# Demo Investigation

## *Endpoints*

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

# Investigation Summary

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

Generated with: Mistral Large Instruct 2407 IQ2 XS 32,768k context

Incident Response Investigation Report

Executive Summary:
This incident response timeline investigation aims to analyze suspicious activities across multiple Windows endpoints within our network. The scope includes identifying and understanding the nature, extent, and impact of potential intrusions on these systems. This investigation is crucial as it addresses the security and integrity of our digital infrastructure, which could have significant implications for our operations and data protection.

Summary of Findings:
The forensic timeline analysis revealed a series of coordinated malicious activities across multiple endpoints (SCRANTON, UTICA, NASHUA, NEWYORK). Key observations include the transfer of Windows executables via command and control (C2) communication, extensive use of PowerShell scripts for execution and persistence, attempts to dump OS credentials, and lateral movement within the network.

Patterns indicate a sophisticated attack with common techniques such as registry modifications for persistence, use of tools like PsExec64.exe for remote execution, and data exfiltration through cloud storage services. The timeline shows consistent efforts to evade detection and establish control over systems, suggesting a coordinated threat actor.

Root Cause Analysis:
The root cause of the incident appears to be an initial compromise via command and control communication, followed by the execution of malicious files. Vulnerabilities in endpoint security allowed for unauthorized access and lateral movement within the network. Misconfigurations or lack of adequate security measures contributed to the success of these intrusions.

Impact Assessment:
The incident has significant implications for our operations and data integrity. Unauthorized access and potential credential harvesting pose a risk to sensitive information. The use of sophisticated persistence mechanisms and lateral movement indicates that multiple systems may have been compromised, affecting overall network security.

# Investigation Summary

Immediate action is required to contain the threat, mitigate further damage, and restore system integrity. This includes isolating affected endpoints, reviewing and updating security protocols, and implementing additional monitoring and detection measures to prevent future incidents.

Incident Narrative:
The adversary initiated their operation on April 30, 2020, at 12:35 AM by transferring tools into the compromised environment of SCRANTON.dmevals.local from an external source (TA0011). They downloaded a Windows executable file identified as 'python.exe' from IP address 192.168.0.4, aligning with MITRE technique TA0011.T1105.000. This action suggests the adversary was establishing command and control by introducing new tools into the network.

On May 1st, 2020, at 7:09 AM UTC, the adversary continued their operation on UTICA.dmevals.local by transferring Mimikatz from a remote server located at IP address 192.168.0.4 (TA0011). The next day, May 2nd, 2020, at 7:55 AM UTC, they used certutil to decode an encoded file and created a new file named 'kxwn.lock' in the user directory of DMEVALS\dschrute (TA0040). Later that same day, at 8:10 AM UTC, the adversary attempted data exfiltration using Microsoft OneDrive with credentials urukhai2020@outlook.com and V@m0s0rc0!2020 from local IP 10.0.1.5 to remote IP 13.107.42.12 over port 61554 (TA0010).

On SCRANTON, the adversary gained initial access through the execution of a disguised file named 'cod.3aka3.scr', which was actually a malicious script masquerading as a screensaver executable at 2:55 AM UTC on May 2nd, 2020. On UTICA, the initial access method was not explicitly observed but involved the decoding of an encoded file using certutil.exe and conhost.exe at 3:01 AM UTC. The initial access on NASHUA was indicated by the execution of Python scripts.

In terms of execution, the adversary employed PowerShell extensively across all endpoints. On SCRANTON, multiple instances of PowerShell were used to extract data from an image file and execute hidden commands. On UTICA, PowerShell was used to download and decode additional payloads from a remote server. On NASHUA, Python scripts and PowerShell commands were executed, followed by the use of cmd.exe for further command execution.

For persistence, the adversary modified the registry on SCRANTON to include a PowerShell script that would run upon logon or boot. On UTICA, a WMI event subscription was created to trigger the execution of a PowerShell script whenever a specific user logged on, ensuring continued access even after system reboots or user logoffs.

