Demo Investigation

Endpoints

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

Investigation Summary

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

Generated with: Mistral Large Instruct 2407 IQ 2M 17,000 context

Executive Summary:

The incident response timeline investigation was conducted to analyze suspicious activities across multiple endpoints within our network. The scope of this investigation included identifying potential command and control (C2) communications, lateral movement, credential dumping, and persistence mechanisms. This incident is significant due to its potential impact on the organization's security posture, data integrity, and operational continuity.

Summary of Findings:

Significant events observed in the timeline include the transfer of Windows PE files into the environment, execution of suspicious processes with masquerading techniques, and multiple instances of PowerShell script blocks being executed for persistence and credential dumping. These activities were detected across several endpoints, including SCRANTON, UTICA, NASHUA, and NEWYORK. The use of tools like 'PSEXESVC.exe' and 'python.exe', along with the creation of files in temporary directories, suggests a coordinated effort to move laterally within the network and deploy malicious software.

Root Cause Analysis:

The root cause of the incident appears to be the initial transfer of Windows PE files into the environment, likely through command and control (C2) channels. Vulnerabilities in endpoint security measures allowed for the execution of suspicious processes and scripts, which facilitated credential dumping and persistence mechanisms. Misconfigurations or weaknesses in network security protocols may have contributed to the success of lateral movement and unauthorized access attempts.

Impact Assessment:

The incident has had a significant impact on operations, data integrity, and overall security. The compromise of multiple user accounts, including 'pbeesly', 'dschrute', and 'kmalone', indicates potential unauthorized access to sensitive information. The establishment of persistence mechanisms and the use of credential dumping techniques pose a risk to ongoing operations and the

Investigation Summary

security of other systems within the network. Immediate remediation efforts are necessary to contain the incident and prevent further compromise.

Incident Narrative:

The adversary initiated their attack on SCRANTON.dmevals.local by executing malware disguised as a screensaver file named 'cod.3aka3.scr' at 02:55 UTC, using Right-to-Left Override (RTLO) to evade detection and trick the user into execution. Shortly after, at 02:57 UTC, a PowerShell process was executed to establish persistence by modifying the registry to include a hidden PowerShell command that would run at startup. At 03:04 UTC, another persistence mechanism was set up by creating a shortcut named 'hostui.lnk' in the Startup folder. To evade detection and analysis, at 03:05 UTC, the adversary employed process injection techniques targeting 'lsass.exe', a critical Windows process.

On UTICA.dmevals.local, the adversary began by using certutil.exe to decode a file named 'kxwn.lock' located in the user directory of 'dschrute' for defense evasion. Following this, PowerShell was used to execute a script that fetched and executed content from a local HTML file, indicating potential execution of malicious code. The adversary continued their efforts by again using certutil.exe to decode the same 'kxwn.lock' file, reinforcing their defense evasion tactics. To maintain persistence, the attacker created a Windows Management Instrumentation (WMI) event subscription named 'WindowsParentalControlMigration', designed to trigger PowerShell execution whenever the user 'dschrute' logged on. The PowerShell command executed upon this event included downloading and running a script from an external source. The attacker continued to execute PowerShell scripts, likely for various purposes such as reconnaissance or further exploitation. Additionally, they used rundll32.exe to load a DLL file named 'kxwn.lock', which was previously decoded using certutil.exe, indicating an attempt to execute code from the decoded file.

On NASHUA.dmevals.local, the timeline begins with the execution of Python scripts by a user named 'pbeesly' on May 2nd, 2020, at 3:15 AM UTC, suggesting that the adversary might be attempting to gain initial access or execute malicious code. The Python script then spawns a PowerShell process, indicating further execution of commands and scripts, potentially aimed at exploring the network or stealing data. Shortly after, at 3:16 AM UTC, a RAR archive is created on the desktop, which could be part of an exfiltration attempt or preparation for further malicious activities. The PowerShell process initiates this action, suggesting that the adversary is using multiple scripting languages to evade detection. At 3:16 AM UTC, a command prompt (cmd.exe) is executed, followed by the use of SDelete, a software deployment tool, to delete files from the system, indicating defense evasion tactics. The registry

Investigation Summary

modifications associated with SDelete further support this intent, as they accept the End User License Agreement (EULA) for the tool, allowing it to run without user intervention. The timeline shows repeated use of SDelete to delete specific files, including the RAR archive created earlier and another file in the user's AppData directory, reinforcing the defense evasion tactics.

