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: Mistral Large Instruct 2407 IQ2 XXS 32,768k context

Endpoint Forensics Report

The following endpoint forensics report details a sophisticated and coordinated attack on our network, involving multiple endpoints: SCRANTON, UTICA, NASHUA, and NEWYORK. The attack commenced on May 2nd at 02:58 UTC with the execution of a PowerShell script on SCRANTON, marking the first instance of lateral movement using remote services (T1021). This activity continued with connections to multiple IP addresses and ports, including attempts to access RDP services. Around 03:11 UTC, the adversary began using software deployment tools like PsExec64.exe for further lateral movement, targeting user credentials and attempting to run Python scripts on remote systems until at least 03:28 UTC. Notably, logon events were recorded for user 'pbeesly' from a remote IP address, indicating successful lateral movement.

Simultaneously, at 07:55 UTC on UTICA, the adversary executed another PowerShell script, initiating network connections over port 443 to download additional payloads or instructions. By 07:58 UTC, they escalated their efforts using PowerShell to download and execute a malicious file from an external server. This activity continued until 08:21 UTC with multiple network connections established over ports 443 and 5985, leveraging techniques like Remote Services (T1021), Windows Management Instrumentation (T1047), and RDP for lateral movement.

On May 5th at 03:10:24 UTC, the adversary continued their campaign on NASHUA by logging into a remote service using valid accounts and accessing network share objects. They executed processes like 'PSEXESVC.exe' and 'python.exe' under various user contexts to maintain control over multiple systems. This pattern of logins and process executions continued, with repeated access to network share objects and execution of 'python.exe' and 'conhost.exe'. The final recorded event at 03:15:03 UTC showed the execution of 'PSEXESVC.exe' and 'python.exe', again under different user contexts.

Throughout these events, the adversary demonstrated a systematic effort to compromise and control multiple systems within the network, leveraging remote execution (TA0002) and lateral movement (TA0008) tactics. They used valid accounts, software deployment tools, and remote services to move stealthily across the network while avoiding detection.

Investigation Summary

Concurrent with these activities, significant events were observed in the attack timeline that indicate a coordinated attack across multiple endpoints. Notable activities include the transfer of suspicious executables via command and control channels, execution of PowerShell scripts, registry modifications, credential dumping, and lateral movement. Patterns suggest a sophisticated intrusion involving command and control, persistence, evasion, credential access, lateral movement, and remote control.

The attack on SCRANTON began at 02:58 UTC with Initial Access (TA0001) via execution of a masqueraded file. Persistence (TA0003) was established through registry modifications and PowerShell scripts hidden within an image file. Between 03:04 and 03:21 UTC, Execution (TA0002) of PowerShell scripts and file deletions using SDelete were observed, indicating active exploration and evidence removal. At 05:05 UTC, process injection targeting 'lsass.exe' signaled further Execution (TA0002) and Defense Evasion (TA0005). Throughout the attack, PowerShell was extensively used for command and scripting, with PsExec64 employed for lateral movement. The final observed action at 03:21 UTC involved an obfuscated PowerShell script, suggesting ongoing evasion efforts.

At 07:58 UTC on UTICA, Initial Access (TA0001) was achieved via PowerShell commands executing malicious code. Defense Evasion (TA0005) was noted with a script downloaded from an external URL disabling security measures. Between 07:58 and 08:21 UTC, Execution (TA0002) of PowerShell commands decoded blobs and ran executables like 'm.exe'. At 08:34 UTC, a rundll32 command loaded a DLL from a suspicious path, indicating further Defense Evasion (TA0005). Persistence (TA0003) was evident through WMI event subscriptions and registry modifications.

NASHUA's attack commenced at 03:16 UTC with Execution (TA0002) of a Python script, followed by PowerShell and Command Shell processes. Data exfiltration was suggested by file compression using Rar.exe. Defense Evasion (TA0005) was prominent as cmd.exe and sdelete64.exe deleted files, including the archive and other system files. Registry modifications showed acceptance of SDelete's EULA, indicating deliberate use of tools to cover tracks.

