2023

SECURITY REPORT

PCAP Analysis of Agent Tesla attack

github.com/Abdibimantara abdibimantara.github.io abdibimantara91@gmail.com

Daftar Isi

Executive Summary

Berdasarkan postingan resmi yang dibuat oleh tim Palo Alto Network Unit 42, Terdapat aktivitas anomaly yang terindikasi sebagai Aktivitas Agent-Tesla. Agent Tesla adalah salah satu malware yang termasuk kedalam remote access trojan (RAT) yang memiliki kemamampuan dalam pencurian serta penyusupan informasi sensitif dari device yang terinfeksi. Malware tersebut dapat mencuri berbagai jenis data, termasuk Keystrokes dan Kredential login yang digunakan di browser serta data email klien dari device terinfeksi. Berdasarkan dari proses identifikasi, Data yang berhasil dicuri mencakup informasi seperti sistem operasi, nama akun pengguna Windows, CPU, jumlah RAM, dan alamat IP publik dari device yang terinfeksi.

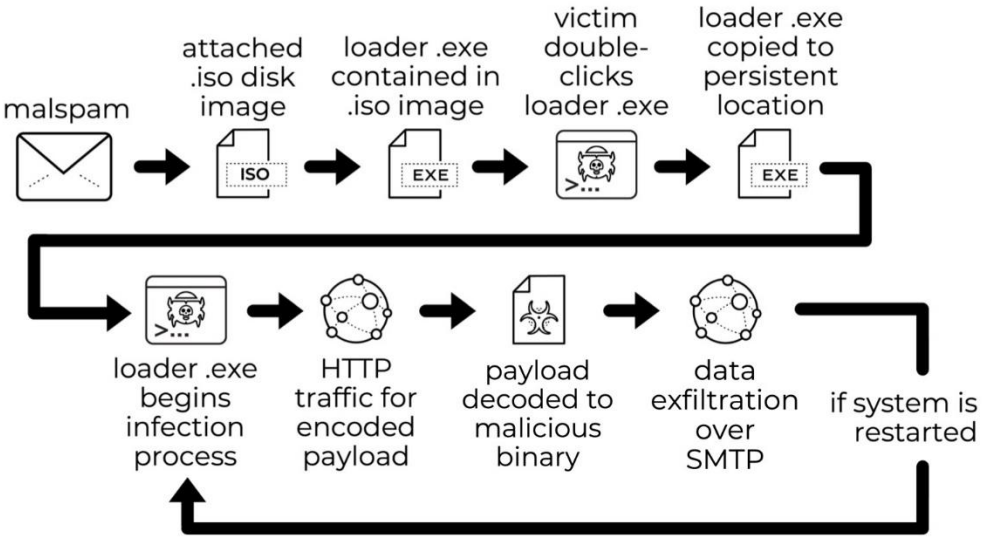
Latar Belakang

Pada awal tahun 2023, Palo Alto Network Unit 42 merilis portingan resmi meraka melalui twitter mengenai aktivitas Agent Tesla dari kemungkinan infeksi OriginLogger yang ditemukan pada hari kami 5 januari 2023. Berikut kami mendapati file pcap network traffic yang berisi aktivitas dari sample malware tersebut. aktivitas tersebut berupa Post-Infection yaitu traffic SMTP yang berisi data tidak terenkrispi berupa data yang dicuri dari komputer terinfkesi.

Alur Aktivitas Infeksi Agent-Tesla

Berdasarkan informasi resmi yang dikeluarkan oleh Palo Alto Network Unit 42, aktivitas Agent-Tesla dimulai dengan file yang bernama "Payment Copy_Chase Bank_pdf.iso". FIle tersebut menggunakan ektensi file iso yang dimana seletelah di esktrak akan memunculkan file baru dengan nama "Payment Copy_Chase Bank_pdf.exe", terdapat perbedaan file pertama

dengan kedua yaitu ekstensi file .iso dan .exe. Disini terlihat mencurigakan, dikarenakan file tersebut memiliki double ekstensi yaitu .pdf dan .exe. Program .exe tersebut akan dijalankan secara terus menerus melalui proses registri update. Setelah file .exe tersebut dijalankan, secara otomati device yang terinfeksi akan mencoba melakukan koneksi terhadap server attacker melalui payload decoded to malicious binary. setelah berhasil menjalin koneksi C2C, attacker dapat dengan mudah melalukan pencurian data atau biasa dikenal dengan "data exfiltration" melalui protokol SMTP.



