Apr 14 2024

NETMANAGEIT

Intelligence Report

Zero-Day Exploitation of Unauthenticated Remote Code Execution Vulnerability in GlobalProtect (CVE-2024-3400)

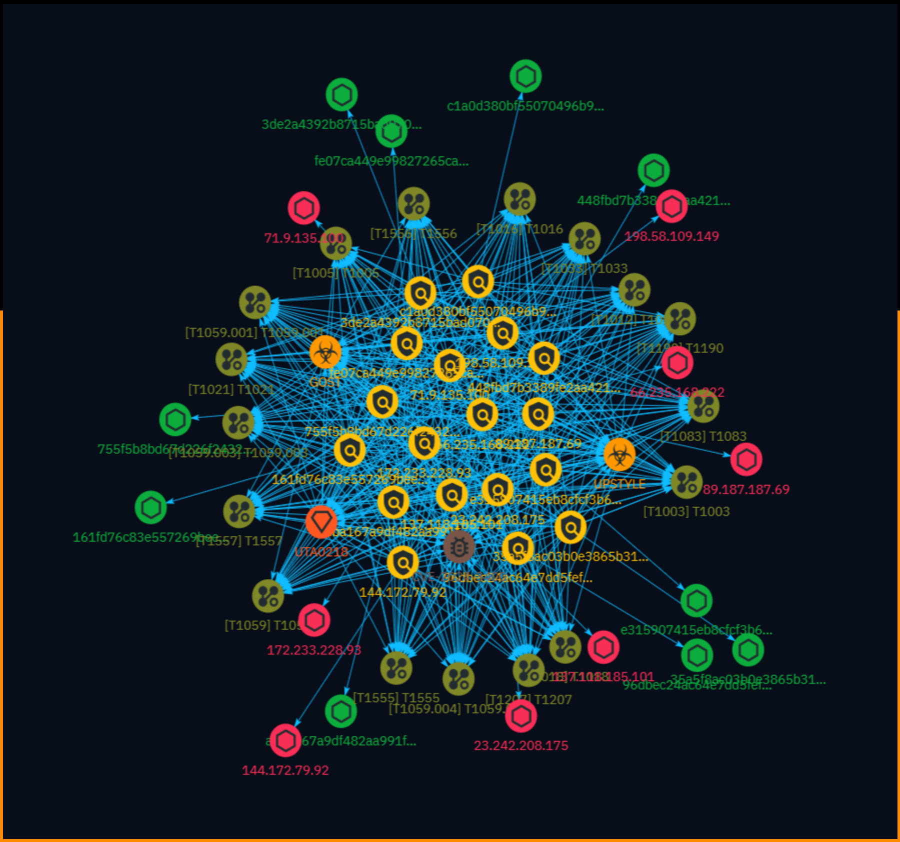

Table of contents

Overview

Entities

Observables

External References

Overview

Description

This report details the discovery and exploitation of a critical zero-day vulnerability (CVE-2024-3400) in Palo Alto Networks GlobalProtect firewall appliances, allowing remote code execution. The threat actor, tracked as UTA0218, exploited this flaw to compromise devices, exfiltrate data, and move laterally within victims' networks. The report analyzes the UPSTYLE backdoor used, post-exploitation activities, infrastructure, detection methods, and response recommendations.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

