**A blue planet in space

Description automatically generated**A logo with a triangle and a blue triangle

Description automatically generatedA cartoon of an astronaut holding a computer

Description automatically generated

A black background with white text

Description automatically generatedA black background with white text

Description automatically generated

**RED TEAM ASSESSEMENT REPORT**

|  |
| --- |
| **ACME Corp. Purple Team 2024** |

REDTEAM001

Wednesday, May 7, 2025

TABLE OF CONTENTS

[**EXECUTIVE SUMMARY** 3](#_Toc197518384)

[OVERVIEW 3](#_Toc197518385)

[OBJECTIVES 3](#_Toc197518386)

[POSITIVE SECURITY OBSERVATIONS 4](#_Toc197518387)

[SUMMARY OF RECOMMENDATIONS 4](#_Toc197518388)

[TESTING PROGRESS 4](#_Toc197518389)

[UNIQUE VULNERABILITIES 4](#_Toc197518390)

[REMEDIATION PROGRESS 5](#_Toc197518391)

[**TESTING SUMMARY** 6](#_Toc197518392)

[SCENARIOS TESTED 6](#_Toc197518393)

[APPROACH & OUTCOMES 6](#_Toc197518394)

[HIGH VALUE TARGET(s) 6](#_Toc197518395)

[OUT OF SCOPE 6](#_Toc197518396)

[ASSUMPTIONS AND CONSTRAINTS 7](#_Toc197518397)

[**ATTACKCHAINS** 11](#_Toc197518398)

[1. Full compromise of Office 365 Administration Portal 11](#_Toc197518399)

[**DETAILED FINDINGS** 13](#_Toc197518400)

[1. [3.0.0] LLMNR/NBT-NS Poisoning and SMB Relay 13](#_Toc197518401)

[2. [3.1.0] Account Discovery 25](#_Toc197518402)

[3. [3.2.0] Adversary-in-the-Middle 31](#_Toc197518403)

[4. [3.2.0] Account Manipulation 36](#_Toc197518404)

[5. [3.1.0] Brute Force 44](#_Toc197518405)

[6. [3.1.0] Bypass User Account Control 47](#_Toc197518406)

[7. [3.2.0] Cached Domain Credentials 54](#_Toc197518407)

[8. [2.1.0] ARP Cache Poisoning 58](#_Toc197518408)

[9. [2.1.0] Automated Collection 62](#_Toc197518409)

[10. [2.1.0] Automated Exfiltration 68](#_Toc197518410)

[**VULNERABILITIES** 71](#_Toc197518411)

[1. Hosts Respond with Hashes/Challenge-Responses to Spoofed Hostnames 71](#_Toc197518412)

# **EXECUTIVE SUMMARY**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| OVERVIEW | | | | | |
| The AttackForge OffSec Team (OffSec) performed a Red Team engagement on Wayne Enterprises between Monday 5th of May to Friday 23rd of May, 2025.  The engagement performed by OffSec employed real-world adversary techniques to target the systems under test. The sequence of activities in this approach involved open source intelligence (OSINT) collection, enumeration, exploitation, and attacks aligned with the MITRE ATT&CK Framework in order to perform goal-specific operational impacts. The goals and outcomes are detailed in the section Objectives within this report.  The purpose this assessment is to validate Wayne Enterprise’s existing resilience to said objectives, and to provide detailed information on any identified gaps which could be used to further train the cyber security operations team (Blue Team).  There were a number of positive security observations identified during the course of this assessment. Those are detailed within the section Positive Security Observations.  There was also a number of gaps identified and OffSec has provided specific recommendations for reducing the risks imposed by these issues. Those are detailed within the section Summary of Recommendations.  OffSec appreciates the opportunity to support Wayne Enterprises with its cyber security. We look forward to assisting you and the Wayne Enterprises IT Staff in future endeavours. | | | | | |
| OBJECTIVES | | | | | |
| **OBJECTIVE** | | | **TYPE** | **OUTCOME** | |
| Breach Wayne Enterprises internet-facing perimeter to gain persistent foothold on Wayne Enterprise corporate domain. | | | Primary | Failed | |
| Breach Wayne Enterprises physical security controls at Gotham City headquarters to gain persistent foothold on Wayne Enterprises corporate domain. | | | Primary | Successful | |
| Gain access to Wayne Enterprises secure engineering domain. | | | Primary | Successful | |
| Exfiltrate secret bat mobile schematics. | | | Primary | Successful | |
| Gain access to Finance and People portal to increase the annual salary and bonuses for the employee "Alfred Thaddeus Crane Pennyworth" | | | Secondary | Failed | |
| POSITIVE SECURITY OBSERVATIONS | | | | | |
| The following positive security observations were observed during this assessment:   * Limited internet-facing perimeter. Only a handful of exposed internet-facing services. * Strong security controls enforced on the external network perimeter. Only a few vulnerabilities were found within external Wayne Enterprise services. * Limited number of domain admin user accounts enabled. | | | | | |
| SUMMARY OF RECOMMENDATIONS | | | | | |
| The following recommendations are made to Wayne Enterprises as a result of this assessment:  **Recommendation 1: Strengthened Access Controls.**  Implement stricter access control policies, including biometric authentication, multi-factor authentication, and enhanced surveillance systems.  **Recommendation 2: Improved Data Handling**.  Develop and enforce data security protocols, including proper disposal of sensitive information and secure storage practices.  **Recommendation 3: Enhanced Security Awareness Training**.  Provide regular, targeted security awareness training to employees, focusing on phishing, social engineering, and other common threats.  **Recommendation 4:Refined Incident Response Plan**.  Conduct regular incident response drills and simulations to assess the effectiveness of incident response capabilities and make necessary adjustments. | | | | | |
| TESTING PROGRESS | | | | | |
| Start | **Jan 07 2024** | **Passed** MITRE ATT&CK Techniques | | | **9** |
| End | **Jan 26 2024** | **Failed** MITRE ATT&CK Techniques | | | **1** |
| Completed | **100%** | **Total** MITRE ATT&CK Techniques | | | **10** |
| UNIQUE VULNERABILITIES | | | | | |
| Total | **1** | image | | | |
| Critical | **0** |
| High | **1** |
| Medium | **0** |
| Low | **0** |
| Info | **0** |
| REMEDIATION PROGRESS | | | | | |
| Open | **1** | image | | | |
| Retest | **0** |
| Closed | **0** |

# **TESTING SUMMARY**

|  |  |  |
| --- | --- | --- |
| SCENARIOS TESTED | | |
| The following scenarios were assessed:   * Attacker discovers internet-facing services for Wayne Enterprises and attempts to compromise those services. * Attacker attempts to breach physical security of Building A, Floor 9 of Wayne Enterprises headquarters located in downtown Gotham City and plug into the corporate network. * Attacker launches a targeted phishing attack against selected high-value Wayne Enterprises IT Staff. * Attacker has gained access to an employee laptop with an active VPN service. | | |
| APPROACH & OUTCOMES | | |
| **TACTIC** | **ATTEMPTED TECHNIQUES** | **SUCCESSFUL** |
| Discovery | **1** | **0** |
| Persistence | **1** | **0** |
| Privilege Escalation | **2** | **0** |
| Credential Access | **5** | **1** |
| Collection | **4** | **1** |
| Exfiltration | **1** | **0** |
| Defense Evasion | **1** | **0** |
| HIGH VALUE TARGET(s) | | |
| 1. 10.0.0.1/24 2. IT System Analyst 3. Wayne Headquarters 4. bat-api.attackforge.com 5. bat-portal.attackforge.com | | |
| OUT OF SCOPE | | |
| The following items were agreed to be out-of-scope for this assessment:   * Destructive physical and attacks that would cause operational impact to Wayne Enterprises. * Removing items from physical locations, such as laptops and files. * Changing employee data in Finance and People portal. | | |
| ASSUMPTIONS AND CONSTRAINTS | | |
| The following assumptions have been taken into consideration:   1. External internet-facing systems identified to be owned by Wayne Enterprises are in-scope for testing. 2. Any personnel identifiable as a Wayne Enterprises employee is in-scope for potential phishing attacks. 3. All floors located in the Wayne Enterprises headquarters building in downtown Gotham City are in-scope. 4. Bat mobile schematics are available to authorised users from within the Wayne Enterprises secure engineering network. | | |

**ATTACKS**

|  |  |  |  |
| --- | --- | --- | --- |
| **TECHNIQUE** | **SUCCESSFUL** | **VULNS FOUND** | |
| **Account Discovery** | A blue x in a circle  AI-generated content may be incorrect. | TOTAL | 0 |
| CRITICAL | 0 |
| HIGH | 0 |
| MEDIUM | 0 |
| LOW | 0 |
| INFO | 0 |
| **Account Manipulation** | A blue x in a circle  AI-generated content may be incorrect. | TOTAL | 0 |
| CRITICAL | 0 |
| HIGH | 0 |
| MEDIUM | 0 |
| LOW | 0 |
| INFO | 0 |
| **ARP Cache Poisoning** | A blue x in a circle  AI-generated content may be incorrect. | TOTAL | 0 |
| CRITICAL | 0 |
| HIGH | 0 |
| MEDIUM | 0 |
| LOW | 0 |
| INFO | 0 |
| **Automated Collection** | A blue x in a circle  AI-generated content may be incorrect. | TOTAL | 0 |
| CRITICAL | 0 |
| HIGH | 0 |
| MEDIUM | 0 |
| LOW | 0 |
| INFO | 0 |
| **Automated Exfiltration** | A blue x in a circle  AI-generated content may be incorrect. | TOTAL | 0 |
| CRITICAL | 0 |
| HIGH | 0 |
| MEDIUM | 0 |
| LOW | 0 |
| INFO | 0 |
| **Brute Force** | A blue x in a circle  AI-generated content may be incorrect. | TOTAL | 0 |
| CRITICAL | 0 |
| HIGH | 0 |
| MEDIUM | 0 |
| LOW | 0 |
| INFO | 0 |
| **Bypass User Account Control** | A blue x in a circle  AI-generated content may be incorrect. | TOTAL | 0 |
| CRITICAL | 0 |
| HIGH | 0 |
| MEDIUM | 0 |
| LOW | 0 |
| INFO | 0 |
| **Cached Domain Credentials** | A blue x in a circle  AI-generated content may be incorrect. | TOTAL | 0 |
| CRITICAL | 0 |
| HIGH | 0 |
| MEDIUM | 0 |
| LOW | 0 |
| INFO | 0 |
| **LLMNR/NBT-NS Poisoning and SMB Relay** | A blue check mark in a circle  AI-generated content may be incorrect. | TOTAL | 1 |
| CRITICAL | 0 |
| HIGH | 1 |
| MEDIUM | 0 |
| LOW | 0 |
| INFO | 0 |
| **Adversary-in-the-Middle** | A blue x in a circle  AI-generated content may be incorrect. | TOTAL | 0 |
| CRITICAL | 0 |
| HIGH | 0 |
| MEDIUM | 0 |
| LOW | 0 |
| INFO | 0 |

**FINDINGS**

|  |  |  |  |
| --- | --- | --- | --- |
| **PRIORITY** | **VULNERABILITY** | **RELATED TECHNIQUES** | **REMEDIATION STATUS** |
| **HIGH** | **Hosts Respond with Hashes/Challenge-Responses to Spoofed Hostnames** | * LLMNR/NBT-NS Poisoning and SMB Relay | A blue x in a circle  AI-generated content may be incorrect. |

# **ATTACKCHAINS**

1. ***Full compromise of Office 365 Administration Portal***

## Full compromise of Office 365 Administration Portal

|  |
| --- |
| A cartoon of a person with a computer  AI-generated content may be incorrect. |
| **Internal Attacker**  Attacker who has gained access to an internal network host via a phishing, social engineering or malware attack; via compromised Internet-facing host; or by breaching physical security controls at any Wayne Enterprises site with connectivity to internal network. |
| A white arrow in a red circle  AI-generated content may be incorrect. |
| A computer screen with a red and black siren  AI-generated content may be incorrect. |
| **Action**  Collect information from internal network. |
| A white arrow in a red circle  AI-generated content may be incorrect. |
| A computer with a skull and crossbones on it  AI-generated content may be incorrect. |
| **Exploit High Vulnerability**  Exploiting LLMNR and NBT-NS poisoning, retrieve credential challenge/responses from the network. |
| A white arrow in a red circle  AI-generated content may be incorrect. |
| A computer screen with a red and black siren  AI-generated content may be incorrect. |
| **Action**  Subject challenge/responses to offline password cracking attack to recover valid credentials. |
| A white arrow in a red circle  AI-generated content may be incorrect. |
| A computer servers with crowns  AI-generated content may be incorrect. |
| **Target Server**  Search for systems that utilise the same credentials. Gain access to critical systems (such as Office 365 Admin Portal) that only require usernames/passwords to log in. |
| A white arrow in a red circle  AI-generated content may be incorrect. |
| A hand holding a flag  AI-generated content may be incorrect. |
| **Captured Flag**  Full compromise of Office 365 administration portal. Exfiltrate all sensitive data. |
|  |

