

# MALWARE ANALYSIS

2540123403 - BERTRAND REDONDO MULYONO  
2502064303 - BETRAND GABRIALDI LEONARD  
2540125024 - FELYSIA MEYTRI  
2540123100 - VICTOR BENAYA

Start Slide

**Link**  
**Malware**

<https://www.malware-traffic-analysis.net/2021/02/08/index.html>



# Executive Summary

Pada tanggal 8 Februari 2021, Windows DESKTOP-MGVG60Z milik Bill Cook terinfeksi oleh tiga malware, yaitu Hancitor, Cobalt Strike, dan Ficker Stealer Malware.



### Details from Victim

- IP Address: 10.2.8.101
- Hostname: DESKTOP-MGVG60Z
- MAC address: 00:12:79:41:c2:aa
- Windows User Account: bill.cook

Data didapatkan dari NBNS dan Kerberos Protocol.

```
Frame 799: 285 bytes on wire (2280 bits), 285 bytes captured (2280 bits) on interface 0
Ethernet II, Src: HewlettP_41:c2:aa (00:12:79:41:c2:aa), Dst: Dell_...
Internet Protocol Version 4, Src: 10.2.8.101, Dst: 10.2.8.255
Transmission Control Protocol, Src Port: 49702, Dst Port: 88, Seq: 1000000000
Kerberos
  Record Mark: 227 bytes
  as-req
    pvno: 5
    msg-type: krb-as-req (10)
    padata: 1 item
    req-body
      Padding: 0
      kdc-options: 40810010
      cname
        name-type: KR85-NT-PRINCIPAL (1)
        cname-string: 1 item
          CNameString: bill.cook
      realm: ASCOLIMITED
      sname
        till: 2037-09-13 02:48:05 (UTC)
        rtime: 2037-09-13 02:48:05 (UTC)
        nonce: 1171320312
      etype: 6 items
      addresses: 1 item DESKTOP-MGVG60Z<20>
```

```
Wireshark · Packet 16 · 2021-02-08-1
Frame 16: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0
Ethernet II, Src: HewlettP_41:c2:aa (00:12:79:41:c2:aa), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 10.2.8.101, Dst: 10.2.8.255
User Datagram Protocol, Src Port: 137, Dst Port: 137
NetBIOS Name Service
  Transaction ID: 0xbcb2
  Flags: 0x2910, Opcode: Registration, Recursion desired, Broadcast
    0... .. = Response: Message is a query
    .010 1... .. = Opcode: Registration (5)
    .... ..0. .... = Truncated: Message is not truncated
    .... ..1 .... = Recursion desired: Do query recursively
    .... ..1 .... = Broadcast: Broadcast packet
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 1
  Queries
    DESKTOP-MGVG60Z<20>: type NB, class IN
      Name: DESKTOP-MGVG60Z<20> (Server service)
      Type: NB (32)
      Class: IN (1)
  Additional records
    DESKTOP-MGVG60Z<20>: type NB, class IN
      Name: DESKTOP-MGVG60Z<20> (Server service)
      Type: NB (32)
      Class: IN (1)
      Time to live: 3 days, 11 hours, 20 minutes
      Data length: 6
      Name flags: 0x0000, ONT: B-node (B-node, unique)
      Addr: 10.2.8.101
```

