2 - 4 October, 2024 / Dublin, Ireland

DOWN THE GRAYRABBIT HOLE – EXPOSING UNC3569 AND ITS MODUS OPERANDI

Steve Su, Aragorn Tseng, Chi-Yu You & Cristiana Brafman Kittner

Google, Japan, Taiwan, Singapore & USA

stevusufocus@google.com

ABSTRACT

In this paper we provide an in-depth analysis of UNC3569, a prolific and sophisticated threat actor operating within the Chinese cybercriminal and cyber contractor-for-hire ecosystem, mostly operating out of China. UNC3569 consistently exploits known vulnerabilities in widely used software to infiltrate organizations across a wide range of industries worldwide. The group's activities are not limited to a specific region or sector, demonstrating a global reach and sophisticated targeting. UNC3569 uses a multifaceted toolset that includes both custom-developed malware and commercial tools acquired from other providers. This diverse arsenal allows the group to adapt its tactics, techniques and procedures (TTPs) to different targets and environments, enhancing its effectiveness and operational success. Evidence suggests potential connections between UNC3569 and other established People's Republic of China (PRC)-nexus threat actors, including UNC251 and UNC3246. These connections, along with shared infrastructure, tools and tactics, point to a complex web of affiliations and collaborative efforts within the broader PRC threat landscape. Connections between UNC3569 and other long-standing PRC-nexus threat actors UNC251 and UNC3246, coupled with historic TTPs, are evidence of a broader technology ecosystem solidifying in the Chinese threat landscape. This is further evidenced by the i-SOON leak that occurred in February 2024. UNC3569 shares connections with the PRC-based company i-SOON, including the use of an IP address linked to i-SOON operators. The i-SOON leak suggests a potential business relationship and operational collaboration between i-SOON and UNC3569 [1]. Significantly, this research sheds light on the potential connections among threat actors linked to China's Ministry of State Security (MSS) and those operating under the cover of front companies.

INTRODUCTION

UNC3569 is a PRC-nexus threat group that prioritizes efficiency, adopting notable n-day exploits for network-facing services, and using multifaceted hacking toolsets to expand its operation. UNC3569's TTPs reveal a penchant for using anti-virus bypass techniques, popular public tools, custom tools, and connections with cyber mercenaries in an increasingly complex ecosystem. Further, UNC3569 has a potential business relationship and operational collaboration with i-SOON, a private contractor company based in Sichuan, China.

Operational targeting

UNC3569 has conducted cyber operations against a multitude of industries worldwide. The group's targets span the government, education, technology and finance sectors, demonstrating an indiscriminate reach. While the group's operations are concentrated in East and Southeast Asia, UNC3569's reach extends to other regions, including the United States, highlighting the global nature of their campaigns. Figure 1 shows a map of the affected regions, and Figure 2 shows the targeted industries.

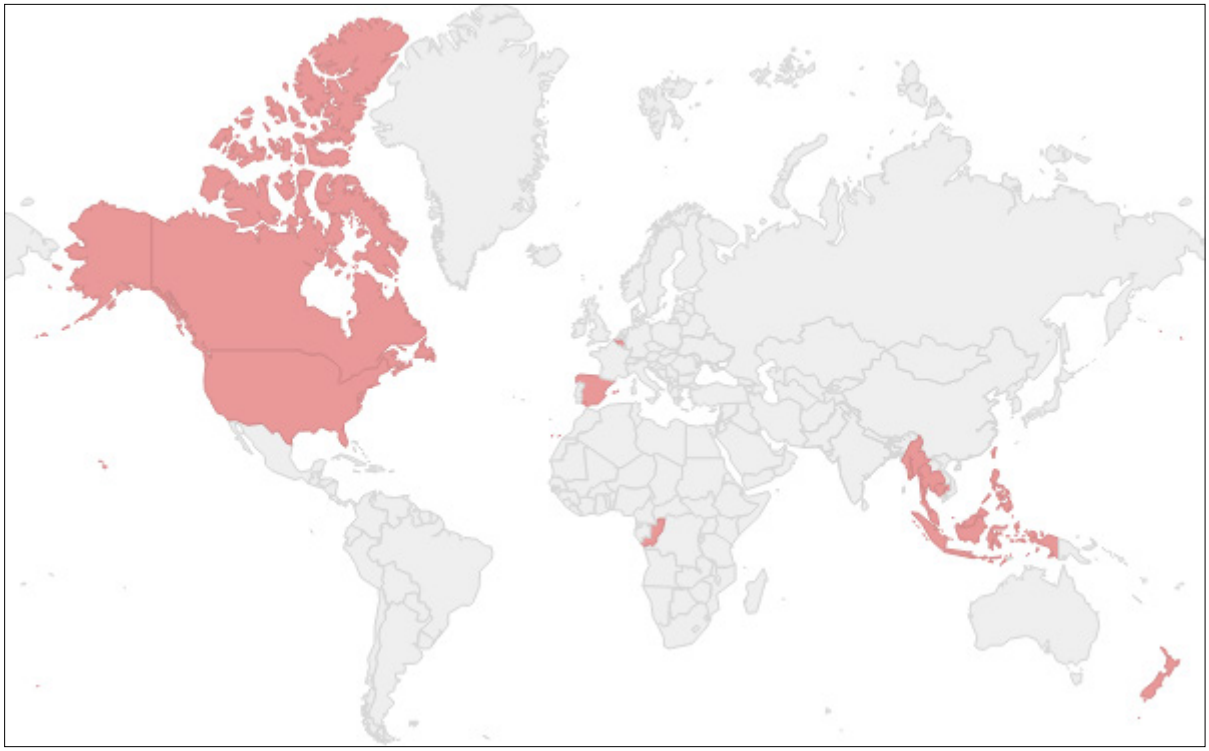


Figure 1: Map of the affected regions.

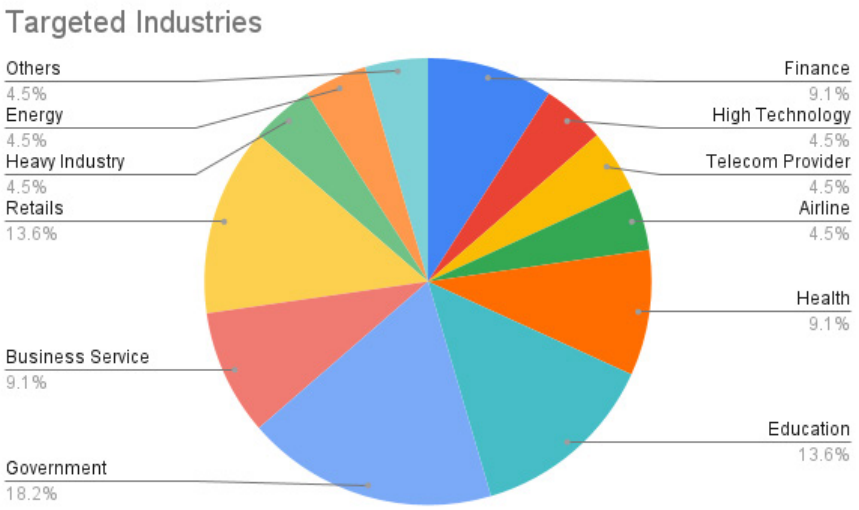


Figure 2: Affected industries.

Efficiency-first modus operandi

UNC3569's efficiency-driven approach, combined with vulnerability exploitation, infrastructure configuration, anti-virus evasion techniques and a diverse toolset, underscores the need to understand the complex relationships that exist within this ecosystem in the cyber threat landscape.

UNC3569 consistently exploits n-day vulnerabilities for services provided by vendors such as *Apache*, *Microsoft*, *IBM*, *VMware* and *Oracle*. The attackers use publicly available scanners to find the loopholes.

A simple public reconnaissance tool, script and BEACON usually come after initial exploitation. A primary backdoor – DRAFTGRAPH, CROSSWALK or the custom GRAYRABBIT – is included in the attack to offer other remote control features. The payload is often obfuscated with an additional binary layer, including techniques such as XOR encoding, custom shellcode loaders (see the example of RABBITCAVE), the public anti-AV project AtomLdr [2], or the group's proprietary downloader RABBITFUR. The group has also used commercially available Chinese remote control tools like *Ping32*.

UNC3569's command-and-control (C2) infrastructure reveals patterns in server configurations and subdomain usage. Similarities in server setups suggest potential automation in the deployment process. These C&C servers are multifunctional, hosting various malware controllers and serving as distribution points for malware. UNC3569 further diversifies its infrastructure by creating distinct subdomains for hosting different malware families, adding another layer of complexity to its operations.

THREAT OPERATIONS

Habitual tactics – initial entry by abusing n-day exploits

Since 2021, UNC3569 has exploited popular n-day CVEs in widely used software, such as CVE-2021-44228 and CVE-2022-21587, to gain access to target organizations. Upon successful exploitation, the attackers typically deploy the OXEEYE tool (OXEEYE is a publicly available port-forwarding utility originally named 'iox' [3]) using the SIDESTEP launcher for reconnaissance purposes. This is often followed by the deployment of Cobalt Strike BEACON on the compromised server to establish a foothold for further operations.

In February 2023, UNC3569 targeted a US media and entertainment company, exploiting CVE-2022-47986, which allowed the attackers to execute arbitrary commands on the *Aspera Faspex* server. This exploit allowed for the use of PowerShell to download malicious components to the target server. This led to a DLL sideload attack deploying the BEACON payload. Subsequently, lateral movement was achieved to several servers. Additional tools used in this campaign included SIDESTEP, which was embedded in OXEEYE for reconnaissance.

Additional evidence observed in July 2023 further suggests UNC3569's ongoing use of OXEEYE and GRAYRABBIT. This toolset was discovered on the *Microsoft OneDrive*, which was abused as DRAFTGRAPH C2 infrastructure. This suggests that the group continues to rely on established TTPs for initial compromise and reconnaissance.

Leaked command logs

A command log file linked to UNC3569 was inadvertently exposed via an open directory on the group's server (8.210.141.104) at the end of 2022. Analysis of this log revealed UNC3569's targeting and victimology by showing

reconnaissance activities against a broad range of targets in Southeast Asia and Oceania, including government agencies, educational institutions, telecommunication providers, airlines, and organizations within the heavy industry and energy sectors. While the log does not confirm successful breaches, it nevertheless provides insight into the hacking tools and techniques used by UNC3569 in its attempts.

The following is an example of the workflow used to test the target server:

1. Download multiple ProxyShell exploit tools for testing:

- Proxyshell-auto [4]
  - Exploit tool based on CVE-2021-34473, CVE-2021-31206, CVE-2021-34523, CVE-2021-31207
- proxyshell [5]
  - Exploit tool based on the *Microsoft Exchange* CVE-2021-34473, CVE-2021-34523, CVE-2021-31207
- ProxyVulns [6]
  - [ProxyLogon] CVE-2021-26855 & CVE-2021-27065 Fixed RawIdentity Bug Exploit
  - [ProxyOracle] CVE-2021-31195 & CVE-2021-31196 Exploit Chains
  - [ProxyShell] CVE-2021-34473, CVE-2021-34523 & CVE-2021-31207 Exploit Chains

2. Download the *Palo Alto PAN-OS* scanner and *Mikrotick* tools to scan the organization's firewall portal server and network devices:

- panos-scanner [7]

  Determine the *Palo Alto PAN-OS* software version of a remote *GlobalProtect* portal or management interface
- mikrotik-tools [8]
  - Jailbreak tool for *Mikrotik* devices
- PaloAltoRceDetectionAndExploit [9]
  - Exploit tool based on CVE-2017-15944

3. After successfully opening a connection to the portal server, the actor tries to install Cobalt Strike and webshells on that server:

- CVE-2021-34473-Exchange-ProxyShell [10]
- cs2modrewrite [11]

4. To grab the code execution permission, the actor then tries the following projects:

- CVE-2021-21985_PoC [12]
- CVE-2018-1207 [13]

5. Finally, the actor executes the simple Python FTP server, probably used for data harvesting.

Supply chain attacks and targeted servers on the cloud

In November 2021, UNC3569 initiated a campaign targeting servers hosted on major cloud and VPS providers. The group employed the SERVEPLUG backdoor alongside the STREAMSERVE backdoor. For *Linux*-based servers, UNC3569 hosted an open directory server to deliver the ANGRYREBEL.LINUX backdoor. The victims were located in Eastern and Southeastern Asia.

This cluster of activity has previously targeted entities throughout the same geographic area using malicious domains that masquerade as services such as *Amazon Web Services* and *Microsoft Support Services*.