# **DETAILED FINDINGS**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **TECHNIQUE** | | | | | | | | | |
| [3.0.0] LLMNR/NBT-NS Poisoning and SMB Relay | | | | | | | | | |
| **DETAILS** | | | | | | | | | |
| By responding to LLMNR/NBT-NS network traffic, adversaries may spoof an authoritative source for name resolution to force communication with an adversary controlled system. This activity may be used to collect or relay authentication materials.  Link-Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBT-NS) are Microsoft Windows components that serve as alternate methods of host identification. LLMNR is based upon the Domain Name System (DNS) format and allows hosts on the same local link to perform name resolution for other hosts. NBT-NS identifies systems on a local network by their NetBIOS name.  Adversaries can spoof an authoritative source for name resolution on a victim network by responding to LLMNR (UDP 5355)/NBT-NS (UDP 137) traffic as if they know the identity of the requested host, effectively poisoning the service so that the victims will communicate with the adversary controlled system. If the requested host belongs to a resource that requires identification/authentication, the username and NTLMv2 hash will then be sent to the adversary controlled system. The adversary can then collect the hash information sent over the wire through tools that monitor the ports for traffic or through [Network Sniffing](https://attack.mitre.org/techniques/T1040) and crack the hashes offline through [Brute Force](https://attack.mitre.org/techniques/T1110) to obtain the plaintext passwords.  In some cases where an adversary has access to a system that is in the authentication path between systems or when automated scans that use credentials attempt to authenticate to an adversary controlled system, the NTLMv1/v2 hashes can be intercepted and relayed to access and execute code against a target system. The relay step can happen in conjunction with poisoning but may also be independent of it. Additionally, adversaries may encapsulate the NTLMv1/v2 hashes into various protocols, such as LDAP, SMB, MSSQL and HTTP, to expand and use multiple services with the valid NTLM response.  Several tools may be used to poison name services within local networks such as NBNSpoof, Metasploit, and [Responder](https://attack.mitre.org/software/S0174).  image Figure 1 | | | | | | | | | |
| **OUTCOME** | | | **Successful** | | | | | | |
| **ATTACK SOURCE** | | | 192.168.0.1, 192.168.0.2 | | | | | | |
| **CRITICAL STEPS** | | | | | | | | | |
| **STEP** | **DETAILS** | | | | | | | | |
| 1 | Suspendisse mollis eros erat, sit amet vestibulum sapien imperdiet nec. Cras mi tellus, malesuada viverra felis eu, vulputate elementum mauris. Pellentesque ut diam quis velit molestie cursus eu et risus. Fusce pellentesque arcu ac finibus egestas. Nunc sem lorem, malesuada vel libero sed, hendrerit faucibus nibh. Suspendisse potenti. Etiam pulvinar erat tincidunt, faucibus elit eget, tincidunt dui. Nulla facilisi. Sed semper lorem nec ligula vehicula laoreet. Nulla mollis bibendum purus, id elementum lectus mattis id. Nunc leo est, semper id rhoncus ac, porta sed lacus. | | | | | | | | |
| 2 | Aliquam pretium, purus sit amet pretium ornare, odio leo gravida enim, nec pretium risus nulla eu lacus. Vivamus non eros luctus, elementum ligula vel, faucibus lacus. Fusce auctor rhoncus ornare. Praesent suscipit, mi in semper cursus, neque turpis vulputate sapien, non auctor lectus massa et tortor. Integer non accumsan dui. Maecenas dui diam, posuere sit amet viverra eget, aliquam sed justo. Duis turpis nisi, elementum sit amet arcu at, fringilla iaculis dolor. Donec sed consectetur lorem. | | | | | | | | |
| **EXECUTION START** | | | Mon Mar 18 2024 09:15:00 | | | | | | |
| **EXECUTION END** | | | Mon Mar 18 2024 09:20:00 | | | | | | |
| **EXECUTION NOTES** | | | | | | | | | |
| Run the tool Responder on an active broadcast domain:  image Figure 2  User attempts to search for a share that doesn't exist:  image Figure 3  View the LLMNR request in Responder:  image Figure 4  Get the user’s hashed credentials:  image Figure 5  Crack the hash using a tool such as Hashcat:  image Figure 6 | | | | | | | | | |
| **TESTER NOTES** | | | | | | | | | |
| During testing, it was discovered that hosts within the internal network utilised either LLMNR, NBT-NS or both to discover hosts on the network that aren't listed by the DNS server. This allowed the Red Team to capture valid password hashes/challenge-responses and usernames that could be reused to connect to hosts or was later subjected a password cracking attack.  image Figure 7 | | | | | | | | | |
| **MITRE ATT&CK REFERENCES** | | | | | | | | | |
| **Domain** | | | | Enterprise | | | | | |
| **Tactics** | | | | Credential Access, Collection | | | | | |
| **Spec. Version** | | | | 3.0.0 | | | | | |
| **Kill Chain Phases** | | | | **Kill Chain Name** | | **Phase Name** | | | |
| 1. mitre-attack | | Credential Access | | | |
| 1. mitre-attack | | Collection | | | |
| **Platforms** | | | | Windows | | | | | |
| **Data Sources** | | | | * Service: Service Creation * Network Traffic: Network Traffic Flow * Network Traffic: Network Traffic Content * Windows Registry: Windows Registry Key Modification | | | | | |
| **Detections** | | | | **Data Source** | | **Data Component** | | **Detects** | |
| 1. General | | General | | Monitor HKLM\Software\Policies\Microsoft\Windows NT\DNSClient for changes to the "EnableMulticast" DWORD value. A value of “0” indicates LLMNR is disabled. (Citation: Sternsecurity LLMNR-NBTNS)  Monitor for traffic on ports UDP 5355 and UDP 137 if LLMNR/NetBIOS is disabled by security policy.  Deploy an LLMNR/NBT-NS spoofing detection tool.(Citation: GitHub Conveigh) Monitoring of Windows event logs for event IDs 4697 and 7045 may help in detecting successful relay techniques.(Citation: Secure Ideas SMB Relay) | |
| 1. Service | | Service Creation | | Monitor for newly constructed services/daemons through Windows event logs for event IDs 4697 and 7045. (Citation: Secure Ideas SMB Relay) Deploy an LLMNR/NBT-NS spoofing detection tool.(Citation: GitHub Conveigh) | |
| 1. Network Traffic | | Network Traffic Flow | | Monitor for network traffic originating from unknown/unexpected hardware devices. Local network traffic metadata (such as source MAC addressing) as well as usage of network management protocols such as DHCP may be helpful in identifying hardware. | |
| 1. Network Traffic | | Network Traffic Content | | Monitor for traffic on ports UDP 5355 and UDP 137 if LLMNR/NetBIOS is disabled by security policy. | |
| 1. Windows Registry | | Windows Registry Key Modification | | Monitor HKLM\Software\Policies\Microsoft\Windows NT\DNSClient for changes to the "EnableMulticast" DWORD value. A value of "0" indicates LLMNR is disabled. | |
| **Mitigations** | | | | **Mitigation** | | **Description** | | | |
| Disable or Remove Feature or Program | | Disable LLMNR and NetBIOS in local computer security settings or by group policy if they are not needed within an environment. (Citation: ADSecurity Windows Secure Baseline) | | | |
| Network Intrusion Prevention | | Network intrusion detection and prevention systems that can identify traffic patterns indicative of AiTM activity can be used to mitigate activity at the network level. | | | |
| Network Segmentation | | Network segmentation can be used to isolate infrastructure components that do not require broad network access. This may mitigate, or at least alleviate, the scope of AiTM activity. | | | |
| Filter Network Traffic | | Use host-based security software to block LLMNR/NetBIOS traffic. Enabling SMB Signing can stop NTLMv2 relay attacks.(Citation: byt3bl33d3r NTLM Relaying)(Citation: Secure Ideas SMB Relay)(Citation: Microsoft SMB Packet Signing) | | | |
| **External References** | | | | **Name** | **Id** | | **Description** | | **URL** |
| mitre-attack | T1557.001 | |  | | https://attack.mitre.org/techniques/T1557/001 |
| Rapid7 LLMNR Spoofer |  | | Francois, R. (n.d.). LLMNR Spoofer. Retrieved November 17, 2017. | | https://www.rapid7.com/db/modules/auxiliary/spoof/llmnr/llmnr\_response |
| GitHub Responder |  | | Gaffie, L. (2016, August 25). Responder. Retrieved November 17, 2017. | | https://github.com/SpiderLabs/Responder |
| Secure Ideas SMB Relay |  | | Kuehn, E. (2018, April 11). Ever Run a Relay? Why SMB Relays Should Be On Your Mind. Retrieved February 7, 2019. | | https://blog.secureideas.com/2018/04/ever-run-a-relay-why-smb-relays-should-be-on-your-mind.html |
| TechNet NetBIOS |  | | Microsoft. (n.d.). NetBIOS Name Resolution. Retrieved November 17, 2017. | | https://technet.microsoft.com/library/cc958811.aspx |
| GitHub NBNSpoof |  | | Nomex. (2014, February 7). NBNSpoof. Retrieved November 17, 2017. | | https://github.com/nomex/nbnspoof |
| GitHub Conveigh |  | | Robertson, K. (2016, August 28). Conveigh. Retrieved November 17, 2017. | | https://github.com/Kevin-Robertson/Conveigh |
| byt3bl33d3r NTLM Relaying |  | | Salvati, M. (2017, June 2). Practical guide to NTLM Relaying in 2017 (A.K.A getting a foothold in under 5 minutes). Retrieved February 7, 2019. | | https://byt3bl33d3r.github.io/practical-guide-to-ntlm-relaying-in-2017-aka-getting-a-foothold-in-under-5-minutes.html |
| Sternsecurity LLMNR-NBTNS |  | | Sternstein, J. (2013, November). Local Network Attacks: LLMNR and NBT-NS Poisoning. Retrieved November 17, 2017. | | https://www.sternsecurity.com/blog/local-network-attacks-llmnr-and-nbt-ns-poisoning |
| Wikipedia LLMNR |  | | Wikipedia. (2016, July 7). Link-Local Multicast Name Resolution. Retrieved November 17, 2017. | | https://en.wikipedia.org/wiki/Link-Local\_Multicast\_Name\_Resolution |
| **EXECUTION FLOWS** | | | | | | | | | |
| Impacket | | | | [Impacket](https://attack.mitre.org/software/S0357) modules like ntlmrelayx and smbrelayx can be used in conjunction with [Network Sniffing](https://attack.mitre.org/techniques/T1040) and [LLMNR/NBT-NS Poisoning and SMB Relay](https://attack.mitre.org/techniques/T1557/001) to gather NetNTLM credentials for [Brute Force](https://attack.mitre.org/techniques/T1110) or relay attacks that can gain code execution.  [Impacket](https://attack.mitre.org/software/S0357) is an open source collection of modules written in Python for programmatically constructing and manipulating network protocols. [Impacket](https://attack.mitre.org/software/S0357) contains several tools for remote service execution, Kerberos manipulation, Windows credential dumping, packet sniffing, and relay attacks. | | | | | |
| Empire | | | | [Empire](https://attack.mitre.org/software/S0363) can use Inveigh to conduct name service poisoning for credential theft and associated relay attacks.  [Empire](https://attack.mitre.org/software/S0363) is an open source, cross-platform remote administration and post-exploitation framework that is publicly available on GitHub. While the tool itself is primarily written in Python, the post-exploitation agents are written in pure [PowerShell](https://attack.mitre.org/techniques/T1059/001) for Windows and Python for Linux/macOS. [Empire](https://attack.mitre.org/software/S0363) was one of five tools singled out by a joint report on public hacking tools being widely used by adversaries. | | | | | |
| PoshC2 | | | | [PoshC2](https://attack.mitre.org/software/S0378) can use Inveigh to conduct name service poisoning for credential theft and associated relay attacks.  [PoshC2](https://attack.mitre.org/software/S0378) is an open source remote administration and post-exploitation framework that is publicly available on GitHub. The server-side components of the tool are primarily written in Python, while the implants are written in [PowerShell](https://attack.mitre.org/techniques/T1059/001). Although [PoshC2](https://attack.mitre.org/software/S0378) is primarily focused on Windows implantation, it does contain a basic Python dropper for Linux/macOS. | | | | | |
| Lazarus Group | | | | [Lazarus Group](https://attack.mitre.org/groups/G0032) executed [Responder](https://attack.mitre.org/software/S0174) using the command [Responder file path] -i [IP address] -rPv on a compromised host to harvest credentials and move laterally.  [Lazarus Group](https://attack.mitre.org/groups/G0032) is a North Korean state-sponsored cyber threat group that has been attributed to the Reconnaissance General Bureau. The group has been active since at least 2009 and was reportedly responsible for the November 2014 destructive wiper attack against Sony Pictures Entertainment as part of a campaign named Operation Blockbuster by Novetta. Malware used by [Lazarus Group](https://attack.mitre.org/groups/G0032) correlates to other reported campaigns, including Operation Flame, Operation 1Mission, Operation Troy, DarkSeoul, and Ten Days of Rain. North Korean group definitions are known to have significant overlap, and some security researchers report all North Korean state-sponsored cyber activity under the name [Lazarus Group](https://attack.mitre.org/groups/G0032) instead of tracking clusters or subgroups, such as [Andariel](https://attack.mitre.org/groups/G0138), [APT37](https://attack.mitre.org/groups/G0067), [APT38](https://attack.mitre.org/groups/G0082), and [Kimsuky](https://attack.mitre.org/groups/G0094). | | | | | |
| Wizard Spider | | | | [Wizard Spider](https://attack.mitre.org/groups/G0102) has used the Invoke-Inveigh PowerShell cmdlets, likely for name service poisoning.  [Wizard Spider](https://attack.mitre.org/groups/G0102) is a Russia-based financially motivated threat group originally known for the creation and deployment of [TrickBot](https://attack.mitre.org/software/S0266) since at least 2016. [Wizard Spider](https://attack.mitre.org/groups/G0102) possesses a diverse arsenal of tools and has conducted ransomware campaigns against a variety of organizations, ranging from major corporations to hospitals. | | | | | |
| Pupy | | | | [Pupy](https://attack.mitre.org/software/S0192) can sniff plaintext network credentials and use NBNS Spoofing to poison name services.  [Pupy](https://attack.mitre.org/software/S0192) is an open source, cross-platform (Windows, Linux, OSX, Android) remote administration and post-exploitation tool. It is written in Python and can be generated as a payload in several different ways (Windows exe, Python file, PowerShell oneliner/file, Linux elf, APK, Rubber Ducky, etc.). [Pupy](https://attack.mitre.org/software/S0192) is publicly available on GitHub. | | | | | |
| Responder | | | | [Responder](https://attack.mitre.org/software/S0174) is used to poison name services to gather hashes and credentials from systems within a local network.  Responder is an open source tool used for LLMNR, NBT-NS and MDNS poisoning, with built-in HTTP/SMB/MSSQL/FTP/LDAP rogue authentication server supporting NTLMv1/NTLMv2/LMv2, Extended Security NTLMSSP and Basic HTTP authentication. | | | | | |
| **VULNERABILITY** | | | | | | | | | |
| **PRIORITY** | | **High** | | | | | | | |
| **TITLE** | | Hosts Respond with Hashes/Challenge-Responses to Spoofed Hostnames | | | | | | | |
| **CVSSv3** | | Base: **8.1**  Temporal: **8.1**  Environmental: **8.1**  Vector: **CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N** | | | | | | | |
| **DESCRIPTION** | | During the assessment, it was discovered that hosts within the internal network utilised either **LLMNR, NBT-NS** or both to discover hosts on the network that aren't listed by the DNS server. This functionality allows an attacker to capture valid password hashes/challenge-responses and usernames that can be reused to connect to hosts or conduct a password cracking attack. | | | | | | | |
| **ATTACK SCENARIO** | | If an attacker can position themselves on an internal network segment and respond to requests from hosts that are looking for other hosts not listed by the DNS server, they will then receive the hash or challenge-response and username of the person using that host.  image Figure 8  The attacker then uses a Pass-The-Hash type attack to connect to hosts within the network in the event that NTLM hashes are captured, alternatively, if NTLMv1 or NTLMv2 hashes are captured, a password cracking attack is conducted and recovered credentials are used to connect to hosts either using psexec or RDP. | | | | | | | |
| **REMEDIATION ADVICE** | | Disable LLMNR and NBT-NS which prevent hosts from being able to broadcast other hosts that they are looking for. If this does not happen, a malicious attacker cannot respond to requests for missing hosts and spoof it's identity. | | | | | | | |
| **EVIDENCE** | | No further evidence. | | | | | | | |
| **AFFECTED ASSET** | | | | | | | | | |
| **STATUS** | | **Open** | | | | | | | |
| **AFFECTED** | | **10.0.0.1/24** | | | | | | | |
| **ATTACK NARRATIVE** | | For this assessment, attackers were placed on the 10.0.0.1/24 network segment.  This attack was executed from host 10.0.0.55. | | | | | | | |
| **REMEDIATION NOTES** | | *01/14/2024*  John P. is already working on disabling this.  image Figure 9 | | | | | | | |
| **POC** | | Run the tool Responder on an active broadcast domain:  image Figure 10  User attempts to search for a share that doesn't exist:  image Figure 11  View the LLMNR request in Responder:  image Figure 12  Get the user’s hashed credentials:  image Figure 13  Crack the hash using a tool such as Hashcat:  image Figure 14 | | | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **TECHNIQUE** | | | | | | |
| [3.1.0] Account Discovery | | | | | | |
| **DETAILS** | | | | | | |
| Adversaries may attempt to get a listing of valid accounts, usernames, or email addresses on a system or within a compromised environment. This information can help adversaries determine which accounts exist, which can aid in follow-on behaviour such as brute-forcing, spear-phishing attacks, or account takeovers e.g., [Valid Accounts](https://attack.mitre.org/techniques/T1078). Adversaries may use several methods to enumerate accounts, including abuse of existing tools, built-in commands, and potential misconfigurations that leak account names and roles or permissions in the targeted environment. For examples, cloud environments typically provide easily accessible interfaces to obtain user lists. On hosts, adversaries can use default [PowerShell](https://attack.mitre.org/techniques/T1059/001) and other command line functionality to identify accounts. Information about email addresses and accounts may also be extracted by searching an infected system’s files. | | | | | | |
| **MITRE ATT&CK REFERENCES** | | | | | | |
| **Domain** | Enterprise | | | | | |
| **Tactics** | Discovery | | | | | |
| **Spec. Version** | 3.1.0 | | | | | |
| **Kill Chain Phases** | **Kill Chain Name** | | **Phase Name** | | | |
| 1. mitre-attack | | Discovery | | | |
| **Platforms** | Windows, Azure AD, Office 365, SaaS, IaaS, Linux, macOS, Google Workspace | | | | | |
| **Data Sources** | * Process: Process Creation * Command: Command Execution * File: File Access | | | | | |
| **Detections** | **Data Source** | | **Data Component** | | **Detects** | |
| 1. General | | General | | System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Lateral Movement, based on the information obtained. Monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). Monitor for processes that can be used to enumerate user accounts, such as net.exe and net1.exe, especially when executed in quick succession.(Citation: Elastic - Koadiac Detection with EQL) | |
