tweets/2022-01-17-IOCs-for-Astaroth-Guildma-infection.txt

github.com/pan-unit42/tweets/blob/master/2022-01-17-IOCs-for-Astaroth-Guildma-infection.txt

pan-unit42

pan-unit42/**tweets**

4 Contributors | 0 Issues | 70 Stars | 15 Forks

2022-01-17 (MONDAY) - BRAZIL EMAIL PUSHING ASTAROTH/GUILDMA MALWARE
EMAIL HEADERS:
Received: from 46.148.234[.]126 (EHLO brasilirib07.iribfinanceiroorgbrasil[.]cloud)
by [recipient's mail server] with SMTPs
(version=TLS1_3 cipher=TLS_AES_128_GCM_SHA256);
Mon, 17 Jan 2022 19:31:47 +0000
Received: by brasilirib07.iribfinanceiroorgbrasil[.]cloud (Postfix, from userid 33)
id E89FC12E8AAD; Mon, 17 Jan 2022 16:27:38 -0300 (-03)
To: [recipient's email address]
Subject: Referente ao Pedido-6569RWW6A5C - 3NA7P12P92FDTE5I9H13G0FNZIR1I
MIME-Version: 1.0

From: Silvia Monteiro - DPT.F.D.NFe <envionotafiscal426@silvia.onmicrosoft.com>

Date: Mon, 17 Jan 2022 16:27:38 -0300

Reply-To: envionotafiscal426@silvia.onmicrosoft.com

LINK FROM EMAIL:

- hxxp://is[.]gd/Oc6aNo/M23DELDYZ1LElZiMrK/Z0AY20k2D2/

TRAFFIC FOR INITIAL ZIP ARCHIVE:

- 104.21.86.54 port 80 - y7iar15iowe.netirib[.]one - domain hosting zip archive

- zeb.mi.imati.cnr[.]it - legitimate domain generating traffic caused by domain hosting zip archive

TRAFFIC GENERATED BY CONTENTS OF ZIP ARCHIVE:

- 104.21.48.111 port 80 - 49oujr.elthalion[.]cfd - GET /?1/

- 172.67.194[.]164 port 80 - 1svdca3awt.reizorandir[.]sbs - HEAD /?62056502781677888

- 172.67.194[.]164 port 80 - 1svdca3awt.reizorandir[.]sbs - GET /?62056502781677888

- 172.67.194[.]164 port 80 - 1svdca3awt.reizorandir[.]sbs - HEAD /?56861426256676731

- 172.67.194[.]164 port 80 - 1svdca3awt.reizorandir[.]sbs - GET /?56861426256676731

- 172.67.194[.]164 port 80 - 1svdca3awt.reizorandir[.]sbs - HEAD /?35182482159686492

- 172.67.194[.]164 port 80 - 1svdca3awt.reizorandir[.]sbs - GET /?35182482159686492

- 172.67.194[.]164 port 80 - 1svdca3awt.reizorandir[.]sbs - HEAD /?69258597556636986

- 172.67.194[.]164 port 80 - 1svdca3awt.reizorandir[.]sbs - GET /?69258597556636986

- 172.67.194[.]164 port 80 - 1svdca3awt.reizorandir[.]sbs - HEAD /?60652078311677931

- 172.67.194[.]164 port 80 - 1svdca3awt.reizorandir[.]sbs - GET /?60652078311677931

- 172.67.194[.]164 port 80 - 1svdca3awt.reizorandir[.]sbs - HEAD /?42495298528678061

- 172.67.194[.]164 port 80 - 1svdca3awt.reizorandir[.]sbs - GET /?42495298528678061

- 172.67.194[.]164 port 80 - 1svdca3awt.reizorandir[.]sbs - HEAD /?68939448389637041

- 172.67.194[.]164 port 80 - 1svdca3awt.reizorandir[.]sbs - GET /?68939448389637041

- hundreds of DNS queries to different domains following the same format ad the four used below

- 172.67.197[.]42 port 80 - d36c259d9ddee6a5075920479f3c30df.bihcreuomegscmedfuaggprjrjomosga[.]cf - POST /

- 104.21.76[.]154 port 80 - b1de04354c314704bffdcf6da5989fd7.bihcreuomegscmedfuaggprjrjomosga[.]cf - POST /

- 172.67.198[.]188 port 80 - e25fa991460f33251405b284f08b84b4.jfhobjjddhsrspocbcorushsgcjhmgsg[.]gq - POST /

- 104.21.44[.]107 port 80 - 4f7afe1492603307b978fbffb672156a.jfhobjjddhsrspocbcorushsgcjhmgsg[.]gq - POST /

FILES FROM AN INFECTED WINDOWS HOST:

- SHA256 hash: d55076ddb14bb738c21af1b6350cd071ec9a83bb26cf627ea403d8f482d912b3

- File size: 481 bytes

- File name: FFDADSIURE_637.11847.20547.zip

- File description: zip archive downloaded from link in the email

- SHA256 hash: 4149af6393383f2d52407bb2ed0eee4649f3cacfd8b2d18967e6c2a4fd5078a0

- File size: 338 bytes

- File name: FFDADSIURE_.764.004378.96425?.cmd

- File description: batch script extracted from above zip archive

- SHA256 hash: b03f5df4eb85bf5af00edab4fa5cce11abcb75e980f31e434fd957b86428d631

- File size: 110 bytes

- File location: C:\Users\Public\Videos\ks9.Hta

- File description: HTML script dropped after running above batch script

- SHA256 hash:
9f0568fd4af722756a30ead152d90db4c38f06ae01cdb6e5ff7696007b25015a

- File size: 1,697 bytes

- File location: C:\Users\[username]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\winupdate.setup989dedbb0212.lnk

- File description: Windows shortcut used to keep the infection persistent

COMMAND RUN BY ABOVE WINDOWS SHORTCUT:

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -windowstyle hidden -Command C:\Windows\Temp\bhriwgjtvqazbeciqbmivay37695086602\setupcl?.exe C:\Windows\Temp\bhriwgjtvqazbeciqbmivay37695086602\tty

NOTABLE FILES AT
C:\WINDOWS\TEMP\BHRIWGJTVQAZBECIQBMIVAY37695086602\

- SHA256 hash:
739b2dd012ea183895cc01116906f339c9aa1c0baabf6f22c8e59e25a0c12917

- File size: 211,456 bytes

- File location: C:\Windows\system32\bitsadmin.exe

- File location: C:\Windows\Temp\bhriwgjtvqazbeciqbmivay37695086602\out.exe

- File description: Copy of legitimate system file from C:\Windows\system32\bitsadmin.exe

- Note: Not malicious, but utilized during this infection

- SHA256 hash:
b712286d4d36c74fa32127f848b79cfb857fdc2b1c84bbbee285cf34752443a2

- File size: 932,223 bytes

- File location: C:\Windows\Temp\bhriwgjtvqazbeciqbmivay37695086602\sqlite3.dll

- File description: Legitimate DLL for SQLite version 3.30.1

- Note: Not malicious, but utilized during this infection

- SHA256 hash:
237d1bca6e056df5bb16a1216a434634109478f882d3b1d58344c801d184f95d

- File size: 893,608 bytes

- File location: C:\Windows\Temp\bhriwgjtvqazbeciqbmivay37695086602\setupcl?.exe

- File description: Copy of AutoIt3.exe version 3.3.14.5

- Note 1: Not malicious, but utilized during this infection

- Note 2: AutoIt v3 is a freeware BASIC-like scripting language designed for automating the Windows GUI and general scripting.

- SHA256 hash:
841c97fdd8b434be673d22df68a378913800ab089a53c335221d63fa95caa52a

- File size: 28,006 bytes

- File location: C:\Windows\Temp\bhriwgjtvqazbeciqbmivay37695086602\ttx

- File description: malicious binary, AutoIt v3 compiled script

- SHA256 hash:
485ed71cf4a39221d57656cb9f8c3fe87210e8a7b4de053611febea84a8a5d97

- File size: 27,864 bytes

- File location: C:\Windows\Temp\bhriwgjtvqazbeciqbmivay37695086602\tty

- File description: malicious binary, AutoIt v3 compiled script

- SHA256 hash:
560498979df4664e3d9aafc72504014da2d0dcf7480a8ea051c443313ff0e2df

- File size: 1,387,680 bytes

- File location: C:\Windows\Temp\bhriwgjtvqazbeciqbmivay37695086602\dart.dll

- File type: ASCII text (Base64 string, twice encoded), not malicious unless decoded

- SHA256 hash:
6a94418da55c81aeea4bf4d0d888a05c6ce67d2d18b417c4296851ceaa67c516

- File size: 1,824,304 bytes

- File location: C:\Windows\Temp\bhriwgjtvqazbeciqbmivay37695086602\darts.dll

- File type: ASCII text (Base64 string, twice encoded), not malicious unless decoded

- SHA256 hash:
20ed67c588295a375d220f9557a0a7b798c9cc21181798c8f0e6d4f0d35049db

- File size: 4,210,154 bytes

- File location: C:\Windows\Temp\bhriwgjtvqazbeciqbmivay37695086602\log33.dll

- File description: Encoded binary, XOR-ed with hex string
994C2693C964B2592C168B45A25128140A0502010000000000000000000000000, not malicious unless decoded

- SHA256 hash:
5d82afd889fd5af9485f3816a81c90c9c3b321a35ec20504fd2868e5e6428ce0

- File size: 780,569 bytes

- File description: malicious DLL decoded from dart.dll

- File type: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows

- SHA256 hash:
79bba1f2f78495031be02c85daf25ff9f586013de148a2cb6ca68bcdaa1e8485

- File size: 1,026,169 bytes

- File description: malicious DLL decoded from darts.dll

- File type: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows

- SHA256 hash:
4605553f18de62be3a13e1661d9a8457ebc33f6730bc898c03792fee0da56763

- File size: 4,210,154 bytes

- File description: malicious DLL decoded from log33.dll

- File type: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows