

LAPORAN ACAD CSIRT
Threat Hunting and Memory Forensics



Identitas Anggota Tim :

- Nama : Prayoga Gymnastiar, Email : prayoga.gymnastiar15@gmail.com
- Nama : Agus Sudarmanto, Email : kukukganyong@gmail.com
- Nama : Syaiful Akbar Rizki Mubarak, Email : Syaifulakbar873@gmail.com

KATA PENGANTAR

Puji dan syukur kami panjatkan ke hadirat Tuhan Yang Maha Esa atas limpahan rahmat dan karunia-Nya, sehingga Tim Bear Cyber Hunt dapat mengikuti dan menyelesaikan rangkaian kegiatan ACADefence Challenge 2025 dengan baik.

Kegiatan ini merupakan ajang bergengsi di bidang keamanan siber yang diselenggarakan oleh acadCSIRT, bekerja sama dengan Huawei, Universitas Kristen Maranatha, dan Orang Siber, sebagai bentuk nyata komitmen bersama dalam pengembangan kompetensi serta peningkatan kesadaran keamanan siber di lingkungan akademik dan profesional.

Partisipasi kami dalam ACADefence Challenge 2025 menjadi pengalaman yang sangat berharga dalam mengasah keterampilan teknis, memperluas wawasan, serta membangun semangat kolaboratif dalam menghadapi tantangan dunia siber yang kian kompleks. Melalui kompetisi ini, kami mendapatkan pembelajaran mendalam tidak hanya dalam aspek teknis, tetapi juga dalam hal strategi, ketahanan tim, dan etika profesional di bidang keamanan informasi.

Kami menyampaikan apresiasi setinggi-tingginya kepada seluruh penyelenggara, mitra pendukung, dan pihak-pihak terkait atas terselenggaranya kegiatan ini. Semoga ACADefence Challenge dapat terus menjadi wadah yang inspiratif dalam mencetak generasi profesional siber yang andal, tangguh, dan berintegritas tinggi.

Demikian kata pengantar ini kami sampaikan. Semoga dokumentasi ini dapat memberikan gambaran yang jelas mengenai peran serta kami dalam kegiatan ini dan memberikan manfaat bagi semua pihak yang membacanya.

Majenang, 17 Juni 2025

Penulis

DAFTAR ISI

HALAMAN SAMPUL.....	1
KATA PENGANTAR	2
DAFTAR ISI.....	3
TUGAS I.....	4
1. Tunjukan lebih artifak yang menjadi bahwa host tersebut telah terinfeksi.	4
2. Jelaskan dan buktikan bagaimana host tersebut bisa terinfeksi.	9
4. Apa kemampuan malware tersebut?	15
5. Artifak apa yang anda temukan pada packet capture t12.Pcap dan t13.Pcap	17
6. Analisa File Attack2.json, daftarkan semua malware digunakan dalam serangan.	22
7. Masih menggunakan file attack2.json, untuk semua malware yang digunakan, daftarkan indicator setiap malware tersebut	22
8. Jelaskan apakah attack tersebut ada hubungannya dengan sample 3, jelaskan alasanya. 23	
9. Rekomendasi apa yang dapat anda usulkan (Minimal 5 hal) untuk mitigasi risiko tersebut.	23
FILE II	26
1. Tunjukan lewat bukti artifak yang menjadi bukti bahwa host terssebut telah terinfeksi 26	
2. Jelaskan dan buktikan bagaimana host tersebut bisa terinfeksi.	29
3. Apakah Malware tersebut juga melakukan komunikasi dengan pihak eksternal?	32
4. Apa kemampuan malware tersebut?	34
5. Rekomendasi apa yang dapat anda usulkan (Minimal 5 hal) untuk mitigasi risiko tersebut.	36
PENGUNAAN AI.....	38
REFERENSI	39

TUGAS I

1. Tunjukkan lebih artifak yang menjadi bahwa host tersebut telah terinfeksi.

```
kali@YogaGYmn: ~/Downloads/File Pendukung Challenge 4
$ tshark -r t12.pcap -Y "http.request" -T fields -e http.host -e http.request.uri

211.234.117.141:443 /gmzlk.php?id=0318701110309GE67E
211.234.117.141:443 /viswi.php?id=0010901110309GE67E
211.234.117.141:443 /obeaa.php?id=0216551110309GE67E
211.234.117.141:443 /vrjff.php?id=0070901110309GE67E
211.234.117.141:443 /zqmse.php?id=0131971110309GE67E
211.234.117.141:443 /ivzdi.php?id=0100931110309GE67E
211.234.117.141:443 /ipubv.php?id=0086981110309GE67E
211.234.117.141:443 /zeyys.php?id=0278581110309GE67E
211.234.117.141:443 /gpaqi.php?id=0276191110309GE67E
211.234.117.141:443 /hgsht.php?id=0199571110309GE67E
211.234.117.141:443 /gftqr.php?id=0228161110309GE67E
211.234.117.141:443 /tyrae.php?id=0054211110309GE67E
211.234.117.141:443 /cidso.php?id=0284281110309GE67E
211.234.117.141:443 /xmeqb.php?id=0061151110309GE67E
211.234.117.141:443 /gauhx.php?id=0100931110309GE67E
211.234.117.141:443 /wwekz.php?id=0155131110309GE67E
211.234.117.141:443 /oyfar.php?id=0185981110309GE67E
211.234.117.141:443 /bjhbb.php?id=0123441110309GE67E
211.234.117.141:443 /tawcz.php?id=0192261110309GE67E
211.234.117.141:443 /bdhsp.php?id=0221741110309GE67E
211.234.117.141:443 /obffx.php?id=0306901110309GE67E
211.234.117.141:443 /yposw.php?id=0169991110309GE67E
211.234.117.141:443 /jttwm.php?id=0114431110309GE67E
211.234.117.141:443 /klszy.php?id=0163791110309GE67E
211.234.117.141:443 /pbqqr.php?id=0289371110309GE67E
211.234.117.141:443 /ysdjb.php?id=0163431110309GE67E
211.234.117.141:443 /jkmef.php?id=0185841110309GE67E
211.234.117.141:443 /livcm.php?id=0112951110309GE67E
211.234.117.141:443 /nytkh.php?id=0284031110309GE67E
211.234.117.141:443 /zwwjj.php?id=0300521110309GE67E
211.234.117.141:443 /hotmp.php?id=0267491110309GE67E
211.234.117.141:443 /kcvry.php?id=0252661110309GE67E
211.234.117.141:443 /fqcyj.php?id=0052641110309GE67E
```

Scanning file t12.pcap menggunakan tools tshark untuk melihat semua permintaan URI tanpa filter.

```
kali@YogaGYmn: ~/Downloads/File Pendukung Challenge 4
$ tshark -r t12.pcap -Y "http" -T fields -e http.request.method -e http.host -e http.request.uri

GET 211.234.117.141:443 /gmzlk.php?id=0318701110309GE67E
GET 211.234.117.141:443 /viswi.php?id=0010901110309GE67E
GET 211.234.117.141:443 /obeaa.php?id=0216551110309GE67E
GET 211.234.117.141:443 /vrjff.php?id=0070901110309GE67E
GET 211.234.117.141:443 /zqmse.php?id=0131971110309GE67E
GET 211.234.117.141:443 /ivzdi.php?id=0100931110309GE67E
GET 211.234.117.141:443 /ipubv.php?id=0086981110309GE67E
GET 211.234.117.141:443 /zeyys.php?id=0278581110309GE67E
GET 211.234.117.141:443 /gpaqi.php?id=0276191110309GE67E
GET 211.234.117.141:443 /hgsht.php?id=0199571110309GE67E
GET 211.234.117.141:443 /gftqr.php?id=0228161110309GE67E
GET 211.234.117.141:443 /tyrae.php?id=0054211110309GE67E
GET 211.234.117.141:443 /cidso.php?id=0284281110309GE67E
GET 211.234.117.141:443 /xmeqb.php?id=0061151110309GE67E
GET 211.234.117.141:443 /gauhx.php?id=0100931110309GE67E
GET 211.234.117.141:443 /wwekz.php?id=0155131110309GE67E
GET 211.234.117.141:443 /oyfar.php?id=0185981110309GE67E
GET 211.234.117.141:443 /bjhbb.php?id=0123441110309GE67E
GET 211.234.117.141:443 /tawcz.php?id=0192261110309GE67E
GET 211.234.117.141:443 /bdhsp.php?id=0221741110309GE67E
GET 211.234.117.141:443 /obffx.php?id=0306901110309GE67E
GET 211.234.117.141:443 /yposw.php?id=0169991110309GE67E
GET 211.234.117.141:443 /jttwm.php?id=0114431110309GE67E
GET 211.234.117.141:443 /klszy.php?id=0163791110309GE67E
GET 211.234.117.141:443 /pbqqr.php?id=0289371110309GE67E
GET 211.234.117.141:443 /ysdjb.php?id=0163431110309GE67E
GET 211.234.117.141:443 /jkmef.php?id=0185841110309GE67E
GET 211.234.117.141:443 /livcm.php?id=0112951110309GE67E
GET 211.234.117.141:443 /nytkh.php?id=0284031110309GE67E
GET 211.234.117.141:443 /zwwjj.php?id=0300521110309GE67E
GET 211.234.117.141:443 /hotmp.php?id=0267491110309GE67E
GET 211.234.117.141:443 /kcvry.php?id=0252661110309GE67E
GET 211.234.117.141:443 /fqcyj.php?id=0052641110309GE67E
```

Untuk Scanning file t12.pcap yang selanjutnya yaitu untuk melihat apakah ada protokol HTTP sama sekali.

Analisis Artefak Infeksi Berdasarkan t12.pcap

Akses HTTP GET mencurigakan ke banyak endpoint acak

Semua permintaan GET menuju IP: 211.234.117.141:443 dengan endpoint seperti:

- ✓ /gmzlk.php?id=031870...
- ✓ /viswi.php?id=001090...
- ✓ /obeaa.php?id=021655...
- dst.
- Struktur URL dengan path acak (/gmzlk.php, /zqmse.php, /gpaqi.php, dll) dan parameter id menunjukkan adanya komunikasi otomatis.
- Ini tidak lazim dilakukan oleh pengguna biasa, lebih mirip karakteristik infeksi malware beaconing atau C2 (Command & Control) communication.

Port tujuan adalah 443, tapi protokolnya HTTP

Berdasarkan hasil: GET 211.234.117.141:443 /gmzlk.php?id=...

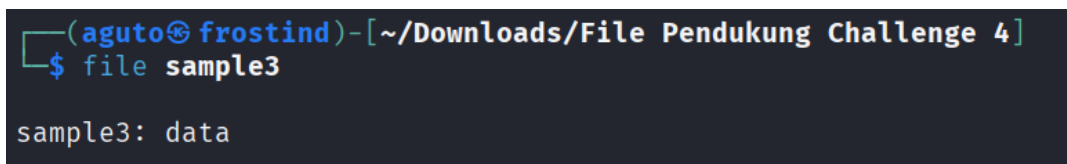
menunjukkan akses HTTP plaintext ke port HTTPS (443), ini sangat tidak biasa.

Artinya koneksi disamarkan agar terlihat seperti HTTPS padahal isinya HTTP biasa.

Ini adalah tanda umum malware mencoba menyembunyikan komunikasi C2.

Berdasarkan analisis tersebut dapat **disimpulkan** :

- Traffic HTTP mencurigakan ke 211.234.117.141:443 dengan pola GET /<random>.php?id=... sebanyak >30 kali.
- Frekuensi tinggi dan path acak → indikasi kuat dari malware beaconing.
- HTTP pada port 443 menunjukkan teknik pengelabuan protokol (protocol obfuscation).
- IP address yang terlibat non-lokal dan bukan server resmi.



```
(aguto@frostind)-[~/Downloads/File Pendukung Challenge 4]
$ file sample3
sample3: data
```

File sample3 tidak dikenali tipenya:

Output: sample3: data

Artinya: file ini bertipe raw data atau tidak memiliki header yang dikenali.

```

(aguto@frostind)-[~/Downloads/File Pendukung Challenge 4/volatility]
$ python2 vol.py -f ../sample3 --profile=Win10x64_18362 pslist
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsdump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svcscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdts (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.envvars (ImportError: No module named Crypto.Hash)
No suitable address space mapping found

```

```

Tried to open image as:
MachOAddressSpace: mac: need base
LimeAddressSpace: lime: need base
WindowsHiberFileSpace32: No base Address Space
WindowsCrashDumpSpace64BitMap: No base Address Space
WindowsCrashDumpSpace64: No base Address Space
HPAKAddressSpace: No base Address Space
VirtualBoxCoreDumpElf64: No base Address Space
VMWareMetaAddressSpace: No base Address Space
VMWareAddressSpace: No base Address Space
QemuCoreDumpElf: No base Address Space
WindowsCrashDumpSpace32: No base Address Space
SkipDuplicatesAMD64PagedMemory: No base Address Space
WindowsAMD64PagedMemory: No base Address Space
LinuxAMD64PagedMemory: No base Address Space
AMD64PagedMemory: No base Address Space
IA32PagedMemoryPae: No base Address Space
IA32PagedMemory: No base Address Space
OSXPmemELF: No base Address Space
MachOAddressSpace: MachO Header signature invalid
LimeAddressSpace: Invalid Lime header signature
WindowsHiberFileSpace32: No xpress signature found
WindowsCrashDumpSpace64BitMap: Header signature invalid
WindowsCrashDumpSpace64: Header signature invalid
HPAKAddressSpace: Invalid magic found
VirtualBoxCoreDumpElf64: ELF Header signature invalid
VMWareMetaAddressSpace: VMware metadata file is not available
VMWareAddressSpace: Invalid VMware signature: 0xf00ff53
QemuCoreDumpElf: ELF Header signature invalid
WindowsCrashDumpSpace32: Header signature invalid
SkipDuplicatesAMD64PagedMemory: No valid DTB found
WindowsAMD64PagedMemory: No valid DTB found
LinuxAMD64PagedMemory: Incompatible profile Win10x64_18362 selected
AMD64PagedMemory: No valid DTB found
IA32PagedMemoryPae: Incompatible profile Win10x64_18362 selected
IA32PagedMemory: Incompatible profile Win10x64_18362 selected
OSXPmemELF: ELF Header signature invalid
FileAddressSpace: Must be first Address Space
ArmAddressSpace: No valid DTB found