Defense evasion techniques were employed across all endpoints. On SCRANTON, the

## Investigation Summary

adversary injected processes into legitimate system processes like lsass.exe and used Sysinternals tools such as sdelete64.exe and PsExec64.exe to clean up traces of their activities. On UTICA, the use of certutil.exe for decoding files and the execution of sdclt.exe to run arbitrary commands were observed. On NASHUA, sdelete64.exe was used to delete specific files systematically, and registry modifications were made to accept the EULA for Sysinternals' SDelete tool, ensuring uninterrupted use.

The adversary initiated privilege escalation and credential access activities across multiple endpoints on May 2nd, 2020. At 3:05 AM UTC, on SCRANTON.dmevals.local, a PowerShell process executed a script to decode hidden commands from an image file, suggesting potential misuse of privileges or unauthorized access under the user account 'DMEVALS\pbeesly'. At 3:58 AM UTC, the adversary accessed the Local Security Authority Subsystem Service (LSASS) process memory, likely to harvest credential material.

On UTICA.dmevals.local, beginning at 7:59 AM UTC, the user 'DMEVALS\dschrute' executed a process named 'm.exe', attempting to dump credentials from LSASS memory using commands like 'sekurlsa::logonpasswords'. At 8:07 AM UTC, a PowerShell script invoked commands related to 'lsadump::lsa /inject /name:krbtgt', indicating further credential dumping attempts. System processes such as 'wininit.exe' and 'services.exe' were executed by 'NT AUTHORITY\SYSTEM' at 8:12 AM UTC, suggesting potential manipulation of system services to facilitate credential dumping. PowerShell scripts executed at 8:20 AM and 8:21 AM UTC invoked Mimikatz commands related to Kerberos golden ticket creation, aiming to gain persistent access by impersonating a legitimate user or service account.

On NEWYORK.dmevals.local, the adversary executed 'm.exe' to dump credentials from LSASS memory, targeting the 'krbtgt' account. Multiple instances of 'm.exe' were executed within a short timeframe, loading system libraries not typically associated with legitimate LSASS operations.

The adversary initiated a sequence of actions aimed at lateral movement and remote execution within the network, beginning on May 2nd, 2020, at 3:12 AM UTC with the execution of PowerShell commands to decode an image file into executable code on SCRANTON.dmevals.local. This was followed by establishing multiple network connections to different IP addresses, suggesting attempts to explore and gain access to other systems within the network.

At around 3:12 AM UTC, the adversary utilized PsExec64 to execute commands on remote machines, targeting specific ports associated with administrative services such as port 445 and port 80. By 3:21 AM UTC, the adversary had successfully logged into a remote machine using Remote Desktop Protocol (RDP),

## Investigation Summary

indicating successful lateral movement and potential further compromise of the target system.

On UTICA.dmevals.local, the first instance of malware execution occurred when PowerShell was used to download and execute a script from a remote server, indicating potential remote services usage for lateral movement. The adversary also leveraged Windows Management Instrumentation (WMI) to execute malicious payloads, evident in the use of WMI commands to download and run executables from remote servers. Multiple network connections were established with various IP addresses, including those associated with known remote services like SSH and RDP, further supporting the notion of lateral movement. The adversary's actions included logging into a computer using Remote Desktop Protocol (RDP), followed by additional PowerShell commands executed to download and run scripts from remote servers, indicating a persistent effort to maintain control over the system and potentially exfiltrate data.

On NASHUA.dmevals.local, the activity began with multiple instances of remote services access using valid accounts, specifically user 'pbeesly' from the domain 'DMEVALS.LOCAL', originating from IP address '10.0.1.4'. These logins were followed by access to network share objects, suggesting attempts at lateral movement and data access across different systems. Subsequently, there are several instances of software deployment tools being utilized for potential lateral movement. The execution of 'PSEXESVC.exe' under the SYSTEM account indicates the use of administrative privileges, which could be leveraged to execute commands on remote systems. Additionally, the repeated execution of 'python.exe' from a temporary directory suggests the running of scripts or payloads that may facilitate further lateral movement or data exfiltration.

