2023

SECURITY REPORT

Gozi Infection via Malspam

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

TLP:CLEAR

Daftar Isi

Executive Summary

Berdasarkan postingan resmi Palo Alto Unit 42 yang dimuat di twitter, terdapat aktivitas penyebaran Malware Gozi melalui aktivitas Malspam. Aktivitas tersebut terdeteksi pada tanggal 6 Maret 2023. Gozi merupakan salah satu malware yang termasuk dalam kategori Spyware Trojan. Dimana malware tersebut dapat mengakibatkan pencurian data sensitive terhadap device yang telah terinfeksi.

Latar Belakang

Pada bulan Maret tahun 2023, Palo Alto Network Unit 42 merilis portingan resmi meraka melalui twitter mengenai aktivitas infeksi malware Gozi melalui Malspam yang ditemukan pada hari Senin 06 Maret 2023. Berikut kami mendapati beberapa artifact dari aktivitas anomali tersebut yaitu sample malware serta file pcap network traffic yang berisi aktivitas Compromise dari sample malware tersebut.

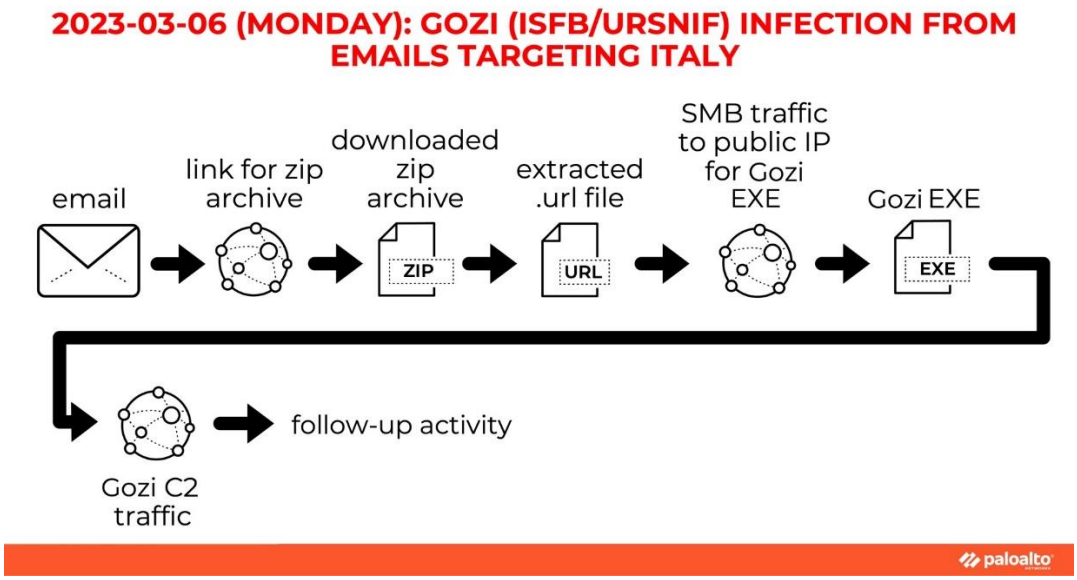
Requirements

Dalam melakukan proses analysis, 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. Disni kami menggunakan sistem operasi Linux Remnux berbasis Ubuntu yang telah dilengkapi dengan tools pendukung.

Selain itu disini kami juga 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 wireshark dikarenakann dukungan fitur yang lebih banyak, disini kami menggunakan wireshark versi terbaru yaitu 4.0.1.

Alur Infeksi Malware Gozi

Berdasarkan informasi yang dimuat pada postingan resmi twitter palo alto network unit 42, Diketahui aktivitas infeksi malware Gozi dimulai dari pengiriman email. Email tersebut memuat suatu link yang berisi perintah untuk mendownload suatu file yang bekstensi .zip. ketika file .zip tersebut di ekstraksi, akan menghasilkan suatu file lagi yang berktensi .url. dimana file .url tersebut berisi ip public dari server gozi dan akan secara otomatis melakukan download file server.exe yang sebernarnya adalah file malware Gozi. Setelah file server.exe tersebut diinstall, secara otomatis terjadi koneksi *Compromise* terhadap device tersebut dengan server gozi.