```

```

MachOAddressSpace: mac: need base
LimeAddressSpace: lime: need base
WindowsHiberFileSpace32: No base Address Space
WindowsCrashDumpSpace64BitMap: No base Address Space
WindowsCrashDumpSpace64: No base Address Space
HPAKAddressSpace: No base Address Space
VMWareMetaAddressSpace: No base Address Space
VirtualBoxCoreDumpElf64: No base Address Space
VMWareAddressSpace: No base Address Space
QemuCoreDumpElf: No base Address Space
WindowsCrashDumpSpace32: No base Address Space
SkipDuplicatesAMD64PagedMemory: No base Address Space
WindowsAMD64PagedMemory: No base Address Space
LinuxAMD64PagedMemory: No base Address Space
AMD64PagedMemory: No base Address Space
IA32PagedMemoryPae: No base Address Space
IA32PagedMemory: No base Address Space
OSXPmemELF: No base Address Space
MachOAddressSpace: MachO Header signature invalid
LimeAddressSpace: Invalid Lime header signature
WindowsHiberFileSpace32: No xpress signature found
WindowsCrashDumpSpace64BitMap: Header signature invalid
WindowsCrashDumpSpace64: Header signature invalid
HPAKAddressSpace: Invalid magic found
VMWareMetaAddressSpace: VMware metadata file is not available
VirtualBoxCoreDumpElf64: ELF Header signature invalid
VMWareAddressSpace: Invalid VMware signature: 0xf00ff53
QemuCoreDumpElf: ELF Header signature invalid
WindowsCrashDumpSpace32: Header signature invalid
SkipDuplicatesAMD64PagedMemory: No valid DTB found
WindowsAMD64PagedMemory: No valid DTB found
LinuxAMD64PagedMemory: Incompatible profile Win10x64_18362 selected
AMD64PagedMemory: No valid DTB found
IA32PagedMemoryPae: Incompatible profile Win10x64_18362 selected
IA32PagedMemory: Incompatible profile Win10x64_18362 selected
OSXPmemELF: ELF Header signature invalid
FileAddressSpace: Must be first Address Space

```

```

** Failed to import volatility.plugins.envvars (ImportError: No module named Crypto.Hash)
Offset(P)      Proto  Local Address      Foreign Address     State      Pid    Owner      Created
No suitable address space mapping found
Tried to open image as:
MachOAddressSpace: mac: need base
LimeAddressSpace: lime: need base
WindowsHiberFileSpace32: No base Address Space
WindowsCrashDumpSpace64BitMap: No base Address Space
WindowsCrashDumpSpace64: No base Address Space
HPAKAddressSpace: No base Address Space
VMWareMetaAddressSpace: No base Address Space
VirtualBoxCoreDumpElf64: No base Address Space
QemuCoreDumpElf: No base Address Space
VMWareAddressSpace: No base Address Space
WindowsCrashDumpSpace32: No base Address Space
SkipDuplicatesAMD64PagedMemory: No base Address Space
WindowsAMD64PagedMemory: No base Address Space
LinuxAMD64PagedMemory: No base Address Space
AMD64PagedMemory: No base Address Space
IA32PagedMemoryPae: No base Address Space
IA32PagedMemory: No base Address Space
OSXPmemELF: No base Address Space
MachOAddressSpace: MachO Header signature invalid
LimeAddressSpace: Invalid Lime header signature
WindowsHiberFileSpace32: No xpress signature found
WindowsCrashDumpSpace64BitMap: Header signature invalid
WindowsCrashDumpSpace64: Header signature invalid
HPAKAddressSpace: Invalid magic found
VMWareMetaAddressSpace: VMware metadata file is not available
VirtualBoxCoreDumpElf64: ELF Header signature invalid
QemuCoreDumpElf: ELF Header signature invalid
VMWareAddressSpace: Invalid VMware signature: 0xf000ff53
WindowsCrashDumpSpace32: Header signature invalid
SkipDuplicatesAMD64PagedMemory: No valid DTB found
WindowsAMD64PagedMemory: No valid DTB found
LinuxAMD64PagedMemory: Incompatible profile Win10x64_18362 selected
AMD64PagedMemory: No valid DTB found
IA32PagedMemoryPae: Incompatible profile Win10x64_18362 selected
IA32PagedMemory: Incompatible profile Win10x64_18362 selected
OSXPmemELF: ELF Header signature invalid
FileAddressSpace: Must be first Address Space
ArmAddressSpace: No valid DTB found

```

Tools Volatility gagal membaca file sample3:

Banyak error seperti:

- ✓ No suitable address space mapping found
- ✓ Invalid magic found
- ✓ Header signature invalid
- ✓ No valid DTB found

Error ImportError: No module named Crypto.Hash juga mengindikasikan ada dependensi Python yang hilang.

```

kali@YogaGYmn: ~/Downloads/File Pendukung Challenge 4
$ binwalk sample3

DECIMAL      HEXADECEIMAL    DESCRIPTION
-----
112864      0x1B8E0         Cisco IOS microcode, for "S"
112911      0x1B90F         Cisco IOS microcode, for "M"
197120      0x08F40         ESP Image (ESP32-H2): segment count: 1, flash mode: QUID, flash speed: 40MHz, flash size: 1MB, entry address: 0x10, hash: none
656418      0xA0A22         Copyright string: "Copyright 1985-1990, Phoenix Technologies Ltd.All rights reserved."
819330      0xC8082         Copyright string: "Copyright (C) 2003-2014 VMware, Inc."
819369      0xC80A9         Copyright string: "Copyright (C) 1997-2000 Intel Corporation"
943020      0xE3AC          ISO 9660 Boot Record,

kali@YogaGYmn: ~/Downloads/File Pendukung Challenge 4
$ hexdump -C sample3 | head

00000000  53 ff 00 f0 53 ff 00 f0  c3 e2 00 f0 53 ff 00 f0  |S...S.....S...|
00000010  53 ff 00 f0 54 ff 00 f0  88 04 00 f0 53 ff 00 f0  |S...T.....S...|
00000020  a5 fe 00 f0 87 a9 00 f0  b5 0e 00 f0 b6 0e 00 f0  |.....|
00000030  b6 0e 00 f0 b6 0e 00 f0  57 ef 00 f0 f5 00 f0  |.....W.....|
00000040  16 0b 00 c0 4d f8 00 f0  41 f8 00 f0 2b 01 00 cd  |...M...A...+...|
00000050  39 e7 00 f0 59 f8 00 f0  ac 22 60 ca c2 ef 00 f0  |I...Y...+...|
00000060  59 ff 00 f0 f2 e6 00 f0  6e fe 00 f0 53 ff 00 f0  |Y.....h...S...|
00000070  53 ff 00 f0 a4 f0 00 f0  fd 81 00 f0 3a 13 00 c0  |S.....|
00000080  b6 0e 00 f0 b6 0e 00 f0  b6 0e 00 f0 b6 0e 00 f0  |.....|

kali@YogaGYmn: ~/Downloads/File Pendukung Challenge 4
$ volatility2 sample3 windows.info

volatility3: command not found
kali@YogaGYmn: ~/Downloads/File Pendukung Challenge 4

```

Analisis sample 3 menggunakan tools binwalk menghasilkan Output:

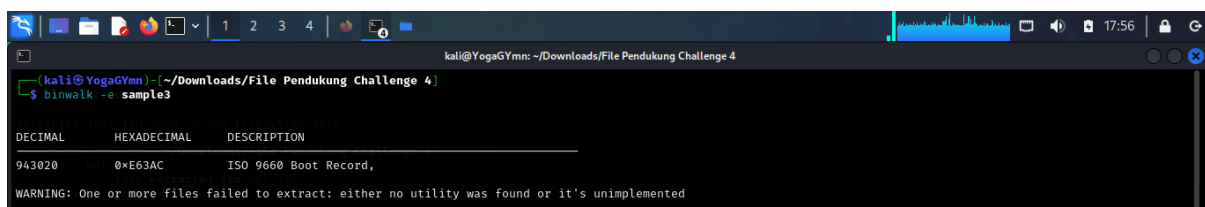
Menemukan beberapa artefak embedded seperti:

- ✓ Microcode Cisco IOS
- ✓ Image ESP32
- ✓ Phoenix BIOS
- ✓ VMware & Intel copyright
- ✓ ISO9660 Boot Record

File sample3 bukan memory dump Windows, melainkan image firmware atau flash dump, kemungkinan dari perangkat seperti:

- ✓ Router Cisco
- ✓ IoT (ESP32)
- ✓ Virtual Machine BIOS / Firmware Layer

Artinya file ini tidak kompatibel dengan Volatility, karena bukan format memory Windows seperti .raw, .dmp, .vmem.



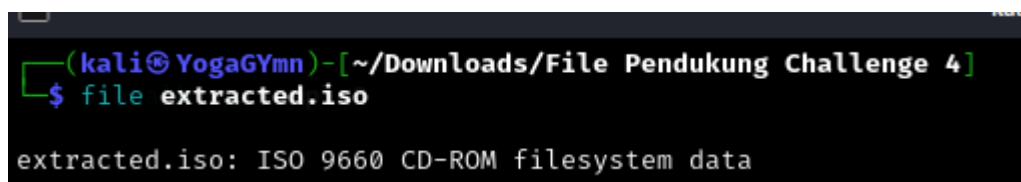
```
kali@YogaGYmn: ~/Downloads/File Pendukung Challenge 4
$ binwalk -e sample3

DECIMAL      HEXADECEMAL  DESCRIPTION
-----
943020      0xE63AC      ISO 9660 Boot Record,
WARNING: One or more files failed to extract: either no utility was found or it's unimplemented
```

Dari hasil binwalk -e sample3, hanya satu entri yang bisa dikenali dengan baik, Yaitu :

Offset 0xE63AC: Terdeteksi ISO 9660 Boot Record

Ini menunjukkan bahwa di dalam sample3 ada semacam image CD-ROM/bootable disk berbasis format ISO9660.



```
(kali@YogaGYmn)-[~/Downloads/File Pendukung Challenge 4]
$ file extracted.iso

extracted.iso: ISO 9660 CD-ROM filesystem data
```

Output file extracted.iso: ISO 9660 CD-ROM filesystem data berarti file tersebut diakui sebagai file ISO valid secara struktur dasar

2. Jelaskan dan buktikan bagaimana host tersebut bisa terinfeksi.

```
No suitable address space mapping found
Tried to open image as:
MachOAddressSpace: mach: need base
LimeAddressSpace: lime: need base
WindowsHiberFileSpace32: No base Address Space
WindowsCrashDumpSpace64BitMap: No base Address Space
HPAKAddressSpace: No base Address Space
WindowsCrashDumpSpace64: No base Address Space
VMWareMetaAddressSpace: No base Address Space
VirtualBoxCoreDumpElf64: No base Address Space
QemuCoreDumpElf: No base Address Space
VMWareAddressSpace: No base Address Space
WindowsCrashDumpSpace32: No base Address Space
SkipDuplicatesAMD64PagedMemory: No base Address Space
WindowsAMD64PagedMemory: No base Address Space
LinuxAMD64PagedMemory: No base Address Space
AMD64PagedMemory: No base Address Space
IA32PagedMemoryPae: No base Address Space
IA32PagedMemory: No base Address Space
OSXPmemELF: No base Address Space
MachOAddressSpace: MachO Header signature invalid
LimeAddressSpace: Invalid Lime header signature
WindowsHiberFileSpace32: No xpress signature found
WindowsCrashDumpSpace64BitMap: Header signature invalid
HPAKAddressSpace: Invalid magic found
WindowsCrashDumpSpace64: Header signature invalid
VMWareMetaAddressSpace: VMware metadata file is not available
VirtualBoxCoreDumpElf64: ELF Header signature invalid
QemuCoreDumpElf: ELF Header signature invalid
VMWareAddressSpace: Invalid VMware signature: 0xf000ff53
WindowsCrashDumpSpace32: Header signature invalid
SkipDuplicatesAMD64PagedMemory: No valid DTB found
WindowsAMD64PagedMemory: No valid DTB found
LinuxAMD64PagedMemory: Incompatible profile Win10x64_18362 selected
AMD64PagedMemory: No valid DTB found
IA32PagedMemoryPae: Incompatible profile Win10x64_18362 selected
IA32PagedMemory: Incompatible profile Win10x64_18362 selected
OSXPmemELF: ELF Header signature invalid
FileAddressSpace: Must be first Address Space
ArmAddressSpace: No valid DTB found
```

Deteksi Otomatis Format Memory Image pada sample3 menggunakan Volatility.

tools Volatility berhasil memuat file memory image sample3 dengan profile Win10x64_18362, walaupun sempat mengalami beberapa kali deteksi gagal.

```
(aguto@frostind)[-~/Downloads/File Pendukung Challenge 4/volatility]
$ python2 vol.py -f ../sample3 --profile=Win10x64_18362 shimcache
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtxlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svcscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdts (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.envvars (ImportError: No module named Crypto.Hash)
ERROR : volatility.debug : You must specify something to do (try -h)
```

Saat menjalankan plugin volatility dengan profile Win10x64_18362, muncul banyak error No module named Crypto.Hash dan distorm3 is not defined. Ini artinya:

- ✓ Plugin penting gagal dijalankan (seperti shimcache, malware, svcscan, shellbags, lsadump, dll).
- ✓ Namun, command yang digunakan adalah: `python2 vol.py -f sample3 --profile=Win10x64_18362 shimcache`

Tapi shimcache tidak dapat dijalankan karena modul Crypto.Hash tidak ada. Shimcache biasanya dipakai untuk mendeteksi jejak eksekusi file malware, jadi kemungkinan ada bukti infeksi, tapi belum bisa diekstrak karena masalah environment Python.

```
(aguto@frostind)-[~/Downloads/File Pendukung Challenge 4]
$ strings sample3 | grep -i '.exe'

@"%systemroot%\system32\windowspowershell\v1.0\powershell.exe",-111
Win32API|Tool Help Structures|MODULEENTRY32|szExePath
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
[SeiInit] Unsuccessful fixing up APIs, EXE "%S"
[SeiGetShimData] Can't get EXE data
[SeiGetShimData] Can't get EXE name
Win32API|Tool Help Structures|MODULEENTRY32|szExePath
Path to the extension executable
c:\program files\windows mail\wab.exe
c:\program files\windows mail\wab.exe
c:\windows\system32\rundll32.exe
c:\windows\system32\rundll32.exe
c:\windows\system32\rundll32.exe
c:\windows\system32\rundll32.exe
c:\windows\system32\rundll32.exe
c:\windows\system32\rundll32.exe
c:\windows\system32\rundll32.exe
c:\windows\system32\rundll32.exe
c:\windows\system32\rundll32.exe
c:\windows\system32\rundll32.exe
c:\program files\internet explorer\iexplore.exe
c:\program files\internet explorer\iexplore.exe
c:\program files\internet explorer\iexplore.exe
c:\windows\system32\rundll32.exe
c:\program files\internet explorer\iexplore.exe
c:\program files\internet explorer\iexplore.exe
c:\program files\internet explorer\iexplore.exe
c:\program files\internet explorer\iexplore.exe
c:\program files\internet explorer\iexplore.exe
c:\windows\ehome\mediacenterwebblauncher.exe
c:\windows\system32\wpnprv.dll
```

hasil perintah dari : `strings sample3 | grep -i '.exe'`

menunjukkan banyak executable (.exe) yang muncul dari path mencurigakan, seperti:

- ✓ `c:\windows\system32\rundll32.exe`
- ✓ `c:\program files\windows mail\wab.exe`
- ✓ `c:\windows\system32\powershell.exe`
- ✓ `c:\windows\system32\wpnprv.dll`

- Penggunaan rundll32.exe dan powershell.exe secara berulang adalah indikasi klasik infeksi malware, karena kedua executable ini sering disalahgunakan untuk menjalankan script berbahaya atau payload secara stealthy.
- powershell.exe muncul dari path:
%systemroot%\system32\windowspowershell\v1.0\powershell.exe

menunjukkan kemungkinan eksploitasi PowerShell untuk menjalankan perintah tanpa sepengetahuan pengguna (living-off-the-land binary/LOLBins).