Overall, the timeline indicates a systematic approach by the adversary to gain unauthorized access and move laterally within the network, utilizing both legitimate tools and exploiting existing vulnerabilities to achieve their objectives. The use of PowerShell, WMI, RDP, PsExec64, and other remote services highlights the sophistication and intent behind these actions, suggesting a deliberate effort to compromise and control the network environment.

In summary, the adversary established command and control by transferring tools into compromised environments, prepared for data collection and exfiltration by decoding files and creating archives, and attempted to move data out of the network through a cloud storage service. These actions indicate a systematic approach to infiltrate, collect, and exfiltrate data from multiple endpoints within the victim network.

# NASHUA.dmevals.local Summary

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

Summary of Findings:
The timeline reveals a series of coordinated actions indicative of lateral movement and data exfiltration within the network. The attacker leveraged remote services and software deployment tools to access and manipulate files across different systems. Notably, there were multiple instances of file creation, modification, and deletion, suggesting a systematic approach to gathering and removing sensitive information. The use of Python scripts and PowerShell commands further indicates a sophisticated attempt at data collection and exfiltration.

Root Cause Analysis:
The root cause of the incident appears to be an initial network connection from IP 10.0.1.6 to 10.0.0.4, which facilitated unauthorized access and subsequent lateral movement. Vulnerabilities in remote services and software deployment tools were exploited to gain further access and execute malicious activities. The attacker's ability to create and delete files, as well as execute commands, indicates a lack of proper security controls and permissions management within the network.

Impact Assessment:
The incident had significant implications for data integrity and operational security. Sensitive files were accessed, compressed, and potentially exfiltrated, posing a risk to confidential information. The use of legitimate administrative tools like PowerShell and Python scripts for malicious purposes highlights the need for enhanced monitoring and control over such tools. The systematic deletion of files suggests an attempt to cover tracks and hinder forensic investigation. Overall, the incident underscores the importance of robust security measures and continuous monitoring to detect and mitigate similar threats in the future.

Narrative:
The adversary initiated their attack by executing Python scripts on the target system, indicating a potential initial access attempt through command and script interpreter techniques. This was followed by the execution of PowerShell commands, suggesting further attempts at gaining control over the system. The use of Rar.exe to archive files hints at data exfiltration or preparation for such activities.

# NASHUA.dmevals.local Summary

Subsequently, the adversary executed cmd.exe and sdelete64.exe, indicating a possible attempt to cover their tracks by deleting specific files. This behavior aligns with defense evasion tactics, as the adversary aims to avoid detection by removing evidence of their presence. The repeated use of sdelete64.exe on different file paths suggests a systematic approach to erasing traces of their activities.

The registry modifications observed during these actions indicate that the adversary accepted the EULA for Sysinternals' SDelete tool, which is used for securely deleting files. This further supports the defense evasion hypothesis, as the adversary ensures they can use this tool without interruption.

The timeline data indicates a series of events involving potential lateral movement and remote execution within a network environment. The activity begins with multiple instances of remote services access using valid accounts, specifically user 'pbeesly' from the domain 'DMEVALS.LOCAL', originating from IP address '10.0.1.4'. These logins were followed by access to network share objects, suggesting attempts at lateral movement and data access across different systems.

Subsequently, there are several instances of software deployment tools being utilized for potential lateral movement. The execution of 'PSEXESVC.exe' under the SYSTEM account indicates the use of administrative privileges, which could be leveraged to execute commands on remote systems. Additionally, the repeated execution of 'python.exe' from a temporary directory suggests the running of scripts or payloads that may facilitate further lateral movement or data exfiltration.

The pattern of logins and network share accesses, coupled with the use of administrative tools and script execution, strongly indicates an adversary attempting to move laterally through the network. The repeated access attempts and consistent use of specific tools suggest a methodical approach to gaining control over multiple systems within the network environment. This activity aligns with MITRE tactics for Lateral Movement (TA0008) and potentially Remote Execution (TA0002), as the adversary appears to be executing code remotely and moving between different nodes in the network.