On May 2nd, multiple endpoints within the network were targeted by a series of sophisticated attacks aimed at privilege escalation and credential access. The earliest activity was recorded at 07:59:10 UTC on UTICA, where 'm.exe' attempted to dump credentials from LSASS memory, followed by similar activities on NEWYORK at 08:04:25 UTC. PowerShell commands were executed on SCRANTON at 02:57:44 and later on UTICA around 08:13:26, indicating the use of mimikatz and kerberos golden ticket creation to impersonate users and facilitate lateral movement.

Investigation Summary

The attackers employed a systematic approach, using processes like 'lsass.exe', 'wininit.exe', and 'services.exe' to access system-level processes and manipulate cached domain credentials. Notably, the LSASS process was targeted on all endpoints, with SCRANTON showing an additional attempt at 03:16:16. The loading of libraries such as 'cryptdll.dll', 'samlib.dll', and 'hid.dll' on NEWYORK further supports the credential dumping activities.

The consistent use of 'm.exe' with commands like 'sekurlsa::logonpasswords exit' and 'lsadump::lsa /inject /name:krbtgt' across endpoints suggests a coordinated effort to extract sensitive information from the systems' memory, aligning with MITRE ATT&CK techniques TA0006 (Credential Access) and TA0004 (Privilege Escalation). The attackers' focus on LSASS memory dumping and cached domain credentials indicates a clear intent to gain higher-level permissions and facilitate further unauthorized access within the network.

On April 30th, at 00:35 UTC, an adversary initiated suspicious file transfers on SCRANTON, indicating potential command and control establishment (TA0011) by transferring a Windows executable named 'python.exe' from an internal IP address. This activity suggests preparation for further commands or data collection routines, signaling risks of data exfiltration (TA0010) and network integrity impact (TA0040).

On May 1st, at 07:29 UTC on UTICA, an executable file named 'mimikatz' was transferred from an external IP address, suggesting further tool transfer via command and control channels. On May 2nd, at 03:46 UTC on NASHUA, a process executed 'Rar.exe', indicating data collection and archiving activities (TA009). The adversary created an archive file named 'working.zip' from files in the user’s AppData Roaming directory, preparing collected data for exfiltration.

Later on May 2nd, at 7:58 UTC on UTICA, a file named 'kxwn.lock' was created and decoded using 'certutil.exe', indicating additional tool transfer activity. At 08:39 UTC, the adversary attempted to exfiltrate data to Microsoft OneDrive (TA0010) and established a network connection to an external IP.

These activities across multiple endpoints show a clear pattern of data collection, control establishment, and data exfiltration, aligning with MITRE techniques TA09 Collection, TA0011 Command and Control, and TA0010 Exfiltration. The adversary's actions suggest preparation for data theft and potential network impact.

The root cause of the incident appears to be the transfer of malicious executables via command and control channels, followed by execution on

Investigation Summary

compromised endpoints. Vulnerabilities such as unauthorized network connections, weak passwords, and insufficient endpoint security contributed to the incident. Misconfigurations in registry settings and startup folder entries facilitated persistence mechanisms.

The incident has significant implications for operations and data integrity. Unauthorized access and lateral movement indicate a potential compromise of sensitive information. Credential dumping activities suggest that attackers may have gained access to user credentials, posing risks to further unauthorized access and data exfiltration. The use of cloud storage services indicates potential data loss. Immediate action is required to mitigate ongoing risks and secure the network.

NASHUA.dmevals.local Summary

Endpoint Forensics Report

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 incident timeline reveals a series of coordinated actions indicating an intrusion into the network beginning at 03:05:32 UTC on May 2, 2020. An initial network connection from IP address '10.0.1.6' to '10.0.0.4' over port 445 suggests a potential lateral movement attempt. This was followed by the creation and execution of suspicious files such as 'python.exe' and 'PSEXESVC.exe'. User 'pbeesly' logged in from remote IP '10.0.1.4' several times, with corresponding network share access events recorded. The execution of various scripts and commands, including PowerShell and Python interpreters, indicates a sophisticated attack pattern. The creation and deletion of files like 'Rar.exe', 'sdelete64.exe', and compressed archives suggest data exfiltration activities. Repeated logins, file creations, and executions point to a coordinated effort by an attacker to gain unauthorized access and manipulate the system. The use of legitimate tools like PowerShell for malicious purposes is a common tactic in advanced attacks.

