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: gemma 2 it 27b Q8 0 32,000 context

The incident appears to have originated from malicious executables delivered through phishing emails or compromised websites. These executables allowed attackers to establish initial access on SCRANTON.dmevals.local by executing PowerShell code disguised as a legitimate file. This established persistence through registry modifications and created a backdoor for remote access using PsExec. The attacker then leveraged this foothold to deploy keystroke logging software and attempted lateral movement to NASHUA.dmevals.local. On UTICA.dmevals.local, the attacker executed PowerShell commands through conhost.exe and certutil.exe, downloaded obfuscated scripts from a remote server (192.168.0.4:443), and used mimikatz to steal credentials. They established persistence by creating a WMI event subscription triggered on user login events. On NASHUA.dmevals.local, the attacker executed python.exe followed by powershell.exe and cmd.exe to run a rar executable which was subsequently deleted using sdelete64.exe after modifying the registry to accept its EULA. The attacker also used sdelete64.exe to delete files from the user's desktop and roaming profile directories.

On May 2nd at 7:59 AM UTC, an adversary used 'm.exe' to dump credentials from LSASS memory on UTICA.dmevals.local. This activity was followed by a PowerShell script execution that invoked 'lsadump::lsa /inject /name:krbtgt' and another PowerShell command executed mimikatz with parameters indicating an attempt to obtain Kerberos tickets for the user 'kmalone' and domain 'dmevals.local'. The adversary also accessed cached domain credentials using wininit.exe and services.exe processes on UTICA.dmevals.local. On SCRANTON.dmevals.local, an attacker used PowerShell to execute a script that extracted data from an image file and decoded it into executable code which then opened the LSASS process for memory analysis. This suggests they were attempting to steal credentials stored in the LSASS process. On NEWYORK.dmevals.local, 'm.exe' targeted the Local Security Authority Subsystem Service (LSASS) and leveraged debugging privileges to interact with it, likely attempting to extract sensitive information like passwords or other authentication material. The attacker used several system libraries related to security and credential management during this interaction. This suggests an attempt to gain elevated access by stealing credentials from the system.

The attacker's initial access on SCRANTON.dmevals.local was as user 'pbeesly', who then used PowerShell to establish connections with other systems on the

Investigation Summary

network, leveraging these connections to initiate new PowerShell processes remotely via RDP on ports 80 and 39. They then utilized PsExec to connect to NASHUA.dmevals.local using the account 'dmevals\pbeesly' with password 'Fl0nk3rt0n!T0by', indicating lateral movement using both built-in tools and third-party software. The attacker continued to use PsExec to connect to NASHUA.dmevals.local multiple times, suggesting persistence or network exploration. On NASHUA.dmevals.local, user 'pbeesly' accessed a network share on multiple occasions and used it to execute python scripts via PSEXESVC.exe, potentially leveraging software deployment tools like SCCM for lateral movement within the DMEVALS.LOCAL domain. This repeated access to network shares followed by script execution suggests remote code execution and further lateral movement. The user 'pbeesly' repeatedly logged into different machines from IP address 10.0.1.4, suggesting its use as a staging point.

The attacker leveraged PowerShell to download and execute code from 192.168.0.4 on UTICA.dmevals.local at 7:55 AM UTC, followed by connections to the same IP address for potential persistence or communication with their infrastructure. This was followed by multiple PowerShell commands using WMI to connect to port 5985, commonly used by WinRM, indicating lateral movement attempts. At 8:02 AM UTC, more code was downloaded from 192.168.0.4 and connected to port 5985 on another machine, continuing the pattern of lateral movement using WinRM. A remote desktop connection was made from 'dschrute' to IP address 172.18.39.2 at 8:17 AM UTC.

