigurations in remote services like RDP and inadequate user privilege management also contributed to the successful execution of the attacks. The lack of robust detection mechanisms and timely response protocols further enabled the threat actor to operate undetected within the network, escalating the severity of the incidents.

Impact Assessment:
The incidents have had a significant impact on the organization, compromising data integrity, operational continuity, and potentially exposing sensitive information to unauthorized access. The attacks have highlighted weaknesses in the organization's cybersecurity posture, raising concerns about the potential for further breaches and data exfiltration. The incidents underscore the critical need for immediate remediation actions, enhanced security measures,

Investigation Summary

and comprehensive cybersecurity training for staff to mitigate future risks and safeguard the organization's digital assets.

Forensics Analysis Summary:
The investigation uncovered a sophisticated intrusion characterized by a strategic use of various techniques to achieve the attackers' objectives while evading detection. Initial access was gained through the exploitation of PowerShell, Command and Scripting Interpreter, and Python scripts, allowing the adversary to establish a foothold within the network. Subsequently, the adversary executed malicious code, compressed files, and securely deleted files using a combination of scripting languages and legitimate tools.

To maintain persistence, the adversary manipulated registry run keys, startup folders, and leveraged Windows Management Instrumentation Event Subscription to ensure continued access to compromised systems. They also employed software deployment tools like PsExec to move laterally through the network, potentially gaining remote code execution on multiple systems. Additionally, the adversary injected portable executables into processes, evading process-based defenses and potentially escalating privileges.

Throughout the intrusion, the adversary employed defense evasion techniques such as masquerading, right-to-left override, process injection, and portable executable injection to disguise malicious files, evade detection, and run code within the context of legitimate processes like lsass.exe. The deliberate effort to evade detection through obfuscation, event-triggered execution, and the strategic use of legitimate tools indicates a well-planned and coordinated attack aimed at achieving their objectives while remaining undetected within the network.

Access and Mobility Analysis:
The coordinated attack focused on Privilege Escalation and Credential Access tactics. Adversaries targeted LSASS memory through PowerShell commands and malicious executables to extract sensitive credential materials, demonstrating a strategic approach to escalate privileges and potentially move laterally within the network. The use of tools like Mimikatz and procdump further emphasizes the intent to harvest credentials for unauthorized access. The combination of PowerShell execution and LSASS manipulation underscores a calculated effort to exploit system vulnerabilities and gain higher-level permissions, posing a significant threat to the security of the endpoints and network.

The adversaries initially gained access by running malicious PowerShell scripts, establishing a foothold on the network. They then leveraged remote services like SSH, WinRM, and RDP to move laterally across systems, potentially

Investigation Summary

exploring the network and escalating privileges. Exploitation of software deployment tools and legitimate protocols like WMI and ARD enabled the adversaries to execute commands, blend in with normal traffic, and maintain persistence within the network. This strategic and persistent approach aimed at compromising multiple systems highlights a sophisticated attack strategy.

Data Movement and Exfiltration Analysis:
The sophisticated adversary operation focused on data movement tactics aligned with MITRE ATT&CK. The adversaries initiated Ingress Tool Transfer activities, introducing tools like Mimikatz and python.exe into compromised environments, indicating a strategic approach towards Collection. Subsequently, they engaged in Exfiltration techniques, utilizing cloud storage and web services to transfer data out of victim networks, aligning with the Exfiltration tactic. Command and Control was evident through the use of external systems to control compromised devices and move data, showcasing a coordinated effort to maintain communication and control within the victim's network. Additionally, the compression of data files using 'Rar.exe' highlighted potential data staging activities, emphasizing the adversaries' intent to manipulate data movement for their objectives. These actions underscore the critical need for thorough investigation and response to mitigate further risks and protect data integrity.

