Demo Investigation

Endpoints

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

Investigation Summary

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

Generated with: Mixtral 8x7b Instruct Q5 K M 32,768 context

On May 2nd, 2020 at approximately 3:10 AM UTC, a user with the username 'pbeesly' and domain 'DMEVALS.LOCAL' initiated remote access to a system with IP address '10.0.1.4' using Remote Services (TA0008.T1021.000). The user then accessed a network share object, followed by the execution of software deployment tools to execute 'PSEXESVC.exe' with system privileges and 'python.exe' under the user 'pbeesly'. This pattern repeated several times over the next few minutes, indicating lateral movement throughout the network (TA0008). At 3:15 AM UTC, a final authentication was performed by 'pbeesly' into another remote system, followed by the execution of 'PSEXESVC.exe' and 'python.exe', suggesting potential unauthorized access to additional systems or data within the network for malicious purposes (TA0002).

At 3:15 AM UTC, an adversary gained initial access to the 'SCRANTON.dmevals.local' endpoint by using spearphishing with a malicious attachment (TA0001 Initial Access). The file was renamed using Right-to-Left Override (RLO), which is a non-printing Unicode character that causes text following it to be displayed in reverse, making it appear benign. This technique has been used in targeted intrusions and criminal activity. Once executed, the malware created a persistence mechanism by modifying the registry to run at startup (TA0003 Persistence). The adversary then executed additional scripts using PowerShell (TA0002 Execution) and injected code into lsass.exe (TA0005 Defense Evasion), potentially for privilege escalation or lateral movement.

On May 2nd, 2020 at approximately 3:16 AM UTC, the adversary executed Sdelete64.exe on the 'DMEVALS\pbeesly' endpoint once more, this time targeting a file on the desktop named 'working.zip'. This pattern of behavior indicates a deliberate and systematic approach to data deletion, potentially in an attempt to remove evidence of their activities.

On April 30th, 2020 at 00:35:26 UTC, an adversary established command and control (TA0011) with an external system located at IP address 192.168.0.4 on the SCRANTON endpoint. Through this connection, a Windows Portable Executable (PE) file classified as python.exe was transferred to the victim endpoint, indicating TA0011 Command and Control: Ingress Tool Transfer technique.

On May 1st at 07:09:23 AM, an adversary initiated tool transfer through command

Investigation Summary

and control (TA0011) on the UTICA endpoint, transferring mimikatz, a Windows Portable Executable (PE) file used for lateral movement.

On May 1st at 07:55:26 AM, an adversary executed certutil.exe to decode and create a lock file in the user's AppData directory on the UTICA endpoint, indicating further collection activity (TA0009).

On May 2nd, 2020 at 03:16:19 UTC, an adversary executed a command using Rar.exe to archive collected data on the NASHUA endpoint (TA0009), indicating TA0009 Collection: Archive Collected Data technique.

On May 2nd at 08:09:58 AM, data exfiltration was initiated through a cloud storage service hosted on Microsoft Docs using net.exe command to establish a connection with the remote IP address 13.107.42.12 over HTTPS protocol (TA0010) on the UTICA endpoint, indicating TA0010 Exfiltration: Data Compressed technique.

At this time, there is no evidence of impact to systems or data integrity (TA0040). However, it is important to monitor for potential manipulation, interruption, or destruction of systems and data as the attack progresses.

The investigation revealed a coordinated attack targeting multiple endpoints in our network. Key events include unauthorized access attempts, lateral movement, data exfiltration, and credential harvesting activities. The following trends were observed across the affected endpoints:
 Unauthorized remote desktop protocol (RDP) connections from external IP addresses.
 Use of legitimate system tools for malicious purposes, such as PowerShell scripts and certutil.exe to obfuscate files or information.
 Creation and execution of unauthorized binaries, including python.exe, PSEXESVC.exe, m.exe, Rar.exe, and sdelete64.exe.
 Attempts to dump OS credentials using lsass.exe process injection.
Multiple Kerberos authentication ticket (TGT) and service ticket requests, indicating potential credential harvesting activities.

The root cause of the incident appears to be a combination of vulnerabilities, misconfigurations, and weak security practices. Specifically, we identified the following contributing factors:
 Lack of multi-factor authentication (MFA) for remote access to endpoints.
Unpatched software or outdated operating systems on some endpoints.
Weak password policies allowing brute force attacks or credential stuffing.
Insufficient network segmentation, enabling lateral movement between endpoints.

