Internet Storm Center

isc.sans.edu/diary/Brazil+malspam+pushes+Astaroth+(Guildma)+malware/28962

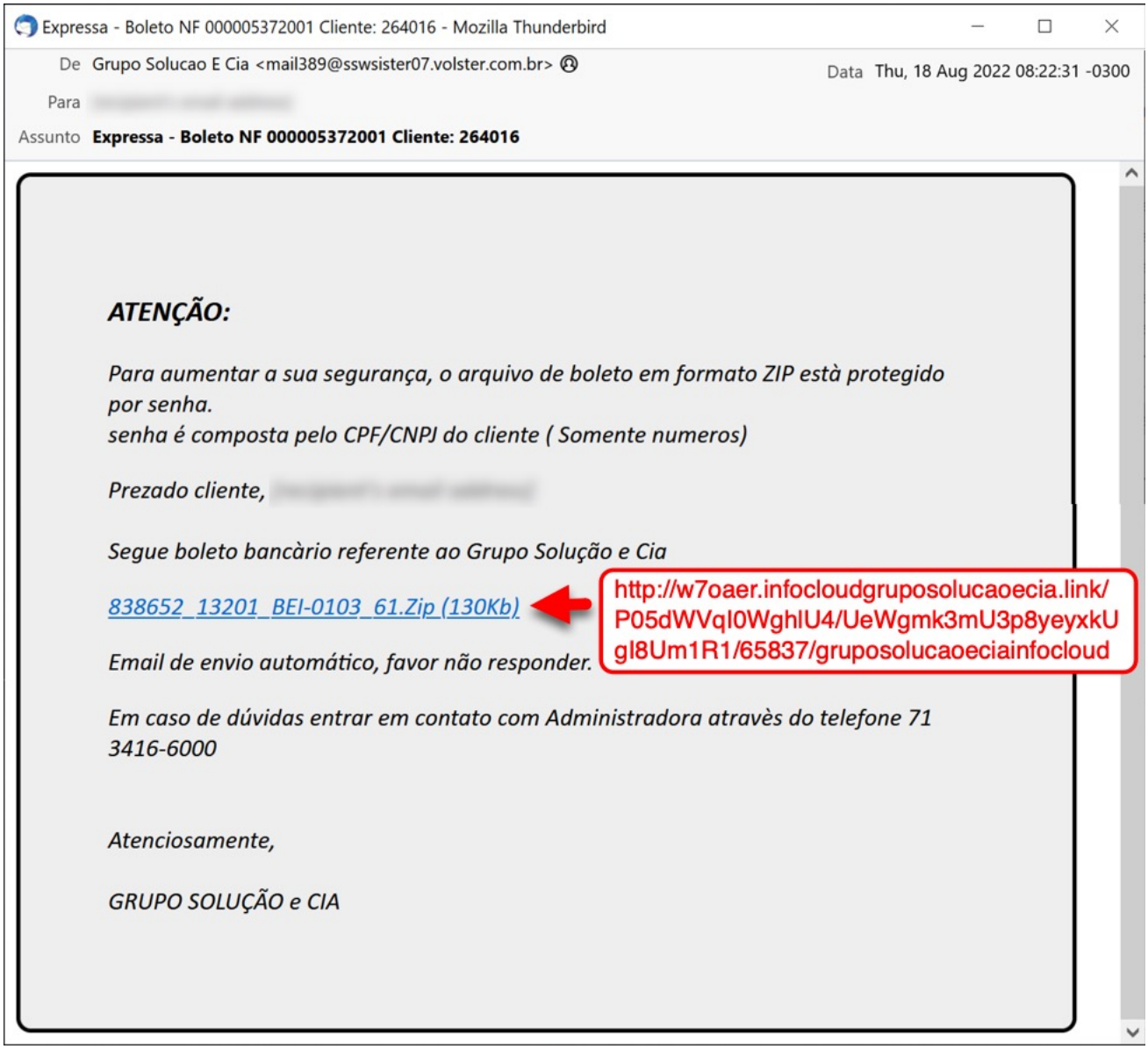
Brazil malspam pushes Astaroth (Guildma) malware

Published: 2022-08-19
Last Updated: 2022-08-19 22:43:52 UTC
by Brad Duncan (Version: 1)
0 comment(s)