On May 1st, an adversary established command and control with UTICA.dmevals.local by transferring a malicious executable file named mimikatz. The next day, they used certutil to decode another file from a hidden location on the same system. Data was then exfiltrated using net.exe to a cloud storage service associated with an Outlook email address. On SCRANTON.dmevals.local, an executable file was downloaded from an external IP address and saved on the endpoint, suggesting a potential attempt to establish communication for further malicious activity. On NASHUA.dmevals.local, an adversary used a utility to compress files on a user's desktop into a zip archive named "working.zip" before exfiltrating them. This indicates data collection and potential exfiltration attempts are underway across multiple endpoints.

The attacker utilized process injection into lsass on SCRANTON.dmevals.local, obfuscated code within images, and employed PowerShell for malicious actions while leveraging legitimate system utilities like sdelete and conhost to blend in with normal activity. They also used 'certutil.exe' with a base64 encoded payload and attempted to use 'net.exe' to connect to a remote server. The attacker's use of obfuscation techniques on both SCRANTON.dmevals.local and UTICA.dmevals.local, along with the deletion of files using sdelete64.exe on NASHUA.dmevals.local suggests an attempt to evade detection and maintain

Investigation Summary

long-term presence within the network. The attacker's actions indicate a high risk of data exfiltration, as evidenced by attempts to compress and remove sensitive files from the network.

The use of 'lsadump' indicates a targeted effort to extract specific credentials, potentially those belonging to the krbtgt account which is a highly privileged account used for Kerberos authentication. The attacker demonstrated a preference for PowerShell scripting for both command execution and data exfiltration, suggesting familiarity with this toolset. This incident highlights vulnerabilities in our security posture, particularly regarding endpoint protection and user education on phishing threats.

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:
A timeline of events indicates a potential data exfiltration incident involving the user account "pbeesly" on the endpoint "NASHUA.dmevals.local". The activity began with suspicious network connections to IP address 10.0.0.4, followed by the creation and execution of Python scripts and PowerShell commands for file manipulation and data collection.

The attacker established a connection to a remote system (10.0.0.4) using SMB protocol on port 445. This was followed by the creation of "python.exe" and "PSEXESVC.exe" files, suggesting potential malware deployment or remote access tools. The user account then accessed shared folders and executed scripts to enumerate and compress sensitive files from various directories, including those containing keywords like "psw", "pass", and "admin". These files were archived into a zip file named "working.zip" in the AppData directory.

The attacker used PowerShell to gather data from user profiles, specifically targeting files with extensions commonly associated with credentials or sensitive information (doc, xls, ppt, pdf, rar, etc.). The compressed archive was then created using Rar.exe and stored in the AppData directory before being deleted along with other tools like "sdelete64.exe".

The attacker's actions indicate a targeted approach focused on data exfiltration, potentially aiming to steal sensitive information from the user's profile. The use of PowerShell for file enumeration and compression suggests an attempt to evade detection while gathering specific types of files. The deletion of these tools after execution further points towards malicious intent.

Root Cause Analysis:
The incident likely stemmed from a compromised account or weak credentials allowing unauthorized access to "pbeesly". This could be due to phishing, malware infection, or exploitation of vulnerabilities in the system. The attacker leveraged legitimate tools like PowerShell and Rar.exe for data exfiltration, highlighting the need for robust endpoint security measures and user awareness training.

Impact Assessment:

NASHUA.dmevals.local Summary

The incident poses a significant risk to data confidentiality as sensitive information may have been compromised. The attacker's access to user profiles and potential exfiltration of files containing passwords or login credentials could lead to further breaches or unauthorized access to other systems. Immediate action is required to secure the affected system, investigate the extent of data loss, and implement stronger security controls to prevent future incidents.

Further investigation is needed to determine the scope of the breach and identify any compromised data. This includes analyzing logs from 10.0.0.4 for additional activity and reviewing user "pbeesly" for suspicious behavior.

