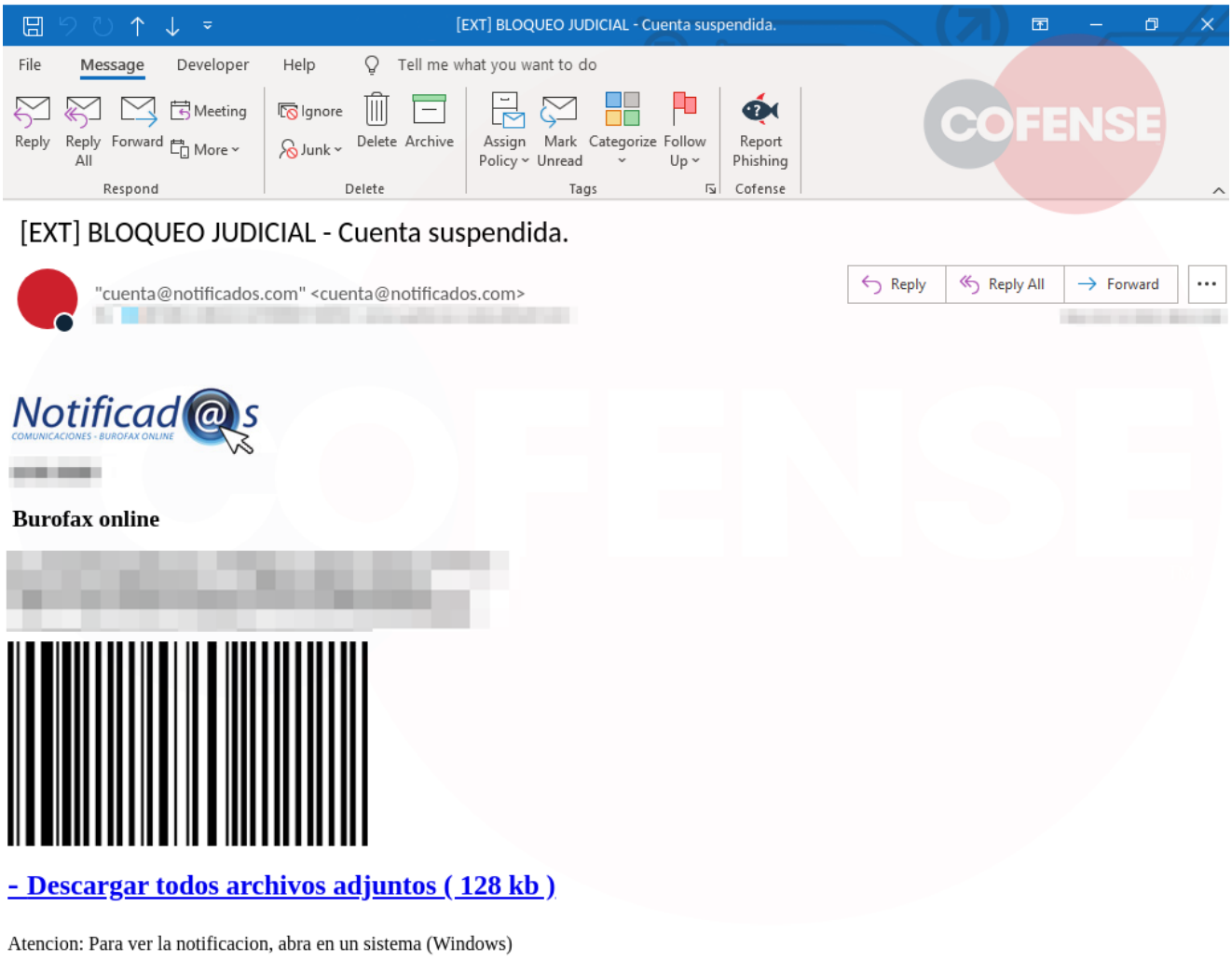
AutoHotKey Leveraged by Metamorfo/Mekotio Banking Trojan

cofense.com/blog/autohotkey-banking-trojan/

By Cofense

March 11, 2021



Phish Found in Environments Protected by SEGs

Proofpoint

FireEye ETP

Microsoft EOP

Trend Micro

By Elmer Hernandez, Cofense Phishing Defense Center

The Cofense Phishing Defense Center (PDC) has observed banking Trojans abusing AutoHotKey (AHK) and the AHK compiler to evade detection and steal users' information. In this post we take a brief look at the case of Mekotio, also known as Metamorfo, a banking Trojan with Latin American origins that is now expanding its reach to victims across Europe.

Phishing Email

Figures 1 and 2 are two example emails sent as the campaign's first step, both targeting Spanish users. Figure 2 is a simple request to download a password-protected file and is devoid of context. While Figure 1 is a more elaborate spoofed notification about pending legal documents, with a link that downloads a ZIP file.

