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: Mixtral 8x7b Instruct Q6 K 32,768 context

Executive Summary:
Incident Response Timeline Investigation Report

Introduction:
This report presents an executive summary of our incident response timeline investigation for the recent security event affecting SCRANTON, UTICA, NASHUA, and NEWYORK endpoints within the DMEVALS.LOCAL domain. The purpose of this investigation is to provide a clear overview of the incident's scope, objectives, and potential impact on the organization.

Summary of Findings:
Our analysis revealed several significant events across multiple endpoints in the DMEVALS.LOCAL domain. On SCRANTON, an adversary established a Command and Control (C2) channel using Risk Informational technique TA11.T1105.000 to transfer a Windows Portable Executable (PE) file on April 30th at 00:35:26 UTC. On May 2nd, the adversary executed an executable named 'â€®cod.3aka3.scr' using Risk High technique TA0002.T1036.002 Masquerading with Right-to-Left Override at 02:55:56 UTC. This resulted in the creation of a new file named 'Draft.Zip'.

On UTICA, an adversary executed a Windows PE file on May 1st at 07:09 UTC, indicating TA0011.T1105.000 Command and Control: Ingress Tool Transfer activity. On May 2nd, the adversary engaged in various techniques to evade detection, extract credentials, maintain persistence, exfiltrate data, and move laterally within the network.

On NASHUA, an intrusion attempt was observed on May 2nd at 03:05:32 UTC, involving a series of file creations, deletions, and network connections between local and remote IP addresses. The attacker also attempted to cover their tracks by using Sdelete64.exe to remove residual data from the system.

On NEWYORK, an intrusion attempt was observed on May 2nd at 8:02:44 AM UTC, involving OS credential dumping techniques and potential privilege escalation through Kerberos authentication tickets. The attacker may have gained access to sensitive information or attempted to move laterally within the network.

Root Cause Analysis:

Investigation Summary

The root cause of this incident can be attributed to vulnerabilities, misconfigurations, or weaknesses in the endpoints' security posture. These issues allowed the adversary to establish a command and control channel, execute malicious code, extract credentials, maintain persistence, exfiltrate data, and move laterally within the network.

Impact Assessment:
The incident has impacted operations, data integrity, and confidentiality across multiple endpoints in the DMEVALS.LOCAL domain. The adversary's actions have resulted in potential unauthorized access to sensitive information, disrupted normal business operations, and introduced security risks for the organization.

In conclusion, this incident highlights the importance of maintaining a robust endpoint security posture and implementing effective incident response measures. We recommend addressing identified vulnerabilities, misconfigurations, or weaknesses to prevent future incidents and ensure the continued protection of organizational assets.Tradecraft Summary:
Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'. The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Investigation Summary

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'. The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'. The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and

Investigation Summary

utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'. The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Investigation Summary

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'. The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'. The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

Investigation Summary

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'. The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'.

Investigation Summary

The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'. The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to

Investigation Summary

delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'. The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'. The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was

Investigation Summary

repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'. The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Investigation Summary

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'. The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'. The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and

Investigation Summary

utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'. The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Investigation Summary

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'. The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'. The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

Investigation Summary

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'. The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'.

Investigation Summary

The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'. The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to

Investigation Summary

delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'. The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'. The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was

Investigation Summary

repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'. The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Investigation Summary

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'. The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'. The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and

Investigation Summary

utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'. The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Investigation Summary

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'. The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'. The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

Investigation Summary

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'. The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'.

Investigation Summary

The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'. The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to

Investigation Summary

delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'. The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'. The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was

Investigation Summary

repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'. The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Investigation Summary

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'. The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'. The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and

Investigation Summary

utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'. The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Investigation Summary

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'. The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'. The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

Investigation Summary

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'. The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'.

Investigation Summary

The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a PowerShell script, followed by execution of additional commands using cmd.exe and Sdelete64.exe to delete files from the endpoint. The adversary demonstrated persistence by adding an autostart entry in the registry for continued access. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows

Analysis Summary:
On May 2nd, 2020 at approximately 1:35 AM UTC, an adversary executed a PowerShell script on a Windows endpoint using the user account 'DMEVALS\pam'. The script was used to modify the registry and add an autostart entry for persistence. At 1:47 AM UTC, the adversary executed a series of commands using cmd.exe and Sdelete64.exe, a command-line utility for securely deleting files, to delete files from the user's Temp directory. The same sequence of events was repeated for two additional directories on the user's desktop and in their home directory.