Investigation Summary

The incident has potentially compromised the confidentiality and integrity of sensitive data residing on affected endpoints. The unauthorized access attempts, lateral movement, and credential harvesting activities pose a significant risk to our organization's security posture. We recommend immediate action to address identified vulnerabilities and strengthen endpoint security measures.

This incident response timeline investigation has highlighted the importance of proactive cybersecurity measures and continuous monitoring for potential threats. Our organization must take swift action to mitigate the impact of this incident, addressing identified vulnerabilities and enhancing our overall security posture. We will continue to monitor the situation closely and provide updates as necessary.

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 suspicious events on the endpoint, primarily involving file modifications, process executions, network connections, and logon activities. The following key findings are noteworthy:

A user account 'pbeesly' was observed connecting to remote IP addresses 10.0.0.4 and 10.0.1.4 via the SMB protocol (TCP port 445). This activity occurred at various intervals throughout the timeline, indicating potential lateral movement or data transfer attempts.

Multiple instances of file modifications were detected in 'C:\Windows\Temp' and 'C:\Users\pbeesly\AppData\Roaming'. These files include python.exe, PSEXESVC.exe, Rar.exe, sdelete64.exe, and working.zip. The presence of these files suggests the execution of scripts or tools that may be malicious in nature.

Process executions involving python.exe, PSEXESVC.exe, Rar.exe, sdelete64.exe, cmd.exe, and powershell.exe were observed. These processes are commonly associated with scripting, remote access, compression, and deletion activities, further indicating potential malicious intent.

The timeline includes several instances of PowerShell script execution, which may be indicative of an attacker leveraging this powerful tool to perform various tasks, such as file enumeration, compression, and data exfiltration.

A PowerShell script was observed collecting files with sensitive extensions and keywords from the user's profile directory into a zip archive named 'working.zip'. This activity is consistent with data exfiltration techniques often employed by threat actors to gather and compress sensitive files for later extraction.

The timeline reveals attempts to delete files, such as Rar.exe, sdelete64.exe, and working.zip, which may indicate an attempt to cover the attacker's tracks or evade detection.

Root Cause Analysis:
The root cause of this incident can be attributed to a combination of factors:

The presence of multiple suspicious files on the endpoint suggests that the system may have been compromised through phishing, malicious downloads, or exploitation of vulnerabilities.

The use of PowerShell for potentially malicious purposes indicates a failure in security policies and controls to prevent or detect unauthorized script execution.

NASHUA.dmevals.local Summary

The lack of file integrity monitoring and deletion prevention mechanisms allowed the attacker to modify, execute, and delete files without being detected.
The absence of strong access control policies may have facilitated lateral movement by granting excessive permissions to user accounts like 'pbeesly'.

Impact Assessment:
The incident has had the following impacts on operations, data integrity, and confidentiality:
Potential Data Exfiltration: The PowerShell script's collection of sensitive files into a zip archive suggests that data exfiltration may have occurred. A thorough analysis of the extracted data is required to determine the extent and nature of any potential data loss.
System Compromise: The presence of suspicious files and process executions indicates that the endpoint may have been compromised, potentially allowing unauthorized access or control over the system.
Security Controls Bypassed: The successful execution and deletion of tools like Rar.exe, sdelete64.exe, and working.zip demonstrate a failure in security controls designed to prevent, detect, and respond to malicious activities.
Reputational Damage: If sensitive data has been exfiltrated, the organization may face reputational damage, regulatory fines, or legal action depending on the nature of the breached information.

Recommendations for Remediation and Prevention:
Implement strict access control policies to minimize lateral movement and limit user privileges.
Regularly update and patch systems to address known vulnerabilities that could be exploited by attackers.
Implement file integrity monitoring solutions to detect unauthorized modifications, deletions, or executions of critical files.
Establish robust security policies and controls to prevent the execution of unauthorized scripts or tools, such as PowerShell, cmd.exe, or python.exe.
Conduct regular security awareness training for employees to help them recognize and respond to phishing attempts or other social engineering tactics.
Implement a comprehensive backup and recovery strategy to ensure data availability in the event of a breach or ransomware attack.
Continuously monitor network traffic, endpoint activities, and system logs to detect and respond to potential threats in real-time.