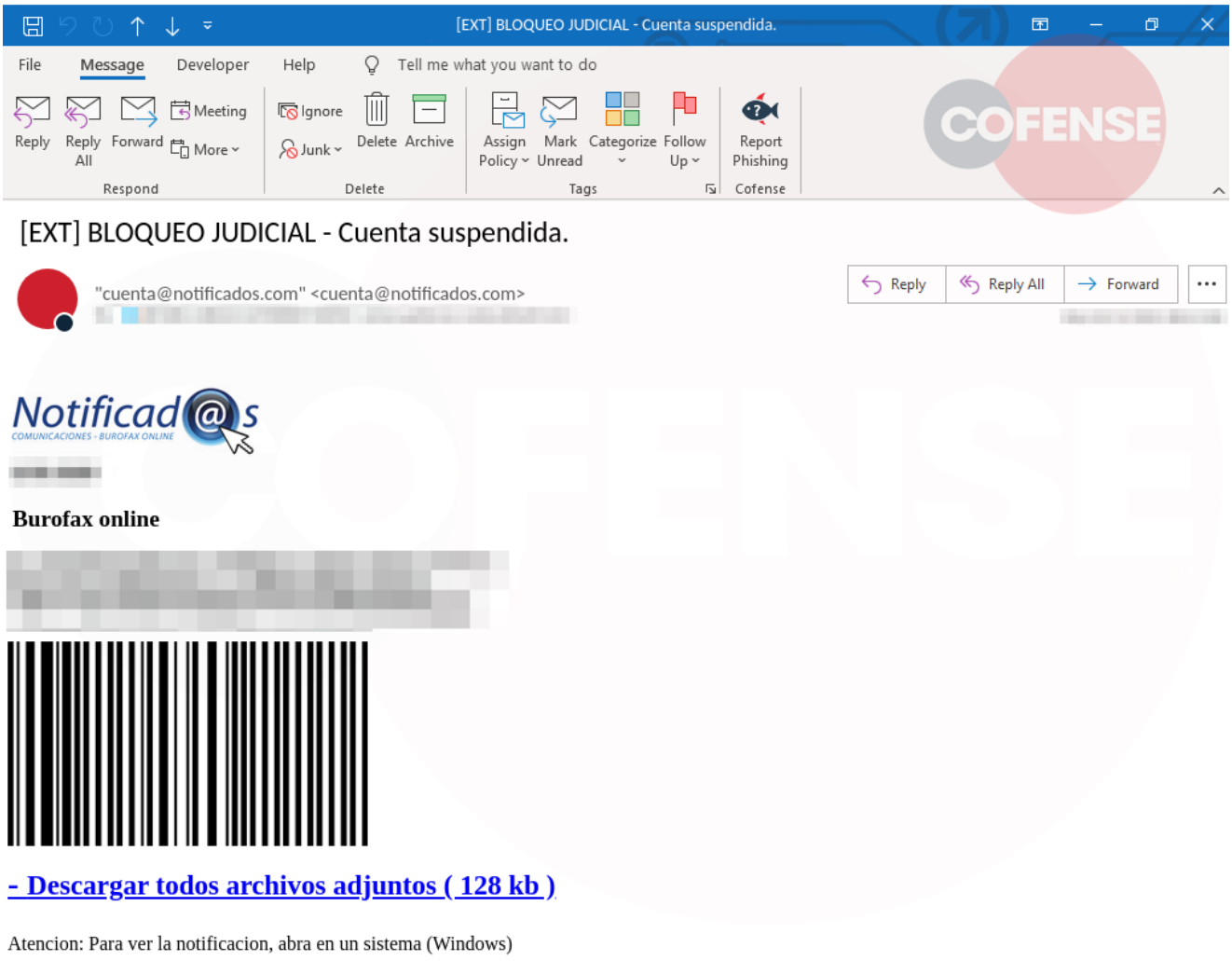


Figure 1 – Email 1

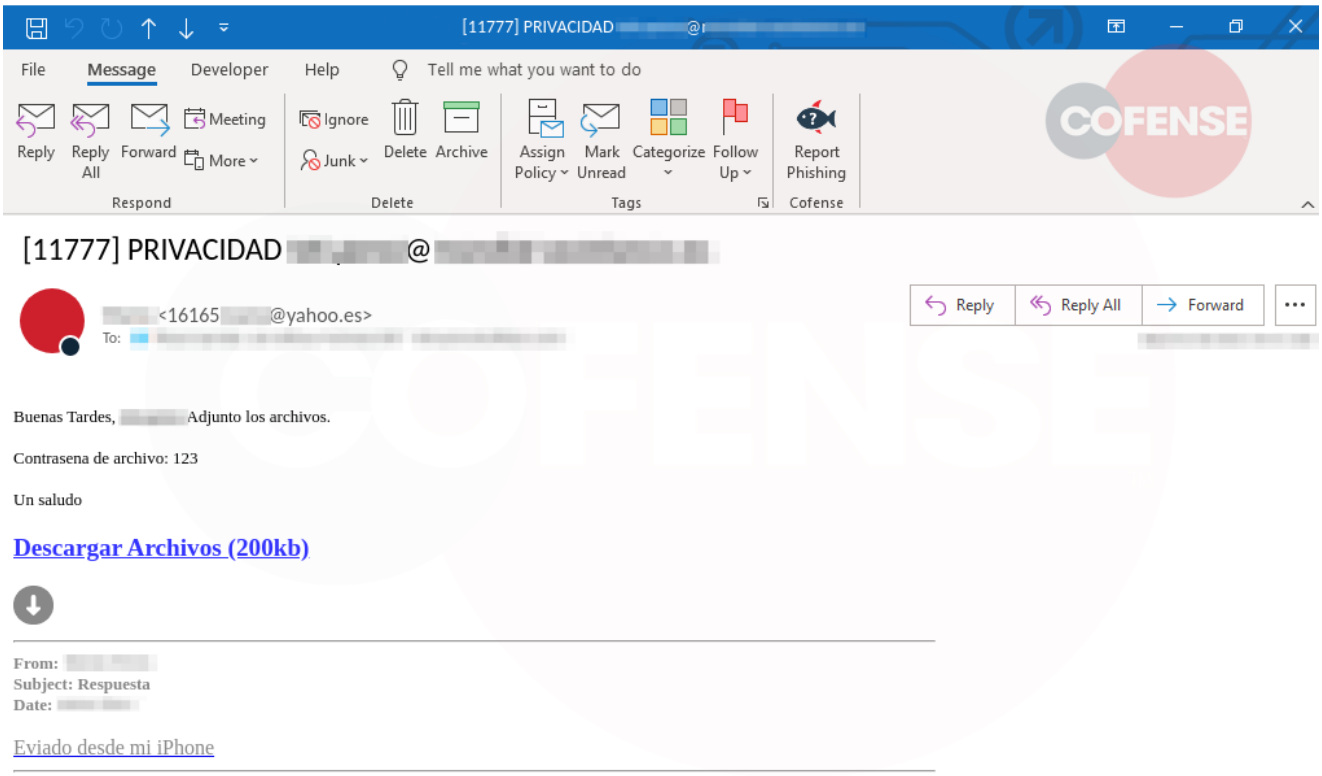


Figure 2 – Email 2

Delivery: Malicious MSI and Finger Commands

The PDC encountered two main mechanisms delivering the payload. In the first instance there is a ZIP file containing an MSI file that includes a malicious domain harboring 32 and 64-bit versions of a second ZIP file (Figure 3).

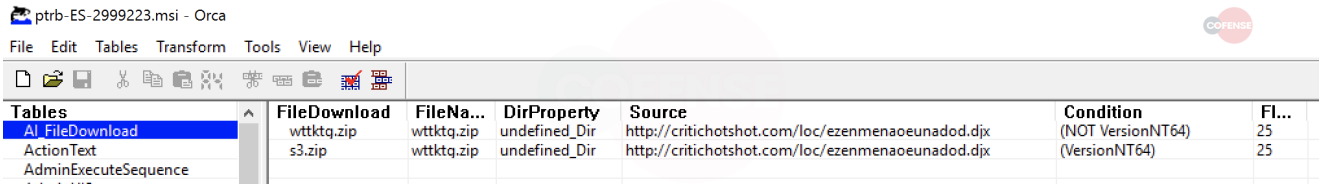


Figure 3 – Payload Domain

The Custom Actions table of these MSI files confirms the malicious intent. This table enables the incorporation of custom code to the installation package and is often abused by attackers. Figure 4 shows an action titled “dqidwlCTIewiuap” containing obfuscated JavaScript. The JavaScript is responsible for downloading the correct version of the ZIP file from the payload site, unzipping its contents, renaming and placing it into a new randomly named folder.

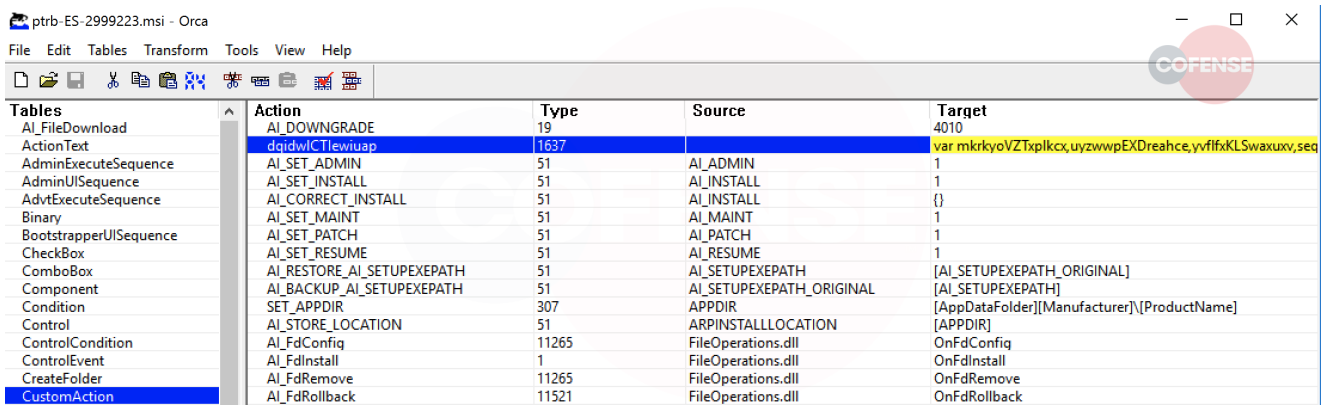


Figure 4 – Custom Actions Table

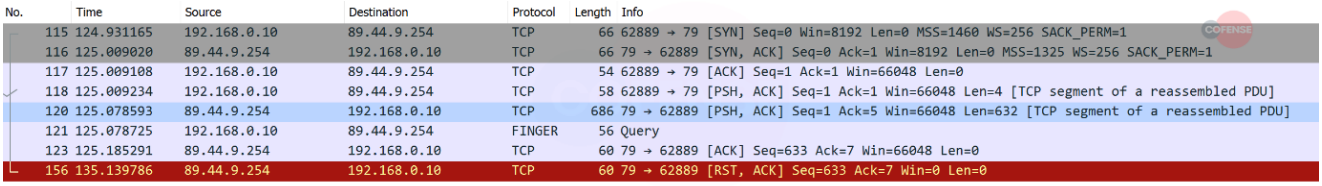
Figure 5 – Obfuscated JavaScript

In the second scenario the original ZIP file drops an LNK or shortcut file containing a malicious Finger command. Finger.exe is a native Windows command that allows the retrieval of information about a remote user.

Figure 6 shows the malicious Finger query. The command contacts a server at 89[.]44[.]9[.]254 and displays the contents of a hosted file in a command shell. The file in question is a PowerShell script that will run in this shell.

Figure 6 – Finger Command

Figures 7 and 8 show the TCP stream with the Finger server and the PowerShell script sent by it. The script carries out similar actions to the MSI: it downloads a ZIP file, renames it, copies it to a newly created folder and unzips it there.



No.	Time	Source	Destination	Protocol	Length	Info
115	124.931165	192.168.0.10	89.44.9.254	TCP	66	62889 → 79 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
116	125.009020	89.44.9.254	192.168.0.10	TCP	66	79 → 62889 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1325 WS=256 SACK_PERM=1
117	125.009108	192.168.0.10	89.44.9.254	TCP	54	62889 → 79 [ACK] Seq=1 Ack=1 Win=66048 Len=0
118	125.009234	192.168.0.10	89.44.9.254	TCP	58	62889 → 79 [PSH, ACK] Seq=1 Ack=1 Win=66048 Len=4 [TCP segment of a reassembled PDU]
120	125.078593	89.44.9.254	192.168.0.10	TCP	686	79 → 62889 [PSH, ACK] Seq=1 Ack=5 Win=66048 Len=632 [TCP segment of a reassembled PDU]
121	125.078725	192.168.0.10	89.44.9.254	FINGER	56	Query
123	125.185291	89.44.9.254	192.168.0.10	TCP	60	79 → 62889 [ACK] Seq=633 Ack=7 Win=66048 Len=0
156	135.139786	89.44.9.254	192.168.0.10	TCP	60	79 → 62889 [RST, ACK] Seq=633 Ack=7 Win=0 Len=0

Figure 7 – TCP Stream

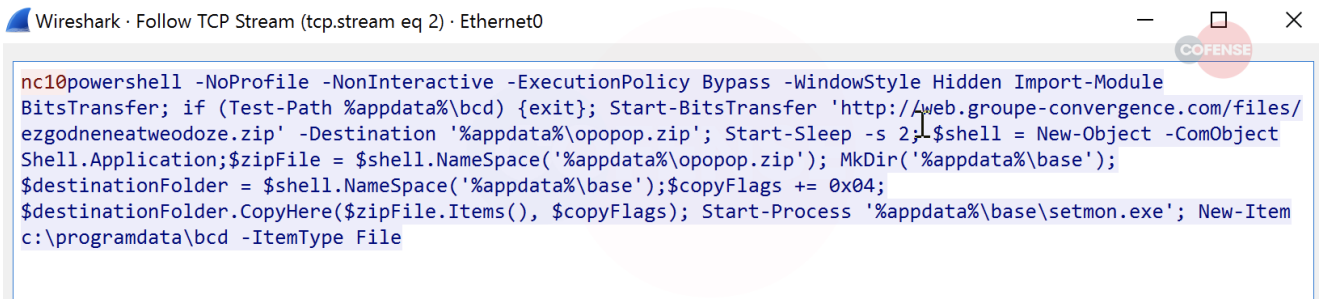


Figure 8 – PowerShell Script

The PDC also saw both tactics combined in at least one case, by incorporating the malicious Finger command directly into the MSI Custom Actions table (Figure 9).

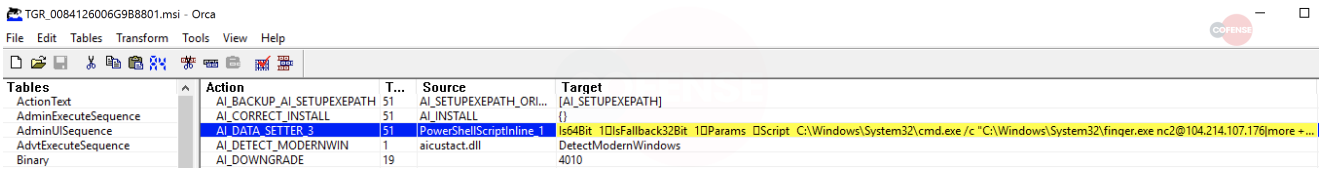


Figure 9 – Finger Command Within MSI

AutoHotKey and Mekotio

This second ZIP file contains three files: the legitimate AHK compiler executable (.exe), a malicious AHK script (.ahk) and the Mekotio banking Trojan (.dll). AHK is a scripting language for Windows originally developed to create keyboard shortcuts (i.e. hot keys). In the example below (Figure 10), all files were dropped in C:\\ProgramData\{random name}.

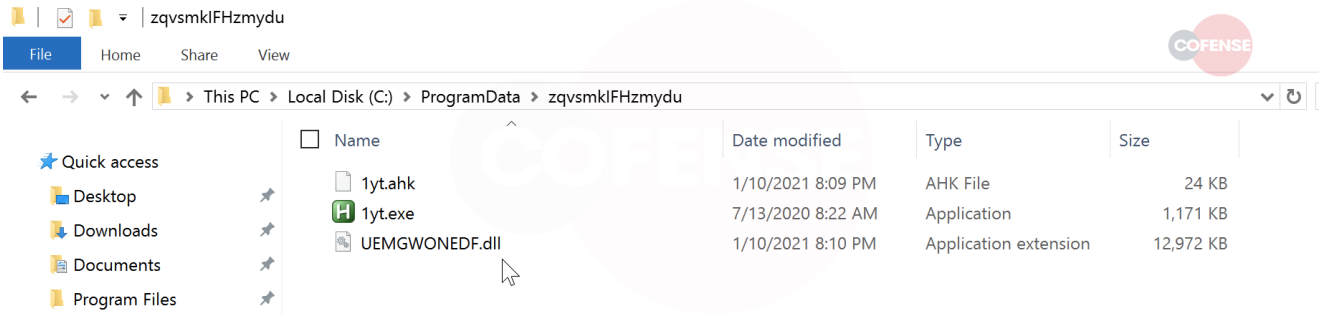


Figure 10 – Dropped Files

The execution chain can be summarized in the following way: before exiting, the MSI or PowerShell script will run the AHK compiler, the AHK compiler will execute the AHK script and the AHK script will load Mekotio into the AHK compiler memory. We can verify this by taking a look at the loaded modules in Figure 11.

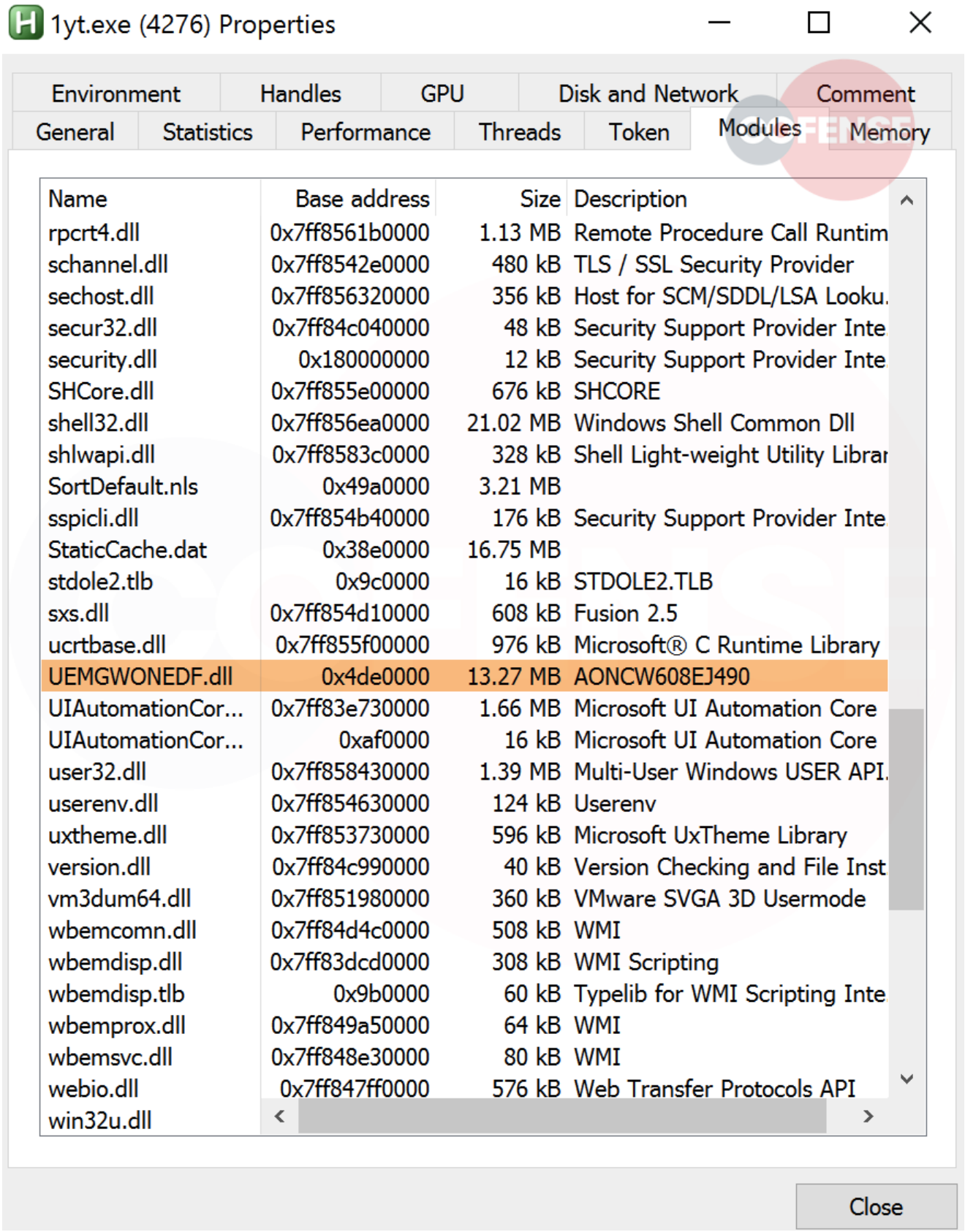


Figure 11 – Mekotio Loaded

Mekotio will then operate from within the AHK compiler process, using the signed binary as a front to make detection more difficult for endpoint solutions.

For persistence it drops copies of all three files in a new folder. It will then use a run key to initiate the execution chain every time the system restarts by executing the renamed copy of the AHK compiler.

```
[RegSetValue] lyt.exe:4276 > HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\(Default)  =  C:\Users\REM\vuU\gur.exe
```

Figure 12 – Run Key for AHK Compiler Copy "gur.exe"

Mekotio monitors browser activity looking for targeted banks. Figure 13 displays some of the targeted institutions in the form of strings in the AHK compiler process memory. We can see banks not only from Latin American, but from Spain, France and Portugal. Once it identifies a target, Mekotio is known to present the user with a fake version of the webpage.

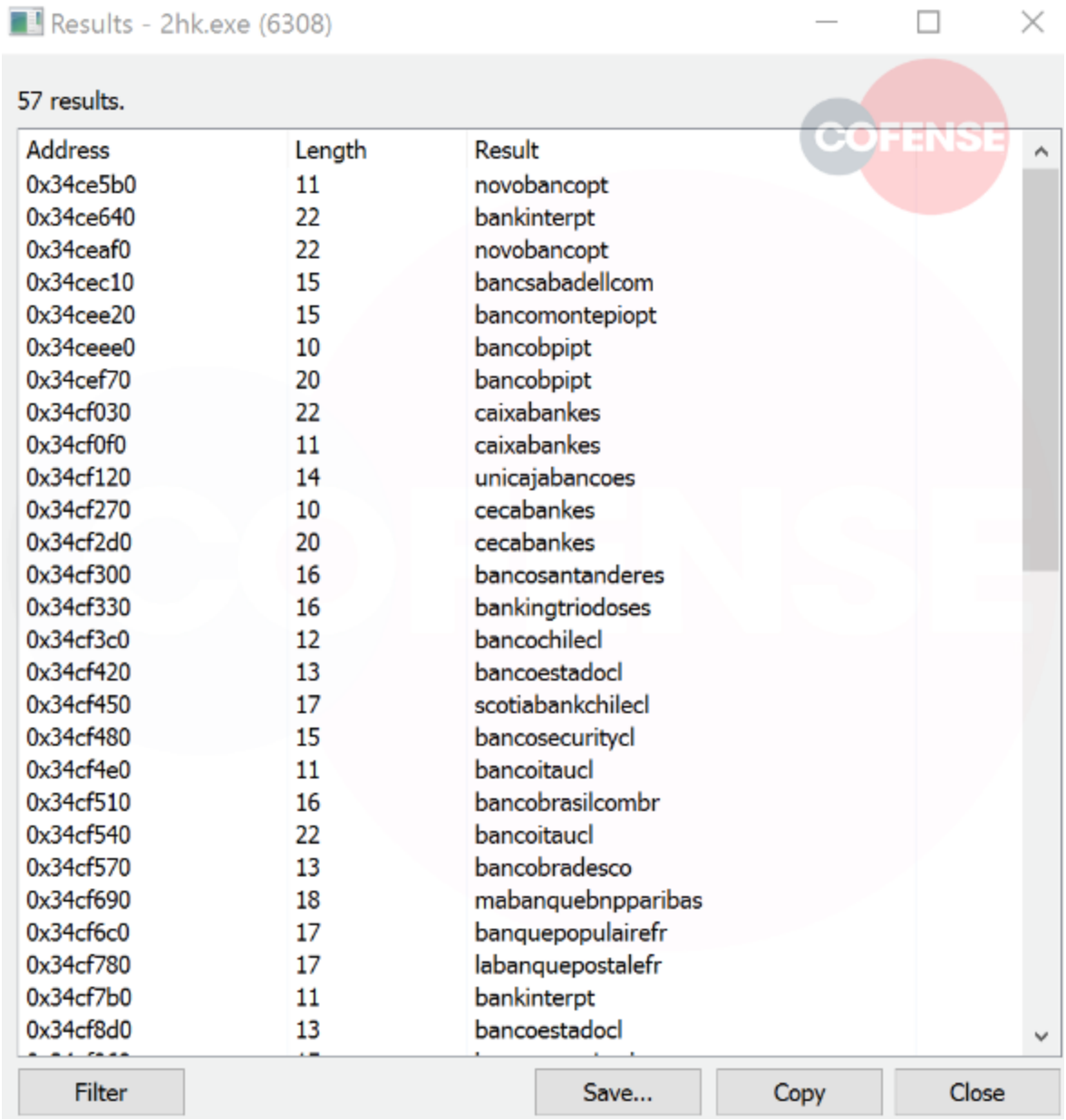


Figure 13 – Memory Strings

Mekotio disables specific registry browser values associated with password and form suggestions and autocompletion (Figure 14). This forces the user to type in sensitive information, even if they have it saved in their browser history, allowing the malware to capture credentials with its keylogging capabilities.

```
[RegSetValue] 1yt.exe:4276 > HKCU\SOFTWARE\Microsoft\Internet Explorer\Main\Use FormSuggest  =  No
[RegSetValue] 1yt.exe:4276 > HKCU\SOFTWARE\Microsoft\Internet Explorer\Main\FormSuggest Passwords  =  No
[RegSetValue] 1yt.exe:4276 > HKCU\SOFTWARE\Microsoft\Internet Explorer\Main\FormSuggest PW Ask  =  No
[RegSetValue] 1yt.exe:4276 > HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\AutoComplete\AutoSuggest  =  No
```

Figure 14 – Registry Values

The Trojan can also monitor Bitcoin addresses copied to the clipboard and replace them with one belonging to the attackers. Figures 15a to 15c show this process. As of this writing, this specific attacker address had a balance of 0.01957271 BTC, approximately USD $800 (Figure 16).

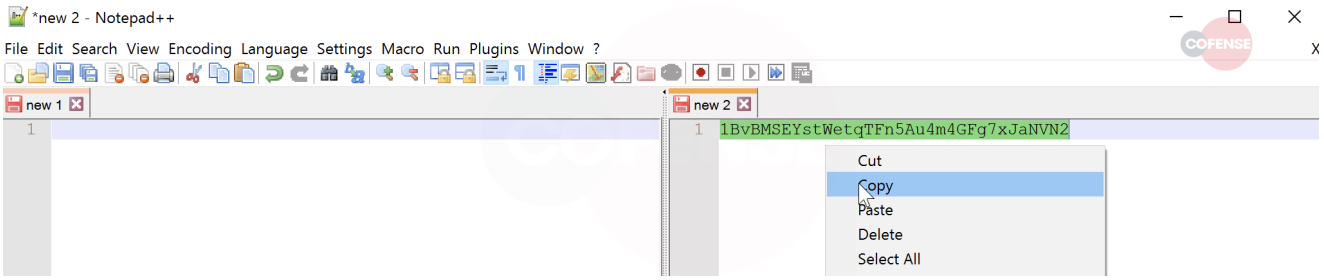


Figure 15a – Copying Example BTC Address

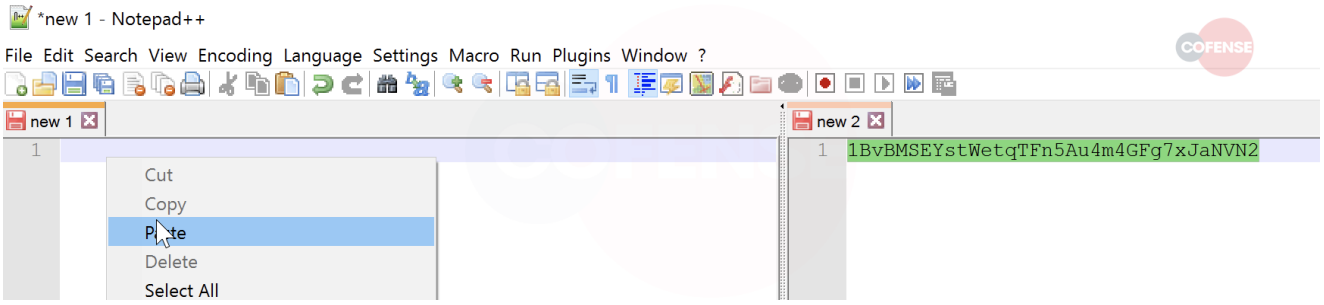


Figure 15b – Pasting Example BTC Address

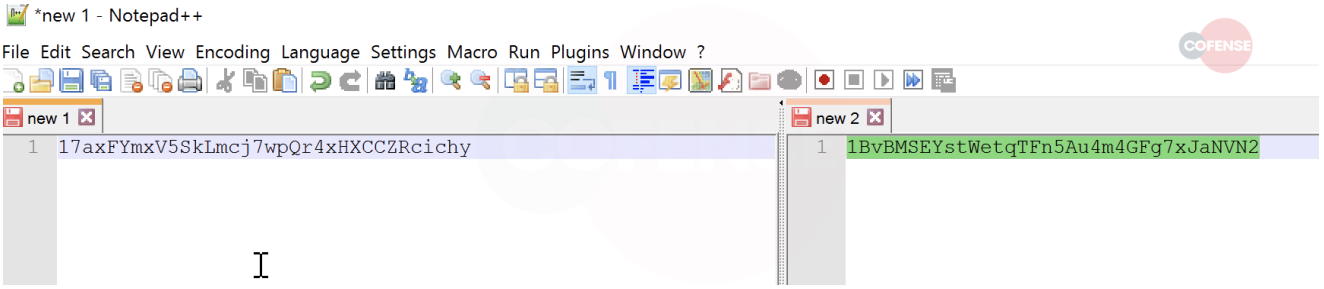


Figure 15c – BTC Address is replaced

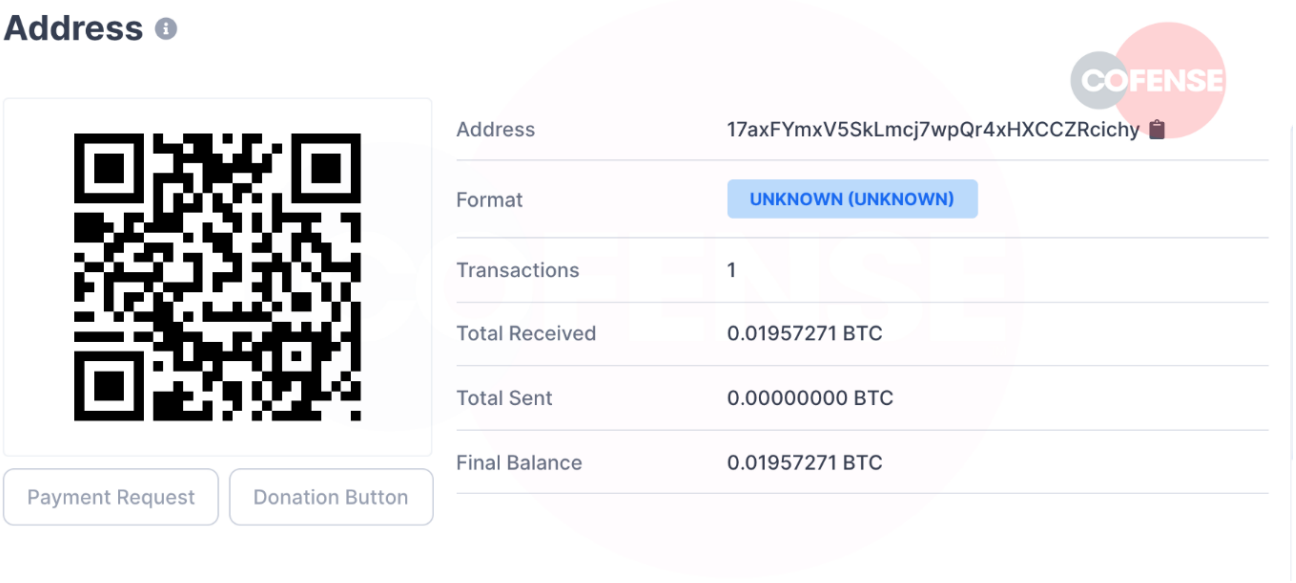


Figure 16 – BTC Balance

The above functionalities are neither exhaustive nor exclusive to Mekotio. The main takeaway is that legitimate binaries can be leveraged as a façade for malicious activity. Vigilance is key. If a file or process is not meant to be there, it's best to check.

Indicators of Compromise

Infection Domain	IP
hxxp://priyadarsiniculturalsociety[.]com//images/?hash=%email%	51[.]81[.]75[.]131
hxxp://hothiphopbeats[.]com//images/?hash=%email%	209[.]40[.]193[.]208
hXXp://www3[.]santoandre[.]sp[.]gov[.]br/assistencia/wp-folha/TGR	189[.]1[.]163[.]21

Payload Domain	IP
hxxp://critichotshot[.]com/loc/	162[.]255[.]118[.]194
hxxps://thaipoliticstoday[.]com/saudi-news-tq1vh/	172[.]67[.]181[.]248
hXXp://web[.]groupe-convergence[.]com/	213[.]186[.]33[.]69
hXXp://www[.]aralimp[.]com[.]br/wp-content/upgrade/TGR/SII_000492106006B8[.]zip	177[.]12[.]164[.]108
hXXp://umc24[.]club//wp-content/gallery/	217[.]160[.]0[.]235
hXXps://leopard-hunt[.]com//wp-content/userr/20AVW5RSJKV8948[.]zip	104[.]21[.]63[.]133 172[.]67[.]145[.]198

–	89[.]44[.]9[.]254
–	104[.]214[.]107[.]176

C2	IP
es[.]sslhermanos[.]com	45[.]147[.]229[.]128 45[.]147[.]231[.]119
hxxp://40[.]112[.]173[.]53/again/?oriudfjdfij88	40[.]112[.]173[.]53