On May 2nd, 2020, multiple endpoints within the dmevals domain experienced activities indicative of privilege escalation and credential access attempts by an adversary. The earliest observed activity occurred at 02:58 UTC on SCRANTON.dmevals.local, where user 'DMEVALS\pbeesly' executed a PowerShell script to manipulate a bitmap image, likely to evade detection mechanisms. At 03:05 UTC, the same endpoint saw attempts to open and dump credentials from the LSASS memory, suggesting an effort to harvest sensitive information for privilege escalation or lateral movement.

At 07:59 UTC, UTICA.dmevals.local experienced a similar credential dumping attempt when user 'DMEVALS\dschrute' executed the process 'm.exe', targeting LSASS memory. This was followed by multiple process executions at 08:12 UTC involving 'wininit.exe' and 'services.exe' under the 'NT AUTHORITY\SYSTEM' account, interacting with LSASS and creating a file in the System32 directory, indicating potential system tampering for persistence. PowerShell script blocks executed at 08:07 UTC and 08:21 UTC invoked Mimikatz commands, suggesting attempts to create or use golden tickets for unauthorized access.

Concurrently, at 08:04 UTC on NEWYORK.dmevals.local, user 'DMEVALS\mscott' executed the process 'm.exe', attempting to dump credentials from LSASS memory using commands associated with handling cryptographic operations and security account management. The loading of libraries such as 'cryptdll.dll' and 'samlib.dll' further supports this credential access attempt.

The timeline analysis reveals a coordinated effort by an adversary to execute remote commands and move laterally within the network across multiple endpoints: SCRANTON, UTICA, and NASHUA. The activities align with MITRE Tactics Remote Execution (TA0002) and Lateral Movement (TA0008).

On May 2, 2020, at 7:55 AM UTC, the adversary initiated their attack on UTICA by executing PowerShell commands to download and run scripts from a remote server. This activity continued with another PowerShell command at 7:59 AM UTC, which downloaded an executable file ('m.exe') for credential extraction. Between 7:58 AM and 8:04 AM UTC, multiple network connections were established to another internal IP address using WinRM (port 5985), indicating lateral movement. At 8:17 AM UTC, the adversary logged into UTICA via RDP from an external IP address, suggesting further lateral movement and potential control over the system.

Investigation Summary

On SCRANTON, a PowerShell script executed by user 'DMEVALS\pbeesly' decoded and ran hidden code from an image file in the Downloads folder, followed by network connections to remote IP addresses over port 443 for possible command-and-control communication or data exfiltration. Another PowerShell script was executed, followed by network connections to various services on different ports, including HTTP (port 80), LDAP (port 389), and WinRM (port 5985). Multiple instances of PsExec64.exe were then executed, targeting a remote system ('NASHUA') using valid domain credentials, indicating attempts at lateral movement and remote code execution.

On NASHUA, the timeline begins with medium-risk lateral movement involving access to a network share object named *\ADMIN$ and attempting access to 'Temp\python.exe'. This was followed by multiple instances of low-risk lateral movement, involving the execution of PSEXESVC.exe and python.exe processes under different user contexts, including 'NT AUTHORITY\SYSTEM' and 'DMEVALS\pbeesly'. The use of these tools suggests attempts to spread malicious code across multiple systems or accounts methodically.

The coordinated execution of PowerShell scripts, PsExec64.exe, python.exe, and the establishment of network connections using WinRM and RDP across SCRANTON, UTICA, and NASHUA demonstrate a systematic approach by the adversary to move laterally within the network, execute commands remotely, and potentially exfiltrate data or maintain control over compromised systems.

On April 30th, 2020, at 00:35:26 UTC, adversaries initiated command and control communication by transferring a tool identified as 'python.exe' into the compromised environment on endpoint SCRANTON.dmevals.local from an external system with IP address 192.168.0.4. This action suggests preparation for further commands or tools execution, potentially leading to data collection and exfiltration activities.