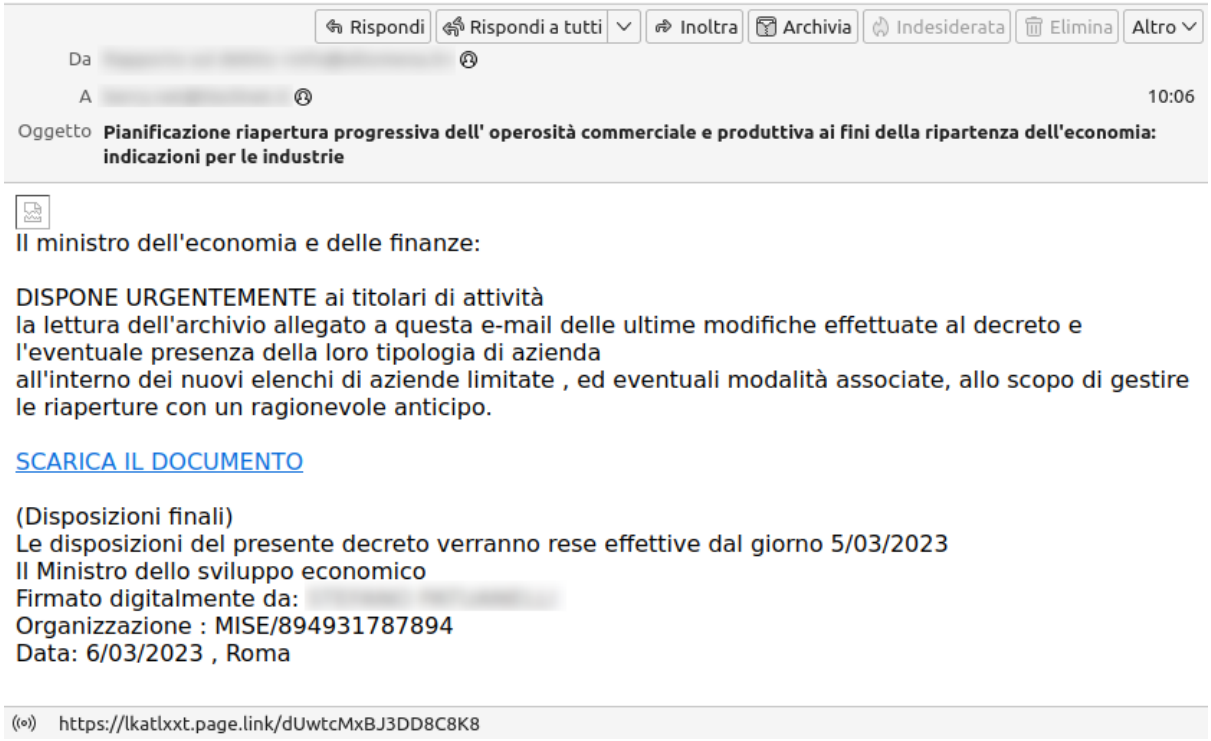


Gambar 1. Alur Infeksi Malware Gozi

Identifikasi Sample Malware

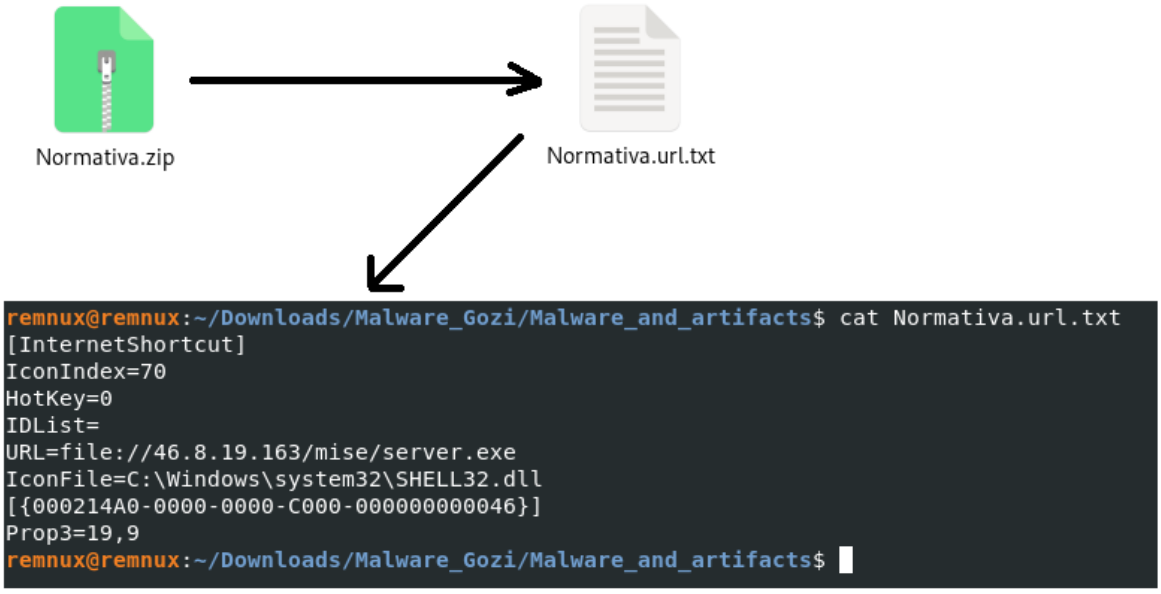
Dalam melakukan proses identifikasi sample malware Gozi, kami menggunakan lingkungan sistem opreasi linux Remnux berbasis Ubuntu. Proses identifikasi dimulai dengan menyelidiksi email spam yang digunakan sebagai perantara untuk menyebarkan infeksi malware Gozi. Berikut adalah detail dari file Normativa.zip

- Nama : Normariva.zip
- File ekstensi : .zip
- File size : 474 bytes
- SHA256 : 57befac41319e7e1fc9d6cd5637240fa766bdbc 562d7720bb04beee36113ae10
- MD5 : 497ae00a80cd4024046cab183833773f
- SHA1 : e1bdd085cd85d03d2dcf76c3659619fa921633aa



Gambar 2. Screenshoot tampilan email Malspam

Berdasarkan gambar 2, diketahui bahwa email tersebut menggunakan subject yaitu "**pianificazione riapertura progressiva dell' operosita commerciale e produttiva ai fini della ripartenza dell'economia: indicazioni per le industrie**", yang jika kami artikan menjadi "merencanakan pembukaan