# MALWARE ANALYSIS

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

Malware Analysis

Start Slide

# Malware Analysis

## Link

## Malware

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

# Malware Analysis

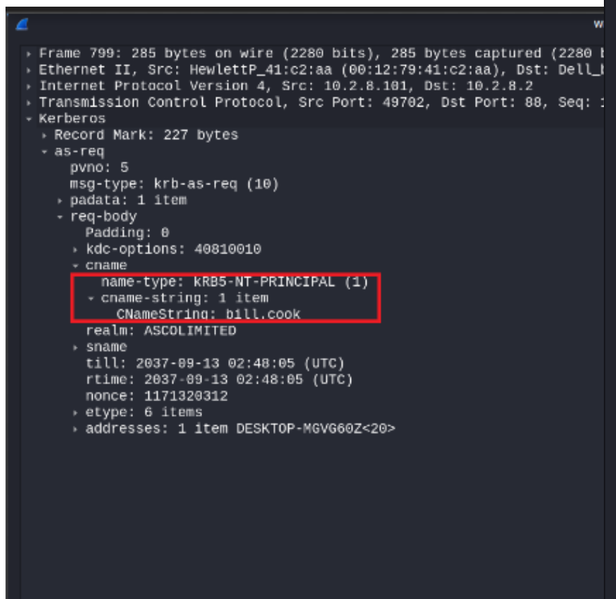
## Executive Summary

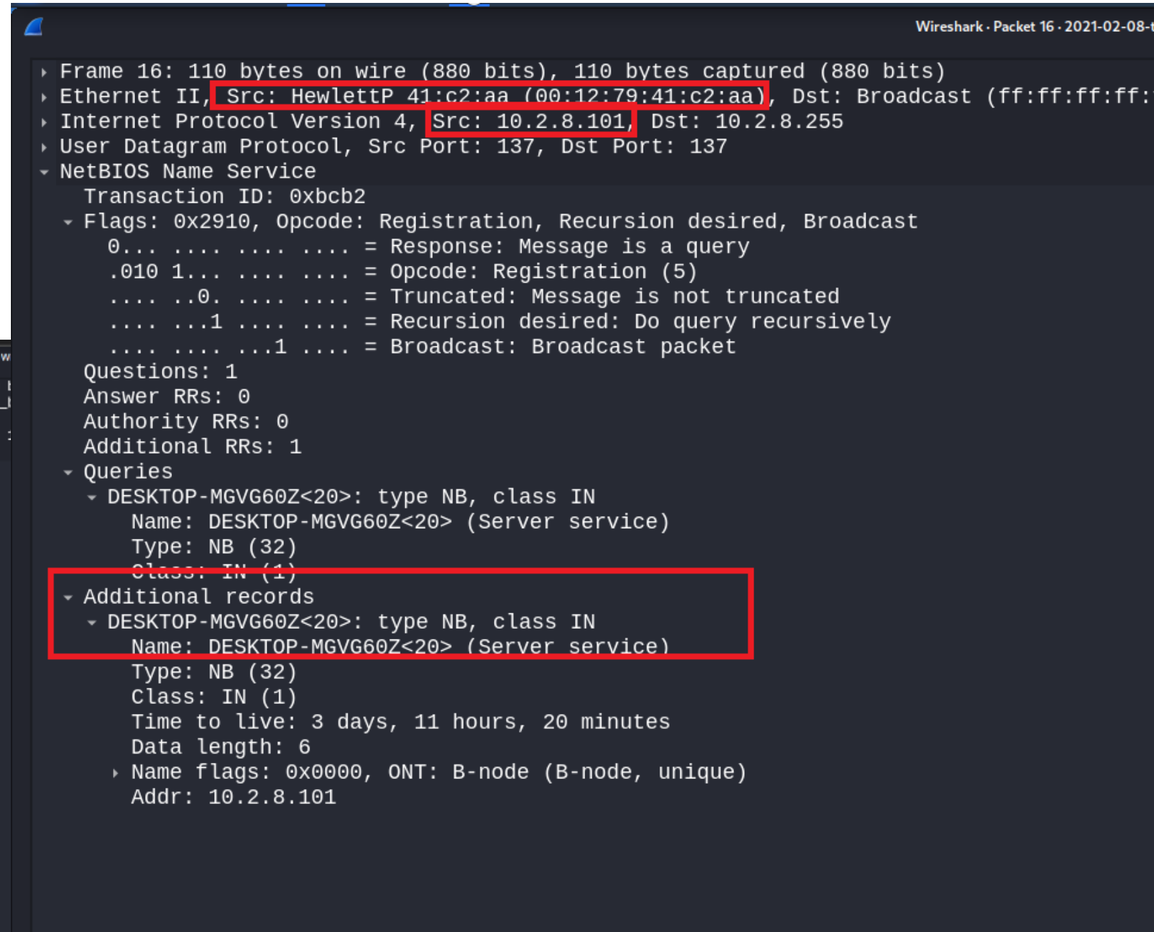
Pada tanggal 8 Februari 2021, Windows DESKTOP-MGVG60Z milik Bill Cook terinfeksi oleh tiga malware, yaitu Hancitor, Cobalt Strike, dan Ficker Stealer Malware.