Root Cause Analysis:
The root cause of this incident appears to be a combination of vulnerabilities and misconfigurations that allowed unauthorized access and lateral movement within the network. The initial network connection over port 445, commonly used for Windows file sharing services, suggests that open ports and weak authentication mechanisms were exploited. Repeated logins by user 'pbeesly' from remote IP addresses indicate a compromised account or improper access controls. The execution of suspicious files and scripts further highlights the presence of malware or unauthorized software on the system.

Impact Assessment:
The incident had significant implications for data integrity and operational security. The creation and execution of malicious files, combined with the exfiltration of sensitive data, poses a substantial risk to confidential information. The use of PowerShell scripts to compress and archive files indicates that the attacker was able to access and manipulate critical data. The deletion of files such as 'Rar.exe' and 'sdelete64.exe' suggests an attempt to cover tracks, making forensic analysis more challenging. Repeated network connections and file executions indicate a persistent threat within the

NASHUA.dmevals.local Summary

network, potentially leading to further compromises if not addressed promptly. The incident underscores the need for robust access controls, regular system audits, and proactive monitoring to detect and mitigate such threats effectively.

Incident Narrative:
The attack began on May 2nd at 03:15 UTC with the execution of a Python script by user 'DMEVALS\pbeesly'. This was followed by the initiation of PowerShell and Windows Command Shell processes, indicating the adversary's attempt to execute malicious code. The attacker then used Rar.exe to compress files into a hidden archive, suggesting data exfiltration or preparation for further actions. Subsequently, the adversary employed cmd.exe and sdelete64.exe to delete specific files, including the previously created archive and other files on the system. This action aligns with the Defense Evasion tactic, as the attacker aimed to remove traces of their activities. The use of software deployment tools like sdelete64.exe further indicates an attempt to leverage third-party applications for lateral movement or additional actions within the network.

The timeline data indicates a series of events suggesting an adversary's attempt to move laterally across the network and execute malicious code on multiple systems. The activity began at 03:10:24 UTC with user 'pbeesly' logging into a remote service from IP address 10.0.1.4 within the DMEVALS.LOCAL domain, followed by access to network share objects, indicating potential lateral movement using valid accounts and remote services. Subsequent events show the execution of various processes, including 'PSEXESVC.exe' and 'python.exe', initiated under different user contexts such as 'NT AUTHORITY\SYSTEM' and 'DMEVALS\pbeesly'. These executions suggest that the adversary was leveraging software deployment tools to gain remote code execution on multiple systems, a common technique in lateral movement tactics.

At 03:16:19 on May 2nd, a process executed on the endpoint, indicating potential data collection and archiving activities by an adversary. The process involved the execution of 'Rar.exe', a utility used for compressing and encrypting files, suggesting that the adversary was preparing collected data for exfiltration. The command line arguments showed the creation of an archive file named 'working.zip' from a source file located in the user's AppData Roaming directory. This activity aligns with the MITRE ATT&CK technique TA0009 Collection, specifically T1560 Archive Collected Data and T1560.001 Archive via Utility. The use of 'Rar.exe' to compress and encrypt data before exfiltration indicates that the adversary was likely preparing sensitive information for extraction from the network, aiming to obfuscate the data and minimize its size during transmission. This action is a precursor to potential exfiltration (TA0010), where the adversary would attempt to steal the data from the

NASHUA.dmevals.local Summary

compromised system. The user 'DMEVALS\pbeesly' was associated with this activity, suggesting that the adversary might have gained access to their account or is impersonating them.

Overall, these events point towards a staging phase in an attack lifecycle, where the adversary is preparing collected data for exfiltration while attempting to avoid detection. The incident underscores the need for robust security measures to prevent and mitigate such intrusions effectively.

