
# Cisco Talos shares insights related to recent cyber attack on Cisco

By Nick Biasini

WEDNESDAY, AUGUST 10, 2022 15:30

HEADLINES

THIS POST IS ALSO AVAILABLE IN:

日本語 (Japanese)

## Update History

| DATE | DESCRIPTION OF UPDATES |
|---|---|
| Aug. 10th 2022 | Adding clarifying details on activity involving active directory. |
| Aug. 10th 2022 | Update made to the Cisco Response and Recommendations section related to MFA. |

## Executive summary

- On May 24, 2022, Cisco became aware of a potential compromise. Since that point, Cisco Security Incident Response (CSIRT) and Cisco Talos have been working to remediate.
- During the investigation, it was determined that a Cisco employee's credentials were compromised after an attacker gained control of a personal Google account where credentials saved in the victim's browser were being synchronized.
- The attacker conducted a series of sophisticated voice phishing attacks under the guise of various trusted organizations attempting to convince the victim to accept multi-factor authentication (MFA) push notifications initiated by the attacker. The

RELATED CONTENT

Talos joins CISA to counter cyber threats against non-profits, activists and other at-risk communities

MAY 14, 2024 08:42

Commercial spyware tools can threaten democratic values by enabling governments to conduct covert surveillance on citizens, undermining privacy rights and freedom of expression.

What's the deal with the massive backlog of vulnerabilities at the NVD?

APRIL 19, 2024 08:00

Given the state of the NVD and vulnerability management, we felt it was worth looking at the current state of the NVD, how we got to this point, what it means for security teams, and where we go from here.

New decryptor for Babuk Tortilla ransomware variant released

JANUARY 9, 2024 04:00

Cisco Talos obtained executable code capable of decrypting files affected by the Babuk Tortilla ransomware variant, allowing Talos to extract and share the private decryption key used by the threat actor.

attacker ultimately succeeded in achieving an MFA push acceptance, granting them access to VPN in the context of the targeted user.

- CSIRT and Talos are responding to the event and we have not identified any evidence suggesting that the attacker gained access to critical internal systems, such as those related to product development, code signing, etc.
- After obtaining initial access, the threat actor conducted a variety of activities to maintain access, minimize forensic artifacts, and increase their level of access to systems within the environment.
- The threat actor was successfully removed from the environment and displayed persistence, repeatedly attempting to regain access in the weeks following the attack; however, these attempts were unsuccessful.
- We assess with moderate to high confidence that this attack was conducted by an adversary that has been previously identified as an initial access broker (IAB) with ties to the UNC2447 cybercrime gang, Lapsus$ threat actor group, and Yanluowang ransomware operators.
- For further information see the Cisco Response page here.

## Initial vector

Initial access to the Cisco VPN was achieved via the successful compromise of a Cisco employee's personal Google account. The user had enabled password syncing via Google Chrome and had stored their Cisco credentials in their browser, enabling that information to synchronize to their Google account. After obtaining the user's credentials, the attacker attempted to bypass multifactor authentication (MFA) using a variety of techniques, including voice phishing (aka "vishing") and MFA fatigue, the process of sending a high volume of push requests to the target's mobile device until the user accepts, either accidentally or simply to attempt to silence the repeated push notifications they are receiving. Vishing is an increasingly common social engineering technique whereby attackers try to trick employees into divulging sensitive information over the phone. In this instance, an employee reported that they received multiple calls over several days in which the callers – who spoke in English with various international accents and dialects – purported to be associated with support organizations trusted by the user.

Once the attacker had obtained initial access, they enrolled a series of new devices for MFA and authenticated successfully to the Cisco VPN. The attacker then escalated to administrative privileges, allowing them to login to multiple systems, which alerted our Cisco Security Incident Response Team (CSIRT), who subsequently responded to the incident. The actor in question dropped a variety of tools, including remote access tools like LogMeIn and TeamViewer, offensive security tools such as Cobalt Strike, PowerSploit, Mimikatz, and Impacket, and added their own backdoor accounts and persistence mechanisms.

## Post-compromise TTPs

Following initial access to the environment, the threat actor conducted a variety of activities for the purposes of maintaining access, minimizing forensic artifacts, and increasing their level of access to systems within the environment.