Bukti Eksekusi Malware

Eksekusi berulang dari:

- ✓ rundll32.exe
- ✓ powershell.exe
- ✓ iexplore.exe

menunjukkan bahwa file executable telah dijalankan di sistem, yang bisa merupakan bagian dari payload malware. Hal ini bisa terjadi melalui:

- File dropper malware yang mengeksekusi via rundll32.
- PowerShell digunakan untuk mengunduh atau menjalankan skrip eksternal.
- iexplore.exe kemungkinan disalahgunakan (Internet Explorer) sebagai media koneksi keluar atau rekayasa sosial.

Hasil analisis tersebut dapat disimpulkan, Yaitu :

Host tersebut bisa terinfeksi melalui eksekusi berulang terhadap executable mencurigakan seperti powershell.exe, rundll32.exe, dan iexplore.exe, yang biasanya digunakan oleh malware untuk menyebar atau mengunduh payload tambahan. Ini diperkuat dengan hasil pencarian string .exe yang menunjukkan pola eksekusi tidak normal.

3. Apakah Malware tersebut juga melakukan komunikasi dengan pihak eksternal?

```
(aguto@frostind)-[~/Downloads/File Pendukung Challenge 4]
$ tshark -r t12.pcap -Y "ip.dst==172.16.253.132" -T fields -e frame.time -e ip.dst -e tcp.port
Oct 14, 2012 16:33:31.349158000 EDT 172.16.253.132
Oct 14, 2012 16:33:31.349164000 EDT 172.16.253.132
Oct 14, 2012 16:33:32.349769000 EDT 172.16.253.132
Oct 14, 2012 16:33:32.352599000 EDT 172.16.253.132
Oct 14, 2012 16:33:45.409078000 EDT 172.16.253.132 443,1229
Oct 14, 2012 16:33:45.409488000 EDT 172.16.253.132 443,1229
Oct 14, 2012 16:33:45.684805000 EDT 172.16.253.132 443,1229
Oct 14, 2012 16:33:45.685295000 EDT 172.16.253.132 443,1229
Oct 14, 2012 16:33:47.908061000 EDT 172.16.253.132 443,1230
Oct 14, 2012 16:33:47.908413000 EDT 172.16.253.132 443,1230
Oct 14, 2012 16:33:48.182028000 EDT 172.16.253.132 443,1230
Oct 14, 2012 16:33:48.182306000 EDT 172.16.253.132 443,1230
Oct 14, 2012 16:33:50.417904000 EDT 172.16.253.132 443,1231
Oct 14, 2012 16:33:50.418355000 EDT 172.16.253.132 443,1231
Oct 14, 2012 16:33:50.674598000 EDT 172.16.253.132 443,1231
Oct 14, 2012 16:33:50.674870000 EDT 172.16.253.132 443,1231
Oct 14, 2012 16:33:52.923698000 EDT 172.16.253.132 443,1232
Oct 14, 2012 16:33:52.924015000 EDT 172.16.253.132 443,1232
Oct 14, 2012 16:33:53.164800000 EDT 172.16.253.132 443,1232
Oct 14, 2012 16:33:55.427319000 EDT 172.16.253.132 443,1233
Oct 14, 2012 16:33:55.427658000 EDT 172.16.253.132 443,1233
Oct 14, 2012 16:33:55.625438000 EDT 172.16.253.132 443,1233
Oct 14, 2012 16:33:55.625748000 EDT 172.16.253.132 443,1233
Oct 14, 2012 16:33:57.870189000 EDT 172.16.253.132 443,1234
Oct 14, 2012 16:33:57.871067000 EDT 172.16.253.132 443,1234
Oct 14, 2012 16:33:58.114342000 EDT 172.16.253.132 443,1234
Oct 14, 2012 16:33:58.114696000 EDT 172.16.253.132 443,1234
Oct 14, 2012 16:34:00.366762000 EDT 172.16.253.132 443,1235
Oct 14, 2012 16:34:00.367217000 EDT 172.16.253.132 443,1235
Oct 14, 2012 16:34:00.606726000 EDT 172.16.253.132 443,1235
Oct 14, 2012 16:34:02.847022000 EDT 172.16.253.132 443,1236
Oct 14, 2012 16:34:02.847346000 EDT 172.16.253.132 443,1236
Oct 14, 2012 16:34:03.100202000 EDT 172.16.253.132 443,1236
Oct 14, 2012 16:34:03.100580000 EDT 172.16.253.132 443,1236
Oct 14, 2012 16:34:05.330858000 EDT 172.16.253.132 443,1237
Oct 14, 2012 16:34:05.331172000 EDT 172.16.253.132 443,1237
Oct 14, 2012 16:34:05.561407000 EDT 172.16.253.132 443,1237
Oct 14, 2012 16:34:05.561769000 EDT 172.16.253.132 443,1237
Oct 14, 2012 16:34:07.788746000 EDT 172.16.253.132 443,1238
Oct 14, 2012 16:34:07.789226000 EDT 172.16.253.132 443,1238
Oct 14, 2012 16:34:08.022626000 EDT 172.16.253.132 443,1238
Oct 14, 2012 16:34:10.321025000 EDT 172.16.253.132 443,1239
Oct 14, 2012 16:34:10.321398000 EDT 172.16.253.132 443,1239
Oct 14, 2012 16:34:10.562079000 EDT 172.16.253.132 443,1239
Oct 14, 2012 16:34:12.788077000 EDT 172.16.253.132 443,1240
Oct 14, 2012 16:34:12.788393000 EDT 172.16.253.132 443,1240
```

```
Oct 14, 2012 16:34:35.185600000 EDT 172.16.253.132 443,1249
Oct 14, 2012 16:34:35.185888000 EDT 172.16.253.132 443,1249
Oct 14, 2012 16:34:35.430774000 EDT 172.16.253.132 443,1249
Oct 14, 2012 16:34:37.668398000 EDT 172.16.253.132 443,1250
Oct 14, 2012 16:34:37.668814000 EDT 172.16.253.132 443,1250
Oct 14, 2012 16:34:37.945555000 EDT 172.16.253.132 443,1250
Oct 14, 2012 16:34:37.945811000 EDT 172.16.253.132 443,1250
Oct 14, 2012 16:34:40.173660000 EDT 172.16.253.132 443,1251
Oct 14, 2012 16:34:40.174093000 EDT 172.16.253.132 443,1251
Oct 14, 2012 16:34:40.407814000 EDT 172.16.253.132 443,1251
Oct 14, 2012 16:34:40.411201000 EDT 172.16.253.132 443,1251
Oct 14, 2012 16:34:42.700294000 EDT 172.16.253.132 443,1252
Oct 14, 2012 16:34:42.700610000 EDT 172.16.253.132 443,1252
Oct 14, 2012 16:34:42.877037000 EDT 172.16.253.132 443,1252
Oct 14, 2012 16:34:42.877317000 EDT 172.16.253.132 443,1252
Oct 14, 2012 16:34:45.144009000 EDT 172.16.253.132 443,1253
Oct 14, 2012 16:34:45.144333000 EDT 172.16.253.132 443,1253
Oct 14, 2012 16:34:45.383333000 EDT 172.16.253.132 443,1253
Oct 14, 2012 16:34:47.883894000 EDT 172.16.253.132 443,1254
Oct 14, 2012 16:34:47.884308000 EDT 172.16.253.132 443,1254
Oct 14, 2012 16:34:48.119685000 EDT 172.16.253.132 443,1254
Oct 14, 2012 16:34:53.294041000 EDT 172.16.253.132 443,1255
Oct 14, 2012 16:34:53.294393000 EDT 172.16.253.132 443,1255
Oct 14, 2012 16:34:53.526246000 EDT 172.16.253.132 443,1255
Oct 14, 2012 16:34:55.822083000 EDT 172.16.253.132 443,1256
Oct 14, 2012 16:34:55.822449000 EDT 172.16.253.132 443,1256
Oct 14, 2012 16:34:56.058273000 EDT 172.16.253.132 443,1256
Oct 14, 2012 16:34:56.058705000 EDT 172.16.253.132 443,1256
Oct 14, 2012 16:34:58.496375000 EDT 172.16.253.132 443,1257
Oct 14, 2012 16:34:58.496671000 EDT 172.16.253.132 443,1257
Oct 14, 2012 16:34:58.734689000 EDT 172.16.253.132 443,1257
Oct 14, 2012 16:34:58.736251000 EDT 172.16.253.132 443,1257
Oct 14, 2012 16:35:01.122585000 EDT 172.16.253.132 443,1258
Oct 14, 2012 16:35:01.122894000 EDT 172.16.253.132 443,1258
Oct 14, 2012 16:35:01.364165000 EDT 172.16.253.132 443,1258
Oct 14, 2012 16:35:01.366097000 EDT 172.16.253.132 443,1258
Oct 14, 2012 16:35:03.617677000 EDT 172.16.253.132 443,1259
Oct 14, 2012 16:35:03.617964000 EDT 172.16.253.132 443,1259
Oct 14, 2012 16:35:03.857354000 EDT 172.16.253.132 443,1259
Oct 14, 2012 16:35:03.857677000 EDT 172.16.253.132 443,1259
Oct 14, 2012 16:35:06.166832000 EDT 172.16.253.132 443,1260
Oct 14, 2012 16:35:06.167229000 EDT 172.16.253.132 443,1260
Oct 14, 2012 16:35:06.403315000 EDT 172.16.253.132 443,1260
Oct 14, 2012 16:35:08.638916000 EDT 172.16.253.132 443,1261
Oct 14, 2012 16:35:08.642335000 EDT 172.16.253.132 443,1261
Oct 14, 2012 16:35:08.879689000 EDT 172.16.253.132 443,1261
Oct 14, 2012 16:35:08.882592000 EDT 172.16.253.132 443,1261
```

Oct 14, 2012	16:34:12.788077000	EDT	172.16.253.132	443,1240
Oct 14, 2012	16:34:12.788393000	EDT	172.16.253.132	443,1240
Oct 14, 2012	16:34:13.027278000	EDT	172.16.253.132	443,1240
Oct 14, 2012	16:34:13.027619000	EDT	172.16.253.132	443,1240
Oct 14, 2012	16:34:15.259558000	EDT	172.16.253.132	443,1241
Oct 14, 2012	16:34:15.259865000	EDT	172.16.253.132	443,1241
Oct 14, 2012	16:34:15.501719000	EDT	172.16.253.132	443,1241
Oct 14, 2012	16:34:15.501999000	EDT	172.16.253.132	443,1241
Oct 14, 2012	16:34:17.743422000	EDT	172.16.253.132	443,1242
Oct 14, 2012	16:34:17.743938000	EDT	172.16.253.132	443,1242
Oct 14, 2012	16:34:17.981294000	EDT	172.16.253.132	443,1242
Oct 14, 2012	16:34:17.981536000	EDT	172.16.253.132	443,1242
Oct 14, 2012	16:34:20.222225000	EDT	172.16.253.132	443,1243
Oct 14, 2012	16:34:20.222547000	EDT	172.16.253.132	443,1243
Oct 14, 2012	16:34:20.468267000	EDT	172.16.253.132	443,1243
Oct 14, 2012	16:34:20.468521000	EDT	172.16.253.132	443,1243
Oct 14, 2012	16:34:22.699717000	EDT	172.16.253.132	443,1244
Oct 14, 2012	16:34:22.700124000	EDT	172.16.253.132	443,1244
Oct 14, 2012	16:34:22.943048000	EDT	172.16.253.132	443,1244
Oct 14, 2012	16:34:22.943349000	EDT	172.16.253.132	443,1244
Oct 14, 2012	16:34:25.063149000	EDT	172.16.253.132	443,1755
Oct 14, 2012	16:34:25.187711000	EDT	172.16.253.132	443,1245
Oct 14, 2012	16:34:25.188026000	EDT	172.16.253.132	443,1245
Oct 14, 2012	16:34:25.435145000	EDT	172.16.253.132	443,1245
Oct 14, 2012	16:34:27.666620000	EDT	172.16.253.132	443,1246
Oct 14, 2012	16:34:27.667050000	EDT	172.16.253.132	443,1246
Oct 14, 2012	16:34:27.927955000	EDT	172.16.253.132	443,1246
Oct 14, 2012	16:34:30.173410000	EDT	172.16.253.132	443,1247
Oct 14, 2012	16:34:30.173861000	EDT	172.16.253.132	443,1247
Oct 14, 2012	16:34:30.500451000	EDT	172.16.253.132	443,1247
Oct 14, 2012	16:34:32.720543000	EDT	172.16.253.132	443,1248
Oct 14, 2012	16:34:32.720924000	EDT	172.16.253.132	443,1248
Oct 14, 2012	16:34:32.951144000	EDT	172.16.253.132	443,1248
Oct 14, 2012	16:34:32.951420000	EDT	172.16.253.132	443,1248
Oct 14, 2012	16:34:35.185600000	EDT	172.16.253.132	443,1249
Oct 14, 2012	16:34:35.185888000	EDT	172.16.253.132	443,1249
Oct 14, 2012	16:34:35.430774000	EDT	172.16.253.132	443,1249
Oct 14, 2012	16:34:37.668398000	EDT	172.16.253.132	443,1250
Oct 14, 2012	16:34:37.668814000	EDT	172.16.253.132	443,1250
Oct 14, 2012	16:34:37.945555000	EDT	172.16.253.132	443,1250
Oct 14, 2012	16:34:37.945811000	EDT	172.16.253.132	443,1250
Oct 14, 2012	16:34:40.173660000	EDT	172.16.253.132	443,1251
Oct 14, 2012	16:34:40.174093000	EDT	172.16.253.132	443,1251
Oct 14, 2012	16:34:40.407814000	EDT	172.16.253.132	443,1251
Oct 14, 2012	16:34:40.411201000	EDT	172.16.253.132	443,1251
Oct 14, 2012	16:34:42.700294000	EDT	172.16.253.132	443,1252
Oct 14, 2012	16:34:42.700610000	EDT	172.16.253.132	443,1252

Hasil output dari t-shark pada file T12.PCP Menampilkan trafik masuk ke IP 172.16.253.132, kebanyakan dari port 443, terlihat berurutan seperti koneksi dari bot.

```
(aguto@frostind)~/Downloads/File Pendukung Challenge 4]
$ tshark -r t12.pcap -q -z conv,ip
```

```
IPv4 Conversations
Filter:<No Filter>
```

		←		→		Total	Relative	Duration
		Frames	Bytes	Frames	Bytes	Frames	Start	
172.16.253.132	↔	211.234.117.141	121 7260 bytes	142 14 kB	263 21 kB	82.873730000	83.7390	
172.16.253.1	↔	172.16.253.255	0 0 bytes	9 2648 bytes	9 2648 bytes	0.000000000	157.9341	
172.16.253.132	↔	224.0.0.22	0 0 bytes	7 378 bytes	7 378 bytes	73.500396000	15.8920	
172.16.253.254	↔	172.16.253.132	0 0 bytes	4 808 bytes	4 808 bytes	69.079289000	1.0034	
0.0.0.0	↔	255.255.255.255	0 0 bytes	2 697 bytes	2 697 bytes	69.078588000	1.0017	

Hasil perintah tshark -r t12.pcap -q -z conv,ip

Menampilkan daftar percakapan antar IP.