| 1. Process | | Process Creation | | Monitor for processes that can be used to enumerate user accounts and groups such as net.exe and net1.exe, especially when executed in quick succession.(Citation: Elastic - Koadiac Detection with EQL) Information may also be acquired through Windows system management tools such as [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). | |
| 1. Command | | Command Execution | | Monitor logs and other sources of command execution history for actions that could be taken to gather information about accounts, including the use of calls to cloud APIs that perform account discovery. System and network discovery techniques normally occur throughout an operation as an adversary learns the environment, and also to an extent in normal network operations. Therefore discovery data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Lateral Movement, based on the information obtained. | |
| 1. File | | File Access | | Monitor access to file resources that contain local accounts and groups information such as /etc/passwd, /Users directories, and the SAM database. If access requires high privileges, look for non-admin objects (such as users or processes) attempting to access restricted file resources. | |
| **Mitigations** | **Mitigation** | | **Description** | | | |
| Operating System Configuration | | Prevent administrator accounts from being enumerated when an application is elevating through UAC since it can lead to the disclosure of account names. The Registry key is located HKLM\ SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\CredUI\EnumerateAdministrators. It can be disabled through GPO: Computer Configuration &gt; [Policies] &gt; Administrative Templates &gt; Windows Components &gt; Credential User Interface: E numerate administrator accounts on elevation. (Citation: UCF STIG Elevation Account Enumeration) | | | |
| **External References** | **Name** | **Id** | | **Description** | | **URL** |
| mitre-attack | T1087 | |  | | https://attack.mitre.org/techniques/T1087 |
| Elastic - Koadiac Detection with EQL |  | | Stepanic, D.. (2020, January 13). Embracing offensive tooling: Building detections against Koadic using EQL. Retrieved November 30, 2020. | | https://www.elastic.co/blog/embracing-offensive-tooling-building-detections-against-koadic-using-eql |
| **EXECUTION FLOWS** | | | | | | |
| ShimRatReporter | [ShimRatReporter](https://attack.mitre.org/software/S0445) listed all non-privileged and privileged accounts available on the machine.(Citation: FOX-IT May 2016 Mofang)  [ShimRatReporter](https://attack.mitre.org/software/S0445) is a tool used by suspected Chinese adversary [Mofang](https://attack.mitre.org/groups/G0103) to automatically conduct initial discovery. The details from this discovery are used to customize follow-on payloads (such as [ShimRat](https://attack.mitre.org/software/S0444)) as well as set up faux infrastructure which mimics the adversary's targets. [ShimRatReporter](https://attack.mitre.org/software/S0445) has been used in campaigns targeting multiple countries and sectors including government, military, critical infrastructure, automobile, and weapons development.(Citation: FOX-IT May 2016 Mofang) | | | | | |
| Woody RAT | [Woody RAT](https://attack.mitre.org/software/S1065) can identify administrator accounts on an infected machine.(Citation: MalwareBytes WoodyRAT Aug 2022)  [Woody RAT](https://attack.mitre.org/software/S1065) is a remote access trojan (RAT) that has been used since at least August 2021 against Russian organizations.(Citation: MalwareBytes WoodyRAT Aug 2022) | | | | | |
| XCSSET | [XCSSET](https://attack.mitre.org/software/S0658) attempts to discover accounts from various locations such as a user's Evernote, AppleID, Telegram, Skype, and WeChat data.(Citation: trendmicro xcsset xcode project 2020)  [XCSSET](https://attack.mitre.org/software/S0658) is a macOS modular backdoor that targets Xcode application developers. [XCSSET](https://attack.mitre.org/software/S0658) was first observed in August 2020 and has been used to install a backdoor component, modify browser applications, conduct collection, and provide ransomware-like encryption capabilities.(Citation: trendmicro xcsset xcode project 2020) | | | | | |
| SolarWinds Compromise | During the [SolarWinds Compromise](https://attack.mitre.org/campaigns/C0024), [APT29](https://attack.mitre.org/groups/G0016) obtained a list of users and their roles from an Exchange server using `Get-ManagementRoleAssignment`.(Citation: Volexity SolarWinds)  The [SolarWinds Compromise](https://attack.mitre.org/campaigns/C0024) was a sophisticated supply chain cyber operation conducted by [APT29](https://attack.mitre.org/groups/G0016) that was discovered in mid-December 2020. [APT29](https://attack.mitre.org/groups/G0016) used customized malware to inject malicious code into the SolarWinds Orion software build process that was later distributed through a normal software update; they also used password spraying, token theft, API abuse, spear phishing, and other supply chain attacks to compromise user accounts and leverage their associated access. Victims of this campaign included government, consulting, technology, telecom, and other organizations in North America, Europe, Asia, and the Middle East. Industry reporting initially referred to the actors involved in this campaign as UNC2452, NOBELIUM, StellarParticle, Dark Halo, and SolarStorm.(Citation: SolarWinds Advisory Dec 2020)(Citation: SolarWinds Sunburst Sunspot Update January 2021)(Citation: FireEye SUNBURST Backdoor December 2020)(Citation: Volexity SolarWinds)(Citation: CrowdStrike StellarParticle January 2022)(Citation: Unit 42 SolarStorm December 2020)(Citation: Microsoft Analyzing Solorigate Dec 2020)(Citation: Microsoft Internal Solorigate Investigation Blog) In April 2021, the US and UK governments attributed the [SolarWinds Compromise](https://attack.mitre.org/campaigns/C0024) to Russia's Foreign Intelligence Service (SVR); public statements included citations to [APT29](https://attack.mitre.org/groups/G0016), Cozy Bear, and The Dukes.(Citation: NSA Joint Advisory SVR SolarWinds April 2021)(Citation: UK NSCS Russia SolarWinds April 2021)(Citation: Mandiant UNC2452 APT29 April 2022) The US government assessed that of the approximately 18,000 affected public and private sector customers of Solar Winds’ Orion product, a much smaller number were compromised by follow-on [APT29](https://attack.mitre.org/groups/G0016) activity on their systems.(Citation: USG Joint Statement SolarWinds January 2021) | | | | | |
| FIN13 | [FIN13](https://attack.mitre.org/groups/G1016) has enumerated all users and their roles from a victim's main treasury system.(Citation: Mandiant FIN13 Aug 2022)  [FIN13](https://attack.mitre.org/groups/G1016) is a financially motivated cyber threat group that has targeted the financial, retail, and hospitality industries in Mexico and Latin America, as early as 2016. [FIN13](https://attack.mitre.org/groups/G1016) achieves its objectives by stealing intellectual property, financial data, mergers and acquisition information, or PII.(Citation: Mandiant FIN13 Aug 2022)(Citation: Sygnia Elephant Beetle Jan 2022) | | | | | |
| APT29 | [APT29](https://attack.mitre.org/groups/G0016) obtained a list of users and their roles from an Exchange server using Get-ManagementRoleAssignment.(Citation: Volexity SolarWinds)  [APT29](https://attack.mitre.org/groups/G0016) is threat group that has been attributed to Russia's Foreign Intelligence Service (SVR).(Citation: White House Imposing Costs RU Gov April 2021)(Citation: UK Gov Malign RIS Activity April 2021) They have operated since at least 2008, often targeting government networks in Europe and NATO member countries, research institutes, and think tanks. [APT29](https://attack.mitre.org/groups/G0016) reportedly compromised the Democratic National Committee starting in the summer of 2015.(Citation: F-Secure The Dukes)(Citation: GRIZZLY STEPPE JAR)(Citation: Crowdstrike DNC June 2016)(Citation: UK Gov UK Exposes Russia SolarWinds April 2021) In April 2021, the US and UK governments attributed the [SolarWinds Compromise](https://attack.mitre.org/campaigns/C0024) to the SVR; public statements included citations to [APT29](https://attack.mitre.org/groups/G0016), Cozy Bear, and The Dukes.(Citation: NSA Joint Advisory SVR SolarWinds April 2021)(Citation: UK NSCS Russia SolarWinds April 2021) Industry reporting also referred to the actors involved in this campaign as UNC2452, NOBELIUM, StellarParticle, Dark Halo, and SolarStorm.(Citation: FireEye SUNBURST Backdoor December 2020)(Citation: MSTIC NOBELIUM Mar 2021)(Citation: CrowdStrike SUNSPOT Implant January 2021)(Citation: Volexity SolarWinds)(Citation: Cybersecurity Advisory SVR TTP May 2021)(Citation: Unit 42 SolarStorm December 2020) | | | | | |
| UNC2452 | [UNC2452](https://attack.mitre.org/groups/G0118) obtained a list of users and their roles from an Exchange server using Get-ManagementRoleAssignment.(Citation: Volexity SolarWinds)  [UNC2452](https://attack.mitre.org/groups/G0118) is a suspected Russian state-sponsored threat group responsible for the 2020 SolarWinds software supply chain intrusion.(Citation: FireEye SUNBURST Backdoor December 2020) Victims of this campaign include government, consulting, technology, telecom, and other organizations in North America, Europe, Asia, and the Middle East.(Citation: FireEye SUNBURST Backdoor December 2020) The group also compromised at least one think tank by late 2019.(Citation: Volexity SolarWinds) | | | | | |
| APT32 | [APT32](https://attack.mitre.org/groups/G0050) enumerated administrative users and DC servers using the commands net localgroup administrators and net group "Domain Controllers" /domain.  [APT32](https://attack.mitre.org/groups/G0050) is a suspected Vietnam-based threat group that has been active since at least 2014. The group has targeted multiple private sector industries as well as foreign governments, dissidents, and journalists with a strong focus on Southeast Asian countries like Vietnam, the Philippines, Laos, and Cambodia. They have extensively used strategic web compromises to compromise victims.(Citation: FireEye APT32 May 2017)(Citation: Volexity OceanLotus Nov 2017)(Citation: ESET OceanLotus) | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **TECHNIQUE** | | | | | | |
| [3.2.0] Adversary-in-the-Middle | | | | | | |
| **DETAILS** | | | | | | |
| Adversaries may attempt to position themselves between two or more networked devices using an adversary-in-the-middle (AiTM) technique to support follow-on behaviors such as [Network Sniffing](https://attack.mitre.org/techniques/T1040), [Transmitted Data Manipulation](https://attack.mitre.org/techniques/T1565/002), or replay attacks ([Exploitation for Credential Access](https://attack.mitre.org/techniques/T1212)). By abusing features of common networking protocols that can determine the flow of network traffic (e.g. ARP, DNS, LLMNR, etc.), adversaries may force a device to communicate through an adversary controlled system so they can collect information or perform additional actions.(Citation: Rapid7 MiTM Basics) For example, adversaries may manipulate victim DNS settings to enable other malicious activities such as preventing/redirecting users from accessing legitimate sites and/or pushing additional malware.(Citation: ttint\_rat)(Citation: dns\_changer\_trojans)(Citation: ad\_blocker\_with\_miner) Adversaries may also manipulate DNS and leverage their position in order to intercept user credentials and session cookies.(Citation: volexity\_0day\_sophos\_FW) [Downgrade Attack](https://attack.mitre.org/techniques/T1562/010)s can also be used to establish an AiTM position, such as by negotiating a less secure, deprecated, or weaker version of communication protocol (SSL/TLS) or encryption algorithm.(Citation: mitm\_tls\_downgrade\_att)(Citation: taxonomy\_downgrade\_att\_tls)(Citation: tlseminar\_downgrade\_att) Adversaries may also leverage the AiTM position to attempt to monitor and/or modify traffic, such as in [Transmitted Data Manipulation](https://attack.mitre.org/techniques/T1565/002). Adversaries can setup a position similar to AiTM to prevent traffic from flowing to the appropriate destination, potentially to [Impair Defenses](https://attack.mitre.org/techniques/T1562) and/or in support of a [Network Denial of Service](https://attack.mitre.org/techniques/T1498). | | | | | | |
| **MITRE ATT&CK REFERENCES** | | | | | | |
| **Domain** | Enterprise | | | | | |
| **Tactics** | Credential Access, Collection | | | | | |
| **Spec. Version** | 3.2.0 | | | | | |
| **Kill Chain Phases** | **Kill Chain Name** | | **Phase Name** | | | |
| 1. mitre-attack | | Credential Access | | | |
| 1. mitre-attack | | Collection | | | |
| **Platforms** | Windows, macOS, Linux, Network | | | | | |
| **Data Sources** | * Application Log: Application Log Content * Network Traffic: Network Traffic Content * Windows Registry: Windows Registry Key Modification * Network Traffic: Network Traffic Flow * Service: Service Creation | | | | | |
| **Detections** | **Data Source** | | **Data Component** | | **Detects** | |
| 1. General | | General | | Monitor network traffic for anomalies associated with known AiTM behavior. Consider monitoring for modifications to system configuration files involved in shaping network traffic flow. | |
| 1. Application Log | | Application Log Content | | Monitor application logs for changes to settings and other events associated with network protocols and other services commonly abused for AiTM.(Citation: dhcp\_serv\_op\_events) | |
| 1. Network Traffic | | Network Traffic Content | | Monitor network traffic for anomalies associated with known AiTM behavior. | |
| 1. Windows Registry | | Windows Registry Key Modification | | Monitor HKLM\Software\Policies\Microsoft\Windows NT\DNSClient for changes to the "EnableMulticast" DWORD value. A value of "0" indicates LLMNR is disabled. | |
| 1. Network Traffic | | Network Traffic Flow | | Monitor for network traffic originating from unknown/unexpected hardware devices. Local network traffic metadata (such as source MAC addressing) as well as usage of network management protocols such as DHCP may be helpful in identifying hardware. | |
| 1. Service | | Service Creation | | Monitor for newly constructed services/daemons through Windows event logs for event IDs 4697 and 7045. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as remote logins or process creation events. | |
| **Mitigations** | **Mitigation** | | **Description** | | | |
| Filter Network Traffic | | Use network appliances and host-based security software to block network traffic that is not necessary within the environment, such as legacy protocols that may be leveraged for AiTM conditions. | | | |
| Encrypt Sensitive Information | | Ensure that all wired and/or wireless traffic is encrypted appropriately. Use best practices for authentication protocols, such as Kerberos, and ensure web traffic that may contain credentials is protected by SSL/TLS. | | | |
| Limit Access to Resource Over Network | | Limit access to network infrastructure and resources that can be used to reshape traffic or otherwise produce AiTM conditions. | | | |
| Disable or Remove Feature or Program | | Disable legacy network protocols that may be used to intercept network traffic if applicable, especially those that are not needed within an environment. | | | |
| User Training | | Train users to be suspicious about certificate errors. Adversaries may use their own certificates in an attempt to intercept HTTPS traffic. Certificate errors may arise when the application’s certificate does not match the one expected by the host. | | | |
| Network Intrusion Prevention | | Network intrusion detection and prevention systems that can identify traffic patterns indicative of AiTM activity can be used to mitigate activity at the network level. | | | |
| Network Segmentation | | Network segmentation can be used to isolate infrastructure components that do not require broad network access. This may mitigate, or at least alleviate, the scope of AiTM activity. | | | |
| **External References** | **Name** | **Id** | | **Description** | | **URL** |
| mitre-attack | T1557 | | undefined | | https://attack.mitre.org/techniques/T1557 |
| dns\_changer\_trojans | undefined | | Abendan, O. (2012, June 14). How DNS Changer Trojans Direct Users to Threats. Retrieved October 28, 2021. | | https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/125/how-dns-changer-trojans-direct-users-to-threats |
| volexity\_0day\_sophos\_FW | undefined | | Adair, S., Lancaster, T., Volexity Threat Research. (2022, June 15). DriftingCloud: Zero-Day Sophos Firewall Exploitation and an Insidious Breach. Retrieved July 1, 2022. | | https://www.volexity.com/blog/2022/06/15/driftingcloud-zero-day-sophos-firewall-exploitation-and-an-insidious-breach/ |
| taxonomy\_downgrade\_att\_tls | undefined | | Alashwali, E. S., Rasmussen, K. (2019, January 26). What's in a Downgrade? A Taxonomy of Downgrade Attacks in the TLS Protocol and Application Protocols Using TLS. Retrieved December 7, 2021. | | https://arxiv.org/abs/1809.05681 |
| ad\_blocker\_with\_miner | undefined | | Kuzmenko, A.. (2021, March 10). Ad blocker with miner included. Retrieved October 28, 2021. | | https://securelist.com/ad-blocker-with-miner-included/101105/ |
| mitm\_tls\_downgrade\_att | undefined | | praetorian Editorial Team. (2014, August 19). Man-in-the-Middle TLS Protocol Downgrade Attack. Retrieved December 8, 2021. | | https://www.praetorian.com/blog/man-in-the-middle-tls-ssl-protocol-downgrade-attack/ |
| Rapid7 MiTM Basics | undefined | | Rapid7. (n.d.). Man-in-the-Middle (MITM) Attacks. Retrieved March 2, 2020. | | https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/ |
| tlseminar\_downgrade\_att | undefined | | Team Cinnamon. (2017, February 3). Downgrade Attacks. Retrieved December 9, 2021. | | https://tlseminar.github.io/downgrade-attacks/ |
| ttint\_rat | undefined | | Tu, L. Ma, Y. Ye, G. (2020, October 1). Ttint: An IoT Remote Access Trojan spread through 2 0-day vulnerabilities. Retrieved October 28, 2021. | | https://blog.netlab.360.com/ttint-an-iot-remote-control-trojan-spread-through-2-0-day-vulnerabilities/ |
| **EXECUTION FLOWS** | | | | | | |
| Dok | [Dok](https://attack.mitre.org/software/S0281) proxies web traffic to potentially monitor and alter victim HTTP(S) traffic.(Citation: objsee mac malware 2017)(Citation: CheckPoint Dok)  [Dok](https://attack.mitre.org/software/S0281) is a Trojan application disguised as a .zip file that is able to collect user credentials and install a malicious proxy server to redirect a user's network traffic (i.e. [Adversary-in-the-Middle](https://attack.mitre.org/techniques/T1557)).(Citation: objsee mac malware 2017)(Citation: hexed osx.dok analysis 2019)(Citation: CheckPoint Dok) | | | | | |