Once on a system, the threat actor began to enumerate the environment, using common built-in Windows utilities to identify the user and group membership configuration of the system, hostname, and identify the context of the user account under which they were operating. We periodically observed the attacker issuing commands containing typographical errors, indicating manual operator interaction was occurring within the environment.

After establishing access to the VPN, the attacker then began to use the compromised user account to logon to a large number of systems before beginning to pivot further into

the environment. They moved into the Citrix environment, compromising a series of Citrix servers and eventually obtained privileged access to domain controllers.

After obtaining access to the domain controllers, the attacker began attempting to dump NTDS from them using "ntdsutil.exe" consistent with the following syntax:

```
powershell ntdsutil.exe 'ac i ntds' 'ifm' 'create full c:\users\public'
q q
```

They then worked to exfiltrate the dumped NTDS over SMB (TCP/445) from the domain controller to the VPN system under their control.

After obtaining access to credential databases, the attacker was observed leveraging machine accounts for privileged authentication and lateral movement across the environment.

Consistent with activity we previously observed in other separate but similar attacks, the adversary created an administrative user called "z" on the system using the built-in Windows "net.exe" commands. This account was then added to the local Administrators group. We also observed instances where the threat actor changed the password of existing local user accounts to the same value shown below. Notably, we have observed the creation of the "z" account by this actor in previous engagements prior to the Russian invasion of Ukraine.

```
C:\Windows\system32\net user z Lh199211* /add
```

```
C:\Windows\system32\net localgroup administrators z /add
```

This account was then used in some cases to execute additional utilities, such as adfind or secretsdump, to attempt to enumerate the directory services environment and obtain additional credentials. Additionally, the threat actor was observed attempting to extract registry information, including the SAM database on compromised windows hosts.

```
reg save hklm\system system
```

```
reg save hklm\sam sam
```

```
reg save HKLM\security sec
```

On some systems, the attacker was observed employing MiniDump from Mimikatz to dump LSASS.

```
tasklist | findstr lsass
```

```
rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump [LSASS_PID]
C:\windows\temp\lsass.dmp full
```

The attacker also took steps to remove evidence of activities performed on compromised systems by deleting the previously created local Administrator account. They also used the "wevtutil.exe" utility to identify and clear event logs generated on the system.

```
wevtutil.exe el
```

```
wevtutil.exe cl [LOGNAME]
```

In many cases, we observed the attacker removing the previously created local administrator account.

```
net user z /delete
```

To move files between systems within the environment, the threat actor often leveraged Remote Desktop Protocol (RDP) and Citrix. We observed them modifying the host-based firewall configurations to enable RDP access to systems.

```
netsh advfirewall firewall set rule group=remote desktop new enable=Yes
```

We also observed the installation of additional remote access tools, such as TeamViewer and LogMeIn.

```
C:\Windows\System32\msiexec.exe /i C:\Users\
[USERNAME]\Pictures\LogMeIn.msi
```

The attacker frequently leveraged Windows logon bypass techniques to maintain the ability to access systems in the environment with elevated privileges. They frequently relied upon PSEXESVC.exe to remotely add the following Registry key values:

```
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options\narrator.exe /v Debugger /t REG_SZ /d
C:\windows\system32\cmd.exe /f
```

```
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options\sethc.exe /v Debugger /t REG_SZ /d C:\windows\system32\cmd.exe
/f
```

This enabled the attacker to leverage the accessibility features present on the Windows logon screen to spawn a SYSTEM level command prompt, granting them complete control of the systems. In several cases, we observed the attacker adding these keys but not further interacting with the system, possibly as a persistence mechanism to be used later as their primary privileged access is revoked.

Throughout the attack, we observed attempts to exfiltrate information from the environment. We confirmed that the only successful data exfiltration that occurred during the attack included the contents of a Box folder that was associated with a compromised employee's account and employee authentication data from active directory. The Box data obtained by the adversary in this case was not sensitive.

