

Malware Traffic Analysis



BUMBLEBEE INFECTION WITH COBALT STRIKE ANALYSIS



DATA DIRI ANGGOTA



2540120603
Nicolas Saputra Gunawan

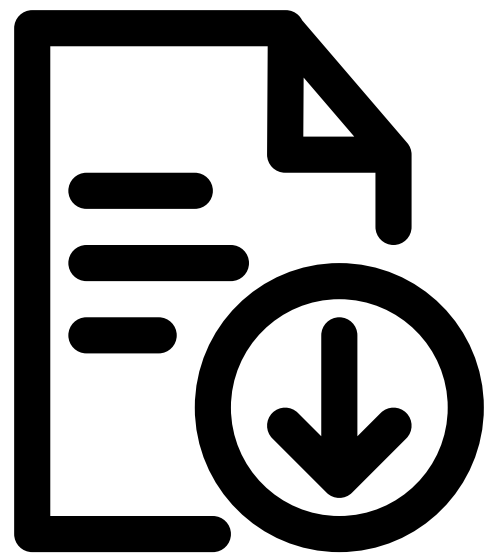
2540124620
Jeffrey Jingga

2540119633
Mikael Wiryamanta Wijaya

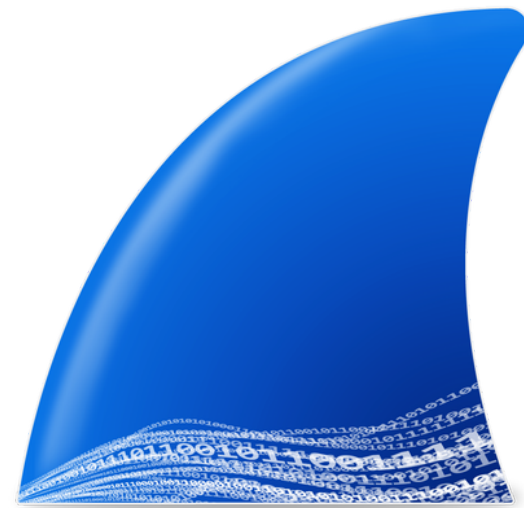
2540124740
Satya Kusuma

2540115181
Pitra Winarianto

Step By Step



Unduh *PCAP FILE*



Analisa *infection traffic* menggunakan *wireshark*



VirusTotal

Periksa
URL/hostname
dengan *VirusTotal*



Kesimpulan

Source [PCAP FILE]

2022-12-07 (WEDNESDAY) - BUMBLEBEE INFECTION WITH COBALT STRIKE

src : <https://www.malware-traffic-analysis.net/2022/12/07/index.html>

<https://www.malware-traffic-analysis.net/2022/12/07/index.html>

[Kali Forums](#) [Kali NetHunter](#) [Exploit-DB](#) [Google Hacking DB](#) [OffSec](#)

MALWARE-TRAFFIC-ANALYSIS.NET

2022-12-07 (WEDNESDAY) - BUMBLEBEE INFECTION WITH COBALT STRIKE

REFERENCE:

- https://twitter.com/Unit42_Intel/status/1600587285577203715

NOTES:

- Zip files are password-protected. If you don't know the password, see the "about" page of this website.

ASSOCIATED FILES:

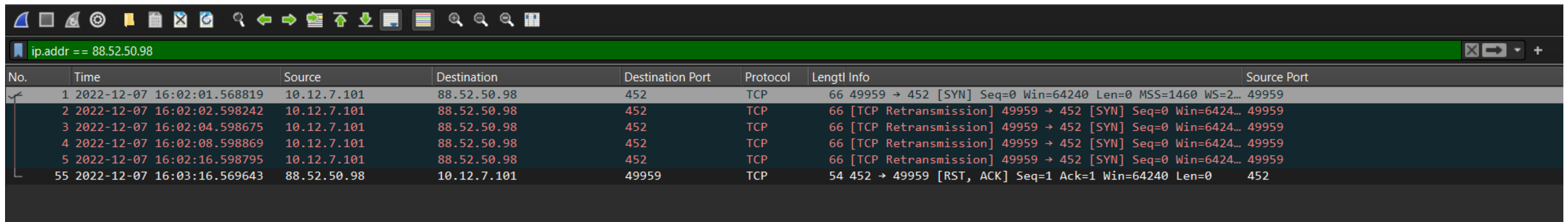
- [2022-12-07-IOCs-for-Bumblebee-infection-with-Cobalt-Strike.txt.zip](#) 1.8 kB (1,777 bytes)
- [2022-12-07-Bumblebee-infection-with-Cobalt-Strike.pcap.zip](#) 1.5 MB (1,535,190 bytes)
- [2022-12-07-Bumblebee-malware-and-artifacts.zip](#) 1.4 MB (1,436,871 bytes)