NEWYORK.dmevals.local Summary

Endpoint Forensics Report

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

On May 2nd, 2020, a series of events occurred on the endpoint NEWYORK.dmevals.local indicating an unauthorized access attempt. At 8:04 AM UTC, suspicious activity was detected involving the execution of 'm.exe', which attempted to dump OS credentials and interacted with LSASS memory. This activity is associated with the MITRE ATT&CK technique T1003 (OS Credential Dumping). The process executed under the user 'DMEVALS\mscott' and created a file in the System32 directory, suggesting potential malicious intent.

The incident began at 8:04 AM UTC with the execution of 'm.exe', using the command '"C:\Windows\System32\m.exe" privilege::debug "lsadump::lsa /inject /name:krbtgt" exit'. This action was performed by the user 'DMEVALS\mscott' and is associated with the MITRE ATT&CK technique TA0006.T1003.001 (LSASS Memory). Simultaneously, several libraries were loaded, including 'cryptdll.dll', 'samlib.dll', 'hid.dll', and 'WinSCard.dll', which may have supported the credential dumping process. The LSASS process was also opened, indicating direct interaction with this critical system component. These activities are consistent with an adversary attempting to gain access to sensitive credential information, likely for lateral movement or further unauthorized access within the network.

The repeated execution and exit of 'm.exe' with the same command suggests a systematic approach to credential dumping, potentially automating the process. The involvement of LSASS memory dumping and the loading of various system libraries indicates a sophisticated attempt to gather sensitive information from the endpoint. This sequence of events aligns with both credential access (TA0006) and privilege escalation (TA0004) tactics, as the adversary seeks higher-level permissions and access to restricted information.

The root cause of this incident appears to be an unauthorized access attempt facilitated by the execution of 'm.exe'. The process executed under the user 'DMEVALS\mscott' and interacted with LSASS memory, indicating a potential exploitation of system vulnerabilities. The creation of files in the System32 directory suggests that the attacker may have leveraged elevated privileges to perform these actions.

NEWYORK.dmevals.local Summary

The incident had significant implications for data integrity and security. The unauthorized access attempt involved credential dumping, which could lead to further compromise if not mitigated promptly. The execution of 'm.exe' under the user 'DMEVALS\mscott' suggests that the attacker gained elevated privileges, posing a risk to sensitive data and system integrity. Additionally, the request for Kerberos service tickets indicates potential lateral movement within the network. Immediate action is required to contain the threat and assess the extent of the compromise.

Overall, these activities highlight a concerted effort to compromise the security of the endpoint by leveraging system weaknesses and misconfigurations, with potential implications for broader network security.

UTICA.dmevals.local Summary

Endpoint Forensics Report

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 timeline reveals a series of coordinated actions indicating an adversary's presence within the network. On May 1st, an unauthorized tool transfer was detected from an external system to the compromised environment, specifically a Windows PE file identified as 'mimikatz'. This tool is commonly used for credential dumping and other nefarious activities. Following this, on May 2nd, PowerShell scripts were executed, suggesting command and scripting interpreter usage. Notably, OS credential dumping was observed multiple times, with the 'm.exe' process being a recurrent actor. Patterns in the timeline suggest a coordinated effort to establish persistence and further compromise the network through event-triggered executions and WMI subscriptions.

Root Cause Analysis:
The root cause of this incident appears to be an initial unauthorized access leading to the transfer of malicious tools, such as 'mimikatz', into the environment. This was likely facilitated by a vulnerability or misconfiguration that allowed external communication and tool transfer. The use of PowerShell for script execution and the recurrent OS credential dumping activities indicate exploitation of administrative privileges and potential lateral movement within the network.

Impact Assessment:
The incident has significant implications for operational security, data integrity, and overall network health. The unauthorized tool transfer and subsequent credential dumping activities suggest that sensitive information may have been compromised. Persistent threats, such as event-triggered executions via WMI subscriptions, indicate an ongoing risk to the network's integrity. Immediate remediation actions are required to contain the threat and mitigate further damage. The incident underscores the need for enhanced security measures, including regular audits of administrative privileges and monitoring of external communications.

Incident Narrative:
On May 2nd, 2020, a series of suspicious activities were detected on a Windows system within the network, indicating potential credential access, privilege

UTICA.dmevals.local Summary

escalation, lateral movement, and data exfiltration by an adversary. The timeline begins at 07:59:10 UTC with the execution of 'm.exe', a process that attempted to dump credentials from the Local Security Authority Subsystem Service (LSASS) memory using commands like 'sekurlsa::logonpasswords exit'. This activity continued with multiple library loads and process executions, including 'lsass.exe' and 'wininit.exe', suggesting an attempt to access and manipulate system-level processes.

At 07:55 UTC, the adversary began their attack by executing a PowerShell script, marking the first appearance of malware on the system. This script initiated a network connection to a remote IP address over port 443, likely attempting to download additional payloads or instructions. Subsequent activities involved further PowerShell executions and network connections, including interactions with Windows Management Instrumentation (WMI) and Remote Desktop Protocol (RDP).

By 07:58 UTC, the adversary had escalated their efforts, using PowerShell to download and execute a malicious file from an external server. This activity continued until 08:21 UTC, with multiple network connections established between the compromised system and various remote IP addresses, primarily over ports 443 and 5985. These actions suggest that the adversary was leveraging valid accounts to move laterally within the network, using techniques such as Remote Services, Windows Remote Management (WinRM), and RDP.

At 07:58 UTC, a PowerShell command downloaded and executed a script from an external URL, indicating potential initial access through network-based techniques. The script appeared to disable security measures and execute additional commands, suggesting defense evasion tactics. Between 07:58 and 08:09 UTC, multiple PowerShell commands were executed, including those that decode blobs and run executables like 'm.exe'. These actions align with execution tactics aimed at running adversary-controlled code on the system.

At 08:14 UTC, a rundll32 command was executed, loading a DLL from a suspicious path, which could be part of defense evasion techniques to hide malicious activities. Throughout the timeline, there were indications of persistence tactics, such as creating WMI event subscriptions and modifying registry values, suggesting that the adversary was attempting to maintain their foothold on the system.

On May 1st at 07:09:23 UTC, an executable file named 'mimikatz' was transferred to the system from an external IP address (192.168.0.4), suggesting an ingress tool transfer via command and control channels. The next day, on May 2nd at 07:55:27 UTC, a file named 'kxwn.lock' was created in the user directory, followed by its decoding using 'certutil.exe', indicating further tool transfer

UTICA.dmevals.local Summary

activity. Later that day, at 08:09:58 UTC, the adversary attempted to exfiltrate data to a cloud storage service (Microsoft OneDrive) using 'net.exe' and established a network connection to an external IP (13.107.42.12). These activities align with MITRE techniques for Collection, Command and Control, and Exfiltration, showing a clear pattern of data collection, control establishment, and data exfiltration.

The adversary's use of PowerShell scripts and remote services indicates a sophisticated approach to lateral movement, likely aiming to spread their control across multiple systems within the network. The consistent pattern of network connections and PowerShell executions suggests that the adversary was methodically expanding their access while maintaining stealth. This activity aligns with MITRE's Tactics, Techniques, and Procedures (TTPs) for Lateral Movement, specifically techniques like Remote Services and Windows Management Instrumentation.

Overall, the timeline reveals a systematic effort to compromise and control multiple systems within the network, leveraging remote execution and lateral movement tactics to achieve broader objectives. The use of PowerShell and other command interpreters is prominent, highlighting the versatility of these tools in cyber attacks. The incident underscores the need for enhanced security measures to prevent and detect such intrusions effectively.