In the weeks following the eviction of the attacker from the environment, we observed continuous attempts to re-establish access. In most cases, the attacker was observed targeting weak password rotation hygiene following mandated employee password resets. They primarily targeted users who they believed would have made single character changes to their previous passwords, attempting to leverage these credentials to authenticate and regain access to the Cisco VPN. The attacker was initially leveraging traffic anonymization services like Tor; however, after experiencing limited success, they switched to attempting to establish new VPN sessions from residential IP space using accounts previously compromised during the initial stages of the attack. We also observed the registration of several additional domains referencing the organization while responding to the attack and took action on them before they could be used for malicious purposes.

After being successfully removed from the environment, the adversary also repeatedly attempted to establish email communications with executive members of the organization but did not make any specific threats or extortion demands. In one email, they included a screenshot showing the directory listing of the Box data that was previously exfiltrated as described earlier. Below is a screenshot of one of the received emails. The adversary redacted the directory listing screenshot prior to sending the email.

## Backdoor analysis

The actor dropped a series of payloads onto systems, which we continue to analyze. The first payload is a simple backdoor that takes commands from a command and control (C2) server and executes them on the end system via the Windows Command Processor. The commands are sent in JSON blobs and are standard for a backdoor. There is a “DELETE_SELF” command that removes the backdoor from the system completely. Another, more interesting, command, “WIPE”, instructs the backdoor to remove the last executed command from memory, likely with the intent of negatively impacting forensic analysis on any impacted hosts.

Commands are retrieved by making HTTP GET requests to the C2 server using the following structure:

```
/bot/cmd.php?botid=%.8x
```

The malware also communicates with the C2 server via HTTP GET requests that feature the following structure:

```
/bot/gate.php?botid=%.8x
```

Following the initial request from the infected system, the C2 server responds with a SHA256 hash. We observed additional requests made every 10 seconds.

The aforementioned HTTP requests are sent using the following user-agent string:

```
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/99.0.4844.51 Safari/537.36 Edg/99.0.1150.36
Trailer/95.3.1132.33
```

The malware also creates a file called “bdata.ini” in the malware’s current working directory that contains a value derived from the volume serial number present on the

infected system. In instances where this backdoor was executed, the malware was observed running from the following directory location:

```
C:\users\public\win\cmd.exe
```

The attacker was frequently observed staging tooling in directory locations under the Public user profile on systems from which they were operating.

Based upon analysis of C2 infrastructure associated with this backdoor, we assess that the C2 server was set up specifically for this attack.

## Attack attribution

Based upon artifacts obtained, tactics, techniques, and procedures (TTPs) identified, infrastructure used, and a thorough analysis of the backdoor utilized in this attack, we assess with moderate to high confidence that this attack was conducted by an adversary that has been previously identified as an initial access broker (IAB) with ties to both UNC2447 and Lapsus$. IABs typically attempt to obtain privileged access to corporate network environments and then monetize that access by selling it to other threat actors who can then leverage it for a variety of purposes. We have also observed previous activity linking this threat actor to the Yanluowang ransomware gang, including the use of the Yanluowang data leak site for posting data stolen from compromised organizations.

UNC2447 is a financially-motivated threat actor with a nexus to Russia that has been previously observed conducting ransomware attacks and leveraging a technique known as “double extortion,” in which data is exfiltrated prior to ransomware deployment in an attempt to coerce victims into paying ransom demands. Prior reporting indicates that UNC2447 has been observed operating  a variety of ransomware, including FIVEHANDS, HELLOKITTY, and more.

Apart from UNC2447, some of the TTPs discovered during the course of our investigation match those of the Lapsus$. Lapsus$ is a threat actor group that is reported to have been responsible for several previous notable breaches of corporate environments. Several arrests of Lapsus$ members were reported earlier this year. Lapsus$ has been observed compromising corporate environments and attempting to exfiltrate sensitive information.

While we did not observe ransomware deployment in this attack, the TTPs used were consistent with “pre-ransomware activity,” activity commonly observed leading up to the deployment of ransomware in victim environments. Many of the TTPs observed are consistent with activity observed by CTIR during previous engagements. Our analysis also suggests reuse of server-side infrastructure associated with these previous engagements as well. In previous engagements, we also did not observe deployment of ransomware in the victim environments.

## Cisco response and recommendations

Cisco implemented a company-wide password reset immediately upon learning of the incident. CTIR previously observed similar TTPs in numerous investigations since 2021. Our findings and subsequent security protections resulting from those customer engagements helped us slow and contain the attacker’s progression. We created two ClamAV signatures, which are listed below.