# 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.

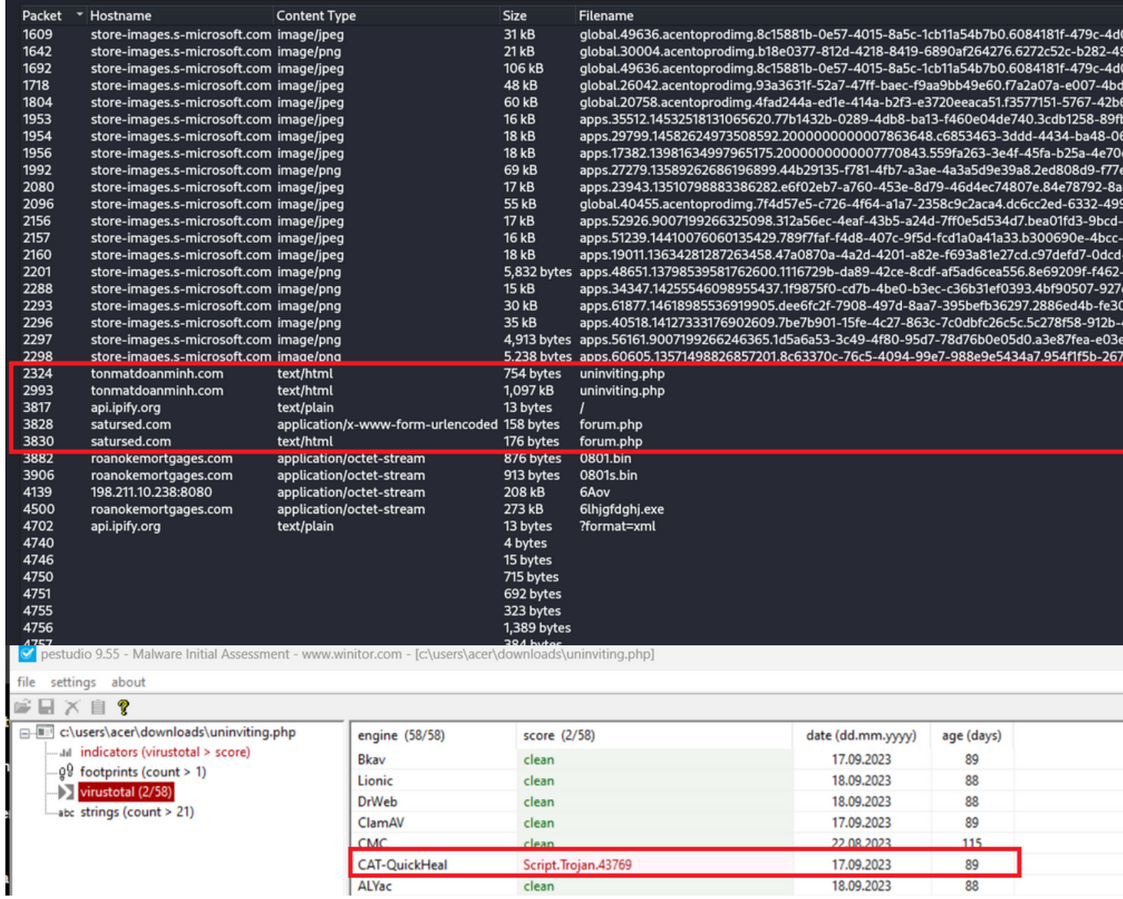


# IOCs

## 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 satursed.com (alamat IP: 213.5.229.12) dan api.ipify.org (berjalan di port 80).



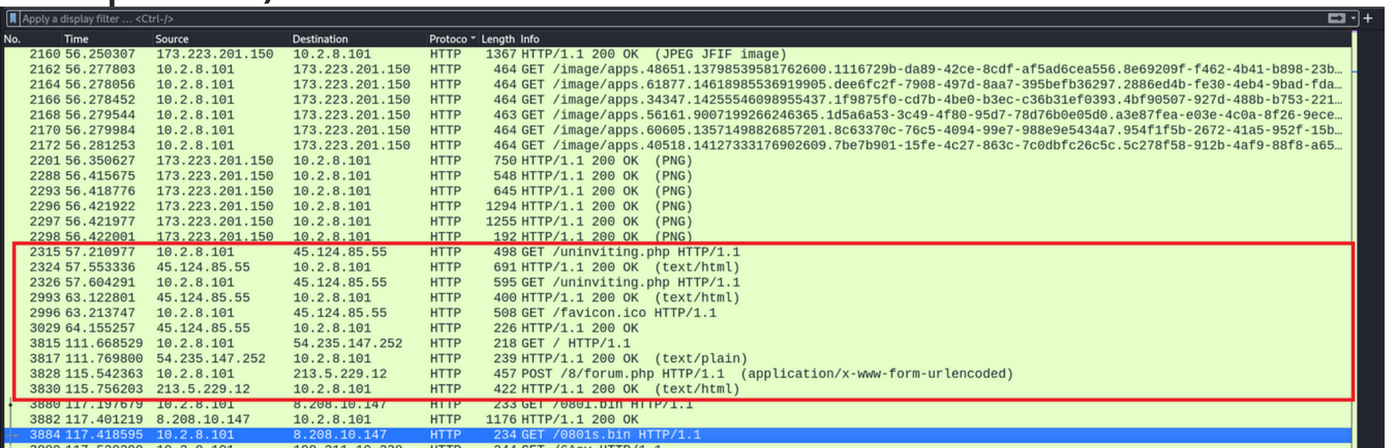
| Packet | Hostname | Content Type | Size | Filename |
|---|---|---|---|---|
| 1609 | store-images.s-microsoft.com | image/jpeg | 31 kB | global.49636.acentoprodimg.8c15881b-0e57-4015-8a5c-1cb11a54b7b0.6084181f-479c-4d |
| 1642 | store-images.s-microsoft.com | image/png | 21 kB | global.30004.acentoprodimg.b18e0377-812d-4218-8419-6890af264276.6272c52c-b282-4 |
| 1692 | store-images.s-microsoft.com | image/jpeg | 106 kB | global.49636.acentoprodimg.8c15881b-0e57-4015-8a5c-1cb11a54b7b0.6084181f-479c-4d |
| 1718 | store-images.s-microsoft.com | image/jpeg | 48 kB | global.26042.acentoprodimg.93a3631f-52a7-47ff-baec-f9aa9bb49e60.f7a2a07a-e007-4bd |
| 1804 | store-images.s-microsoft.com | image/jpeg | 60 kB | global.20758.acentoprodimg.4fad244a-ed1e-414a-b2f3-e3720eeaca51.f3577151-5767-42b6 |
| 1953 | store-images.s-microsoft.com | image/jpeg | 16 kB | apps.35512.14532518131065620.77b1432b-0289-4db8-ba13-f460e04de740.3cdb1258-89f |
| 1954 | store-images.s-microsoft.com | image/jpeg | 18 kB | apps.29799.14582624973508592.2000000000007863648.c6853463-3ddd-4434-ba48-0 |