The adversary demonstrated proficiency with Windows command line tools and utilized PowerShell, cmd.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicateAccess Summary:
On May 2nd, 2020 at 7:59:10 AM UTC, an account with the name 'DMEVALS\dschrute' executed a command on their endpoint that attempted to dump credentials from the operating system and software using the tool Mimikatz. This action is consistent with the MITRE tactic Credential Access (TA0006) and sub-technique OS Credential Dumping (T1003).

Investigation Summary

At 8:04:25 AM UTC, a process execute event was triggered when 'm.exe' was executed with the command "C:\Windows\System32\m.exe" privilege::debug "lsadump::lsa /inject /name:krbtgt" exit as user DMEVALS\mscott with parent process ID 4176. This event is indicative of TA0006 Credential Access, specifically OS Credential Dumping (T1003) and LSASS Memory (T1003.001).

At 8:05:29 AM UTC, a process execute event was triggered when 'mimikatz.exe' was executed with the command "C:\Users\pam\Desktop\mimikatz.exe" privilege::debug exit as user DMEVALS\pam with parent process ID 1524. This event is indicative of TA0006 Credential Access, specifically OS Credential Dumping (T1003) and LSASS Memory (T1003.001).

At 8:07:56 AM UTC, an Invoke-Command was executed in a PowerShell session that ran Mimikatz with the command 'C:\Windows\System32\m.exe privilege::debug "lsadump::lsa /inject /name:krbtgt" exit'. This action is consistent with the MITRE tactic Credential Access (TA0006) and sub-technique OS Credential Dumping (T1003).

At 8:20:07 AM UTC, a user executed a command in PowerShell that ran Mimikatz with the command 'invoke-mimikatz-Evals -command "kerberos::golden /domain:dmevals.local / sid:S-1-5-21-1719095684-3458891352-3955206944 / [illegible] consistent with the MITRE tactic Credential Access (TA0006) and sub-technique OS Credential Dumping (T1003).

At 8:21:59 AM UTC, a user executed a command in PowerShell that ran Mimikatz with the command 'invoke-mimikatz-Evals -command "kerberos::golden /domain:dmevals.local / sid:S-1-5-21-1719095684-3458891352-3955206944 / [illegible] consistent with the MITRE tactic Credential Access (TA0006) and sub-technique OS Credential Dumping (T1003).

In summary, there were multiple instances of credential access on May 2nd, 2020. The first instance occurred at 7:59:10 AM UTC when an account with the name 'DMEVALS\dschrute' executed a command that attempted to dump credentials from the operating system and software using the tool Mimikatz. The second instance occurred at 8:04:25 AM UTC when 'm.exe' was executed with the command "C:\Windows\System32\m.exe" privilege::debug "lsadump::lsa /inject /name:krbtgt" exit as user DMEVALS\mscott with parent process ID 4176. The third instance occurred at 8:05:29 AM UTC when 'mimikatz.exe' was executed with the command "C:\Users\pam\Desktop\mimikatz.exe" privilege::debug exit as user DMEVALS\pam with parent process ID 1524. The fourth instance occurred at 8:07:56 AM UTC when an Invoke-Command was executed in a PowerShell session that

Investigation Summary

ran Mimikatz with the command 'C:\Windows\System32\m.exe privilege::debug "lsadump /inject /name:krbtgt" exit'. The fifth and sixth instances occurred at 8:20:07 AM UTC and 8:21:59 AM UTC respectively when a user executed commands in PowerShell that ran Mimikatz with the command 'invoke-mimikatz-Evals -command "kerberos::golden /domain:dmevals.local / s[illegible]alone /ptt"'. These events indicate a potential compromise of the system, as an adversary may be attempting to escalate privileges by dumping credentials from LSASS memory. It is recommended to investigate these events further and take necessary actions to secure the system, such as changing passwords for affected accounts and reviewing audit logs for any suspicious activity.Mobility Summary:

On May 2nd, 2020 at approximately 03:08 UTC, an endpoint with IP address 10.0.1.4 began making multiple network connections to various remote systems on ports 80 and 389. At 03:09 UTC, the same endpoint made a connection to an internal system over port 5985, indicating the use of Windows Remote Management for lateral movement. At 03:10 UTC, user 'pbeesly' remotely accessed a network share object on IP address 10.0.1.4 using Remote Services (TA0008.T1021.000). This was followed by the use of Software Deployment Tools (TA0008.T1072.000) to execute PSEXESVC.exe and python.exe, with conhost.exe also being executed as a child process of python.exe. The repeated pattern of Remote Services (TA0008.T1021.000) and Software Deployment Tools (TA0008.T1072.000) usage by user 'pbeesly' suggests an attempt at lateral movement throughout the network, potentially indicating a reconnaissance phase for further malicious activity. The execution of PSEXESVC.exe and python.exe may indicate attempts to establish remote command and control or execute malicious code on the target system. At 03:20 UTC, the same endpoint made a connection to an internal system over port 3389 using Remote Desktop Protocol (TA0008.T1076), indicating further lateral movement. These actions align with the MITRE tactics TA0002 - Execution and TA0008 - Lateral Movement, as they involve executing code on remote systems and moving through the network to expand access and gather information.

Analysis Summary:

On April 30th, 2020 at 00:35:26 UTC, an adversary transferred a tool or other file from an external system into the compromised environment through the command and control channel on SCRANTON.dmevals.local (TA0011). The next day, May 1st at 07:09:23 UTC, mimikatz was retrieved using TA0011 on UTICA.dmevals.local. On May 2nd, Rar.exe was executed on NASHUA.dmevals.local to archive and encrypt a file located on the desktop into a new zip file in the roaming directory (TA0009). At 07:55:26 UTC, certutil.exe was used to decode a blob file into kxwn.lock in the user's AppData directory using TA0011 on UTICA.dmevals.local again. At 08:09:58 UTC, net.exe was executed to connect to a OneDrive account with the username urukhai2020@outlook.com and password V@m0s0rc0!2020 using TA0010 on UTICA.dmevals.local, indicating data exfiltration may have occurred (TA0010). There is no evidence of any Impact

Investigation Summary

(TA0040) tactics being employed at this time. However, further investigation would be required to confirm whether the data was successfully exfiltrated and if it was altered in any way prior to transfer.

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

Executive Summary:
Summary of Findings:
On May 2nd, 2020, an adversary executed a Python script on a Windows endpoint using the user account 'DMEVALS\\pbeesly'. This was followed by the execution of PowerShell and Rar.exe, which were used to archive files in the user's AppData\Roaming directory. The archived file was then deleted from the Temp directory using Sdelete64.exe, a command-line utility for securely deleting files. This sequence of events was repeated for two additional directories on the endpoint.

The adversary demonstrated proficiency with Windows command line tools and utilized Python, PowerShell, Rar.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

Impact Assessment:
The impact of this incident includes potential data exfiltration, as sensitive files were targeted and compressed for extraction. The use of legitimate administrative tools like PowerShell and SDelete for malicious purposes further complicates the assessment of damage. It is crucial to review the contents of the archived file and investigate any unauthorized access or modification of critical data.

In conclusion, this incident underscores the importance of robust endpoint security, regular system patching, and vigilant monitoring of network activities. Further investigation is required to ascertain the full extent of the breach and identify potential threat actors.

Detailed Narrative:
On May 2nd, 2020 at 3:15 AM UTC, an adversary executed a Python script on a Windows endpoint using the user account 'DMEVALS\\pbeesly'. This was followed by the execution of PowerShell and Rar.exe, which were used to archive files in the user's AppData\Roaming directory. The archived file was then deleted from the Temp directory using Sdelete64.exe, a command-line utility for securely deleting files. This sequence of events was repeated for two additional directories on the endpoint.

NASHUA.dmevals.local Summary

The adversary demonstrated proficiency with Windows command line tools and utilized Python, PowerShell, Rar.exe, and Sdelete64.exe to execute commands and manipulate files on the endpoint. The use of these tools for file deletion may indicate an attempt to evade detection or cover their tracks.

The adversary's actions align with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The initial access was gained through user interaction with a Python script, followed by execution of additional commands using PowerShell and Rar.exe. The adversary demonstrated persistence by repeating the same sequence of events for multiple directories on the endpoint. Finally, the use of Sdelete64.exe to securely delete files is indicative of defense evasion techniques.

During this incident, user 'pbeesly' from domain DMEVALS.LOCAL remotely accessed a network share object on IP address 10.0.1.4 using Remote Services (TA0008.T1021.000). This was followed by the use of Software Deployment Tools (TA0008.T1072.000) to check for desired access on a network share object, specifically the Temp directory and python.exe file.

At 03:16 AM UTC, user 'pbeesly' again remotely accessed a network share object on IP address 10.0.1.4 using Remote Services (TA0008.T1021.000). This was followed by the use of Software Deployment Tools (TA0008.T1072.000) to execute PSEXESVC.exe and python.exe, with conhost.exe also being executed as a child process of python.exe.

The repeated pattern of Remote Services (TA0008.T1021.000) and Software Deployment Tools (TA0008.T1072.000) usage by user 'pbeesly' suggests an attempt at lateral movement throughout the network, potentially indicating a reconnaissance phase for further malicious activity. The execution of PSEXESVC.exe and python.exe may indicate attempts to establish remote command and control or execute malicious code on the target system.

On May 2nd, 2020 at 03:16:19 UTC, an executable named 'Rar.exe' was run from the temporary directory with the command to archive and encrypt a file located on the desktop into a new zip file in the roaming directory. This behavior aligns with the MITRE ATT&CK tactic Collection (TA0009) as it represents an attempt to gather data of interest, specifically by compressing and potentially encrypting it for easier transport. The use of encryption may also indicate an effort to avoid detection during exfiltration.

At this time, there is no evidence of the data being transferred out of the network, which would align with the Exfiltration (TA0010) tactic. However, the use of a third-party utility such as 7-Zip or WinRAR for archiving and encryption suggests that the adversary may have established Command and Control

NASHUA.dmevals.local Summary

(TA0011) over the system to execute this command.

Additionally, there is no indication at this time of any Impact (TA0040) tactics being employed, such as data manipulation or destruction. However, further investigation would be required to confirm whether the data was successfully exfiltrated and if it was altered in any way prior to transfer.

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:
On May 2nd, 2020, an adversary gained access to the DMEVALS network via a Windows machine (10.0.1.5) and proceeded to dump credentials from the operating system using the tool 'mimikatz'. The attacker then requested Kerberos authentication tickets for lateral movement within the network.

The adversary initiated their activities by executing wsmprovhost.exe, which spawned a new process (m.exe) that executed mimikatz to dump credentials from memory. This action was followed by the creation of a file named m.exe in C:\Windows\System32.

The attacker then requested Kerberos authentication tickets for lateral movement within the network, specifically targeting the krbtgt account. The adversary successfully obtained a Ticket Granting Ticket (TGT) and multiple service tickets, indicating they had gained access to the domain controller.

Tradecraft Summary:
The adversary employed credential dumping techniques using the tool 'mimikatz' to extract credentials from memory on a Windows machine. They then requested Kerberos authentication tickets for lateral movement within the network, specifically targeting the krbtgt account. The successful acquisition of a Ticket Granting Ticket (TGT) and multiple service tickets indicates that the adversary had gained access to the domain controller.

Access Summary:
On May 2nd, 2020 at 8:04:25 AM UTC, a process execute event was triggered when 'm.exe' was executed with the command "C:\Windows\System32\m.exe" privilege::debug "lsadump::dcsync /user:krbtgt" exit as user DMEVALS\mscott with parent process ID 4176. This event is indicative of TA0006 Credential Access, specifically OS Credential Dumping (T1003) and LSASS Memory (T1003.001). The execution of this command attempts to access credential material stored in the process memory of the Local Security Authority Subsystem Service (LSASS), which can be used for lateral movement and restricted information access.

Following the process execute event, several library load events were triggered including cryptdll.dll, samlib.dll, hid.dll, and WinSCard.dll. These libraries

NEWYORK.dmevals.local Summary

are commonly loaded when attempting to dump credentials from LSASS memory. An open process event was also triggered targeting 'C:\windows\system32\lsass.exe', which is the process that stores credential material in Windows.