SOURCE

[Click here](#) to return to the main page.

Infection Traffic

88.52.50.98 port 452



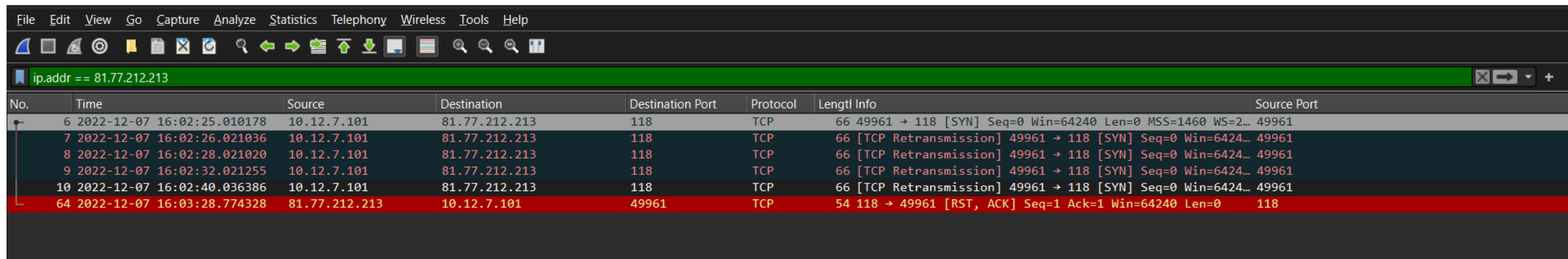
No.	Time	Source	Destination	Destination Port	Protocol	Length	Info	Source Port
1	2022-12-07 16:02:01.568819	10.12.7.101	88.52.50.98	452	TCP	66	49959 → 452 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=2...	49959
2	2022-12-07 16:02:02.598242	10.12.7.101	88.52.50.98	452	TCP	66	[TCP Retransmission] 49959 → 452 [SYN] Seq=0 Win=6424...	49959
3	2022-12-07 16:02:04.598675	10.12.7.101	88.52.50.98	452	TCP	66	[TCP Retransmission] 49959 → 452 [SYN] Seq=0 Win=6424...	49959
4	2022-12-07 16:02:08.598869	10.12.7.101	88.52.50.98	452	TCP	66	[TCP Retransmission] 49959 → 452 [SYN] Seq=0 Win=6424...	49959
5	2022-12-07 16:02:16.598795	10.12.7.101	88.52.50.98	452	TCP	66	[TCP Retransmission] 49959 → 452 [SYN] Seq=0 Win=6424...	49959
55	2022-12-07 16:03:16.569643	88.52.50.98	10.12.7.101	49959	TCP	54	452 → 49959 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0	452

Pada *packets* di atas, kami berspekulasi bahwa ip --> 10.12.7.101 merupakan ip *suspect*. Diketahui bahwa ip tersebut secara konsektif melakukan *request* TCP SYN. Tujuannya yaitu untuk membuka koneksi TCP dan memulai *3-way handshake*.

Diketahui pada paket ke 55, terdapat TCP [RST, ACK] pada *info section*. Hal ini mengindikasikan bahwa koneksi TCP ditutup akibat terdapat kesalahan dalam proses koneksi.

Infection Traffic

81.77.212.213 port 118



No.	Time	Source	Destination	Destination Port	Protocol	Length	Info	Source Port
6	2022-12-07 16:02:25.010178	10.12.7.101	81.77.212.213	118	TCP	66	49961 → 118 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=2...	49961
7	2022-12-07 16:02:26.021036	10.12.7.101	81.77.212.213	118	TCP	66	[TCP Retransmission] 49961 → 118 [SYN] Seq=0 Win=6424...	49961
8	2022-12-07 16:02:28.021020	10.12.7.101	81.77.212.213	118	TCP	66	[TCP Retransmission] 49961 → 118 [SYN] Seq=0 Win=6424...	49961
9	2022-12-07 16:02:32.021255	10.12.7.101	81.77.212.213	118	TCP	66	[TCP Retransmission] 49961 → 118 [SYN] Seq=0 Win=6424...	49961
10	2022-12-07 16:02:40.036386	10.12.7.101	81.77.212.213	118	TCP	66	[TCP Retransmission] 49961 → 118 [SYN] Seq=0 Win=6424...	49961
64	2022-12-07 16:03:28.774328	81.77.212.213	10.12.7.101	49961	TCP	54	118 → 49961 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0	118

Sama seperti sebelumnya, pada *packets* di atas, kami berspekulasi bahwa ip --> 10.12.7.101 merupakan ip *suspect*. Lalu, diketahui bahwa ip tersebut melakukan *request* TCP SYN berkali kali. Namun disini, terdapat perbedaan tujuan dari TCP SYN *scan* yang dilakukan.

Diketahui pada paket ke 64, terdapat TCP [RST, ACK] pada *info section*. Hal ini mengindikasikan bahwa koneksi TCP ditutup akibat terdapat kesalahan dalam proses koneksi.

Infection Traffic

139.177.146.137 port 443

4222	2022-12-07	16:53:50.003929	10.12.7.101	20.200.99.223	443 TLSv1...	clients.co...	Client Hello
4254	2022-12-07	16:54:03.612527	10.12.7.101	139.177.146.137	443 TLSv1...		Client Hello
4279	2022-12-07	16:54:37.560925	10.12.7.101	139.177.146.137	443 TLSv1...		Client Hello
4306	2022-12-07	16:54:55.591253	10.12.7.101	208.111.176.192	80 HTTP		GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?480734d00ec288a2 HTTP/1.1
4321	2022-12-07	16:55:09.202332	10.12.7.101	139.177.146.137	443 TLSv1...		Client Hello
4347	2022-12-07	16:55:38.751642	10.12.7.101	139.177.146.137	443 TLSv1...		Client Hello
4378	2022-12-07	16:56:05.939129	10.12.7.101	139.177.146.137	443 TLSv1...		Client Hello
4403	2022-12-07	16:56:38.880742	10.12.7.101	139.177.146.137	443 TLSv1...		Client Hello
4428	2022-12-07	16:57:11.564875	10.12.7.101	139.177.146.137	443 TLSv1...		Client Hello
4453	2022-12-07	16:57:40.095470	10.12.7.101	139.177.146.137	443 TLSv1...		Client Hello
4480	2022-12-07	16:57:59.287217	10.12.7.101	40.119.249.228	443 TLSv1...	settings-w...	Client Hello
4509	2022-12-07	16:58:08.976208	10.12.7.101	139.177.146.137	443 TLSv1...		Client Hello
4534	2022-12-07	16:58:12.811730	10.12.7.101	23.108.57.213	443 TLSv1...	ceyuvigi.c...	Client Hello
4607	2022-12-07	16:58:15.074770	10.12.7.101	23.108.57.213	443 TLSv1...	ceyuvigi.c...	Client Hello
4624	2022-12-07	16:58:20.627271	10.12.7.101	23.108.57.213	443 TLSv1...	ceyuvigi.c...	Client Hello
4641	2022-12-07	16:58:25.553306	10.12.7.101	23.108.57.213	443 TLSv1...	ceyuvigi.c...	Client Hello

Kami berspekulasi bahwa *packets* di atas merupakan *traffic* ke C2 Bumblebee. Pada *packets* di atas, diketahui *suspect* melakukan *request repetitive* ke C2 Bumblebee yang merupakan *salah satu ip yang digunakan untuk melakukan komunikasi*.

Infection Traffic

23.108.57.213 port 443

```
4400 2022-12-07 16:57:59.207217 10.12.7.101 40.119.249.220 443 TLSv1... settings-w... Client Hello
4509 2022-12-07 16:58:08.976208 10.12.7.101 139.177.146.137 443 TLSv1... Client Hello
4534 2022-12-07 16:58:12.811730 10.12.7.101 23.108.57.213 443 TLSv1... ceyuvigi.c... Client Hello
4607 2022-12-07 16:58:15.074770 10.12.7.101 23.108.57.213 443 TLSv1... ceyuvigi.c... Client Hello
4624 2022-12-07 16:58:20.627271 10.12.7.101 23.108.57.213 443 TLSv1... ceyuvigi.c... Client Hello
4641 2022-12-07 16:58:25.553396 10.12.7.101 23.108.57.213 443 TLSv1... ceyuvigi.c... Client Hello
4659 2022-12-07 16:58:30.137862 10.12.7.101 23.108.57.213 443 TLSv1... ceyuvigi.c... Client Hello
4718 2022-12-07 16:58:30.975787 10.12.7.101 23.108.57.213 443 TLSv1... ceyuvigi.c... Client Hello
4735 2022-12-07 16:58:38.225188 10.12.7.101 23.108.57.213 443 TLSv1... ceyuvigi.c... Client Hello
4772 2022-12-07 16:58:38.924498 10.12.7.101 23.108.57.213 443 TLSv1... ceyuvigi.c... Client Hello
4791 2022-12-07 16:58:40.933451 10.12.7.101 139.177.146.137 443 TLSv1... Client Hello
4814 2022-12-07 16:58:44.074861 10.12.7.101 23.108.57.213 443 TLSv1... ceyuvigi.c... Client Hello
4841 2022-12-07 16:58:52.124985 10.12.7.101 23.108.57.213 443 TLSv1... ceyuvigi.c... Client Hello
4939 2022-12-07 16:58:52.719906 10.12.7.101 23.108.57.213 443 TLSv1... ceyuvigi.c... Client Hello
4956 2022-12-07 16:58:57.196523 10.12.7.101 23.108.57.213 443 TLSv1... ceyuvigi.c... Client Hello
5478 2022-12-07 16:58:59.848961 10.12.7.101 23.108.57.213 443 TLSv1... ceyuvigi.c... Client Hello
5499 2022-12-07 16:59:00.603247 10.12.7.101 104.94.77.31 80 HTTP GET / HTTP/1.1
5500 2022-12-07 16:59:00.603504 10.12.7.101 23.108.57.213 443 TLSv1... ceyuvigi.c... Client Hello
```

Kami berspekulasi bahwa *packets* di atas merupakan *traffic* yang TLS yang dikirim dari *suspect* ke ip yang terdeteksi sebagai domain *ceyuvigi.com* yang merupakan ip malicious (*botnet server*) yang dibuat diatas *cobaltstrike* .

Virus Total

ceyuvigi.com | 23.108.57.213

9
/ 90

Community Score

9 security vendors flagged this URL as malicious

<http://ceyuvigi.com/>
ceyuvigi.com

Reanalyze

Search

Graph

API

Last Analysis Date
26 days ago

DETECTION

DETAILS

COMMUNITY

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

Crowdsourced context

HIGH 0

MEDIUM 1

LOW 0

INFO 0

SUCCESS 0

ThreatFox IOCs for 2022-12-08 - according to source ArcSight Threat Intelligence - 1 year ago

→ Cobalt Strike botnet C2 domain (confidence level: 100%)

Security vendors' analysis

Do you want to automate checks?

AlphaSOC	Malware	Avira	Malware
BitDefender	Malware	ESTsecurity	Malicious
Forcepoint ThreatSeeker	Malicious	Fortinet	Malware
G-Data	Malware	Seclookup	Malicious
Sophos	Malicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean

<http://ceyuvigi.com/> atau ceyuvigi.com merupakan botnet C2 dari Cobalt Strike dengan confidence level sebesar 100%

Kesimpulan

Berdasarkan hasil yang ditampilkan di virustotal.com, dapat disimpulkan bahwa benar terdapat indikasi serangan malware bumblebee. Pernyataan ini didukung dengan hostname DGA yang digunakan dan IP --> 23.108.57.213:443 yang digunakan tercatat di virustotal.com merupakan common host yang biasa digunakan oleh malware bumblebee.

THANK YOU!