Analysis:
A user account belonging to 'DMEVALS\pbeesly' was used to execute python.exe followed by powershell.exe and then cmd.exe. The adversary leveraged these tools to run a rar executable, which was subsequently deleted using sdelete64.exe. The adversary also modified the registry to accept the EULA for sdelete64.exe. This activity suggests an attempt to execute malicious code on the system. The use of multiple scripting languages and the deletion of files after execution could indicate an effort to obfuscate their presence on the system, potentially as part of a larger attack. The adversary then used sdelete64.exe to delete additional files from the user's desktop and roaming profile directories. This suggests they may be trying to remove evidence of their activity or prepare for further actions. The repeated use of sdelete64.exe against different file paths indicates a possible attempt to clean up traces of malicious code or data exfiltration.

The adversary utilized 'pbeesly's access to network shares on multiple occasions, executing python scripts via PSEXESVC.exe. This suggests they are leveraging legitimate tools for lateral movement within the DMEVALS.LOCAL domain, potentially using software deployment systems like SCCM or similar systems to move between machines. The repeated access to network shares followed by execution of python scripts indicates a pattern of activity consistent with remote code execution and potential lateral movement across the network. The adversary used a utility to compress files on the user's desktop into a zip archive before exfiltrating them. The compressed file was created in the user's temporary directory and named "working.zip". This, combined with the repeated access to network shares followed by execution of Python scripts indicates a possible attempt to spread malicious code or commands across the network, potentially using 'pbeesly's credentials to gain access and execute code on other machines. The use of PSEXESVC.exe further suggests they are leveraging existing administrative tools for this purpose.

NASHUA.dmevals.local Summary

The attacker's actions suggest a targeted approach focused on data exfiltration. They leveraged legitimate tools like PowerShell and Rar.exe, indicating an attempt to evade detection while gathering specific types of files. The deletion of these tools after execution points towards malicious intent and a desire to obfuscate their presence. The repeated use of sdelete64.exe against different file paths indicates a possible attempt to clean up traces of malicious code or data exfiltration. This, combined with the access to network shares and execution of Python scripts via PSEXESVC.exe, suggests they may be using 'pbeesly's credentials for lateral movement within the DMEVALS.LOCAL domain, potentially leveraging software deployment tools like SCCM or similar systems to move between machines.

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:

At 08:02:44 UTC, the process wsmprovhost.exe was executed by user mscott. Shortly after, a connection was made from the endpoint to IP address 10.0.0.4 on port 5985. User dschrute logged onto the system at 08:03:20 UTC, followed by the creation of a file named m.exe in the System32 directory at 08:03:47 UTC. This file was then executed with elevated privileges at 08:04:25 UTC and loaded several libraries including cryptdll.dll, samlib.dll, hid.dll, and WinSCard.dll before opening lsass.exe. The process then exited. A Kerberos authentication ticket was requested at 08:16:32 UTC followed by additional service tickets being requested at 08:16:32 and 08:18:06. User kmalone logged onto the system at 08:22:24 UTC.

This activity suggests an adversary used the process 'm.exe' to target the Local Security Authority Subsystem Service (LSASS). LSASS is known to store credentials in memory and was accessed by 'm.exe'. The adversary leveraged debugging privileges to interact with LSASS, likely attempting to extract sensitive information like passwords or other authentication material. This suggests an attempt to gain elevated access by stealing credentials from the system. The use of libraries such as cryptdll.dll, samlib.dll, hid.dll, and WinSCard.dll during this interaction further supports this assessment, as these are often associated with accessing and manipulating user accounts and cryptographic keys. The adversary's actions indicate a targeted effort to extract specific credentials, potentially those belonging to the krbtgt account which is a highly privileged account used for Kerberos authentication. The subsequent Kerberos ticket requests at 08:16:32 and 08:18:06 suggest a potential Golden Ticket attack, where stolen credentials are used to forge authentication tickets for lateral movement within the network.

This incident indicates a compromise of the endpoint and potentially the network due to credential theft. Stolen credentials could be used to access sensitive data or escalate privileges on other systems. The attacker may have gained persistent access through the Golden Ticket technique, allowing them to move laterally and maintain presence on the network.