The adversary attempted to archive and compress collected data on a compromised system using Rar.exe, a utility for creating compressed archives. The command executed was intended to create or update a password-protected archive named 'working.zip' located at 'C:\Users\pbeesly\Desktop\working.zip', with the source files being 'C:\Users\pbeesly\AppData\Roaming\working.zip'. This action suggests that the adversary was preparing data for exfiltration, possibly to

## NASHUA.dmevals.local Summary

evade detection by compressing and encrypting the information. The process was executed under the user account 'DMEVALS\pbeesly', indicating potential compromise of this user's credentials or session.

# 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 a coordinated attack on an endpoint within the DMEVALS domain. The attack began with the execution of 'wsmprovhost.exe', followed by network connections and file modifications. Notably, OS credential dumping was detected, where the adversary attempted to extract credentials using 'm.exe' targeting LSASS memory. This activity suggests a deliberate effort to gain unauthorized access to sensitive information.

Root Cause Analysis
The root cause of this incident is attributed to the execution of malicious processes and credential dumping attempts on the endpoint. The attacker leveraged 'wsmprovhost.exe' and 'm.exe' to perform these actions, indicating a potential vulnerability in the system that allowed such executions. Additionally, the successful network connections and file modifications suggest possible misconfigurations or lack of adequate security controls.

Impact Assessment
The incident has significant implications for operational security and data integrity. The attempted credential dumping poses a risk of unauthorized access to sensitive information, which could lead to further compromises and potential lateral movement within the network. The detection of Kerberos authentication ticket requests indicates that the attacker may have gained elevated privileges, exacerbating the impact on operations. Immediate remediation actions are necessary to mitigate the risk of further compromise and ensure the integrity of the network and data.

Detailed Narrative
The adversary attempted to gain unauthorized access to credentials stored on a Windows system by executing a series of commands using 'm.exe', a suspicious process likely designed for malicious purposes. The command aimed to dump credentials from the Local Security Authority Subsystem Service (LSASS) memory, specifically targeting the 'krbtgt' account, which is typically used for Kerberos ticket-granting tickets. This activity aligns with the MITRE ATT&CK technique T1003.001, indicating an attempt to access sensitive credential material stored in LSASS process memory.

## NEWYORK.dmevals.local Summary

The adversary executed multiple instances of 'm.exe' within a short timeframe, suggesting repeated attempts or scripted automation. The process loaded several system libraries such as 'cryptdll.dll', 'samlib.dll', 'hid.dll', and 'WinSCard.dll', which are not typically associated with legitimate LSASS operations, further indicating malicious intent.

The repeated execution of 'm.exe' and the loading of unusual libraries suggest that the adversary was attempting to exploit system weaknesses or misconfigurations to escalate privileges (TA0004). The focus on credential dumping (TA0006) indicates an effort to obtain account names and passwords, likely for lateral movement within the network.

The timeline shows a clear pattern of credential access attempts, with potential privilege escalation as a secondary goal. This activity poses a significant risk to the security of the system and the broader network, as successful credential theft could lead to unauthorized access and further compromise.

# 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

Executive Summary
The timeline reveals a series of coordinated actions indicating an advanced persistent threat (APT) attack on the network. On May 1st, 2020, at 7:09 AM UTC, an adversary transferred Mimikatz, a credential dumping tool, from an external IP address to the compromised system. This was followed by multiple PowerShell script executions on May 2nd, including commands that disabled security measures and executed additional scripts. The attacker then used Mimikatz to dump credentials from the Local Security Authority Subsystem Service (LSASS) memory, indicating a significant escalation in privilege access.

Summary of Findings
The timeline reveals a series of coordinated actions indicating an advanced persistent threat (APT) attack on the network. On May 1st, 2020, at 7:09 AM UTC, an adversary transferred Mimikatz, a credential dumping tool, from an external IP address to the compromised system. This was followed by multiple PowerShell script executions on May 2nd, including commands that disabled security measures and executed additional scripts. The attacker then used Mimikatz to dump credentials from the Local Security Authority Subsystem Service (LSASS) memory, indicating a significant escalation in privilege access.