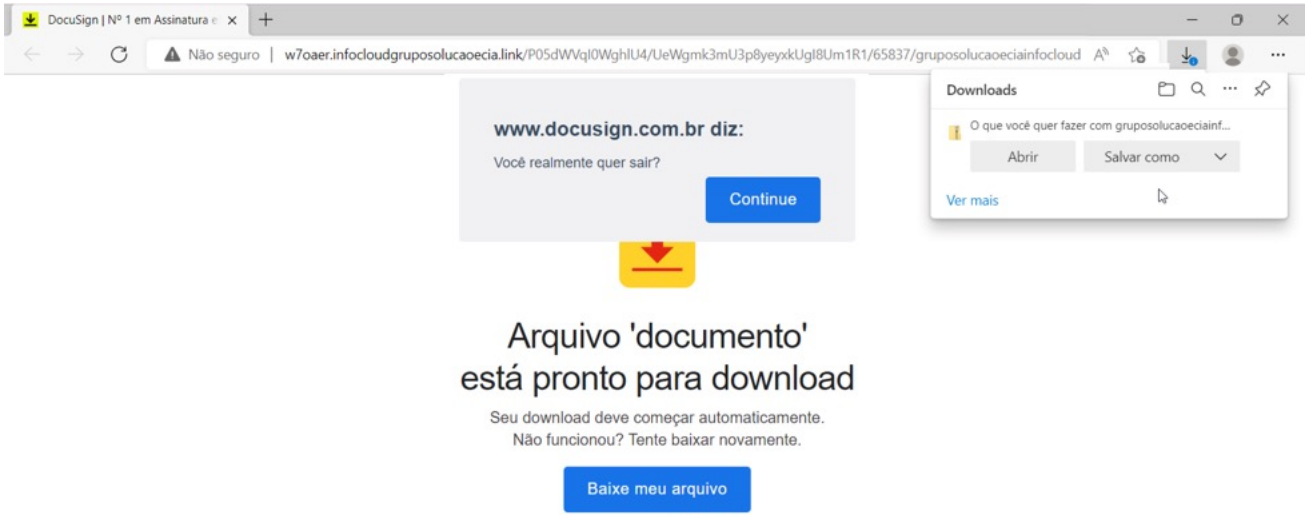
Introduction

Today's diary is a quick post of an Astaroth (Guildma) malware infection I generated todayy on Friday 2022-08-19 from a malicious Boleto-themed email pretending to be from Grupo Solução & CIA. Boleto is a payment method used in Brazil, while Grupo Solução & CIA is Brazil-based company.