| Kimsuky | [Kimsuky](https://attack.mitre.org/groups/G0094) has used modified versions of PHProxy to examine web traffic between the victim and the accessed website.(Citation: CISA AA20-301A Kimsuky)  [Kimsuky](https://attack.mitre.org/groups/G0094) is a North Korea-based cyber espionage group that has been active since at least 2012. The group initially focused on targeting South Korean government entities, think tanks, and individuals identified as experts in various fields, and expanded its operations to include the United States, Russia, Europe, and the UN. [Kimsuky](https://attack.mitre.org/groups/G0094) has focused its intelligence collection activities on foreign policy and national security issues related to the Korean peninsula, nuclear policy, and sanctions.(Citation: EST Kimsuky April 2019)(Citation: BRI Kimsuky April 2019)(Citation: Cybereason Kimsuky November 2020)(Citation: Malwarebytes Kimsuky June 2021)(Citation: CISA AA20-301A Kimsuky) [Kimsuky](https://attack.mitre.org/groups/G0094) was assessed to be responsible for the 2014 Korea Hydro & Nuclear Power Co. compromise; other notable campaigns include Operation STOLEN PENCIL (2018), Operation Kabar Cobra (2019), and Operation Smoke Screen (2019).(Citation: Netscout Stolen Pencil Dec 2018)(Citation: EST Kimsuky SmokeScreen April 2019)(Citation: AhnLab Kimsuky Kabar Cobra Feb 2019) North Korean group definitions are known to have significant overlap, and some security researchers report all North Korean state-sponsored cyber activity under the name [Lazarus Group](https://attack.mitre.org/groups/G0032) instead of tracking clusters or subgroups. | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **TECHNIQUE** | | | | | | |
| [3.2.0] Account Manipulation | | | | | | |
| **DETAILS** | | | | | | |
| Adversaries may manipulate accounts to maintain and/or elevate access to victim systems. Account manipulation may consist of any action that preserves or modifies adversary access to a compromised account, such as modifying credentials or permission groups. These actions could also include account activity designed to subvert security policies, such as performing iterative password updates to bypass password duration policies and preserve the life of compromised credentials. In order to create or manipulate accounts, the adversary must already have sufficient permissions on systems or the domain. However, account manipulation may also lead to privilege escalation where modifications grant access to additional roles, permissions, or higher-privileged [Valid Accounts](https://attack.mitre.org/techniques/T1078). | | | | | | |
| **MITRE ATT&CK REFERENCES** | | | | | | |
| **Domain** | Enterprise | | | | | |
| **Tactics** | Persistence, Privilege Escalation | | | | | |
| **Spec. Version** | 3.2.0 | | | | | |
| **Kill Chain Phases** | **Kill Chain Name** | | **Phase Name** | | | |
| 1. mitre-attack | | Persistence | | | |
| 1. mitre-attack | | Privilege Escalation | | | |
| **Platforms** | Windows, Azure AD, Office 365, IaaS, Linux, macOS, Google Workspace, SaaS, Network, Containers | | | | | |
| **Data Sources** | * Command: Command Execution * Process: Process Creation * Active Directory: Active Directory Object Modification * File: File Modification * Group: Group Modification * User Account: User Account Modification | | | | | |
| **Detections** | **Data Source** | | **Data Component** | | **Detects** | |
| 1. General | | General | | Collect events that correlate with changes to account objects and/or permissions on systems and the domain, such as event IDs 4738, 4728 and 4670.(Citation: Microsoft User Modified Event)(Citation: Microsoft Security Event 4670)(Citation: Microsoft Security Event 4670) Monitor for modification of accounts in correlation with other suspicious activity. Changes may occur at unusual times or from unusual systems. Especially flag events where the subject and target accounts differ(Citation: InsiderThreat ChangeNTLM July 2017) or that include additional flags such as changing a password without knowledge of the old password.(Citation: GitHub Mimikatz Issue 92 June 2017)  Monitor for use of credentials at unusual times or to unusual systems or services. This may also correlate with other suspicious activity.  Monitor for unusual permissions changes that may indicate excessively broad permissions being granted to compromised accounts. However, account manipulation may also lead to privilege escalation where modifications grant access to additional roles, permissions, or higher-privileged [Valid Accounts](https://attack.mitre.org/techniques/T1078) | |
| 1. Command | | Command Execution | | Monitor executed commands and arguments for suspicious commands to modify accounts or account settings (including files such as the `authorized\_keys` or `/etc/ssh/sshd\_config`).  Monitor executed commands and arguments of suspicious commands (such as `Add-MailboxPermission`) that may be indicative of modifying the permissions of Exchange and other related service settings. | |
| 1. Process | | Process Creation | | Monitor for newly constructed processes indicative of modifying account settings, such as those that modify `authorized\_keys` or `/etc/ssh/sshd\_config` files. | |
| 1. Active Directory | | Active Directory Object Modification | | Monitor for the registration or joining of new device objects in Active Directory. Raise alerts when new devices are registered or joined without using MFA.(Citation: Microsoft Azure AD Security Operations for Devices) | |
| 1. File | | File Modification | | Monitor for changes made to files related to account settings, such as `/etc/ssh/sshd\_config` and the authorized\_keys file for each user on a system. | |
| 1. Group | | Group Modification | | Monitor events for changes to account objects and/or permissions on systems and the domain, such as event IDs 4738, 4728 and 4670. | |
| 1. User Account | | User Account Modification | | Monitor events for changes to account objects and/or permissions on systems and the domain, such as event IDs 4738, 4728 and 4670. Monitor for modification of accounts in correlation with other suspicious activity. Changes may occur at unusual times or from unusual systems. Especially flag events where the subject and target accounts differ or that include additional flags such as changing a password without knowledge of the old password.    Monitor for unusual permissions changes that may indicate excessively broad permissions being granted to compromised accounts. | |
| **Mitigations** | **Mitigation** | | **Description** | | | |
| Network Segmentation | | Configure access controls and firewalls to limit access to critical systems and domain controllers. Most cloud environments support separate virtual private cloud (VPC) instances that enable further segmentation of cloud systems. | | | |
| User Account Management | | Ensure that low-privileged user accounts do not have permissions to modify accounts or account-related policies. | | | |
| Multi-factor Authentication | | Use multi-factor authentication for user and privileged accounts. | | | |
| Privileged Account Management | | Do not allow domain administrator accounts to be used for day-to-day operations that may expose them to potential adversaries on unprivileged systems. | | | |
| Operating System Configuration | | Protect domain controllers by ensuring proper security configuration for critical servers to limit access by potentially unnecessary protocols and services, such as SMB file sharing. | | | |
| Operating System Configuration | | Protect domain controllers by ensuring proper security configuration for critical servers to limit access by potentially unnecessary protocols and services, such as SMB file sharing. | | | |
| **External References** | **Name** | **Id** | | **Description** | | **URL** |
| mitre-attack | T1098 | | undefined | | https://attack.mitre.org/techniques/T1098 |
| Microsoft Security Event 4670 | undefined | | Franklin Smith, R. (n.d.). Windows Security Log Event ID 4670. Retrieved November 4, 2019. | | https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4670 |
| Microsoft User Modified Event | undefined | | Lich, B., Miroshnikov, A. (2017, April 5). 4738(S): A user account was changed. Retrieved June 30, 2017. | | https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4738 |
| InsiderThreat ChangeNTLM July 2017 | undefined | | Warren, J. (2017, July 11). Manipulating User Passwords with Mimikatz. Retrieved December 4, 2017. | | https://blog.stealthbits.com/manipulating-user-passwords-with-mimikatz-SetNTLM-ChangeNTLM |
| GitHub Mimikatz Issue 92 June 2017 | undefined | | Warren, J. (2017, June 22). lsadump::changentlm and lsadump::setntlm work, but generate Windows events #92. Retrieved December 4, 2017. | | https://github.com/gentilkiwi/mimikatz/issues/92 |
| **EXECUTION FLOWS** | | | | | | |
| Lazarus Group | [Lazarus Group](https://attack.mitre.org/groups/G0032) malware WhiskeyDelta-Two contains a function that attempts to rename the administrator’s account.(Citation: Novetta Blockbuster)(Citation: Novetta Blockbuster Destructive Malware)  [Lazarus Group](https://attack.mitre.org/groups/G0032) is a North Korean state-sponsored cyber threat group that has been attributed to the Reconnaissance General Bureau.(Citation: US-CERT HIDDEN COBRA June 2017)(Citation: Treasury North Korean Cyber Groups September 2019) The group has been active since at least 2009 and was reportedly responsible for the November 2014 destructive wiper attack against Sony Pictures Entertainment as part of a campaign named Operation Blockbuster by Novetta. Malware used by [Lazarus Group](https://attack.mitre.org/groups/G0032) correlates to other reported campaigns, including Operation Flame, Operation 1Mission, Operation Troy, DarkSeoul, and Ten Days of Rain. (Citation: Novetta Blockbuster) North Korean group definitions are known to have significant overlap, and some security researchers report all North Korean state-sponsored cyber activity under the name [Lazarus Group](https://attack.mitre.org/groups/G0032) instead of tracking clusters or subgroups, such as [Andariel](https://attack.mitre.org/groups/G0138), [APT37](https://attack.mitre.org/groups/G0067), [APT38](https://attack.mitre.org/groups/G0082), and [Kimsuky](https://attack.mitre.org/groups/G0094). | | | | | |
| SMOKEDHAM | [SMOKEDHAM](https://attack.mitre.org/software/S0649) has added user accounts to local Admin groups.(Citation: FireEye SMOKEDHAM June 2021)  [SMOKEDHAM](https://attack.mitre.org/software/S0649) is a Powershell-based .NET backdoor that was first reported in May 2021; it has been used by at least one ransomware-as-a-service affiliate.(Citation: FireEye Shining A Light on DARKSIDE May 2021)(Citation: FireEye SMOKEDHAM June 2021) | | | | | |
| APT41 | [APT41](https://attack.mitre.org/groups/G0096) has added user accounts to the User and Admin groups.(Citation: FireEye APT41 Aug 2019)  [APT41](https://attack.mitre.org/groups/G0096) is a threat group that researchers have assessed as Chinese state-sponsored espionage group that also conducts financially-motivated operations. Active since at least 2012, [APT41](https://attack.mitre.org/groups/G0096) has been observed targeting healthcare, telecom, technology, and video game industries in 14 countries. [APT41](https://attack.mitre.org/groups/G0096) overlaps at least partially with public reporting on groups including BARIUM and [Winnti Group](https://attack.mitre.org/groups/G0044).(Citation: FireEye APT41 Aug 2019)(Citation: Group IB APT 41 June 2021) | | | | | |
| APT3 | [APT3](https://attack.mitre.org/groups/G0022) has been known to add created accounts to local admin groups to maintain elevated access.(Citation: aptsim)  [APT3](https://attack.mitre.org/groups/G0022) is a China-based threat group that researchers have attributed to China's Ministry of State Security.(Citation: FireEye Clandestine Wolf)(Citation: Recorded Future APT3 May 2017) This group is responsible for the campaigns known as Operation Clandestine Fox, Operation Clandestine Wolf, and Operation Double Tap.(Citation: FireEye Clandestine Wolf)(Citation: FireEye Operation Double Tap) As of June 2015, the group appears to have shifted from targeting primarily US victims to primarily political organizations in Hong Kong.(Citation: Symantec Buckeye) In 2017, MITRE developed an APT3 Adversary Emulation Plan.(Citation: APT3 Adversary Emulation Plan) | | | | | |
| Mimikatz | The [Mimikatz](https://attack.mitre.org/software/S0002) credential dumper has been extended to include Skeleton Key domain controller authentication bypass functionality. The LSADUMP::ChangeNTLM and LSADUMP::SetNTLM modules can also manipulate the password hash of an account without knowing the clear text value.(Citation: Adsecurity Mimikatz Guide)(Citation: Metcalf 2015)  [Mimikatz](https://attack.mitre.org/software/S0002) is a credential dumper capable of obtaining plaintext Windows account logins and passwords, along with many other features that make it useful for testing the security of networks. (Citation: Deply Mimikatz) (Citation: Adsecurity Mimikatz Guide) | | | | | |
| Magic Hound | [Magic Hound](https://attack.mitre.org/groups/G0059) has added a user named DefaultAccount to the Administrators and Remote Desktop Users groups.(Citation: DFIR Report APT35 ProxyShell March 2022)  [Magic Hound](https://attack.mitre.org/groups/G0059) is an Iranian-sponsored threat group that conducts long term, resource-intensive cyber espionage operations, likely on behalf of the Islamic Revolutionary Guard Corps. They have targeted European, U.S., and Middle Eastern government and military personnel, academics, journalists, and organizations such as the World Health Organization (WHO), via complex social engineering campaigns since at least 2014.(Citation: FireEye APT35 2018)(Citation: ClearSky Kittens Back 3 August 2020)(Citation: Certfa Charming Kitten January 2021)(Citation: Secureworks COBALT ILLUSION Threat Profile)(Citation: Proofpoint TA453 July2021) | | | | | |
| Dragonfly | [Dragonfly](https://attack.mitre.org/groups/G0035) has added newly created accounts to the administrators group to maintain elevated access.(Citation: US-CERT TA18-074A)  [Dragonfly](https://attack.mitre.org/groups/G0035) is a cyber espionage group that has been attributed to Russia's Federal Security Service (FSB) Center 16.(Citation: DOJ Russia Targeting Critical Infrastructure March 2022)(Citation: UK GOV FSB Factsheet April 2022) Active since at least 2010, [Dragonfly](https://attack.mitre.org/groups/G0035) has targeted defense and aviation companies, government entities, companies related to industrial control systems, and critical infrastructure sectors worldwide through supply chain, spearphishing, and drive-by compromise attacks.(Citation: Symantec Dragonfly)(Citation: Secureworks IRON LIBERTY July 2019)(Citation: Symantec Dragonfly Sept 2017)(Citation: Fortune Dragonfly 2.0 Sept 2017)(Citation: Gigamon Berserk Bear October 2021)(Citation: CISA AA20-296A Berserk Bear December 2020)(Citation: Symantec Dragonfly 2.0 October 2017) | | | | | |
| FIN13 | [FIN13](https://attack.mitre.org/groups/G1016) has assigned newly created accounts the sysadmin role to maintain persistence.(Citation: Sygnia Elephant Beetle Jan 2022)  [FIN13](https://attack.mitre.org/groups/G1016) is a financially motivated cyber threat group that has targeted the financial, retail, and hospitality industries in Mexico and Latin America, as early as 2016. [FIN13](https://attack.mitre.org/groups/G1016) achieves its objectives by stealing intellectual property, financial data, mergers and acquisition information, or PII.(Citation: Mandiant FIN13 Aug 2022)(Citation: Sygnia Elephant Beetle Jan 2022) | | | | | |
| 2016 Ukraine Electric Power Attack | During the [2016 Ukraine Electric Power Attack](https://attack.mitre.org/campaigns/C0025), [Sandworm Team](https://attack.mitre.org/groups/G0034) used the `sp\_addlinkedsrvlogin` command in MS-SQL to create a link between a created account and other servers in the network.(Citation: Dragos Crashoverride 2018)  [2016 Ukraine Electric Power Attack](https://attack.mitre.org/campaigns/C0025) was a [Sandworm Team](https://attack.mitre.org/groups/G0034) campaign during which they used [Industroyer](https://attack.mitre.org/software/S0604) malware to target and disrupt distribution substations within the Ukrainian power grid. This campaign was the second major public attack conducted against Ukraine by [Sandworm Team](https://attack.mitre.org/groups/G0034).(Citation: ESET Industroyer)(Citation: Dragos Crashoverride 2018) | | | | | |
| HAFNIUM | [HAFNIUM](https://attack.mitre.org/groups/G0125) has granted privileges to domain accounts.(Citation: Volexity Exchange Marauder March 2021)  [HAFNIUM](https://attack.mitre.org/groups/G0125) is a likely state-sponsored cyber espionage group operating out of China that has been active since at least January 2021. [HAFNIUM](https://attack.mitre.org/groups/G0125) primarily targets entities in the US across a number of industry sectors, including infectious disease researchers, law firms, higher education institutions, defense contractors, policy think tanks, and NGOs.(Citation: Microsoft HAFNIUM March 2020)(Citation: Volexity Exchange Marauder March 2021) | | | | | |
| ServHelper | [ServHelper](https://attack.mitre.org/software/S0382) has added a user named "supportaccount" to the Remote Desktop Users and Administrators groups.(Citation: Proofpoint TA505 Jan 2019)  [ServHelper](https://attack.mitre.org/software/S0382) is a backdoor first observed in late 2018. The backdoor is written in Delphi and is typically delivered as a DLL file.(Citation: Proofpoint TA505 Jan 2019) | | | | | |
| Kimsuky | [Kimsuky](https://attack.mitre.org/groups/G0094) has added accounts to specific groups with net localgroup.(Citation: KISA Operation Muzabi)  [Kimsuky](https://attack.mitre.org/groups/G0094) is a North Korea-based cyber espionage group that has been active since at least 2012. The group initially focused on targeting South Korean government entities, think tanks, and individuals identified as experts in various fields, and expanded its operations to include the United States, Russia, Europe, and the UN. [Kimsuky](https://attack.mitre.org/groups/G0094) has focused its intelligence collection activities on foreign policy and national security issues related to the Korean peninsula, nuclear policy, and sanctions.(Citation: EST Kimsuky April 2019)(Citation: BRI Kimsuky April 2019)(Citation: Cybereason Kimsuky November 2020)(Citation: Malwarebytes Kimsuky June 2021)(Citation: CISA AA20-301A Kimsuky) [Kimsuky](https://attack.mitre.org/groups/G0094) was assessed to be responsible for the 2014 Korea Hydro & Nuclear Power Co. compromise; other notable campaigns include Operation STOLEN PENCIL (2018), Operation Kabar Cobra (2019), and Operation Smoke Screen (2019).(Citation: Netscout Stolen Pencil Dec 2018)(Citation: EST Kimsuky SmokeScreen April 2019)(Citation: AhnLab Kimsuky Kabar Cobra Feb 2019) North Korean group definitions are known to have significant overlap, and some security researchers report all North Korean state-sponsored cyber activity under the name [Lazarus Group](https://attack.mitre.org/groups/G0032) instead of tracking clusters or subgroups. | | | | | |
| Calisto | [Calisto](https://attack.mitre.org/software/S0274) adds permissions and remote logins to all users.(Citation: Symantec Calisto July 2018)  [Calisto](https://attack.mitre.org/software/S0274) is a macOS Trojan that opens a backdoor on the compromised machine. [Calisto](https://attack.mitre.org/software/S0274) is believed to have first been developed in 2016. (Citation: Securelist Calisto July 2018) (Citation: Symantec Calisto July 2018) | | | | | |