Incident Narrative:
On May 2nd, 2020 at approximately 3:15 AM UTC, an adversary initiated a series of actions on a Windows endpoint associated with the user account 'DMEVALS\pbeesly'. The initial event involved the execution of Python via the

NASHUA.dmevals.local Summary

command line interface. This was followed by the spawning of PowerShell and the subsequent execution of Rar.exe to archive files in the user's AppData directory.

The adversary continued their actions at 3:16 AM UTC with the execution of cmd.exe, which then invoked Sdelete64.exe to delete archived files from both the Temp and AppData directories. The use of Sdelete64.exe suggests an attempt to evade detection by forensic analysis tools.

At 3:17 AM UTC, the adversary executed Sdelete64.exe once more, this time targeting a file on the desktop named 'working.zip'. This pattern of behavior indicates a deliberate and systematic approach to data deletion, potentially in an attempt to remove evidence of their activities.

The timeline entries suggest that the adversary employed various techniques associated with the MITRE Tactics Initial Access (TA0001), Execution (TA0002), Persistence (TA0003) and Defense Evasion (TA0005). The use of Python, PowerShell, cmd.exe, and Sdelete64.exe for execution and evasion tactics demonstrate a sophisticated level of proficiency in Windows-based systems.

The adversary's actions suggest that they may have gained initial access through spearphishing or exploiting weaknesses on public-facing web servers. They then established a foothold by executing malicious code via Python and PowerShell, achieving their objectives through the use of Rar.exe. The adversary maintained persistence by leveraging third-party software deployment tools such as Sdelete64.exe to evade detection and remove traces of their activities.

During this incident, the adversary demonstrated a pattern of lateral movement throughout the network. At 3:10 AM UTC, the user 'pbeesly' authenticated into a remote system with IP address '10.0.1.4'. This authentication was performed using Remote Services (TA0008.T1021.000) and was followed by the access of a network share object. Shortly after, at 3:11 AM UTC, software deployment tools were used to execute 'PSEXESVC.exe' with system privileges and 'python.exe' under the user 'pbeesly'. This pattern repeated several times over the next few minutes, indicating lateral movement throughout the network. At 3:15 AM UTC, a final authentication was performed by 'pbeesly' into another remote system, followed by the execution of 'PSEXESVC.exe' and 'python.exe'. This activity suggests that the user may have been attempting to gain unauthorized access to additional systems or data within the network for potential malicious purposes.

At 03:16:19 UTC, an adversary executed a command using Rar.exe to archive collected data on the endpoint (TA0009). The archive was created in the user's

NASHUA.dmevals.local Summary

AppData\Roaming directory with the name working.zip and contained files from the desktop. This technique is used for obfuscating and minimizing the amount of data sent over the network prior to exfiltration (TA0009.T1560). The use of a third-party utility, Rar.exe, suggests that this adversary may have preplanned their attack or has performed similar attacks in the past.

At this time, it is unclear if the adversary has successfully exfiltrated the data (TA0010). However, the use of an archive utility indicates a potential for data exfiltration in the near future. The adversary may also establish command and control communication with compromised systems within the victim network to facilitate exfiltration (TA0011).

Additionally, there is no evidence at this time that the adversary has caused any impact to the system or data integrity (TA0040). However, it is important to monitor for potential manipulation, interruption, or destruction of systems and data as the attack progresses.

NEWYORK.dmevals.local Summary

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

Summary of Findings:
On May 2nd, 2020 at approximately 8:03 AM UTC, an unauthorized user with the username 'dschrute' successfully logged into the DMEVALS domain via a remote IP address (10.0.1.5). This event was followed by the creation of a new executable file named 'm.exe' in the Windows System32 directory at 8:03:47 AM UTC, which was executed with debug privileges and injected into the Local Security Authority Subsystem Service (LSASS) process memory to dump credentials associated with the krbtgt account. This action is indicative of Credential Access (TA0006), specifically OS Credential Dumping (T1003). The execution of 'm.exe' was performed by a user named 'DMEVALS\mscott', suggesting that the user may have been attempting to escalate privileges or gain unauthorized access to restricted information.

The injection of 'm.exe' into LSASS process memory triggered several Library Load events, including cryptdll.dll, samlib.dll, hid.dll, and WinSCard.dll, which are commonly used by adversaries for credential dumping and lateral movement. The Open Process event targeting lsass.exe indicates that the process was opened with the intention of accessing its memory space.