100 / 100

Content

N/A

Indicator

Name

89.187.187.69

Description

ISP: Datacamp Limited **OS:** - -------------------------- Services: **443:** ``` HTTP/1.1 400 Bad Request Server: squid Mime-Version: 1.0 Date: Tue, 09 Apr 2024 08:53:27 GMT Content-Type: text/html;charset=utf-8 Content-Length: 0 X-Squid-Error: ERR_INVALID_URL 0 X-Cache: MISS from us-lax-v039.prod.surfshark.com X-Cache-Lookup: NONE from us-lax-v039.prod.surfshark.com:443 Connection: close Trailer: S-- ``` HEARTBLEED: 2024/04/09 08:53:32 89.187.187.69:443 - SAFE ------------------ **4000:** ``` HTTP/1.1 400 Bad Request Content-Type: text/plain Connection: close 400 Bad Request ``` ------------------ **6443:** ``` HTTP/1.1 400 Bad Request Server: squid Mime-Version: 1.0 Date: Fri, 29 Mar 2024 23:29:11 GMT Content-Type: text/html;charset=utf-8 Content-Length: 0 X-Squid-Error: ERR_INVALID_URL 0 X-Cache: MISS from us-lax-v039.prod.surfshark.com X-Cache-Lookup: NONE from us-lax-v039.prod.surfshark.com:6443 Connection: close Trailer: S-- ``` HEARTBLEED: 2024/03/29 23:29:29 89.187.187.69:6443 - SAFE ------------------ **28851:** ``` DHT Nodes 56.56.56.56 14392 100.49.58.97 25650 58.105.100.50 12346 245.123.182.126 39840 36.7.56.56 14392 56.56.56.56 13098 114.45.170.237 36466 226.65.25.91 30151 76.206.228.103 14392 56.56.56.56 14392 50.142.114.114 25883 124.26.115.250 6124 117.222.248.114 51200 56.56.56.56 14392 56.56.39.150 37148 230.229.95.110 54926 163.48.117.211 53670 4.3.56.56 14392 56.56.56.56 9160 183.74.184.48 57083 109.190.31.14 29503 10.131.110.249 14392 56.56.56.56 14392 34.178.226.121 34622 233.179.8.101 35535 115.55.74.193 35938 56.56.56.56 14392 56.56.34.165 31431 89.146.165.1 13462 106.103.115.48 38424 252.159.56.56 14392 56.56.56.56 8560 255.178.81.10 26084 65.113.225.219 28924 ``` ------------------ **44106:** ``` DHT Nodes 100.190.213.56 52119 34.126.19.80 8227 209.254.41.193 33471 185.1.94.75 49701 109.100.102.121 64850 152.78.148.217 26909 121.107.235.76 60148 136.46.153.76 13071 182.26.192.186 24578 16.32.39.115 19544 134.239.25.58 35796 181.36.246.91 38530 66.51.170.3 6881 96.59.222.11 32534 63.238.29.163 57842 9.105.122.50 34318 102.107.5.159 59639 26.225.98.90 62605 24.66.232.176 45176 18.2.136.235 11017 162.198.36.27 36252 231.168.26.225 27821 146.71.219.112 2678 235.71.118.159 9365 89.227.84.1 19190

141.101.7.64 8844 109.71.126.117 33874 35.112.252.237 36289 153.169.225.113 52862 72.92.76.23 12265 57.93.109.95 20719 155.247.27.61 7789 69.89.98.201 29659 72.63.83.204 11611 ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '89.187.187.69']

