More Data Exfiltration

Published: 2020-01-10. **Last Updated**: 2020-01-10 06:38:52 UTC
by Xavier Mertens (Version: 1)

2 comment(s)

Yesterday, I posted a quick analysis of a malicious document that exfiltrates data from the compromised computer[1]. Here is another found that also exfiltrate data. The malware is delivered in an ACE archive. This file format remains common in phishing campaigns because the detection rate is lower at email gateways (many of them can't handle the file format). The archive contains a PE file called 'Payment Copy.exe' (SHA256:88a6e2fd417d145b55125338b9f53ed3e16a6b27fae9a3042e187b5aa15d27aa). The payload is unknown on VT at this time.

The list of searched files and registry keys is interesting. Many credentials databases and files are tested by the malware. Here is a list of extracted paths:

```
%USERPROFILE%\AppData\Local\Google\Chrome\User Data\LOGIN DATA
%USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\4lddcdcq.hh3fwg7c.default\LOGINS.JSON
%USERPROFILE%\AppData\Local\TENCENT\QQBROWSER\USER DATA\DEFAULT\ENCRYPTEDSTORAGE
%USERPROFILE%\AppData\Roaming\OPERA SOFTWARE\OPERA STABLE\LOGIN DATA
%USERPROFILE%\AppData\Local\YANDEX\YANDEXBROWSER\USER DATA
%USERPROFILE%\AppData\Local\360CHROME\CHROME\USER DATA
%USERPROFILE%\AppData\Local\IRIDIUM\USER DATA
%USERPROFILE%\AppData\Local\COMODO\DRAGON\USER DATA
%USERPROFILE%\AppData\Local\MAPLESTUDIO\CHROMEPLUS\USER DATA
%USERPROFILE%\AppData\Local\CHROMIUM\USER DATA
%USERPROFILE%\AppData\Local\TORCH\USER DATA
%USERPROFILE%\AppData\Local\7STAR\7STAR\USER DATA
%USERPROFILE%\AppData\Local\AMIGO\USER DATA
%USERPROFILE%\AppData\Local\BRAVESOFTWARE\BRAVE-BROWSER\USER DATA
%USERPROFILE%\AppData\Local\CENTBROWSER\USER DATA
%USERPROFILE%\AppData\Local\CHEDOT\USER DATA
%USERPROFILE%\AppData\Local\COCCOC\BROWSER\USER DATA
%USERPROFILE%\AppData\Local\ELEMENTS BROWSER\USER DATA
%USERPROFILE%\AppData\Local\EPIC PRIVACY BROWSER\USER DATA
%USERPROFILE%\AppData\Local\KOMETA\USER DATA
%USERPROFILE%\AppData\Local\ORBITUM\USER DATA
%USERPROFILE%\AppData\Local\SPUTNIK\SPUTNIK\USER DATA
%USERPROFILE%\AppData\Local\UCOZMEDIA\URAN\USER DATA
%USERPROFILE%\AppData\Local\VIVALDI\USER DATA
%USERPROFILE%\AppData\Local\CATALINAGROUP\CITRIO\USER DATA
%USERPROFILE%\AppData\Local\LIEBAO\USER DATA
%USERPROFILE%\AppData\Local\FENRIR INC\SLEIPNIR5\SETTING\MODULES\CHROMIUMVIEWER
%USERPROFILE%\AppData\Local\QIP SURF\USER DATA
%USERPROFILE%\AppData\Local\COOWON\COOWON\USER DATA
```

```
%USERPROFILE%\AppData\Roaming\NETGATE TECHNOLOGIES\BLACKHAWK\PROFILES.INI
%USERPROFILE%\AppData\Roaming\8PECXSTUDIOS\CYBERFOX\PROFILES.INI
%USERPROFILE%\AppData\Roaming\K-MELEON\PROFILES.INI
%USERPROFILE%\AppData\Roaming\Mozilla\ICECAT\PROFILES.INI
%USERPROFILE%\AppData\Roaming\COMODO\ICEDRAGON\PROFILES.INI
%USERPROFILE%\AppData\Roaming\MOONCHILD PRODUCTIONS\PALE MOON\PROFILES.INI
%USERPROFILE%\AppData\Roaming\WATERFOX\PROFILES.INI
%USERPROFILE%\AppData\Local\FALKON\PROFILES\PROFILES.INI
Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password
%USERPROFILE%\AppData\Roaming\THUNDERBIRD\PROFILES.INI
%USERPROFILE%\AppData\Local\VIRTUALSTORE\PROGRAM FILES\FOXMAIL\MAIL