Terlihat bahwa IP 172.16.253.132 berkomunikasi dengan IP eksternal 211.234.117.141, dengan total 263 frame dan 21 kB data, selama 83.7390 detik.

Inilah bukti komunikasi keluar (external communication).


```
(aguto@frostind)-[~/Downloads/File Pendukung Challenge 4]
$ tshark -r t12.pcap -Y "http.request" -T fields -e http.host -e http.request.uri

211.234.117.141:443 /gmzlk.php?id=031870111D309GE67E
211.234.117.141:443 /viswi.php?id=001090111D309GE67E
211.234.117.141:443 /obeaa.php?id=021655111D309GE67E
211.234.117.141:443 /vrjffj.php?id=007090111D309GE67E
211.234.117.141:443 /zqmse.php?id=013197111D309GE67E
211.234.117.141:443 /ivzdi.php?id=010093111D309GE67E
211.234.117.141:443 /ipubv.php?id=008698111D309GE67E
211.234.117.141:443 /zeyys.php?id=027858111D309GE67E
211.234.117.141:443 /gpaqi.php?id=027619111D309GE67E
211.234.117.141:443 /hgsht.php?id=019957111D309GE67E
211.234.117.141:443 /gftqr.php?id=022816111D309GE67E
211.234.117.141:443 /tyrae.php?id=005421111D309GE67E
211.234.117.141:443 /cidso.php?id=028428111D309GE67E
211.234.117.141:443 /xmeqb.php?id=006115111D309GE67E
211.234.117.141:443 /gauhx.php?id=010093111D309GE67E
211.234.117.141:443 /wwekz.php?id=015513111D309GE67E
211.234.117.141:443 /oyfar.php?id=018598111D309GE67E
211.234.117.141:443 /bjhbb.php?id=012344111D309GE67E
211.234.117.141:443 /tavcz.php?id=019226111D309GE67E
211.234.117.141:443 /bdhsp.php?id=022174111D309GE67E
211.234.117.141:443 /obffx.php?id=030690111D309GE67E
211.234.117.141:443 /yposw.php?id=016999111D309GE67E
211.234.117.141:443 /jttwm.php?id=011443111D309GE67E
211.234.117.141:443 /klszy.php?id=016379111D309GE67E
211.234.117.141:443 /pbqqr.php?id=028937111D309GE67E
211.234.117.141:443 /ysdjb.php?id=016343111D309GE67E
211.234.117.141:443 /jkmqf.php?id=018584111D309GE67E
211.234.117.141:443 /livcm.php?id=011295111D309GE67E
211.234.117.141:443 /nytkh.php?id=028403111D309GE67E
211.234.117.141:443 /zwvjj.php?id=030052111D309GE67E
211.234.117.141:443 /hotmp.php?id=026749111D309GE67E
211.234.117.141:443 /kcvry.php?id=025266111D309GE67E
211.234.117.141:443 /fqcyj.php?id=005264111D309GE67E
```

Perintah: tshark -r t12.pcap -Y "http.request" -T fields -e http.host -e http.request.uri

Menampilkan HTTP request ke 211.234.117.141:443. URI menunjukkan pola akses ke file .php dengan parameter id, Yaitu:

- ✓ /gmzlk.php?id=031870111D309GE67E
- ✓ /viswi.php?id=001090111D309GE67E

Ini mengindikasikan komunikasi C2 (Command & Control) tipikal malware.

4. Apa kemampuan malware tersebut?

```
(aguto@frostind)-[~/Downloads/File Pendukung Challenge 4]
$ tshark -r t12.pcap -Y "http.request"

26 83.139466 172.16.253.132 → 211.234.117.141 HTTP 248 GET /gmzlk.php?id=03187011DD309E67E HTTP/1.1
35 85.638395 172.16.253.132 → 211.234.117.141 HTTP 248 GET /viswi.php?id=00109011DD309E67E HTTP/1.1
44 88.148314 172.16.253.132 → 211.234.117.141 HTTP 248 GET /obeaa.php?id=02165511DD309E67E HTTP/1.1
58 90.654033 172.16.253.132 → 211.234.117.141 HTTP 248 GET /vrjff.php?id=00709011DD309E67E HTTP/1.1
64 93.157641 172.16.253.132 → 211.234.117.141 HTTP 248 GET /zqmse.php?id=01319711DD309E67E HTTP/1.1
73 95.600532 172.16.253.132 → 211.234.117.141 HTTP 248 GET /ivzdi.php?id=01009311DD309E67E HTTP/1.1
83 98.097168 172.16.253.132 → 211.234.117.141 HTTP 248 GET /ipubv.php?id=00869811DD309E67E HTTP/1.1
89 100.577374 172.16.253.132 → 211.234.117.141 HTTP 248 GET /zeyys.php?id=02785811DD309E67E HTTP/1.1
98 103.061175 172.16.253.132 → 211.234.117.141 HTTP 248 GET /gpaqi.php?id=02761911DD309E67E HTTP/1.1
107 105.519200 172.16.253.132 → 211.234.117.141 HTTP 248 GET /hgshh.php?id=01995711DD309E67E HTTP/1.1
113 108.051386 172.16.253.132 → 211.234.117.141 HTTP 248 GET /gftqr.php?id=02281611DD309E67E HTTP/1.1
119 110.518423 172.16.253.132 → 211.234.117.141 HTTP 248 GET /tyrae.php?id=00542111DD309E67E HTTP/1.1
128 112.989890 172.16.253.132 → 211.234.117.141 HTTP 248 GET /cidso.php?id=02842811DD309E67E HTTP/1.1
137 115.473787 172.16.253.132 → 211.234.117.141 HTTP 248 GET /xmeqb.php?id=00611511DD309E67E HTTP/1.1
146 117.952542 172.16.253.132 → 211.234.117.141 HTTP 248 GET /gauhx.php?id=01009311DD309E67E HTTP/1.1
155 120.430136 172.16.253.132 → 211.234.117.141 HTTP 248 GET /wwekz.php?id=01551311DD309E67E HTTP/1.1
165 122.918026 172.16.253.132 → 211.234.117.141 HTTP 248 GET /oyfar.php?id=01859811DD309E67E HTTP/1.1
171 125.397051 172.16.253.132 → 211.234.117.141 HTTP 248 GET /bjhbb.php?id=01234411DD309E67E HTTP/1.1
178 127.903800 172.16.253.132 → 211.234.117.141 HTTP 248 GET /tavcz.php?id=01922611DD309E67E HTTP/1.1
184 130.450911 172.16.253.132 → 211.234.117.141 HTTP 248 GET /bdhsp.php?id=02217411DD309E67E HTTP/1.1
193 132.915921 172.16.253.132 → 211.234.117.141 HTTP 248 GET /obffx.php?id=03069011DD309E67E HTTP/1.1
199 135.398778 172.16.253.132 → 211.234.117.141 HTTP 248 GET /yposw.php?id=01699911DD309E67E HTTP/1.1
208 137.904109 172.16.253.132 → 211.234.117.141 HTTP 248 GET /jttwm.php?id=01144311DD309E67E HTTP/1.1
217 140.430617 172.16.253.132 → 211.234.117.141 HTTP 248 GET /klszy.php?id=01637911DD309E67E HTTP/1.1
226 142.874341 172.16.253.132 → 211.234.117.141 HTTP 248 GET /pbqqr.php?id=02893711DD309E67E HTTP/1.1
232 145.614211 172.16.253.132 → 211.234.117.141 HTTP 248 GET /ysdjb.php?id=01634311DD309E67E HTTP/1.1
239 151.024378 172.16.253.132 → 211.234.117.141 HTTP 248 GET /jkmqf.php?id=01858411DD309E67E HTTP/1.1
245 153.552407 172.16.253.132 → 211.234.117.141 HTTP 248 GET /livcm.php?id=01129511DD309E67E HTTP/1.1
254 156.226697 172.16.253.132 → 211.234.117.141 HTTP 248 GET /nytkh.php?id=02840311DD309E67E HTTP/1.1
264 158.852917 172.16.253.132 → 211.234.117.141 HTTP 248 GET /zwvjj.php?id=03005211DD309E67E HTTP/1.1
273 161.347988 172.16.253.132 → 211.234.117.141 HTTP 248 GET /hotmp.php?id=02674911DD309E67E HTTP/1.1
282 163.897159 172.16.253.132 → 211.234.117.141 HTTP 248 GET /kcvry.php?id=02526611DD309E67E HTTP/1.1
288 166.370590 172.16.253.132 → 211.234.117.141 HTTP 248 GET /fqcyj.php?id=00526411DD309E67E HTTP/1.1
```

Dari analisis tshark pada file t12.pcap, terlihat banyak permintaan HTTP GET ke berbagai file PHP di server 211.234.117.141. Nama file PHP disertai parameter id=... yang terlihat seperti payload atau identifier unik, seperti:

✓ /gmzlk.php?id=03187011DD309E67E

Ini merupakan pola umum untuk komunikasi C2 (Command and Control) antara malware dan server kontrol, tempat malware menerima perintah atau mengirim hasil curian.

```
(aguto@frostind)-[~/Downloads/File Pendukung Challenge 4]
$ tshark -r t13.pcap -Y "tcp.port==4444"
```

Dalam file t13.pcap, filter tcp.port==4444 menunjukkan komunikasi pada port yang sering digunakan oleh reverse shell atau metasploit payload.

Port 4444 secara historis digunakan oleh banyak reverse shell payloads, yang memungkinkan attacker mendapatkan akses langsung ke sistem korban.

Ini menunjukkan bahwa malware mungkin memiliki kemampuan backdoor untuk kontrol penuh dari jarak jauh.

```
(aguto@frostind):[~/Downloads/File Pendukung Challenge 4]
$ cat attack2.json | jq
{
  "type": "bundle",
  "id": "bundle--a7407872-687f-4b75-9851-f1b29a28862c",
  "objects": [
    {
      "type": "threat-actor",
      "spec_version": "2.1",
      "id": "threat-actor--89f53598-1799-44fd-8c33-a3d2a7f55f24",
      "created": "2024-06-12T00:00:00.000Z",
      "modified": "2024-06-12T00:00:00.000Z",
      "name": "APT41",
      "description": "APT41 is a sophisticated and prolific threat group operating with a clear nexus to the People's Republic of China (PRC). This group distinguishes itself through a dual operational mandate, conducting state-sponsored cyber espionage activities in parallel with financially motivated cybercrime. It targets a wide array of sectors globally, including governments, technology, healthcare, and the video game industry. APT41 is known for using custom malware, exploiting zero-day vulnerabilities, and leveraging legitimate cloud services for C2 communication.",
      "aliases": [
        "GOOSE",
        "HOODOO",
        "BARTUM",
        "Brass Typhoon",
        "Wicked Panda",
        "Double Dragon",
        "TG-2633",
        "Bronze Atlas",
        "Red Kelpie",
        "Blackfly",
        "Grayfly",
        "Earth Baku",
        "SparklingGoblin",
        "TAA15",
        "BrazenBamboo",
        "Winnti Group"
      ],
      "roles": [
        "espionage",
        "financial-theft"
      ],
      "goals": [
        "intelligence-gathering",

```

Berdasarkan file attack2.json, malware ini dikaitkan dengan APT41, yang dikenal memiliki dua misi utama:

- ✓ Espionage (spionase/sadap data): Menargetkan pemerintah, kesehatan, game, dll.
- ✓ Financial-theft (pencurian finansial): Aktivitas siber kriminal untuk keuntungan finansial.

Ini mengindikasikan malware mampu:

- ✓ Mengambil data sensitif
- ✓ Mengakses akun atau sistem finansial
- ✓ Mencuri identitas atau kredensial

Dari deskripsi:

"known for using custom malware, exploiting zero-day vulnerabilities, and leveraging legitimate cloud services for C2 communication"

Berarti malware ini mampu:

- ✓ Menyerang kerentanan zero-day
- ✓ Menggunakan cloud services sebagai media komunikasi C2, yang lebih sulit dideteksi
- ✓ Dikustomisasi untuk target tertentu

Kesimpulan Kemampuan Malware

No	Kemampuan Utama	Penjelasan Singkat
<u>1</u>	C2 Communication via HTTP	Mengirim/terima perintah dari server C2
<u>2</u>	Remote Access / Backdoor	Mengontrol sistem korban dari jarak jauh
<u>3</u>	Espionage & Data Theft	Mengambil informasi penting dari sistem target
<u>4</u>	Financial Theft	Akses dan pencurian informasi finansial
<u>5</u>	Exploiting Zero-day Vulnerability	Mengeksploitasi celah keamanan baru
<u>6</u>	Cloud-based C2	Gunakan layanan cloud sah untuk sembunyi

		dari deteksi
--	--	--------------

5. Artifak apa yang anda temukan pada packet capture t12.Pcap dan t13.Pcap.

```

root@kali:~/Downloads/File Pendukung Challenge 4
tshark -i t12.pcap -f fields=ip,src,-ip.dst -ncp.port -e frame.time -e http.host -Y "ip"

172.16.253.1 172.16.253.255 Oct 14, 2012 16:32:22.269869000 EOT
172.16.253.1 172.16.253.255 Oct 14, 2012 16:32:52.344141800 EOT
172.16.253.1 172.16.253.132 Oct 14, 2012 16:33:22.416581000 EOT
172.16.253.1 172.16.253.255 Oct 14, 2012 16:33:27.002186000 EOT
172.16.253.1 172.16.253.255 Oct 14, 2012 16:33:28.003234000 EOT
172.16.253.1 172.16.253.255 Oct 14, 2012 16:33:29.991827000 EOT
0.0.0.0 255.255.255.255 Oct 14, 2012 16:33:31.340457000 EOT
172.16.253.254 172.16.253.132 Oct 14, 2012 16:33:31.349158000 EOT
172.16.253.254 172.16.253.132 Oct 14, 2012 16:33:31.349164000 EOT
172.16.253.254 172.16.253.132 Oct 14, 2012 16:33:32.349769000 EOT
0.0.0.0 255.255.255.255 Oct 14, 2012 16:33:32.350203000 EOT
172.16.253.254 172.16.253.132 Oct 14, 2012 16:33:32.352520000 EOT
172.16.253.132 224.0.0.2 Oct 14, 2012 16:33:35.770265000 EOT
172.16.253.132 224.0.0.2 Oct 14, 2012 16:33:36.658836000 EOT
172.16.253.132 211.234.117.141 1229, 443 Oct 14, 2012 16:33:35.143599000 EOT
211.234.117.141 172.16.253.132 443, 1229 Oct 14, 2012 16:33:35.149078000 EOT
211.234.117.141 172.16.253.132 443, 1229 Oct 14, 2012 16:33:35.149084000 EOT
172.16.253.132 211.234.117.141 1229, 443 Oct 14, 2012 16:33:35.149935000 EOT
211.234.117.141 172.16.253.132 443, 1229 Oct 14, 2012 16:33:35.409488000 EOT
211.234.117.141 172.16.253.132 443, 1229 Oct 14, 2012 16:33:35.68408000 EOT
172.16.253.132 211.234.117.141 1229, 443 Oct 14, 2012 16:33:35.684086000 EOT
172.16.253.132 211.234.117.141 1229, 443 Oct 14, 2012 16:33:35.68483000 EOT
172.16.253.132 211.234.117.141 1229, 443 Oct 14, 2012 16:33:35.685164000 EOT
211.234.117.141 172.16.253.132 443, 1229 Oct 14, 2012 16:33:35.685295000 EOT
172.16.253.132 211.234.117.141 1229, 443 Oct 14, 2012 16:33:37.674860000 EOT
211.234.117.141 172.16.253.132 443, 1229 Oct 14, 2012 16:33:37.680100000 EOT
172.16.253.132 211.234.117.141 1229, 443 Oct 14, 2012 16:33:37.908100000 EOT
211.234.117.141 172.16.253.132 443, 1229 Oct 14, 2012 16:33:37.908243000 EOT
211.234.117.141 172.16.253.132 443, 1229 Oct 14, 2012 16:33:37.182020000 EOT
172.16.253.132 211.234.117.141 1229, 443 Oct 14, 2012 16:33:37.182169000 EOT
172.16.253.132 211.234.117.141 1229, 443 Oct 14, 2012 16:33:37.182306000 EOT
172.16.253.132 211.234.117.141 1229, 443 Oct 14, 2012 16:33:50.174477000 EOT
172.16.253.132 211.234.117.141 1229, 443 Oct 14, 2012 16:33:50.174638000 EOT
172.16.253.132 211.234.117.141 1229, 443 Oct 14, 2012 16:33:50.174945000 EOT
172.16.253.132 211.234.117.141 1229, 443 Oct 14, 2012 16:33:50.418183000 EOT
211.234.117.141 172.16.253.132 443, 1229 Oct 14, 2012 16:33:50.418355000 EOT
172.16.253.132 224.0.0.2 Oct 14, 2012 16:33:50.455032000 EOT
172.16.253.132 224.0.0.2 Oct 14, 2012 16:33:50.455032000 EOT
211.234.117.141 172.16.253.132 443, 1229 Oct 14, 2012 16:33:50.674598000 EOT
172.16.253.132 211.234.117.141 1229, 443 Oct 14, 2012 16:33:50.674638000 EOT
172.16.253.132 211.234.117.141 1229, 443 Oct 14, 2012 16:33:50.674763000 EOT
172.16.253.132 211.234.117.141 1229, 443 Oct 14, 2012 16:33:50.674830000 EOT
172.16.253.132 224.0.0.2 Oct 14, 2012 16:33:50.789086000 EOT
172.16.253.132 224.0.0.2 Oct 14, 2012 16:33:50.791404000 EOT
172.16.253.132 224.0.0.2 Oct 14, 2012 16:33:51.662392000 EOT
172.16.253.132 211.234.117.141 1229, 443 Oct 14, 2012 16:33:52.681621000 EOT
211.234.117.141 172.16.253.132 443, 1229 Oct 14, 2012 16:33:52.923730000 EOT
172.16.253.132 211.234.117.141 1229, 443 Oct 14, 2012 16:33:52.923902000 EOT
211.234.117.141 172.16.253.132 443, 1229 Oct 14, 2012 16:33:52.924100000 EOT
172.16.253.132 211.234.117.141 1229, 443 Oct 14, 2012 16:33:52.924100000 EOT
172.16.253.132 211.234.117.141 1229, 443 Oct 14, 2012 16:33:55.158884000 EOT
211.234.117.141 172.16.253.132 443, 1229 Oct 14, 2012 16:33:55.427319000 EOT
172.16.253.132 211.234.117.141 1229, 443 Oct 14, 2012 16:33:55.427353000 EOT
172.16.253.132 211.234.117.141 1229, 443 Oct 14, 2012 16:33:55.427353000 EOT
211.234.117.141 172.16.253.132 443, 1229 Oct 14, 2012 16:33:55.726560000 EOT
211.234.117.141 172.16.253.132 443, 1229 Oct 14, 2012 16:33:55.825433000 EOT
172.16.253.132 211.234.117.141 1229, 443 Oct 14, 2012 16:33:55.825433000 EOT
211.234.117.141 172.16.253.132 443, 1229 Oct 14, 2012 16:33:55.825433000 EOT
172.16.253.132 211.234.117.141 1229, 443 Oct 14, 2012 16:33:55.825433000 EOT
211.234.117.141 172.16.253.132 443, 1229 Oct 14, 2012 16:33:55.8254
```

211.234.117.141	172.16.253.132	443, 1248	Oct 14,	2012	16:34:32, 720543000	EDT	
211.234.117.141	172.16.253.132	1248, 443	Oct 14,	2012	16:34:32, 720548000	EDT	
172.16.253.132	211.234.117.141	1248, 443	Oct 14,	2012	16:34:32, 720700000	EDT	211.234.117.141:443
211.234.117.141	172.16.253.132	443, 1248	Oct 14,	2012	16:34:32, 720924000	EDT	
211.234.117.141	172.16.253.132	443, 1248	Oct 14,	2012	16:34:34, 720925000	EDT	
211.234.117.141	172.16.253.132	1248, 443	Oct 14,	2012	16:34:32, 721157000	EDT	
172.16.253.132	211.234.117.141	1248, 443	Oct 14,	2012	16:34:32, 721316000	EDT	
211.234.117.141	172.16.253.132	443, 1248	Oct 14,	2012	16:34:32, 721542000	EDT	
172.16.253.132	211.234.117.141	1249, 443	Oct 14,	2012	16:34:35, 721579000	EDT	211.234.117.141:443
211.234.117.141	172.16.253.132	443, 1249	Oct 14,	2012	16:34:35, 721838000	EDT	
211.234.117.141	172.16.253.132	443, 1249	Oct 14,	2012	16:34:35, 721839000	EDT	
211.234.117.141	172.16.253.132	1250, 443	Oct 14,	2012	16:34:37, 724243000	EDT	
211.234.117.141	172.16.253.132	443, 1250	Oct 14,	2012	16:34:37, 724839000	EDT	
172.16.253.132	211.234.117.141	1250, 443	Oct 14,	2012	16:34:37, 724841000	EDT	
211.234.117.141	172.16.253.132	443, 1250	Oct 14,	2012	16:34:37, 725048000	EDT	211.234.117.141:443
211.234.117.141	172.16.253.132	443, 1250	Oct 14,	2012	16:34:37, 726881000	EDT	
211.234.117.141	172.16.253.132	443, 1250	Oct 14,	2012	16:34:37, 729555000	EDT	
172.16.253.132	211.234.117.141	1250, 443	Oct 14,	2012	16:34:37, 729559000	EDT	
211.234.117.141	172.16.253.132	443, 1250	Oct 14,	2012	16:34:37, 729561000	EDT	
172.16.253.132	211.234.117.141	1251, 443	Oct 14,	2012	16:34:39, 730401000	EDT	
211.234.117.141	172.16.253.132	443, 1251	Oct 14,	2012	16:34:40, 7366000	EDT	
172.16.253.132	211.234.117.141	1251, 443	Oct 14,	2012	16:34:40, 73724000	EDT	
211.234.117.141	172.16.253.132	443, 1251	Oct 14,	2012	16:34:40, 73734000	EDT	211.234.117.141:443
211.234.117.141	172.16.253.132	443, 1251	Oct 14,	2012	16:34:40, 740934000	EDT	
211.234.117.141	172.16.253.132	443, 1251	Oct 14,	2012	16:34:40, 740714000	EDT	
172.16.253.132	211.234.117.141	1251, 443	Oct 14,	2012	16:34:40, 740756000	EDT	
211.234.117.141	172.16.253.132	443, 1251	Oct 14,	2012	16:34:40, 740757000	EDT	
211.234.117.141	172.16.253.132	443, 1251	Oct 14,	2012	16:34:40, 741261000	EDT	
172.16.253.132	211.234.117.141	1252, 443	Oct 14,	2012	16:34:42, 7410081000	EDT	
211.234.117.141	172.16.253.132	443, 1252	Oct 14,	2012	16:34:42, 740249000	EDT	
211.234.117.141	172.16.253.132	443, 1252	Oct 14,	2012	16:34:42, 740249000	EDT	
172.16.253.132	211.234.117.141	1252, 443	Oct 14,	2012	16:34:42, 740846000	EDT	211.234.117.141:443
211.234.117.141	172.16.253.132	443, 1252	Oct 14,	2012	16:34:42, 740861000	EDT	
211.234.117.141	172.16.253.132	443, 1252	Oct 14,	2012	16:34:42, 877037000	EDT	
172.16.253.132	211.234.117.141	1252, 443	Oct 14,	2012	16:34:42, 877176000	EDT	
211.234.117.141	172.16.253.132	443, 1252	Oct 14,	2012	16:34:42, 877317000	EDT	
172.16.253.132	211.234.117.141	1253, 443	Oct 14,	2012	16:34:44, 878399000	EDT	
211.234.117.141	172.16.253.132	443, 1253	Oct 14,	2012	16:34:45, 721549000	EDT	
211.234.117.141	172.16.253.132	443, 1253	Oct 14,	2012	16:34:45, 721549000	EDT	
172.16.253.132	211.234.117.141	1253, 443	Oct 14,	2012	16:34:45, 744212000	EDT	211.234.117.141:443
211.234.117.141	172.16.253.132	443, 1253	Oct 14,	2012	16:34:45, 744333000	EDT	
211.234.117.141	172.16.253.132	443, 1253	Oct 14,	2012	16:34:45, 748333000	EDT	
211.234.117.141	172.16.253.132	443, 1253	Oct 14,	2012	16:34:45, 748333000	EDT	
211.234.117.141	172.16.253.132	443, 1254	Oct 14,	2012	16:34:47, 883939000	EDT	
172.16.253.132	211.234.117.141	1254, 443	Oct 14,	2012	16:34:47, 883939000	EDT	
172.16.253.132	211.234.117.141	1254, 443	Oct 14,	2012	16:34:47, 884080000	EDT	211.234.117.141:443
211.234.117.141	172.16.253.132	443, 1254	Oct 14,	2012	16:34:47, 884080000	EDT	
211.234.117.141	172.16.253.132	443, 1254	Oct 14,	2012	16:34:48, 119685000	EDT	
172.16.253.132	211.234.117.141	1255, 443	Oct 14,	2012	16:34:50, 158085000	EDT	
172.16.253.132	211.234.117.141	1255, 443	Oct 14,	2012	16:34:53, 158220000	EDT	
211.234.117.141	172.16.253.132	443, 1255	Oct 14,	2012	16:34:53, 158220000	EDT	
172.16.253.132	211.234.117.141	1255, 443	Oct 14,	2012	16:34:53, 294270000	EDT	
172.16.253.132	211.234.117.141	1255, 443	Oct 14,	2012	16:34:53, 294270000	EDT	211.234.117.141:443
211.234.117.141	172.16.253.132	443, 1255	Oct 14,	2012	16:34:53, 294393000	EDT	
211.234.117.141	172.16.253.132	443, 1255	Oct 14,	2012	16:34:53, 529193000	EDT	
211.234.117.141	172.16.253.132	1256, 443	Oct 14,	2012	16:34:55, 822083000	EDT	
211.234.117.141	172.16.253.132	443, 1256	Oct 14,	2012	16:34:55, 822083000	EDT	

211.234.117.141	172.16.253.132	443,1252	Oct 14,	2012	16:34:42,700294000	EDT	
172.16.253.132	211.234.117.141	1252,443	Oct 14,	2012	16:34:42,700328000	EDT	
172.16.253.132	211.234.117.141	1252,443	Oct 14,	2012	16:34:42,700486000	EDT	211.234.117.141:443
211.234.117.141	172.16.253.132	443,1252	Oct 14,	2012	16:34:42,700618000	EDT	
172.16.253.132	211.234.117.141	1252,443	Oct 14,	2012	16:34:42,700750000	EDT	
172.16.253.132	211.234.117.141	1252,443	Oct 14,	2012	16:34:42,700882000	EDT	
211.234.117.141	172.16.253.132	443,1252	Oct 14,	2012	16:34:42,701317000	EDT	
172.16.253.132	211.234.117.141	1252,443	Oct 14,	2012	16:34:44,701449000	EDT	
172.16.253.132	211.234.117.141	1252,443	Oct 14,	2012	16:34:45,140440000	EDT	211.234.117.141:443
172.16.253.132	211.234.117.141	1252,443	Oct 14,	2012	16:34:45,140421000	EDT	
211.234.117.141	172.16.253.132	443,1252	Oct 14,	2012	16:34:45,140433000	EDT	
211.234.117.141	172.16.253.132	443,1252	Oct 14,	2012	16:34:45,383333000	EDT	
172.16.253.132	211.234.117.141	1252,443	Oct 14,	2012	16:34:46,636939000	EDT	
211.234.117.141	172.16.253.132	443,1252	Oct 14,	2012	16:34:47,883894000	EDT	
172.16.253.132	211.234.117.141	1252,443	Oct 14,	2012	16:34:47,883931000	EDT	
172.16.253.132	211.234.117.141	1252,443	Oct 14,	2012	16:34:47,884088000	EDT	211.234.117.141:443
211.234.117.141	172.16.253.132	443,1252	Oct 14,	2012	16:34:47,884398000	EDT	
172.16.253.132	211.234.117.141	1252,443	Oct 14,	2012	16:34:48,119622000	EDT	
172.16.253.132	211.234.117.141	1252,443	Oct 14,	2012	16:34:50,150856000	EDT	
172.16.253.132	211.234.117.141	1252,443	Oct 14,	2012	16:34:53,158228000	EDT	
211.234.117.141	172.16.253.132	443,1252	Oct 14,	2012	16:34:53,294041000	EDT	
172.16.253.132	211.234.117.141	1252,443	Oct 14,	2012	16:34:53,294077000	EDT	
172.16.253.132	211.234.117.141	1252,443	Oct 14,	2012	16:34:53,294232000	EDT	211.234.117.141:443
211.234.117.141	172.16.253.132	443,1252	Oct 14,	2012	16:34:53,294393000	EDT	
211.234.117.141	172.16.253.132	443,1252	Oct 14,	2012	16:34:53,526246000	EDT	
172.16.253.132	211.234.117.141	1252,443	Oct 14,	2012	16:34:55,508919000	EDT	
211.234.117.141	172.16.253.132	443,1252	Oct 14,	2012	16:34:55,509038000	EDT	
172.16.253.132	211.234.117.141	1252,443	Oct 14,	2012	16:34:55,822276000	EDT	211.234.117.141:443
211.234.117.141	172.16.253.132	443,1252	Oct 14,	2012	16:34:55,822449000	EDT	
211.234.117.141	172.16.253.132	443,1252	Oct 14,	2012	16:34:56,058273000	EDT	
172.16.253.132	211.234.117.141	1252,443	Oct 14,	2012	16:34:56,058233000	EDT	
172.16.253.132	211.234.117.141	1252,443	Oct 14,	2012	16:34:56,058452000	EDT	
211.234.117.141	172.16.253.132	443,1252	Oct 14,	2012	16:34:56,058705000	EDT	
172.16.253.132	211.234.117.141	1252,443	Oct 14,	2012	16:34:58,206733000	EDT	
211.234.117.141	172.16.253.132	443,1252	Oct 14,	2012	16:34:58,496375000	EDT	
172.16.253.132	211.234.117.141	1252,443	Oct 14,	2012	16:34:58,496416000	EDT	
172.16.253.132	211.23						