- Win.Exploit.Kolobko-9950675-0
- Win.Backdoor.Kolobko-9950676-0

Threat actors commonly use social engineering techniques to compromise targets, and despite the frequency of such attacks, organizations continue to face challenges mitigating those threats. User education is paramount in thwarting such attacks, including making sure employees know the legitimate ways that support personnel will contact users so that employees can identify fraudulent attempts to obtain sensitive information.

Given the actor's demonstrated proficiency in using a wide array of techniques to obtain initial access, user education is also a key part of countering MFA bypass techniques. Equally important to implementing MFA is ensuring that employees are educated on what to do and how to respond if they get errant push requests on their respective phones. It is also essential to educate employees about who to contact if such incidents do arise to help determine if the event was a technical issue or malicious.

For Duo it is beneficial to implement strong device verification by enforcing stricter controls around device status to limit or block enrollment and access from unmanaged or unknown devices. Additionally, leveraging risk detection to highlight events like a brand-new device being used from unrealistic location or attack patterns like logins brute force can help detect unauthorized access.

Prior to allowing VPN connections from remote endpoints, ensure that posture checking is configured to enforce a baseline set of security controls. This ensures that the connecting devices match  the security requirements present in the environment. This can also prevent rogue devices that have not been previously approved from connecting to the corporate network environment.

Network segmentation is another important security control that organizations should employ, as it provides enhanced protection for high-value assets and also enables more effective detection and response capabilities in situations where an adversary is able to gain initial access into the environment.

Centralized log collection can help minimize the lack of visibility that results when an attacker take active steps to remove logs from systems. Ensuring that the log data generated by endpoints is centrally collected and analyzed for anomalous or overtly malicious behavior can provide early indication when an attack is underway.

In many cases, threat actors have been observed targeting the backup infrastructure in an attempt to further remove an organization's ability to recover following an attack. Ensuring that backups are offline and periodically tested can help mitigate this risk and ensure an organization's ability to effectively recover following an attack.

Auditing of command line execution on endpoints can also provide increased visibility into actions being performed on systems in the environment and can be used to detect suspicious execution of built-in Windows utilities, which is commonly observed during intrusions where threat actors rely on benign applications or utilities already present in the environment for enumeration, privilege escalation, and lateral movement activities.

## Mitre ATT&CK mapping

All of the previously described TTPs that were observed in this attack are listed below based on the phase of the attack in which they occurred.

### Initial Access

ATT&CK Technique : Phishing (T1566)

ATT&CK Technique : Valid Accounts (T1078)

### Execution

ATT&CK Technique : System Services: Service Execution (T1569.002)

## Persistence

ATT&CK Technique : Create Account: Local Account (T1136.001)

ATT&CK Technique : Account Manipulation: Device Registration (T1098.005)

## Privilege Escalation

ATT&CK Technique : Event Triggered Execution: Image File Execution Options Injection (T1546.012)

## Defense Evasion

ATT&CK Technique : Indicator Removal on Host (T1070)

ATT&CK Technique : Indicator Removal on Host: Clear Windows Event Logs (T1070.001)

ATT&CK Technique : Masquerading: Match Legitimate Name or Location (T1036.005)

ATT&CK Technique : Impair Defenses: Disable or Modify System Firewall (T1562.004)

ATT&CK Technique : Modify Registry (T1112)

## Credential Access

ATT&CK Technique : OS Credential Dumping: LSASS Memory (T1003.001)

ATT&CK Technique : OS Credential Dumping: Security Account Manager (T1003.002)

ATT&CK Technique : OS Credential Dumping: NTDS (T1003.003)

ATT&CK Technique : Multi-Factor Authentication Request Generation (T1621)

## Lateral Movement

ATT&CK Technique : Remote Services (T1021)

## Discovery

ATT&CK Technique : Query Registry (T1012)

## Command and Control

ATT&CK Technique : Application Layer Protocol: Web Protocols (T1071.001)

ATT&CK Technique : Remote Access Software (T1219)

ATT&CK Technique: Encrypted Channel: Asymmetric Cryptography (T1573.002)

ATT&CK Technique : Proxy: Multi-hop Proxy (T1090.003)

## Exfiltration

ATT&CK Technique : Exfiltration Over Alternative Protocol (T1048)

# Indicators of compromise

The following indicators of compromise were observed associated with this attack.