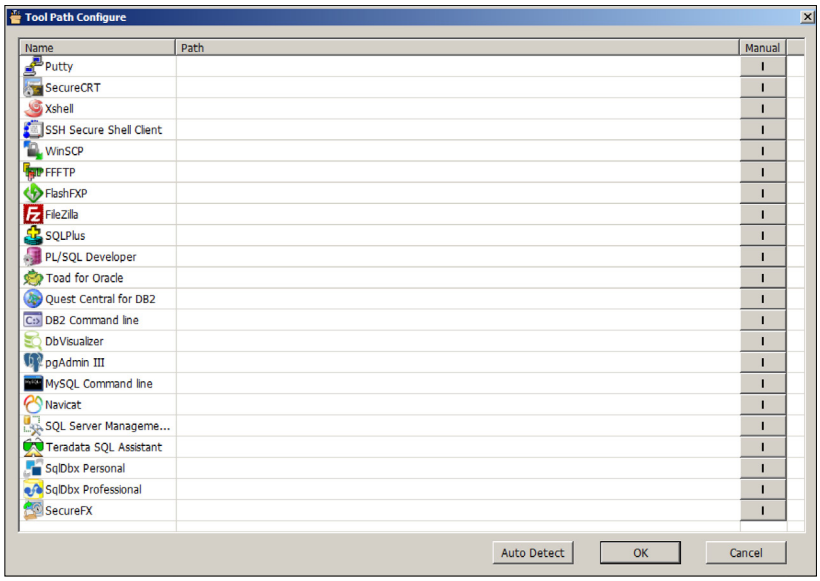
CrowdStrike reported that, when executed, the backdoor retrieves and executes a second-stage script from an external source [14]. Attackers then deploy more malicious payloads to compromised hosts, including a malicious DLL loader that decrypts and launches a shellcode in memory that then injects an embedded payload into an instance of notepad.exe. *CrowdStrike* says it believes the attack was conducted by a China-nexus threat actor that previously targeted several online gaming firms in Asia, even though there are differences in the delivered malicious payload, targeting scope, and supply chain attack mechanism.

Several steps and organizations were reportedly involved in the campaign:

- Chinese cloud configuration tool *Bastion*
- *Qianxin* VPN software
- Communication software *Comm100* (see [15]) and *Live Chat* software
- *LiveHelp100* to drop the backdoor to the target server and disguise the malware components.

To cover the malicious traffic, the attackers registered C2 domains masquerading as normal *AWS* or *AlibabaCloud* domains, as they had also done in previous operations.

Trojanized server configuration tool



Trojanized Qianxin VPN

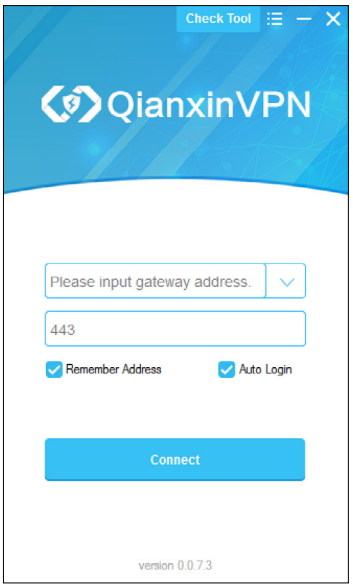


Table 1: Trojanized samples.

After gaining initial access, UNC3569 deployed reconnaissance tools to gather system information and capture screenshots in the environment. The attackers used their custom Golang-based tool, SKYNEEDLE, which is capable of collecting system data, stealing browser information (including *Tencent QQ* and *WeChat* data), and taking screenshots. The actor also used a powerful command-line tool, HackBrowserData [16], for decrypting and exporting browser data – it supports the most popular browsers on the market and can be run on *Windows*, *macOS* and *Linux*.

False SSL certificate error message delivering legitimate remote access control tools

During March 2023 malicious C&C server ssl.stream-google.com, controlled by UNC3569, displayed a fake SSL certificate error page in Simplified Chinese regardless of the host's locale. Clicking the links '安装证书' ('Install SSL certificate') or '安装新证书继续网站 (安全)' ('Install New SSL Certificate and Continue [Safe]') or the button '点击更新' ('Click to Update'), all resulted in malware being downloaded and run from https://chuanqiliebiao-1314[.]oss-cn-shanghai[.]aliyuncs[.]com/wp-content/update.msi. The downloaded file update.msi (MD5: 5bae7a0ab1f9788f8fab89c5e8da5c07) contains the legitimate remote monitoring software *Ping32*, which is developed by China-based company *NSecsoft* (origin: 安在软件), along with a configuration C&C server, '154.211.18.93'.

Figure 3: Inauthentic web page.

```
<div class="icon"></div>
          <div>如果您想获得 Chrome 最高级别的安全保护，请<a href="https://chuanqiliebiao-1314[.]
oss-cn-shanghai[.]aliyuncs[.]com/wp-content/update.msi" id="enhanced-protection-link">安装
证书</a></div>
        </label>
      </div>
    </div>
    <div class="nav-wrapper">
      <a href="https://chuanqiliebiao-1314[.]oss-cn-shanghai[.]aliyuncs[.]com/wp-content/
update.msi"><button id="primary-button">点击更新</button></a>
      <button id="proceed-button" class="secondary-button small-link hidden"></button>
      <button id="details-button" class="secondary-button small-link" aria-
expanded="true">隐藏详情</button>
    </div>
    <div id="details" class="">
      <p>此服务器其安全证书有误。出现此问题的原因可能是配置有误或您的连接被拦截了。</p>
      <p id="final-paragraph"><a href="https://chuanqiliebiao-1314[.]oss-cn-shanghai[.]
aliyuncs[.]com/wp-content/update.msi" id="proceed-link" class="small-link">安装新证书继续网站
（安全）</a></p>
    </div>
```

Table 2: Source page of ssl.stream-google.com.

The malware downloaded from ssl.stream-google.com is hosted on chuanqiliebiao-1314.oss-cn-shanghai.aliyuncs.com, which is a private server for the video game *The Tales*.

Figure 4: Screenshot of the video game hosted on the private server.

The ownership of chuanqiliebiao-1314.oss-cn-shanghai.aliyuncs.com is unclear. It was registered in 2020 but started to deliver UNC3569 malware in October 2022.

Figure 5: Timeline of the malicious domains.

An inauthentic web page contains cross-site scripting (XSS) to deliver a payload via 'http://x[.]ofo[.]ac/4BKZ', which collects screenshots of infected machines. The script modules are available on Chinese security forum *52pojie* [17]. The author of the code, sysalong [18], has an open-source version, xss_pt [19], released to the public.

There is another inauthentic page hosted on the 'x.ofo.ac' server. This leads the user to download BEACON (MD5: 2e73b0ade618cdc967165d1310eec29c) from 'http://x[.]ofo[.]ac/update.exe' and connects to C&C servers 'api.active-microsoft.com' and 'css.bustring.com'.

Malware distributed from the Aliyun Cloud server

URL	Observed time	MD5	Hosted malware	C&C server
https://chuanqiliebiao-1314[.]oss-cn-shanghai[.]aliyuncs[.]com/wp-content/ssl.exe	2022-10-28	8ae14f0b21f9689418525b716a47bb23	BEACON	api.active-microsoft.com css.bustring.com
https://chuanqiliebiao-1314[.]oss-cn-shanghai[.]aliyuncs[.]com/wp-content/plugins/Ssl-update.exe	2023-03-06	5f7764e2c6fd2185f4df9fb2873f1fe8	TROCHILUS	bro.brorth.com
https://chuanqiliebiao-1314[.]oss-cn-shanghai[.]aliyuncs[.]com/wp-content/update.msi	2023-04-14	5bae7a0ab1f9788f8fab89c5e8da5c07	Ping32	154.211.18.93
https://chuanqiliebiao-1314[.]oss-cn-shanghai[.]aliyuncs[.]com/wp-content/v2.msi	2023-05-19	83ae23baeb8ca5f7053aa0d62d4ce806	Ping32	154.211.18.193

Table 3: Malware hosted on the private server.

The URL https://chuanqiliebiao-1314[.]oss-cn-shanghai[.]aliyuncs[.]com/wp-content/v2.msi is set to download the installer of an updater. The updater subsequently downloads and deploys the latest version of the *Ping32* tool to the target system:

- v2.msi (MD5: 83ae23baeb8ca5f7053aa0d62d4ce806)
  - Installer of *Ping32* updater

After the installation is done, it further executes:

- setup_ip_154.211.18.193.exe (MD5: ffbfb09021bad36aeaf4a8f9bdd0d324)
  - Ping32 updater
  - Signed by a certificate with the organization name 'Shandong Anzai Information Technology CO., Ltd.', valid to 2019 Oct 18, 11:59 PM GMT

The URL https://chuanqiliebiao-1314[.]oss-cn-shanghai[.]aliyuncs[.]com/wp-content/plugins/Ssl-update.exe will download a dropper (MD5: 5f7764e2c6fd2185f4df9fb2873f1fe8), dubbed 'DOUBLESTEP', with the *Google Chrome* icon. The dropper is embedded with TROCHILUS (MD5: f39c17172d605c0195d61d72173758c1) with the RC4 key 'a3s1df3a1sd3ad18a0s8daf0':

- Ssl-update.exe (MD5: 5f7764e2c6fd2185f4df9fb2873f1fe8)
  - DOUBLESTEP dropper
  - *Windows* executable with *Google Chrome* icon
- N/A (MD5:f39c17172d605c0195d61d72173758c1)
  - Customised TROCHILUS backdoor

The related infra cs.bustring.com was abused by two different simply designed downloaders, FIBERSTEP and DATASTEP. The difference is the APIs and protocols. FIBERSTEP uses APIs like InternetOpenUrlA, InternetReadFile and CreateFiber for downloading and executing the downloaded file:

- upload.exe (MD5: 4638bea432f067799818131b1d6b3e5c)
  - FIBERSTEP downloader
  - Download URL: http://cs[.]bustring[.]com:80/c/msdownload/update/others/2021/11/
- (noname) (MD5:20cb281a8b8aa5a107a9bc28d2666beb)
  - Encrypted payload downloaded by FIBERSTEP

The payload is decrypted as BEACON:

- (noname) (MD5:de35a4657d1474fde2720c754b81fad8)
  - BEACON
  - C&C: cs.bustring.com, css.brorth.com

On the other hand, DATASTEP uses low-level APIs like socket, connect and VirtualProtect to achieve the same goal:

- untitled5.exe (MD5: 8d15b18af679f41d342612bacfe4b448)
  - DATASTEP downloader
  - C&C: 154.196.13.135 (resolved by cs.bustring.com)
  - Payload is not available

Distribute Cobalt Strike BEACON from the cloud

From March to August 2023, UNC3569 conducted an operation leveraging *GitHub* accounts 'kkecho123' and 'powerhelp' to distribute its backdoor.

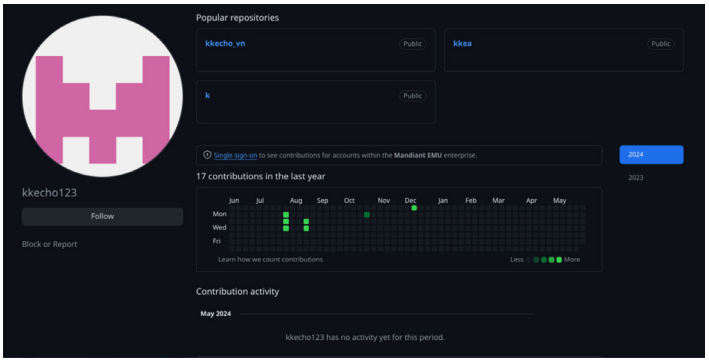


Figure 6: GitHub account 'kkecho123' used to distribute backdoor.

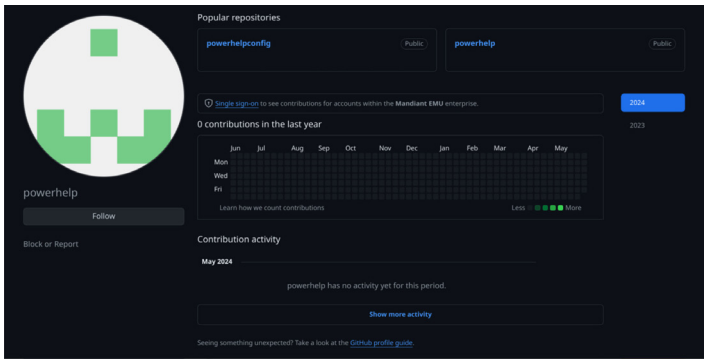


Figure 7: GitHub account 'powerhelp' used to distribute backdoor.