| Sandworm Team | [Sandworm Team](https://attack.mitre.org/groups/G0034) used the sp\_addlinkedsrvlogin command in MS-SQL to create a link between a created account and other servers in the network.(Citation: Dragos Crashoverride 2018)  [Sandworm Team](https://attack.mitre.org/groups/G0034) is a destructive threat group that has been attributed to Russia's General Staff Main Intelligence Directorate (GRU) Main Center for Special Technologies (GTsST) military unit 74455.(Citation: US District Court Indictment GRU Unit 74455 October 2020)(Citation: UK NCSC Olympic Attacks October 2020) This group has been active since at least 2009.(Citation: iSIGHT Sandworm 2014)(Citation: CrowdStrike VOODOO BEAR)(Citation: USDOJ Sandworm Feb 2020)(Citation: NCSC Sandworm Feb 2020) In October 2020, the US indicted six GRU Unit 74455 officers associated with [Sandworm Team](https://attack.mitre.org/groups/G0034) for the following cyber operations: the 2015 and 2016 attacks against Ukrainian electrical companies and government organizations, the 2017 worldwide [NotPetya](https://attack.mitre.org/software/S0368) attack, targeting of the 2017 French presidential campaign, the 2018 [Olympic Destroyer](https://attack.mitre.org/software/S0365) attack against the Winter Olympic Games, the 2018 operation against the Organisation for the Prohibition of Chemical Weapons, and attacks against the country of Georgia in 2018 and 2019.(Citation: US District Court Indictment GRU Unit 74455 October 2020)(Citation: UK NCSC Olympic Attacks October 2020) Some of these were conducted with the assistance of GRU Unit 26165, which is also referred to as [APT28](https://attack.mitre.org/groups/G0007).(Citation: US District Court Indictment GRU Oct 2018) | | | | | |
| Dragonfly 2.0 | [Dragonfly 2.0](https://attack.mitre.org/groups/G0074) added newly created accounts to the administrators group to maintain elevated access.(Citation: US-CERT TA18-074A)(Citation: US-CERT APT Energy Oct 2017)  [Dragonfly 2.0](https://attack.mitre.org/groups/G0074) is a suspected Russian group that has targeted government entities and multiple U.S. critical infrastructure sectors since at least December 2015. (Citation: US-CERT TA18-074A) (Citation: Symantec Dragonfly Sept 2017) There is debate over the extent of overlap between [Dragonfly 2.0](https://attack.mitre.org/groups/G0074) and [Dragonfly](https://attack.mitre.org/groups/G0035), but there is sufficient evidence to lead to these being tracked as two separate groups. (Citation: Fortune Dragonfly 2.0 Sept 2017)(Citation: Dragos DYMALLOY ) | | | | | |
| Magic Hound | [Magic Hound](https://attack.mitre.org/groups/G0059) granted compromised email accounts read access to the email boxes of additional targeted accounts. The group then was able to authenticate to the intended victim's OWA (Outlook Web Access) portal and read hundreds of email communications for information on Middle East organizations.  [Magic Hound](https://attack.mitre.org/groups/G0059) is an Iranian-sponsored threat group that conducts long term, resource-intensive cyber espionage operations, likely on behalf of the Islamic Revolutionary Guard Corps. They have targeted European, U.S., and Middle Eastern government and military personnel, academics, journalists, and organizations such as the World Health Organization (WHO), via complex social engineering campaigns since at least 2014.(Citation: FireEye APT35 2018)(Citation: ClearSky Kittens Back 3 August 2020)(Citation: Certfa Charming Kitten January 2021)(Citation: Secureworks COBALT ILLUSION Threat Profile)(Citation: Proofpoint TA453 July2021) | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **TECHNIQUE** | | | | | | |
| [3.1.0] Brute Force | | | | | | |
| **DETAILS** | | | | | | |
| Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained. Without knowledge of the password for an account or set of accounts, an adversary may systematically guess the password using a repetitive or iterative mechanism. Brute forcing passwords can take place via interaction with a service that will check the validity of those credentials or offline against previously acquired credential data, such as password hashes. Brute forcing credentials may take place at various points during a breach. For example, adversaries may attempt to brute force access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) within a victim environment leveraging knowledge gathered from other post-compromise behaviors such as [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), [Account Discovery](https://attack.mitre.org/techniques/T1087), or [Password Policy Discovery](https://attack.mitre.org/techniques/T1201). Adversaries may also combine brute forcing activity with behaviors such as [External Remote Services](https://attack.mitre.org/techniques/T1133) as part of Initial Access. | | | | | | |
| **MITRE ATT&CK REFERENCES** | | | | | | |
| **Domain** | Enterprise | | | | | |
| **Tactics** | Credential Access | | | | | |
| **Spec. Version** | 3.1.0 | | | | | |
| **Kill Chain Phases** | **Kill Chain Name** | | **Phase Name** | | | |
| 1. mitre-attack | | Credential Access | | | |
| **Platforms** | Windows, Azure AD, Office 365, SaaS, IaaS, Linux, macOS, Google Workspace, Containers, Network | | | | | |
| **Data Sources** | * User Account: User Account Authentication * Command: Command Execution * Application Log: Application Log Content | | | | | |
| **Detections** | **Data Source** | | **Data Component** | | **Detects** | |
| 1. General | | General | | Monitor authentication logs for system and application login failures of [Valid Accounts](https://attack.mitre.org/techniques/T1078). If authentication failures are high, then there may be a brute force attempt to gain access to a system using legitimate credentials. Also monitor for many failed authentication attempts across various accounts that may result from password spraying attempts. It is difficult to detect when hashes are cracked, since this is generally done outside the scope of the target network. | |
| 1. User Account | | User Account Authentication | | Monitor for many failed authentication attempts across various accounts that may result from password spraying attempts. It is difficult to detect when hashes are cracked, since this is generally done outside the scope of the target network. | |
| 1. Command | | Command Execution | | Monitor executed commands and arguments that may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained. | |
| 1. Application Log | | Application Log Content | | Monitor authentication logs for system and application login failures of [Valid Accounts](https://attack.mitre.org/techniques/T1078). If authentication failures are high, then there may be a brute force attempt to gain access to a system using legitimate credentials. | |
| **Mitigations** | **Mitigation** | | **Description** | | | |
| User Account Management | | Proactively reset accounts that are known to be part of breached credentials either immediately, or after detecting bruteforce attempts. | | | |
| Account Use Policies | | Set account lockout policies after a certain number of failed login attempts to prevent passwords from being guessed. Too strict a policy may create a denial of service condition and render environments un-usable, with all accounts used in the brute force being locked-out. Use conditional access policies to block logins from non-compliant devices or from outside defined organization IP ranges.(Citation: Microsoft Common Conditional Access Policies) | | | |
| Multi-factor Authentication | | Use multi-factor authentication. Where possible, also enable multi-factor authentication on externally facing services. | | | |
| Password Policies | | Refer to NIST guidelines when creating password policies.(Citation: NIST 800-63-3) | | | |
| **External References** | **Name** | **Id** | | **Description** | | **URL** |
| mitre-attack | T1110 | | undefined | | https://attack.mitre.org/techniques/T1110 |
| **EXECUTION FLOWS** | | | | | | |
| Fox Kitten | [Fox Kitten](https://attack.mitre.org/groups/G0117) has brute forced RDP credentials.(Citation: ClearSky Pay2Kitten December 2020)  [Fox Kitten](https://attack.mitre.org/groups/G0117) is threat actor with a suspected nexus to the Iranian government that has been active since at least 2017 against entities in the Middle East, North Africa, Europe, Australia, and North America. [Fox Kitten](https://attack.mitre.org/groups/G0117) has targeted multiple industrial verticals including oil and gas, technology, government, defense, healthcare, manufacturing, and engineering.(Citation: ClearkSky Fox Kitten February 2020)(Citation: CrowdStrike PIONEER KITTEN August 2020)(Citation: Dragos PARISITE )(Citation: ClearSky Pay2Kitten December 2020) | | | | | |
| HEXANE | [HEXANE](https://attack.mitre.org/groups/G1001) has used brute force attacks to compromise valid credentials.(Citation: SecureWorks August 2019)  [HEXANE](https://attack.mitre.org/groups/G1001) is a cyber espionage threat group that has targeted oil & gas, telecommunications, aviation, and internet service provider organizations since at least 2017. Targeted companies have been located in the Middle East and Africa, including Israel, Saudi Arabia, Kuwait, Morocco, and Tunisia. [HEXANE](https://attack.mitre.org/groups/G1001)'s TTPs appear similar to [APT33](https://attack.mitre.org/groups/G0064) and [OilRig](https://attack.mitre.org/groups/G0049) but due to differences in victims and tools it is tracked as a separate entity.(Citation: Dragos Hexane)(Citation: Kaspersky Lyceum October 2021)(Citation: ClearSky Siamesekitten August 2021)(Citation: Accenture Lyceum Targets November 2021) | | | | | |
| Chaos | [Chaos](https://attack.mitre.org/software/S0220) conducts brute force attacks against SSH services to gain initial access.(Citation: Chaos Stolen Backdoor)  [Chaos](https://attack.mitre.org/software/S0220) is Linux malware that compromises systems by brute force attacks against SSH services. Once installed, it provides a reverse shell to its controllers, triggered by unsolicited packets. (Citation: Chaos Stolen Backdoor) | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **TECHNIQUE** | | | | | | |
| [3.1.0] Bypass User Account Control | | | | | | |
| **DETAILS** | | | | | | |
| Adversaries may bypass UAC mechanisms to elevate process privileges on system. Windows User Account Control (UAC) allows a program to elevate its privileges (tracked as integrity levels ranging from low to high) to perform a task under administrator-level permissions, possibly by prompting the user for confirmation. The impact to the user ranges from denying the operation under high enforcement to allowing the user to perform the action if they are in the local administrators group and click through the prompt or allowing them to enter an administrator password to complete the action.(Citation: TechNet How UAC Works) If the UAC protection level of a computer is set to anything but the highest level, certain Windows programs can elevate privileges or execute some elevated [Component Object Model](https://attack.mitre.org/techniques/T1559/001) objects without prompting the user through the UAC notification box.(Citation: TechNet Inside UAC)(Citation: MSDN COM Elevation) An example of this is use of [Rundll32](https://attack.mitre.org/techniques/T1218/011) to load a specifically crafted DLL which loads an auto-elevated [Component Object Model](https://attack.mitre.org/techniques/T1559/001) object and performs a file operation in a protected directory which would typically require elevated access. Malicious software may also be injected into a trusted process to gain elevated privileges without prompting a user.(Citation: Davidson Windows) Many methods have been discovered to bypass UAC. The Github readme page for UACME contains an extensive list of methods(Citation: Github UACMe) that have been discovered and implemented, but may not be a comprehensive list of bypasses. Additional bypass methods are regularly discovered and some used in the wild, such as: \* eventvwr.exe can auto-elevate and execute a specified binary or script.(Citation: enigma0x3 Fileless UAC Bypass)(Citation: Fortinet Fareit) Another bypass is possible through some lateral movement techniques if credentials for an account with administrator privileges are known, since UAC is a single system security mechanism, and the privilege or integrity of a process running on one system will be unknown on remote systems and default to high integrity.(Citation: SANS UAC Bypass) | | | | | | |
| **MITRE ATT&CK REFERENCES** | | | | | | |
| **Domain** | Enterprise | | | | | |
| **Tactics** | Privilege Escalation, Defense Evasion | | | | | |
| **Spec. Version** | 3.1.0 | | | | | |
| **Permissions Required** | Administrator, User | | | | | |
| **Defense Bypassed** | Windows User Account Control | | | | | |
| **Kill Chain Phases** | **Kill Chain Name** | | **Phase Name** | | | |
| 1. mitre-attack | | Privilege Escalation | | | |
| 1. mitre-attack | | Defense Evasion | | | |
| **Platforms** | Windows | | | | | |
| **Data Sources** | * Windows Registry: Windows Registry Key Modification * Command: Command Execution * Process: Process Creation * Process: Process Metadata | | | | | |
| **Detections** | **Data Source** | | **Data Component** | | **Detects** | |
| 1. General | | General | | There are many ways to perform UAC bypasses when a user is in the local administrator group on a system, so it may be difficult to target detection on all variations. Efforts should likely be placed on mitigation and collecting enough information on process launches and actions that could be performed before and after a UAC bypass is performed. Monitor process API calls for behavior that may be indicative of [Process Injection](https://attack.mitre.org/techniques/T1055) and unusual loaded DLLs through [DLL Search Order Hijacking](https://attack.mitre.org/techniques/T1574/001), which indicate attempts to gain access to higher privileged processes.  Some UAC bypass methods rely on modifying specific, user-accessible Registry settings. For example:  \* The eventvwr.exe bypass uses the [HKEY\_CURRENT\_USER]\Software\Classes\mscfile\shell\open\command Registry key.(Citation: enigma0x3 Fileless UAC Bypass)  \* The sdclt.exe bypass uses the [HKEY\_CURRENT\_USER]\Software\Microsoft\Windows\CurrentVersion\App Paths\control.exe and [HKEY\_CURRENT\_USER]\Software\Classes\exefile\shell\runas\command\isolatedCommand Registry keys.(Citation: enigma0x3 sdclt app paths)(Citation: enigma0x3 sdclt bypass)  Analysts should monitor these Registry settings for unauthorized changes. | |
| 1. Windows Registry | | Windows Registry Key Modification | | Some UAC bypass methods rely on modifying specific, user-accessible Registry settings. For example: \* The eventvwr.exe bypass uses the [HKEY\_CURRENT\_USER]\Software\Classes\mscfile\shell\open\command Registry key.(Citation: enigma0x3 Fileless UAC Bypass) \* The sdclt.exe bypass uses the [HKEY\_CURRENT\_USER]\Software\Microsoft\Windows\CurrentVersion\App Paths\control.exe and [HKEY\_CURRENT\_USER]\Software\Classes\exefile\shell\runas\command\isolatedCommand Registry keys.(Citation: enigma0x3 sdclt app paths)(Citation: enigma0x3 sdclt bypass) Analysts should monitor these Registry settings for unauthorized changes.  UAC Bypass is an interesting technique in that new implementations are regularly found and existing implementations may be fixed (i.e., patched) by Microsoft in new builds of Windows. Therefore, it is important to validate than detections for UAC Bypass are still relevant (i.e., they target non-patched implementations).   Note: Sysmon Event ID 12 (Registry Key Create/Delete), Sysmon Event ID 13 (Registry Value Set), and Sysmon Event ID 14 (Registry Key and Value Rename) are useful for creating detections around Registry Key Modification in the context of UAC Bypass. | |
| 1. Command | | Command Execution | | Monitor executed commands and arguments that may bypass UAC mechanisms to elevate process privileges on system. | |
| 1. Process | | Process Creation | | Monitor newly executed processes, such as eventvwr.exe and sdclt.exe, that may bypass UAC mechanisms to elevate process privileges on system.  Threat actors often, after compromising a machine, try to disable User Access Control (UAC) to escalate privileges. This is often done by changing the registry key for system policies using “reg.exe”, a legitimate tool provided by Microsoft for modifying the registry via command prompt or scripts. This action interferes with UAC and may enable a threat actor to escalate privileges on the compromised system, thereby allowing further exploitation of the system.   Analytic 1 : UAC Bypass  possible\_uac\_bypass = filter processes where (  integrity\_level == "High" and  (parent\_image\_path == "c:\windows\system32\fodhelper.exe") or  (command\_line == "\*.exe\"\*cleanmgr.exe /autoclean\*") or  (image\_path == "c:\program files\windows media player\osk.exe") or  (parent\_image\_path == "c:\windows\system32\slui.exe") or  (parent\_command\_line == '"c:\windows\system32\dism.exe"\*""\*.xml"' and image\_path != "c:\users\\*\appdata\local\temp\\*\dismhost.exe") or  (command\_line == '"c:\windows\system32\wusa.exe"\*/quiet\*' and user != "NOT\_TRANSLATED" and current\_working\_directory == "c:\windows\system32\" and parent\_image\_path != "c:\windows\explorer.exe") or  (parent\_image\_path == "c:\windows\\*dccw.exe" and image\_path != "c:\windows\system32\cttune.exe"))    Analytic 2 : Disable UAC  cmd\_processes = filter processes where (  (parent\_image = "C:\\Windows\\System32\\cmd.exe") AND (command\_line = "reg.exe%HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\System%REG\_DWORD /d 0%")) | |
| 1. Process | | Process Metadata | | Monitor contextual data about a running process, which may include information such as environment variables, image name, user/owner that may bypass UAC mechanisms to elevate process privileges on system. | |
| **Mitigations** | **Mitigation** | | **Description** | | | |
| Update Software | | Consider updating Windows to the latest version and patch level to utilize the latest protective measures against UAC bypass.(Citation: Github UACMe) | | | |
| Audit | | Check for common UAC bypass weaknesses on Windows systems to be aware of the risk posture and address issues where appropriate.(Citation: Github UACMe) | | | |
| User Account Control | | Although UAC bypass techniques exist, it is still prudent to use the highest enforcement level for UAC when possible and mitigate bypass opportunities that exist with techniques such as [DLL Search Order Hijacking](https://attack.mitre.org/techniques/T1574/001). | | | |
| Privileged Account Management | | Remove users from the local administrator group on systems. | | | |
| **External References** | **Name** | **Id** | | **Description** | | **URL** |
| mitre-attack | T1548.002 | | undefined | | https://attack.mitre.org/techniques/T1548/002 |
| Davidson Windows | undefined | | Davidson, L. (n.d.). Windows 7 UAC whitelist. Retrieved November 12, 2014. | | http://www.pretentiousname.com/misc/win7\_uac\_whitelist2.html |
| TechNet How UAC Works | undefined | | Lich, B. (2016, May 31). How User Account Control Works. Retrieved June 3, 2016. | | https://technet.microsoft.com/en-us/itpro/windows/keep-secure/how-user-account-control-works |