On May 1st, 2020, at 7:09 AM UTC, adversaries transferred a Windows executable file identified as 'mimikatz' from an external IP address (192.168.0.4) to endpoint UTICA.dmevals.local. This tool is commonly used for credential theft and could be part of the adversaries' collection efforts to gather sensitive information.

On May 2nd, 2020, at 3:16 AM UTC, a process executed on endpoint NASHUA.dmevals.local involving 'Rar.exe', creating an archive file named 'working.zip' in the user's Desktop directory from files within the AppData\Roaming folder. This activity aligns with MITRE ATT&CK technique TA0009.T1560.001, indicating a potential staging phase for data exfiltration.

Investigation Summary

Later that day, at 7:55 AM UTC on endpoint UTICA.dmevals.local, adversaries used 'certutil.exe' to decode a file named 'kxwn.lock', created in the user directory of 'dschrute'. This action suggests data staging for exfiltration.

At 8:09 AM UTC on endpoint UTICA.dmevals.local, adversaries executed a command using 'net.exe' to map a network drive to a cloud storage service (Microsoft OneDrive) using credentials provided in the command. This action was followed by an outbound network connection to an IP address associated with Microsoft’s live services, indicating that data exfiltration was likely underway.

These activities collectively show a pattern of tool transfer for command and control, credential theft for collection, data staging for exfiltration, and the use of legitimate web services for data exfiltration. The adversaries' actions indicate a focus on stealing sensitive information from compromised systems while minimizing detection.

NASHUA.dmevals.local Summary

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

Summary of Findings

The timeline data reveals multiple instances of lateral movement within the network using software deployment tools. The initial event involved an attempt to access a network share object, specifically targeting 'Temp\python.exe' on the ADMIN$ share. Subsequently, several processes were executed under different user accounts, including 'NT AUTHORITY\SYSTEM' and 'DMEVALS\pbeesly'. The execution of 'PSEXESVC.exe', a tool commonly used for remote administration, was observed multiple times, followed by the repeated execution of 'python.exe' from the Temp directory. This pattern suggests a coordinated effort to move laterally within the network and potentially execute malicious scripts or commands.

Root Cause Analysis

The root cause of this incident appears to be the exploitation of software deployment tools for lateral movement. The adversary likely gained access to these tools, which are typically used for legitimate administrative purposes, and leveraged them to spread across the network. The repeated execution of 'PSEXESVC.exe' and 'python.exe' under different user accounts indicates that the attacker was able to gain elevated privileges and execute commands remotely. This could be due to vulnerabilities or misconfigurations in the software deployment tools, allowing unauthorized access and control.

Impact Assessment

The incident has significant implications for network security and data integrity. The use of software deployment tools for lateral movement suggests that multiple systems within the network may have been compromised. This could lead to further exploitation, data exfiltration, or disruption of operations. The execution of 'python.exe' from the Temp directory raises concerns about potential malicious scripts being run on affected systems, which could result in data corruption or loss. Additionally, the involvement of administrative accounts like 'NT AUTHORITY\SYSTEM' indicates that the attacker may have gained high-level access to critical systems, posing a severe risk to overall network security and operations.

Narrative Summary

The timeline begins with the execution of Python scripts by a user named 'pbeesly' on May 2nd, 2020, at 3:15 AM UTC. This activity suggests that the

NASHUA.dmevals.local Summary

adversary might be attempting to gain initial access (TA0001) or execute malicious code (TA0002). The Python script then spawns a PowerShell process, indicating further execution of commands and scripts (TA0002), potentially aimed at exploring the network or stealing data.

Shortly after, at 3:16 AM UTC, a RAR archive is created on the desktop, which could be part of an exfiltration attempt or preparation for further malicious activities. The PowerShell process initiates this action, suggesting that the adversary is using multiple scripting languages to evade detection (TA0005).

At 3:16 AM UTC, a command prompt (cmd.exe) is executed, followed by the use of SDelete, a software deployment tool (TA0002), to delete files from the system. This sequence indicates that the adversary is attempting to clean up traces of their activities, which aligns with defense evasion tactics (TA0005). The registry modifications associated with SDelete further support this intent, as they accept the End User License Agreement (EULA) for the tool, allowing it to run without user intervention.