UNC3569 used BEACON stager samples to download additional payloads from *GitHub* accounts. This allowed the attacker to easily switch payloads as needed. The *GitHub* change logs show evidence that the actor uploaded UNC3569's GRAYRABBIT (MD5: ea5deef56e6dab4477fe68ed57eda16e) after having uploaded BEACON (MD5: dafca5bf5c132bede69df7f272efc11b):

- msinfo64.exe (MD5: 4a97cfabeda07881aef8f5f406100685)
  - Get URL file from https://raw[.]githubusercontent[.]com/kkecho123/k/main/vbsf.vpn
- Vbsf.vpn (MD5: 7692afef71320aeee7de6845576c9c35)
  - vbsf.vpn on the *GitHub* account
  - Encrypted BEACON payload uploaded to *GitHub* at 2023-05-22
- Vbsf.vpn (MD5: 249bbb18b91e9639719427a3691a1bee)
  - vbsf.vpn on the *GitHub* account
  - Encrypted BEACON payload uploaded to *GitHub* at 2023-08-15
- Vbsf.vpn (MD5: ea5deef56e6dab4477fe68ed57eda16e)
  - vbsf.vpn on the *GitHub* account
  - Encrypted GRAYRABBIT payload uploaded to *GitHub* on 2023-08-16
- (Noname) (MD5: 8def8c562e718d38291baae0dbeb683e)
  - GRAYRABBIT
  - Decrypt from (MD5: ea5deef56e6dab4477fe68ed57eda16e)
  - C2: 103.218.242.86:443

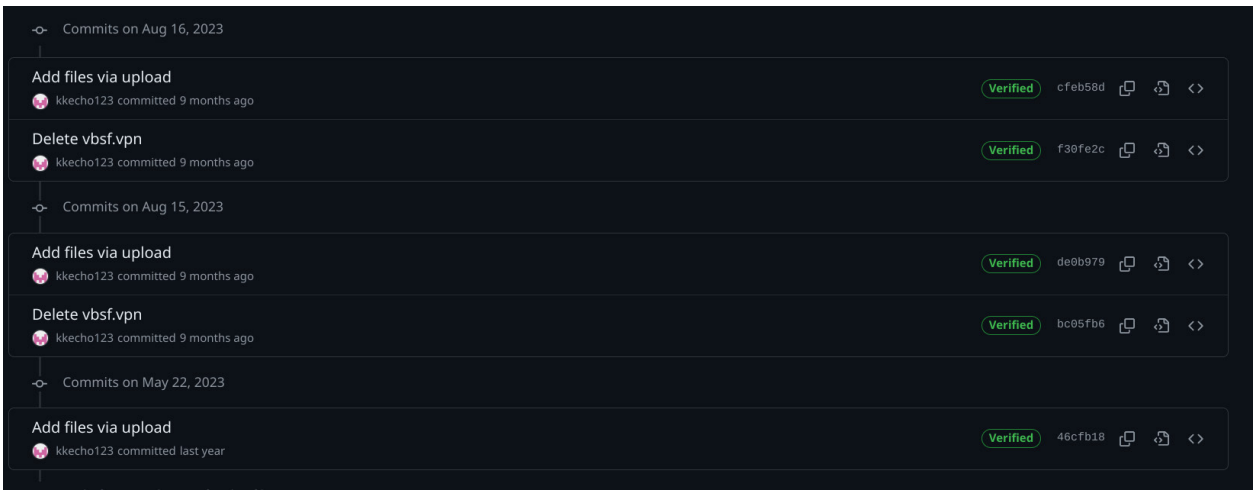


Figure 8: Change logs on GitHub.

Among the malware samples used, one stager shellcode is executed by the Rust shellcode runner (MD5: c42f517698f4b8130057c81fae239f73) with a unique PDB string. The C2 domain is a fake *Microsoft* domain, 'beta-microsoft.com'.

- art.exe (MD5: C42f517698f4b8130057c81fae239f73)
  - Rust-based shellcode runner with BEACON embedded
  - PDB: C:\Users\MECHREVO\work\shellcode_runner\target\release\deps\shellcode_runner.pdb
  - C2: beta-microsoft.com

UNC3569 used this launcher (MD5: d108bee31eae53a247991bb9770af0bb) to run GRAYRABBIT:

- (Noname) (MD5:d108bee31eae53a247991bb9770af0bb)
  - Rust-based shellcode runner with GRAYRABBIT embedded
  - PDB: C:\Users\MECHREVO\work\shellcode_runner\target\release\deps\shellcode_runner.pdb
  - Decrypted payload 1391b5fbb9e53f952d51a23b3ebf9d43
- (Noname) (MD5:1391b5fbb9e53f952d51a23b3ebf9d43)
  - Shellcode to launch embedded GRAYRABBIT
- (Noname) (MD5: 8def8c562e718d38291baae0dbeb683e)
  - GRAYRABBIT
  - C2: 103.218.242.86:443

Use of DRAFTGRAPH backdoor

UNC3569 leverages cloud services like *OneDrive* for operational infrastructure and strategic cloud storage to complement operations. In one example, a DRAFTGRAPH sample (MD5: 2377abd182e56db339e005c5cf9448c7) was configured to abuse *OneDrive* as its C2 server. The attacker had other payloads stored in the cloud space, including SIDESTEP loader, the CROSSWALK backdoor, the GRAYRABBIT backdoor, and a SIDESTEP sample with the OXEEYE tool.

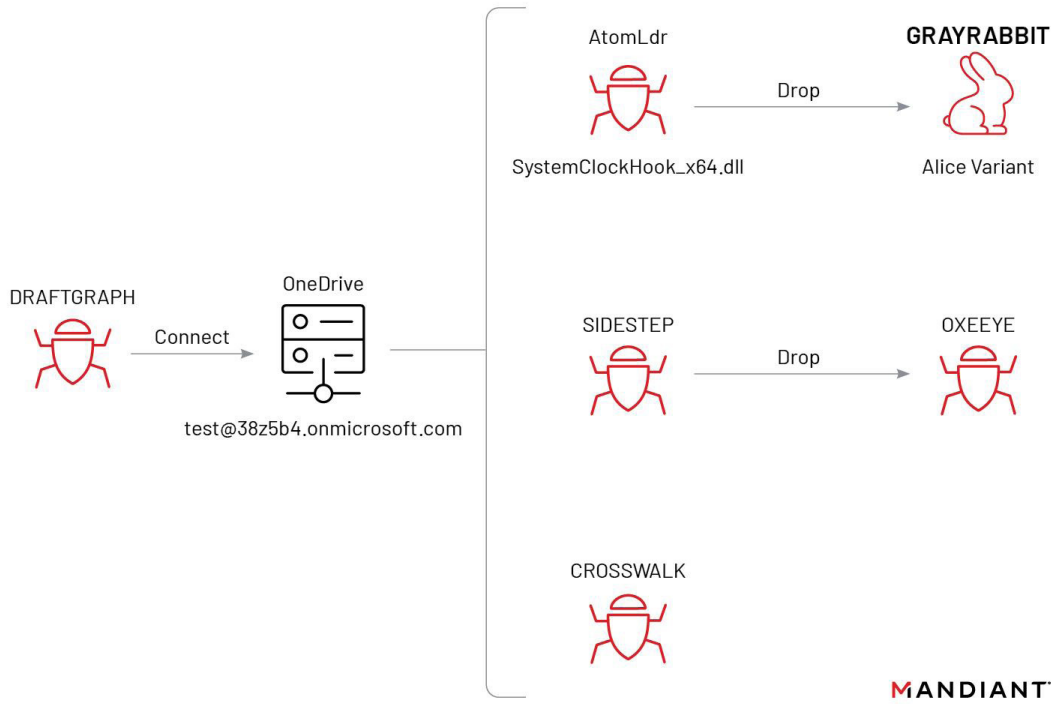


Figure 9: UNC3569 has GRAYRABBIT, CROSSWALK, SIDESTEP and DRAFTGRAPH in its arsenal.

Referring back to the *GitHub* project kkecho123/kkecho_vn mentioned in the previous section, the attacker had another DRAFTGRAPH backdoor sample (MD5:3d5a962d4429d6de28a38e46d9b73d12) on the *GitHub* project, but it was later deleted.

Figure 10: Change log of DRAFTGRAPH deletion.

Use of publicly available botnet tool

UNC3569 has used a commercial botnet tool created by the Chinese-speaking developer team @fucccccci. The exact nature of the relationship between UNC3569 and the developers remains unclear, with possibilities ranging from a simple purchase of the tool to a collaborative arrangement. UNC3569 uses this malware payload installer tool to deploy the SOGU backdoor, demonstrating a willingness to leverage external resources to enhance its operational capabilities.

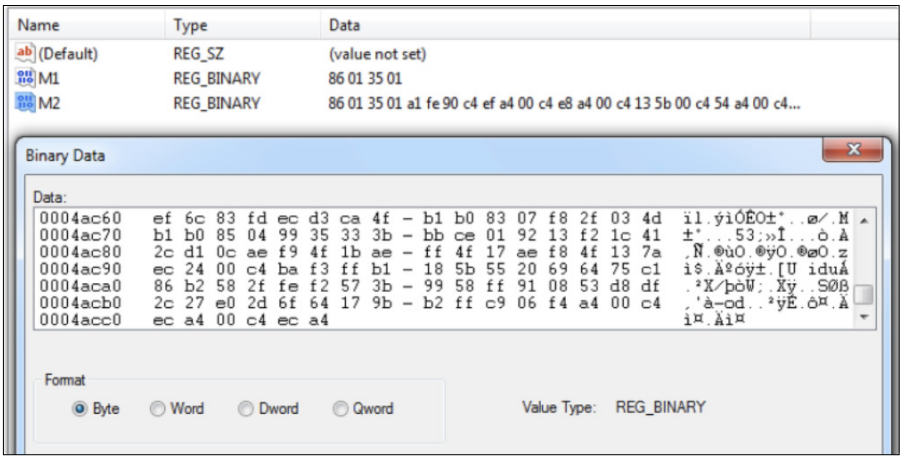
Figure 11: This tool is developed by a Chinese-speaking botnet tool developer team whose tools are sold via the Telegram account @fucccccci.

UNC3569 has a SOGU sample (MD5: 2355190aeed42b5698d7307c51fbe07c) that calls back to the group's C2 domain 'ap123.fbi.cab':

- AppInsta.dll (MD5: 2355190aeed42b5698d7307c51fbe07c)
  - Write the embedded payload DATAS_D32.res, DATAS_D64.res, DATAS_L32.res, DATAS_SD.res to system registry
    - »DATAS/D32.res (MD5: 3200133d1376de9bb17b80e7e87f60c1)
    - »DATAS/D64.res (MD5: ad17df8a613788cedc69a3063249da66)
    - »DATAS/L32.res (MD5: 8207afeffd0aac1403f93c30ebc27f65)
    - »DATAS/SD.res (MD5: 500adad3001db3bea1cec8b9c369f152)
  - FVTFiles.sys (MD5: d26ea66b33aa4731fb86007e988add1b)
    - »Decrypt from DATAS/D32, Windows System Driver x86
  - FVTFiles.sys (MD5: 28bb4efb9e1dc71b10d1500167be0793)
    - »Decrypt from DATAS/D64, Windows System Driver x64
  - (Noname) (MD5: 3c186f8c18a153b85a026e9613c1ec64)
    - »Decrypt from DATAS/L32, downloader to inject received payload into newly created svchost.exe process
  - (Noname) (MD5: 064feeaab875d0a7076f573e90f34570)
    - »Decrypt from DATAS/SD, SOGU backdoor payload
    - »C2: ap123.fbi.cab

Upon successful exploitation, the dropper initiates a series of actions on the compromised system. These include:

- Find and decrypt resource L32 (encrypted EXE component, second-stage payload downloader) and SD (shellcode, SOGU installer).
- Combine the decrypted payloads together (attach the shellcode behind the downloader).
- Encrypt the combined payloads using a four-byte XOR key.
- Create registers under the key 'HKLM\SOFTWARE\DtSft\d1\' to preserve the payload, decryption key and timestamp.
- Check the current process architecture is x86 (or x64) and decrypt the corresponding resource D32 (or D64) driver component to the system folder.
- Register a new system service for persistence.



M1: Preserve hard-coded four-byte binary timestamp.

M2: The binary data preserved with the format [four-byte timestamp preserved in M1 (0x86013501) + encrypted payload (size of L32 + size of SD)]

M3: The XOR key used to decrypt the encrypted payload preserved in M3 ('ec a4 00 c4')

Figure 12: Concealed payload in the newly created registries.

The configuration block size of the embedded SOGU backdoor is 0x0150C, with the following information in the table:

```
sogu_config_encoder: sogu_20120123
sogu_config_size: 5388
hide_service: true
keylog: true
delete_self: true
memo1: 1234
memo0: 1234
```

The FMSfProtect.sys component (MD5: e9194bd20e9bd6f6f5e572796514b285) and the method used for persistence with SOGU within the registry is identical to a demonstration sample provided by the @fucccci developer team.