UTICA.dmevals.local Summary

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

Summary of Findings:

A malicious executable was downloaded from an external system on May 1st at 07:09 UTC. This executable was then used to execute PowerShell commands that retrieved additional code from a remote server and dumped credentials from memory. The attacker established persistence through WMI event subscriptions, allowing for continued execution even after the initial session ended.

Root Cause Analysis:
The incident originated with the download of a malicious executable. This suggests a lack of adequate endpoint protection or user awareness training as the primary cause.

Impact Assessment:
The attacker gained access to sensitive credentials including domain administrator credentials and potentially compromised the Kerberos ticket granting service (TGS) for further lateral movement within the network. The attacker also established persistence, indicating an intent to maintain long-term presence on the system.

Tradecraft Summary:
On May 1st at 07:09 UTC, a malicious executable was downloaded from an external system and executed. This initiated activity by leveraging conhost.exe and certutil.exe to download and execute obfuscated scripts from a remote server (192.168.0.4:443) which contained malicious code. The attacker used PowerShell to download additional tools like 'm.exe' and attempted to steal credentials with mimikatz, indicating their intent was likely data exfiltration or lateral movement within the network. They established persistence by creating a WMI event subscription that triggers execution of malicious code upon user login events. This suggests they are aiming for long-term access to the compromised system. The attacker also used obfuscation techniques and attempted to hide their activity through various PowerShell commands, demonstrating an attempt to evade detection.

The attacker's use of 'certutil.exe' with a base64 encoded payload is a common tactic to bypass security solutions that rely on signature-based detection. This combined with the download of mimikatz suggests they are looking for

UTICA.dmevals.local Summary

credentials and potentially aiming to escalate privileges or move laterally within the network. The attacker also attempted to use 'net.exe' to connect to a remote server, possibly exfiltrating data.

The following day at 7:55 AM UTC, the adversary used PowerShell to download and execute code from the same IP address (192.168.0.4). This was followed by additional network connections to the same IP address, suggesting an attempt to establish persistence or further communication with the attacker's infrastructure. Shortly after, there were multiple instances of PowerShell commands using WMI for potential credential dumping and establishing connections to port 5985, which is commonly used by WinRM. This indicates a possible attempt to move laterally within the network.

At 7:59 AM UTC, 'm.exe' was used to dump credentials from LSASS memory. This activity was followed by a PowerShell script execution that invoked 'lsadump::lsa /inject /name:krbtgt'. Later, another PowerShell command executed mimikatz with parameters indicating an attempt to obtain Kerberos tickets for the user 'kmalone' and domain 'dmevals.local'. The adversary also accessed cached domain credentials using wininit.exe and services.exe processes. These actions suggest a pattern of credential theft and potential privilege escalation attempts, possibly aiming to gain higher-level access within the network by acquiring sensitive information like passwords and Kerberos tickets for lateral movement or further exploitation.

The use of 'm.exe' with 'sekurlsa::logonpasswords' indicates an attempt to extract credentials from LSASS memory, while the PowerShell commands suggest a more targeted approach using mimikatz to obtain specific user credentials and potentially elevate privileges through Kerberos ticket manipulation. The adversary's focus on obtaining both clear text passwords and Kerberos tickets implies a desire for persistent access and lateral movement within the network.

Later, at 8:02 AM, there were more PowerShell commands downloading code from the same IP address (192.168.0.4) and connecting to port 5985 on another machine, suggesting continued lateral movement using WinRM. This pattern of establishing connections to port 5985 continued throughout the morning. Finally, at 8:17 AM, there was a successful remote desktop connection from 'dschrute' to a different IP address (172.18.39.2), suggesting further movement across the network using RDP. This activity is consistent with an attacker gaining access and moving laterally through the network, potentially seeking additional targets or sensitive information.

The attacker also used 'net.exe' to exfiltrate data to a cloud storage service associated with an Outlook email address. This suggests that the adversary is

UTICA.dmevals.local Summary

likely collecting sensitive information and sending it to a remote server for further use or analysis. The use of a legitimate web service like OneDrive for exfiltration indicates an attempt to blend in with normal network traffic and avoid detection.