| 1956 | store-images.s-microsoft.com | image/jpeg | 18 kB | apps.17382.13981634997965175.2000000000007770843.559fa263-3e4f-45fa-b25a-4e70 |
| 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.84e78792-8a |
| 2096 | store-images.s-microsoft.com | image/jpeg | 55 kB | global.40455.acentoprodimg.7f4d57e5-c726-4f64-a1a7-2358c9c2aca4.dc6cc2ed-6332-495 |
| 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-4bcc |
| 2160 | store-images.s-microsoft.com | image/jpeg | 18 kB | apps.19011.13634281287263458.47a0870a-4a2d-4201-a82e-f693a81e27cd.c97defd7-0dcd |
| 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-c36b31ef0393.4bf90507-927 |
| 2293 | store-images.s-microsoft.com | image/png | 30 kB | apps.61877.14618985536919905.dee6fc2f-7908-497d-8aa7-395befb36297.2886ed4b-fe30 |
| 2296 | store-images.s-microsoft.com | image/png | 35 kB | apps.40518.14127333176902609.7be7b901-15fe-4c27-863c-7c0dbfc26c5c.5c278f58-912b |
| 2297 | store-images.s-microsoft.com | image/png | 4,913 bytes | apps.56161.9007199266246365.1d5a6a53-3c49-4f80-95d7-78d76b0e05d0.a3e87fea-e03e |
| 2298 | store-images.s-microsoft.com | image/png | 5,238 bytes | apps.60605.13571498826857201.8c63370c-76c5-4094-99e7-988e9e5434a7.954f1f5b-267 |
| 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 | |