Name

66.235.168.222

Description

ISP: Tier.Net Technologies LLC **OS:** - ------------------------- Services: **443:** ``` HTTP/1.1 400 Bad Request Server: squid Mime-Version: 1.0 Date: Fri, 05 Apr 2024 16:32:02 GMT Content-Type: text/html;charset=utf-8 Content-Length: 0 X-Squid-Error: ERR_INVALID_URL 0 X-Cache: MISS from us-bdn-v022.prod.surfshark.com X-Cache-Lookup: NONE from us-bdn-v022.prod.surfshark.com:443 Connection: close Trailer: S-- ``` HEARTBLEED: 2024/04/05 16:32:29 66.235.168.222:443 - SAFE ------------------ **4000:** ``` HTTP/1.1 400 Bad Request Content-Type: text/plain Connection: close 400 Bad Request ``` ------------------ **6443:** ``` HTTP/1.1 400 Bad Request Server: squid Mime-Version: 1.0 Date: Thu, 04 Apr 2024 14:50:06 GMT Content-Type: text/html;charset=utf-8 Content-Length: 0 X-Squid-Error: ERR_INVALID_URL 0 X-Cache: MISS from us-bdn-v022.prod.surfshark.com X-Cache-Lookup: NONE from us-bdn-v022.prod.surfshark.com:6443 Connection: close Trailer: S-- ``` HEARTBLEED: 2024/04/04 14:50:13 66.235.168.222:6443 - SAFE ------------------ **17633:** ``` DHT Nodes 114.83.129.121 59086 202.155.130.199 28864 215.46.138.5 16398 188.67.222.113 23481 160.56.114.234 13924 52.119.77.178 8223 124.17.40.55 49061 29.91.47.64 21057 182.121.26.233 28730 171.255.51.219 32348 90.51.31.218 32192 46.133.95.244 27671 185.148.0.160 6881 118.24.78.105 29521 255.74.236.41 52666 171.242.251.227 18044 194.103.164.92 45618 26.225.118.142 37595 60.135.12.62 39204 94.13.28.6 46919 222.179.18.179 7986 225.19.209.169 30525 214.30.5.64 28714 75.107.54.64 4666 152.243.173.136 36594 46.166.191.28 11111 119.206.92.21 14473 87.217.0.55 31271 50.139.253.97 30747 110.93.92.251 3530 151.89.117.29 4777 194.153.164.0 58117 48.46.40.11 57118 160.13.218.62 22922 ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '66.235.168.222']

Name

71.9.135.100

Description

ISP: Charter Communications **OS:** Linux ------------------------- Services: **22:** ``` SSH-2.0-dropbear_2019.78 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQCLiFBHP8ouIS4S8IHmgm6tD2sBWfCXoQcYaCRz92CCKuZQ CGr2wJBF0JbdS0+gx03WoSklfqP21yULQHWC2nWP6sE2L3f1/l/GUCInO+249KyTM1+Agd8mADgP w7GDy6xiWLeHxNw42ppPEMMTApNJJtXl98xwVe6Vl2TRolmRPOifHk1OyR8s0kvGsCh8gdqASJoh9kjM9EGlYZZhTW3WDPn6vYizR8x+nPv0F3wdvday3AWkd/fXgqp+FNE0nytaGHoYqonLR+hUWVI+ 7hekiSTk4WVJVeB0sdySPIs9GMUpxHgi/k8kl9TO5bjb5eP/iOH0nuk+6RxVjOu989Dx Fingerprint: 3e:17:d2:77:f7:c0:f1:7c:ab:1e:49:73:bf:cd:89:7a Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp521 ecdh-sha2-nistp384 ecdh-sha2-nistp256 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 kexguess2@matt.ucc.asn.au Server Host Key Algorithms: ecdsa-sha2-nistp256 ssh-rsa ssh-dss Encryption Algorithms: aes128-ctr aes256-ctr MAC Algorithms: hmac-sha1 hmac-sha2-256 Compression Algorithms: none ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '71.9.135.100']

Name

23.242.208.175

Description

ISP: Charter Communications Inc **OS:** - ------------------------- Services: **443:** ``` HTTP/1.1 200 OK Date: Thu, 04 Apr 2024 08:33:47 GMT Content-Type: text/html Content-Length: 21519 Connection: keep-alive Accept-Ranges: bytes ETag: "1896110815" Last-Modified: Fri, 22 Jun 2018 16:22:01 GMT Server: Lighttpd Strict-Transport-Security: max-age=63072000 ``` HEARTBLEED: 2024/04/04 08:34:03 23.242.208.175:443 - SAFE ------------------ **1194:** ``` @\xf2?\x1aw\xa8;\x081\x00\x00\x00\x00\x00 ``` ------------------ **8443:** ``` HTTP/1.0 200 OK Server: httpd/2.0 x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block Date: Wed, 03 Apr 2024 06:54:58 GMT Content-Type: text/html Connection: close ``` HEARTBLEED: 2024/04/03 06:55:12 23.242.208.175:8443 - SAFE ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '23.242.208.175']