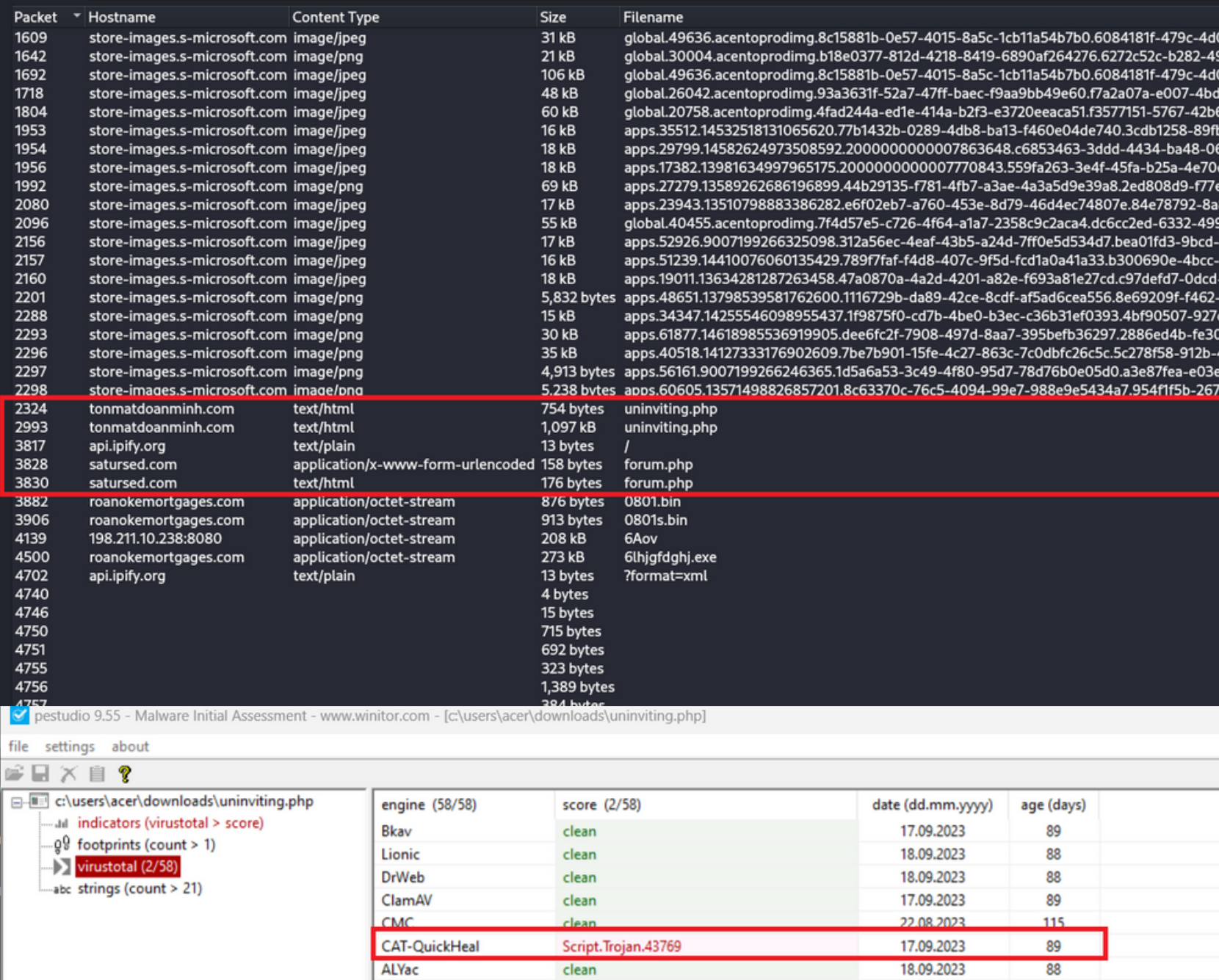


# Computer Forensic

# IOCs

# Hancitor Malware Indication

- File mencurigakan bernama uninvited.php di dalam lalu lintas dari tinmatdoanminh.com (alamat IP: 45.124.85.55) yang terindikasi malware didalamnya.
- Indikasi lain dari traffic tersebut adalah forum.php dari saturesd.com (alamat IP: 213.5.229.12) dan api.ipify.org (berjalan di port 80).



No.	Time	Source	Destination	Protocol	Length	Info
2160	56.250307	173.223.201.150	10.2.8.101	HTTP	1367	HTTP/1.1 200 OK (JPEG JFIF image)
2162	56.277803	10.2.8.101	173.223.201.150	HTTP	464	GET /image/apps.48651.13798539581762600.1116729b-da89-42ce-8cdf-af5ad6cea556.8e69209f-f462-4b41-b898-23b...
2164	56.278056	10.2.8.101	173.223.201.150	HTTP	464	GET /image/apps.61877.14618985536919905.dee6fc2f-7908-497d-8aa7-395befb36297.2886ed4b-fe30-4eb4-9bad-fda...
2166	56.278452	10.2.8.101	173.223.201.150	HTTP	464	GET /image/apps.34347.14255546098955437.1f9875f0-cd7b-4be0-b3ec-c36b31ef0393.4bf90507-927d-488b-b753-221...
2168	56.279544	10.2.8.101	173.223.201.150	HTTP	463	GET /image/apps.56161.9007199266246365.1d5a6a53-3c49-4f80-95d7-78d76b0e05d0.a3e87fea-e03e-4c0a-8f26-9ece...
2170	56.279984	10.2.8.101	173.223.201.150	HTTP	464	GET /image/apps.60605.13571498826857201.8c63370c-76c5-4094-99e7-988e9e5434a7.954f1f5b-2672-41a5-952f-15b...
2172	56.281253	10.2.8.101	173.223.201.150	HTTP	464	GET /image/apps.40518.14127333176902609.7be7b901-15fe-4c27-863c-7c0dbfc26c5c.5c278f58-912b-4af9-88f8-a65...
2201	56.350627	173.223.201.150	10.2.8.101	HTTP	750	HTTP/1.1 200 OK (PNG)
2288	56.415675	173.223.201.150	10.2.8.101	HTTP	548	HTTP/1.1 200 OK (PNG)
2293	56.418776	173.223.201.150	10.2.8.101	HTTP	645	HTTP/1.1 200 OK (PNG)
2296	56.421922	173.223.201.150	10.2.8.101	HTTP	1294	HTTP/1.1 200 OK (PNG)
2297	56.421977	173.223.201.150	10.2.8.101	HTTP	1255	HTTP/1.1 200 OK (PNG)
2298	56.422001	173.223.201.150	10.2.8.101	HTTP	192	HTTP/1.1 200 OK (PNG)
2315	57.210977	10.2.8.101	45.124.85.55	HTTP	498	GET /uninviting.php HTTP/1.1
2324	57.553336	45.124.85.55	10.2.8.101	HTTP	691	HTTP/1.1 200 OK (text/html)
2326	57.604291	10.2.8.101	45.124.85.55	HTTP	595	GET /uninviting.php HTTP/1.1
2993	63.122801	45.124.85.55	10.2.8.101	HTTP	400	HTTP/1.1 200 OK (text/html)
2996	63.213747	10.2.8.101	45.124.85.55	HTTP	508	GET /favicon.ico HTTP/1.1
3029	64.155257	45.124.85.55	10.2.8.101	HTTP	226	HTTP/1.1 200 OK
3815	111.668529	10.2.8.101	54.235.147.252	HTTP	218	GET / HTTP/1.1
3817	111.769800	54.235.147.252	10.2.8.101	HTTP	239	HTTP/1.1 200 OK (text/plain)
3828	115.542363	10.2.8.101	213.5.229.12	HTTP	457	POST /forum.php HTTP/1.1 (application/x-www-form-urlencoded)
3830	115.756203	213.5.229.12	10.2.8.101	HTTP	422	HTTP/1.1 200 OK (text/html)
3880	117.197679	10.2.8.101	8.208.10.147	HTTP	233	GET /0801s.bin HTTP/1.1
3882	117.401219	8.208.10.147	10.2.8.101	HTTP	1176	HTTP/1.1 200 OK
3884	117.418595	10.2.8.101	8.208.10.147	HTTP	234	GET /0801s.bin HTTP/1.1
3886	117.420000	10.2.8.101	8.208.10.147	HTTP	234	GET /0801s.bin HTTP/1.1