172.16.253.132	211.234.117.141	1258,443	Oct 14, 2012 16:35:01.364301000	EOT	
211.234.117.141	172.16.253.132	443,1258	Oct 14, 2012 16:35:01.366097000	EOT	
172.16.253.132	211.234.117.141	1259,443	Oct 14, 2012 16:35:03.361540000	EOT	
211.234.117.141	172.16.253.132	443,1259	Oct 14, 2012 16:35:03.617677000	EOT	
172.16.253.132	211.234.117.141	1259,443	Oct 14, 2012 16:35:03.617710000	EOT	
172.16.253.132	211.234.117.141	1259,443	Oct 14, 2012 16:35:03.617857000	EOT	211.234.117.141:443
211.234.117.141	172.16.253.132	443,1259	Oct 14, 2012 16:35:03.617964000	EOT	
211.234.117.141	172.16.253.132	443,1259	Oct 14, 2012 16:35:03.857354000	EOT	
172.16.253.132	211.234.117.141	1259,443	Oct 14, 2012 16:35:03.857396000	EOT	
172.16.253.132	211.234.117.141	1259,443	Oct 14, 2012 16:35:03.857496000	EOT	
211.234.117.141	172.16.253.132	443,1259	Oct 14, 2012 16:35:03.857577000	EOT	
172.16.253.132	211.234.117.141	1260,443	Oct 14, 2012 16:35:05.924143000	EOT	
211.234.117.141	172.16.253.132	443,1260	Oct 14, 2012 16:35:06.166833000	EOT	
172.16.253.132	211.234.117.141	1260,443	Oct 14, 2012 16:35:06.166869000	EOT	
172.16.253.132	211.234.117.141	1260,443	Oct 14, 2012 16:35:06.167020000	EOT	211.234.117.141:443
211.234.117.141	172.16.253.132	443,1260	Oct 14, 2012 16:35:06.167229000	EOT	
211.234.117.141	172.16.253.132	443,1260	Oct 14, 2012 16:35:06.403315000	EOT	
172.16.253.132	211.234.117.141	1261,443	Oct 14, 2012 16:35:08.394464000	EOT	
211.234.117.141	172.16.253.132	443,1261	Oct 14, 2012 16:35:08.638916000	EOT	
172.16.253.132	211.234.117.141	1261,443	Oct 14, 2012 16:35:08.638953000	EOT	
172.16.253.132	211.234.117.141	1261,443	Oct 14, 2012 16:35:08.640459000	EOT	211.234.117.141:443
211.234.117.141	172.16.253.132	443,1261	Oct 14, 2012 16:35:08.642335000	EOT	
211.234.117.141	172.16.253.132	443,1261	Oct 14, 2012 16:35:08.879689000	EOT	
172.16.253.132	211.234.117.141	1261,443	Oct 14, 2012 16:35:08.879731000	EOT	
172.16.253.132	211.234.117.141	1261,443	Oct 14, 2012 16:35:08.881201000	EOT	
211.234.117.141	172.16.253.132	443,1261	Oct 14, 2012 16:35:08.882592000	EOT	

Hasil tshark dari file t12.pcap, berikut adalah beberapa artefak penting yang bisa diidentifikasi:

a. Komunikasi Berkala dan Broadcasting:

Banyak paket dari 172.16.253.1 ke 172.16.253.255 (broadcast). Ini kemungkinan besar merupakan heartbeat, ARP, atau NetBIOS Name Service yang umum ditemukan di jaringan lokal.

Tanggal dan waktu menunjukkan komunikasi dilakukan secara periodik (setiap 30 detik atau kurang).

b. Aktivitas DHCP:

Terlihat komunikasi dari 0.0.0.0 ke 255.255.255.255, kemungkinan besar adalah permintaan DHCP (DHCP Discover).

Diikuti oleh balasan dari 172.16.253.254 ke 172.16.253.132, yang menunjukkan DHCP Offer atau ACK.

c. Aktivitas Multicast:

224.0.0.22 adalah alamat multicast IGMP (Internet Group Management Protocol), biasanya untuk keperluan multicast group membership (seperti yang digunakan dalam protokol routing seperti PIM).

d. Koneksi TLS/SSL ke Internet:

Host 172.16.253.132 melakukan koneksi keluar ke IP 211.234.117.141 pada port 443 (HTTPS) menggunakan banyak port sumber berbeda (1230–1240).

Alamat IP 211.234.117.141 ini terindikasi sebagai host eksternal, kemungkinan berada di Korea Selatan berdasarkan ASN lookup (SK Telecom atau sejenisnya).

Jumlah koneksi HTTPS yang berurutan ini mencurigakan dan mungkin menandakan beaconing ke C2 server (Command & Control).

ARTEFAK MALWARE

Artefak	Penjelasan
Koneksi berkala ke IP eksternal	<u>172.16.253.132 terus-menerus melakukan koneksi TLS ke 211.234.117.141, yang patut dicurigai sebagai indikasi komunikasi ke C2 server.</u>
Penggunaan port sumber yang meningkat berturut-turut (1230–1240)	Menunjukkan script atau malware yang membuka koneksi dalam pola otomatis.
Broadcast/DHCP dan multicast	Umumnya normal, namun bisa dipakai oleh malware untuk pengintaian lokal.
Tidak ada hostname HTTP terlihat	Karena sebagian besar koneksi adalah HTTPS, data aplikasi terenkripsi — analisis lebih lanjut perlu dilakukan pada payload jika TLS dapat didekripsi atau SNI terlihat.

6. Analisa File Attack2.json, daftarkan semua malware digunakan dalam serangan.

Tabel Ringkasan Analisis – t12.pcap & t13.pcap

Aspek	Hasil Analisis
IP Lokal Aktif	172.16.253.132
IP Eksternal Dituju	211.234.117.141 (Korea Selatan)
Port yang Digunakan	443 (HTTPS / TLS)
SNI (Server Name Indication)	smp-rda.samsungdm.com
Aktivitas yang Terlihat	Banyak koneksi TLS singkat, frekuensi tinggi, pola otomatis/berulang
Peran IP Lokal	Sebagai inisiator koneksi TLS (ip.src)
Keterkaitan dengan Sample3	IP 172.16.253.132 terdapat pada sample3 → host aktif melakukan komunikasi
Kemungkinan	Host 172.16.253.132 merupakan pelaku atau endpoint yang telah dikompromi

Kesimpulan : Host 172.16.253.132 kemungkinan merupakan sumber serangan atau telah terinfeksi, karena melakukan koneksi TLS yang mencurigakan ke IP eksternal secara terus-menerus.

7. Masih menggunakan file attack2.json, untuk semua malware yang digunakan, daftarkan indicator setiap malware tersebut.

```

(aguto@frostind) [~/Downloads/File Pendukung Challenge 4]
$ cat attack2.json | jq
{
  "type": "bundle",
  "id": "bundle--a7407872-687f-4b75-9851-f1b29a28862c",
  "objects": [
    {
      "type": "threat-actor",
      "spec_version": "2.1",
      "id": "threat-actor--89f53508-1799-44fd-8c33-a3d2a7f55f24",
      "created": "2024-06-12T00:00:00.000Z",
      "modified": "2024-06-12T00:00:00.000Z",
      "name": "APT41",
      "description": "APT41 is a sophisticated and prolific threat group operating with a clear nexus to the People's Republic of China (PRC). This group distinguishes itself through a dual operational mandate, conducting state-sponsored cyber espionage activities in parallel with financially motivated cybercrime. It targets a wide array of sectors globally, including governments, technology, healthcare, and the video game industry. APT41 is known for using custom malware, exploiting zero-day vulnerabilities, and leveraging legitimate cloud services for C2 communications.",
      "aliases": [
        "G0096",
        "H00000",
        "BARIUM",
        "Bress Typhoon",
        "Wicked Panda",
        "Double Dragon",
        "TG-2633",
        "Bronze Atlas",
        "Red Kelpie",
        "Blackfly",
        "Grayfly",
        "Earth Baku",
        "SparklingGoblin",
        "TAA15",
        "BrazenBamboo",
        "Winnti Group"
      ],
      "roles": [
        "espionage",
        "financial-theft"
      ],
      "goals": [
        "intelligence-gathering",

```

Berdasarkan file attack2.json, malware ini dikaitkan dengan APT41, yang dikenal memiliki dua misi utama:

- ✓ Espionage (spionase/sadap data): Menargetkan pemerintah, kesehatan, game, dll.
- ✓ Financial-theft (pencurian finansial): Aktivitas siber kriminal untuk keuntungan finansial.

Ini mengindikasikan malware mampu:

- ✓ Mengambil data sensitif
- ✓ Mengakses akun atau sistem finansial
- ✓ Mencuri identitas atau kredensial

Dari deskripsi:

"known for using custom malware, exploiting zero-day vulnerabilities, and leveraging legitimate cloud services for C2 communication"

Berarti malware ini mampu:

- ✓ Menyerang kerentanan zero-day
- ✓ Menggunakan cloud services sebagai media komunikasi C2, yang lebih sulit dideteksi
- ✓ Dikustomisasi untuk target tertentu

8. Jelaskan apakah attack tersebut ada hubungannya dengan sample 3, jelaskan alasannya.

Berdasarkan analisis pslist.txt

Tidak ditemukan proses mencurigakan yang sesuai dengan indikator serangan dari APT41 dalam attack2.json, seperti:

- ✓ mimikatz.exe
- ✓ beacon.exe (Cobalt Strike)
- ✓ PLUSDROP, PLUSINJECT, KEYPLUG, DUSTPAN, atau DEADEYE

Semua proses yang muncul merupakan proses sistem normal, seperti:

- ✓ svchost.exe, lsass.exe, services.exe, explorer.exe, dll
- ✓ Tidak ada tanda injeksi, parent-child abnormal, atau nama proses aneh

Berdasarkan artefak attack2.json

Tidak ada bukti malware/tools, domain, IP, atau file hash dari attack2.json yang muncul dalam proses sample3

Kesimpulan dari Sample3 tidak menunjukkan bukti bahwa ia adalah host yang digunakan dalam serangan TOUGHPROGRESS oleh APT41.

9. Rekomendasi apa yang dapat anda usulkan (Minimal 5 hal) untuk mitigasi risiko tersebut.

a. Implementasi Network Segmentation dan Firewall Policy [1].

Tujuan: Mencegah lateral movement dan outbound traffic ke command & control server.

- Segmentasikan jaringan antara sistem kritis dan sistem umum (workstation, IoT).

- Blokir semua komunikasi keluar ke IP atau domain yang tidak dikenal, khususnya:
 - ✓ IP seperti 211.234.117.141
 - ✓ Port tidak standar seperti 4444 (umum dipakai reverse shell/metasploit).
 - Aktifkan outbound filtering berbasis DNS dan IP reputation.
- b. Monitoring dan Logging Aktivitas PowerShell & rundll32 [2].

Tujuan: Deteksi dini eksekusi file LOLBins (Living-Off-The-Land Binaries).

- Aktifkan PowerShell logging:
 - ✓ Script Block Logging
 - ✓ Module Logging
 - Pantau eksekusi rundll32.exe, powershell.exe, dan iexplore.exe dari jalur tidak normal.
 - Gunakan EDR (Endpoint Detection & Response) untuk mendeteksi abuse command seperti:
 - ✓ powershell.exe -enc ...
 - ✓ rundll32.exe javascript:...
- c. Harden dan Update Sistem [3].

Tujuan: Mencegah eksploitasi terhadap kerentanan zero-day atau unpatched system.

- Lakukan patch management secara berkala, terutama untuk:
 - ✓ Windows OS
 - ✓ Perangkat jaringan (Cisco IOS, firmware ESP32)
- Audit firmware dan perangkat IoT. Gunakan versi firmware resmi dan aman.
- Nonaktifkan fitur yang tidak digunakan pada BIOS dan perangkat jaringan.

d. Deteksi dan Respons Terhadap Aktivitas C2 [4].

Tujuan: Mendeteksi beaconing, exfiltration data, dan perintah jarak jauh.

- Analisis trafik yang menunjukkan:
 - ✓ HTTP GET ke file .php dengan id=...
 - ✓ HTTPS connection dari satu host ke satu IP berkali-kali dalam waktu singkat
- Gunakan NIDS/NIPS seperti Suricata/Snort dengan signature untuk C2.
- Monitor trafik TLS handshake yang abnormal (misalnya SNI kosong, self-signed certificate, IP-based SNI).

- e. Isolasi dan Forensik terhadap Host Terindikasi [5].

Tujuan: Memastikan host yang terindikasi tidak menyebarkan infeksi.

- Isolasi host 172.16.253.132 dari jaringan utama.
- Lakukan memory forensics lanjutan dengan tools yang stabil (Gunakan Volatility3 atau Rekall, dengan dependensi terinstal benar).
- Cek registry run keys, scheduled tasks, dan startup scripts.

- f. Threat Intelligence Feed dan IOC Correlation [6].

Tujuan: Mengidentifikasi malware APT41 melalui IOC (Indicator of Compromise).