Root Cause Analysis
The root cause of this incident is attributed to an external actor gaining unauthorized access and transferring malicious tools into the network environment. The attacker exploited vulnerabilities within the system, such as weak security configurations that allowed for the execution of PowerShell scripts without proper authentication or monitoring. The use of Mimikatz further indicates a targeted attempt to gain higher-level credentials, suggesting a sophisticated threat actor with specific objectives.

Impact Assessment
The incident has had significant implications on network security and data integrity. The unauthorized access and credential dumping pose a risk of further compromise, including potential exfiltration of sensitive information or additional malicious activities. The use of PowerShell scripts to disable security measures highlights the attacker's intent to maintain persistence

## UTICA.dmevals.local Summary

within the network. Immediate remediation actions are required to contain the threat, assess the extent of the compromise, and implement stronger security controls to prevent future incidents.

Narrative Summary
The adversary gained initial access through unknown means and began executing commands using PowerShell and other command-line interpreters on a Windows system under the user account 'DMEVALS\dschrute'. The first observed activity was the execution of 'conhost.exe' followed by 'certutil.exe', which decoded an encoded file located in the user's AppData directory. This suggests that the adversary may have already placed this file on the system as part of their initial access or through a previous action not captured in the timeline.

The adversary then executed multiple instances of 'csc.exe', a C compiler, indicating they were compiling and possibly running custom code on the system. This was followed by the execution of 'sdclt.exe', which is typically associated with security center settings but can be used to execute arbitrary commands. The adversary also executed PowerShell scripts that downloaded and decoded additional payloads from a remote server, indicating further command and control (C2) activity.

The use of 'certutil.exe' for decoding files was repeated multiple times, suggesting the adversary was obfuscating their actions by encoding data. The PowerShell scripts executed included commands to bypass security measures and execute downloaded code, indicating defense evasion techniques. A notable event was the creation of a Windows Management Instrumentation (WMI) event subscription that triggered the execution of a PowerShell script whenever a specific user logged on. This persistence mechanism ensures that the adversary's access is maintained even if the system reboots or the user logs off and back on.

Additionally, the adversary used 'net.exe' to map a network drive, indicating potential lateral movement within the network. The use of 'rundll32.exe' to execute a function from a DLL file further suggests the adversary was running custom code designed to evade detection.

Beginning at 07:59:10 UTC on May 2nd, 2020, the user 'DMEVALS\dschrute' executed a process named 'm.exe', which attempted to dump credentials from the Local Security Authority Subsystem Service (LSASS) memory using commands like 'sekurlsa::logonpasswords'. This activity indicates an attempt to access and potentially steal credential material stored in LSASS, a common target for adversaries seeking to escalate privileges.

At 08:12:26 UTC, system processes such as 'wininit.exe' and 'services.exe' were

## UTICA.dmevals.local Summary

executed by 'NT AUTHORITY\SYSTEM', indicating potential manipulation of system services to facilitate credential dumping. The creation of a file in the System32 directory ('C:\Windows\System32\LogFiles\Scm\SCM.EVM') suggests that the adversary may be staging or logging their activities for further exploitation.

Finally, at 08:19:56 and 08:21:59 UTC, PowerShell scripts were executed to invoke Mimikatz commands related to Kerberos golden ticket creation. These commands aimed to create a golden ticket with specific domain and user details, indicating an attempt to gain persistent access to the network by impersonating a legitimate user or service account.

The adversary initiated a series of actions aimed at executing malicious code and moving laterally across the network. The first instance of malware execution occurred when PowerShell was used to download and execute a script from a remote server, indicating potential remote services usage for lateral movement. This activity continued with multiple instances of PowerShell commands being executed to download and run additional scripts, suggesting an attempt to gather information or further compromise the system.

The adversary also leveraged Windows Management Instrumentation (WMI) to execute malicious payloads, indicating a sophisticated approach to lateral movement and remote execution. This was evident in the use of WMI commands to download and run executables from remote servers. Additionally, there were multiple network connections established with various IP addresses, including those associated with known remote services like SSH and RDP, further supporting the notion of lateral movement.