NASHUA.dmevals.local Summary

Endpoint Name: NASHUA.dmevals.local
Operating System: Windows
First Event Timestamp: 05/02/2020 02:55:24
Last Event Timestamp: 05/02/2020 08:29:22
Observed IP Addresses: 10.0.1.6
Observed Users: DMEVALS\pbeesly, pbeesly

Summary of Findings:
The investigation uncovered a sophisticated attack aimed at lateral movement within the network. The adversary, utilizing the compromised account 'pbeesly' from the domain 'DMEVALS.LOCAL', engaged in lateral movement activities through Remote Services and Software Deployment Tools. Notably, the creation of suspicious files like 'python.exe' and 'PSEXESVC.exe' in critical system directories, along with repeated logon events and network connections to remote IPs, suggests a deliberate effort to move laterally and establish persistence. The use of PowerShell and command-line interpreters further facilitated the execution of malicious commands, indicating a multi-stage attack strategy.

Root Cause Analysis:
The incident's root cause can be attributed to the initial compromise of valid domain credentials, potentially through phishing or credential harvesting techniques. Weaknesses in endpoint security configurations allowed the adversary to leverage legitimate tools and protocols for unauthorized lateral movement. The presence of unauthorized files like 'python.exe' and 'PSEXESVC.exe' underscores potential gaps in endpoint protection and monitoring, enabling the adversary to execute malicious code and move laterally across the network undetected.

Impact Assessment:
The incident has had a significant impact on network security and data integrity. The unauthorized lateral movement activities have compromised the confidentiality and availability of sensitive information stored on endpoints. The exfiltration of data, as evidenced by the compression and archiving of files into 'working.zip', poses a severe risk to data confidentiality. Furthermore, the use of tools like 'sdelete64.exe' for file deletion indicates attempts to cover tracks, potentially hindering forensic analysis and incident response efforts. The incident underscores the critical need for enhanced endpoint security measures and continuous monitoring to detect and respond to such advanced threats effectively.

Tradecraft, Access, Mobility, and Data Movement Summary:
The timeline reveals a sophisticated intrusion where the adversary utilized various techniques to gain initial access, execute malicious code, maintain persistence, and evade detection. The adversary started by executing Python

NASHUA.dmevals.local Summary

scripts through the command-line interpreter, followed by leveraging PowerShell to run commands for file compression. Subsequently, they used the Windows Command Shell to securely delete files, indicating a deliberate attempt to cover their tracks.

Furthermore, the adversary exploited software deployment tools to move laterally within the network, potentially aiming to gain remote code execution on multiple systems. This strategic use of legitimate tools showcases a calculated approach to maintain access and potentially exfiltrate sensitive information without raising suspicion. The modifications made to the registry settings suggest an effort to ensure their tools and actions remain undetected by security measures.

The timeline data reveals a series of events indicating lateral movement and remote execution within the network. An adversary, using valid credentials, leveraged remote services such as SSH and VNC to access systems remotely. This access allowed them to move laterally through the network, potentially exploring and gaining control over multiple systems. Additionally, the adversary exploited software deployment tools to execute malicious code, enabling them to move laterally and potentially perform actions like data exfiltration or system compromise.

On May 2, 2020, at 03:16:19 UTC, an adversary executed the 'Rar.exe' utility on a Windows system to compress data files located on the user's desktop and in the AppData directory. This action aligns with the Collection tactic (TA0009) as the adversary archived the collected data using a compression utility. The use of 'Rar.exe' to create a ZIP file suggests an attempt to obfuscate and minimize the data for exfiltration, indicating a potential data staging activity.

The compression of data files using 'Rar.exe' falls under the Archive via Utility technique (TA0009.T1560.001), where adversaries leverage utilities to compress and encrypt data before exfiltration. By compressing the data, the adversary aims to make the exfiltration process more efficient and less conspicuous. This technique is commonly employed to avoid detection and facilitate the transfer of stolen information over the network.

The execution of 'Rar.exe' to compress data aligns with the Exfiltration tactic (TA0010), where adversaries aim to steal data from the target network. The use of compression utilities like 'Rar.exe' enables adversaries to prepare the stolen data for exfiltration while minimizing the risk of detection during the data transfer process. This action indicates a deliberate effort to conceal the exfiltrated data and maintain operational security.