## Hashes (SHA256)

184a2570d71eedc3c77b63fd9d2a066cd025d20ceef0f75d428c6f7e5c6965f3
2fc5bf9edcfa19d48e235315e8f571638c99a1220be867e24f3965328fe94a03
542c9da985633d027317e9a226ee70b4f0742dcbc59dfd2d4e59977bb870058d
61176a5756c7b953bc31e5a53580d640629980a344aa5ff147a20fb7d770b610
753952aed395ea845c52e3037f19738cfc9a415070515de277e1a1baeff20647
8df89eef51cdf43b2a992ade6ad998b267ebb5e61305aeb765e4232e66eaf79a
8e5733484982d0833abbd9c73a05a667ec2d9d005bbf517b1c8cd4b1daf57190
99be6e7e31f0a1d7eebd1e45ac3b9398384c1f0fa594565137abb14dc28c8a7f
bb62138d173de997b36e9b07c20b2ca13ea15e9e6cd75ea0e8162e0d3ded83b7
eb3452c64970f805f1448b78cd3c05d851d758421896edd5dfbe68e08e783d18

## IP Addresses

104.131.30[.]201
108.191.224[.]47
131.150.216[.]118
134.209.88[.]140
138.68.227[.]71
139.177.192[.]145
139.60.160[.]20
139.60.161[.]99
143.198.110[.]248
143.198.131[.]210
159.65.246[.]188
161.35.137[.]163
162.33.177[.]27
162.33.178[.]244
162.33.179[.]17
165.227.219[.]211
165.227.23[.]218
165.232.154[.]73
166.205.190[.]23
167.99.160[.]91
172.56.42[.]39
172.58.220[.]52
172.58.239[.]34
174.205.239[.]164
176.59.109[.]115
178.128.171[.]206
185.220.100[.]244
185.220.101[.]10
185.220.101[.]13
185.220.101[.]15
185.220.101[.]16
185.220.101[.]2
185.220.101[.]20
185.220.101[.]34
185.220.101[.]45
185.220.101[.]6
185.220.101[.]65
185.220.101[.]73
185.220.101[.]79
185.220.102[.]242
185.220.102[.]250
192.241.133[.]130
194.165.16[.]98
195.149.87[.]136
24.6.144[.]43
45.145.67[.]170
45.227.255[.]215

45.32.141[.]138
45.32.228[.]189
45.32.228[.]190
45.55.36[.]143
45.61.136[.]207
45.61.136[.]5
45.61.136[.]83
46.161.27[.]117
5.165.200[.]7
52.154.0[.]241
64.227.0[.]177
64.4.238[.]56
65.188.102[.]43
66.42.97[.]210
67.171.114[.]251
68.183.200[.]63
68.46.232[.]60
73.153.192[.]98
74.119.194[.]203
74.119.194[.]4
76.22.236[.]142
82.116.32[.]77
87.251.67[.]41
94.142.241[.]194

## Domains

cisco-help[.]cf
cisco-helpdesk[.]cf
ciscovpn1[.]com
ciscovpn2[.]com
ciscovpn3[.]com
devcisco[.]com
devciscoprograms[.]com
helpzonecisco[.]com
kazaboldu[.]net
mycisco[.]cf
mycisco[.]gq
mycisco-helpdesk[.]ml
primecisco[.]com
pwresetcisco[.]com

## Email Addresses

costacancordia[@]protonmail[.]com

SHARE THIS POST

Microsoft Advisories

**INCIDENT RESPONSE**

Talos IR Capabilities

Emergency Support

**SECURITY RESOURCES**

Open Source Security Tools

Intelligence Categories Reference

Secure Endpoint Naming Reference

**MEDIA**

Talos Intelligence Blog

Threat Source Newsletter

Beers with Talos Podcast

Talos Takes Podcast

Talos Videos

**SUPPORT**

Support Documentation

**COMPANY**

About Talos

Careers

Cisco Security

**FOLLOW US**