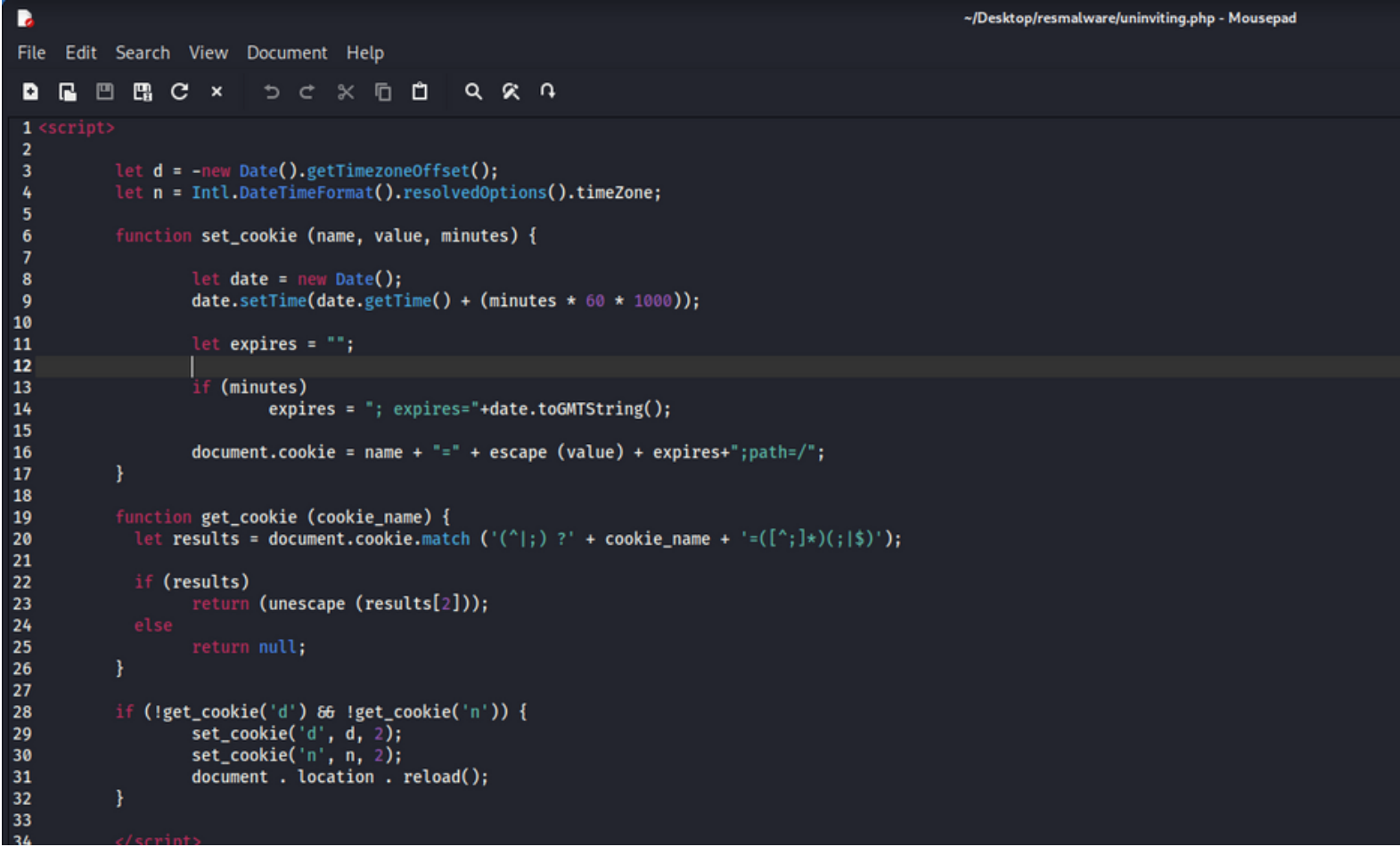
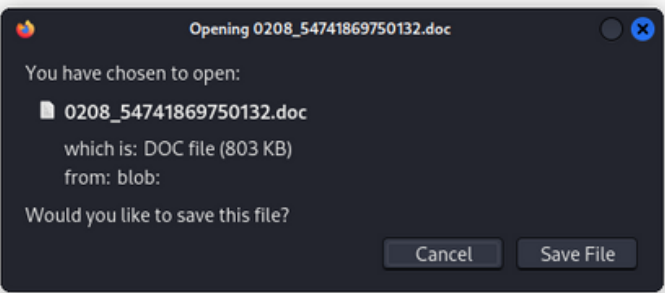
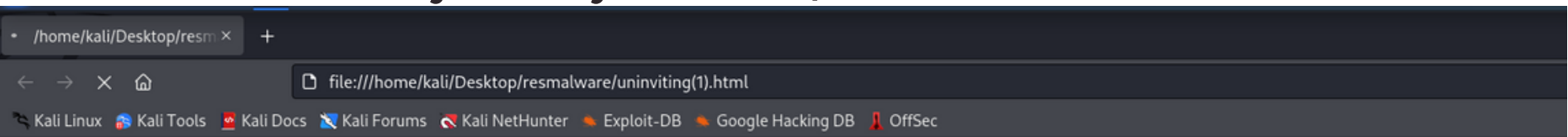
# Malware Analysis