The demo sample can be downloaded from the URL http://ddos[.]tttseo[.]com/ddos/ddos.zip. The dropper exhibits identical behaviours in executing an embedded SOGU backdoor and maintaining the payload within the same registry key, specifically 'HKLM\\SOFTWARE\\DtSft\\d1\\M2'. The demo SOGU sample employs a distinct password, 'chinatongyi2022', within its configuration block. This password translates to '中国统一2022', signifying 'Chinese unification'.

```
C2: mail.tttseo.com:53
sogu_config_encoder: sogu_20141118b
campaign_id: fish
password: chinatongyi2022
dns-server: 8.8.8.8
dns-server: 8.8.4.4
dns-server: 114.114.114.114
hide_service: true
keylog: true
delete_self: true
Extended Configuration Parameters
lateral_icmp_port: 1357
sogu_config_size: 13988
install_type: NONE
lateral_tcp_port: 1357
reg_hive: HKEY_LOCAL_MACHINE
lateral_custom_ff_port: 1357
lateral_udp_port: 1357
screenshot_options: 16 %AUTO%\\DSSM\\screen false 50 10 3 50
process_inject_targets_SP:
 %windir%\\system32\\rundll32.exe
 %windir%\\system32\\dllhost.exe
 %windir%\\system32\\msiexec.exe
```

The SOGU backdoor uses 'mail.tttseo.com' as its C2 domain. This domain is noteworthy as it is a sibling domain of 'ddos.tttseo.com', where the @fucccci developer team's home page is located.

C2 INFRASTRUCTURE ANALYSIS

Geolocation and service provider preference

The threat actor likes to rent a serial number of IP addresses under the same class B or class C subnet for operational convenience. That's why we see more than 67% of the C2 server IP addresses in the same location: Hong Kong and Singapore.

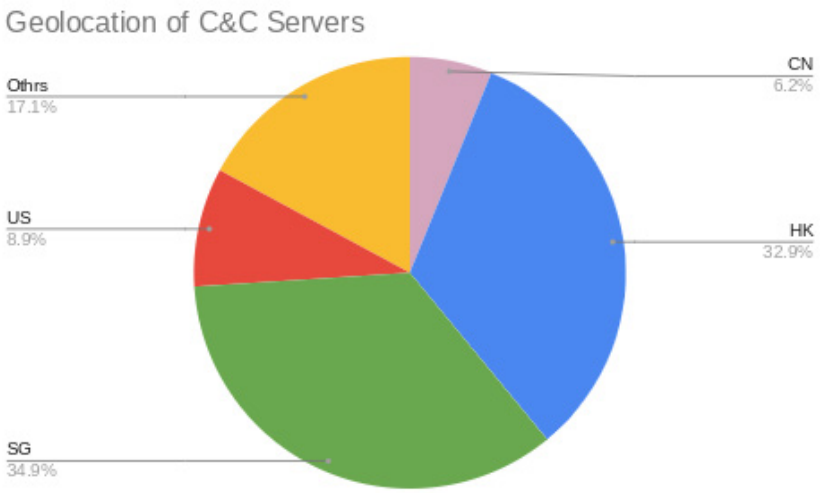


Figure 13: Most of the C2 servers are located in Hong Kong and Singapore.

Precisely because of this tactic, about 50% of the IP addresses originate from the actor's favourite service providers (i.e. *Choopa*, *Alibaba Cloud* and *IT Novation Cloud*).

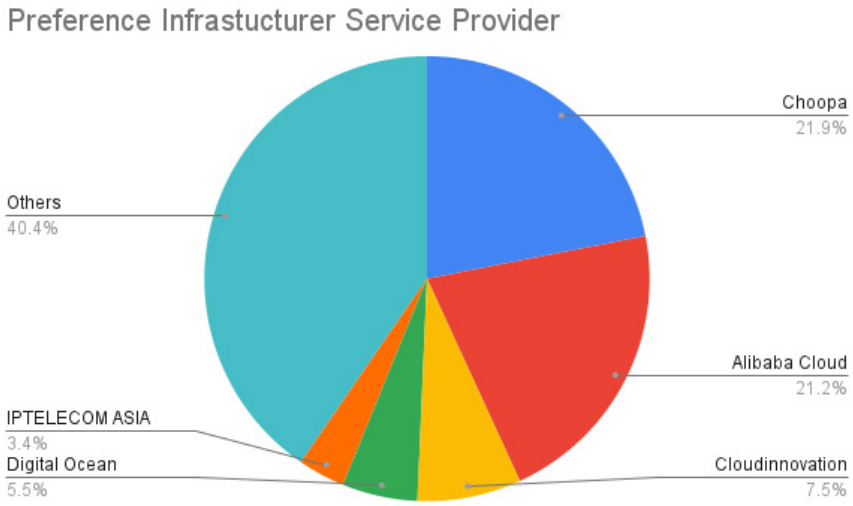


Figure 14: Most of the C2 servers are from Choopa, Alibaba Cloud and IT Novation Cloud.

Command-and-control domains spoof legitimate websites, subdomains created for malware families

Our research shows that UNC3569 often registers C2 domains that spoof well-known organizations and brands. This is most likely done to blend in with legitimate traffic and evade detection. These domains often serve as C2s for multiple different malware families, potentially even spanning different operations.

Interestingly, UNC3569 uses sibling subdomains under the same domain zone, with each subdomain seemingly allocated to a different malware family. Based on our observations and research, some of the sibling domains appear to register additional domains for their own operating convenience. The sibling domains that start with 'cs' are associated with the

Cobalt Strike BEACON, and the sibling domain that starts with 'plug' is associated with SOGU, also known as PlugX. This suggests that UNC3569 uses specific subdomains within a domain to host and distribute different malware families.

Fbi.cab

The fake FBI domain is one of the group's favourites. The actor registered at least 11 different subdomains under this domain zone, five of which are observed to be used as the C2 server for malware such as KEYPLUG, SOGU, Cobalt Strike BEACON, GRAYRABBIT and Gh0st.

We summarize our findings on this infrastructure in Table 4.

C&C server	Malware	MD5	Description
v2.fbi.cab	GRAYRABBIT	c97fddb7a96f168b1eccaf4c95468dba	
ap123.fbi.cab	SOGU	2355190aeed42b5698d7307c51fbe07c	SOGU sample wrapped by the commercial botnet tool from @fucccci
xp.fbi.cab	SOGU	d751e18272ec62a33d5468963b93ab2b	
cs.fib.cab	BEACON.Stager	bf426ecb47ec9bc9a4c8ab1ed0268663	Masquerades as document file
sf.fbi.cab	GH0ST	7b027d93ebd128260a043bb06ad1cf51	Masquerades as *Adobe Manager*
gen.fbi.cab	KEYPLUG.LINUX	f9029a1455738901380d887f3b3ca6ad	
os.fbi.cab	KEYPLUG.LINUX	e9021b834ff35ae4234841bffbe3c099	

Table 4: Malware associated with fbi.cab subdomains.

Active-microsoft.com

This fake *Microsoft* domain zone is another of UNC3569's favourites. The subdomains are associated with SOGU, Cobalt Strike BEACON, and the downloader LITTLEEGRET.

C&C server	Malware	MD5	Description
cdn.active-microsoft.com	BEACON.Stager	8ae14f0b21f9689418525b716a47bb23	Masquerades as *Adobe Manager*
ns1.active-microsoft.com	BEACON	3a9c326214d16782314e29a5c7a95dc0	
ns2.active-microsoft.com	BEACON	3a9c326214d16782314e29a5c7a95dc0	
plug.active-microsoft.com	SOGU	99a6637268d7965fa60c8f8a004b2cf7	SOGU sample wrapped by the commercial botnet tool from @fucccci
tjj.active-microsoft.com	LITTLEEGRET	5a122e86a8f134e42ebae8510404df3d	Simple downloader to run second stage

Table 5: Malware associated with active-microsoft.com subdomains.

Ofo.ac

Under this domain zone, UNC3569 has used the *Linux* backdoor HELLOBOT together with SOGU and Cobalt Strike BEACON in its operations.

C&C server	Malware	MD5	Description
aw.ofo.ac	SOGU	5ba969da1347cb0e8dea7513f0dac827	SOGU sample wrapped by the commercial botnet tool from @fucccci
cdn.ofo.ac	SOGU	648ea096099a8bf0c32d0a8ac04d4d68	SOGU sample wrapped by the commercial botnet tool from @fucccci
go.ofo.ac	HELLOBOT	41eda76872fa2a966e1d1ed16e88cc6b	

Table 6: Malware associated with ofo.ac subdomains.

Apart from the malicious domain zone above, the actor also registered a number of other malicious domain zones, shown in Figure 15.

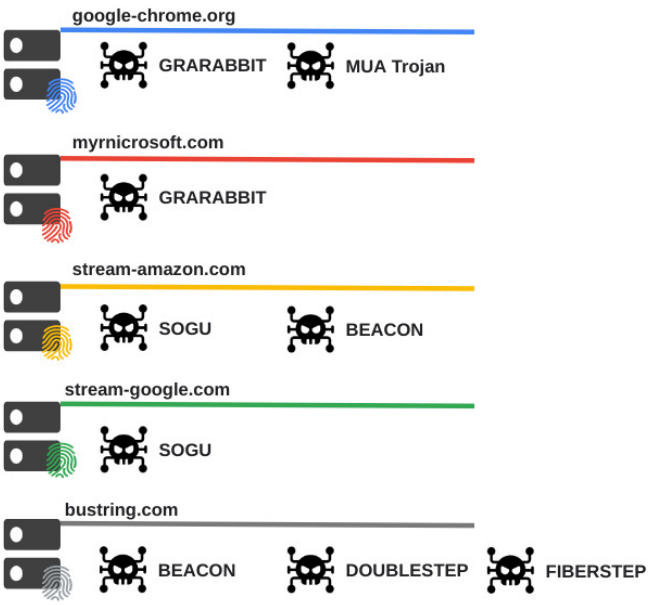


Figure 15: Malware on different domain zones.

Notably, the forged *Google Chrome* domain 'version.google-chrome.org' was found in a GRAYRABBIT sample, which masqueraded as an *Adobe Flash* application. Although we didn't find other backdoors associated with the rest of the sibling domains under the google-chrome.org zone, two of them ('data.google-chrome.org' and 'xss.google-chrome.org') resolved to the same IP address during the suspect operation time (18 Aug 2022 – 31 Dec 2022).

Extend infrastructure efficiently with similar GRAYRABBIT server configuration

Based on commonalities in UNC3569's infrastructure, we surmise that the actor deployed its operation environment either on different servers with similar configurations or on a copied VM image, to use the new infrastructure more efficiently.

Server IP	Backdoor	Service provider	Open ports
8.218.120.134	GRAYRABBIT	ALIBABA-CN-NET Alibaba US Technology Co., Ltd. (45102)	443/UNKNOWN, 139/NETBIOS, 445/SMB, 3389/RDP, 47001/HTTP
8.218.124.102	GRAYRABBIT	ALIBABA-CN-NET Alibaba US Technology Co., Ltd. (45102)	443/UNKNOWN, 9999/UNKNOWN, 139/NETBIOS, 445/SMB, 3389/RDP
8.210.232.195	GRAYRABBIT	ALIBABA-CN-NET Alibaba US Technology Co., Ltd. (45102)	443/UNKNOWN, 139/NETBIOS, 445/SMB, 3389/RDP, 7001/UNKNOWN, 47001/HTTP
103.218.242.86	GRAYRABBIT & CROSSWALK	UCLOUD-HK-AS-AP UCLOUD INFORMATION TECHNOLOGY HK LIMITED (135377)	443/UNKNOWN, 139/NETBIOS, 445/SMB, 3389/RDP, 5985/HTTP, 47001/HTTP
152.32.134.159	GRAYRABBIT & CROSSWALK	UCLOUD-HK-AS-AP UCLOUD INFORMATION TECHNOLOGY HK LIMITED (135377)	80/HTTP, 137/NETBIOS, 139/NETBIOS, 445/SMB, 3389/RDP, 5985/HTTP, 47001/HTTP

Table 7: GRAYRABBIT server configuration.

TOOLING

UNC3569 incorporates publicly available tools as well as some that are only available from private sources.

Private tools

UNC3569 uses a number of backdoors commonly shared among PRC-nexus operations:

- SOGU
- CROSSWALK
- KEYPLUG.LINUX
- ANGRYREBEL.LINUX

Other backdoors are observed in UNC3569 or suspected related clusters of activity:

- GRAYRABBIT
- HELLOBOT
- DRAFTGRAPH
- STREAMSERVE
- SERVEPLUG
- SKYNEEDLE
- ELECTRONAURA

UNC3569 also boasts .NET capability to enable a .NET-based malware dropper to deploy the SOGU backdoor. Among the SOGU samples, we found one with keyword 'whg', which is evidence that this shellcode source could originally have been developed by the Chinese hacker Zhao Jibin [20]. This sample communicates with a different C2 domain, 'cdn.ofo.ac'.