The use of debug privileges allows the process to bypass security restrictions and access sensitive system resources, which could be used for further exploitation or unauthorized access. This suggests an attempt at Privilege Escalation (TA0004). The successful login from another user 'kmalone' at 8:22:24 AM UTC via the same remote IP address (10.0.1.5) indicates that lateral movement or privilege escalation has already occurred, necessitating immediate remediation efforts and a thorough review of network access controls and authentication policies.

Root Cause Analysis:
The root cause of this incident can be attributed to weak credential management practices, as evidenced by the successful dumping of credentials from the LSASS memory space. This vulnerability was further exacerbated by the presence of a remote user with access to the DMEVALS domain, which may indicate inadequate network segmentation or access control policies.

Impact Assessment:
The unauthorized credential dumping and subsequent Kerberos ticket requests

NEWYORK.dmevals.local Summary

pose a significant risk to the integrity and confidentiality of sensitive data within the DMEVALS environment. The successful login from another user via the same remote IP address suggests that lateral movement or privilege escalation has already occurred, necessitating immediate remediation efforts and a thorough review of network access controls and authentication policies.

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:
On May 1st, 2020 at approximately 7:09 AM UTC, an adversary transferred a Windows Portable Executable (PE) file onto the endpoint from an external system using Command and Control technique TA0011.T1105. The PE file was identified as mimikatz, a tool used for retrieving credentials.

On May 2nd, 2020 at approximately 7:58 AM UTC, the adversary executed PowerShell commands to download and execute a script from an external system using Command and Scripting Interpreter technique TA0002.T1059. The script was used to retrieve content from a webpage and execute it.

At approximately 7:59 AM UTC, the adversary executed a tool to dump credentials from the local operating system's memory using OS Credential Dumping technique TA0006.T1003. The tool was executed with debug privileges and targeted the Local Security Authority Subsystem Service (LSASS) process.

At approximately 8:00 AM UTC, the adversary established persistence on the endpoint by creating a Windows Management Instrumentation (WMI) Event Subscription using Event Triggered Execution technique TA0003.T1546. The subscription was designed to trigger when a specific user logged in and execute a PowerShell command.

At approximately 8:01 AM UTC, the adversary executed another PowerShell script to bypass security mechanisms using Command and Scripting Interpreter technique TA0002.T1059.

At approximately 8:07 AM UTC, the adversary again dumped credentials from the local operating system's memory using OS Credential Dumping technique TA0006.T1003. This time, the adversary injected code into the LSASS process to extract the credentials.

At approximately 8:12 AM UTC, the adversary created a file in the Windows System32 directory using File Modification technique TA0004. The file was used to store information about services running on the endpoint.

At approximately 8:14 AM UTC, the adversary executed another PowerShell script to evade defenses using Command and Scripting Interpreter technique

UTICA.dmevals.local Summary

TA0005.T1059.

At approximately 8:20 AM UTC, the adversary again dumped credentials from the local operating system's memory using OS Credential Dumping technique TA0006.T1003. This time, the adversary used a tool called mimikatz to extract the credentials in a golden ticket format.

Root Cause Analysis:
The root cause of this incident was the compromise of an endpoint by an adversary using Command and Control technique TA0011.T1105 to transfer a credential dumping tool onto the endpoint. The adversary then used various techniques, including OS Credential Dumping (TA0006.T1003), Command and Scripting Interpreter (TA0002.T1059), Persistence (TA0003.T1546), Defense Evasion (TA0005.T1059), and File Modification (TA0004) to extract credentials, establish persistence, evade defenses, and modify system files.

Impact Assessment:
The impact of this incident on operations, data integrity, and confidentiality is significant. The adversary was able to extract credentials from the local operating system's memory, potentially gaining access to sensitive information and systems within the network. Additionally, the adversary established persistence on the endpoint, allowing them to maintain access and control over the system. The modification of system files could also impact the stability and functionality of the endpoint. It is recommended that a thorough investigation be conducted to identify any additional compromised endpoints or systems and to remediate any vulnerabilities or misconfigurations that contributed to the incident.Tradecraft Summary:
 The adversary is attempting to gain initial access and establish persistence on a Windows endpoint by abusing PowerShell (TA0002.T1059.001) and other command line interfaces (TA0002.T1059). The attacker uses certutil.exe, csc.exe, and powershell.exe to decode and execute a base64 encoded script from an external source. This technique is used multiple times in quick succession, indicating the adversary's persistence (TA0003) in attempting to gain access. The attacker also uses conhost.exe to hide their malicious PowerShell commands.