Name

172.233.228.93

Description

- **Zip Code:** N/A - **ISP:** Akamai Connected Cloud - **ASN:** 63949 - **Organization:** Akamai Connected Cloud - **Is Crawler:** False - **Timezone:** America/New_York - **Mobile:** False - **Host:** 172-233-228-93.ip.linodeusercontent.com - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** Virginia - **City:** Ashburn - **Latitude:** 39.05 - **Longitude:** -77.49

Pattern Type

stix

Pattern

[ipv4-addr:value = '172.233.228.93']

Name

198.58.109.149

Description

ISP: Akamai Connected Cloud **OS:** Windows Server 2022 (build 10.0.20348) -------------------------- Services: **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00 Remote Desktop Protocol NTLM Info: OS: Windows Server 2022 OS Build: 10.0.20348 Target Name: MEOCLOUD NetBIOS Domain Name: MEOCLOUD NetBIOS Computer Name: MEOCLOUD DNS Domain Name: meocloud FQDN: meocloud ; Administrator SES ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '198.58.109.149']

Name

137.118.185.101

Description

ISP: Wilkes Communications, Inc. **OS:** ASUSWRT -------------------------- Services: **8443:** ``` HTTP/1.0 200 OK Server: httpd/2.0 x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block Date: Sun, 17 Mar 2024 11:46:58 GMT Content-Type: text/html

Connection: close ``` HEARTBLEED: 2024/03/17 11:47:18 137.118.185.101:8443 - SAFE

Pattern Type

stix

Pattern

[ipv4-addr:value = '137.118.185.101']

Name

fe07ca449e99827265ca95f9f56ec6543a4c5b712ed50038a9a153199e95a0b7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'fe07ca449e99827265ca95f9f56ec6543a4c5b712ed50038a9a153199e95a0b7']

Name

e315907415eb8cfcf3b6a4cd6602b392a3fe8ee0f79a2d51a81a928dbce950f8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'e315907415eb8cfcf3b6a4cd6602b392a3fe8ee0f79a2d51a81a928dbce950f8']

Name

adba167a9df482aa991faaa0e0cde1182fb9acfbb0dc8d19148ce634608bab87

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'adba167a9df482aa991faaa0e0cde1182fb9acfbb0dc8d19148ce634608bab87']

Name

c1a0d380bf55070496b9420b970dfc5c2c4ad0a598083b9077493e8b8035f1e9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'c1a0d380bf55070496b9420b970dfc5c2c4ad0a598083b9077493e8b8035f1e9']

Name

96dbec24ac64e7dd5fef6e2c26214c8fe5be3486d5c92d21d5dcb4f6c4e365b9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'96dbec24ac64e7dd5fef6e2c26214c8fe5be3486d5c92d21d5dcb4f6c4e365b9']

Name

755f5b8bd67d226f24329dc960f59e11cb5735b930b4ed30b2df77572efb32e8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'755f5b8bd67d226f24329dc960f59e11cb5735b930b4ed30b2df77572efb32e8']

Name

448fbd7b3389fe2aa421de224d065cea7064de0869a036610e5363c931df5b7c

Description

Sliver_Implant_32bit

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'448fbd7b3389fe2aa421de224d065cea7064de0869a036610e5363c931df5b7c']

Name

144.172.79.92

Description

- **Zip Code:** N/A - **ISP:** RouterHosting - **ASN:** 14956 - **Organization:** RouterHosting - **Is Crawler:** False - **Timezone:** America/New_York - **Mobile:** False - **Host:** 144.172.79.92 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** Florida - **City:** Miami - **Latitude:** 25.78 - **Longitude:** -80.18