kembali kegiatan komersial dan produktif secara bertahap untuk memulai kembali perekonomian: indikasi untuk industri". Melihat dari subject email tersebut, seperti memiliki maksud yang cukup penting, sehingga dapat membuat pembaca untuk mengikuti intruksi yang diperintahkan dalam pesan tersebut. Pada email tersebut kami mendapati attachment berupa link url yang mengarah ke htpps://nhatheptienchebinhduong [.]com/mise/Normativa.zip. pada link tersebut korban akan secara otomatis mendownload file bernama Normativa.zip. Dimana saat kami mendapati bahwa "Normativa" dalam bahas italia memiki arti "peraturan", sehingga hal ini dapat dengan mudah menipu korban bahwa file tersebut sebagai file normal.

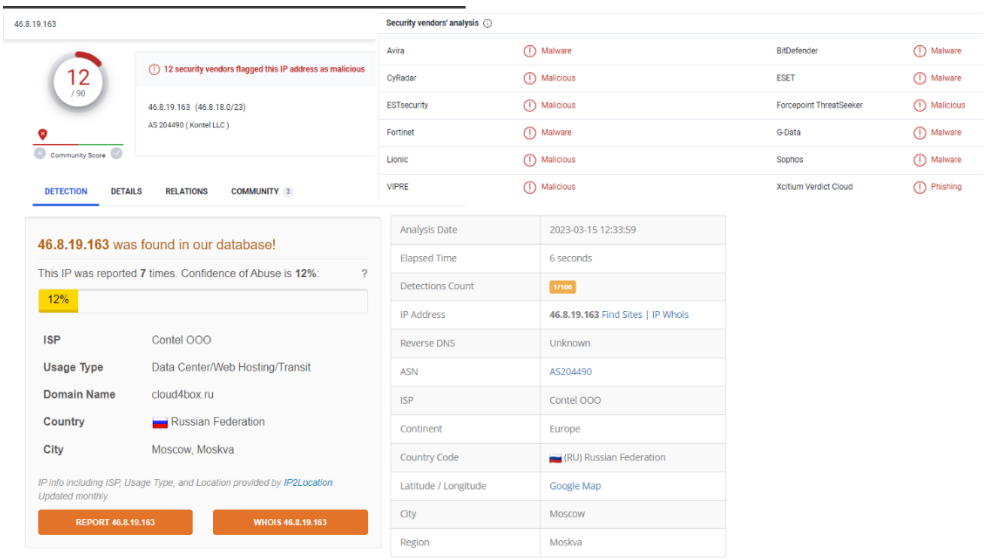


Gambar 3. File Normativa

Berdasarkan gambar 3, file Normativa yang didownload dari attachment link url email menggunakan ekstensi file .zip. Setelah di ekstraksi, file tersebut berubah menjadi Normativa.url.txt. Disini kami melihat double ekstension, sehingga file tersebut terindikasi