The adversary attempts to evade defenses by obfuscating files and information with certutil.exe (TA0005.T1027). They also use rundll32.exe to load a DLL from the user's AppData directory, which may be an attempt to execute malicious code.

The adversary establishes persistence by creating a WMI Event Subscription (TA0003.T1546.003) that triggers a PowerShell command upon user login. This technique allows the attacker to maintain access even if the initial foothold is lost, increasing their chances of success in achieving their objectives.

UTICA.dmevals.local Summary

The adversary's use of common system tools and techniques suggests they may be attempting an opportunistic intrusion rather than a targeted one. However, the persistence and evasion tactics used indicate a sophisticated level of knowledge and skill, which could also suggest a more advanced threat actor. Further analysis is required to determine the true intent and capabilities of the adversary.Access Summary:
On 05/02/2020 at 07:59:10 UTC, a user with the account name 'DMEVALS\dschrute' executed a command using Mimikatz to dump credentials from LSASS memory on the target host. This action was taken in an attempt to access credential material stored in the process memory of the Local Security Authority Subsystem Service (LSASS). The attacker may have used this information to perform lateral movement and access restricted information.

At 08:07:56 UTC, a PowerShell script was executed that dumped credentials from LSASS memory using Mimikatz. This action was taken in an attempt to steal account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software.

At 08:12:26 UTC, the attacker executed a command that dumped credentials from LSASS memory using Mimikatz. This action was taken in an attempt to steal account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software.

At 08:20:07 UTC, a PowerShell script was executed that dumped credentials from LSASS memory using Mimikatz. This action was taken in an attempt to steal account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software.

At 08:21:59 UTC, a PowerShell script was executed that dumped credentials from LSASS memory using Mimikatz. This action was taken in an attempt to steal account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software.

The attacker used Mimikatz to dump credentials from LSASS memory multiple times during this timeline. The attacker may have used these credentials to perform lateral movement and access restricted information on the target host.Mobility Summary:
A few paragraphs is sufficient.

The timeline data shows a series of events related to Remote Execution and Lateral Movement tactics in the MITRE ATT&CK framework. The first set of events at 07:55:27 UTC involves the execution of a PowerShell command that reads content from a local file and pipes it into IEX, which is an alias for

UTICA.dmevals.local Summary

Invoke-Expression. This technique is consistent with TA0002 Execution as it indicates an attempt to run malicious code on a local system. The remote IP address 192.168.0.4 is involved in this command, indicating potential remote services being used for execution.

Following the initial execution event, there are multiple network connection events at 07:58:04 and 07:59:09 UTC to the same remote IP address 192.168.0.4 over port 443. These connections suggest that the system is attempting to establish a secure communication channel with the remote host, possibly for further malicious activities such as data exfiltration or command and control.

At 07:59:09 UTC, there is an event related to TA0008 Lateral Movement: Windows Management Instrumentation (WMI). This technique involves using WMI to execute a PowerShell command that downloads a file from the remote IP address 192.168.0.4 and saves it as "m.exe" on the local system. The command then executes the new binary with specific arguments, indicating an attempt to extract password hashes from memory using Mimikatz or a similar tool. This technique is consistent with TA0008 Lateral Movement as it involves moving laterally within the network by exploiting remote services and gaining unauthorized access to other systems.

At 07:59:10 UTC, there is another set of network connection events to the same remote IP address 192.168.0.4 over port 8080. This connection suggests that the system is attempting to download additional malicious tools or payloads from the remote host for further activities.

At 08:02:44 UTC, there are multiple network connection events related to TA0008 Lateral Movement: Windows Remote Management (WinRM). These connections involve communication with a remote system over WinRM on port 5985, which is the default HTTP port for this protocol. The use of WinRM suggests that the adversary may be attempting to move laterally within the network by using valid accounts and executing commands on remote systems.

At 08:17:58 UTC, there is an event related to TA0008 Lateral Movement: Remote Desktop Protocol (RDP). This technique involves logging into a remote system using RDP, which allows for interactive access to the remote desktop. The use of RDP suggests that the adversary may be attempting to move laterally within the network by accessing other systems and potentially escalating privileges or establishing persistence on those systems.

In summary, the timeline data shows a series of events related to Remote Execution and Lateral Movement tactics in the MITRE ATT&CK framework. The adversary appears to be using various techniques such as PowerShell execution, WMI, WinRM, and RDP to move laterally within the network and execute malicious

UTICA.dmevals.local Summary

code on remote systems. These activities suggest a potential compromise of the network and may indicate an attempt to exfiltrate data or establish long-term persistence for future attacks.Data Movement Summary:

On May 1st at 07:09:23 AM, a tool transfer was initiated by an adversary through command and control (TA0011). The transferred file was identified as mimikatz, a Windows Portable Executable (PE) file used for lateral movement. On the following day, May 2nd at 07:55:26 AM, the adversary executed certutil.exe to decode and create a lock file in the user's AppData directory. This action is indicative of further collection activity (TA0009). At 08:09:58 AM, data exfiltration was initiated through a cloud storage service hosted on Microsoft Docs, using the net.exe command to establish a connection with the remote IP address 13.107.42.12 over HTTPS protocol (TA0010). This event suggests that the adversary has successfully collected and exfiltrated data from the compromised system, potentially staging it for further use or impact (TA0040).

SCRANTON.dmevals.local Summary

Endpoint Name: SCRANTON.dmevals.local
Operating System: Windows
First Event Timestamp: 08/25/2011 18:27:29
Last Event Timestamp: 05/02/2020 08:29:16
Observed IP Addresses: 10.0.1.4
Observed Users: DMEVALS\pbeesly, pbeesly, DMEVALS\mscott, DMEVALS\kmalone, kmalone

Summary of Findings:
On April 30th at approximately 12:35 AM UTC, an adversary initiated command and control (C2) communication with the victim network to transfer a tool or other file from an external system into the compromised environment. The transferred file was identified as python.exe and originated from IP address 192.168.0.4.

On May 2nd at approximately 3:55 AM UTC, the adversary executed a malicious script disguised as cod.3aka3.scr, which was initially stopped by endpoint detection and response (EDR) software. The same day at around 4:57 AM UTC, the adversary established persistence on the victim system through modifying registry keys to execute a PowerShell command upon user logon.

At approximately 5:00 AM UTC, the adversary executed a payload from monkey.png, which was previously downloaded onto the victim system. The payload created an executable file named hostui.lnk in the Start Menu's startup folder to maintain persistence across reboots.

Root Cause Analysis:
The root cause of this incident can be attributed to a successful phishing attempt or another form of social engineering, which led to the initial compromise and subsequent malware execution on the victim system. The adversary exploited a misconfiguration in the endpoint's security settings, allowing them to execute the python.exe downloader without raising any alarms.

Impact Assessment:
The incident has had a moderate impact on operations, as the adversary was able to establish persistence and execute malicious payloads on the victim system. The data integrity of files and information stored on the affected system may be at risk due to the adversary's actions. Furthermore, the adversary's access to the network poses a significant threat to other systems within the environment. Immediate action should be taken to isolate the compromised system and remediate any vulnerabilities or misconfigurations that facilitated the attack.

Incident Narrative:
On April 30th at approximately 12:35 AM UTC, an adversary initiated command and

SCRANTON.dmevals.local Summary

control (C2) communication with the victim network to transfer a tool or other file from an external system into the compromised environment. The transferred file was identified as python.exe and originated from IP address 192.168.0.4. This action is indicative of TA0011 Command and Control: Ingress Tool Transfer technique, where adversaries transfer tools or other files from an external system into a compromised environment to further exploit the victim endpoint.

On May 2nd at approximately 3:55 AM UTC, the adversary executed a malicious script disguised as cod.3aka3.scr, which was initially stopped by endpoint detection and response (EDR) software. However, the adversary persisted in their attempts to execute the payload and succeeded at around 4:57 AM UTC by modifying registry keys to execute a PowerShell command upon user logon. This activity is consistent with TA0003 Persistence technique, where adversaries create mechanisms to maintain their foothold on compromised systems.

At approximately 5:00 AM UTC, the adversary executed a payload from monkey.png, which was previously downloaded onto the victim system. The payload created an executable file named hostui.lnk in the Start Menu's startup folder to maintain persistence across reboots. This activity is indicative of TA0004 Defense Evasion technique, where adversaries use living-off-the-land binaries or legitimate tools to evade detection and hinder analysis.

The adversary then proceeded to move laterally through the network using a combination of WinRM, PsExec, and RDP. At approximately 03:08 UTC, a host with IP address 10.0.1.4 began making connections to remote hosts over TCP port 80 and 389. The first connection was made to an internal host with IP address 192.168.0.5, followed by connections to two domain controllers at 10.0.0.4. After establishing these connections, the host initiated a connection to another internal host with IP address 10.0.1.6 over TCP port 5985, which is commonly used for Windows Remote Management (WinRM). This activity suggests that an adversary may be attempting to use WinRM as a method of lateral movement within the network.

At approximately 03:09 UTC, the host with IP address 10.0.1.4 made additional connections to the internal host at 10.0.1.6 over TCP port 5985. This activity is consistent with an adversary attempting to use WinRM for lateral movement within the network.

At approximately 03:11 UTC, a process named PsExec64.exe was executed on the host with IP address 10.0.1.4 with the command line argument "-accepteula \\NASHUA -u dmevals\pbeesly -p Fl0nk3rt0n!T0by -i 2 C:\Windows\Temp\python.exe". This activity suggests that an adversary may be attempting to use PsExec, a legitimate software deployment tool, for lateral movement within the network.

SCRANTON.dmevals.local Summary

At approximately 03:12 UTC, another instance of PsExec64.exe was executed on the host with IP address 10.0.1.4 with the same command line argument as before. This activity is consistent with an adversary attempting to use PsExec for lateral movement within the network.

At approximately 03:13 UTC, yet another instance of PsExec64.exe was executed on the host with IP address 10.0.1.4 with the same command line argument as before. This activity is consistent with an adversary attempting to use PsExec for lateral movement within the network.

At approximately 03:14 UTC, another instance of PsExec64.exe was executed on the host with IP address 10.0.1.4 with the same command line argument as before. This activity is consistent with an adversary attempting to use PsExec for lateral movement within the network.

At approximately 03:20 UTC, a user named pbeesly logged into a remote host with IP address 172.18.39.2 using Remote Desktop Protocol (RDP). This activity suggests that an adversary may be attempting to use RDP for lateral movement within the network.

In summary, between approximately 03:08 and 03:20 UTC on May 2nd, 2020, an adversary used a combination of WinRM, PsExec, and RDP to move laterally through the network and execute code on remote hosts. This activity is consistent with tactics, techniques, and procedures (TTPs) associated with Remote Execution (TA0002) and Lateral Movement (TA0008).

On May 2nd at approximately 3:55 AM UTC, the adversary executed a malicious script disguised as cod.3aka3.scr, which was initially stopped by endpoint detection and response (EDR) software. The same day at around 4:57 AM UTC, the adversary established persistence on the victim system through modifying registry keys to execute a PowerShell command upon user logon.

At approximately 5:00 AM UTC, the adversary executed a payload from monkey.png, which was previously downloaded onto the victim system. The payload created an executable file named hostui.lnk in the Start Menu's startup folder to maintain persistence across reboots. This activity is indicative of TA0004 Defense Evasion technique, where adversaries use living-off-the-land binaries or legitimate tools to evade detection and hinder analysis.

On April 30th at approximately 12:35 AM UTC, an adversary initiated command and control (C2) communication with the victim network to transfer a tool or other file from an external system into the compromised environment. The transferred file was identified as python.exe and originated from IP address 192.168.0.4.

SCRANTON.dmevals.local Summary

This action is indicative of TA0011 Command and Control: Ingress Tool Transfer technique, where adversaries transfer tools or other files from an external system into a compromised environment to further exploit the victim endpoint.

The adversary then proceeded to move laterally through the network using a combination of WinRM, PsExec, and RDP. At approximately 03:08 UTC, a host with IP address 10.0.1.4 began making connections to remote hosts over TCP port 80 and 389. The first connection was made to an internal host with IP address 192.168.0.5, followed by connections to two domain controllers at 10.0.0.4. After establishing these connections, the host initiated a connection to another internal host with IP address 10.0.1.6 over TCP port 5985, which is commonly used for Windows Remote Management (WinRM). This activity suggests that an adversary may be attempting to use WinRM as a method of lateral movement within the network.

At approximately 03:09 UTC, the host with IP address 10.0.1.4 made additional connections to the internal host at 10.0.1.6 over TCP port 5985. This activity is consistent with an adversary attempting to use WinRM for lateral movement within the network.

At approximately 03:11 UTC, a process named PsExec64.exe was executed on the host with IP address 10.0.1.4 with the command line argument "-accepteula \\NASHUA -u dmevals\pbeesly -p Fl0nk3rt0n!T0by -i 2 C:\Windows\Temp\python.exe". This activity suggests that an adversary may be attempting to use PsExec, a legitimate software deployment tool, for lateral movement within the network.

At approximately 03:12 UTC, another instance of PsExec64.exe was executed on the host with IP address 10.0.1.4 with the same command line argument as before. This activity is consistent with an adversary attempting to use PsExec for lateral movement within the network.

At approximately 03:13 UTC, yet another instance of PsExec64.exe was executed on the host with IP address 10.0.1.4 with the same command line argument as before. This activity is consistent with an adversary attempting to use PsExec for lateral movement within the network.

At approximately 03:14 UTC, another instance of PsExec64.exe was executed on the host with IP address 10.0.1.4 with the same command line argument as before. This activity is consistent with an adversary attempting to use PsExec for lateral movement within the network.

At approximately 03:20 UTC, a user named pbeesly logged into a remote host with IP address 172.18.39.2 using Remote Desktop Protocol (RDP). This activity

SCRANTON.dmevals.local Summary

suggests that an adversary may be attempting to use RDP for lateral movement within the network.

In summary, between approximately 03:08 and 03:20 UTC on May 2nd, 2020, an adversary used a combination of WinRM, PsExec, and RDP to move laterally through the network and execute code on remote hosts. This activity is consistent with tactics, techniques, and procedures (TTPs) associated with Remote Execution (TA0002) and Lateral Movement (TA0008).

On May 2nd at approximately 3:55 AM UTC, the adversary executed a malicious script disguised as cod.3aka3.scr, which was initially stopped by endpoint detection and response (EDR) software. The same day at around 4:57 AM UTC, the adversary established persistence on the victim system through modifying registry keys to execute a PowerShell command upon user logon.

At approximately 5:00 AM UTC, the adversary executed a payload from monkey.png, which was previously downloaded onto the victim system. The payload created an executable file named hostui.lnk in the Start Menu's startup folder to maintain persistence across reboots. This activity is indicative of TA0004 Defense Evasion technique, where adversaries use living-off-the-land binaries or legitimate tools to evade detection and hinder analysis.

On April 30th at approximately 12:35 AM UTC, an adversary initiated command and control (C2) communication with the victim network to transfer a tool or other file from an external system into the compromised environment. The transferred file was identified as python.exe and originated from IP address 192.168.0.4. This action is indicative of TA0011 Command and Control: Ingress Tool Transfer technique, where adversaries transfer tools or other files from an external system into a compromised environment to further exploit the victim endpoint.

The root cause of this incident can be attributed to a successful phishing attempt or another form of social engineering, which led to the initial compromise and subsequent malware execution on the victim system. The adversary exploited a misconfiguration in the endpoint's security settings, allowing them to execute the python.exe downloader without raising any alarms.

Impact Assessment:
The incident has had a moderate impact on operations, as the adversary was able to establish persistence and execute malicious payloads on the victim system. The data integrity of files and information stored on the affected system may be at risk due to the adversary's actions. Furthermore, the adversary's access to the network poses a significant threat to other systems within the environment. Immediate action should be taken to isolate the compromised system and remediate any vulnerabilities or misconfigurations that facilitated the

SCRANTON.dmevals.local Summary

attack.

In conclusion, this incident involved an adversary using various techniques such as C2 communication, lateral movement, persistence, and defense evasion to compromise a victim endpoint and move laterally through the network. The root cause of the incident can be attributed to a successful phishing attempt or another form of social engineering, which led to the initial compromise and subsequent malware execution on the victim system. The impact of the incident has been moderate, with the adversary able to establish persistence and execute malicious payloads on the victim system. Immediate action should be taken to isolate the compromised system and remediate any vulnerabilities or misconfigurations that facilitated the attack.