pestudio 9.55 - Malware Initial Assessment - www.winitor.com - [c:\users\acer\downloads\uninviting.php]

file settings about

c:\users\acer\downloads\uninviting.php
- indicators (virustotal > score)
- footprints (count > 1)
- virustotal (2/58)
- strings (count > 21)

| engine (58/58) | score (2/58) | date (dd.mm.yyyy) | age (days) |
|---|---|---|---|
| Bkav | clean | 17.09.2023 | 89 |
| Lionic | clean | 18.09.2023 | 88 |
| DrWeb | clean | 18.09.2023 | 88 |
| ClamAV | clean | 17.09.2023 | 89 |
| CMC | clean | 22.08.2023 | 115 |
| CAT-QuickHeal | Script.Trojan.43769 | 17.09.2023 | 89 |
| ALYac | clean | 18.09.2023 | 88 |



Apply a display filter ... <Ctrl-/>

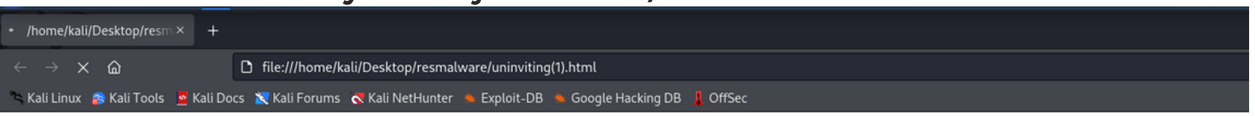
| No. | Time | Source | Destination | Protoco | Length | Info |
|---|---|---|---|---|---|---|
| 2160 | 56.250307 | 173.223.201.150 | 10.2.8.101 | HTTP | 1367 | HTTP/1.1 200 OK (JPEG JFIF image) |
| 2162 | 56.277803 | 10.2.8.101 | 173.223.201.150 | HTTP | 464 | GET /image/apps.48651.13798539581762600.1116729b-da89-42ce-8cdf-af5ad6cea556.8e69209f-f462-4b41-b898-23b… |
| 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 /8/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 /0801.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 |