The timeline shows repeated use of SDelete to delete specific files, including the RAR archive created earlier and another file in the user's AppData directory. This systematic cleanup suggests a methodical approach by the adversary to remove evidence of their presence on the system, reinforcing the defense evasion tactics (TA0005).

The timeline also reveals medium-risk events involving lateral movement through software deployment tools, specifically targeting a network share object named *\ADMIN$ and attempting access to 'Temp\python.exe'. This initial action suggests an adversary might be probing for potential entry points or testing access permissions within the network.

Multiple instances of low-risk lateral movement are detected, involving the execution of PSEXESVC.exe and python.exe processes. These executions occur under different user contexts, including 'NT AUTHORITY\SYSTEM' and 'DMEVALS\pbeesly', indicating potential attempts to spread malicious code across multiple systems or accounts. The repeated execution of these processes suggests a systematic approach to infiltrate and control various endpoints within the network.

The use of PSEXESVC.exe, a tool often associated with remote administration, coupled with python.exe executions, implies that the adversary is leveraging legitimate tools for lateral movement and potential execution of malicious scripts or commands. The conhost.exe process, which typically handles console windows, also appears in conjunction with these activities, suggesting attempts to manage command-line interfaces remotely.

NASHUA.dmevals.local Summary

The pattern of executing PSEXESVC.exe followed by python.exe and conhost.exe across different timestamps indicates a methodical approach to spread control throughout the network. This behavior is consistent with an adversary trying to establish a foothold and expand their influence within the compromised environment, potentially aiming for further exploitation or data exfiltration.

On May 2nd, 2020, at 3:16 AM UTC, a process executed on the endpoint involving 'Rar.exe', a utility commonly used for compressing and archiving data. The command issued was designed to create an archive file named 'working.zip' in the user's Desktop directory, incorporating files from another location within the user's AppData\Roaming folder. This activity aligns with the MITRE ATT&CK technique TA0009.T1560.001, where adversaries archive collected data prior to exfiltration, likely aiming to obfuscate and minimize the amount of data sent over the network. The user associated with this activity was 'DMEVALS\pbeesly', suggesting that either this user's account has been compromised or they are involved in the suspicious activity. This event indicates a potential staging phase for data exfiltration, where sensitive information might be prepared for extraction from the network.

Overall, the timeline reveals a series of coordinated actions aimed at lateral movement and potential remote execution, utilizing software deployment tools and legitimate system processes to achieve broader control over the network. The use of Python, PowerShell, and command prompt, along with tools like SDelete, demonstrates a sophisticated approach to evade defenses and maintain persistence (TA0003) on the compromised system.

NEWYORK.dmevals.local Summary

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

Summary of Findings
The timeline reveals a sequence of events indicating credential access attempts on an endpoint within the DMEVALS domain. The initial activity involved the execution of 'wsmprovhost.exe' by user 'DMEVALS\mscott', followed by a network connection to another machine in the same subnet. Shortly after, there was a Windows logon event for user 'dschrute'. A suspicious file named 'm.exe' was created and subsequently executed with commands suggesting OS credential dumping targeting LSASS memory. The process involved loading several system libraries and opening the Local Security Authority Subsystem Service (LSASS) process, which is a common technique for extracting credentials from memory. Multiple Kerberos authentication ticket requests were observed, including a request for a Golden Ticket, indicating potential lateral movement within the network.

Root Cause Analysis
The root cause of this incident appears to be the execution of 'm.exe', likely a malicious tool designed for credential dumping. The creation and execution of this file by user 'DMEVALS\mscott' suggest that this account may have been compromised or is being used by an insider threat. The network connection established before these activities could indicate command and control communication or initial reconnaissance. The vulnerability lies in the ability to execute such tools on the endpoint, possibly due to insufficient access controls or lack of proper monitoring and detection mechanisms.

Impact Assessment
The incident poses significant risks to data integrity and operational security. Successful credential dumping can lead to unauthorized access to sensitive information and further lateral movement within the network. The request for a Golden Ticket suggests that the adversary may have gained domain-level access, which could compromise the entire domain's security. This incident underscores the need for robust endpoint protection, access control measures, and continuous monitoring to detect and mitigate such threats promptly.