# Computer Forensic

## IOCs

# Hancitor Malware Indication

- Ketika korban menjalankan file tersebut (univiting.php), program mengambil cookie korban dan membuat file malware baru (Ubah ekstensinya menjadi .html).



# Malware Analysis



Computer Forensic

IOCs

Cobalt Strike Malware Indication

- Terdapat file mencurigikan bernama 0801.bin dan 0801s.bin dari roanokemortgages.com (alamat IP: 8.208.10.147).
- Saat file .bin tersebut berhasil terkirim, dari alamat IP 198.211.10.238 mengirimkan file bernama 6AoV yang dimana terindikasi malware didalamnya.

2993	tonmatdoanminh.com	text/html	1,097 kB	uninviting.php
3817	api.ipify.org	text/plain	13 bytes	/
3828	saturdaysed.com	application/x-www-form-urlencoded	158 bytes	forum.php
3830	saturdaysed.com	text/html	176 bytes	forum.php
3882	roanokemortgages.com	application/octet-stream	876 bytes	0801.bin
3906	roanokemortgages.com	application/octet-stream	913 bytes	0801s.bin
4139	198.211.10.238:8080	application/octet-stream	208 kB	6Aov
4500	roanokemortgages.com	application/octet-stream	273 kB	6lhjgfdghj.exe
4702	api.ipify.org	text/plain	13 bytes	?format=xml
4740			4 bytes	
4746			15 bytes	
4750			715 bytes	

engine (58/58)	score (15/58)	date (dd.mm.yyyy)	age (days)
Bkav	clean	25.02.2022	660
Lionic	clean	25.02.2022	660
MicroWorld-eScan	Trojan.Shellcode.11.Gen	25.02.2022	660
FireEye	Trojan.Shellcode.11.Gen	25.02.2022	660
CAT-QuickHeal	clean	25.02.2022	660
ALYac	Trojan.Shellcode.11.Gen	25.02.2022	660
Malwarebytes	clean	25.02.2022	660
Zillya	clean	24.02.2022	661
Sangfor	clean	24.12.2021	723
K7AntiVirus	clean	25.02.2022	660
K7GW	clean	25.02.2022	660
Baidu	clean	18.03.2019	1735
VirIT	clean	25.02.2022	660
Cyren	clean	25.02.2022	660
Symantec	Trojan.Gen.MBT	25.02.2022	660
ESET-NOD32	clean	25.02.2022	660
TrendMicro-HouseCall	Trojan.Win32.COBALT.SMD.hp	25.02.2022	660
Avast	clean	25.02.2022	660
ClamAV	clean	25.02.2022	660
Kaspersky	clean	25.02.2022	660
BitDefender	Trojan.Shellcode.11.Gen	25.02.2022	660
NANO-Antivirus	clean	25.02.2022	660
SUPERAntiSpyware	clean	19.02.2022	666
Tencent	clean	25.02.2022	660
Ad-Aware	Trojan.Shellcode.11.Gen	25.02.2022	660
Emsisoft	Trojan.Shellcode.11.Gen (B)	25.02.2022	660
Comodo	clean	25.02.2022	660
F-Secure	clean	25.02.2022	660
DrWeb	BackDoor.Meterpreter.152	25.02.2022	660
VIPRE	clean	19.01.2022	697
TrendMicro	Trojan.Win32.COBALT.SMD.hp	25.02.2022	660
McAfee-GW-Edition	clean	25.02.2022	660
CMC	clean	26.10.2021	782
Sophos	ATK/Cobalt-D	25.02.2022	660
Ikarus	Trojan.Shellcode	25.02.2022	660
GData	Trojan.Shellcode.11.Gen	25.02.2022	660
Jiangmin	clean	25.02.2022	660

3911	117.633163	8.208.10.147	10.2.8.101	TCP	54 80 → 49757 [ACK] Seq=2282 Ack=545 Win=64240 Len=0
3910	117.633062	10.2.8.101	8.208.10.147	HTTP	239 GET /6lhjgfdghj.exe HTTP/1.1
3908	117.631299	10.2.8.101	8.208.10.147	TCP	54 49757 → 80 [ACK] Seq=360 Ack=2282 Win=65535 Len=0
3906	117.631213	8.208.10.147	10.2.8.101	HTTP	1213 HTTP/1.1 200 OK
3885	117.418712	8.208.10.147	10.2.8.101	TCP	54 80 → 49757 [ACK] Seq=1123 Ack=360 Win=64240 Len=0
3884	117.418595	10.2.8.101	8.208.10.147	HTTP	234 GET /0801s.bin HTTP/1.1
3883	117.401345	10.2.8.101	8.208.10.147	TCP	54 49757 → 80 [ACK] Seq=180 Ack=1123 Win=65535 Len=0
3882	117.401219	8.208.10.147	10.2.8.101	HTTP	1176 HTTP/1.1 200 OK
3881	117.197787	8.208.10.147	10.2.8.101	TCP	54 80 → 49757 [ACK] Seq=1 Ack=180 Win=64240 Len=0
3880	117.197679	10.2.8.101	8.208.10.147	HTTP	233 GET /0801.bin HTTP/1.1
3879	117.197578	10.2.8.101	8.208.10.147	TCP	54 49757 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0

Malware Analysis

Computer Forensic

IOCs

Ficker Stealer Malware Indication

- File mencurigakan bernama 6lhjgfdghj.exe sebagai indikasi malware. Ficker Stealer yang berasal dari roanokemortgages.com (alamat IP: 8.208.10.147).

Source: <https://github.com/pan-unit42/iocs-Hancitor/blob/main/APPENDIX-D-Samples-of-Ficker-Stealer-Associated-With-Hancitor.txt>

- Indikasi lainnya adalah api.ipify.org di port 80.

pestudio 9.55 - Malware Initial Assessment - www.winitor.com - [c:\users\acer\downloads\6lhjgfdghj.exe]				
file settings about				
c:\users\acer\downloads\6lhjgfdghj.exe				
indicators (virustotal > score)	engine (72/72)	score (61/72)	date (dd.mm.yyyy)	age (days)
footprints (count > 12)	Bkav	W32.AIDetectMalware	09.12.2023	6
virustotal (61/72)	Lionic	Trojan.Win32.Zudochka.4lc	10.12.2023	5
dos-header (size > 64 bytes)	tehttris	clean	10.12.2023	5
dos-stub (size > 64 bytes)	MicroWorld-eScan	Gen:Variant.Doina.10823	10.12.2023	5
rich-header (n/a)	CMC	clean	22.08.2023	115
file-header (executable > 32-bit)	CAT-QuickHeal	Trojan.Ficker.S21872906	09.12.2023	6
optional-header (subsystem > GUI)	Skyhigh	BehavesLike.Win32.Generic.dh	10.12.2023	5
directories (count > 3)	McAfee	GenericRXNQ-MSI778E0DD65703	10.12.2023	5
sections (flag > name)				
libraries (flag > 2) *	Malwarebytes	Malware.AI.2072518380	10.12.2023	5
imports (flag > 120) *	VIPRE	Gen:Variant.Doina.10823	09.12.2023	6
exports (n/a)	Sangfor	Trojan.Win32.Save.a	22.11.2023	23
thread-local-storage (count > 3)	KTAntiVirus	Trojan ( 0001555e1 )	04.12.2023	11
.NET (n/a)	Alibaba	TrojanDownloader.Win32/Stealer.12c8f4a0	27.05.2019	1663
resources (n/a)	KTGW	Trojan ( 0001555e1 )	04.12.2023	11
strings (count > 4694)	Cybereason	malicious.d8cfc0	02.11.2023	43
debug (n/a)	Arcabit	Trojan.Doina.D2A47	10.12.2023	5
manifest (n/a)	Baidu	clean	18.03.2019	1733
version (n/a)	VirIT	Trojan.Win32.PWSStealer.CSDD	07.12.2023	8
certificate (n/a)	Symantec	ML.Attribute.HighConfidence	09.12.2023	6
overlay (signature > unknown)	Elastic	Windows.Trojan.Fickerstealer	08.12.2023	7
	ESET-NOD32	a variant of Win32/Agent.UKB	09.12.2023	6
	Cynet	Malicious (score: 100)	10.12.2023	5
	APEX	clean	28.11.2023	17
	Paloalto	clean	10.12.2023	5