%USERPROFILE%\AppData\Local\VIRTUALSTORE\PROGRAM FILES (X86)\FOXMAIL\MAIL
%USERPROFILE%\AppData\Roaming\OPERA MAIL\OPERA MAIL\WAND.DAT
%USERPROFILE%\AppData\Roaming\POCOMAIL\ACCOUNTS.INI
%USERPROFILE%\AppData\Roaming\THE BAT!
%USERPROFILE%\AppData\Roaming\POSTBOX\PROFILES.INI
%USERPROFILE%\AppData\Roaming\CLAWS-MAIL
%USERPROFILE%\AppData\Roaming\CLAWS-MAIL\CLAWSRC
%USERPROFILE%\AppData\Local\Temp\FOLDER.LST
%USERPROFILE%\AppData\Roaming\TRILLIAN\USERS\GLOBAL\ACCOUNTS.DAT
%USERPROFILE%\AppData\Roaming\PSI\PROFILES
%USERPROFILE%\AppData\Roaming\PSI+\PROFILES
%USERPROFILE%\AppData\Roaming\IPSWITCH\WS_FTP\SITES\WS_FTP.INI
%USERPROFILE%\AppData\Roaming\COREFTP\SITES.IDX
C:\FTP NAVIGATOR\FTPLIST.TXT
%USERPROFILE%\AppData\Roaming\FLASHFXP\3QUICK.DAT
%USERPROFILE%\AppData\Roaming\SMARTFTP\CLIENT 2.0\FAVORITES\QUICK CONNECT
C:\CFTP\FTPLIST.TXT
%USERPROFILE%\AppData\Roaming\FTPGETTER\SERVERS.XML
C:\Program Files (x86)\JDOWNLOADER\CONFIG\DATABASE.SCRIPT
%USERPROFILE%\AppData\Local\Temp\LOG.TMP
\REGISTRY\USER\S-1-5-21-2529703413-2662079939-3113469119-500\Software\Microsoft\Windows NT\CurrentVersion
\REGISTRY\USER\S-1-5-21-2529703413-2662079939-3113469119-500\Software\Aerofox\FoxmailPreview
\REGISTRY\USER\S-1-5-21-2529703413-2662079939-3113469119-500\Software\Aerofox\Foxmail\V3.1
\REGISTRY\USER\S-1-5-21-2529703413-2662079939-3113469119-500\Software\IncrediMail\Identities
\REGISTRY\USER\S-1-5-21-2529703413-2662079939-3113469119-500\Software\Qualcomm\Eudora\CommandLine
\REGISTRY\USER\S-1-5-21-2529703413-2662079939-3113469119-500\Software\RimArts\B2\Settings
\REGISTRY\USER\S-1-5-21-2529703413-2662079939-3113469119-500\Software\OpenVPN-GUI\configs
\REGISTRY\USER\S-1-5-21-2529703413-2662079939-3113469119-500\SOFTWARE\Martin Prikryl\WinSCP 2\Sessions
\REGISTRY\USER\S-1-5-21-2529703413-2662079939-3113469119-500\Software\FTPWare\COREFTP\Sites
\REGISTRY\USER\S-1-5-21-2529703413-2662079939-3113469119-500\Software\DownloadManager\Passwords
```

Who said that the browser market is restricted to IE, Firefox, Chrome, Safari & Opera?

Another tool used by the malware attracted my attention: 'plutil.exe'. It's a tool that is part of the Apple Application Support 32-bit program. This tool is completely legit and is available when you install an Apple software on your Windows system (Safari, iCloud, ...). Its purpose is to process Properly List files[2] used by Apple.

```
C:\Program Files (x86)\Common Files\Apple\Apple Application Support\plutil.exe -convert xml1 -s -o \
   "%USERPROFILE%\AppData\Local\Temp\fixed_keychain.xml" \
   "%USERPROFILE%\AppData\Roaming\Apple Computer\Preferences\keychain.plist"
```

It could be a good idea to track access to these paths by uncommon process names (example via a Sysmon specific configuration)

[1] https://isc.sans.edu/forums/diary/Quick+Analyzis+of+another+Maldoc/25694/
[2]

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

Keywords: Exfiltration Malware

2 comment(s)

Comments

@Xme Did you find the IP/Domain that it was reporting back to?

Anonymous
Jan 10th 2020
4 years ago

Exfiltration to iris-center[.]ai

Anonymous
Jan 11th 2020
4 years ago

Login here to join the discussion.

Top of page

Diary Archives