GRAYRABBIT

GRAYRABBIT is one of the malware families that UNC3569 has used repeatedly over the years across multiple different attacks. It is a lightweight and simple backdoor that supports simple file operation, system information collection, running modularized plugins, and executing a remote command shell.

UNC3569 seems to use GRAYRABBIT as its first-stage trojan for early stage infiltration. The attackers have varied the malware that delivers GRAYRABBIT and used it together with other powerful remote control tools, but seem to be most comfortable with GRAYRABBIT. We have continuously observed their use of GRAYRABBIT since November 2021.

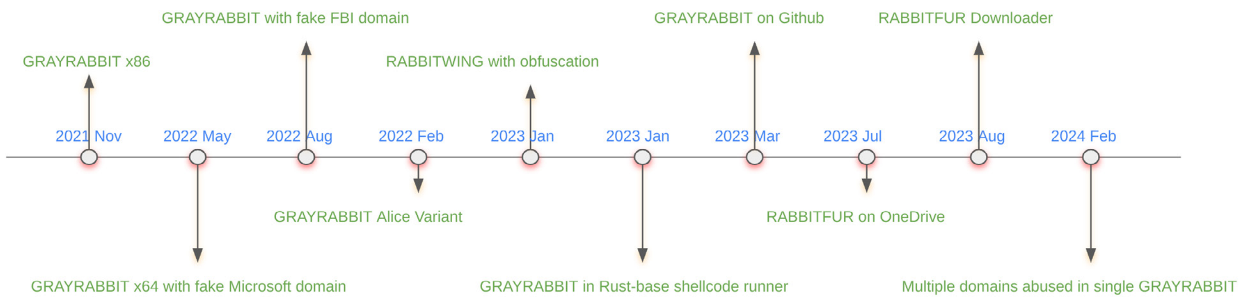


Figure 16: GRAYRABBIT activity timeline.

GRAYRABBIT has both x86 and x64 variants.

The earliest x86 sample (MD5: 6467ecbbb69aaab966f02ff27d359e42) is a C++ application that was downloaded from the malicious domain 'wps-cn.com'. The domain name likely references *WPS Office*, a popular word processor in China. This GRAYRABBIT backdoor communicates with 152.32.134.159, which is also set up as a CROSSWALK C2 server on a different traffic port. Notably, UNC3569 abused another server, 103.218.242.86, for both GRAYRABBIT and CROSSWALK as a C2 server on different ports, again around 2023–2024.

MD5	Filename	C2	Timestamp	Description
9ce73f397c765588aee3c9a82d8579e6	updatexxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.exe	152.32.134.159:443	First seen timestamp: 2021-11-13 23:38:04	Dropper, CROSSWALK payload has no proxy credential, ITW=http://wps-cn[.]com/updatexxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.exe
6467ecbbb69aaab966f02ff27d359e42	corexxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.exe	152.32.134.159:9999	First seen timestamp: 2021-11-15 22:26:58	ITW=http://wps-cn[.]com/corexxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.exe

Table 8: CROSSWALK malware dropper and malware sample details.

The earliest x64 version of GRAYRABBIT (MD5: 0921396ce1da2ac2bebb0c76b11a39dd) appeared in May 2022. This sample differs from the initial x86 sample in that part of the related remote commands were replaced by numbers. This made the file commands consistent with the earliest x86 variant.

GRAYRABBIT seems to be used as a disposable first-stage trojan. Compared to the variety of different dropper and downloader samples used together with GRAYRABBIT, the backdoor itself has evolved very little over two years.

Most of the samples share mostly the same code structures and only have a few minor modifications, such as encrypting the C2 domain and changing the number of export functions. This suggests that this tool may be a disposable backdoor with more complex tools saved for later infection stages.

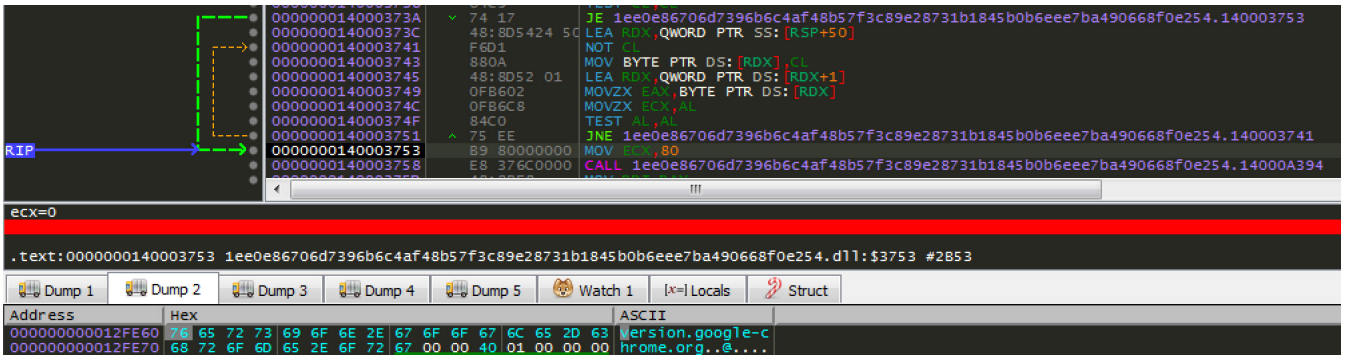


Figure 17: C2 domain decryption by simple XOR operation.

The earliest x86 variant (MD5: 6467ecbbb69aaab966f02ff27d359e42) and the earliest x64 variant (MD5: c97fddb7a96f168b1eccaf4c95468dba) share highly similar command structure. Notably, however, the file-related commands replace string commands in favour of numeric commands in the x64 variant.

CMD string 1	CMD string 2	Command code	Description
msg	-	core	Used to run CoreClientInstall or CoreClientStart PE export functions
msg	-	0x1	Create CMD.exe console; if console exists, execute CMD command
msg	-	0x2	Terminate CMD.exe console
msg	-	0x3	Initialize and run modules from the C2 controller
msg	-	0x4	Report Hostname, UserName, ProcessID and module filename to C2 server Data in format: [Hostname]+[Username]+[Module Filename]:[ProcessID]|
msg	-	0x5	Terminate CMD.exe console and backdoor process
msg	-	0x7	Execute module function
file	f_c	(0x665F6300)	Copy file
file	f_e	(0x665F6500)	Execute file
file	f_s	(0x665F7300)	Search file

Table 9: GRAYRABBIT x86 command structure.

CMD string 1	CMD string 2	Command code	Description
msg	-	core	Used to run CoreClientInstall or CoreClientStart PE export functions
msg	-	0x1	Create CMD.exe console; if console exists, execute CMD command
msg	-	0x3	Execute code or function and write execution results to the log file
msg	-	0x4	Terminate CMD.exe console
msg	-	0x5	Initialize and run modules from the C2 controller
msg	-	0x6	Report Hostname, UserName, ProcessID, and module filename to C2 server Data in format: [Hostname]+[Username]+[Module]
msg	-	0x7	Terminate CMD.exe console and backdoor process
file	0x63		Copy file
file	0x65		Execute file
file	0x73		Search file

Table 10: GRAYRABBIT x64 command structure.

The C2 traffic pattern response packets related to GRAYRABBIT samples can be divided into four parts dedicated to command strings, export functions, one-byte command codes for the msg functionality, and a four-byte command code for the command functionality. The following packet structure response delineation was observed:

Data offset	Bytes	Received content	Description
Recv_data [0]		DWORD command string ‘msg’ or ‘file’	Specifies command string type as msg or file-related function
Recv_data [12]		Command string ‘core’	Specifies core command string used to run export functions related to GRAYRABBIT payload
Recv_data [268]	1 byte	Command code for msg series	1-byte numeric code to designate specific msg-related commands
Recv_data [276]	4 bytes	Command code for file series	4-byte string value to designate specific file-related commands

Table 11: Traffic pattern of GRAYRABBIT.

Some of the x64 variant samples have a unique PDB string with username ‘alice’, but we don’t see many significant differences between the rest of samples.

For the reader’s convenient reference, we summarize the different variants of GRAYRABBIT and related tools in Table 12.

Variant	Launcher	Features
GRAYRABBIT (x86)	N/A	1. Exports: CoreClientInstall, CoreClientStart, Start 2. C2 domain in plaintext
GRAYRABBIT (x64)	RABBITCAVE, RABBITWING, RABBITFUR	1. Two types of exports: - CoreClientInstall, start, start - CoreClientInstall, CoreClientStart, start 2. Three types of C2 domain format: - Plaintext - Divided into a couple of Hexadecimal strings - Byte operation encoded
GRAYRABBIT (x64 with Alice pdb string)	AtomLdr, RABBITMOUND	Alice variant 1. Exports: CoreClientInstall, CoreClientStart, Start 2. C2 domain in plaintext 3. Unique PDB string = ‘C:\Users\alice\source\sr\corecpp_r\x64\Release\corecpp.pdb’

Table 12: Versions of GRAYRABBIT.

Bypassing anti-virus

The UNC3569 actor prefers to use public tools or to quickly build new simple downloader or dropper components alongside obfuscation, shellcode, and simple encryption methods to escape detection by anti-virus software for the early stage of the attack.

Shellcode dropper

UNC3569 used a short section of shellcode as its backdoor launcher. This shellcode decrypts the embedded PE payload using a simple XOR operation and then executes the payload. The shellcode was interlaced into many *Windows* applications to deliver GRAYRABBIT.

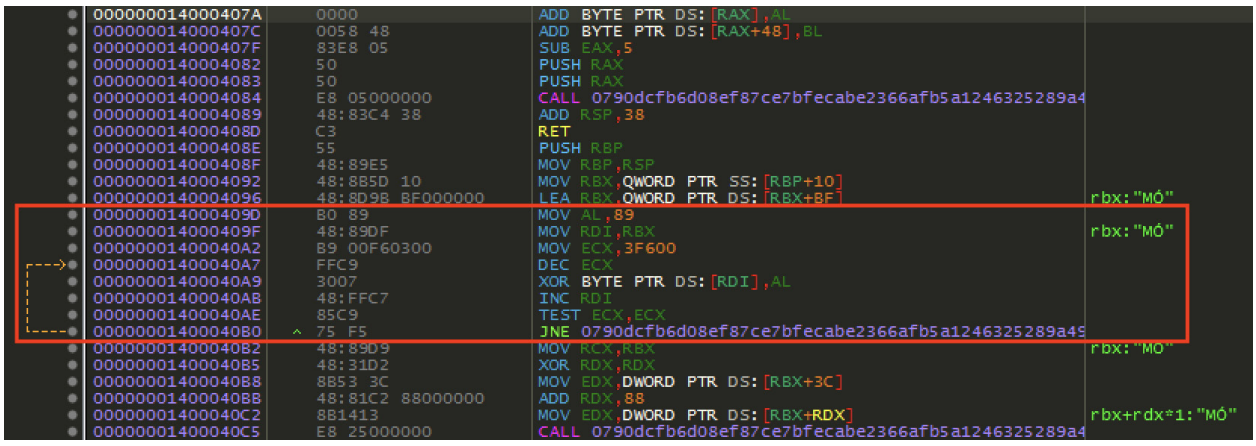


Figure 18: XOR decryption routine in the shellcode.

Shellcode runner and backdoor dropper

To evade detection and anti-virus software, UNC3569 developed multiple shellcode runners and backdoor droppers, and modified code structures, API usage, obfuscation techniques and decryption routines to make detection increasingly challenging.

The use of a Rust-based shellcode runner – potentially a commercial tool shared among different actors – may be an indication of the group's approach and blending with other activity.

RABBITMOUND

API combination:
VirtualAlloc,
VirtualProtect
CreateThread

Decryption routine:
Single-byte XOR decryption routine

```
lib_kernel32 = GetModuleHandleA("kernel32.dll");
_VirtualAlloc = GetProcAddress(lib_kernel32, "VirtualAlloc");
_lib_kernel32_ = GetModuleHandleA("kernel32.dll");
GetProcAddress(_lib_kernel32_, "VirtualProtect");
lib_kernel32__ = GetModuleHandleA("kernel32.dll");
_CreateThread = GetProcAddress(lib_kernel32__, "CreateThread");
lib_kernel32___ = GetModuleHandleA("kernel32.dll");
_WaitForSingleObject = GetProcAddress(lib_kernel32___, "WaitForSingleObject");
qmemcpy(&v19, &unk_40404A, 0x3F4ABui64);
v10 = (void (__fastcall *)(__int64, signed __int64))_WaitForSingleObject;
v11 = ((__int64 (__fastcall *)(_QWORD, signed __int64, signed __int64, signed __int64))_VirtualAlloc)(
        0i64,
        0x3F4ABi64,
        0x3000i64,
        64i64);
v12 = (char *)v11;
v13 = v11;
v14 = 0i64;
qmemcpy(v12, &v19, 0x3F4ABui64);
do
  *(_BYTE *)(v13 + v14++) ^= 1u;
while ( v14 != 259242 );
v15 = 0;
v16 = ((__int64 (__fastcall *)(_QWORD, _QWORD, __int64, _QWORD, int, char *))_CreateThread)(
```

Figure 19: RABBITMOUND.