Pattern Type

stix

Pattern

[ipv4-addr:value = '144.172.79.92']

Name

3de2a4392b8715bad070b2ae12243f166ead37830f7c6d24e778985927f9caac

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3de2a4392b8715bad070b2ae12243f166ead37830f7c6d24e778985927f9caac']

Name

35a5f8ac03b0e3865b3177892420cb34233c55240f452f00f9004e274a85703c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '35a5f8ac03b0e3865b3177892420cb34233c55240f452f00f9004e274a85703c']

Name

161fd76c83e557269bee39a57baa2ccbbac679f59d9adff1e1b73b0f4bb277a6

Description

is__elf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '161fd76c83e557269bee39a57baa2ccbbac679f59d9adff1e1b73b0f4bb277a6']

Vulnerability

Name
CVE-2024-3400
Description
Palo Alto Networks PAN-OS GlobalProtect feature contains a command injection vulnerability that allows an unauthenticated attacker to execute commands with root privileges on the firewall.

Malware

Name
GOST

Name
UPSTYLE

Intrusion-Set

Name
UTA0218

Attack-Pattern

Name

T1556

ID

T1556

Description

Adversaries may modify authentication mechanisms and processes to access user credentials or enable otherwise unwarranted access to accounts. The authentication process is handled by mechanisms, such as the Local Security Authentication Server (LSASS) process and the Security Accounts Manager (SAM) on Windows, pluggable authentication modules (PAM) on Unix-based systems, and authorization plugins on MacOS systems, responsible for gathering, storing, and validating credentials. By modifying an authentication process, an adversary may be able to authenticate to a service or system without using [Valid Accounts](https://attack.mitre.org/techniques/T1078). Adversaries may maliciously modify a part of this process to either reveal credentials or bypass authentication mechanisms. Compromised credentials or access may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access and remote desktop.

Name

T1018

ID

T1018

Description

Adversaries may attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for Lateral Movement from the current system. Functionality could exist within remote access tools to enable this, but utilities available on the operating system could also be used such as [Ping](https://attack.mitre.org/software/S0097) or `net view` using [Net](https://attack.mitre.org/software/S0039). Adversaries may also analyze data from local host files (ex: `C:\Windows\System32\Drivers\etc\hosts` or `/etc/hosts`) or other passive means (such as local [Arp](https://attack.mitre.org/software/S0099) cache entries) in order to discover the presence of remote systems in an environment. Adversaries may also target discovery of network infrastructure as well as leverage [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands on network devices to gather detailed information about systems within a network (e.g. `show cdp neighbors`, `show arp`).(Citation: US-CERT-TA18-106A)(Citation: CISA AR21-126A FIVEHANDS May 2021)

Name

T1059.003

ID

T1059.003

Description

Adversaries may abuse the Windows command shell for execution. The Windows command shell ([cmd](https://attack.mitre.org/software/S0106)) is the primary command prompt on Windows systems. The Windows command prompt can be used to control almost any aspect of a system, with various permission levels required for different subsets of commands. The command prompt can be invoked remotely via [Remote Services](https://attack.mitre.org/techniques/T1021) such as [SSH](https://attack.mitre.org/techniques/T1021/004).(Citation: SSH in Windows) Batch files (ex: .bat or .cmd) also provide the shell with a list of sequential commands to run, as well as normal scripting operations such as conditionals and loops. Common uses of batch files include long or repetitive tasks, or the need to run the same set of commands on multiple systems. Adversaries may leverage [cmd](https://attack.mitre.org/software/S0106) to execute various commands and payloads. Common uses include [cmd](https://attack.mitre.org/software/S0106) to execute a single command, or abusing [cmd](https://attack.mitre.org/software/S0106) interactively with input and output forwarded over a command and control channel.