sebagai anomaly. Dengan menggunakan command cat, kami mengetahui bahwa file Normativa.url.txt tersebut terdiri dari beberapa instruction (string). Berikut adalah beberapa point yang menjadi fokus kami

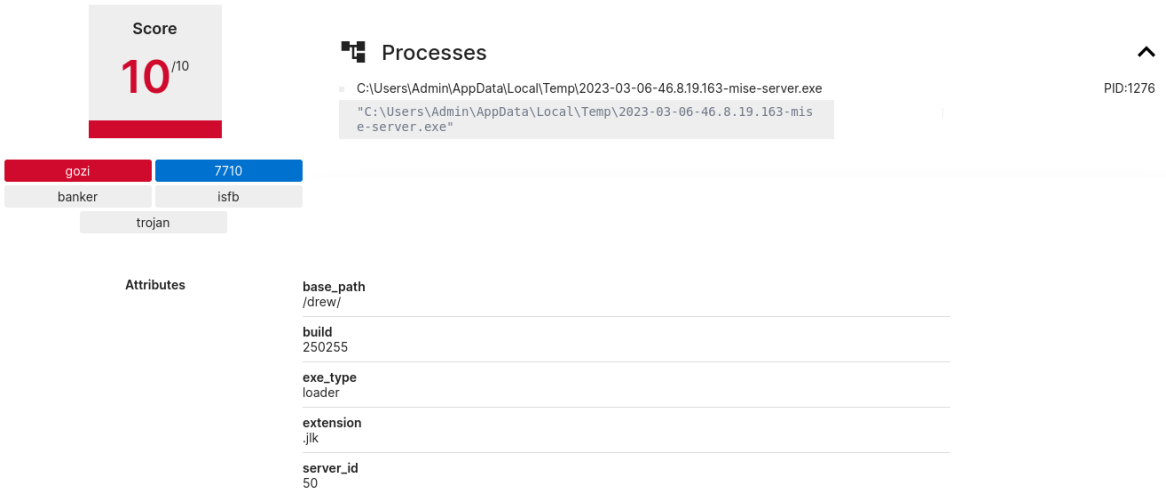
- [Internet Shortcut] : memungkinkan pengguna untuk membuka halaman, file, atau sumber daya yang terletak di lokasi Internet atau situs Web yang jauh. Pintasan biasanya diimplementasikan sebagai file kecil yang berisi target URI atau GUID ke objek, atau nama file program target yang diwakili oleh pintasan.
- URL : url disini berati adalah link yang akan menjadi tujuan dari instruction Internet Shortcut. Link tersebut adalah file://46.()8(.)19(.)163/mise/server.exe
- IconFile : menunjukkan proses apa yang akan dijalankan host tersebut saat membuka file Normativa.url.txt. Terlihat bahwa host akan menjalan proses C:\Windows\system32\SHELL32.dll. dimana SHELL32.dll merupakan library yang berisi fungsi Windows Shell API, yang digunakan untuk membuka halaman web dan file
- IOC : Link url yang dipakai berisi ip address yang berasal dari negara Russia. Dimana ip tersebut temasuk sebagai ip bad reputations, sebanyak 12 security vendors flagged this IP address as malicious pada virus totals, sebanyak 7 kali telah dilaporkan pada abuseipdb serta mendapatkan blacklist score 1/106 pada website ipvoid



Gambar 4. Identifikasi ip reputation Normativa

Setelah membuka file Normativa.url.txt secara otomatis kami melakukan download file baru dengan nama server.exe. kami mencoba melakukan analysis file menggunakan bantuan sandbox dari hatching.triage. Berikut adalah detail file server.exe