The execution of this command and subsequent events indicate a potential compromise of the system, as an adversary may be attempting to escalate privileges by dumping credentials from LSASS memory. The use of 'm.exe' with the specified command suggests that the adversary has gained administrative access to the system and is using built-in Windows tools to dump credentials. It is recommended to investigate this event further and take necessary actions to secure the system, such as changing passwords for affected accounts and reviewing audit logs for any suspicious activity.

Mobility Summary:
The adversary's successful acquisition of a Ticket Granting Ticket (TGT) and multiple service tickets indicates that they have gained access to the domain controller. This level of access provides the adversary with the ability to move laterally within the network, potentially escalating privileges and gaining unauthorized access to sensitive data stored on other machines.

Data Summary:
The successful execution of 'mimikatz' for credential dumping highlights a broader issue with security controls and configurations within the DMEVALS environment. The presence of such tools indicates that the network may be vulnerable to similar attacks in the future, potentially leading to further exploitation of vulnerabilities or theft of confidential data.

Root Cause Analysis:
The root cause of this incident was an unpatched vulnerability on the Windows machine (10.0.1.5), which allowed the adversary to execute 'mimikatz' for credential dumping. The attacker likely exploited a known vulnerability or misconfiguration, enabling them to gain access and escalate privileges within the network.

Impact Assessment:
The incident had significant consequences on DMEVALS' operations, data integrity, and confidentiality. The adversary successfully obtained valid Kerberos authentication tickets for lateral movement within the network, potentially gaining access to sensitive information stored on other machines. This unauthorized access could lead to further exploitation of vulnerabilities or theft of confidential data.

Immediate action is required to identify and remediate any weaknesses

NEWYORK.dmevals.local Summary

contributing to this incident, ensuring the protection of sensitive data and systems. Recommended actions include patching known vulnerabilities, implementing multi-factor authentication, reviewing access controls, monitoring network traffic for suspicious activity, and conducting regular security audits.

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

On May 2nd, 2020 at approximately 7:55 UTC, an adversary initiated a series of actions on a Windows endpoint associated with the user DMEVALS\dschrute. The initial event involved the execution of PowerShell via conhost.exe, which is commonly used to execute command-line interfaces and scripts. Shortly after at 7:55:26 UTC, certutil.exe was executed in an attempt to decode a file named kxwn.lock located within the user's AppData\Roaming\Microsoft directory. This action is indicative of Defense Evasion (TA0005) as adversaries often abuse built-in system tools like certutil.exe to obfuscate their activities and evade detection.

At 7:57 AM UTC, the adversary executed csc.exe, a Ccompiler, multiple times with different command line arguments. This technique is consistent with Execution (TA0002) as it allows for the compilation and execution of malicious code on the target system. Following this, at 7:58 AM UTC, the adversary executed sdclt.exe, a Windows System File used to initiate Disk Cleanup, twice in quick succession. This action is likely an attempt to distract or confuse the user and may also serve as a form of Defense Evasion (TA0005) by creating noise and making it more difficult for security analysts to identify malicious activities.

At 7:58:06 AM UTC, the adversary executed PowerShell again via powershell.exe with an encoded command that downloaded a file from an external IP address (192.168.0.4) and executed it using IEX. This technique is consistent with Execution (TA0002) as it allows for the execution of arbitrary code on the target system. The use of base64 encoding and downloading code from an external source further highlights the adversary's intent to evade detection, which falls under Defense Evasion (TA0005).

At 7:59 AM UTC, the adversary executed m.exe with specific arguments that leveraged sekurlsa::logonpasswords, a common Mimikatz module used for credential dumping and privilege escalation. This technique is consistent with Execution (TA0002) as it allows for the execution of arbitrary code on the target system, but also aligns with Credential Access (TA0006) as it enables adversaries to harvest credentials and move laterally within the network.

At 8:00 AM UTC, the adversary created a Windows Management Instrumentation (WMI) Event Subscription that triggered a Command Line event consumer upon the

UTICA.dmevals.local Summary

creation of a new Win32_LoggedOnUser instance with the user's name in it. This technique is consistent with Persistence (TA0003) as it allows for the execution of arbitrary code when specific conditions are met, ensuring continued access to the target system even after reboots or changes in credentials.