RABBITNEST

API combination:
VirtualAlloc
VirtualProtect
RtlCopyMemory
CreateThread

Decryption routine:
16-byte key XOR decryption routine

```
ModuleHandleW = GetModuleHandleW(L"kernel32.dll");
VirtualAlloc = (LPVOID (__stdcall *)(LPVOID, SIZE_T, DWORD, DWORD))GetProcAddress(ModuleHandleW, "VirtualAlloc"
v8 = GetModuleHandleW(L"kernel32.dll");
GetProcAddress(v8, "VirtualProtect");
v9 = GetModuleHandleW(L"kernel32.dll");
CreateThread = (HANDLE (__stdcall *)(LPSECURITY_ATTRIBUTES, SIZE_T, LPTHREAD_START_ROUTINE, LPVOID, DWORD, LPDW
v11 = GetModuleHandleW(L"kernel32.dll");
WaitForSingleObject = (DWORD (__stdcall *)(HANDLE, DWORD))GetProcAddress(v11, "WaitForSingleObject");
v13 = GetModuleHandleW(L"kernel32.dll");
RtlCopyMemory = GetProcAddress(v13, "RtlCopyMemory");
memcpy(Src, qword_14000A370, sizeof(Src));
v22 = xmmword_14002A8C0;
v21 = xmmword_14002A8D0;
sub_1400010AC(v23);
sub_14000157A(v23, Src, 0x20550i64);
memcpy(v24, Src, 0x20542ui64);
for ( i = 0i64; i != 8277; ++i )
  v24[i] = (__int128)_mm_xor_ps((__m128)v24[i], (__m128)keystring_14002A8E0);
memset(v26, 0, 0x3F4ACui64);
v20 = 0x3F4AC;
```

Figure 20: RABBITNEST.

Rust-based shellcode runner

API combination:
LoadResource
VirtualAlloc

```
000000013FF62BDE   0F2985 00010000      movaps xmmword ptr ss:[rbp+100],xmm0
000000013FF62BE5   48:8D05 442B0200     lea rax,qword ptr ds:[13FF85730]          000000013FF85730:&"src\\main.rs"
000000013FF62BEC   48:894424 20         mov qword ptr ss:[rsp+20],rax             [rsp+20]:&"src\\main.rs"
000000013FF62BF1   48:8D0D E0280200     lea rcx,qword ptr ds:[13FF854D8]          000000013FF854D8:"called `Result::unwrap()` on an `Err` v
000000013FF62BF8   4C:8D0D 09290200     lea r9,qword ptr ds:[13FF85508]           r9:&"PE"
000000013FF62BFF   4C:8D85 00010000     lea r8,qword ptr ss:[rbp+100]
000000013FF62C06   BA 2B000000          mov edx,2B                                2B:'+'
000000013FF62C0B   E8 20140200          call 7ae55c34aedc14e8ace09ad2f5cc0d74b48d5aa
000000013FF62C10   E9 75010000          jmp 7ae55c34aedc14e8ace09ad2f5cc0d74b48d5aa6
000000013FF62C15   66:C785 30010000 0A0( mov word ptr ss:[rbp+130],A               A:'\n'
000000013FF62C1E   48:C785 38010000 000( mov qword ptr ss:[rbp+138],0
000000013FF62C29   48:8D8D 30010000     lea rcx,qword ptr ss:[rbp+130]
000000013FF62C30   E8 5B0A0000          call 7ae55c34aedc14e8ace09ad2f5cc0d74b48d5aa
000000013FF62C35   41:B8 0A000000       mov r8d,A                                 A:'\n'
000000013FF62C3B   48:89F9              mov rcx,rdi
000000013FF62C3E   48:89C2              mov rdx,rax
000000013FF62C41   E8 06F40100          call <JMP.&FindResourceW>
000000013FF62C46   48:89C3              mov rbx,rax
000000013FF62C49   48:8B8D 38010000     mov rcx,qword ptr ss:[rbp+138]
000000013FF62C50   48:85C9              test rcx,rcx
000000013FF62C53   74 1A                je 7ae55c34aedc14e8ace09ad2f5cc0d74b48d5aa68
000000013FF62C55   48:8B95 30010000     mov rdx,qword ptr ss:[rbp+130]
000000013FF62C5C   48:85D2              test rdx,rdx
000000013FF62C5F   74 0E                je 7ae55c34aedc14e8ace09ad2f5cc0d74b48d5aa68
000000013FF62C61   48:01D2              add rdx,rdx
000000013FF62C64   41:B8 02000000       mov r8d,2
000000013FF62C6A   E8 E1090000          call 7ae55c34aedc14e8ace09ad2f5cc0d74b48d5aa
000000013FF62C6F   48:85DB              test rbx,rbx
000000013FF62C72   75 1E                jne 7ae55c34aedc14e8ace09ad2f5cc0d74b48d5aa6
000000013FF62C74   48:8D05 CD2A0200     lea rax,qword ptr ds:[13FF85748]          000000013FF85748:"Failed to find resource.Failed to load
000000013FF62C7B   48:8985 38010000     mov qword ptr ss:[rbp+138],rax
000000013FF62C82   48:C785 40010000 180( mov qword ptr ss:[rbp+140],18
000000013FF62C8D   E9 ECF6FFFF          jmp 7ae55c34aedc14e8ace09ad2f5cc0d74b48d5aa6
000000013FF62C92   48:89F9              mov rcx,rdi
000000013FF62C95   48:89DA              mov rdx,rbx
```

Figure 21: Rust-based shellcode runner.

Downloader

We also observed that UNC3569 used a simple downloader, RABBITFUR, to deliver the GRAYRABBIT backdoor. The payload, hosted on an open directory server, is a shellcode with the GRAYRABBIT backdoor encoded by a single-byte

XOR operation. Forged *Microsoft* domains, including 'https://cloudwps[.]cn/chr0me/payload' and its sibling domains, serve as C2 domains for the backdoor.

Launcher

SIDESTEP is a shellcode launcher that UNC3569 used to run its reconnaissance tool OXEEYE.

```
flOldProtect = 0;
FileW = CreateFileW(String1, 0xC0000000, 3u, 0i64, 3u, 0x80u, 0i64);
FileMappingW = CreateFileMappingW(FileW, 0i64, 4u, 0, 0, 0i64);
if ( !FileMappingW )
  exit(0);
FileSize = GetFileSize(FileW, 0i64);
CloseHandle(FileW);
v3 = MapViewOfFile(FileMappingW, 4u, 0, 0, 0i64);
ProcessHeap = GetProcessHeap();
lpAddress = HeapAlloc(ProcessHeap, 8u, FileSize + 100);
memmove(lpAddress, v3, FileSize + 1);
sub_180001F50(v3, FileSize);
UnmapViewOfFile(v3);
Sleep(0x1F4u);
VirtualProtect(lpAddress, FileSize + 50, 0x40u, &flOldProtect);
((void (*)(void))lpAddress)();
```

Figure 22: SIDESTEP code snippets.

Component type	Component
Downloader	RABBITFUR
Dropper	AtomLdr, RABBITNEST, RABBITASH, RABBITMOUND, RABBITWING, Rust-based shellcode runner
Launcher	SIDESTEP

Table 13: UNC3569's malware components.

Public tools

UNC3569 uses public hacking tools for various reasons: proven effectiveness, adaptability, and cost-efficiency compared to developing custom tools. Public tools usually have a track record of success and can be customized to suit specific needs. This is also a cost-effective way for the group to achieve its purpose, whereas developing new custom tools from scratch requires significant time and resources.

The following are UNC3569's public toolsets that have served as resources for gaining access, reconnaissance, lateral movement, and credential harvesting.

Exploit tools

- Proxyshell-auto [4]
  - CVE-2021-34473
  - CVE-2021-31206
  - CVE-2021-34523
  - CVE-2021-31207
- Proxyshell [5]
  - CVE-2021-34473
  - CVE-2021-34523
  - CVE-2021-31207
- ProxyVulns [6]
  - CVE-2021-26855
  - CVE-2021-27065
  - CVE-2021-31195
  - CVE-2021-31196
  - CVE-2021-34473

  - CVE-2021-34523
  - CVE-2021-31207
- PaloAltoRceDetectionAndExploit [9]
  - CVE-2017-15944
- Other CVEs
  - CVE-2021-44228
  - CVE-2022-47986
  - CVE-2022-21587
  - CVE-2021-26857

Backdoors

- GH0ST
- BEACON
- TROCHILUS

Webshells

- BEHINDER (available on *GitHub* [21])
- REGEORG.NEO (available on *GitHub* [22])

Hacking tools

- HackBrowserData – a credential stealer that is available on *GitHub* [16]
- OXEEYE – a port forwarding and proxy utility, known on *GitHub* simply as 'iox' [3].

Mua-Remote-Control-Trojan (origin: MUA远控木马)

The GRAYRABBIT C2 domain 'version.google-chrome.org' and two other sibling domains resolved to the same IP address, '103.113.157.134', from 27 April 2022 to 16 November 2022. During this time, UNC3569 used this server as C2 for the Mua-Remote-Control-Trojan qwe.dll (MD5: ceb00e0548255bd6205a63f34a60deb7).

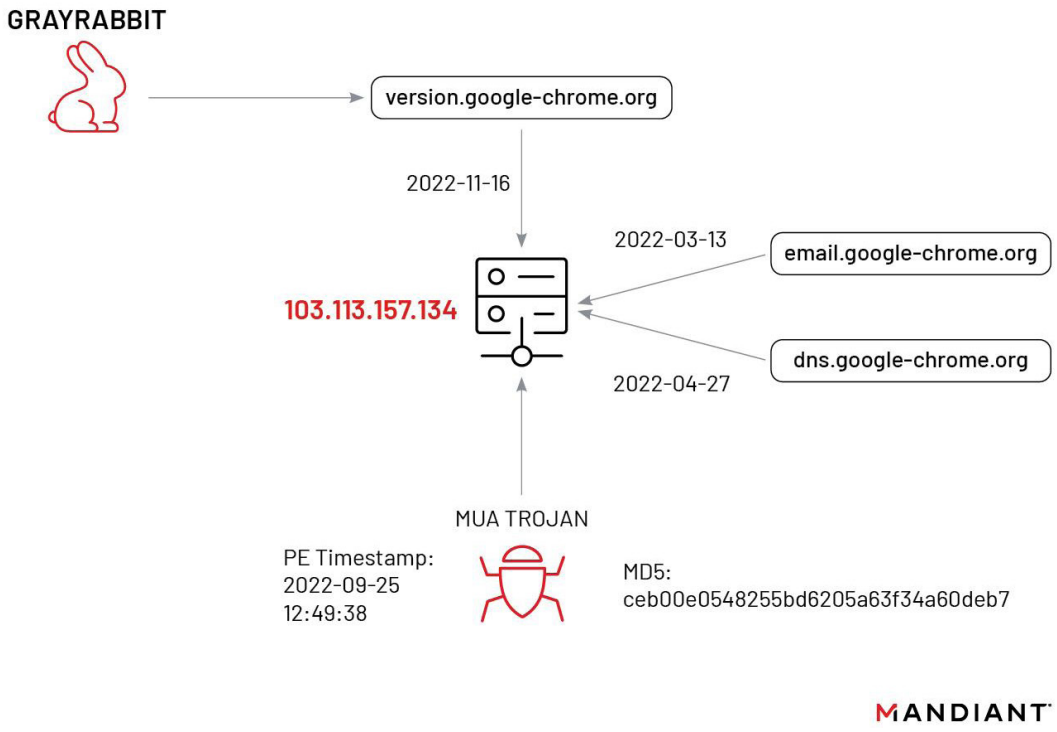


Figure 23: Connection between MUA trojan and GRAYRABBIT.

We surmise that this MUA trojan could be a test sample from UNC3569; however, we don't have evidence to confirm whether they used this simple open-source backdoor in a real-time attack operation, as opposed to just during training.

Commercial tools

NSecsoft Ping32

Ping32 (MD5: ffbfb09021bad36aeaf4a8f9bdd0d324) is a commercial hacking tool used by UNC3569. *Ping32* was originally developed for information technology (IT) department managers to monitor employees and manage mobile storage devices.

To keep the remote controller updated, we found a convenient *NSecsoft* updater also abused by the actor to deliver the latest version of controller.

