NETWORK TRAFFIC ANALYSIS - Task 3

David Muhaimin

PT. AEROSYNTH
2025-06-01

ENVIRONMENT:

- LAN segment range: 172.17.0.0/24
- Domain: bepositive.com
- AD environment name: BEPOSITIVE
- Domain Controller: 172.17.0.17 - win-ctl9xbq9y19.bepositive.com
- LAN segment gateway: 172.17.0.1
- LAN segment broadcast address: 172.17.0.255

BACKGROUD:

Pada awal bulan September 2024, tim IT PT AEROSYNTH menerima alert dari sistem pemantauan jaringan internal yang menunjukkan adanya trafik mencurigakan dari salah satu endpoint di segmen LAN 172.17.0.0/24. Setelah dilakukan capture terhadap lalu lintas menggunakan Wireshark, ditemukan adanya komunikasi abnormal dari sebuah workstation yang diduga merupakan gejala awal infeksi malware. Analisis lebih lanjut dilakukan untuk memastikan jenis ancaman serta korban yang terdampak.

RealTime Events | Escalated Events

ST	CNT	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	2024-09-04 ...	172.17.0.99	59123	172.17.0.17	53	17	ET POLICY Reserved Internal IP Traffic
RT	1	2024-09-04 ...	172.17.0.17	53	172.17.0.99	59123	17	ET POLICY Reserved Internal IP Traffic
RT	25	2024-09-04 ...	172.17.0.17	53	172.17.0.99	62363	17	ET DNS Standard query response, Name Error
RT	3	2024-09-04 ...	172.17.0.99	49766	23.220.251.149	80	6	ET INFO Terse Request for .txt - Likely Hostile
RT	2	2024-09-04 ...	172.17.0.99	49766	23.220.251.149	80	6	ET INFO Microsoft Connection Test
RT	1	2024-09-04 ...	172.17.0.99	49769	172.17.0.17	139	6	ET INFO Potentially unsafe SMBv1 protocol in use
RT	10	2024-09-04 ...	172.17.0.99	49769	172.17.0.17	139	6	GPL NETBIOS SMB Session Setup NTMLSSP unicode asn1 overflow attempt
RT	5	2024-09-04 ...	172.17.0.99	49769	172.17.0.17	139	6	GPL NETBIOS SMB IPC$ unicode share access
RT	10	2024-09-04 ...	172.17.0.99	49769	172.17.0.17	139	6	GPL NETBIOS SMB SMB_COM_TRANSACTION Max Data Count of 0 DOS Attempt
RT	1	2024-09-04 ...	172.17.0.99	49774	172.17.0.17	88	6	GPL RPC kerberos principal name overflow TCP
RT	50	2024-09-04 ...	172.17.0.99	49813	79.124.78.197	80	6	ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1
RT	48	2024-09-04 ...	172.17.0.99	49813	79.124.78.197	80	6	ETPRO TROJAN Win32/Koi Stealer CnC Checkin (POST) M2

TASK:

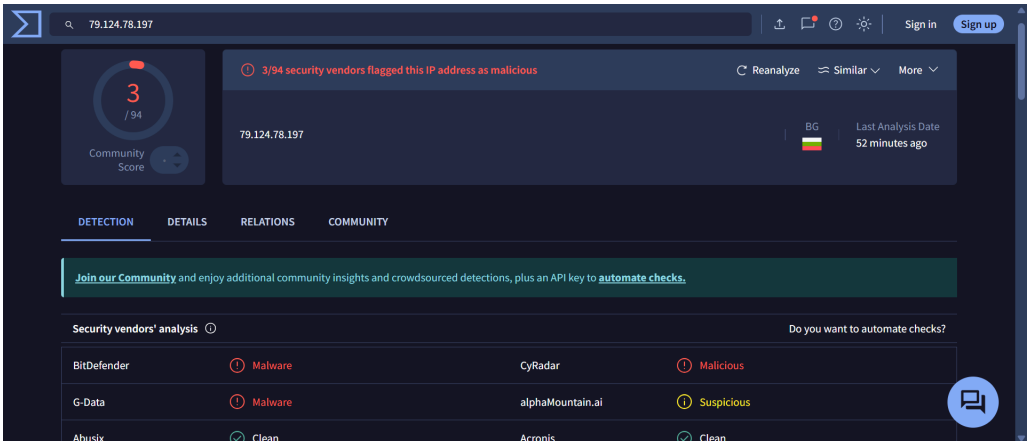
Melakukan investigasi terhadap file .pcap yang berisi lalu lintas jaringan, dengan tujuan:

- Mengidentifikasi korban dari aktivitas malware
- Menganalisis teknik komunikasi yang digunakan oleh malware
- Mendokumentasikan indikator kompromi (IoC) yang ditemukan

- Menyusun laporan insiden sebagai dokumentasi dan bahan mitigasi

EXECUTIVE SUMMARY :

Pada tanggal 4 September 2024, ditemukan indikasi infeksi malware Win32/Koi Stealer pada perangkat dengan hostname DESKTOP-RNVO9AT di jaringan internal PT AEROSYNTH. Perangkat tersebut melakukan koneksi HTTP POST ke IP luar jaringan menggunakan payload yang mencurigakan. Nama akun pengguna pada perangkat adalah afletcher, dan koneksi outbound dilakukan ke domain/IP asing yang mengindikasikan aktivitas pencurian data. Malware ini dikategorikan sebagai info-stealer, yang berpotensi mengirimkan kredensial dan data sensitif dari dalam perusahaan ke server penyerang.



VICTIM DETAILS:

- Hostname: DESKTOP-RNVO9AT
- IP Address: 172.17.0.99
- MAC Address: 18:3D:A2:B6:8D:C4
- User account name : afletcher
- Name of victim : Andrew Fletcher

INDICATOR OF COMPROMISE:

SRC IP : Port	DST IP : Prot	Alert
172.17.0.99:59440	172.17.0.17:53	Akses ke shared folder SMB dari klien terindikasi
172.17.0.99:49888	79.124.78.197:49888	Mengirim data ke server attacker

URL Generating the alert traffic:

172.17.0.99:49888 - 79.124.78.197:49888 - http://79.124.78.197/foots.php

172.17.0.99:49888 - 79.124.78.197:49888 - http://79.124.78.197/index.php?id=&subid=qIOuKk7U