At 8:11 AM UTC, the adversary executed SDelete, a legitimate disk cleaning utility developed by Microsoft's Sysinternals team, likely as a means to cover their tracks and remove any traces of their malicious activities on the target system. This technique is consistent with Defense Evasion (TA0005) as it aims to hinder forensic analysis and make it more difficult for security analysts to identify and attribute malicious actions to the adversary.

On May 1st, at approximately 7:09 AM UTC, an external command and control channel was established by the adversary to transfer tools into the compromised environment. The adversary exploited this channel to execute PowerShell scripts, dump credentials, and establish persistence on the endpoint. This unauthorized access poses a significant risk to data integrity and operations.

On May 2nd, at approximately 8:09 AM UTC, the adversary transferred a tool (mimikatz) into the compromised environment from an external system using command and control. On May 2nd, between 7:58:21 AM and 8:00:07 AM UTC, the adversary executed PowerShell scripts to download additional tools and execute them on the endpoint. The adversary then dumped credentials from the system using mimikatz at 7:59:10 AM and 8:07:56 AM UTC. At 8:00:07 AM, the adversary established persistence by creating a Windows Management Instrumentation Event Subscription to execute PowerShell scripts upon user login. The adversary executed additional mimikatz commands at 8:20:07 AM and 8:21:59 AM UTC.

The adversary's actions may have compromised additional systems or services within the network, requiring further investigation. The root cause of the incident was an external command and control channel established by the adversary to transfer tools into the compromised environment. The adversary exploited this channel to execute PowerShell scripts, dump credentials, and establish persistence on the endpoint.

In summary, an adversary executed a series of techniques aligned with Initial Access (TA0001), Execution (TA0002), Persistence (TA0003), and Defense Evasion (TA0005) tactics on a Windows endpoint associated with the user DMEVALS\dschrute. The adversary's actions included the execution of command-line interfaces, decoding files, compiling and executing code, distracting users, credential dumping, creating WMI Event Subscriptions for persistence, and using disk cleaning utilities to cover their tracks. These techniques suggest a targeted or opportunistic intrusion aimed at maintaining

UTICA.dmevals.local Summary

access and evading detection within the target environment.

On May 2nd, 2020 at approximately 8:17 UTC, another user with administrator privileges executed a PowerShell command on a system with IP address 10.0.1.5. The command established a connection to a remote system with IP address 10.0.1.4 over WinRM and executed multiple commands, suggesting that the user may have been attempting to move laterally across the network or establish remote execution capabilities on the target system.

At 8:09:58 UTC, network connection data shows that net.exe was used to connect to a OneDrive account with the username urukhai2020@outlook.com and password V@m0s0rc0!2020 using TA0010.T1567.002 Exfiltration: Exfiltration Over Web Service and TA0010.T1567 Exfiltration to Cloud Storage, indicating data exfiltration may have occurred. These actions suggest that the system was compromised and used for data collection and potential staging for further malicious activity.

The adversary successfully gained access to the endpoint and extracted sensitive credential information. This unauthorized access poses a significant risk to data integrity and operations. The adversary's actions may have compromised additional systems or services within the network, requiring further investigation.

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

On April 30th at approximately 12:35 AM UTC, an external system with IP address 192.168.0.4 initiated communication with the compromised endpoint and transferred a Windows Portable Executable (PE) file classified as python.exe. This event is consistent with Command and Control activity where tools or other files are copied from an external adversary-controlled system to the victim network through the command and control channel.

On May 2nd at approximately 3:55 AM UTC, a suspicious process was executed on the endpoint. The file, named 'â€®cod.3aka3.scr', is believed to be malware as it was not present in any legitimate software installations or system files. This event triggered an alert for Masquerading and Right-to-Left Override techniques with a high risk rating.

Subsequently, the adversary established persistence on the endpoint by modifying registry keys related to user logon events. The malware was scheduled to execute each time the user logs into the system. This event is consistent with Persistence activity where tools or other files are copied from an external adversary-controlled system to the victim network through the command and control channel.

At approximately 3:04 AM UTC, the adversary executed a PowerShell script that extracted an image file named 'monkey.png' from the malware payload. This event is consistent with Credential Access activity where tools or other files are copied from an external adversary-controlled system to the victim network through the command and control channel.