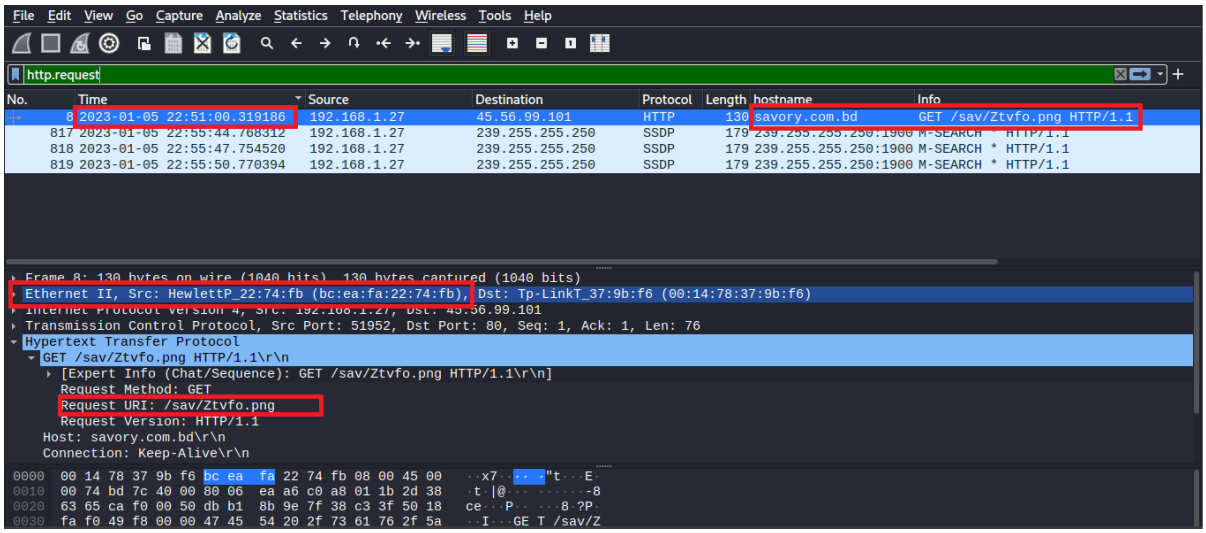
Requirements

Dalam melakukan proses analysis, kami menggunakan tools wireshark. Wireshark adalah salah satu tools yang biasa digunakan oleh para peneliti cybersecurity untuk menganalisa network traffic via pcap. Kami menyarankan untuk menggunakan versi terbaru dari wireishark dikarenakann dukungan fitur yang lebih banyak, disini kami menggunakan wireshark versi terbaru yaitu 4.0.1.

Selain itu disini kami merekomendasikan penggunaan sistem operasi non windows seperti BSD, Linux dan MacOS untuk menganalisa file tersebut. Hal ini untuk menghindari hal yang tidak di inginkan, walaupun file yang dianalisis hanya berisi network traffic dari aktivitas malware.

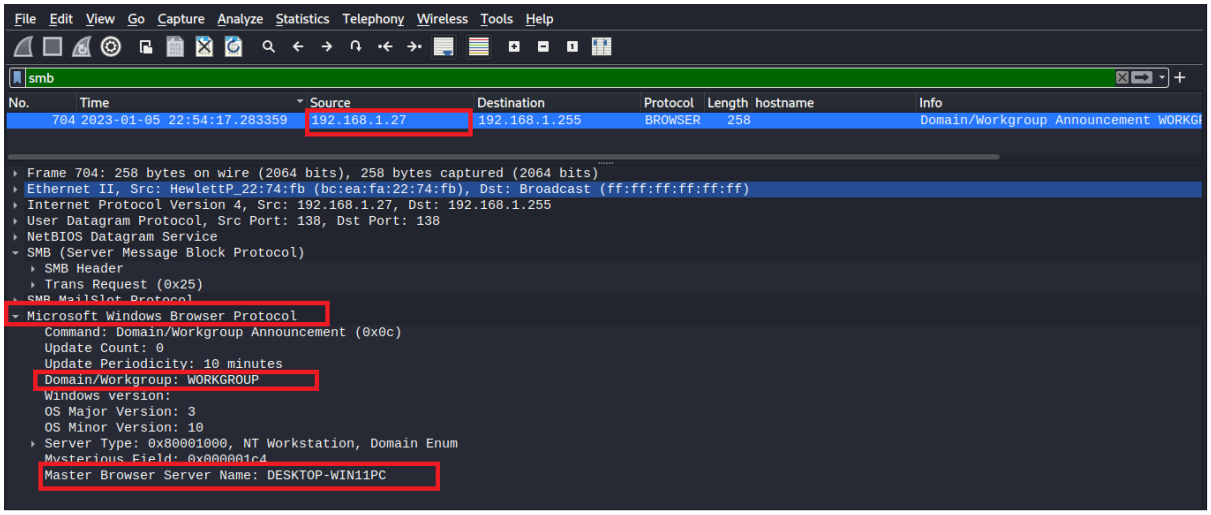
Identifikasi Network Traffic Agent Tesla