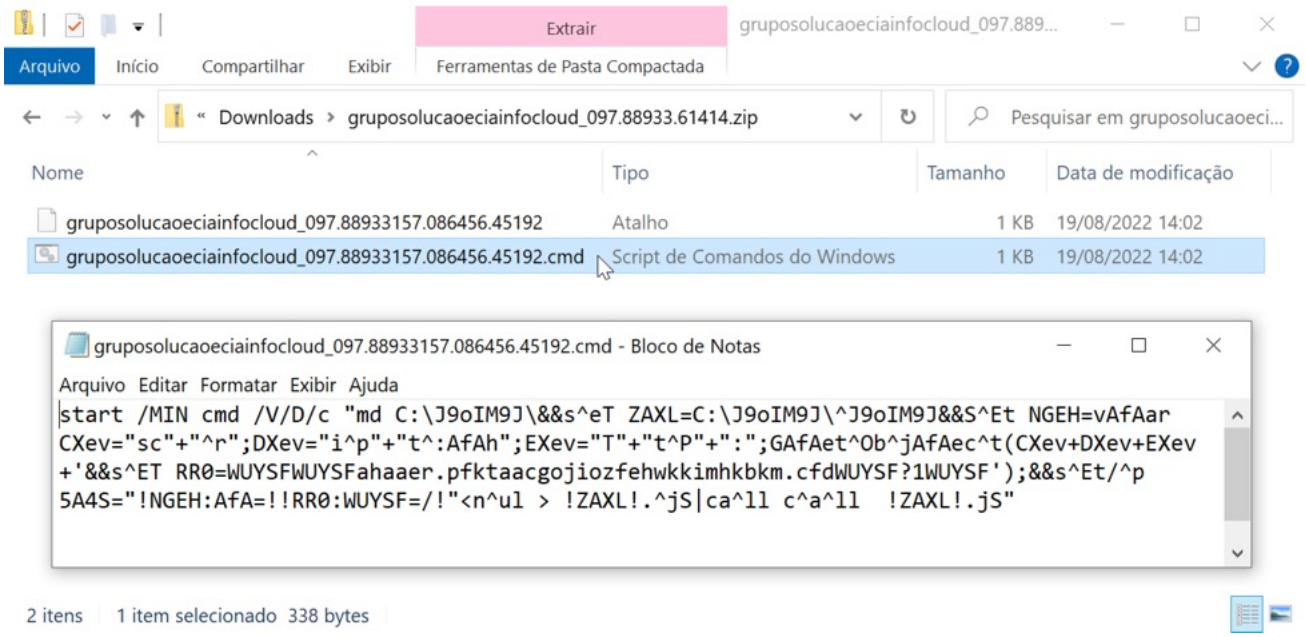
Images from the infection



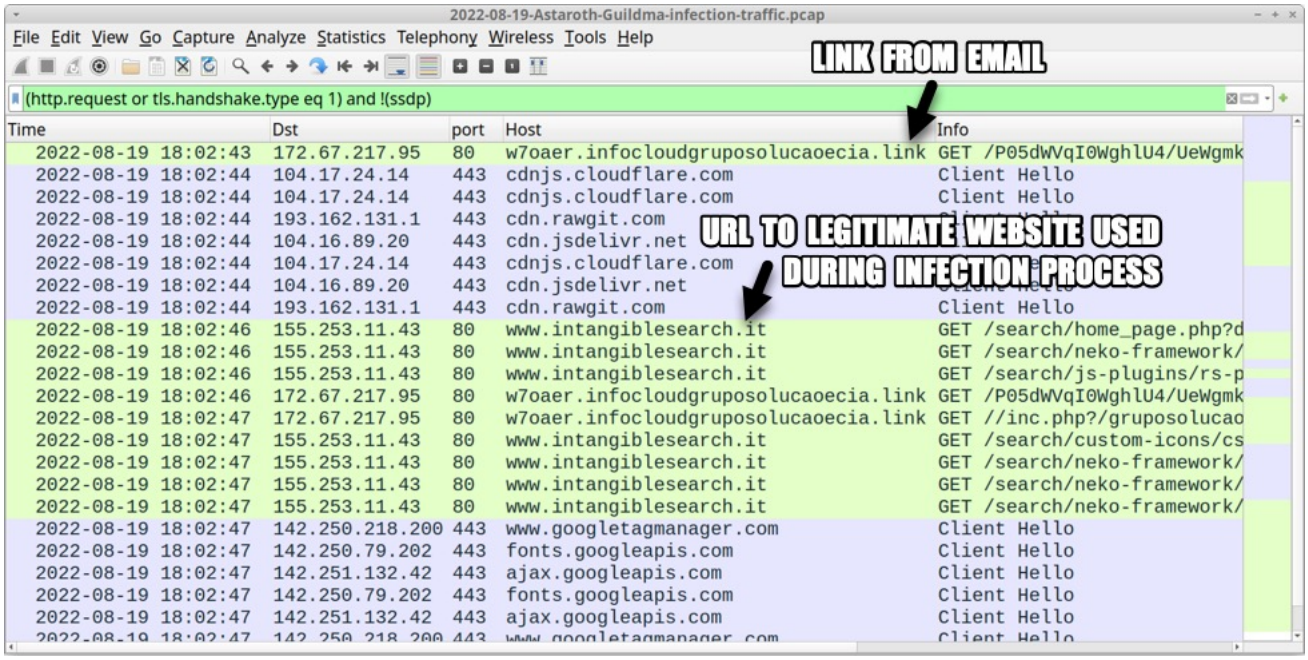
Shown above: Screenshot of the malicious email with link to download a malicious zip archive.



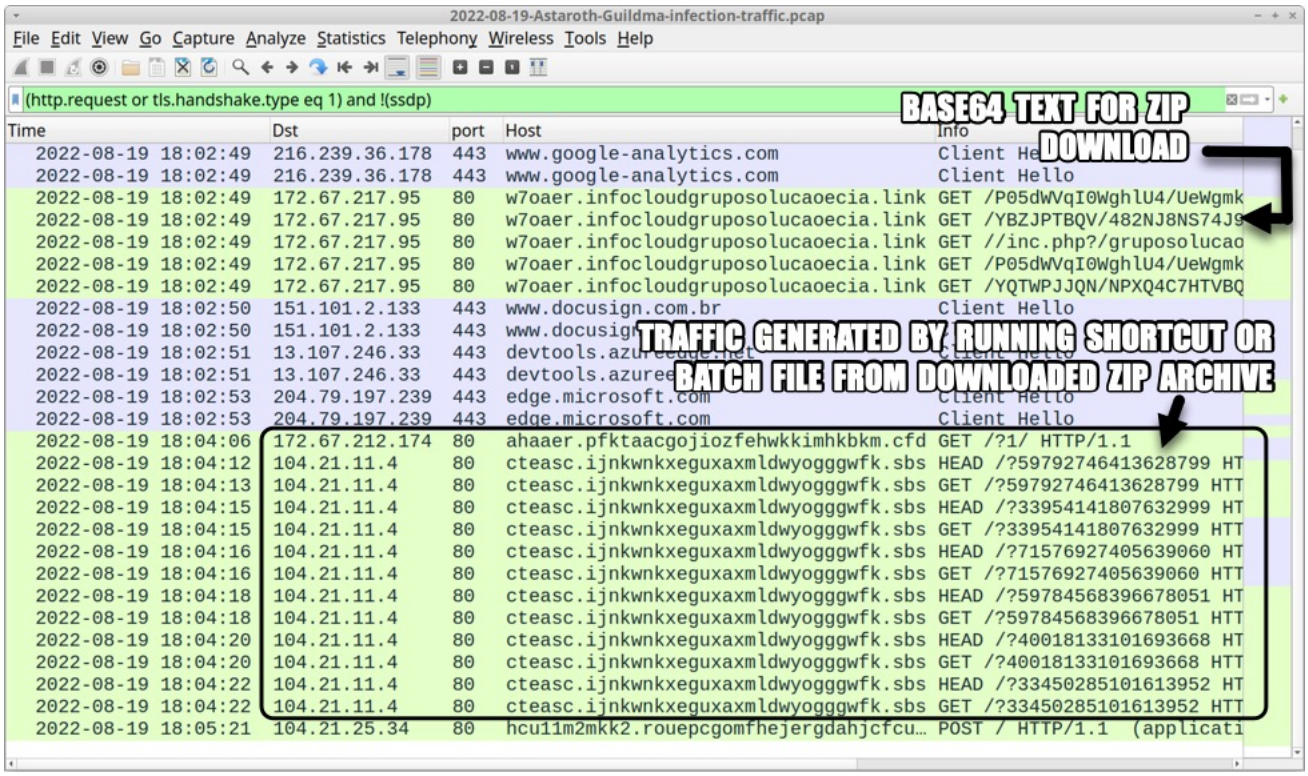
Shown above: Link from email leads to web page pretending to be from Docusign that provides malicious zip archive for download.