2021-02-08-traffic-analysis-exercise.pcap									
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help									
[Apply a display filter ... <Ctrl-/>]									
No.	Time	Source	Destination	Protocol	Length	Info			
3890	117.520365	198.211.10.238	10.2.8.101	TCP	54	8080 → 49758 [ACK] Seq=1 Ack=191 Win=64240 Len=0			
3891	117.598420	198.211.10.238	10.2.8.101	TCP	173	8080 → 49758 [PSH, ACK] Seq=1 Ack=191 Win=64240 Len=119 [TCP segment of a reassembled PDU]			
3892	117.598562	10.2.8.101	198.211.10.238	TCP	54	49758 → 8080 [ACK] Seq=191 Ack=120 Win=65535 Len=0			
3893	117.601615	198.211.10.238	10.2.8.101	TCP	1442	8080 → 49758 [PSH, ACK] Seq=120 Ack=191 Win=64240 Len=1388 [TCP segment of a reassembled PDU]			
3894	117.601737	10.2.8.101	198.211.10.238	TCP	54	49758 → 8080 [ACK] Seq=191 Ack=1508 Win=65535 Len=0			
3895	117.604788	198.211.10.238	10.2.8.101	TCP	1442	8080 → 49758 [PSH, ACK] Seq=1508 Ack=191 Win=64240 Len=1388 [TCP segment of a reassembled PDU]			
3896	117.604883	10.2.8.101	198.211.10.238	TCP	54	49758 → 8080 [ACK] Seq=191 Ack=2896 Win=65535 Len=0			
3897	117.611378	198.211.10.238	10.2.8.101	TCP	1514	8080 → 49758 [ACK] Seq=2896 Ack=191 Win=64240 Len=1460 [TCP segment of a reassembled PDU]			
3898	117.611399	198.211.10.238	10.2.8.101	TCP	1514	8080 → 49758 [ACK] Seq=4356 Ack=191 Win=64240 Len=1460 [TCP segment of a reassembled PDU]			
3899	117.611412	198.211.10.238	10.2.8.101	TCP	1514	8080 → 49758 [ACK] Seq=5816 Ack=191 Win=64240 Len=1460 [TCP segment of a reassembled PDU]			
3900	117.611425	198.211.10.238	10.2.8.101	TCP	1226	8080 → 49758 [PSH, ACK] Seq=7276 Ack=191 Win=64240 Len=1172 [TCP segment of a reassembled PDU]			
3901	117.611488	10.2.8.101	198.211.10.238	TCP	54	49758 → 8080 [ACK] Seq=191 Ack=8448 Win=65535 Len=0			
3902	117.614534	198.211.10.238	10.2.8.101	TCP	1442	8080 → 49758 [PSH, ACK] Seq=8448 Ack=191 Win=64240 Len=1388 [TCP segment of a reassembled PDU]			
3903	117.614596	10.2.8.101	198.211.10.238	TCP	54	49758 → 8080 [ACK] Seq=191 Ack=9836 Win=65535 Len=0			
3904	117.617744	198.211.10.238	10.2.8.101	TCP	1442	8080 → 49758 [PSH, ACK] Seq=9836 Ack=191 Win=64240 Len=1388 [TCP segment of a reassembled PDU]			
3905	117.617805	10.2.8.101	198.211.10.238	TCP	54	49758 → 8080 [ACK] Seq=191 Ack=11224 Win=65535 Len=0			
3906	117.631213	8.208.10.147	10.2.8.101	HTTP	1213	HTTP/1.1 200 OK			
3907	117.631252	198.211.10.238	10.2.8.101	TCP	830	8080 → 49758 [PSH, ACK] Seq=11224 Ack=191 Win=64240 Len=776 [TCP segment of a reassembled PDU]			
3908	117.631299	10.2.8.101	8.208.10.147	TCP	54	49757 → 80 [ACK] Seq=360 Ack=2282 Win=65535 Len=0			
3909	117.631365	10.2.8.101	198.211.10.238	TCP	54	49758 → 8080 [ACK] Seq=191 Ack=12000 Win=65535 Len=0			
3910	117.633062	10.2.8.101	8.208.10.147	HTTP	239	GET /6lhjgfdghj.exe HTTP/1.1			
3911	117.633163	8.208.10.147	10.2.8.101	TCP	54	80 → 49757 [ACK] Seq=2282 Ack=545 Win=64240 Len=0			
3912	117.639379	198.211.10.238	10.2.8.101	TCP	1442	8080 → 49758 [PSH, ACK] Seq=12000 Ack=191 Win=64240 Len=1388 [TCP segment of a reassembled PDU]			
3913	117.639515	10.2.8.101	198.211.10.238	TCP	54	49758 → 8080 [ACK] Seq=191 Ack=13388 Win=65535 Len=0			
3914	117.642431	198.211.10.238	10.2.8.101	TCP	1442	8080 → 49758 [PSH, ACK] Seq=13388 Ack=191 Win=64240 Len=1388 [TCP segment of a reassembled PDU]			
3915	117.642519	10.2.8.101	198.211.10.238	TCP	54	49758 → 8080 [ACK] Seq=191 Ack=14776 Win=65535 Len=0			
3916	117.651480	198.211.10.238	10.2.8.101	TCP	1514	8080 → 49758 [ACK] Seq=14776 Ack=191 Win=64240 Len=1460 [TCP segment of a reassembled PDU]			
Frame 3889: 244 bytes on wire (1952 bits), 244 bytes captured (1952 bits)									
Ethernet II, Src: HewlettP_41:c2:aa (08:12:79:41:c2:aa), Dst: Cisco_12:84:76 (f0:29:29:12:84:76)									
Internet Protocol Version 4, Src: 10.2.8.101, Dst: 198.211.10.238									
Transmission Control Protocol, Src Port: 49758, Dst Port: 8080, Seq: 1, Ack: 1, Len: 190									
Hypertext Transfer Protocol									

Wireshark · Export · HTTP object list				
Text Filter:				
Packet	Hostname	Content Type	Size	Filename
1954	store-images.s-microsoft.com	image/jpeg	18 kB	apps.29799.14582624973508592.20000000000007863648.c6853463-3ddd-4434-ba48-0
1956	store-images.s-microsoft.com	image/jpeg	18 kB	apps.17382.13981634997965175.20000000000007770843.559fa263-3e4f-45fa-b25a-4e7
1992	store-images.s-microsoft.com	image/png	69 kB	apps.27279.13589262686196899.44b29135-f781-4fb7-a3ae-4a3a5d9e39a8.2ed808d9-f77
2080	store-images.s-microsoft.com	image/jpeg	17 kB	apps.23943.13510798883386282.e6f02eb7-a760-453e-8d79-46d4ec74807e.84e78792-8
2096	store-images.s-microsoft.com	image/jpeg	55 kB	global.40455.acentoprodimg.7f4d57e5-c726-4f64-a1a7-2358c9c2aca4.dc6cc2ed-6332-45
2156	store-images.s-microsoft.com	image/jpeg	17 kB	apps.52926.9007199266325098.312a56ec-4eaf-43b5-a24d-7ff0e5d534d7.bea01fd3-9bcd
2157	store-images.s-microsoft.com	image/jpeg	16 kB	apps.51239.14410076060135429.789f7faf-f4d8-407c-9f5d-fcd1a0a41a33.b300690e-4bcd
2160	store-images.s-microsoft.com	image/jpeg	18 kB	apps.19011.13634281287263458.47a0870a-4a2d-4201-a82e-f693a81e27cd.c97defd7-0dc
2201	store-images.s-microsoft.com	image/png	5,832 bytes	apps.48651.13798539581762600.1116729b-da89-42ce-8cdf-af5ad6cea556.8e69209f-f462
2288	store-images.s-microsoft.com	image/png	15 kB	apps.34347.14255546098955437.1f9875f0-cd7b-4be0-b3ec-c36b31ef0393.4bf90507-92
2293	store-images.s-microsoft.com	image/png	30 kB	apps.61877.14618985536919905.dee6fc2f-7908-497d-8aa7-395befb36297.2886ed4b-fe3
2296	store-images.s-microsoft.com	image/png	35 kB	apps.40518.14127333176902609.7be7b901-15fe-4c27-863c-7cd0bfc26c5c.5c278f58-912b
2297	store-images.s-microsoft.com	image/png	4,913 bytes	apps.56161.9007199266246365.1d5a6a53-3c49-4f80-95d7-78d76b0a05d0.a3e87fea-e03
2298	store-images.s-microsoft.com	image/png	5,238 bytes	apps.60605.13571498826857201.8c63370c-76c5-4094-99e7-988e9e5434a7.954f1f5b-26
2324	tonmatdoanminh.com	text/html	754 bytes	uninviting.php
2993	tonmatdoanminh.com	text/html	1,097 kB	uninviting.php
3817	api.ipify.org	text/plain	13 bytes	/
3828	satursed.com	application/x-www-form-urlencoded	158 bytes	forum.php
3830	satursed.com	text/html	176 bytes	forum.php
3882	roanokemortgages.com	application/octet-stream	876 bytes	0801.bin
3906	roanokemortgages.com	application/octet-stream	913 bytes	0801s.bin
4139	198.211.10.238:8080	application/octet-stream	208 kB	6Aov
4500	roanokemortgages.com	application/octet-stream	273 kB	6lhjgfdghj.exe
4702	api.ipify.org	text/plain	13 bytes	?format=xml
4740			4 bytes	
4746			15 bytes	
4750			715 bytes	
4751			692 bytes	
4755			323 bytes	
4756			1,389 bytes	
4757			384 bytes	
4771			17 bytes	
4784			2 bytes	
4793			1,460 bytes	
4797			1,460 bytes	
4821			1,460 bytes	
4828			1,460 bytes	
4834			1,460 bytes	
4840			1,460 bytes	
4841			1,460 bytes	

Malware Analysis



IOCs

Ficker Stealer Malware Indication

- IP Address 185.100.65.29 menandakan efek dari serangan malware ficker stealer.

4725	122.032353	52.114.132.23	10.2.8.101	TCP	54 443 → 49696	[ACK] Seq=7183 Ack=5428 Win=64239 Len=0
4726	122.133933	52.114.132.23	10.2.8.101	TCP	54 443 → 49696	[FIN, PSH, ACK] Seq=7183 Ack=5428 Win=64239 Len=0
4727	122.134050	10.2.8.101	52.114.132.23	TCP	54 49696 → 443	[ACK] Seq=5428 Ack=7184 Win=65535 Len=0
4729	122.216783	10.2.8.101	185.100.65.29	TCP	66 49763 → 80	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
4730	122.605881	185.100.65.29	10.2.8.101	TCP	58 80 → 49763	[SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
4731	122.606013	10.2.8.101	185.100.65.29	TCP	54 49763 → 80	[ACK] Seq=1 Ack=1 Win=64240 Len=0
4735	122.952881	185.100.65.29	10.2.8.101	TCP	95 80 → 49763	[PSH, ACK] Seq=1 Ack=1 Win=64240 Len=41
4736	122.953080	10.2.8.101	185.100.65.29	TCP	62 49763 → 80	[PSH, ACK] Seq=1 Ack=42 Win=64199 Len=8
4737	122.953132	10.2.8.101	185.100.65.29	TCP	67 49763 → 80	[PSH, ACK] Seq=9 Ack=42 Win=64199 Len=13
4738	122.953164	10.2.8.101	185.100.65.29	TCP	68 49763 → 80	[PSH, ACK] Seq=22 Ack=42 Win=64199 Len=14 [TCP segment of a reassembled PDU]
4739	122.953173	185.100.65.29	10.2.8.101	TCP	54 80 → 49763	[ACK] Seq=42 Ack=9 Win=64240 Len=0
4740	122.953204	10.2.8.101	185.100.65.29	TCP	65 49763 → 80	[PSH, ACK] Seq=36 Ack=42 Win=64199 Len=11
4741	122.953218	185.100.65.29	10.2.8.101	TCP	54 80 → 49763	[ACK] Seq=42 Ack=22 Win=64240 Len=0
4742	122.953238	10.2.8.101	185.100.65.29	TCP	65 49763 → 80	[PSH, ACK] Seq=47 Ack=42 Win=64199 Len=11 [TCP segment of a reassembled PDU]
4743	122.953253	185.100.65.29	10.2.8.101	TCP	54 80 → 49763	[ACK] Seq=42 Ack=36 Win=64240 Len=0
4744	122.953286	185.100.65.29	10.2.8.101	TCP	54 80 → 49763	[ACK] Seq=42 Ack=47 Win=64240 Len=0
4745	122.953320	185.100.65.29	10.2.8.101	TCP	54 80 → 49763	[ACK] Seq=42 Ack=58 Win=64240 Len=0
4746	122.953324	10.2.8.101	185.100.65.29	TCP	76 49763 → 80	[PSH, ACK] Seq=58 Ack=42 Win=64199 Len=22
4747	122.953349	185.100.65.29	10.2.8.101	TCP	54 80 → 49763	[ACK] Seq=42 Ack=80 Win=64240 Len=0
4748	122.953379	10.2.8.101	185.100.65.29	TCP	77 49763 → 80	[PSH, ACK] Seq=80 Ack=42 Win=64199 Len=23 [TCP segment of a reassembled PDU]
4749	122.953406	185.100.65.29	10.2.8.101	TCP	54 80 → 49763	[ACK] Seq=42 Ack=103 Win=64240 Len=0
4750	123.168662	10.2.8.101	185.100.65.29	TCP	746 49763 → 80	[PSH, ACK] Seq=103 Ack=42 Win=64199 Len=692
4751	123.168712	10.2.8.101	185.100.65.29	TCP	746 49763 → 80	[PSH, ACK] Seq=795 Ack=42 Win=64199 Len=692
4752	123.168811	185.100.65.29	10.2.8.101	TCP	54 80 → 49763	[ACK] Seq=42 Ack=795 Win=64240 Len=0
4753	123.168864	185.100.65.29	10.2.8.101	TCP	54 80 → 49763	[ACK] Seq=42 Ack=1487 Win=64240 Len=0
4754	123.173040	10.2.8.101	185.100.65.29	TCP	1514 49763 → 80	[ACK] Seq=1487 Ack=42 Win=64199 Len=1460
4755	123.173052	10.2.8.101	185.100.65.29	TCP	493 49763 → 80	[PSH, ACK] Seq=2947 Ack=42 Win=64199 Len=439

**THANK YOU**