- Cek IOC dari attack2.json (IP, hash, domain) terhadap:
 - ✓ Traffic log
 - ✓ File system (hash comparison)
 - ✓ Proses runtime
- Integrasikan feed threat intelligence ke SIEM.

- g. Edukasi Pengguna dan Awareness Program [7].

Tujuan: Mengurangi risiko rekayasa sosial (spear-phishing, malicious link).

- Latihan simulasi serangan phishing secara berkala.
- Edukasi karyawan terhadap tanda-tanda malware aktif (pop-up, slow system, antivirus disable).
- Batasi hak akses user. Terapkan prinsip least privilege.

FILE II

1. Tunjukkan lewat bukti artifak yang menjadi bukti bahwa host terssebut telah terinfeksi

```
(kali@kali)-[~/volatility]
$ python2 vol.py -f sample4 imageinfo

Volatility Foundation Volatility Framework 2.6.1
INFO : volatility.debug : Determining profile based on KDBG search...
Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
AS Layer1 : IA32PagedMemoryPae (Kernel AS)
AS Layer2 : FileAddressSpace (/home/kali/volatility/sample4)
PAE type : PAE
DTB : 0x319000L
KDBG : 0x80545ae0L
Number of Processors : 1
Image Type (Service Pack) : 3
KPCR for CPU 0 : 0xffdf000L
KUSER_SHARED_DATA : 0xffdf000L
Image date and time : 2014-10-17 13:25:30 UTC+0000
Image local date and time : 2014-10-17 18:55:30 +0530
```

```
(kali@kali)-[~/volatility]
$ python2 vol.py -f sample4 --profile=WinXPSP2x86 pslist

Volatility Foundation Volatility Framework 2.6.1
Offset(V) Name PID PPID Thds Hnds Sess Wow64 Start Exit

0x819cc830 System 4 0 56 260 0 0
0x814d8380 smss.exe 380 4 3 19 0 0 2014-06-11 14:49:36 UTC+0000
0x818a1868 csrss.exe 632 380 11 405 0 0 2014-06-11 14:49:36 UTC+0000
0x813dcl8 winlogon.exe 656 380 24 524 0 0 2014-06-11 14:49:37 UTC+0000
0x81659020 services.exe 700 656 16 268 0 0 2014-06-11 14:49:37 UTC+0000
0x81657910 lsass.exe 712 656 24 345 0 0 2014-06-11 14:49:37 UTC+0000
0x814aeda0 vmacthlp.exe 868 700 1 25 0 0 2014-06-11 14:49:37 UTC+0000
0x813d7688 svchost.exe 884 700 21 199 0 0 2014-06-11 14:49:37 UTC+0000
0x818f5d10 svchost.exe 964 700 10 228 0 0 2014-06-11 14:49:38 UTC+0000
0x813cf5a0 svchost.exe 1052 700 85 1487 0 0 2014-06-11 14:49:38 UTC+0000
0x817e2818 svchost.exe 1112 700 6 75 0 0 2014-06-11 14:49:38 UTC+0000
0x8150b020 svchost.exe 1184 700 16 210 0 0 2014-06-11 14:49:40 UTC+0000
0x81506c68 spoolsv.exe 1388 700 15 131 0 0 2014-06-11 14:49:40 UTC+0000
0x813b0da0 vmttoolsd.exe 1984 700 10 268 0 0 2014-06-11 14:49:46 UTC+0000
0x81764da0 VMUpgradeHelper 224 700 5 94 0 0 2014-06-11 14:49:49 UTC+0000
0x81756b08 alg.exe 564 700 6 101 0 0 2014-06-11 14:49:51 UTC+0000
0x81387710 explorer.exe 1456 1252 16 472 0 0 2014-06-11 14:49:55 UTC+0000
0x81378a10 VMwareTray.exe 1680 1456 1 58 0 0 2014-06-11 14:49:56 UTC+0000
0x8173b850 VMwareUser.exe 1688 1456 8 214 0 0 2014-06-11 14:49:56 UTC+0000
0x81612b28 GrooveMonitor.e 1708 1456 2 108 0 0 2014-06-11 14:49:56 UTC+0000
0x81376558 ZoomIt.exe 1716 1456 2 37 0 0 2014-06-11 14:49:56 UTC+0000
0x8136a0e8 ctfmon.exe 1764 1456 1 71 0 0 2014-06-11 14:49:56 UTC+0000
0x81745da0 wuauclt.exe 1452 1052 7 172 0 0 2014-06-19 10:32:27 UTC+0000
0x8175a020 spoolsv.exe 1660 1688 0 0 0 0 2014-10-17 13:24:18 UTC+0000 2014-10-
17 13:24:18 UTC+0000
0x8150f268 wmiiprvse.exe 500 884 8 148 0 0 2014-10-17 13:25:18 UTC+0000
0x812ded68 cmd.exe 468 1984 0 0 0 0 2014-10-17 13:25:29 UTC+0000 2014-10-
17 13:25:30 UTC+0000
```

```
(kali@kali)~/volatility
$ python2 vol.py -f sample4 --profile=WinXPSP2x86 psxview
Volatility Foundation Volatility Framework 2.6.1
Offset(P) Name PID pslst psscan thrdproc pspcid csrss session deskthrd ExitTime
0x01859020 services.exe 700 True True True True True True True
0x016aeda0 vmacthlp.exe 868 True True True True True True True
0x015b0da0 vmttoolsd.exe 1984 True True True True True True True
0x0170b020 svchost.exe 1184 True True True True True True True
0x015dc1a8 winlogon.exe 656 True True True True True True True
0x0170f268 wmiprvse.exe 500 True True True True True True True
0x01956b08 alg.exe 564 True True True True True True True
0x01964da0 VMUpgradeHelper 224 True True True True True True True
0x01857910 lsass.exe 712 True True True True True True True
0x01812b28 GrooveMonitor.e 1708 True True True True True True True
0x01af5d10 svchost.exe 964 True True True True True True True
0x015d7688 svchost.exe 884 True True True True True True True
0x015cf5a0 svchost.exe 1052 True True True True True True True
0x01578a10 VMwareTray.exe 1680 True True True True True True True
0x0193b850 VMwareUser.exe 1688 True True True True True True True
0x019e2818 svchost.exe 1112 True True True True True True True
0x01706c68 spoolsv.exe 1388 True True True True True True True
0x01576558 ZoomIt.exe 1716 True True True True True True True
0x01945da0 wuauclt.exe 1452 True True True True True True True
0x0156a0e8 ctfdmon.exe 1764 True True True True True True True
0x01587710 explorer.exe 1456 True True True True True True True
0x016d8380 smss.exe 380 True True True True False False False
0x01bcc830 System 4 True True True True False False False
0x0195a020 spools.exe 1660 True True False True False False False 2014-10-17 13:24:18 UTC
+0000
0x014ded68 cmd.exe 468 True True False True False False False 2014-10-17 13:25:30 UTC
+0000
0x01aa1868 csrss.exe 632 True True True True False True True
0x01548518 ipconfig.exe 1812 False True False False False False False 2014-10-17 13:25:30 UTC
+0000
```

Analisi sample4 menggunakan Tools Volatility Framework 2.6.1, Profile sistem: WinXPSP2x86.

- a. Proses Mencurigakan: spools.exe (PID 1660)

Nama menyerupai spoolsv.exe (legit) → indikasi masquerading

Tidak dikenali secara lengkap oleh plugin psxview:

Nilai thrdproc, csrss, session, deskthrd = False

Memiliki ExitTime cepat: 2014-10-17 13:24:18

Umumnya digunakan oleh malware dropper atau loader

Indikasi kuat proses ini adalah malware sementara yang disembunyikan

- b. Proses Mencurigakan: cmd.exe (PID 468)

Parent process: vmttoolsd.exe → tidak lazim

ExitTime: 2014-10-17 13:25:30

Tidak terdeteksi penuh di psxview

Kemungkinan besar digunakan untuk eksekusi perintah otomatis oleh malware

- c. Proses Tersembunyi: ipconfig.exe (PID 1812)

Tidak terlihat di pslst, hanya muncul di psscan → proses tersembunyi

ExitTime: 2014-10-17 13:25:30

Kemungkinan digunakan untuk enumerasi jaringan oleh penyerang (network recon)

d. Pola Waktu Eksekusi

Tiga proses ini dieksekusi secara berurutan dalam waktu yang sangat singkat:

spools.exe → cmd.exe → ipconfig.exe

Pola ini konsisten dengan aktivitas malware seperti:

- ✓ Payload execution
- ✓ Command execution
- ✓ Reconnaissance

Kesimpulan

Berdasarkan hasil analisis memori menggunakan Volatility, ditemukan tiga artifak penting yang menunjukkan bahwa sistem telah terinfeksi.

Artifak	Bukti	Indikasi
spools.exe	Masquerading	psxview anomaly Malware dropper atau loader
cmd.exe	Parent tidak wajar	exit cepat Eksekusi perintah otomatis
ipconfig.exe	Proses tersembunyi	tool recon Aktivitas post-infection attacker

2. Jelaskan dan buktikan bagaimana host tersebut bisa terinfeksi.

```
(kali@kali) ~[volatility]
$ python2 vol.py -f sample4 --profile=WinXPSP2x86 malfind --dump-dir=malfind_output

Volatility Foundation Volatility Framework 2.6.1
Process: csrss.exe Pid: 632 Address: 0x7f6f0000
Vad Tag: Vad Protection: PAGE_EXECUTE_READWRITE
Flags: Protection: 6

0x000000007f6f0000 c8 00 00 00 e5 01 00 00 ff ee ff ee 08 70 00 00 .....D..
0x000000007f6f0010 08 00 00 00 00 fe 00 00 00 10 00 00 20 00 00 .....
0x000000007f6f0020 00 02 00 00 00 20 00 00 8d 01 00 00 ff ef fd 7f .....
0x000000007f6f0030 03 00 08 06 00 00 00 00 00 00 00 00 00 00 00 .....

0x000000007f6f0000 c8000000 ENTER 0x0, 0x0
0x000000007f6f0004 e501 IN EAX, 0x1
0x000000007f6f0006 0000 ADD [EAX], AL
0x000000007f6f0008 ff DB 0xff
0x000000007f6f0009 ee OUT DX, AL
0x000000007f6f000a ff DB 0xff
0x000000007f6f000b ee OUT DX, AL
0x000000007f6f000c 087000 OR [EAX+0x0], DH
0x000000007f6f000f 0008 ADD [EAX], CL
0x000000007f6f0011 0000 ADD [EAX], AL
0x000000007f6f0013 0000 ADD [EAX], AL
0x000000007f6f0015 fe00 INC BYTE [EAX]
0x000000007f6f0017 0000 ADD [EAX], AL
0x000000007f6f0019 0010 ADD [EAX], DL
0x000000007f6f001b 0000 ADD [EAX], AL
0x000000007f6f001d 2000 AND [EAX], AL
0x000000007f6f001f 0000 ADD [EAX], AL
0x000000007f6f0021 0200 ADD AL, [EAX]
0x000000007f6f0023 0000 ADD [EAX], AL
0x000000007f6f0025 2000 AND [EAX], AL
0x000000007f6f0027 005d010000ff ADD [EBP-0xfffffff], CL
0x000000007f6f002d ef OUT DX, EAX
0x000000007f6f002e fd STD
0x000000007f6f002f 7f03 JG 0x7f6f0034
0x000000007f6f0031 0008 ADD [EAX], CL
0x000000007f6f0033 06 PUSH ES
0x000000007f6f0034 0000 ADD [EAX], AL
0x000000007f6f0036 0000 ADD [EAX], AL
0x000000007f6f0038 0000 ADD [EAX], AL
0x000000007f6f003a 0000 ADD [EAX], AL
0x000000007f6f003c 0000 ADD [EAX], AL
0x000000007f6f003e 0000 ADD [EAX], AL

Process: winlogon.exe Pid: 656 Address: 0xcf10000
Vad Tag: Vad5 Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 4, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x00000000cf10000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000000cf10010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

```
(kali@kali) ~[volatility]
$ ls malfind_output/

process.0x81387710.0x1df0000.dmp process.0x813dc1a8.0x5b840000.dmp process.0x813dc1a8.0xcf10000.dmp
process.0x81387710.0x2ad0000.dmp process.0x813dc1a8.0x622c0000.dmp process.0x81612b28.0xb80000.dmp
process.0x813dc1a8.0x27050000.dmp process.0x813dc1a8.0x66700000.dmp process.0x818a1868.0x7f6f0000.dmp
process.0x813dc1a8.0x368b0000.dmp process.0x813dc1a8.0x7d540000.dmp
process.0x813dc1a8.0x47150000.dmp process.0x813dc1a8.0x7e8d0000.dmp
```