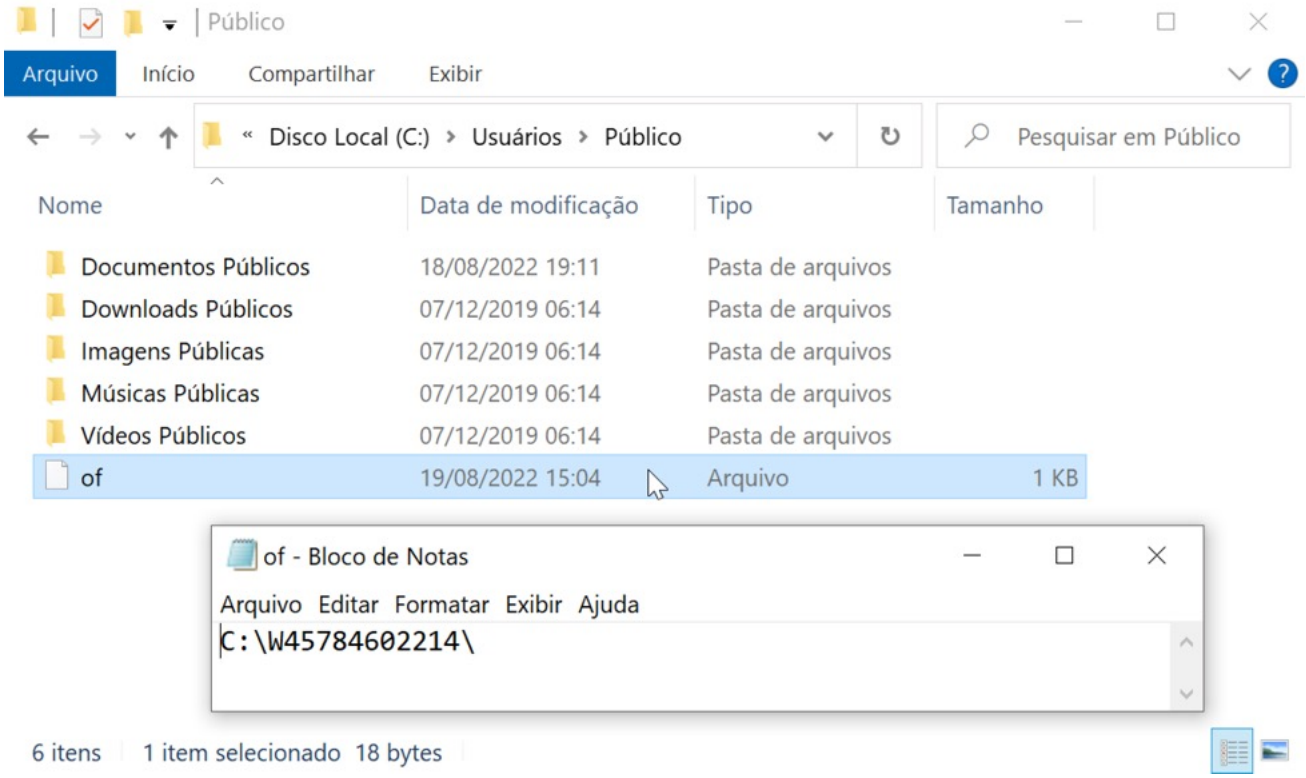
Shown above: Downloaded zip archive contains a Windows shortcut and a batch file. Both are designed to infect a vulnerable Windows host with Astaroth (Guildma).