| SANS UAC Bypass | undefined | | Medin, T. (2013, August 8). PsExec UAC Bypass. Retrieved June 3, 2016. | | http://pen-testing.sans.org/blog/pen-testing/2013/08/08/psexec-uac-bypass |
| MSDN COM Elevation | undefined | | Microsoft. (n.d.). The COM Elevation Moniker. Retrieved July 26, 2016. | | https://msdn.microsoft.com/en-us/library/ms679687.aspx |
| enigma0x3 Fileless UAC Bypass | undefined | | Nelson, M. (2016, August 15). "Fileless" UAC Bypass using eventvwr.exe and Registry Hijacking. Retrieved December 27, 2016. | | https://enigma0x3.net/2016/08/15/fileless-uac-bypass-using-eventvwr-exe-and-registry-hijacking/ |
| enigma0x3 sdclt app paths | undefined | | Nelson, M. (2017, March 14). Bypassing UAC using App Paths. Retrieved May 25, 2017. | | https://enigma0x3.net/2017/03/14/bypassing-uac-using-app-paths/ |
| enigma0x3 sdclt bypass | undefined | | Nelson, M. (2017, March 17). "Fileless" UAC Bypass Using sdclt.exe. Retrieved May 25, 2017. | | https://enigma0x3.net/2017/03/17/fileless-uac-bypass-using-sdclt-exe/ |
| TechNet Inside UAC | undefined | | Russinovich, M. (2009, July). User Account Control: Inside Windows 7 User Account Control. Retrieved July 26, 2016. | | https://technet.microsoft.com/en-US/magazine/2009.07.uac.aspx |
| Fortinet Fareit | undefined | | Salvio, J., Joven, R. (2016, December 16). Malicious Macro Bypasses UAC to Elevate Privilege for Fareit Malware. Retrieved December 27, 2016. | | https://blog.fortinet.com/2016/12/16/malicious-macro-bypasses-uac-to-elevate-privilege-for-fareit-malware |
| Github UACMe | undefined | | UACME Project. (2016, June 16). UACMe. Retrieved July 26, 2016. | | https://github.com/hfiref0x/UACME |
| **EXECUTION FLOWS** | | | | | | |
| BlackEnergy | [BlackEnergy](https://attack.mitre.org/software/S0089) attempts to bypass default User Access Control (UAC) settings by exploiting a backward-compatibility setting found in Windows 7 and later.(Citation: F-Secure BlackEnergy 2014)  [BlackEnergy](https://attack.mitre.org/software/S0089) is a malware toolkit that has been used by both criminal and APT actors. It dates back to at least 2007 and was originally designed to create botnets for use in conducting Distributed Denial of Service (DDoS) attacks, but its use has evolved to support various plug-ins. It is well known for being used during the confrontation between Georgia and Russia in 2008, as well as in targeting Ukrainian institutions. Variants include BlackEnergy 2 and BlackEnergy 3. (Citation: F-Secure BlackEnergy 2014) | | | | | |
| RTM | [RTM](https://attack.mitre.org/software/S0148) can attempt to run the program as admin, then show a fake error message and a legitimate UAC bypass prompt to the user in an attempt to socially engineer the user into escalating privileges.(Citation: ESET RTM Feb 2017)  [RTM](https://attack.mitre.org/software/S0148) is custom malware written in Delphi. It is used by the group of the same name ([RTM](https://attack.mitre.org/software/S0148)). Newer versions of the malware have been reported publicly as Redaman.(Citation: ESET RTM Feb 2017)(Citation: Unit42 Redaman January 2019) | | | | | |
| Cobalt Strike | [Cobalt Strike](https://attack.mitre.org/software/S0154) can use a number of known techniques to bypass Windows UAC.(Citation: cobaltstrike manual)(Citation: Cobalt Strike Manual 4.3 November 2020)  [Cobalt Strike](https://attack.mitre.org/software/S0154) is a commercial, full-featured, remote access tool that bills itself as “adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors”. Cobalt Strike’s interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system.(Citation: cobaltstrike manual) In addition to its own capabilities, [Cobalt Strike](https://attack.mitre.org/software/S0154) leverages the capabilities of other well-known tools such as Metasploit and [Mimikatz](https://attack.mitre.org/software/S0002).(Citation: cobaltstrike manual) | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **TECHNIQUE** | | | | | | |
| [3.2.0] Cached Domain Credentials | | | | | | |
| **DETAILS** | | | | | | |
| Adversaries may attempt to access cached domain credentials used to allow authentication to occur in the event a domain controller is unavailable.(Citation: Microsoft - Cached Creds) On Windows Vista and newer, the hash format is DCC2 (Domain Cached Credentials version 2) hash, also known as MS-Cache v2 hash.(Citation: PassLib mscache) The number of default cached credentials varies and can be altered per system. This hash does not allow pass-the-hash style attacks, and instead requires [Password Cracking](https://attack.mitre.org/techniques/T1110/002) to recover the plaintext password.(Citation: ired mscache) With SYSTEM access, the tools/utilities such as [Mimikatz](https://attack.mitre.org/software/S0002), [Reg](https://attack.mitre.org/software/S0075), and secretsdump.py can be used to extract the cached credentials. Note: Cached credentials for Windows Vista are derived using PBKDF2.(Citation: PassLib mscache) | | | | | | |
| **MITRE ATT&CK REFERENCES** | | | | | | |
| **Domain** | Enterprise | | | | | |
| **Tactics** | Credential Access | | | | | |
| **Spec. Version** | 3.2.0 | | | | | |
| **Kill Chain Phases** | **Kill Chain Name** | | **Phase Name** | | | |
| 1. mitre-attack | | Credential Access | | | |
| **Platforms** | Windows | | | | | |
| **Data Sources** | * Command: Command Execution | | | | | |
| **Detections** | **Data Source** | | **Data Component** | | **Detects** | |
| 1. General | | General | | Monitor processes and command-line arguments for program execution that may be indicative of credential dumping. Remote access tools may contain built-in features or incorporate existing tools like Mimikatz. PowerShell scripts also exist that contain credential dumping functionality, such as PowerSploit's Invoke-Mimikatz module,(Citation: Powersploit) which may require additional logging features to be configured in the operating system to collect necessary information for analysis.  Detection of compromised [Valid Accounts](https://attack.mitre.org/techniques/T1078) in-use by adversaries may help as well. | |
| 1. Command | | Command Execution | | Monitor executed commands and arguments that may attempt to access cached domain credentials used to allow authentication to occur in the event a domain controller is unavailable.(Citation: Microsoft - Cached Creds). Remote access tools may contain built-in features or incorporate existing tools like Mimikatz. PowerShell scripts also exist that contain credential dumping functionality, such as PowerSploit's Invoke-Mimikatz module,(Citation: Powersploit) which may require additional logging features to be configured in the operating system to collect necessary information for analysis. Detection of compromised [Valid Accounts](https://attack.mitre.org/techniques/T1078) in-use by adversaries may help as well. | |
| **Mitigations** | **Mitigation** | | **Description** | | | |
| Active Directory Configuration | | Consider adding users to the "Protected Users" Active Directory security group. This can help limit the caching of users' plaintext credentials.(Citation: Microsoft Protected Users Security Group) | | | |
| User Training | | Limit credential overlap across accounts and systems by training users and administrators not to use the same password for multiple accounts. | | | |
| Password Policies | | Ensure that local administrator accounts have complex, unique passwords across all systems on the network. | | | |
| Operating System Configuration | | Consider limiting the number of cached credentials (HKLM\SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon\cachedlogonscountvalue)(Citation: Tilbury Windows Credentials) | | | |
| Privileged Account Management | | Do not put user or admin domain accounts in the local administrator groups across systems unless they are tightly controlled, as this is often equivalent to having a local administrator account with the same password on all systems. Follow best practices for design and administration of an enterprise network to limit privileged account use across administrative tiers. | | | |
| **External References** | **Name** | **Id** | | **Description** | | **URL** |
| mitre-attack | T1003.005 | | undefined | | https://attack.mitre.org/techniques/T1003/005 |
| PassLib mscache | undefined | | Eli Collins. (2016, November 25). Windows' Domain Cached Credentials v2. Retrieved February 21, 2020. | | https://passlib.readthedocs.io/en/stable/lib/passlib.hash.msdcc2.html |
| ired mscache | undefined | | Mantvydas Baranauskas. (2019, November 16). Dumping and Cracking mscash - Cached Domain Credentials. Retrieved February 21, 2020. | | https://ired.team/offensive-security/credential-access-and-credential-dumping/dumping-and-cracking-mscash-cached-domain-credentials |
| Microsoft - Cached Creds | undefined | | Microsoft. (2016, August 21). Cached and Stored Credentials Technical Overview. Retrieved February 21, 2020. | | https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh994565(v%3Dws.11) |
| Powersploit | undefined | | PowerSploit. (n.d.). Retrieved December 4, 2014. | | https://github.com/mattifestation/PowerSploit |
| **EXECUTION FLOWS** | | | | | | |
| Okrum | [Okrum](https://attack.mitre.org/software/S0439) was seen using modified Quarks PwDump to perform credential dumping.(Citation: ESET Okrum July 2019)  [Okrum](https://attack.mitre.org/software/S0439) is a Windows backdoor that has been seen in use since December 2016 with strong links to [Ke3chang](https://attack.mitre.org/groups/G0004).(Citation: ESET Okrum July 2019) | | | | | |
| APT33 | [APT33](https://attack.mitre.org/groups/G0064) has used a variety of publicly available tools like [LaZagne](https://attack.mitre.org/software/S0349) to gather credentials.(Citation: Symantec Elfin Mar 2019)(Citation: FireEye APT33 Guardrail)  [APT33](https://attack.mitre.org/groups/G0064) is a suspected Iranian threat group that has carried out operations since at least 2013. The group has targeted organizations across multiple industries in the United States, Saudi Arabia, and South Korea, with a particular interest in the aviation and energy sectors. (Citation: FireEye APT33 Sept 2017) (Citation: FireEye APT33 Webinar Sept 2017) | | | | | |
| Leafminer | [Leafminer](https://attack.mitre.org/groups/G0077) used several tools for retrieving login and password information, including LaZagne.(Citation: Symantec Leafminer July 2018)  [Leafminer](https://attack.mitre.org/groups/G0077) is an Iranian threat group that has targeted government organizations and business entities in the Middle East since at least early 2017. (Citation: Symantec Leafminer July 2018) | | | | | |
| Cachedump | [Cachedump](https://attack.mitre.org/software/S0119) can extract cached password hashes from cache entry information.(Citation: Mandiant APT1)  [Cachedump](https://attack.mitre.org/software/S0119) is a publicly-available tool that program extracts cached password hashes from a system’s registry. (Citation: Mandiant APT1) | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **TECHNIQUE** | | | | | | |
| [2.1.0] ARP Cache Poisoning | | | | | | |
| **DETAILS** | | | | | | |
| Adversaries may poison Address Resolution Protocol (ARP) caches to position themselves between the communication of two or more networked devices. This activity may be used to enable follow-on behaviors such as [Network Sniffing](https://attack.mitre.org/techniques/T1040) or [Transmitted Data Manipulation](https://attack.mitre.org/techniques/T1565/002). The ARP protocol is used to resolve IPv4 addresses to link layer addresses, such as a media access control (MAC) address.(Citation: RFC826 ARP) Devices in a local network segment communicate with each other by using link layer addresses. If a networked device does not have the link layer address of a particular networked device, it may send out a broadcast ARP request to the local network to translate the IP address to a MAC address. The device with the associated IP address directly replies with its MAC address. The networked device that made the ARP request will then use as well as store that information in its ARP cache. An adversary may passively wait for an ARP request to poison the ARP cache of the requesting device. The adversary may reply with their MAC address, thus deceiving the victim by making them believe that they are communicating with the intended networked device. For the adversary to poison the ARP cache, their reply must be faster than the one made by the legitimate IP address owner. Adversaries may also send a gratuitous ARP reply that maliciously announces the ownership of a particular IP address to all the devices in the local network segment. The ARP protocol is stateless and does not require authentication. Therefore, devices may wrongly add or update the MAC address of the IP address in their ARP cache.(Citation: Sans ARP Spoofing Aug 2003)(Citation: Cylance Cleaver) Adversaries may use ARP cache poisoning as a means to intercept network traffic. This activity may be used to collect and/or relay data such as credentials, especially those sent over an insecure, unencrypted protocol.(Citation: Sans ARP Spoofing Aug 2003) | | | | | | |
| **MITRE ATT&CK REFERENCES** | | | | | | |
| **Domain** | Enterprise | | | | | |
| **Tactics** | Credential Access, Collection | | | | | |
| **Spec. Version** | 2.1.0 | | | | | |
| **Kill Chain Phases** | **Kill Chain Name** | | **Phase Name** | | | |
| 1. mitre-attack | | Credential Access | | | |
| 1. mitre-attack | | Collection | | | |
| **Platforms** | Linux, Windows, macOS | | | | | |
| **Data Sources** | * Network Traffic: Network Traffic Content * Network Traffic: Network Traffic Flow | | | | | |
| **Detections** | **Data Source** | | **Data Component** | | **Detects** | |
| 1. General | | General | | Monitor network traffic for unusual ARP traffic, gratuitous ARP replies may be suspicious.   Consider collecting changes to ARP caches across endpoints for signs of ARP poisoning. For example, if multiple IP addresses map to a single MAC address, this could be an indicator that the ARP cache has been poisoned. | |
| 1. Network Traffic | | Network Traffic Content | | Monitor network traffic for unusual ARP traffic, gratuitous ARP replies may be suspicious. Consider collecting changes to ARP caches across endpoints for signs of ARP poisoning. For example, if multiple IP addresses map to a single MAC address, this could be an indicator that the ARP cache has been poisoned. | |
| 1. Network Traffic | | Network Traffic Flow | | Monitor for network traffic originating from unknown/unexpected hardware devices. Local network traffic metadata (such as source MAC addressing) as well as usage of network management protocols such as DHCP may be helpful in identifying hardware. | |
| **Mitigations** | **Mitigation** | | **Description** | | | |
| Encrypt Sensitive Information | | Ensure that all wired and/or wireless traffic is encrypted appropriately. Use best practices for authentication protocols, such as Kerberos, and ensure web traffic that may contain credentials is protected by SSL/TLS. | | | |
| Network Intrusion Prevention | | Network intrusion detection and prevention systems that can identify traffic patterns indicative of AiTM activity can be used to mitigate activity at the network level. | | | |
| User Training | | Train users to be suspicious about certificate errors. Adversaries may use their own certificates in an attempt to intercept HTTPS traffic. Certificate errors may arise when the application’s certificate does not match the one expected by the host. | | | |
| Disable or Remove Feature or Program | | Consider disabling updating the ARP cache on gratuitous ARP replies. | | | |
| Limit Access to Resource Over Network | | Create static ARP entries for networked devices. Implementing static ARP entries may be infeasible for large networks. | | | |
| Filter Network Traffic | | Consider enabling DHCP Snooping and Dynamic ARP Inspection on switches to create mappings between IP addresses requested via DHCP and ARP tables and tie the values to a port on the switch that may block bogus traffic.(Citation: Cisco ARP Poisoning Mitigation 2016)(Citation: Juniper DAI 2020) | | | |
| **External References** | **Name** | **Id** | | **Description** | | **URL** |
| mitre-attack | T1557.002 | | undefined | | https://attack.mitre.org/techniques/T1557/002 |
| Cylance Cleaver | undefined | | Cylance. (2014, December). Operation Cleaver. Retrieved September 14, 2017. | | https://web.archive.org/web/20200302085133/https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance\_Operation\_Cleaver\_Report.pdf |
| RFC826 ARP | undefined | | Plummer, D. (1982, November). An Ethernet Address Resolution Protocol. Retrieved October 15, 2020. | | https://tools.ietf.org/html/rfc826 |
| Sans ARP Spoofing Aug 2003 | undefined | | Siles, R. (2003, August). Real World ARP Spoofing. Retrieved October 15, 2020. | | https://pen-testing.sans.org/resources/papers/gcih/real-world-arp-spoofing-105411 |
| **EXECUTION FLOWS** | | | | | | |
| Cleaver | [Cleaver](https://attack.mitre.org/groups/G0003) has used custom tools to facilitate ARP cache poisoning.(Citation: Cylance Cleaver)  [Cleaver](https://attack.mitre.org/groups/G0003) is a threat group that has been attributed to Iranian actors and is responsible for activity tracked as Operation Cleaver. (Citation: Cylance Cleaver) Strong circumstantial evidence suggests Cleaver is linked to Threat Group 2889 (TG-2889). (Citation: Dell Threat Group 2889) | | | | | |
| LuminousMoth | [LuminousMoth](https://attack.mitre.org/groups/G1014) has used ARP spoofing to redirect a compromised machine to an actor-controlled website.(Citation: Bitdefender LuminousMoth July 2021)  [LuminousMoth](https://attack.mitre.org/groups/G1014) is a Chinese-speaking cyber espionage group that has been active since at least October 2020. [LuminousMoth](https://attack.mitre.org/groups/G1014) has targeted high-profile organizations, including government entities, in Myanmar, the Philippines, Thailand, and other parts of Southeast Asia. Some security researchers have concluded there is a connection between [LuminousMoth](https://attack.mitre.org/groups/G1014) and [Mustang Panda](https://attack.mitre.org/groups/G0129) based on similar targeting and TTPs, as well as network infrastructure overlaps.(Citation: Kaspersky LuminousMoth July 2021)(Citation: Bitdefender LuminousMoth July 2021) | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **TECHNIQUE** | | | | | | |
| [2.1.0] Automated Collection | | | | | | |
| **DETAILS** | | | | | | |
| Once established within a system or network, an adversary may use automated techniques for collecting internal data. Methods for performing this technique could include use of a [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059) to search for and copy information fitting set criteria such as file type, location, or name at specific time intervals. In cloud-based environments, adversaries may also use cloud APIs, command line interfaces, or extract, transform, and load (ETL) services to automatically collect data. This functionality could also be built into remote access tools. This technique may incorporate use of other techniques such as [File and [Directory Discovery](https://attack.mitre.org/techniques/T1083) and [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570) to identify and move files, as well as [Cloud Service Dashboard](https://attack.mitre.org/techniques/T1538) and [Cloud Storage Object Discovery](https://attack.mitre.org/techniques/T1619) to identify resources in cloud environments. | | | | | | |