Name

T1012

ID

T1012

Description

Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software. The Registry contains a significant amount of information about the operating system, configuration, software, and security.(Citation: Wikipedia Windows Registry) Information can easily be queried using the [Reg](https://attack.mitre.org/software/S0075) utility, though other means to access the Registry exist. Some of the information may help adversaries to further their operation within a network. Adversaries may use the information from [Query Registry](https://attack.mitre.org/techniques/T1012) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Name

T1059.004

ID

T1059.004

Description

Adversaries may abuse Unix shell commands and scripts for execution. Unix shells are the primary command prompt on Linux and macOS systems, though many variations of the Unix shell exist (e.g. sh, bash, zsh, etc.) depending on the specific OS or distribution.(Citation: DieNet Bash)(Citation: Apple ZShell) Unix shells can control every aspect of a system, with certain commands requiring elevated privileges. Unix shells also support scripts that enable sequential execution of commands as well as other typical programming operations such as conditionals and loops. Common uses of shell scripts include long or repetitive tasks, or the need to run the same set of commands on multiple systems. Adversaries may abuse Unix shells to execute various commands or payloads. Interactive shells may be accessed through command and control channels or during lateral movement such as with [SSH](https://attack.mitre.org/techniques/T1021/004). Adversaries may also leverage shell scripts to deliver and execute multiple commands on victims or as part of payloads used for persistence.

Name

T1059.001

ID

T1059.001

Description

Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system.(Citation: TechNet PowerShell) Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the `Start-Process` cmdlet which can be used to run an executable and the `Invoke-Command` cmdlet which runs a command locally or on a remote computer (though administrator permissions are required to use PowerShell to connect to remote systems). PowerShell may also be used to download and run executables from the Internet, which can be executed from disk or in memory without touching disk. A number of PowerShell-based offensive testing tools are available, including [Empire](https://attack.mitre.org/software/S0363), [PowerSploit](https://attack.mitre.org/software/S0194), [PoshC2](https://attack.mitre.org/software/S0378), and PSAttack.(Citation: Github PSAttack) PowerShell commands/scripts can also be executed without directly invoking the `powershell.exe` binary through interfaces to PowerShell's underlying `System.Management.Automation` assembly DLL exposed through the .NET framework and Windows Common Language Interface (CLI).(Citation: Sixdub PowerPick Jan 2016)(Citation: SilentBreak Offensive PS Dec 2015)(Citation: Microsoft PSfromCsharp APR 2014)

Name

T1083

ID

T1083

Description

Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Adversaries may use the information from [File and Directory Discovery](https://attack.mitre.org/techniques/T1083) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Many command shell utilities can be used to obtain this information. Examples include `dir`, `tree`, `ls`, `find`, and `locate`.(Citation: Windows Commands JPCERT) Custom tools may also be used to gather file and directory information and interact with the [Native API](https://attack.mitre.org/techniques/T1106). Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather file and directory information (e.g. `dir`, `show flash`, and/or `nvram`).(Citation: US-CERT-TA18-106A)

Name

T1059

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python] (https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Name
T1016

ID
T1016

Description
Adversaries may look for details about the network configuration and settings, such as IP and/or MAC addresses, of systems they access or through information discovery of remote systems. Several operating system administration utilities exist that can be used to gather this information. Examples include [Arp](https://attack.mitre.org/software/S0099), [ipconfig](https://attack.mitre.org/software/S0100)/[ifconfig](https://attack.mitre.org/software/S0101), [nbtstat](https://attack.mitre.org/software/S0102), and [route](https://attack.mitre.org/software/S0103). Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather information about configurations and settings, such as IP addresses of configured interfaces and static/dynamic routes (e.g. `show ip route`, `show ip interface`).(Citation: US-CERT-TA18-106A)(Citation: Mandiant APT41 Global Intrusion) Adversaries may use the information from [System Network Configuration Discovery](https://attack.mitre.org/techniques/T1016) during automated discovery to shape follow-on behaviors, including determining certain access within the target network and what actions to do next.