The *NSecsoft* updater's filename determines the first-stage C2 server. When executed, it parses the filename, stores information related to the C2 server in the registry, and starts a second process. This process retrieves the stored information from the registry and fetches 'update.xml' from the C2 server. The XML file contains details about the next payload version, MD5 hash, and filename, which is hosted on the same C2 server. The following are the five different possible filename patterns:

1. 'setup_ip_[IP_addr].exe': the C2 is the [IP_addr] specified in the filename (port 28987 in our case). From the payload of the msi sample downloaded from *VT*, the filename of the updater is setup_ip_154.211.18.193.exe, but the information on *VT* shows that this file has been uploaded with a different filename / [IP_addr].
2. 'setup_wid_[string].exe': the downloader will send an HTTP GET request to cloud.nsecsoft.com::8987/ndns/[string]. If the string matches an existing ID, the server will return the C2 IP address and port.
3. 'setup_[string].exe': same as (2).
4. 'sg_setup.exe': the C2 will be a hard-coded address, in our case: 10.141.186.98 (intranet IP). Likely for testing.
5. Other than the four formats above, the downloader will terminate itself and not start the second process.

CONNECTING THE DOTS

Potential connection with UNC251

Artifacts identified from UNC3569's infrastructure, including multiple signals like a JARM fingerprint, certificate configuration, and habitual naming convention overlap with PRC-nexus cluster UNC3246, suggest either that these two groups may have access to shared resources or that they cooperate closely.

We found the following in terms of connections between UNC3569 and UNC3246:

- A unique JARM fingerprint ('services.jarm.fingerprint:22d19d00022d22d22c22d19d22d22dcade67768786e23ca695466fb7f94658') – evidence that the C2 server 8.218.48.121 has similar Transport Layer Security (TLS) configurations to two servers, 35.201.196.246 and 35.220.154.238, used by UNC3246.
- Both groups employ domains using 'fbi'.
- UNC3569 hosted a VMProtected ANGRYREBEL.LINUX on http://8[.]218[.]48[.]121/caonima, containing a profanity in Chinese Pinyin, 'caonima'. This word is also found in a C2 domain used by UNC3246, 'caonimade.11i.me'. We also see that UNC3246's TTPs contain lots of profanities, such as 'daji8' in 'tools.daji8.me'.

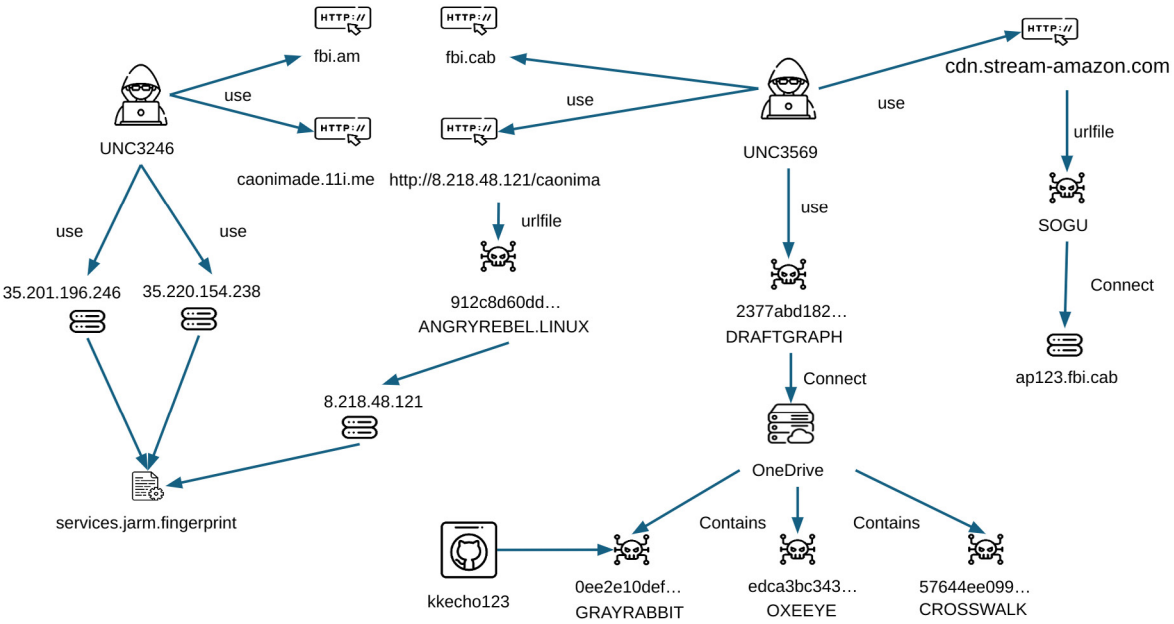


Figure 24: Connections between UNC3569 and UNC3246.

We found the following in terms of connections between UNC251 and UNC3246:

- A shared SSL certificate (MD5: 42f44f647e28f7a0c456811841bff28a)

```
- Version: 3 (0x2)
- Serial Number: 08:55:e5:ae:f0:5b:7c:ba:ba:f3:6a:0f:12:ff:0b:41
- Issuer: C = CN, O = "TrustAsia Technologies, Inc.", OU = Domain Validated SSL, CN =
TrustAsia TLS RSA CA
- Validity
    - Not Before: Dec 20 00:00:00 2019 GMT
    - Not After : Dec 19 12:00:00 2020 GMT
- Subject: CN = ascnhub.com
```

The SSL certificates are associated with the domains 'hack520.co.kr' and 'zhu.kr' used by UNC251 and UNC3246's 'github.wiki'. The 'hack520.co.kr' domain was reported to be used by China-nexus contractor hacker 'Hack520', who manages a VPS hosting service [23].

Similar to UNC251, UNC3569 also has various tools that demonstrate resource sharing among other contractor-nexus hackers, such as CROSSWALK and KEYPLUG.Linux.

Connection with i-SOON

In February 2024, an i-SOON data package was leaked in public and an interesting IP address, 8.218.67.52, appeared in the discussion logs.

According to the conversation logs shown in Figure 25, 兵哥 (wxid_c9yv0nsla3yn22) asked 濤哥 (wxid_zb45i0rc71tk21) for tunnelling server information for a person.

Wxid_zb45i0rc71tk21 responded by providing the proxy server 8.218.67.52 and TCP tunnel information and claimed that this was their own server.

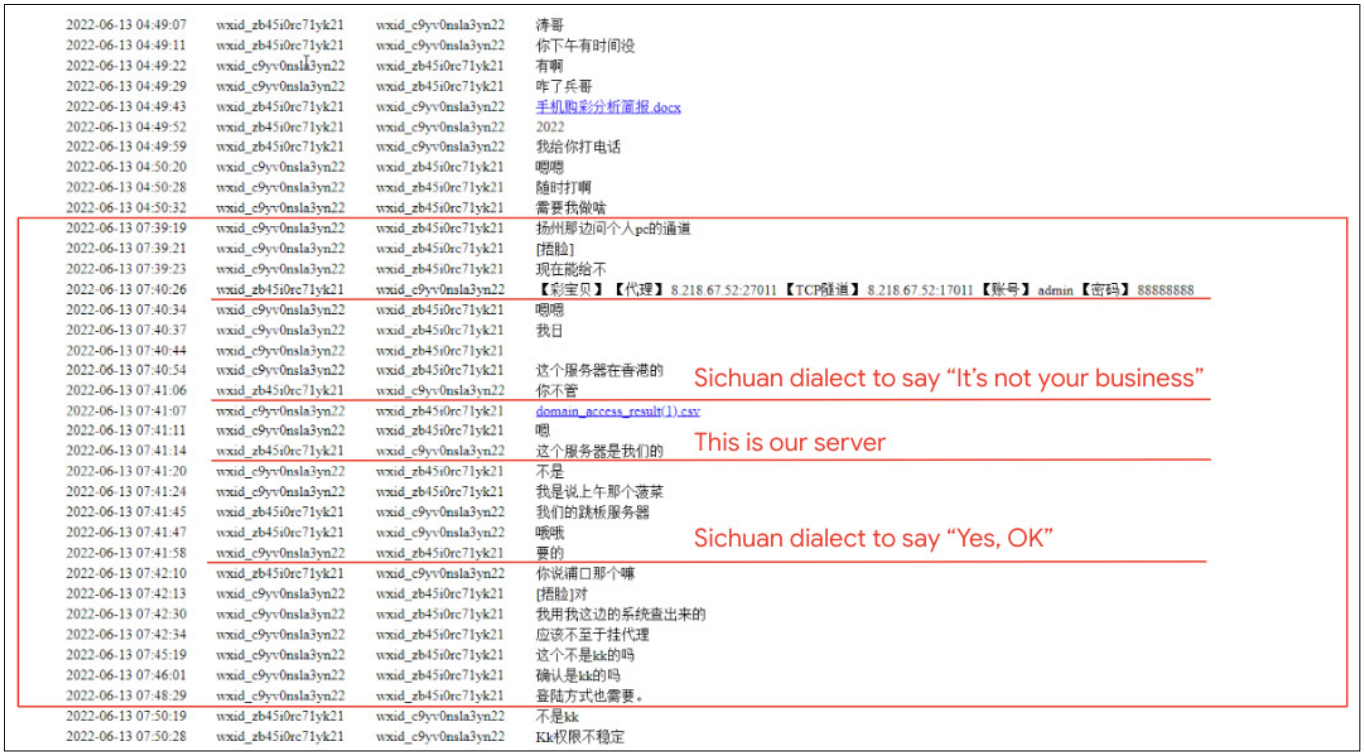


Figure 25: Leaked i-SOON conversation logs.

The proxy server IP address 8.218.67.52 was found abused together with the C2 domain files.amazonawsgarages.com in a sample of the ELECTRONAURA backdoor used by UNC3569. ELECTRONAURA has an anti-debugging feature and capability to report collected system information back to its C2 server. *Trend Micro* reported that the ELECTRONAURA backdoor was being used as the second-stage backdoor in probing weaponized chat applications for supply-chain attacks [24].

Additionally, there were traffic logs that indicated that the actor accessed the GRAYRABBIT server 152.32.134.159 via RDP from the IP addresses 8.219.167.156 and 8.219.138.129.[1]

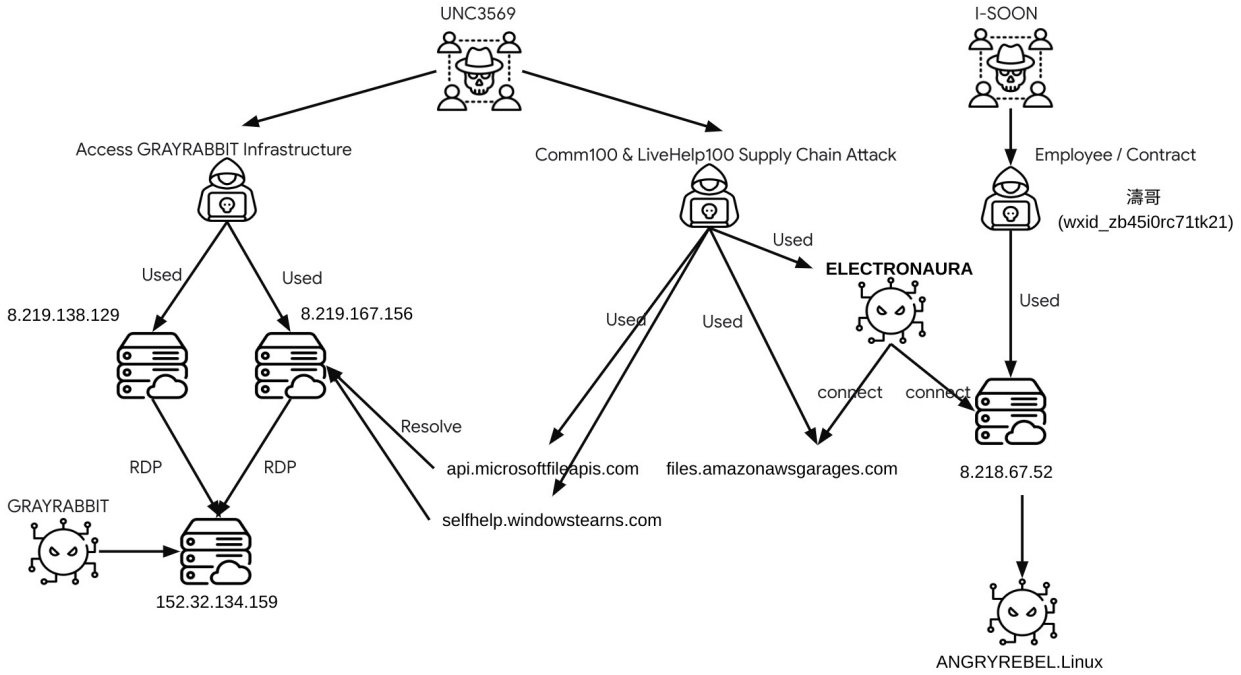


Figure 26: Connections between UNC3569 and i-SOON.