The attacker's actions indicate a targeted intrusion due to their persistence mechanisms and attempts at credential theft. They are actively trying to maintain access and potentially expand their foothold within the network.

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

Executive Summary:

Summary of Findings:

A malicious executable file was downloaded from an external system on April 30th at 00:35 UTC. This file, identified as python.exe, was likely used to establish initial access and deliver a payload. On May 2nd, the payload executed under the user account DMEVALS\pbeesly, masquerading as a legitimate program. The malware then created a shortcut in the Startup folder to ensure persistence on subsequent system boots. The attacker used PowerShell to extract and execute another file named monkey.png which contained malicious code. This code was further used to dump credentials from LSASS memory and inject code into the lsass process, indicating an attempt to elevate privileges and maintain persistent access.

Root Cause Analysis:

The initial compromise likely stemmed from a successful download of a malicious executable. The attacker leveraged PowerShell for various tasks including persistence and credential dumping, suggesting familiarity with common Windows tools and techniques.

Impact Assessment:

The incident resulted in the potential compromise of user credentials and possible elevation of privileges within the system. This could lead to unauthorized access to sensitive data or further lateral movement within the network.

The attack likely began with a phishing email containing a malicious attachment disguised as a legitimate file using a right-to-left override technique to hide its true extension. This led to the execution of PowerShell code which established persistence through registry modifications and created a backdoor for remote access via PsExec, allowing the attacker to maintain control even after system restarts. The attacker then deployed additional tools like keystroke logging software and attempted lateral movement by targeting another

SCRANTON.dmevals.local Summary

machine named NASHUA. Throughout the attack, they leveraged legitimate system utilities like sdelete and conhost to blend in with normal activity while employing PowerShell for further malicious actions. This suggests a targeted approach due to the use of specific usernames and passwords, indicating prior reconnaissance and knowledge of the target environment. The attacker's focus on persistence through multiple methods points towards a desire for long-term access rather than simply stealing data.

The attacker demonstrates an understanding of security tools by utilizing techniques like process injection into lsass and obfuscating their code within images to evade detection, highlighting a sophisticated level of skill. Their actions suggest a goal beyond simple data theft, potentially aiming for deeper network penetration or long-term control over the compromised system. An attacker used PowerShell to execute a script on the endpoint belonging to user 'pbeesly'. The script was designed to extract data from an image file and decode it into executable code which then opened the LSASS process for memory analysis. This suggests the attacker is attempting to steal credentials stored in the LSASS process, likely aiming to gain elevated privileges by obtaining plaintext passwords or hashes.

The attacker's goal appears to be gaining higher-level access on the system. They are using a technique that targets the LSASS process which stores sensitive credential information like user login details and passwords after a user authenticates. This could allow them to move laterally within the network, impersonate users, or gain control of other systems.

An attacker initially gained access to a system as user 'pbeesly' and used PowerShell to establish connections with other systems on the network. The attacker then leveraged these connections to initiate new PowerShell processes on remote systems using the Remote Desktop Protocol, connecting to ports 80 and 389. Following this, they utilized PsExec to connect to another system named NASHUA, utilizing a user account 'dmevals\pbeesly' with password 'Fl0nk3rt0n!T0by'. This suggests an attempt to move laterally through the network using both built-in tools and third-party software. The attacker continued to use PsExec to connect to the same system multiple times, indicating a possible attempt to establish persistence or further explore the network. Finally, they used Remote Desktop Protocol to connect to a remote system from '172.18.39.2'.

The attacker's actions demonstrate a clear pattern of lateral movement across the network, utilizing various techniques to gain access to different systems and potentially escalate privileges. The use of PsExec suggests an attempt to maintain persistence on the network by leveraging existing tools for remote execution. An executable file was downloaded from an external IP address and

SCRANTON.dmevals.local Summary

saved on the endpoint. This suggests a potential adversary is establishing communication with the compromised system for further actions. The file type indicates it could be a tool used for additional malicious activity, possibly data collection or exfiltration.