Detailed Narrative
At 08:04 UTC on May 2nd, 2020, a process named 'm.exe' was executed by user 'DMEVALS\mscott'. This process attempted to dump credentials from the Local

NEWYORK.dmevals.local Summary

Security Authority Subsystem Service (LSASS) memory using the command '"C:\Windows\System32\m.exe" privilege::debug "lsadump::lsa /inject /name:krbtgt" exit'. The execution of 'm.exe' was followed by the loading of several libraries, including 'cryptdll.dll', 'samlib.dll', 'hid.dll', and 'WinSCard.dll', which are typically associated with handling cryptographic operations, security account management, human interface devices, and smart card functions respectively. The process also opened the LSASS executable, indicating an attempt to access or manipulate its memory space. This sequence of events suggests a potential credential dumping operation aimed at extracting sensitive information from the system's memory, which could be used for lateral movement within the network or further privilege escalation. The process exited shortly after these activities, possibly indicating the completion of the intended task or an attempt to evade detection.

The timeline reveals a sequence of events indicating credential access attempts on an endpoint within the DMEVALS domain. The initial activity involved the execution of 'wsmprovhost.exe' by user 'DMEVALS\mscott', followed by a network connection to another machine in the same subnet. Shortly after, there was a Windows logon event for user 'dschrute'. A suspicious file named 'm.exe' was created and subsequently executed with commands suggesting OS credential dumping targeting LSASS memory. The process involved loading several system libraries and opening the Local Security Authority Subsystem Service (LSASS) process, which is a common technique for extracting credentials from memory. Multiple Kerberos authentication ticket requests were observed, including a request for a Golden Ticket, indicating potential lateral movement within the network.

The root cause of this incident appears to be the execution of 'm.exe', likely a malicious tool designed for credential dumping. The creation and execution of this file by user 'DMEVALS\mscott' suggest that this account may have been compromised or is being used by an insider threat. The network connection established before these activities could indicate command and control communication or initial reconnaissance. The vulnerability lies in the ability to execute such tools on the endpoint, possibly due to insufficient access controls or lack of proper monitoring and detection mechanisms.

The incident poses significant risks to data integrity and operational security. Successful credential dumping can lead to unauthorized access to sensitive information and further lateral movement within the network. The request for a Golden Ticket suggests that the adversary may have gained domain-level access, which could compromise the entire domain's security. This incident underscores the need for robust endpoint protection, access control measures, and continuous monitoring to detect and mitigate such threats promptly.

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 08:40:00
Observed IP Addresses: 10.0.1.5, 10.0.0.4, 10.0.1.4, 172.18.39.2, 192.168.0.4
Observed Users: DMEVALS\mscott, DMEVALS\dschrute, dschrute

Summary of Findings:
The timeline reveals a series of coordinated activities indicating an advanced persistent threat (APT) targeting the victim network. On May 1st, 2020, at 7:09 AM UTC, there was evidence of command and control activity with the retrieval of Mimikatz from an external IP address (192.168.0.4). This tool is commonly used for credential dumping. Subsequent events on May 2nd involved multiple instances of PowerShell script execution, including attempts to bypass security measures and execute commands that could facilitate further exploitation.

Notably, at 7:59 AM UTC, there was an attempt to dump OS credentials using Mimikatz, targeting the LSASS memory. This activity suggests a focused effort to gain unauthorized access to sensitive information. Additionally, Windows Management Instrumentation (WMI) event subscriptions were created and executed, indicating persistence mechanisms being established within the network.

Root Cause Analysis:
The root cause of this incident appears to be an initial compromise that allowed the adversary to establish command and control over the victim system. The retrieval of Mimikatz from an external source suggests a phishing attack or another form of social engineering that led to the execution of malicious code on the endpoint. Vulnerabilities in the network's defenses, such as weak access controls or lack of proper monitoring, likely contributed to the adversary's ability to execute these actions undetected.

Impact Assessment:
The incident has significant implications for data integrity and operational security. The use of Mimikatz for credential dumping poses a severe risk as it can expose sensitive credentials, potentially leading to further unauthorized access across the network. The establishment of WMI event subscriptions indicates that the adversary may have set up persistent mechanisms to maintain control over compromised systems, which could lead to ongoing data exfiltration or additional malicious activities.