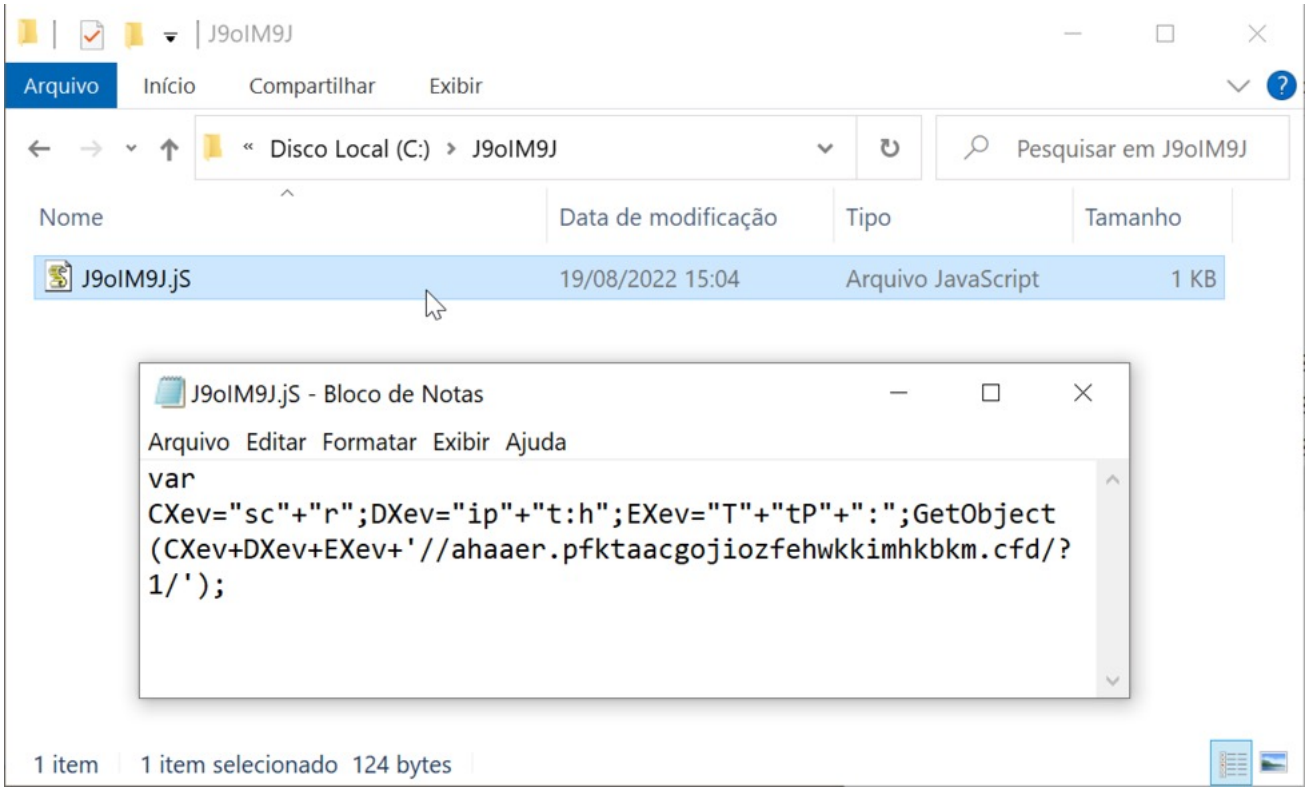
Shown above: Traffic from the infection filtered in Wireshark (part 1 of 3).