Dalam melakukan proses identifikasi, disini kami menggunakan system operasi Linux yaitu Kali linux. Untuk file pcap yang digunakan, dapat didownload pada website "*Malware Traffic analysis*". Kami memulai identifikasi dengan mengunakan filter "http.request", hal ini berdasarkan informasi bahwa aktivitas tersebut akan mencoba melakukan anomaly req htpp. Dan kami mendapati informasi tersebut.



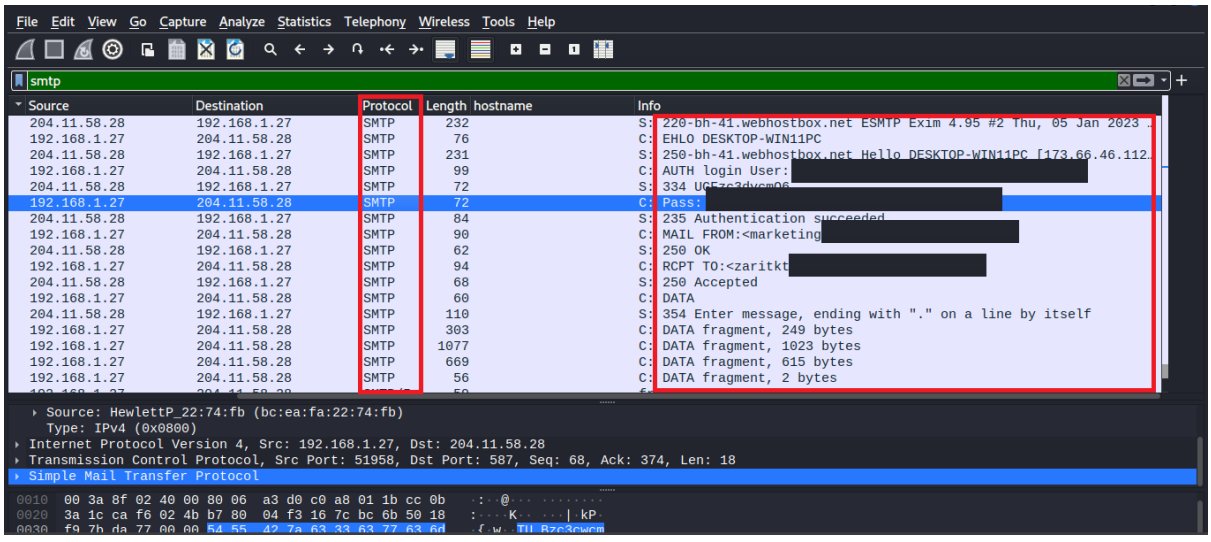
Terlihat bahwa ip address 192.168.1.27 mencoba melakukan komunikasi terhadap ip eksternal dengan menggunakan http metode "GET" pada 2023-01-05 jam 22:51:00 UTC. Berdasarkan dari hasil pengecekkan, ip tersebut mencoba mengakses "/savory.com/sav/Ztvfo.png". Selain itu juga terdapat informasi mengenai mac address dari device tersebut yaitu bc:ea:fa:22:74:fb.

Setelah mengetahui ip dan mac address dari device terinfeksi tersebut, kami mencoba untuk melakukan identifikasi user dengan cara mencari hostname dari device tersebut. Disini kami memanfaantkan filter "SMB". Dimana SMB (Server Message Block) sendiri adalah protokol standar Internet yang digunakan pada sistem operasi Windows untuk berbagi file, printer, dan port serial. Dalam lingkungan jaringan, server membuat sistem file dan sumber daya tersedia untuk klien. Klien membuat permintaan SMB untuk sumber daya, dan server membuat respons SMB dalam apa yang disebut sebagai server klien, protokol respons-permintaan. Umumnya dalam protokol SMB tersebut, dapat dengan mudah untuk mengetahui hostname yang terhubung dalam suatu jaringan.



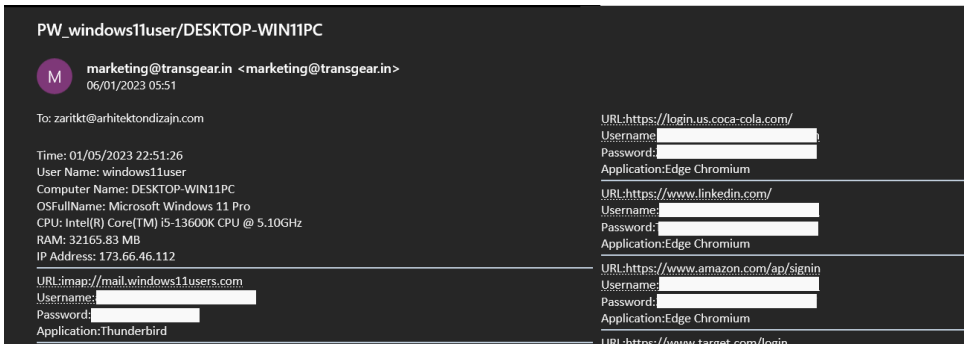
Dengan menggunakan filter “SMB” kami menemukan informasi yang kami inginkan. Terlihat bahwa device dengan ip address 192.168.1.27 yang berada dalam domain “workgroup” menggunakan “DEKSTOP-WIN11PC” sebagai hostnamenya.

Proses identifikasi kami lanjutkan. Disini kami mengetahui bahwa aktivitas Agent-Tesla juga melibatkan penggunaan protokol SMTP. Dimana protokol SMTP atau Simple Mail Transfer Protocol adalah suatu protokol untuk berkomunikasi dengan server guna mengirimkan email dari lokal email ke server, sebelum akhirnya dikirimkan ke server email penerima. Proses ini dikontrol dengan Mail Transfer Agent (MTA) yang ada dalam server email Anda.



Terlihat bahwa data dari protokol “SMTP” tersebut tidak ternekripsi sehingga kami dapat dengan mudah membaca data data tersebut. Hal ini sangat menguntukan dari sisi attacker, dimana dia dapat dengan mudah mendapatkan informasi. Untuk mempermudah proses

indentifikasi, kami mencoba untuk mengeksport beberapa data tersebut kedalam suatu file .eml
.



Setelah berhasil mengekspor kedalam file .eml, kami membuka file tersebut menggunakan aplikasi mail. Berdasarkan gambar diatas, kami mendapati informasi yang sensitif. Dimana informasi tersebut berupa kredential-kredential yang terdapat pada device tersebut. Seperti linkedin, amazon dan lain sebagainya. Disini kami juga mengetahui bahwa, sistem operasi yang diguanakan pada device terinfeksi adalah Windows 11 Pro dengan spesifikasi ram tersedia yaitu 32165.83 MB atau 4 GB serta menggunakan prosesor dari dari product Intel(R) Core ™ i5-13600K dengan clock speed 5.10Hz. Selain itu kami juga mendapati bahwa ip address publik yang digunakan device terinfeksi adalah 178.66.46.112.

REFERENSI

- https://unit42.paloaltonetworks.com/january-wireshark-quiz/
- https://unit42.paloaltonetworks.com/january-wireshark-quiz/#post-126652-_l9tz157aemxs
- https://twitter.com/Unit42_Intel/status/1611379660029366273/photo/4
- https://forensicitguy.github.io/net-downloader-originlogger/#triaging-the-malware
- https://unit42.paloaltonetworks.com/january-wireshark-quiz-answers/#post-126670-_vetnh42c57fg