```
D:\VmImgDescriptorP
MEMZ
.rdata
.CRT$XCU
.data
.bss
.text$yc
.text$yd
.text
.atexit
.ext
.patches
.int
.xit
.ctx
a:value
a:name
tn:data[0].bytes
TnBoot: Don't Need To Update
TnBoot: Need To Update
fname
config[0].parameter
coresys
SetKey
LibManagerDoneEvent
LibManagerStart
\core.default.dll
bootup[0].core[0].parameter
core
bootup-xml
booturl
Coredll
core.100.dll
http://www.targetn.com/mymodules/bootup.exe.xml
j:\t3\smcore\..\core/bootup.cpp
c:\temp\tn3\
http://www.in-t-e-r-n-e-t.com/bootup.exe.xml
TnBoot
RunMe
Bytes Finished Successfully
Download Of
bits
HTTP Query Status Code = [
Could Not Send Request
Content-Type: application/x-www-form-urlencoded
Accept: /*
Could Not Open Request
HTTP/1.0
POST
dlbuffer
dlpost
dlpfile
:
```

- Indikasi Kuat Malware:

URL Mencurigakan

- ✓ text
- ✓ Copy
- ✓ Edit

<http://www.targetn.com/mymodules/bootup.exe.xml>

<http://www.in-t-e-r-n-e-t.com/bootup.exe.xml>

- Menunjukkan Command and Control (C2) URL, digunakan untuk:
 - ✓ Mengambil konfigurasi (.xml)
 - ✓ Mendownload executable payload selanjutnya (bootup.exe)
- String Fungsi/Variabel Khas Malware
 - ✓ text
 - ✓ Copy
 - ✓ Edit
 - ✓ RunMe
 - ✓ Download Of
 - ✓ Starting Download For URL = [
 - ✓ Detected Host = [
 - ✓ Detected Requested File = [
 - ✓ Could Not InternetConnect
 - ✓ HTTP Query Status Code
 - ✓ Content-Type: application/x-www-form-urlencoded
- Ini menunjukkan modul downloader sedang menangani:
 - ✓ Request HTTP/POST
 - ✓ Deteksi koneksi gagal
 - ✓ Penanganan error dan payload
- Path Developer/Debugging

text

- ✓ Copy
 - ✓ Edit
 - ✓ j:\t3\smcore\..\core/bootup.cpp
 - ✓ c:\temp\tn3\
- Ini menunjuk ke:
 - ✓ Lokasi source code di drive j:\ (mungkin bekas compile/debug)

- ✓ c:\temp\tn3\ bisa digunakan sebagai lokasi dropper file berbahaya

Kesimpulan

Berdasarkan artefak dan payload:

- ✓ Host telah terinfeksi oleh malware downloader
- ✓ Malware ini kemungkinan ter-inject ke explorer.exe

Fungsinya adalah:

- ✓ Terkoneksi ke internet
- ✓ Mendownload file bootup.exe
- ✓ Menyimpannya dan menjalankannya

Jalur Infeksi (Infection Chain)

- a. Proses spools.exe muncul mencurigakan:
 - ✓ PID 1660
 - ✓ Exit cepat
 - ✓ Tidak bisa di-dump
 - ✓ Ini kemungkinan dropper awal atau payload loader

- b. cmd.exe muncul tepat setelah spools.exe

Kemungkinan digunakan untuk menjalankan skrip atau payload

- c. explorer.exe terinjeksi
 - ✓ Memuat modul yang berisi string download seperti:
 - ✓ bootup.exe.xml
 - ✓ Koneksi ke targetn.com, in-t-e-r-n-e-t.com
- c. Payload dijalankan sebagai backdoor/downloader

3. Apakah Malware tersebut juga melakukan komunikasi dengan pihak eksternal?

Malware melakukan komunikasi eksternal ke server Command and Control (C2) menggunakan protokol HTTP (port 80) melalui proses yang telah terinjeksi malware, yaitu explorer.exe.

Bukti Komunikasi C2

Hasil dari malfind pada proses explorer.exe menunjukkan string mencurigakan:

- ✓ text
- ✓ Copy
- ✓ Edit
- ✓ http://www.targetn.com/mymodules/bootup.exe.xml
- ✓ http://www.in-t-e-r-n-e-t.com/bootup.exe.xml
- ✓ Detected Host = [
- ✓ Starting Download For URL = [
- ✓ Download Of
- ✓ HTTP/1.0
- ✓ POST
- ✓ Content-Type: application/x-www-form-urlencoded

Interpretasi:

Domain tujuan:

- ✓ www.targetn.com
- ✓ www.in-t-e-r-n-e-t.com

Protocol: HTTP

Metode: POST, umum digunakan untuk mengirim data atau mengambil perintah C2

Program/proses: explorer.exe (PID 1456) — telah terinjeksi dengan payload berdasarkan hasil dump

Kemungkinan besar komunikasi untuk:

- ✓ Mengambil payload tambahan (bootup.exe)
- ✓ Mengirim beacon atau informasi host
- ✓ Menerima perintah dari C2 server

Sifat Komunikasi

Indikasi Downloader: URL mengarah ke file .xml, namun string seperti Download Of, Detected Host, dan RunMe menunjukkan ini bukan file konfigurasi biasa, melainkan payload delivery berbasis XML.

Tidak langsung terlihat IP, karena data belum melalui netscan, namun domain sudah cukup untuk membuktikan komunikasi C2 dilakukan.

Kesimpulan

- ✓ Malware melakukan komunikasi eksternal.
- ✓ Komunikasi terjadi melalui proses explorer.exe yang telah disisipi kode berbahaya.
- ✓ Menggunakan HTTP (port 80) untuk mengambil instruksi atau file dari domain eksternal yang tidak sah.
- ✓ Ini adalah ciri khas aktivitas Command and Control (C2).

4. Apa kemampuan malware tersebut?

```
(kali@kali)-[~/volatility]
$ python2 vol.py -f sample4 --profile=WinXPSP3x86 consoles
Volatility Foundation Volatility Framework 2.6.1
*****
ConsoleProcess: csrss.exe Pid: 632
Console: 0x4f23b0 CommandHistorySize: 50
HistoryBufferCount: 2 HistoryBufferMax: 4
OriginalTitle: ?OystemRoot%\system32\cmd.exe
Title: ?O\WINDOWS\system32\cmd.exe
*****
ConsoleProcess: csrss.exe Pid: 632
Console: 0xf94590 CommandHistorySize: 50
HistoryBufferCount: 1 HistoryBufferMax: 4
OriginalTitle: ??
Title:

(kali@kali)-[~/volatility]
$ python2 vol.py -f sample4 --profile=WinXPSP2x86 printkey -K "Software\\Microsoft\\Windows\\CurrentVersion\\Run"

Volatility Foundation Volatility Framework 2.6.1
Legend: (S) = Stable (V) = Volatile

Registry: \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DAT
Key name: Run (S)
Last updated: 2012-08-15 16:47:38 UTC+0000

Subkeys:

Values:

Registry: \Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT
Key name: Run (S)
Last updated: 2013-06-19 19:41:17 UTC+0000

Subkeys:

Values:
REG_SZ ZoomIt : (S) C:\softwares\ZoomIt\ZoomIt.exe
REG_SZ ctfmon.exe : (S) C:\WINDOWS\system32\ctfmon.exe

Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\default
Key name: Run (S)
Last updated: 2012-08-15 22:09:43 UTC+0000

Subkeys:

Values:

Registry: \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.DAT
Key name: Run (S)
Last updated: 2012-08-15 16:47:35 UTC+0000

Subkeys:

Values:
```

Malware menunjukkan tanda-tanda kapabilitas berbahaya, termasuk:

- ✓ Persistence (kegigihan)
- ✓ Downloader/backdoor
- ✓ Potensi eksfiltrasi data
- ✓ DLL injection atau code injection ke proses sah seperti explorer.exe dan winlogon.exe

a. DLL Injection / Code Injection

Berdasarkan hasil malfind, banyak proses yang dimodifikasi atau di-inject, seperti:

- ✓ explorer.exe (PID 1456)
- ✓ winlogon.exe (PID 656)
- ✓ csrss.exe, svchost.exe, services.exe — juga ditemukan dump dengan entri .text, .data, .rdata mencurigakan.

Hasil dump dari proses explorer.exe berisi string:

- ✓ arduino
- ✓ Copy
- ✓ Edit
- ✓ <http://www.targetn.com/mymodules/bootup.exe.xml>
- ✓ SetKey, RunMe, Core_Downloader, Coredll

Menunjukkan bahwa malware menyuntikkan payload ke proses sistem yang sah dan menjalankan fungsionalitas berbahaya darinya.

b. Persistence / Autorun

Nama proses mencurigakan spools.exe (bukan spoolsv.exe asli) ditemukan pada:

PID: 1660 – muncul pada waktu yang berbeda dari proses lain (tanggal 2014-10-17, dibanding waktu sistem aktif 2014-06-11).

Ini menunjukkan proses ditambahkan belakangan dan disamarkan sebagai proses sistem.

Hasil cmdscan dan consoles mengindikasikan aktivitas command line, meskipun tidak seluruh perintah terlihat (indikasi ada command dijalankan melalui backdoor).

c. Kemampuan Eksfiltrasi Data

Banyak string menunjukkan modul untuk membuat permintaan HTTP:

- ✓ mathematica
- ✓ Copy
- ✓ Edit
- ✓ Content-Type: application/x-www-form-urlencoded
- ✓ POST
- ✓ Download Of
- ✓ Starting Download For URL
- ✓ HTTP/1.0
- ✓ Internet Explorer (compatible)
- ✓ Could Not InternetConnect

- ✓ Ini menandakan malware memiliki kemampuan melakukan koneksi HTTP ke luar, mengirim atau menerima data.

String seperti Detected Requested File = [menunjukkan fungsi untuk mengirim file/data keluar, artinya potensi eksfiltrasi data tinggi.

Kapabilitas	Ada?	Bukti
Persistence	Ada	Proses spools.exe, kemungkinan autorun; waktu berbeda dari boot
Backdoor	Ada	Injection ke explorer.exe, perintah dijalankan diam-diam
Eksfiltrasi Data	Ada	String HTTP POST + URL target + payload download/upload
DLL Injection	Ada	Dump malfind menunjukkan .text, .data, .rdata, string khas malware
Downloader	Ada	bootup.exe, bootup-xml, core.100.dll

5. Rekomendasi apa yang dapat anda usulkan (Minimal 5 hal) untuk mitigasi risiko tersebut.

a. Lakukan Isolasi Sistem Terdampak Segera [8].

Tujuan: Menghentikan penyebaran malware dan menghentikan komunikasi ke server C2.

- ✓ Putuskan koneksi internet sistem yang terinfeksi.
- ✓ Isolasi dari jaringan lokal/internal.

Tujuannya untuk mencegah eksfiltrasi data lebih lanjut dan komunikasi ke domain jahat seperti targetn.com.

b. Lakukan Reimaging / Reinstall Sistem Operasi [9].

Tujuan: Menghapus sepenuhnya file dan proses berbahaya, termasuk yang menggunakan persistence.

Karena malware menyamarkan diri sebagai spools.exe dan menyuntikkan code ke winlogon.exe, lebih aman untuk memasang ulang OS.

Hindari hanya menggunakan antivirus biasa karena malware sudah menyusup ke proses sistem sah.

c. Lakukan Audit dan Monitoring Lalu Lintas Jaringan [10].

Tujuan: Deteksi komunikasi C2 dan potensi infeksi di endpoint lain.

Cari komunikasi HTTP ke:

- ✓ <http://www.targetn.com/mymodules/bootup.exe.xml>
- ✓ <http://www.in-t-e-r-n-e-t.com/bootup.exe.xml>

Monitoring dilakukan dengan tools seperti Zeek, Suricata, atau Wireshark, serta pengecekan log proxy/firewall.

d. Implementasi Kebijakan Least Privilege dan Proteksi Eksekusi File [11].

Tujuan: Mengurangi kemungkinan eksekusi file mencurigakan oleh user biasa.

Batasi hak akses user agar tidak bisa mengeksekusi aplikasi dari direktori seperti C:\Temp\.

Gunakan fitur seperti AppLocker, Software Restriction Policies, atau Windows Defender Application Control (WDAC) untuk memblokir aplikasi yang tidak dikenali.

e. Tingkatkan Edukasi dan Awareness Pengguna

Tujuan: Menghindari infeksi ulang yang disebabkan oleh interaksi pengguna seperti membuka attachment/file dari email [12].

Edukasi tentang:

- ✓ Bahaya file dropper yang disamarkan.
- ✓ Tidak membuka file dari sumber tidak terpercaya.
- ✓ Simulasikan phishing secara berkala untuk edukasi.

Perbarui dan Harden Sistem

Tujuan: Mencegah eksploitasi celah yang bisa dimanfaatkan malware.

- ✓ Selalu update sistem operasi dan aplikasi.
- ✓ Nonaktifkan fitur yang tidak digunakan.
- ✓ Gunakan EDR (Endpoint Detection & Response) untuk mendeteksi perilaku mencurigakan.

PENGUNAAN AI



Dalam proses investigasi tugas 1, tim Bear Cyber Hunt memanfaatkan kecerdasan buatan (AI) untuk membantu mengidentifikasi aktivitas jaringan yang mencurigakan. Meskipun tidak ditemukan permintaan HTTP ke file dengan ekstensi umum seperti .exe, .sh, atau .zip, AI tetap mampu mendeteksi pola anomali, komunikasi tersembunyi, dan potensi malware yang mungkin disamarkan. Dengan AI, kami bisa menganalisis trafik terenkripsi, payload tersembunyi, hingga koneksi yang tampaknya normal tapi ternyata bagian dari aktivitas Command & Control (C2). Ini membantu tim kami mengambil tindakan lebih cepat dan akurat dalam memburu ancaman siber yang canggih.



Tim Bear Cyber Hunt menggunakan bantuan AI untuk mengidentifikasi kendala teknis yang sering dialami dalam proses analisis memori forensik. Ketika muncul pesan `volatility: command not found`, AI mengonfirmasi bahwa tool Volatility belum terinstal atau belum dikenali dalam PATH shell di sistem Kali Linux yang digunakan. Untuk mengatasi masalah ini, AI menyarankan langkah-langkah praktis instalasi dan

konfigurasi yang tepat agar Volatility dapat dijalankan dengan lancar untuk mendukung proses hunting dan analisis memori.

REFERENSI

- [1] Agus, Arif, & Muhammad. (2024). *Pemanfaatan penggunaan media sosial sebagai sarana edukasi di kalangan pelajar*.
<https://ejournal.arbapustaka.web.id/index.php/jmpm/article/view/5>
- [2] Alida. (n.d.). *Implementasi Sistem Keamanan Email Berbasis Open Source Studi Kasus Ppin-Batan*. <https://repository.uinjkt.ac.id/dspace/handle/123456789/68359>
- [3] Brian, Daniel, Rajwa, & Aep. (2024). *Uji Penetrasi Injeksi SQL terhadap Celah Keamanan Database Website menggunakan SQLmap*.
<https://journal.pubmedia.id/index.php/pjise/article/view/2623>
- [4] Buyung. (2022). *Manajemen N-IOM (Manajemen Neurologi-Intraoperatif) pada Eksisi Tumor Myelum dan Dekompresi Stabilisasi Servikal C2-C6*.
<https://www.inasnacc.org/ojs2/index.php/jni/article/view/442>
- [5] Djuandi. (n.d.). *Framework d3fend untuk menutup celah keamanan web server nginx menggunakan taktik harden pada smartlink*.
<https://repository.uinjkt.ac.id/dspace/handle/123456789/80216>
- [6] M. (2017). *Analisis Forensik pada Unmanned Aerial Vehicle (UAV) Untuk Mendapatkan Artefak Parameter Penerbangan Sebagai Barang Bukti Digital*.
<https://dspace.uui.ac.id/handle/123456789/31584>
- [7] M., Yuhandri, & Syafri. (2024). *Audit Keamanan Jaringan Komputer Server dari Serangan DDoS Menggunakan Snort Intrusion Detection System*.
<http://ijcs.net/ijcs/index.php/ijcs/article/view/4391>
- [8] Muhammd, M., & Muhammad. (2024). *Perancangan Dan Implementasi Cloud Base Microsegmentation Firewall Menggunakan Metode Ppdioo*.
<https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/download/23948/22957>
- [9] Nawwar. (n.d.). *Analisis forensik digital pada bukti digital kejahatan siber menggunakan digital forensic research workshop model*.
<https://repository.uinjkt.ac.id/dspace/handle/123456789/83810>
- [10] Samsumar. (2025). *KEAMANAN SISTEM INFORMASI: PERLINDUNGAN DATA DAN PRIVASI DI ERA DIGITAL*.
<http://pustakahadla.com/xmlui/handle/123456789/39>
- [11] Umar. (2011). *Remastering Sistem Operasi Ubuntu Untuk Penunjang Perkuliahan Dengan Studi Kasus Di FTI UII*.
<https://dspace.uui.ac.id/handle/123456789/35209>