The execution of PowerShell scripts and the creation of suspicious files suggest that the adversary has gained a foothold within the network, potentially compromising multiple systems and user accounts. This incident underscores the need for robust security measures, including regular

UTICA.dmevals.local Summary

monitoring, access controls, and incident response protocols to mitigate future threats effectively.

Tradecraft Summary:
The adversary initiated their attack by leveraging obfuscated files or information for defense evasion, using certutil.exe to decode a file named 'kxwn.lock' located in the user directory of 'dschrute'. This action suggests an attempt to hide malicious activities from detection mechanisms. Following this, PowerShell was used to execute a script that fetched and executed content from a local HTML file, indicating potential execution of malicious code. The adversary continued their efforts by again using certutil.exe to decode the same 'kxwn.lock' file, reinforcing their defense evasion tactics.

To maintain persistence, the attacker created a Windows Management Instrumentation (WMI) event subscription named 'WindowsParentalControlMigration'. This subscription was designed to trigger PowerShell execution whenever the user 'dschrute' logged on, ensuring that the adversary could regain control even after system restarts or credential changes. The PowerShell command executed upon this event included downloading and running a script from an external source, further suggesting malicious intent.

The attacker continued to execute PowerShell scripts, likely for various purposes such as reconnaissance or further exploitation. Additionally, they used rundll32.exe to load a DLL file named 'kxwn.lock', which was previously decoded using certutil.exe. This action indicates an attempt to execute code from the decoded file, possibly containing malicious payloads.

Throughout these activities, the adversary demonstrated a combination of defense evasion, execution, and persistence techniques, leveraging tools like PowerShell, certutil.exe, and WMI event subscriptions to maintain control over the compromised system while avoiding detection.

Access Summary:
The timeline data indicates a series of events where an adversary attempts to escalate privileges and access credentials on a system. Initially, at 7:59 AM UTC on May 2, 2020, the user 'DMEVALS\dschrute' executed a process named 'm.exe', which was used to dump credentials from the LSASS memory. This action suggests an attempt to gain unauthorized access to sensitive information stored in system memory. The execution of this process and subsequent library loads indicate that the adversary may have been trying to extract passwords or other authentication material, potentially for lateral movement within the network.

Later, at 8:12 AM UTC, there were multiple process executions involving

UTICA.dmevals.local Summary

'wininit.exe' and 'services.exe', both running under the 'NT AUTHORITY\SYSTEM' account. These processes interacted with LSASS, suggesting further attempts to access or manipulate system credentials. The creation of a file in the System32 directory also points to potential tampering with system files, which could be part of an effort to maintain persistence on the compromised machine.

At 8:07 AM UTC and again at 8:21 AM UTC, PowerShell script blocks were executed, invoking commands that appear to involve Mimikatz, a tool known for credential dumping and manipulation. These actions indicate an attempt to create or use golden tickets, which are forged Kerberos tickets used to gain unauthorized access to resources within the domain.

Mobility Summary:
On May 2, 2020, beginning at 7:55 AM UTC, a series of suspicious activities were observed on a network, indicating potential lateral movement and remote execution by an adversary. The initial activity involved the execution of PowerShell commands that downloaded and executed scripts from a remote server (192.168.0.4). These actions suggest the adversary was attempting to gain control over the system using valid accounts and legitimate tools, a common tactic for stealthy lateral movement.

At 7:59 AM UTC, another PowerShell command was executed, this time downloading an executable file ('m.exe') from the same remote server and running it with specific arguments to extract sensitive information such as passwords. This activity aligns with the adversary's intent to gather credentials for further lateral movement within the network.

Between 7:58 AM and 8:04 AM UTC, multiple network connections were established from the compromised system (10.0.1.5) to another internal IP address (10.0.0.4) on port 5985, which is associated with Windows Remote Management (WinRM). This suggests that the adversary was using WinRM for lateral movement and potentially executing commands on remote systems.

At 8:17 AM UTC, there were two instances of a user ('dschrute') logging into the system via Remote Desktop Protocol (RDP) from an external IP address (172.18.39.2). This indicates that the adversary might have gained access to valid domain credentials and was using RDP for further lateral movement within the network.