NASHUA.dmevals.local Summary

Overall, the timeline event showcases a coordinated effort by the adversary to collect, archive, and potentially stage data for exfiltration. The use of 'Rar.exe' for data compression highlights the adversary's intent to manipulate data movement to achieve their objectives while evading detection. This activity underscores the importance of monitoring and detecting suspicious data movement techniques as part of a robust cybersecurity defense strategy.

NEWYORK.dmevals.local Summary

Endpoint Name: NEWYORK.dmevals.local
Operating System: Windows
First Event Timestamp: 05/02/2020 02:55:25
Last Event Timestamp: 05/02/2020 08:29:21
Observed IP Addresses: 10.0.0.4
Observed Users: pbeesly, DMEVALS\mscott, dschrute, mscott, kmalone

Summary of Findings:
The investigation of the endpoint 'NEWYORK.dmevals.local' running Windows OS has uncovered a series of concerning events indicating potential malicious activities. The timeline analysis reveals unauthorized access and potential credential theft. Notably, user 'mscott' executed a suspicious process 'm.exe' involving OS credential dumping techniques targeting the LSASS memory, posing a significant risk of compromising sensitive account login information. Anomalies such as the creation of 'm.exe' and subsequent requests for Kerberos tickets suggest coordinated malicious activities aimed at escalating privileges within the network, possibly orchestrated by a common threat actor.

Root Cause Analysis:
The root cause of the incident appears to be the exploitation of system vulnerabilities, enabling unauthorized processes and credential dumping. The initial compromise may have resulted from inadequate security measures or social engineering tactics that granted the adversary access to the network. The use of legitimate credentials, particularly by user 'mscott,' underscores potential weaknesses in access control mechanisms that facilitated the unauthorized activities.

Impact Assessment:
The incident poses a severe threat to the organization's operations and data integrity. Unauthorized access and potential credential theft could lead to further system exploitation, data exfiltration, or persistent access by threat actors. The compromise of sensitive credentials not only jeopardizes affected systems but also the overall security posture of the organization. Immediate action is crucial to contain the incident, conduct further investigations for additional compromises, and enhance security measures to prevent future incidents.

Access Summary:
The sophisticated attack on 'NEWYORK.dmevals.local' aimed at escalating privileges and gaining unauthorized access to sensitive information is evident from the timeline analysis. The adversary executed OS credential dumping, specifically targeting LSASS memory to extract credential material. By using a malicious executable, the attacker attempted to inject code to retrieve account login details, potentially including the highly privileged krbtgt account.

NEWYORK.dmevals.local Summary

Furthermore, the adversary leveraged system libraries and processes to facilitate credential dumping, demonstrating a deep understanding of the target environment. Tools like procdump and mimikatz were employed to harvest credentials for lateral movement within the network. Loading specific SSP DLLs into LSASS process memory indicates a strategic approach to accessing encrypted and plaintext passwords stored within the Windows system.

The timeline depicts a well-planned attack focused on privilege escalation and credential theft, showcasing the adversary's sophisticated understanding of system vulnerabilities and deliberate efforts to obtain elevated permissions, posing a significant threat to the network's confidentiality and integrity.

UTICA.dmevals.local Summary

Endpoint Name: UTICA.dmevals.local
Operating System: Windows
First Event Timestamp: 08/25/2011 18:27:29
Last Event Timestamp: 05/02/2020 08:29:23
Observed IP Addresses: 10.0.1.5
Observed Users: DMEVALS\mscott, DMEVALS\dschrute, dschrute

Summary of Findings:
The investigation revealed a series of concerning events indicating a sophisticated attack involving Command and Control techniques, specifically Ingress Tool Transfer. The adversary successfully transferred tools into the compromised environment, utilizing various obfuscation and evasion tactics to avoid detection. Notably, the adversary leveraged PowerShell commands, registry modifications, and lateral movement techniques to spread their influence across the network. The timeline suggests a coordinated effort to establish persistence, exfiltrate data, and conduct credential dumping activities, indicative of a well-planned and persistent threat actor.