- Nama : server .exe
- File ekstensi : .exe
- File size : 319.0 kB
- SHA256 : fc3e7ff40a45bccd83617ea952eccdfc9330 1c6673cce8de33b4bf924b8957d9
- MD5 : 9390d0d62ea148b02178682114e49bc7
- SHA1 : d6c55c43aacb6cc7fde55817747a6dc7f53df51c



Gambar 5. Sandbox Report server.exe

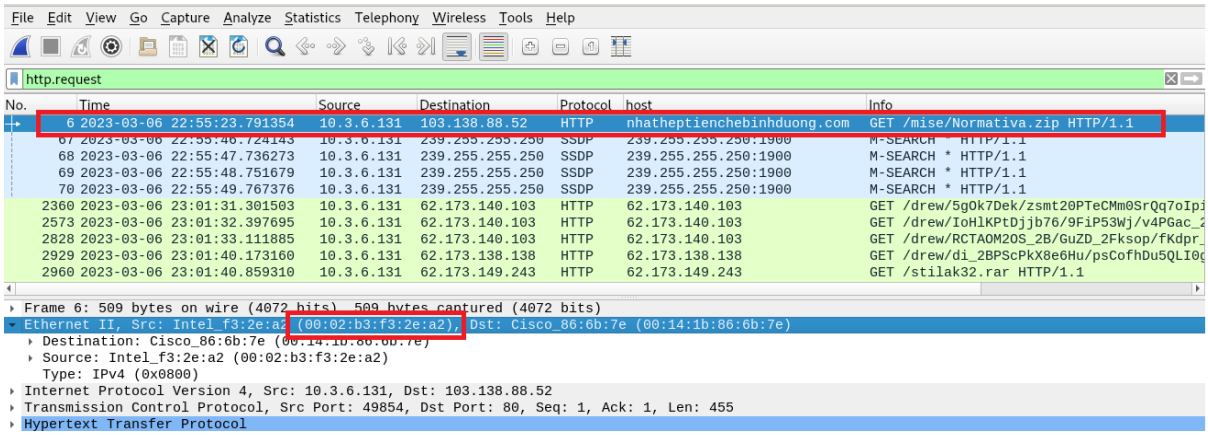
Terlihat bahwa file server.exe mendapatkan nilai 10/10 sebagai malware. File tersebut benar terinentifikasi sebagai malware Gozi banker. Diketahui bahwa malware tersebut tersebut memiliki exe_type yaitu “Loader”. Dimana loader sendiri berfungi sebagai pemanggil atau pemberi pesan bahwa device telah terinfeksi dan siap melakukan koneksi compromise (C2) terhadap server Gozi malware.

Terlihat juga beberapa Indicator of Compromsise (IoC) yang diketahui dari file tersebut yaitu :

- checklist.skype.()com
- 62.()173(.)140.()103
- 31(.)41.()44.()63
- 46(.)8.()19.()239
- 185(.)77(.)96(.)40
- 46(.)8(.)19(.)116
- 31(.)41(.)44(.)48
- 62(.)173(.)139(.)11
- 62(.)173(.)138(.)251