The adversary's actions included logging into a computer using Remote Desktop Protocol (RDP), which is a common technique for expanding access within a compromised network. This was followed by additional PowerShell commands executed to download and run scripts from remote servers, indicating a persistent effort to maintain control over the system and potentially exfiltrate data.

The adversary began their operation by transferring tools into the compromised environment on May 1st, 2020 at 7:09 AM UTC. They retrieved Mimikatz from a remote server located at IP address 192.168.0.4. The next day, on May 2nd, 2020 at 7:55 AM UTC, they used certutil to decode an encoded file and created a new file named 'kxwn.lock' in the user directory of DMEVALS\dschrute. Later that same day, at 8:10 AM UTC, the adversary attempted to exfiltrate data using a web service by connecting to Microsoft OneDrive with credentials urukhai2020@outlook.com and V@m0s0rc0!2020. The connection was made from the local IP 10.0.1.5 to the remote IP 13.107.42.12 over port 61554, using protocol

## UTICA.dmevals.local Summary

TCP (6). This sequence of events suggests that the adversary was preparing for data exfiltration by first transferring necessary tools, then decoding and creating files, and finally attempting to move data out of the network through a cloud storage service.

# 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

Summary of Findings:
The timeline reveals a series of coordinated actions indicating an intrusion into the network environment. On April 30th, 2020, at 00:35:26 UTC, a Python executable was downloaded from an external IP address (192.168.0.4), suggesting initial command and control activity. Subsequently, on May 2nd, 2020, at 02:55:56 UTC, malware execution was detected with the filename 'cod.3aka3.scr', masquerading as a legitimate process. This event marked the first appearance of malicious activity and was later stopped.

Following this, multiple persistence mechanisms were observed. At 02:58:18 UTC on May 2nd, PowerShell scripts were executed to modify registry keys, indicating an attempt to establish long-term access by embedding a script within the system's startup sequence. This activity was repeated at 03:04:23 UTC with the creation of a shortcut in the Startup folder, further entrenching the malicious presence on the system.

Credential dumping attempts were noted at 03:05:16 UTC on May 2nd, targeting LSASS memory to extract sensitive information. Additionally, process injection techniques were employed to evade detection by injecting code into legitimate processes such as 'lsass.exe'. These actions collectively point towards a sophisticated and coordinated attack aimed at gaining unauthorized access and maintaining persistence within the network.

Root Cause Analysis:
The root cause of this incident can be traced back to the initial command and control activity, where an external IP address (192.168.0.4) was used to download a Python executable onto the system. This action facilitated further malicious activities, including the execution of malware and subsequent persistence mechanisms.

Vulnerabilities in the network's security measures allowed for the successful ingress tool transfer and the execution of malicious code. The attacker leveraged PowerShell scripts to modify registry keys and create startup shortcuts, indicating potential misconfigurations or weaknesses in endpoint protection and monitoring systems. Additionally, the ability to dump credentials from LSASS memory suggests that there may be gaps in the system's

## SCRANTON.dmevals.local Summary

security controls, such as insufficient privilege management or inadequate logging and alerting mechanisms.

Impact Assessment:
The incident has significant implications for network operations and data integrity. The successful execution of malware and persistence mechanisms indicates a potential compromise of sensitive information and unauthorized access to critical systems. The credential dumping attempts further exacerbate the risk, as extracted credentials could be used to escalate privileges or gain access to additional resources within the network.

The impact on operations includes potential disruptions in service availability and increased security risks due to the presence of malicious code. Data integrity may also be compromised if the attacker has gained unauthorized access to sensitive information. The incident underscores the need for enhanced security measures, including improved endpoint protection, regular system updates, and robust monitoring and alerting systems to detect and mitigate such threats in the future.

Narrative of Adversary Actions:
The adversary initiated a sequence of actions aimed at gaining unauthorized access and maintaining control over the compromised system. On April 30th, 2020, at 00:35:26 UTC, they downloaded a Python executable from an external IP address (192.168.0.4), indicating initial command and control activity.