SCRANTON.dmevals.local Summary

Endpoint Forensics Report

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 timeline reveals a sequence of events indicating an organized attack on the network starting from April 30th, 2020. Initially, an unauthorized tool transfer was detected, with a Python executable being downloaded from an internal IP address (192.168.0.4). On May 2nd, there were signs of malware execution and persistence mechanisms being established. A suspicious script named 'â€®cod.3aka3.scr' was executed, followed by PowerShell commands that modified the registry to include a hidden command involving an image file ('monkey.png'). This suggests an attempt to entrench the malicious presence on the system.

Root Cause Analysis:

The root cause of this incident appears to be an initial compromise allowing tool transfer into the network, followed by the execution and persistence of malware. The attacker leveraged PowerShell commands to execute scripts and modify the registry, enabling automatic startup of malicious processes. Vulnerabilities in the system's defenses allowed these actions to go undetected initially.

Impact Assessment:

The incident had significant implications for the network's security posture. The attacker successfully transferred tools into the environment and executed malware, establishing persistence mechanisms that could facilitate further attacks. This compromises data integrity and operational security. Additionally, credential dumping attempts were made, indicating a potential risk to user credentials. The overall impact includes compromised system integrity, potential data breaches, and increased risk of future attacks due to the established foothold in the network.

Narrative:

The attack began on April 30th, 2020, with an unauthorized tool transfer where a Python executable was downloaded from an internal IP address (192.168.0.4). On May 2nd at 02:55:56 UTC, the attacker executed a masqueraded file named 'â€®cod.3aka3.scr', likely disguised using Right-to-Left Override (RTLO)

SCRANTON.dmevals.local Summary

techniques to appear benign. At 02:58:18 UTC, the adversary established persistence through registry modifications, creating a startup routine that would execute PowerShell scripts hidden within an image file named 'monkey.png'.

Between 03:04 and 03:21 UTC, the PowerShell script was executed multiple times, suggesting active exploration of the network and potential information gathering. Several files were deleted using SDelete, a software deployment tool, indicating attempts to cover tracks and remove evidence of their activities. At 05:05:16 UTC, process injection targeting 'lsass.exe', a critical system process, was detected, suggesting privilege elevation or stealth maintenance efforts.

Throughout the attack, PowerShell was extensively used for command and scripting, with PsExec64 employed to execute Python scripts on remote systems, indicating lateral movement within the network. The final observed action at 03:21:28 UTC involved executing an obfuscated PowerShell script, further suggesting attempts to evade detection and maintain control over the compromised system.

At 04/30/2020 00:35:26, a suspicious file transfer occurred on the network. A Windows executable named 'python.exe' was downloaded from an internal IP address, indicating command and control efforts by transferring tools into the compromised environment. This activity suggests preparation for further commands or data collection routines, signaling potential risks of data exfiltration and impact on the network's integrity.

At 02:58:44 on May 2nd, a PowerShell command was executed by user 'DMEVALS\pbeesly', involving an image file ('monkey.png') located in the user's Downloads folder. This activity suggests potential obfuscation or encoding of data within the image file, part of a broader attack strategy. Shortly after, at 03:05:16, there was an attempt to access the LSASS process memory, targeting 'C:\windows\system32\lsass.exe', associated with credential dumping techniques aiming to extract sensitive information such as passwords from the system's memory.

The adversary began lateral movement activities by executing a PowerShell script on May 2nd at 02:58 UTC, establishing connections with multiple IP addresses and suggesting attempts to access various systems within the network. This pattern continued throughout the early morning hours, with notable connections to different IPs and ports, including attempts to connect to a remote desktop protocol (RDP) service at 03:20 UTC.

The attacker then shifted focus to using software deployment tools for lateral

SCRANTON.dmevals.local Summary

movement starting around 03:11 UTC, executing PsExec64.exe multiple times and attempting to run Python scripts on remote systems. This activity continued until at least 03:28 UTC, with connections made to various ports such as 445 and 135, indicating attempts to exploit different services on the targeted machines.

At 03:20 UTC, multiple logon events were recorded for user 'pbeesly' from a remote IP address, suggesting successful lateral movement and potential access to additional systems within the network. This sequence of events indicates a systematic effort by the adversary to gain control over multiple machines, likely with the intent to further compromise the network or gather sensitive information.