Identifikasi Network Traffic Gozi Malware

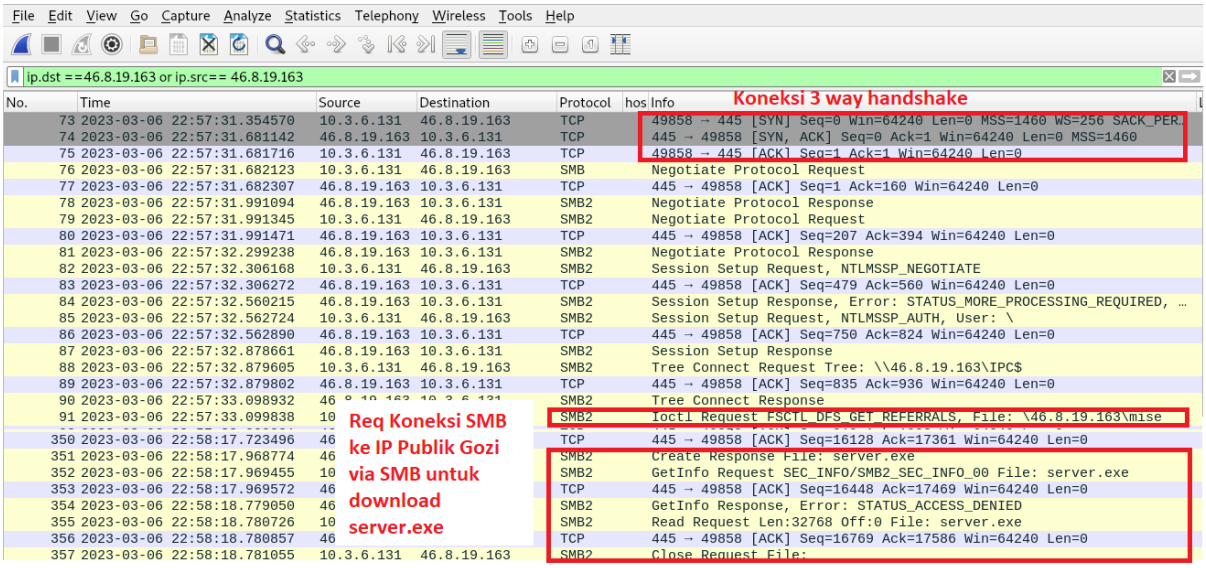
Bagian ini merupakan identifikasi aktivitas penyebaran malware Gozi dari network traffic. Proses identifikasi ini menggunakan bantuan tools wireshark. Kami memulai identifikasi dengan mengunakan filter “http.request”, hal ini berdasarkan informasi bahwa aktivitas tersebut akan mencoba melakukan download file “Normariva.zip” setelah korban mengklik attachment berupa link url.



Gambar 6. HTTP Request Malspam

Terlihat pada gambar 6, korban diketahui melakukan request http dengan metode “GET” dan mendaoatkan response code 200. Terlihat bahwa request http tersebut mengarah ke ip public 103(.)138(.)88.()52 yang berasal dari negara Vietnam dengan hostname yaitu nhatheptienchebinhduong.com. Diketahui bahwa device terinfeksi malspam menggunakan mac address 00:14:1b:86:6b:7e.

Setelah berhasil mendownload file Normativa.zip, user terinfeksi akan diminta untuk menesktraksi file tersebut sehingga menjadi file Normativa.url.txt. Setelah terekstraksi, file tersebut dibuat oleh korban sehingga akan menimbulkan request koneksi kearah ip public lainnya.



Gambar 7. Koneksi SMB Server.exe

Terlihat bahwa pada jam 22:57 berselang 2 menit dari proses download file Normativa.zip, terjadi koneksi awal yang diberasal dari korban. Telihat bahwa ip korban melakukan proses 3 wayhandshake dengan membuat resquest motede “syn” pada ip public yaitu 46(.)8(.)19(.)163 yang berasal dari russia. Terlihat juga bahwa user membuara response request file “server.exe” pada direktori /mise melalui protocol SMB. File server.exe inilah yang merupakan file malware asli yang dinamakan sebagai Gozi malware.

Gambar 8. File Upload

Terlihat bahwa terdapat request metode “POST” yang dilakukan korban kea rah ip public Gozi malware. Diketahui bahwa filename tersebut adalah “B04F.bin” namun kami tidak dapat mengetahui file apa yang di kirim korban ke ip Gozi malware.

Tactic dan Technique

Berdasarkan hasil pengecekkan yang kami lakukan menggunakan file scan.io, diketahui bahwa file “server.exe” terdeteksi menggunakan tactic Defense Evasion dengan technique Software Packing. Software Packing sendiri merupakan metode mengompresi atau mengenkripsi file yang dapat dieksekusi. Mengemas file yang dapat dieksekusi mengubah tanda tangan file dalam upaya untuk menghindari deteksi berbasis tanda tangan. Sebagian besar teknik dekompresi mendekompresi kode yang dapat dieksekusi di memori. Perlindungan perangkat lunak mesin virtual menerjemahkan kode asli yang dapat dieksekusi ke dalam format khusus yang hanya dapat dijalankan oleh mesin virtual khusus. Mesin virtual kemudian dipanggil untuk menjalankan kode ini. Namun saat kami menguji menggunakan Hacting.triage sandbox kami mendapati hamper semua Tactic digunakan oleh malwre tersbeut namun tidak dijelaskan menggunakan technique apa.