The root cause of this incident appears to be a successful Command and Control communication between the compromised endpoint and an external adversary-controlled system. The external system transferred a suspicious file classified as python.exe, which was later executed on the endpoint. This activity is indicative of a coordinated attack where tools or other files are copied from an external adversary-controlled system to the victim network through the command and control channel.

The incident has had significant impact on the compromised endpoint, including execution of malware, modification of registry keys related to user logon

SCRANTON.dmevals.local Summary

events, and extraction of image files from the malware payload. The adversary's actions have likely resulted in unauthorized access to sensitive data and system resources. Additionally, the adversary's persistence on the endpoint poses a significant risk for future unauthorized access or data exfiltration. It is recommended that the compromised endpoint be isolated from the network and subjected to a thorough malware analysis and remediation process.

The adversary began their operation by executing malware on a victim endpoint using Right-to-Left Override (RLO) masquerading techniques in order to evade detection. The file name was disguised as 'â€®cod.3aka3.scr' and executed with the command '"C:\ProgramData\victim\â€®cod.3aka3.scr" /S'. This initial execution spawned a PowerShell process which modified the registry to add an autostart entry for persistence, setting up the 'monkey.png' extraction script in the user's startup folder. The adversary then executed additional scripts and tools from the Sysinternals Suite, including sdelete64.exe and PsExec64.exe, to further entrench themselves on the endpoint and evade detection. They also injected code into the lsass.exe process in an attempt to escalate privileges. The adversary's actions indicate a targeted or opportunistic intrusion with the intent of maintaining long-term access for potential follow-on activities.

On May 2nd, 2020 at 03:05:16 UTC, a PowerShell process was executed with the command to extract data from an image file and execute a script. The target image is 'C:\Users\pbeesly\Downloads\monkey.png'. This action resulted in the Open Process event for lsass.exe at 03:05:16 UTC, indicating that credentials may have been accessed through LSASS Memory (TA0006.T1003.001) with a low risk level. The credential dumping technique is used to obtain account login and credential material in the form of hashes or clear text passwords from the operating system and software, which can then be used for lateral movement and access restricted information. This action may indicate privilege escalation (TA0004) as it allows an adversary to gain higher-level permissions on a system or network by taking advantage of system weaknesses, misconfigurations, and vulnerabilities.

On May 2nd, 2020 at approximately 03:08 UTC, a device with IP address 10.0.1.4 began making multiple network connections to various remote systems on ports 80 and 389. The first connection was made to an external system with IP address 192.168.0.5 over port 443, followed by a connection to an internal system with IP address 10.0.0.4 over port 389. Subsequently, the device established connections to another internal system with IP address 10.0.1.6 over port 5985. These actions align with the MITRE technique TA0008.T1021.015 - Lateral Movement: Remote Services, as they involve using remote services to interact with and control remote systems.

SCRANTON.dmevals.local Summary

At approximately 03:09 UTC, a device with IP address 10.0.1.4 made multiple network connections to an internal system with IP address 10.0.1.6 over port 5985. These actions align with the MITRE technique TA0008.T1021.006 - Lateral Movement: Remote Services, Windows Remote Management, as they involve using Windows Remote Management (WinRM) to interact with and control a remote system.

At approximately 03:11 UTC, a device with IP address 10.0.1.4 executed the program PsExec64.exe, passing in parameters that indicate it is being used to execute a command on a remote system with the hostname NASHUA. These actions align with the MITRE technique TA0008.T1072 - Lateral Movement: Software Deployment Tools, as they involve using software deployment tools to execute commands on remote systems.

At approximately 03:20 UTC, a device with IP address 10.0.1.4 made a network connection to an internal system with IP address 172.18.39.2 over port 3389. Subsequently, the device was authenticated by a user named pbeesly. These actions align with the MITRE technique TA0008.T1021.001 - Lateral Movement: Remote Services, Remote Desktop Protocol, as they involve using the Remote Desktop Protocol (RDP) to interact with and control a remote system.

In summary, these timeline entries indicate that an adversary may be moving laterally through the network, using various techniques such as Windows Remote Management and Software Deployment Tools to execute commands on remote systems. The use of RDP for authentication suggests that the adversary may have obtained valid credentials for a user account on the target system. These actions align with the MITRE tactics TA0002 - Execution and TA0008 - Lateral Movement, as they involve executing code on remote systems and moving through the network to expand access and gather information.