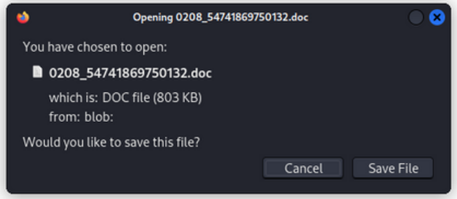
**Malware Analysis**

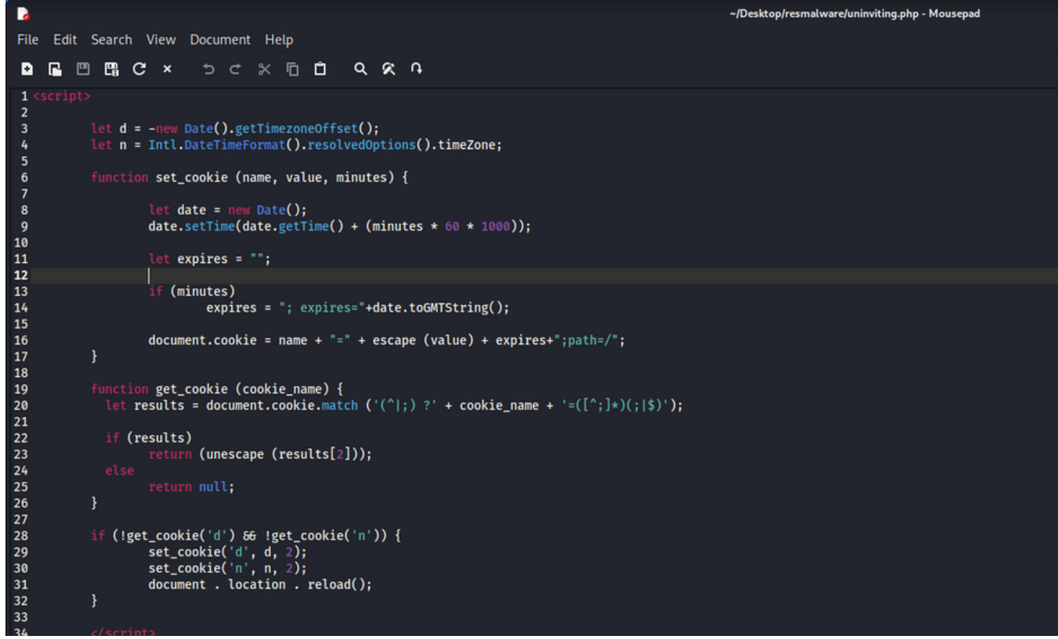
# IOCs

## Hancitor Malware Indication

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



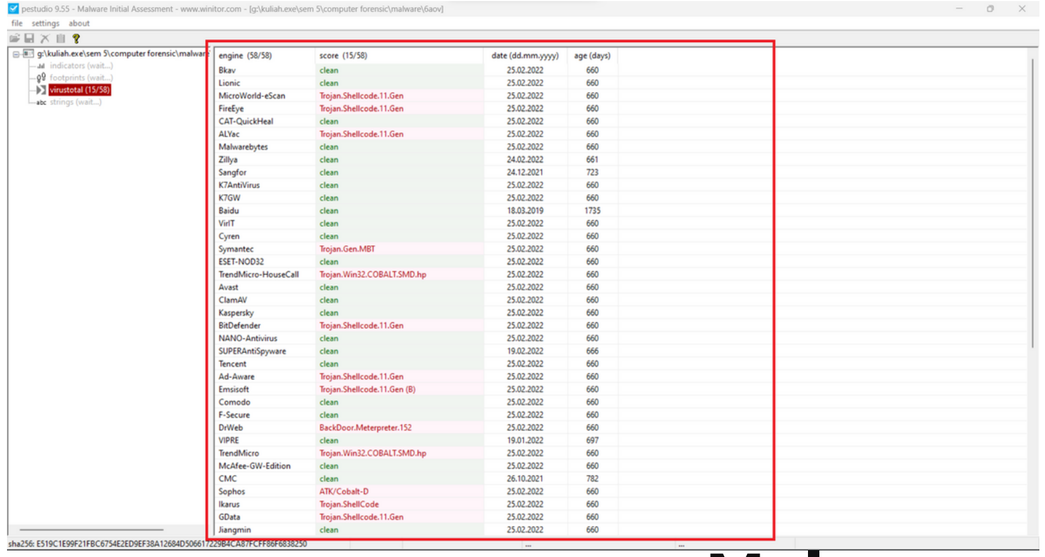

**Malware Analysis**

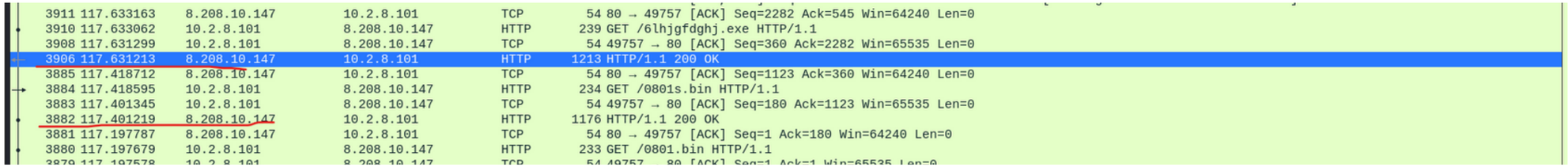
| | | | | |
|---|---|---|---|---|
| 2993 | tonmatdoanminh.com | text/html | 1,097 kB | uninviting.php |
| 3817 | api.ipify.org | text/plain | 13 bytes | / |
| 3828 | satursed.com | application/x-www-form-urlencoded | 158 bytes | forum.php |
| 3830 | satursed.com | text/html | 176 bytes | forum.php |
| 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 | |

# IOCs

## Cobalt Strike Malware Indication

- Terdapat file mencurigakan 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.