Root Cause Analysis:
The root cause of the incident appears to stem from vulnerabilities in the network's security posture, allowing the adversary to exploit weaknesses in tool transfer mechanisms, PowerShell usage, and registry modifications. Misconfigurations in system settings and inadequate monitoring of lateral movement activities facilitated the attacker's ability to move laterally and escalate privileges within the network. The use of common tools like certutil.exe and PowerShell for malicious activities underscores the importance of securing and monitoring these utilities to prevent unauthorized access and data exfiltration.

Impact Assessment:
The incident has had a significant impact on operations, data integrity, and security posture. The compromise of systems through Command and Control activities has potentially exposed sensitive data to unauthorized access and exfiltration. The adversary's actions have disrupted normal operations, compromised system integrity, and potentially compromised user credentials, posing a severe risk to the confidentiality, integrity, and availability of the organization's data and systems. Immediate remediation and enhanced security measures are crucial to mitigate further damage and prevent future incidents.Tradecraft Summary:
The timeline data reveals a sophisticated intrusion where the adversary utilized various techniques across different MITRE tactics. The initial access was gained through the exploitation of PowerShell and Command and Scripting Interpreter to run malicious code, allowing the adversary to establish a foothold within the network. Subsequently, the adversary employed obfuscation

UTICA.dmevals.local Summary

techniques to evade detection, using tools like certutil.exe to decode and execute malicious payloads.

To maintain persistence, the adversary leveraged Windows Management Instrumentation Event Subscription, enabling them to execute arbitrary code triggered by specific events, ensuring continued access to the compromised systems. Additionally, the adversary utilized software deployment tools to move laterally through the network, potentially aiming to escalate privileges or cause widespread impact.

The timeline indicates a deliberate and targeted intrusion, with a focus on maintaining access, evading detection, and potentially expanding control within the network. The use of PowerShell, obfuscation, event-triggered execution, and software deployment tools suggests a well-planned and persistent threat actor seeking to achieve their objectives while remaining undetected.Access Summary:
The timeline reveals a series of events indicating a sophisticated attempt at privilege escalation and credential access. The adversary initially focused on OS credential dumping, specifically targeting LSASS memory to extract login credentials. By executing commands to access and extract credential materials from LSASS, the adversary aimed to elevate their privileges and potentially move laterally within the network. This technique allows them to obtain sensitive information and potentially gain access to restricted areas.

Furthermore, the adversary leveraged PowerShell to execute scripts aimed at dumping credentials and accessing cached domain credentials. By utilizing tools like Mimikatz and invoking specific commands, they attempted to extract and manipulate credentials, potentially for the purpose of gaining unauthorized access or escalating their privileges within the network. These actions demonstrate a clear intent to steal account names and passwords, a critical step in advancing their attack objectives.

Overall, the timeline illustrates a strategic and persistent effort by the adversary to exploit vulnerabilities and weaknesses in the system to escalate their privileges and access sensitive information. The combination of privilege escalation techniques and credential access methods highlights a calculated approach to gaining higher-level permissions and potentially achieving their malicious goals within the network.Mobility Summary:
The timeline data reveals a series of events indicating a sophisticated attack involving lateral movement and remote execution techniques. Initially, the adversary gains a foothold by running malicious PowerShell scripts on a system, allowing them to explore the network. Subsequently, the adversary leverages remote services such as Windows Management Instrumentation (WMI) and Windows Remote Management (WinRM) to move laterally across systems, executing commands and payloads to gather information and potentially escalate privileges.

UTICA.dmevals.local Summary

Furthermore, the adversary exploits Remote Desktop Protocol (RDP) to log into remote systems, potentially using valid accounts obtained through previous stages of the attack. This allows them to interact with systems and expand their access within the network. The use of legitimate protocols and services, such as RDP and WinRM, enables the adversary to blend in with normal network traffic, making detection more challenging.

Overall, the timeline highlights a coordinated effort by the adversary to move laterally within the network, utilizing a combination of remote execution and lateral movement techniques to achieve their objectives. The use of various remote services and protocols demonstrates a multi-faceted approach to compromising systems and potentially exfiltrating sensitive data.Data Movement Summary:
On May 1st, an adversary initiated an Ingress Tool Transfer using Windows PE to retrieve Mimikatz from an external system. This action was followed by another Ingress Tool Transfer on May 2nd, where the adversary leveraged certutil.exe to decode and create a file in the victim's system. These events indicate a pattern of tool transfer into the compromised environment, aligning with the Collection tactic.

Shortly after, on the same day, the adversary engaged in Exfiltration techniques. They exfiltrated data to cloud storage using net.exe to access a cloud storage service and transfer data over HTTPS. This action was coupled with network connections to an external IP, showcasing data being moved out of the victim's network. The use of cloud storage and web services for exfiltration aligns with the Exfiltration tactic.

The combination of Ingress Tool Transfer and Exfiltration over Web Service and Cloud Storage suggests a coordinated effort by the adversary to gather tools, potentially for data exfiltration purposes. The Command and Control tactic is evident in the adversary's use of external systems to control compromised devices and move data, indicating a strategic approach to maintain communication and control within the victim's network.

Overall, the timeline reveals a sophisticated operation where the adversary collected tools, exfiltrated data through various channels, and maintained control over compromised systems. The intent appears to be data theft, with the potential for further impact on the victim's systems and data integrity.

SCRANTON.dmevals.local Summary

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows
First Event Timestamp: 08/25/2011 18:27:29
Last Event Timestamp: 05/02/2020 08:29:16
Observed IP Addresses: 10.0.1.4
Observed Users: DMEVALS\pbeesly, pbeesly, DMEVALS\mscott, DMEVALS\kmalone, kmalone

Summary of Findings:
The investigation revealed a series of concerning events indicating a sophisticated attack on the network. Initially, an Ingress Tool Transfer was detected, involving the download of a Windows Portable Executable file (sha256: ed3e182db635685ad65071473ec1dbaed5fde9f3014716f734b9816b73ac0905) via python.exe from IP 192.168.0.4. Subsequently, the execution of a malicious script disguised as 'cod.3aka3.scr' was observed, leading to the creation of malicious files like 'Draft.Zip' and 'monkey.png' in the user's directories. These actions culminated in the establishment of persistence mechanisms through registry modifications and the deployment of malware like 'javamtsup.exe' and 'hostui.exe' across the network.

Root Cause Analysis:
The incident's root cause can be attributed to multiple factors, including the initial compromise through an Ingress Tool Transfer, likely facilitated by inadequate network segmentation or weak endpoint security controls. The execution of malicious scripts and the subsequent lateral movement through tools like PsExec64.exe exploited misconfigurations in user permissions and insufficient monitoring of network activities. Additionally, the use of PowerShell for various malicious activities underscores the importance of monitoring and restricting PowerShell usage to prevent unauthorized actions.

Impact Assessment:
The impact of this incident is significant, with potential compromises to data integrity, network confidentiality, and operational stability. The presence of persistent malware and unauthorized access tools poses a continued threat to the network's security posture. The exfiltration of sensitive data, such as private keys and the deployment of remote services like Remote Desktop Protocol, could lead to further data breaches and unauthorized access. Immediate remediation actions, including thorough system scans, patching vulnerabilities, and enhancing network security controls, are crucial to mitigating the ongoing risks posed by this incident.Tradecraft Summary:
The timeline reveals a sophisticated intrusion where the adversary employed various techniques to gain initial access, execute malicious code, maintain persistence, and evade detection. The adversary utilized tactics such as masquerading and right-to-left override to disguise malicious files and

SCRANTON.dmevals.local Summary

scripts, aiming to trick users and security tools. This initial access allowed the adversary to execute PowerShell commands and scripts, leveraging the powerful capabilities of PowerShell for discovery and code execution.

To maintain persistence, the adversary manipulated registry run keys and startup folders, ensuring that their malicious code would run automatically upon system boot or user logon. Additionally, the adversary used software deployment tools like PsExec to move laterally through the network, potentially gaining remote code execution on multiple systems. The adversary also injected portable executables into processes, evading process-based defenses and potentially elevating privileges.

The timeline indicates a deliberate effort by the adversary to evade detection through defense evasion techniques like process injection and portable executable injection. By running code in the context of legitimate processes like lsass.exe, the adversary aimed to access system resources and potentially elevate privileges. The use of PowerShell for command and scripting interpretation further enabled the adversary to execute arbitrary commands and scripts, potentially leading to data exfiltration or further compromise.

Overall, the timeline suggests a targeted intrusion with a focus on gaining persistent access, executing malicious code, and evading detection. The adversary's use of multiple techniques across different MITRE tactics indicates a well-planned and coordinated attack aimed at achieving their objectives while remaining undetected within the network.Access Summary:
The timeline data reveals a concerning sequence of events related to Privilege Escalation and Credential Access. Initially, there was an execution of a PowerShell command by a user account named 'pbeesly' to interact with an image file, which could potentially be a method to obfuscate malicious activities. Shortly after this, there was an attempt to access the LSASS process, a critical system component that stores credential materials, indicating an interest in obtaining sensitive information. This action aligns with the Credential Access technique of targeting LSASS memory to steal account credentials.

The PowerShell execution and subsequent targeting of LSASS suggest a potential strategy to escalate privileges by harvesting credentials. By accessing LSASS memory, adversaries can retrieve valuable information like passwords stored in plaintext or encrypted forms. This technique not only enables the theft of credentials but also sets the stage for lateral movement within the network, as compromised credentials can be leveraged to access additional systems and resources.

The combination of PowerShell execution, which can be used for various

SCRANTON.dmevals.local Summary

malicious activities, and the focus on LSASS memory highlights a sophisticated approach to privilege escalation and credential theft. These actions underscore the importance of monitoring and securing critical system processes like LSASS to prevent unauthorized access and potential misuse of privileged information.Mobility Summary:
The timeline data reveals a series of events indicating a sophisticated attack involving lateral movement and remote execution techniques. Initially, the adversary leveraged PowerShell to run malicious code, establishing a foothold on the network. Subsequently, they utilized remote services like SSH and WinRM to move laterally across systems, potentially exploring the network and gaining access to remote machines.

Furthermore, the adversary exploited software deployment tools to execute commands on various endpoints, potentially aiming to propagate their access and control throughout the network. This method allowed them to move laterally and potentially escalate privileges across different systems. Additionally, the use of PsExec to execute commands on remote systems further demonstrates the adversary's intent to expand their reach within the network.

The timeline culminates in the use of Remote Desktop Protocol (RDP) for lateral movement, enabling the adversary to log into systems remotely. This technique could facilitate persistent access and control over compromised endpoints, indicating a strategic effort to maintain a presence within the network. Overall, the combination of remote execution and lateral movement techniques suggests a coordinated and persistent attack aimed at compromising multiple systems within the network.Data Movement Summary:
On April 30, 2020, at 00:35:26 UTC, an event related to Command and Control occurred, specifically focusing on Ingress Tool Transfer. This activity involved the transfer of a Windows Portable Executable (PE) file, identified as a Windows EXE, with a specific SHA256 hash, from an external system to a compromised environment. The file, python.exe, was downloaded from an IP address (192.168.0.4) to a Windows system. This action aligns with the adversary's attempt to establish communication and control within the victim network.

The transfer of this executable file could be indicative of an initial stage in a potential data theft operation. By introducing tools into the compromised environment, adversaries may be preparing to collect sensitive information as part of their Collection tactic. Subsequently, these tools could be utilized for exfiltration purposes, allowing the adversaries to steal data from the network. The use of various utilities and protocols for file transfer, such as PowerShell commands on Windows systems, suggests a deliberate effort to remain stealthy and avoid detection while moving towards their end goal.

SCRANTON.dmevals.local Summary

This sequence of events highlights a concerning pattern of data movement and potential data staging within the victim network. The adversaries' actions align with the tactics of Collection, Exfiltration, Command and Control, and potentially Impact, indicating a sophisticated and strategic approach towards achieving their objectives. The presence of these tools in the compromised environment raises alarms about the adversaries' intent to gather, exfiltrate, and potentially manipulate or disrupt data, emphasizing the critical need for thorough investigation and response to mitigate further risks.