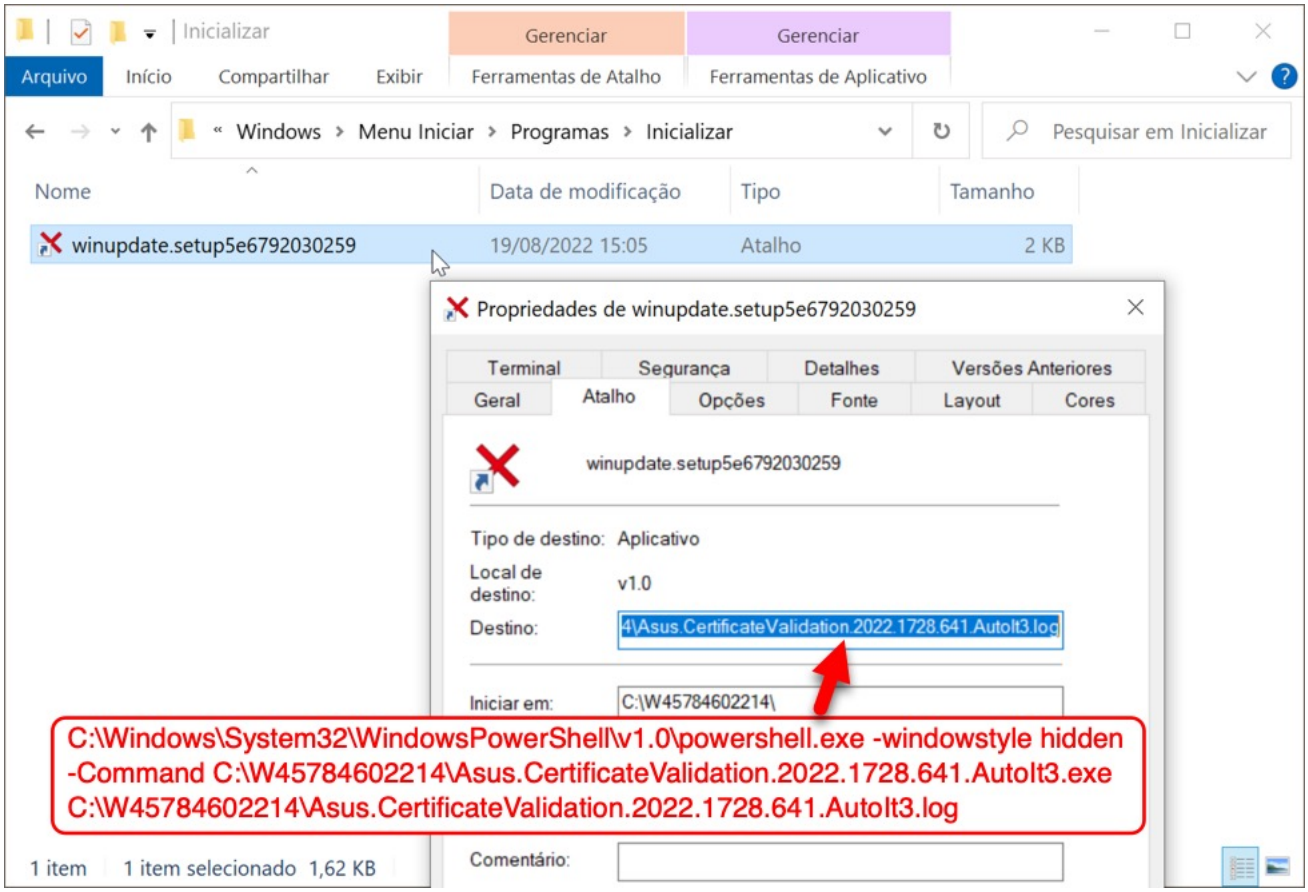
Shown above: Traffic from the infection filtered in Wireshark (part 2 of 3).



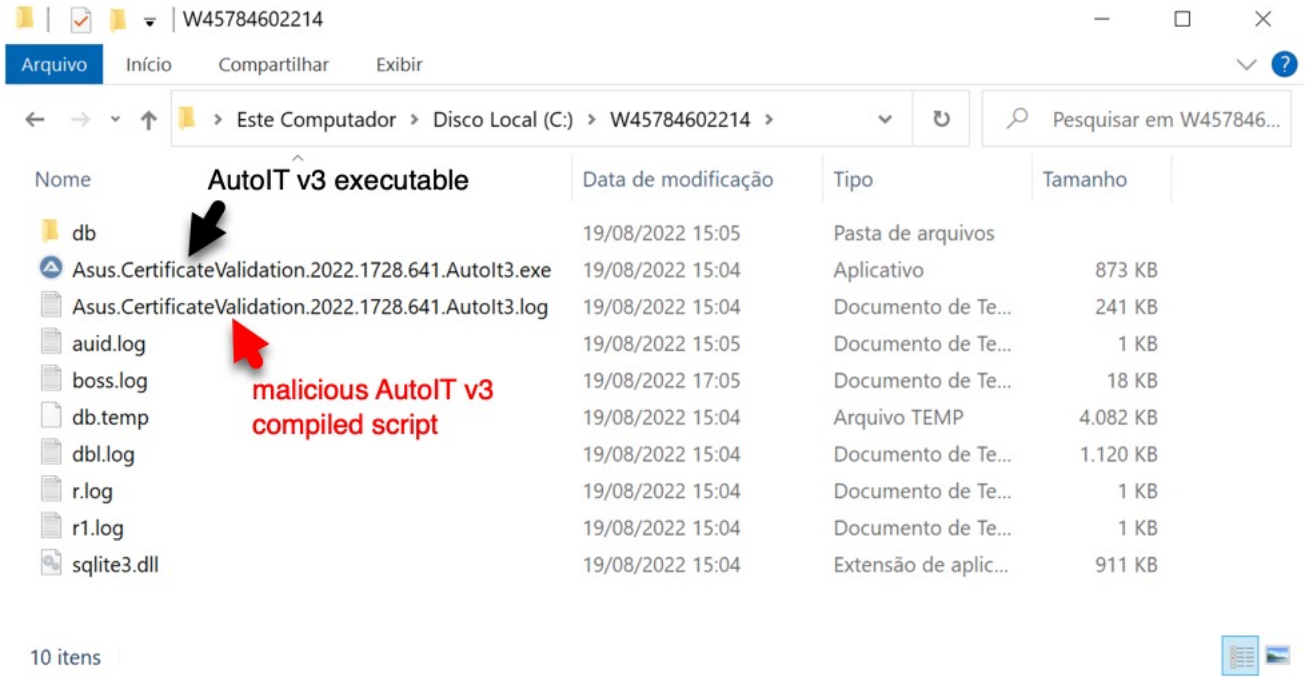
Shown above: Artifact from the infected host's C:\Users\Public directory.