Gambar 9. Tactic dan Technique

Indicator of Compromise (IoC)

Berdasarkan hasil pengecekkan yang kami lakukan serta laporan yang dibuat oleh tim Palo Alto Network Unit 42, didapatkan beberapa Indicator of Compromise (IoC) yang berasal dari aktivitas infeksi malware Gozi tersebut seperti berikut :

- MALWARE FROM AN INFECTION TEST RUN ON 2023-03-06:

    - SHA256 hash: 57befac41319e7e1fc9d6cd5637240fa766bdbc562d7720bb04beee36113ae10
    - File size: 474 bytes
    - File location: hxxps://nhatheptienchebinhduong[.]com/mise/Normativa.zip
    - File description: Zip archive from link in email

    - SHA256 hash: c59dc482b521b021813681f99a8570aa0f57a30bcf42d48667eb09ae635cc9a1
    - File size: 189 bytes
    - File name Normativa.url
    - File description: URL file extracted from the above zip archive

    - SHA256 hash: fc3e7ff40a45bccd83617ea952eccdfc93301c6673cce8de33b4bf924b8957d9
    - File size: 318,976 bytes
    - File location: file://46.8.19[.]163/mise/server.exe
    - File description: Windows EXE for Gozi/ISFB/Ursnif retrieved by the above .url file

- TRAFFIC FROM AN INFECTED WINDOWS HOST:
  - URL FOR INITIAL ZIP DOWNLOAD:
    - 103.138.88[.]52 port 80 - nhatheptienchebinhduong[.]com - GET /mise/Normativa.zip
    - Note: The URL for this is HTTPS, but it can also be retrieved over unencrypted HTTP traffic.

  - SMB TRAFFIC FOR GOZI (ISFB/URSNIF) EXE:
    - 46.8.19[.]163 port 445 - SMB traffic - file://46.8.19[.]163/mise/server.exe

  - GOZI (ISFB/URSNIF) C2:
    - 62.173.140[.]103 port 80 - 62.173.140[.]103 - GET /drew/[base64 string with underscores and backslashes].jlk
    - 62.173.138[.]138 port 80 - 62.173.138[.]138 - GET /drew/[base64 string with underscores and backslashes].gif
    - 62.173.149[.]243 port 80 - 62.173.149[.]243 - GET /stilak32.rar
    - 62.173.149[.]243 port 80 - 62.173.149[.]243 - GET /stilak64.rar
    - 62.173.138[.]138 port 80 - 62.173.138[.]138 - POST /drew/[base64 string with underscores and backslashes].bmp
    - 62.173.149[.]243 port 80 - 62.173.149[.]243 - GET /cook32.rar
    - 62.173.149[.]243 port 80 - 62.173.149[.]243 - GET /cook64.rar
    - 62.173.140[.]94 port 80 - 62.173.140[.]94 - GET /drew/[base64 string with underscores and backslashes].gif
    - 31.41.44[.]60 port 80 - 31.41.44[.]60 - GET /drew/[base64 string with underscores and backslashes].gif
    - 46.8.19[.]233 port 80 - 46.8.19[.]233 - GET /drew/[base64 string with underscores and backslashes].gif
    - 5.44.45[.]201 port 80 - 5.44.45[.]201 - GET /drew/[base64 string with underscores and backslashes].gif
    - 89.116.236[.]41 port 80 - 89.116.236[.]41 - GET /drew/[base64 string with underscores and backslashes].gif
    - 62.173.140[.]76 port 80 - 62.173.140[.]76 - GET /drew/[base64 string with underscores and backslashes].gif

- 31.41.44[.]49 port 80 - 31.41.44[.]49 - GET /drew/[base64 string with underscores and backslashes].gif
- 46.8.19[.]86 port 80 - 46.8.19[.]86 - GET /drew/[base64 string with underscores and backslashes].gif
- 62.173.140[.]94 port 80 - 62.173.140[.]94 - GET /drew/[base64 string with underscores and backslashes].gif

Referensi

- https://twitter.com/Unit42_Intel/status/1633934017031467010/photo/3
- https://twitter.com/AgidCert/status/1632686769203302402
- https://twitter.com/JAMESWT_MHT/status/1632693485739429889
- https://cert-agid.gov.it/wp-content/uploads/2023/03/ursnif_mise_06-03-2023.json_.txt
- https://github.com/pan-unit42/tweets/blob/master/2023-03-06-IOCs-for-Gozi-infection.txt