Between 8:15 AM and 8:40 AM UTC, additional PowerShell commands were executed, downloading scripts from the same remote server (192.168.0.4) and establishing multiple connections to another internal IP address (10.0.1.4) on port 5985. This pattern of activity suggests that the adversary was continuing their lateral movement efforts, potentially compromising additional systems within

UTICA.dmevals.local Summary

the network.

Data Movement Summary:
The adversaries began their operation by transferring tools into the compromised environment on May 1, 2020, at 7:09 AM UTC. They retrieved a Windows executable file identified as 'mimikatz' from an external IP address (192.168.0.4). This tool is commonly used for credential theft and could be part of the adversaries' collection efforts to gather sensitive information.

On May 2, 2020, at 7:55 AM UTC, the adversaries continued their activities by using 'certutil.exe' to decode a file named 'kxwn.lock', which was created in the user directory of 'dschrute'. This action suggests that they were preparing or staging data for exfiltration.

Later that day, at 8:09 AM UTC, the adversaries executed a command using 'net.exe' to map a network drive to a cloud storage service (Microsoft OneDrive) using credentials provided in the command. This action was followed by an outbound network connection to an IP address associated with Microsoft's live services, indicating that data exfiltration was likely underway. The use of a legitimate web service for exfiltration provides cover and makes detection more challenging.

Overall, these activities show a clear pattern of tool transfer, data staging, and exfiltration, suggesting the adversaries were focused on stealing sensitive information from the compromised system.

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, 192.168.0.4
Observed Users: DMEVALS\pbeesly, pbeesly, DMEVALS\mscott, DMEVALS\kmalone, kmalone

Executive Summary:
The timeline data indicates an adversary attempting to establish command and control over compromised systems within a victim network. On April 30, 2020, at 00:35:26 UTC, there was evidence of Ingress Tool Transfer where a Python executable (python.exe) was downloaded from an external IP address (192.168.0.4). This suggests that the adversary may have been trying to introduce additional tools or malware into the environment.

On May 2, 2020, at 02:55:56 UTC, there was a high-risk Execution event involving masquerading and right-to-left override techniques. A suspicious file named 'â€®cod.3aka3.scr' was executed for the first time under the user account 'DMEVALS\pbeesly'. This execution indicates the potential initial infection or activation of malware on the system.

Subsequently, at 02:58:18 UTC, there were multiple Persistence events involving registry modifications and PowerShell executions. The adversary modified a registry key to ensure that a script would run automatically, likely for persistence purposes. This script was designed to extract and execute a payload from an image file (monkey.png).

At 03:04:23 UTC, another Persistence event occurred where a startup link (hostui.lnk) was created in the Start Menu, suggesting further entrenchment of the malware for user logon persistence. Additionally, at 03:05:16 UTC, there were Credential Access and Defense Evasion events. The adversary attempted to dump OS credentials from LSASS memory and injected a process into lsass.exe, indicating efforts to evade detection and gain further control over the system.

Root Cause Analysis:
The root cause of this incident appears to be the initial download of the Python executable (python.exe) from an external IP address on April 30, 2020. This action likely facilitated the adversary's command and control over the compromised system. The subsequent execution of 'â€®cod.3aka3.scr' on May 2, 2020, suggests that this file was the initial malware payload introduced into the environment.

SCRANTON.dmevals.local Summary

Vulnerabilities or weaknesses in the network security may have allowed the adversary to download and execute these files without immediate detection. The use of PowerShell for script execution and registry modifications indicates a potential lack of adequate controls or monitoring on these commonly abused tools.

Impact Assessment:
The incident has significant implications for the victim's operations, data integrity, and security posture. The adversary successfully established command and control over compromised systems, executed malware, and implemented persistence mechanisms to maintain access. This could lead to further exploitation, data exfiltration, or disruption of services.

The credential dumping attempt indicates that the adversary was targeting sensitive information, potentially putting user credentials at risk. The process injection into lsass.exe suggests sophisticated evasion techniques, which could complicate detection and response efforts. Overall, this incident underscores the need for robust security controls, monitoring, and incident response capabilities to mitigate similar threats in the future.

Tradecraft Summary:
The adversary initiated their attack by executing malware disguised as a screensaver file named 'â€®cod.3aka3.scr' on the victim's system at 02:55 UTC. This technique, known as Right-to-Left Override (RTLO), manipulates the display of the filename to appear benign, aiming to evade detection and trick the user into execution. The malware was run by the user 'DMEVALS\pbeesly' with process ID 8524.

Shortly after, at 02:57 UTC, a PowerShell process was executed, likely to establish persistence on the system. This was achieved by modifying the registry to include a hidden PowerShell command that would run at startup, ensuring the adversary's access even after reboots. The command involved decoding an image file ('monkey.png') to extract and execute embedded malicious code.

At 03:04 UTC, another persistence mechanism was set up by creating a shortcut named 'hostui.lnk' in the Startup folder, further ensuring that the malicious PowerShell script would run on system startup. This action solidified the adversary's foothold on the compromised machine.

To evade detection and analysis, at 03:05 UTC, the adversary employed process injection techniques targeting 'lsass.exe', a critical Windows process. By injecting malicious code into this legitimate process, the adversary aimed to hide their activities from security tools and maintain control over the system

SCRANTON.dmevals.local Summary

without raising suspicion.

Access Summary:
The adversary initiated a sequence of actions that suggest attempts at privilege escalation and credential access on May 2nd, 2020. At 03:05:16 UTC, there was an attempt to dump credentials from the LSASS memory, which is a technique used to harvest sensitive information such as passwords stored in system memory. This action indicates that the adversary might be trying to gain higher-level permissions or access additional systems within the network.

Prior to this, at 02:58:44 UTC, a PowerShell script was executed by user 'DMEVALS\pbeesly'. The command involved creating and manipulating a bitmap image to potentially hide malicious code or data, suggesting an attempt to evade detection. This script could be part of the adversary's strategy to gain unauthorized access or escalate privileges within the system.

Immediately following the PowerShell execution, at 03:05:16 UTC, there was an attempt to open the LSASS process, which is a critical component for managing security and authentication on Windows systems. This action aligns with the credential dumping attempt noted earlier, reinforcing the likelihood that the adversary is trying to extract sensitive information from the system's memory.

Mobility Summary:
The timeline begins with a PowerShell script executed on a system by user 'DMEVALS\pbeesly'. This script appears to decode and execute hidden code from an image file located in the user's Downloads folder, suggesting potential malicious activity aimed at executing arbitrary code. Immediately following this execution, network connections are established with remote IP addresses over port 443, indicating possible command-and-control communication or data exfiltration.

Subsequently, another PowerShell script is executed by the same user, followed by a series of network connections to various remote services on different ports, including HTTP (port 80), LDAP (port 389), and WinRM (port 5985). These activities suggest lateral movement within the network, where the adversary might be exploring other systems or attempting to gain access to additional resources.

The timeline then shows multiple instances of PsExec64.exe being executed with specific commands targeting a remote system ('NASHUA') using valid domain credentials. This tool is commonly used for software deployment but can also be abused by adversaries for lateral movement and remote code execution. The network connections associated with these executions involve ports typically used for file sharing (port 445) and RPC services (port 135), further

SCRANTON.dmevals.local Summary

indicating attempts to move across the network and potentially execute commands on other systems.

Finally, there are multiple logon events via Remote Desktop Protocol (RDP) from a remote IP address, suggesting that the adversary is using RDP for lateral movement or to maintain persistence within the network. These activities collectively paint a picture of an adversary leveraging various techniques and tools to move through the network, execute commands remotely, and potentially exfiltrate data or maintain control over compromised systems.

Data Movement Summary:
The adversaries initiated command and control communication by transferring a tool into the compromised environment at 04/30/2020 00:35:26 UTC. The tool, identified as 'python.exe', was downloaded from an external system with IP address 192.168.0.4. This action suggests that the adversaries are preparing to execute further commands or tools on the compromised system, potentially leading to data collection and exfiltration activities. The use of a Windows Portable Executable (PE) file indicates that the tool is likely designed to run on Windows systems, which could be used for various malicious purposes such as gathering sensitive information or establishing persistent access. This initial ingress tool transfer sets the stage for potential data theft and further compromise within the network.