On May 2nd, 2020, the adversary executed a disguised file named 'cod.3aka3.scr', which was actually a malicious script masquerading as a screensaver executable. This file was executed by user DMEVALS\pbeesly at 02:55:56 UTC, marking the first appearance of malware on the system. The adversary then established persistence by modifying the registry to include a PowerShell script that would run upon logon or boot, ensuring their continued access.

Subsequently, multiple instances of PowerShell were executed, indicating the use of command and scripting interpreters for further payload delivery and execution. Notably, at 02:58:44 UTC, a PowerShell script was used to extract data from an image file named 'monkey.png', suggesting the use of steganography to hide malicious code within benign files. This script was executed multiple times, indicating its importance in the adversary's operations.

The adversary also employed defense evasion techniques by injecting processes into legitimate system processes like lsass.exe at 03:05:16 UTC. This technique allows the malicious code to run under the guise of a trusted process, making it harder to detect. Additionally, the use of Sysinternals tools such as

## SCRANTON.dmevals.local Summary

sdelete64.exe and PsExec64.exe was observed, indicating attempts to clean up traces of their activities and deploy additional payloads across the network.

Throughout the timeline, the adversary repeatedly executed PowerShell scripts and used software deployment tools like csc.exe and PsExec64.exe, suggesting a methodical approach to spreading malware and maintaining control over the compromised system. The final observed activity at 03:21:28 UTC involved the execution of hidden PowerShell commands, indicating ongoing efforts to maintain stealthy operations on the endpoint.

The adversary initiated communication with a compromised system within the victim network at 00:35:26 on April 30, 2020, transferring tools from an external source. Specifically, they downloaded a Windows executable file identified as 'python.exe' from the IP address 192.168.0.4. This action aligns with the MITRE technique TA0011.T1105.000, indicating an attempt to establish command and control by transferring tools into the compromised environment. The downloaded file has a SHA-256 hash of 'ed3e182db635685ad65071473ec1dbaed5fde9f3014716f734b9816b73ac0905' and is classified as a Windows EXE. This activity suggests the adversary is preparing to execute further actions, potentially involving data collection or exfiltration, by introducing new tools into the network.

The adversary initiated a PowerShell process on May 2nd, 2020 at 03:05:16 UTC, which executed a script designed to decode and execute hidden commands from an image file named 'monkey.png'. This action was performed under the user account 'DMEVALS\pbeesly', suggesting potential misuse of privileges or unauthorized access. Subsequently, at 03:58:44 UTC, the adversary accessed the Local Security Authority Subsystem Service (LSASS) process memory, likely to harvest credential material such as passwords and authentication tokens. This activity aligns with the MITRE technique TA0006 Credential Access, specifically OS Credential Dumping and LSASS Memory techniques. The combination of these actions indicates a concerted effort by the adversary to escalate privileges and gain unauthorized access to sensitive information or systems, potentially for lateral movement within the network.

The adversary initiated a sequence of actions aimed at lateral movement and remote execution within the network. Beginning on May 2nd, 2020, at 02:58 UTC, the adversary executed PowerShell commands to decode an image file into executable code, indicating potential malicious activity. This was followed by establishing multiple network connections to different IP addresses, suggesting attempts to explore and gain access to other systems within the network.

At around 03:12 UTC, the adversary utilized PsExec64, a legitimate system administration tool, to execute commands on remote machines. This tool was used

## SCRANTON.dmevals.local Summary

repeatedly over several minutes, targeting specific ports associated with administrative services such as port 445 and port 80. The use of these tools and ports suggests that the adversary was attempting to move laterally across the network by leveraging valid accounts and exploiting existing system vulnerabilities.

By 03:21 UTC, the adversary had successfully logged into a remote machine using Remote Desktop Protocol (RDP), indicating successful lateral movement and potential further compromise of the target system. The repeated use of RDP logins suggests that the adversary was attempting to establish persistent access or perform additional reconnaissance on the network.

Overall, the timeline indicates a systematic approach by the adversary to gain unauthorized access and move laterally within the network, utilizing both legitimate tools and exploiting existing vulnerabilities to achieve their objectives.