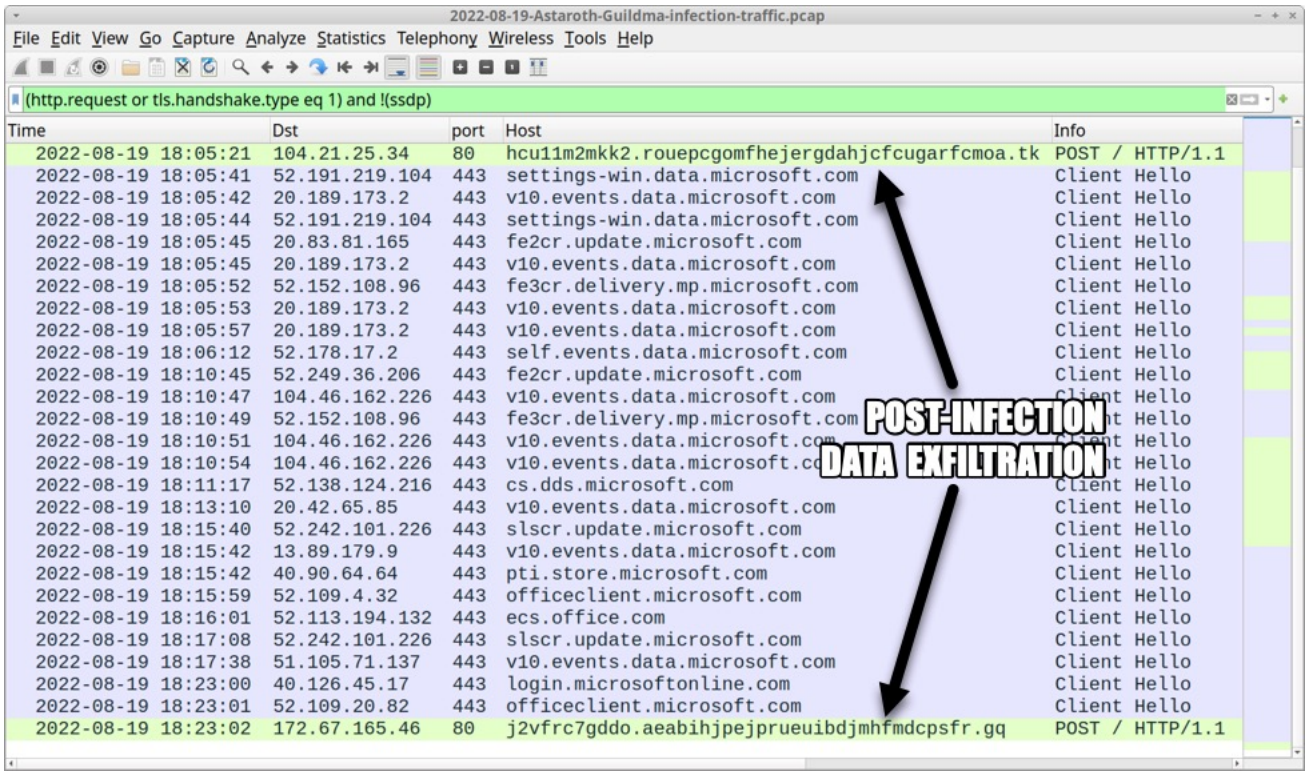
Shown above: Artifact on the infected host's C: drive at C:\J9oIM9J\J9oIM9J.jS.



Shown above: Windows shortcut in the infected user's Roaming\Microsoft\Windows\Start Menu\Programs\Startup directory to keep the infection persistent.



Shown above: Directory with persistent files used for the Astaroth (Guildma) infection.



Shown above: Astaroth (Guildma) performs post-infection data exfiltration through HTTP POST requests.

Indicators of Compromise (IOCs)

Link from email:

hxxp://w7oaer.infocloudgruposolucaoecia[.]link/P05dWVqI0WghlU4/UeWgmk3mU3p8yeyxkUgI8Um1R1/65837/gruposolucaoeciainfocloud

IP address and TCP port for initial malicious domain:

172.67.217[.]95 port 80 - w7oaer.infocloudgruposolucaoecia[.]link

URL to legitimate website generated from iframe in the above traffic:

hxxp://www.intangiblesearch[.]it/search/home_page.php?
db_name=%3Cscript%20src=%22https://ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.js%22%3E%3C/script%3E%3Cscript%20type

Traffic to initial malicious domain that provides zip archive download:

- hxxp://w7oaer.infocloudgruposolucaoecia[.]link/P05dWVqI0WghlU4/UeWgmk3mU3p8yeyxkUgI8Um1R1/65837/gruposolucaoeciainfocloudA\
- hxxp://w7oaer.infocloudgruposolucaoecia[.]link//inc.php?/gruposolucaoeciainfocloud
- hxxp://w7oaer.infocloudgruposolucaoecia[.]link/YBZJPTBQV/482NJ8NS74J9/N6D6WW/gruposolucaoeciainfocloud_097.88933.61414z64y6

Traffic generated by Windows shortcut or batch file from the downloaded zip archive:

- 172.67.212[.]174:80 ahaaer.pfktaacgojiozfehwkkimhkbkm[.]cfd GET /?1/
- 104.21.11[.]4:80 cteasc.ijnkwnkxeguxaxmldwyogggwfk[.]sbs HEAD /?59792746413628799
- 104.21.11[.]4:80 cteasc.ijnkwnkxeguxaxmldwyogggwfk[.]sbs GET /?59792746413628799
- 104.21.11[.]4:80 cteasc.ijnkwnkxeguxaxmldwyogggwfk[.]sbs HEAD /?33954141807632999
- 104.21.11[.]4:80 cteasc.ijnkwnkxeguxaxmldwyogggwfk[.]sbs GET /?33954141807632999
- 104.21.11[.]4:80 cteasc.ijnkwnkxeguxaxmldwyogggwfk[.]sbs HEAD /?71576927405639060
- 104.21.11[.]4:80 cteasc.ijnkwnkxeguxaxmldwyogggwfk[.]sbs GET /?71576927405639060
- 104.21.11[.]4:80 cteasc.ijnkwnkxeguxaxmldwyogggwfk[.]sbs HEAD /?59784568396678051
- 104.21.11[.]4:80 cteasc.ijnkwnkxeguxaxmldwyogggwfk[.]sbs GET /?59784568396678051
- 104.21.11[.]4:80 cteasc.ijnkwnkxeguxaxmldwyogggwfk[.]sbs HEAD /?40018133101693668
- 104.21.11[.]4:80 cteasc.ijnkwnkxeguxaxmldwyogggwfk[.]sbs GET /?40018133101693668
- 104.21.11[.]4:80 cteasc.ijnkwnkxeguxaxmldwyogggwfk[.]sbs HEAD /?33450285101613952
- 104.21.11[.]4:80 cteasc.ijnkwnkxeguxaxmldwyogggwfk[.]sbs GET /?33450285101613952

Data exfiltration through HTTP POST requests:

- 104.21.25[.]34:80 hcu11m2mkk2.rouepcgomfhejergdahjcfcugarfcmoa[.]tk POST /
- 172.67.165[.]46:80 j2vfrc7gddo.aeabihjpejprueuibdjmhfmdcpsfr[.]gq POST /

Example of downloaded zip archive:

SHA256 hash: f254f9deeb61f0a53e021c6c0859ba4e745169322fe2fb91ad2875f5bf077300

- File size: 1,091 bytes
- File name: gruposolucaoeciainfocloud_097.88933.61414.zip

Contents from the above zip archive:

SHA256 hash: 5ca1e9f0e79185dde9655376b8cecc29193ad3e933c7b93dc1a6ce2a60e63bba

- File size: 338 bytes
- File name: gruposolucaoeciainfocloud_097.88933157.086456.45192.cmd

SHA256 hash: db136e87a5835e56d39c225e00b675727dc73a788f90882ad81a1500ac0a17d6

- File size: 1,341 bytes
- File name: gruposolucaoeciainfocloud_097.88933157.086456.45192.lNk

Command from Windows shortcut in Windows Startup folder on the infected Windows host:

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -windowstyle hidden -Command
C:\W45784602214\Asus.CertificateValidation.2022.1728.641.AutoIt3.exe
C:\W45784602214\Asus.CertificateValidation.2022.1728.641.AutoIt3.log
```

Files used for persistent infection:

SHA256 hash: 237d1bca6e056df5bb16a1216a434634109478f882d3b1d58344c801d184f95d

- File size: 893,608 bytes
- File location: C:\W45784602214\Asus.CertificateValidation.2022.1728.641.AutoIt3.exe
- File description: Windows EXE for AutoIt v3, not inherently malicious

SHA256 hash: e31658734d3e0de1d2764636d1b8726f0f8319b0e50b87e5949ec162ae1c0050

- File size: 246,116 bytes
- File location: C:\W45784602214\Asus.CertificateValidation.2022.1728.641.AutoIt3.log
- File description: Malicious data binary, AutoIt v3 compiled script run by above Windows EXE for AutoIt v3

Final words

A pcap of the infection traffic, the associated malware/artifacts, and the email that kicked off this infection are available here.

Brad Duncan
brad [at] malwre-traffic-analysis.net

Keywords: Astaroth Brazil Guildma Malspam
0 comment(s)

Top of page
×

Diary Archives