Name

T1207

ID

T1207

Description

Adversaries may register a rogue Domain Controller to enable manipulation of Active Directory data. DCShadow may be used to create a rogue Domain Controller (DC). DCShadow is a method of manipulating Active Directory (AD) data, including objects and schemas, by registering (or reusing an inactive registration) and simulating the behavior of a DC. (Citation: DCShadow Blog) Once registered, a rogue DC may be able to inject and replicate changes into AD infrastructure for any domain object, including credentials and keys. Registering a rogue DC involves creating a new server and nTDSDSA objects in the Configuration partition of the AD schema, which requires Administrator privileges (either Domain or local to the DC) or the KRBTGT hash. (Citation: Adsecurity Mimikatz Guide) This technique may bypass system logging and security monitors such as security information and event management (SIEM) products (since actions taken on a rogue DC may not be reported to these sensors). (Citation: DCShadow Blog) The technique may also be used to alter and delete replication and other associated metadata to obstruct forensic analysis. Adversaries may also utilize this technique to perform [SID-History Injection](https://attack.mitre.org/techniques/T1134/005) and/or manipulate AD objects (such as accounts, access control lists, schemas) to establish backdoors for Persistence. (Citation: DCShadow Blog)

Name

T1021

ID

T1021

Description

Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to log into a service that accepts remote connections, such as telnet, SSH, and VNC. The adversary may then perform actions as the logged-on user. In an enterprise environment, servers and workstations can be organized into domains. Domains provide centralized identity management, allowing users to login using one set of credentials across the entire network. If an adversary is able to obtain a set of valid domain credentials, they could login to many different machines using remote access protocols such as secure shell (SSH) or remote desktop protocol (RDP).(Citation: SSH Secure Shell)(Citation: TechNet Remote Desktop Services) They could also login to accessible SaaS or IaaS services, such as those that federate their identities to the domain. Legitimate applications (such as [Software Deployment Tools](https://attack.mitre.org/techniques/T1072) and other administrative programs) may utilize [Remote Services](https://attack.mitre.org/techniques/T1021) to access remote hosts. For example, Apple Remote Desktop (ARD) on macOS is native software used for remote management. ARD leverages a blend of protocols, including [VNC](https://attack.mitre.org/techniques/T1021/005) to send the screen and control buffers and [SSH](https://attack.mitre.org/techniques/T1021/004) for secure file transfer. (Citation: Remote Management MDM macOS)(Citation: Kickstart Apple Remote Desktop commands)(Citation: Apple Remote Desktop Admin Guide 3.3) Adversaries can abuse applications such as ARD to gain remote code execution and perform lateral movement. In versions of macOS prior to 10.14, an adversary can escalate an SSH session to an ARD session which enables an adversary to accept TCC (Transparency, Consent, and Control) prompts without user interaction and gain access to data.(Citation: FireEye 2019 Apple Remote Desktop)(Citation: Lockboxx ARD 2019)(Citation: Kickstart Apple Remote Desktop commands)

Name

T1190

ID

T1190

Description

Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration. Exploited applications are often websites/web servers, but can also include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other system with Internet accessible open sockets.(Citation: NVD CVE-2016-6662)(Citation: CIS Multiple SMB Vulnerabilities)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)(Citation: Cisco Blog Legacy Device Attacks)(Citation: NVD CVE-2014-7169) Depending on the flaw being exploited this may also involve [Exploitation for Defense Evasion](https://attack.mitre.org/techniques/T1211). If an application is hosted on cloud-based infrastructure and/or is containerized, then exploiting it may lead to compromise of the underlying instance or container. This can allow an adversary a path to access the cloud or container APIs, exploit container host access via [Escape to Host](https://attack.mitre.org/techniques/T1611), or take advantage of weak identity and access management policies. Adversaries may also exploit edge network infrastructure and related appliances, specifically targeting devices that do not support robust host-based defenses.(Citation: Mandiant Fortinet Zero Day)(Citation: Wired Russia Cyberwar) For websites and databases, the OWASP top 10 and CWE top 25 highlight the most common web-based vulnerabilities.(Citation: OWASP Top 10)(Citation: CWE top 25)