# Malware Analysis

## Computer Forensic

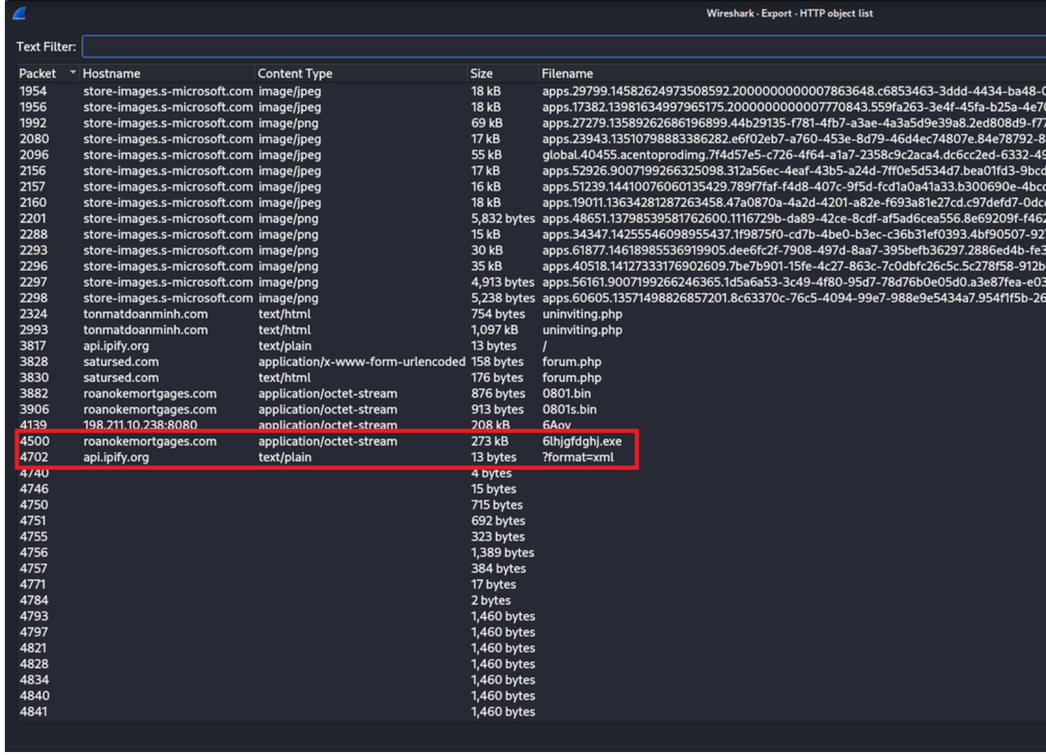
# IOCs

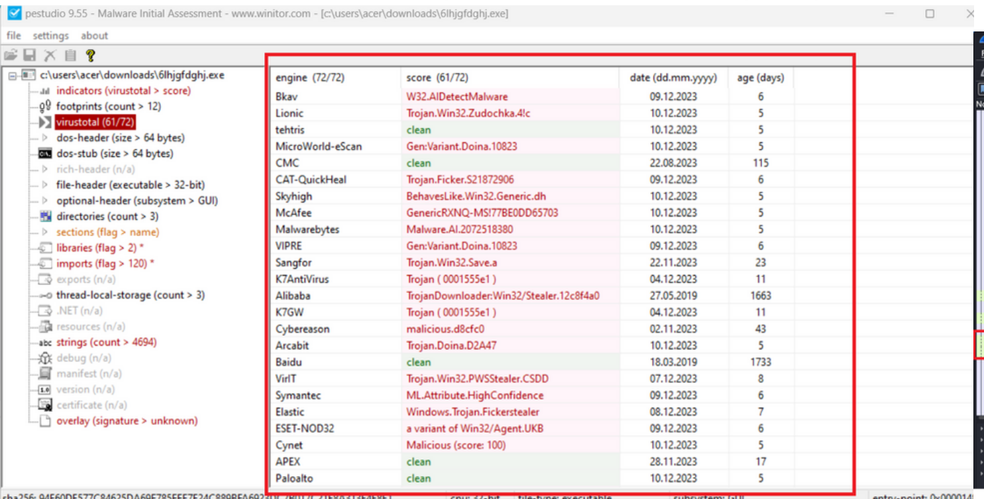
## Ficker Stealer Malware Indication

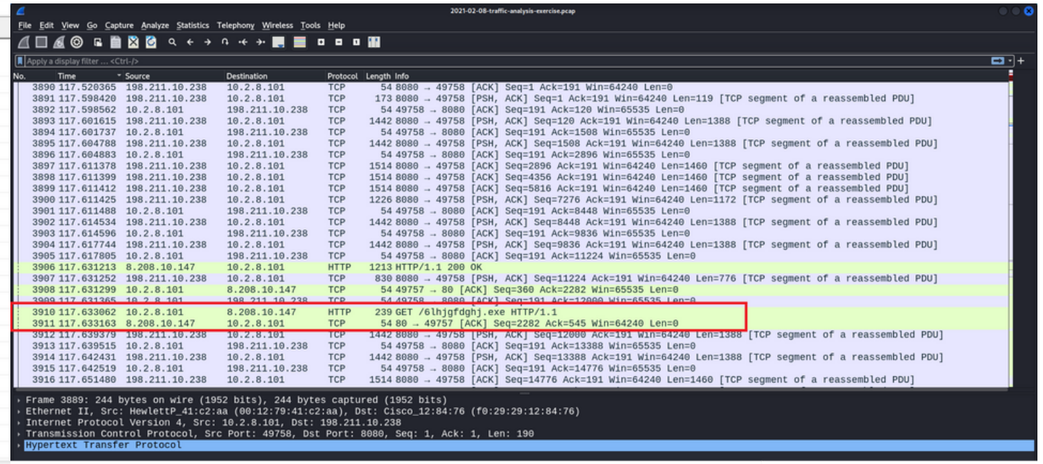
- File mencurigakan bernama 6lhjgfdghj.exe sebagai indikasi malware. Ficker Stealer yang berasal dari roanokemortgages.com (alamat IP: 8.208.10.147).

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.




# 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