| **MITRE ATT&CK REFERENCES** | | | | | | |
| **Domain** | Enterprise | | | | | |
| **Tactics** | Collection | | | | | |
| **Spec. Version** | 2.1.0 | | | | | |
| **Kill Chain Phases** | **Kill Chain Name** | | **Phase Name** | | | |
| 1. mitre-attack | | Collection | | | |
| **Platforms** | Linux, macOS, Windows, IaaS, SaaS | | | | | |
| **Data Sources** | * Command: Command Execution * File: File Access * Script: Script Execution | | | | | |
| **Detections** | **Data Source** | | **Data Component** | | **Detects** | |
| 1. General | | General | | Depending on the method used, actions could include common file system commands and parameters on the command-line interface within batch files or scripts. A sequence of actions like this may be unusual, depending on the system and network environment. Automated collection may occur along with other techniques such as [Data Staged](https://attack.mitre.org/techniques/T1074). As such, file access monitoring that shows an unusual process performing sequential file opens and potentially copy actions to another location on the file system for many files at once may indicate automated collection behavior. Remote access tools with built-in features may interact directly with the Windows API to gather data. Data may also be acquired through Windows system management tools such as [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047) and [PowerShell](https://attack.mitre.org/techniques/T1059/001), as well as through cloud APIs and command line interfaces. | |
| 1. Command | | Command Execution | | Monitor executed commands and arguments for actions that could be taken to collect internal data. | |
| 1. File | | File Access | | Monitor for unexpected files (e.g., .pdf, .docx, .jpg, etc.) viewed for collecting internal data. | |
| 1. Script | | Script Execution | | Monitor for any attempts to enable scripts running on a system would be considered suspicious. If scripts are not commonly used on a system, but enabled, scripts running out of cycle from patching or other administrator functions are suspicious. Scripts should be captured from the file system when possible to determine their actions and intent. | |
| **Mitigations** | **Mitigation** | | **Description** | | | |
| Remote Data Storage | | Encryption and off-system storage of sensitive information may be one way to mitigate collection of files, but may not stop an adversary from acquiring the information if an intrusion persists over a long period of time and the adversary is able to discover and access the data through other means. | | | |
| Encrypt Sensitive Information | | Encryption and off-system storage of sensitive information may be one way to mitigate collection of files, but may not stop an adversary from acquiring the information if an intrusion persists over a long period of time and the adversary is able to discover and access the data through other means. Strong passwords should be used on certain encrypted documents that use them to prevent offline cracking through [Brute Force](https://attack.mitre.org/techniques/T1110) techniques. | | | |
| **External References** | **Name** | **Id** | | **Description** | | **URL** |
| mitre-attack | T1119 | | undefined | | https://attack.mitre.org/techniques/T1119 |
| **EXECUTION FLOWS** | | | | | | |
| T9000 | [T9000](https://attack.mitre.org/software/S0098) searches removable storage devices for files with a pre-defined list of file extensions (e.g. \* .doc, \*.ppt, \*.xls, \*.docx, \*.pptx, \*.xlsx). Any matching files are encrypted and written to a local user directory.(Citation: Palo Alto T9000 Feb 2016)  [T9000](https://attack.mitre.org/software/S0098) is a backdoor that is a newer variant of the T5000 malware family, also known as Plat1. Its primary function is to gather information about the victim. It has been used in multiple targeted attacks against U.S.-based organizations. (Citation: FireEye admin@338 March 2014) (Citation: Palo Alto T9000 Feb 2016) | | | | | |
| Rover | [Rover](https://attack.mitre.org/software/S0090) automatically collects files from the local system and removable drives based on a predefined list of file extensions on a regular timeframe.(Citation: Palo Alto Rover)  [Rover](https://attack.mitre.org/software/S0090) is malware suspected of being used for espionage purposes. It was used in 2015 in a targeted email sent to an Indian Ambassador to Afghanistan. (Citation: Palo Alto Rover) | | | | | |
| Micropsia | [Micropsia](https://attack.mitre.org/software/S0339) executes an RAR tool to recursively archive files based on a predefined list of file extensions (\*.xls, \*.xlsx, \*.csv, \*.odt, \*.doc, \*.docx, \*.ppt, \*.pptx, \*.pdf, \*.mdb, \*.accdb, \*.accde, \*.txt).(Citation: Radware Micropsia July 2018)  [Micropsia](https://attack.mitre.org/software/S0339) is a remote access tool written in Delphi.(Citation: Talos Micropsia June 2017)(Citation: Radware Micropsia July 2018) | | | | | |
| ccf32 | [ccf32](https://attack.mitre.org/software/S1043) can be used to automatically collect files from a compromised host.(Citation: Bitdefender FunnyDream Campaign November 2020)  [ccf32](https://attack.mitre.org/software/S1043) is data collection malware that has been used since at least February 2019, most notably during the [FunnyDream](https://attack.mitre.org/campaigns/C0007) campaign; there is also a similar x64 version.(Citation: Bitdefender FunnyDream Campaign November 2020) | | | | | |
| Gamaredon Group | [Gamaredon Group](https://attack.mitre.org/groups/G0047) has deployed scripts on compromised systems that automatically scan for interesting documents.(Citation: ESET Gamaredon June 2020)  [Gamaredon Group](https://attack.mitre.org/groups/G0047) is a suspected Russian cyber espionage threat group that has targeted military, NGO, judiciary, law enforcement, and non-profit organizations in Ukraine since at least 2013. The name [Gamaredon Group](https://attack.mitre.org/groups/G0047) comes from a misspelling of the word "Armageddon", which was detected in the adversary's early campaigns.(Citation: Palo Alto Gamaredon Feb 2017)(Citation: TrendMicro Gamaredon April 2020)(Citation: ESET Gamaredon June 2020)(Citation: Symantec Shuckworm January 2022)(Citation: Microsoft Actinium February 2022) In November 2021, the Ukrainian government publicly attributed [Gamaredon Group](https://attack.mitre.org/groups/G0047) to Russia's Federal Security Service (FSB) Center 18.(Citation: Bleepingcomputer Gamardeon FSB November 2021)(Citation: Microsoft Actinium February 2022) | | | | | |
| Comnie | [Comnie](https://attack.mitre.org/software/S0244) executes a batch script to store discovery information in %TEMP%\info.dat and then uploads the temporarily file to the remote C2 server.(Citation: Palo Alto Comnie)  [Comnie](https://attack.mitre.org/software/S0244) is a remote backdoor which has been used in attacks in East Asia. (Citation: Palo Alto Comnie) | | | | | |
| Operation Wocao | During [Operation Wocao](https://attack.mitre.org/campaigns/C0014), threat actors used a script to collect information about the infected system.(Citation: FoxIT Wocao December 2019)  [Operation Wocao](https://attack.mitre.org/campaigns/C0014) was a cyber espionage campaign that targeted organizations around the world, including in Brazil, China, France, Germany, Italy, Mexico, Portugal, Spain, the United Kingdom, and the United States. The suspected China-based actors compromised government organizations and managed service providers, as well as aviation, construction, energy, finance, health care, insurance, offshore engineering, software development, and transportation companies.(Citation: FoxIT Wocao December 2019) Security researchers assessed the [Operation Wocao](https://attack.mitre.org/campaigns/C0014) actors used similar TTPs and tools as APT20, suggesting a possible overlap. [Operation Wocao](https://attack.mitre.org/campaigns/C0014) was named after an observed command line entry by one of the threat actors, possibly out of frustration from losing webshell access.(Citation: FoxIT Wocao December 2019) | | | | | |
| ROADTools | [ROADTools](https://attack.mitre.org/software/S0684) automatically gathers data from Azure AD environments using the Azure Graph API.(Citation: Roadtools)  [ROADTools](https://attack.mitre.org/software/S0684) is a framework for enumerating Azure Active Directory environments. The tool is written in Python and publicly available on GitHub.(Citation: ROADtools Github) | | | | | |
| NETWIRE | [NETWIRE](https://attack.mitre.org/software/S0198) can automatically archive collected data.(Citation: Red Canary NETWIRE January 2020)  [NETWIRE](https://attack.mitre.org/software/S0198) is a publicly available, multiplatform remote administration tool (RAT) that has been used by criminal and APT groups since at least 2012.(Citation: FireEye APT33 Sept 2017)(Citation: McAfee Netwire Mar 2015)(Citation: FireEye APT33 Webinar Sept 2017) | | | | | |
| PoshC2 | [PoshC2](https://attack.mitre.org/software/S0378) contains a module for recursively parsing through files and directories to gather valid credit card numbers.(Citation: GitHub PoshC2)  [PoshC2](https://attack.mitre.org/software/S0378) is an open source remote administration and post-exploitation framework that is publicly available on GitHub. The server-side components of the tool are primarily written in Python, while the implants are written in [PowerShell](https://attack.mitre.org/techniques/T1059/001). Although [PoshC2](https://attack.mitre.org/software/S0378) is primarily focused on Windows implantation, it does contain a basic Python dropper for Linux/macOS.(Citation: GitHub PoshC2) | | | | | |
| PoetRAT | [PoetRAT](https://attack.mitre.org/software/S0428) used file system monitoring to track modification and enable automatic exfiltration.(Citation: Talos PoetRAT April 2020)  [PoetRAT](https://attack.mitre.org/software/S0428) is a remote access trojan (RAT) that was first identified in April 2020. [PoetRAT](https://attack.mitre.org/software/S0428) has been used in multiple campaigns against the private and public sectors in Azerbaijan, including ICS and SCADA systems in the energy sector. The STIBNITE activity group has been observed using the malware. [PoetRAT](https://attack.mitre.org/software/S0428) derived its name from references in the code to poet William Shakespeare. (Citation: Talos PoetRAT April 2020)(Citation: Talos PoetRAT October 2020)(Citation: Dragos Threat Report 2020) | | | | | |
| Empire | [Empire](https://attack.mitre.org/software/S0363) can automatically gather the username, domain name, machine name, and other information from a compromised system.(Citation: Talos Frankenstein June 2019)  [Empire](https://attack.mitre.org/software/S0363) is an open source, cross-platform remote administration and post-exploitation framework that is publicly available on GitHub. While the tool itself is primarily written in Python, the post-exploitation agents are written in pure [PowerShell](https://attack.mitre.org/techniques/T1059/001) for Windows and Python for Linux/macOS. [Empire](https://attack.mitre.org/software/S0363) was one of five tools singled out by a joint report on public hacking tools being widely used by adversaries.(Citation: NCSC Joint Report Public Tools)(Citation: Github PowerShell Empire)(Citation: GitHub ATTACK Empire) | | | | | |
| APT1 | [APT1](https://attack.mitre.org/groups/G0006) used a batch script to perform a series of discovery techniques and saves it to a text file.(Citation: Mandiant APT1)  [APT1](https://attack.mitre.org/groups/G0006) is a Chinese threat group that has been attributed to the 2nd Bureau of the People’s Liberation Army (PLA) General Staff Department’s (GSD) 3rd Department, commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398. (Citation: Mandiant APT1) | | | | | |
| Proxysvc | [Proxysvc](https://attack.mitre.org/software/S0238) automatically collects data about the victim and sends it to the control server.(Citation: McAfee GhostSecret)  [Proxysvc](https://attack.mitre.org/software/S0238) is a malicious DLL used by [Lazarus Group](https://attack.mitre.org/groups/G0032) in a campaign known as Operation GhostSecret. It has appeared to be operating undetected since 2017 and was mostly observed in higher education organizations. The goal of [Proxysvc](https://attack.mitre.org/software/S0238) is to deliver additional payloads to the target and to maintain control for the attacker. It is in the form of a DLL that can also be executed as a standalone process. (Citation: McAfee GhostSecret) | | | | | |
| BADNEWS | [BADNEWS](https://attack.mitre.org/software/S0128) monitors USB devices and copies files with certain extensions to a predefined directory.(Citation: TrendMicro Patchwork Dec 2017)  [BADNEWS](https://attack.mitre.org/software/S0128) is malware that has been used by the actors responsible for the [Patchwork](https://attack.mitre.org/groups/G0040) campaign. Its name was given due to its use of RSS feeds, forums, and blogs for command and control. (Citation: Forcepoint Monsoon) (Citation: TrendMicro Patchwork Dec 2017) | | | | | |
| TajMahal | [TajMahal](https://attack.mitre.org/software/S0467) has the ability to index and compress files into a send queue for exfiltration.(Citation: Kaspersky TajMahal April 2019)  [TajMahal](https://attack.mitre.org/software/S0467) is a multifunctional spying framework that has been in use since at least 2014. [TajMahal](https://attack.mitre.org/software/S0467) is comprised of two separate packages, named Tokyo and Yokohama, and can deploy up to 80 plugins.(Citation: Kaspersky TajMahal April 2019) | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **TECHNIQUE** | | | | | | |
| [2.1.0] Automated Exfiltration | | | | | | |
| **DETAILS** | | | | | | |
| Adversaries may exfiltrate data, such as sensitive documents, through the use of automated processing after being gathered during Collection. When automated exfiltration is used, other exfiltration techniques likely apply as well to transfer the information out of the network, such as [Exfiltration Over C2 Channel](https://attack.mitre.org/techniques/T1041) and [Exfiltration Over Alternative Protocol](https://attack.mitre.org/techniques/T1048). | | | | | | |
| **MITRE ATT&CK REFERENCES** | | | | | | |
| **Domain** | Enterprise | | | | | |
| **Tactics** | Exfiltration | | | | | |
| **Spec. Version** | 2.1.0 | | | | | |
| **Kill Chain Phases** | **Kill Chain Name** | | **Phase Name** | | | |
| 1. mitre-attack | | Exfiltration | | | |
| **Platforms** | Linux, macOS, Windows, Network | | | | | |
| **Data Sources** | * Command: Command Execution * Network Traffic: Network Traffic Flow * File: File Access * Network Traffic: Network Connection Creation * Network Traffic: Network Traffic Content * Script: Script Execution | | | | | |
| **Detections** | **Data Source** | | **Data Component** | | **Detects** | |
| 1. General | | General | | Monitor process file access patterns and network behavior. Unrecognized processes or scripts that appear to be traversing file systems and sending network traffic may be suspicious. | |
| 1. Command | | Command Execution | | Monitor executed commands and arguments that may exfiltrate data, such as sensitive documents, through the use of automated processing after being gathered during Collection | |
| 1. Network Traffic | | Network Traffic Flow | | Monitor and analyze network flows associated to protocol(s) that do not follow the expected protocol standards and traffic flows (e.g extraneous packets that do not belong to established flows, or gratuitous or anomalous traffic patterns). Consider analyzing newly constructed network connections that are sent or received by untrusted hosts, unexpected hardware devices, or other uncommon data flows. | |
| 1. File | | File Access | | Monitor for abnormal access to files (i.e. .pdf, .docx, .jpg, etc.), especially sensitive documents, through the use of automated processing after being gathered during Collection. | |
| 1. Network Traffic | | Network Connection Creation | | Monitor for newly constructed network connections associated with processes performing collection activity, especially those involving abnormal/untrusted hosts. | |
| 1. Network Traffic | | Network Traffic Content | | Monitor network traffic content for evidence of data exfiltration, such as gratuitous or anomalous outbound traffic containing collected data. Consider correlation with process monitoring and command lines associated with collection and exfiltration. | |
| 1. Script | | Script Execution | | Monitor for any attempts to enable scripts running on a system would be considered suspicious. If scripts are not commonly used on a system, but enabled, scripts running out of cycle from patching or other administrator functions are suspicious. Scripts should be captured from the file system when possible to determine their actions and intent. | |
| **External References** | **Name** | **Id** | | **Description** | | **URL** |
| mitre-attack | T1020 | | undefined | | https://attack.mitre.org/techniques/T1020 |
| **EXECUTION FLOWS** | | | | | | |
| StrongPity | [StrongPity](https://attack.mitre.org/software/S0491) can automatically exfiltrate collected documents to the C2 server.(Citation: Talos Promethium June 2020)(Citation: Bitdefender StrongPity June 2020)  [StrongPity](https://attack.mitre.org/software/S0491) is an information stealing malware used by [PROMETHIUM](https://attack.mitre.org/groups/G0056).(Citation: Bitdefender StrongPity June 2020)(Citation: Talos Promethium June 2020) | | | | | |
| LightNeuron | [LightNeuron](https://attack.mitre.org/software/S0395) can be configured to automatically exfiltrate files under a specified directory.(Citation: ESET LightNeuron May 2019)  [LightNeuron](https://attack.mitre.org/software/S0395) is a sophisticated backdoor that has targeted Microsoft Exchange servers since at least 2014. [LightNeuron](https://attack.mitre.org/software/S0395) has been used by [Turla](https://attack.mitre.org/groups/G0010) to target diplomatic and foreign affairs-related organizations. The presence of certain strings in the malware suggests a Linux variant of [LightNeuron](https://attack.mitre.org/software/S0395) exists.(Citation: ESET LightNeuron May 2019) | | | | | |
| Frankenstein | During [Frankenstein](https://attack.mitre.org/campaigns/C0001), the threat actors collected information via [Empire](https://attack.mitre.org/software/S0363), which was automatically sent back to the adversary's C2.(Citation: Talos Frankenstein June 2019)  [Frankenstein](https://attack.mitre.org/campaigns/C0001) was described by security researchers as a highly-targeted campaign conducted by moderately sophisticated and highly resourceful threat actors in early 2019. The unidentified actors primarily relied on open source tools, including [Empire](https://attack.mitre.org/software/S0363). The campaign name refers to the actors' ability to piece together several unrelated open-source tool components.(Citation: Talos Frankenstein June 2019) | | | | | |

# **VULNERABILITIES**

|  |  |
| --- | --- |
| **VULNERABILITY** | |
| **PRIORITY** | **High** |
| **TITLE** | Hosts Respond with Hashes/Challenge-Responses to Spoofed Hostnames |
| **CVSSv3** | Base: **8.1**  Temporal: **8.1**  Environmental: **8.1**  Vector: **CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N** |
| **DESCRIPTION** | During the assessment, it was discovered that hosts within the internal network utilised either **LLMNR, NBT-NS** or both to discover hosts on the network that aren't listed by the DNS server. This functionality allows an attacker to capture valid password hashes/challenge-responses and usernames that can be reused to connect to hosts or conduct a password cracking attack. |
| **ATTACK SCENARIO** | If an attacker can position themselves on an internal network segment and respond to requests from hosts that are looking for other hosts not listed by the DNS server, they will then receive the hash or challenge-response and username of the person using that host.  image Figure 8  The attacker then uses a Pass-The-Hash type attack to connect to hosts within the network in the event that NTLM hashes are captured, alternatively, if NTLMv1 or NTLMv2 hashes are captured, a password cracking attack is conducted and recovered credentials are used to connect to hosts either using psexec or RDP. |
| **REMEDIATION ADVICE** | Disable LLMNR and NBT-NS which prevent hosts from being able to broadcast other hosts that they are looking for. If this does not happen, a malicious attacker cannot respond to requests for missing hosts and spoof it's identity. |
| **EVIDENCE** | No further evidence. |
| **AFFECTED ASSET** | |
| **STATUS** | **Open** |
| **AFFECTED** | **10.0.0.1/24** |
| **ATTACK NARRATIVE** | For this assessment, attackers were placed on the 10.0.0.1/24 network segment.  This attack was executed from host 10.0.0.55. |
| **REMEDIATION NOTES** | *01/14/2024*  John P. is already working on disabling this.  image Figure 9 |
| **POC** | Run the tool Responder on an active broadcast domain:  image Figure 10  User attempts to search for a share that doesn't exist:  image Figure 11  View the LLMNR request in Responder:  image Figure 12  Get the user’s hashed credentials:  image Figure 13  Crack the hash using a tool such as Hashcat:  image Figure 14 |

**DOCUMENT CONTROL**

|  |  |
| --- | --- |
| **AUTHOR(S)** | Attack Forge |
| **REVIEWER** | Attack Forge |
| **APPROVER** | Attack Forge |

**VERSION HISTORY**

|  |  |  |  |
| --- | --- | --- | --- |
| **VERSION** | **DESCRIPTION** | **DATE** | **STATUS** |
| 0.1 | Initial Draft | 7/5/24 | DRAFT |

**PROJECT TEAM**

|  |  |  |  |
| --- | --- | --- | --- |
| **TEAM MEMBER** | **JOB TITLE** | **EMAIL** | **PROJECT ROLE** |
| Attack Forge | My Job Title | admin@attackforge.com | Pentest Lead |