CONCLUSION

Operations that overlap with what *Mandiant* tracks as UNC3569 have been reported by *Symantec* [26], *CrowdStrike* [14], *Trend Micro* [24], and others. This group has maintained a high level of activity for years and we expect it to be an ongoing threat to entities of interest to the PRC government in the future. The group's emphasis on operational efficiency has likely allowed it to conduct a wide range of operations. While these operations may be discovered, the group is also able to employ new capabilities to adapt and continue its success.

The complex affiliations between UNC3569, UNC3246 and UNC251, combined with UNC3569's use of open-source tools and its potential ties to state-sponsored actors, demonstrate the difficulty in tracking this activity precisely. As businesses are caught between ageing on-premises activity and the cloud, threat actors like UNC3569 are capitalizing on the vulnerabilities exposed during the transitional period of cloud adoption. Significantly, the use by threat actors of open-source platforms to host payloads further enhances their ability to exploit legitimate services for malicious purposes, hindering detection and mitigation efforts.

The evolution of the GRAYRABBIT backdoor demonstrates the transformation of the threat landscape in the Chinese contractor and mercenary world.

REFERENCES

[1] Sichuan i-Soon Information Technology: Emerging from the Shadows of China's Intelligence Operations. https://advantage.mandiant.com/reports/24-10001719.

[2] NUL0x4C / AtomLdr. https://github.com/NUL0x4C/AtomLdr.

[3] EddieIvan01 / iox. https://github.com/EddieIvan01/iox.

[4] Udyz / proxyshell-auto. https://github.com/Udyz/proxyshell-auto.

[5] horizon3ai / proxyshell. https://github.com/horizon3ai/proxyshell.

[6] hosch3n / ProxyVulns. https://github.com/hosch3n/ProxyVulns.

[7] noperator / panos-scanner. https://github.com/noperator/panos-scanner.

[8] 0ki / mikrotik-tools. https://github.com/0ki/mikrotik-tools.

[1] The server 8.219.167.156 was resolved by C2 domains api.microsoftfileapis.com and selfhelp.windowstearns.com. These two domains were also observed being used in the previous supply-chain attack operation conducted by the same actor. The IoCs overlap in reports by *CrowdStrike* [14] and *Cloud Security Alliance* [25].

[9] surajraghuvanshi / PaloAltoRceDetectionAndExploit. https://github.com/surajraghuvanshi/PaloAltoRceDetectionAndExploit.

[10] je6k / CVE-2021-34473-Exchange-ProxyShell. https://github.com/je6k/CVE-2021-34473-Exchange-ProxyShell.

[11] threatexpress / cs2modrewrite. https://github.com/threatexpress/cs2modrewrite.

[12] alt3kx / CVE-2021-21985_PoC. https://github.com/alt3kx/CVE-2021-21985_PoC.

[13] mgargiullo / cve-2018-1207. https://github.com/mgargiullo/cve-2018-1207.git.

[14] CrowdStrike. Supply Chain Attack via a Trojanized Comm100 Chat Installer. 30 September 2022. https://www.crowdstrike.com/blog/new-supply-chain-attack-leverages-comm100-chat-installer/.

[15] https://advantage.mandiant.com/reports/24-10000191.

[16] moonD4rk / HackBrowserData. https://github.com/moonD4rk/HackBrowserData.

[17] 52pojie. Urgent-phpMyAdmin import sql database file error. https://www.52pojie.cn/thread-1172881-1-1.html.

[18] sysalong. https://woj.app/1439.html.

[19] sysalong / xss_pt. https://github.com/sysalong/xss_pt.

[20] Intrusion Truth. Chinese APTs: Interlinked networks and side hustles. 24 July 2022. https://intrusiontruth.wordpress.com/2022/07/24/chinese-apts-interlinked-networks-and-side-hustles/.

[21] rebeyond / Behinder. https://github.com/rebeyond/Behinder.

[22] L-codes / Neo-reGeorg. https://github.com/L-codes/Neo-reGeorg.

[23] Trend Micro. Examining a Possible Member of the Winnti Group. 19 April 2017. https://www.trendmicro.com/en_za/research/17/d/pigs-malware-examining-possible-member-winnti-group.html.

[24] Horejsi, J.; Chen, J. C. Probing Weaponized Chat Applications Abused in Supply-Chain Attacks. Trend Micro. 14 December 2022. https://www.trendmicro.com/en_no/research/22/l/probing-weaponized-chat-applications-abused-in-supply-chain-atta.html.

[25] Cloud Security Alliance. Supply Chain Attack via a Trojanized Comm100 Chat Installer. 2 November 2022. https://cloudsecurityalliance.org/blog/2022/11/02/supply-chain-attack-via-a-trojanized-comm100-chat-installer.

[26] Symantec. Carderbee: APT Group use Legit Software in Supply Chain Attack Targeting Orgs in Hong Kong. 22 August 2023. https://symantec-enterprise-blogs.security.com/threat-intelligence/carderbee-software-supply-chain-certificate-abuse.

[27] Cyble. Higaisa APT Resurfaces via Phishing Website targeting Chinese Users. 26 October 2023. https://cyble.com/blog/higaisa-apt-resurfaces-via-phishing-website-targeting-chinese-users/.

[28] Passilly, T.; Tartare, M. The SideWalk may be as dangerous as the CROSSWALK. We Live Security. 24 August 2021. https://www.welivesecurity.com/2021/08/24/sidewalk-may-be-as-dangerous-as-crosswalk/.

[29] Brown, R.; Ta, V.; Bienstock, D.; Ackerman, G.; Wolfram, J. Does This Look Infected? A Summary of APT41 Targeting U.S. State Governments. Mandiant. 8 March 2022. https://cloud.google.com/blog/topics/threat-intelligence/apt41-us-state-governments/.

APPENDIX – IOCs

CROSSWALK

```
ddefbecbf799414bac4769e24cc25ec233f860a845ae731ed49e7b2be791c8a9
a31d1515ac1fbc037d2dcbba3fec816b1fbb1d33ac719dff774939ed7a2296d4
5a56bddde6d6e7877ff791d8d87e3b37eac575deb62bc3952674942cc345bcbc (Dropper)
001dc13ecea26a7344816d77d145fdc2d8e26de200bda7c410dfb3a870da2cdd (CROSSWALK Binary)
```

GRAYRABBIT

```
46a5ab30e88476f4c4531a6b7fc1e983b72969721d6c285c70376036233f5e8c
fad2dc7b74f8c2e9d07656a961e2afad914e9a2ae60d361c5b0106e84715542d
06c57766935eff4358acf111536419172dd1067c0ecc9642e3cd99f3248062ec
62031cfedb010a42934fa37a0f9a8f30e4a7b62683278c448c85edf6a2247e8e
1ee0e86706d7396b6c4af48b57f3c89e28731b1845b0b6eee7ba490668f0e254
f3d1778d95a4d159dd79684dee33d1d2a3952ebedb1e567c448ff64140fe14b9
76c9e779324b4607caa0e054abef0887cc05014440cb624a342e89af378deee5
```

782b6c2b7de5fb19310bd0da6482adb810266fce1ff66c054103950b763a966b
d20c46d5bb49a92f4528f9565a4fa58e26b41ef97bf3580f6003b9fe3ba36a15
96e7a1a4cd7d7ebc998bef3e6e3f0c0783494e134d1156a38f2f26903367d6e6
89081cb6e813a2470160758dd379dc8795f5055d426975cd8f7286c524466dce

RABBITNEST

2de211a8ffd369297ff867aff2557f2a5493524b15684643b3b2bcf9638762b1
c5c93ce4bfff60ca583728c76a9dedc266caba376d413b12b37f9514ce8b3781
c1f5f26447e7330fe7a955e22edd4c891ac990f7160ef9eb87fd8205e1720d0c
f84925e7536126360d5b35744a48f280c01c55799fd5c0c09902f60213d19696
2aacbfa94804ed98990af2c09281193481fb785d6bea6fb52d47acd395b6e78c

RABBITASH

71040c61852ff9c6648920c3a63e96f82b3a70aa62ff7a948e2e181fef4bd494
d40f3da965399eaea6f828fb599147b6a26cfa2203adce695dc8db8a026eb1d8

RABBITCAVE

469b4e1a928e30c4f62c29bd1eb204a5c22aa69975bb3928dffb5d44eb091877
b403a2c08163d5c32a66629f844ef76452e9c099ac5437c07b46ca5018fc1a15
0790dcfb6d08ef87ce7bfecabe2366afb5a1246325289a492c10d20a507a9698

RABBITMOUND

21497e412d7c8983b99fee0741ca35a2dae870b8e2c071ac70cb12add80f9ed6
62c72e97fe329e341f9dbedb5ca09cc9271195381db68c01366bf82991e6e25e

RABBITWING

d681b86f61e5bec5fbf2c73010db9b6598a3ecec916f3a56747479f32b46d5a0
46c0f4b6fcd8e5e46dfe6cbd89cdcf047be1cde02b68ffdfb06d4a88c7e1a8e1

RABBITFUR

a5d4adab977c759dc241bbe5b62f7d3e7bd3273bcbf903ac6612d8c138f75f9c

Rust-based dropper

7ae55c34aedc14e8ace09ad2f5cc0d74b48d5aa6851b683df2dee10e6bdb8046

DOUBLESTEP

feab16498369b6a24ee34f57459ebde7f60cbd0e9aa5c943d0718b75db2ce85f
03ccd9ab1ff49b374c233aa89e45b683cbf3b7ee87b3a257421c4e541330ae3e

FIBERSTEP

0502497436bef43a04a8416de7e14ad27c0df29a2e6a9b8d9de7394b07439367

DATASTEP

2c4f14a2bc4baffd0c035c1a5f5c257e9697e728a1f96ee03ba0287ae7defc70

DRAFTGRAPH

fe8f99445ad139160a47b109a8f3291eef9c6a23b4869c48d341380d608ed4cb
fa6043f4812830bd98e2e0d2800ed754d0d3588090f0180659f8f562308691a6

SIDESTEP & OXEEYE

15835b6dd703e69d22d4ab941ccd5f6e78c3abc22ae123366da5e950eaa62e2b SIDESTEP
e0e96d619a80afd6c23ca35bd48bf644184492ad66bf69e9b61563336728b6b4 Encrypted Payload File
efa7c9bebc6d610ec03c9fba6f50787f1c87bf4a4d971c1a1556ecd56488ee89 OXEEYE

TROCHILUS

e91763dab902988273c02781b8e627cadb50b2337a8e0d1c9f529f45bc5f22df

HELLOBOT

69bb8b8d61873ffaf55051fffce8a0ee1419ff1ee054ace288fcebb7e0bc327b

ce89863a16787a6f39c25fd15ee48c4d196223668a264217f5d1cea31f8dc8ef

SOGU

b15fd68eba2c4dc29bbd0d33da7e7f9eab9c1be44b89ce736fee9727feab64f2

35564cf8b7b18a28fff88a7b82e5cd2ec019419ce3d5bb9f2483302a82987af2

5aae195fc44a7163a73406c02057ae5cc79eda87507f09bb956fe745fab328b9

3f3ad56e23986efa52139f86968e01ca6d44dc87300c2871b25743a13e33e5b2

b43fabebea2304f555f5f4c4c567d3810c5c62be4602509414532378e671fba2

KEYPLUG.Linux

36dbc30489d98ed4ca520773929cc775bd7b822c521d688dc2877b37084d3788

9f6f29c960f9421bd7bae9185b135c3a11bc2bc71bf77a2bb257811b263215d6

ELECTRONAURA

2dc08bd401d5396c2f99a41bbdbc378421f43318adc8627a2ae9a63e44f9b147

BEACON

14d2194faa1366d1c1ab2472f2fb3d5ea1641764a96fd33bd68711730c15ff91

Used domains

kf.2023kf1.top

chuanqiliebiao-1314.oss-cn-shanghai.aliyuncs.com

cloudwps.cn

wps-cn.com

www.gobay.info

active-microsoft.com

plug.active-microsoft.com

up.active-microsoft.com

tjj.active-microsoft.com

up.active-microsoft.com

cdn.active-microsoft.com

stream-google.com

api.stream-google.com

ssl.stream-google.com

google-chrome.org

version.google-chrome.org

stream-amazon.com

cdn.stream-amazon.com

up.stream-amazon.com

api.stream-amazon.com

myrnicrosoft.com

profile.myrnicrosoft.com

cloud.myrnicrosoft.com

update.myrnicrosoft.com

center.myrnicrosoft.com

proxyx.myrnicrosoft.com

fbi.cab

ap123.fbi.cab

cs.fbi.cab

xp.fbi.cab

```
sf.fbi.cab
v2.fbi.cab
gen.fbi.cab
os.fbi.cab
ofo.ac
x.ofo.ac
go.ofo.ac
cdn.ofo.ac
aw.ofo.ac
```