Name

T1555

ID

T1555

Description

Adversaries may search for common password storage locations to obtain user credentials. Passwords are stored in several places on a system, depending on the operating system or application holding the credentials. There are also specific applications and services that store passwords to make them easier for users to manage and maintain, such as password managers and cloud secrets vaults. Once credentials are obtained, they can be used to perform lateral movement and access restricted information.

Name

T1005

ID

T1005

Description

Adversaries may search local system sources, such as file systems and configuration files or local databases, to find files of interest and sensitive data prior to Exfiltration. Adversaries may do this using a [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), such as [cmd](https://attack.mitre.org/software/S0106) as well as a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008), which have functionality to interact with the file system to gather information.(Citation: show_run_config_cmd_cisco) Adversaries may also use [Automated Collection](https://attack.mitre.org/techniques/T1119) on the local system.

Name

T1003

ID

T1003

Description

Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform [Lateral Movement](https://attack.mitre.org/tactics/TA0008) and access restricted information. Several of the tools mentioned in associated sub-techniques may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.

Name

T1557

ID

T1557

Description

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).

Name

T1033

ID

T1033

Description

Adversaries may attempt to identify the primary user, currently logged in user, set of users that commonly uses a system, or whether a user is actively using the system. They may do this, for example, by retrieving account usernames or by using [OS Credential Dumping](https://attack.mitre.org/techniques/T1003). The information may be collected in a number of different ways using other Discovery techniques, because user and username details are prevalent throughout a system and include running process ownership, file/directory ownership, session information, and system logs. Adversaries may use the information from [System Owner/User Discovery](https://attack.mitre.org/techniques/T1033) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Various utilities and commands may acquire this information, including `whoami`. In macOS and Linux, the currently logged in user can be identified with `w` and `who`. On macOS the `dscl . list /Users | grep -v '_'` command can also be used to enumerate user accounts. Environment variables, such as `%USERNAME%` and `$USER`, may also be used to access this information. On network devices, [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `show users` and `show ssh` can be used to display users currently logged into the device.(Citation: show_ssh_users_cmd_cisco)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)

IPv4-Addr

Value
89.187.187.69
71.9.135.100
66.235.168.222
23.242.208.175
198.58.109.149
172.233.228.93
144.172.79.92
137.118.185.101

StixFile

Value
fe07ca449e99827265ca95f9f56ec6543a4c5b712ed50038a9a153199e95a0b7
e315907415eb8cfcf3b6a4cd6602b392a3fe8ee0f79a2d51a81a928dbce950f8
c1a0d380bf55070496b9420b970dfc5c2c4ad0a598083b9077493e8b8035f1e9
adba167a9df482aa991faaa0e0cde1182fb9acfbb0dc8d19148ce634608bab87
3de2a4392b8715bad070b2ae12243f166ead37830f7c6d24e778985927f9caac
96dbec24ac64e7dd5fef6e2c26214c8fe5be3486d5c92d21d5dcb4f6c4e365b9
755f5b8bd67d226f24329dc960f59e11cb5735b930b4ed30b2df77572efb32e8
448fbd7b3389fe2aa421de224d065cea7064de0869a036610e5363c931df5b7c
35a5f8ac03b0e3865b3177892420cb34233c55240f452f00f9004e274a85703c
161fd76c83e557269bee39a57baa2ccbbac679f59d9adff1e1b73b0f4bb277a6

External References

- https://www.volexity.com/blog/2024/04/12/zero-day-exploitation-of-unauthenticated-remote-code-execution-vulnerability-in-globalprotect-cve-2024-3400/
- https://otx.alienvault.com/pulse/66198c3b58d2dd2ad4043bc6