

Shell-Health-Check ✓
Heinz/Harvey

Motiv

Emotet manifestiert sich häufig durch ausführbare Dateien im Windows-Benutzer-Profil.

EmoCheck v.0.0.2:

[Result]

Detected Emotet process.

[Emotet Process]

Process Name : mstask.exe

Process ID : 716

Image Path : C:\Users\[username]\AppData\Local\mstask.exe

Ansatz

Der Plan:

Nach ausführbaren Dateien in `c:\users\%USERNAME%` suchen (`findet-emo.sh` unter [Cygwin](#)), technische Details inkl. md5sum in eine Tabelle schreiben, diese gegen eine Whitelist prüfen.

Gegenstand

Hier geht ausschließlich darum, wie ich die Kommandozeile (erneut) lieben lernte, und welche neuen Funktionen bei bekannten Tools ich dabei entdeckt habe.

Shellcheck

ShellCheck is a GPLv3 tool that gives warnings and suggestions for bash/sh shell scripts

- <https://www.shellcheck.net/>
- <https://github.com/koalaman/shellcheck>

Shellcheck

ShellCheck Output

```
Line 143:
typeset -r ue=$'\xC3\xBC'
^-- SC2034: ue appears unused. Verify use (or export if used externally).

Line 144:
typeset -r oe=$'\xC3\xB6'
^-- SC2034: oe appears unused. Verify use (or export if used externally).

Line 145:
typeset -r ae=$'\xC3\xA4'
^-- SC2034: ae appears unused. Verify use (or export if used externally).

[...]

Line 293:
    read
    ^-- SC2162: read without -r will mangle backslashes.

Line 358:
if [ $Verbose -gt 0 ]
    ^-- SC2086: Double quote to prevent globbing and word splitting.

Did you mean: (apply this, apply all SC2086)
if [ "$Verbose" -gt 0 ]
```

find und md5sum

Header

```
$ echo -e "COMPUTERNAME\tUSERNAME\tNowDate\tNowTime\tPermissions\tHardlinks\tUser\tGroup\tSize\tModDate\tModTime\tStatusChgDate\tStatusChgTime\tAccessDate\tAccessTime\tName\tRelPath\tMD5sum" > R0776-kramski-20200325-111901-listing.tsv
```

Datei-Listing

```
$ find /home/kramski -type f \( -iname "*.BAT" -o -iname "*.CMD" [...] -o -iname "*.WSH" \) -printf "R0776\tkramski\t25.03.2020\t11:19:01\t%M\t%n\t%u\t%g\t%s\t%Tx\t%TX\t%Cx\t%CX\t%Ax\t%AX\t%f\t%P\t" -exec sh -c "md5sum '{} ' | cut -d ' ' -f 1" \; >> R0776-kramski-20200325-111901-listing.tsv
```

Funde

R0776-kramski-20200325-083148-listing.tsv - LibreOffice Calc

Datei Bearbeiten Ansicht Einfügen Format Vorlagen Tabelle Daten Extras Fenster Hilfe

fx Σ = COMPUTERNAME

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	COMPUTERNAME	USERNAME	NowDate	NowTime	Permissions	Hardlinks	User	Group	Size	ModDate	ModTime	StatusChgDate	StatusChgTime	AccessDate
2	R0776	kramski	25.03.2020	08:31:48	-wx----	2	kramski	Domain Users	16760	21.05.2019	16:51:42.4194639000	21.05.2019	16:51:42.6066747000	21.05.2019
3	R0776	kramski	25.03.2020	08:31:48	-wx----	2	kramski	Domain Users	167048	21.05.2019	16:51:07.0392098000	21.05.2019	16:51:13.9192067000	21.05.2019
4	R0776	kramski	25.03.2020	08:31:48	-wx----	2	kramski	Domain Users	2763448	21.05.2019	16:51:05.6663306000	21.05.2019	16:51:13.8880049000	21.05.2019
5	R0776	kramski	25.03.2020	08:31:48	-wx----	2	kramski	Domain Users	5738160	21.05.2019	16:51:04.9174874000	21.05.2019	16:51:13.8724040000	21.05.2019
6	R0776	kramski	25.03.2020	08:31:48	-wx----	2	kramski	Domain Users	1992888	21.05.2019	16:51:06.2591648000	21.05.2019	16:51:13.9036058000	21.05.2019
7	R0776	kramski	25.03.2020	08:31:48	-wx----	2	kramski	Domain Users	4278352	21.05.2019	16:51:06.8207972000	21.05.2019	16:51:13.9192067000	21.05.2019
8	R0776	kramski	25.03.2020	08:31:48	-wx----	2	kramski	Domain Users	241760	21.05.2019	16:51:08.6305016000	21.05.2019	16:51:14.1376193000	21.05.2019
9	R0776	kramski	25.03.2020	08:31:48	-wx----	2	kramski	Domain Users	16760	21.05.2019	16:51:42.4194639000	21.05.2019	16:51:42.6066747000	21.05.2019
10	R0776	kramski	25.03.2020	08:31:48	-wx----	2	kramski	Domain Users	241760	21.05.2019	16:51:08.6305016000	21.05.2019	16:51:14.1376193000	21.05.2019
11	R0776	kramski	25.03.2020	08:31:48	-wx----	2	kramski	Domain Users	167048	21.05.2019	16:51:07.0392098000	21.05.2019	16:51:13.9192067000	21.05.2019
12	R0776	kramski	25.03.2020	08:31:48	-wx----	2	kramski	Domain Users	2763448	21.05.2019	16:51:05.6663306000	21.05.2019	16:51:13.8880049000	21.05.2019
13	R0776	kramski	25.03.2020	08:31:48	-wx----	2	kramski	Domain Users	5738160	21.05.2019	16:51:04.9174874000	21.05.2019	16:51:13.8724040000	21.05.2019
14	R0776	kramski	25.03.2020	08:31:48	-wx----	2	kramski	Domain Users	1992888	21.05.2019	16:51:06.2591648000	21.05.2019	16:51:13.9036058000	21.05.2019
15	R0776	kramski	25.03.2020	08:31:48	-wx----	2	kramski	Domain Users	4278352	21.05.2019	16:51:06.8207972000	21.05.2019	16:51:13.9192067000	21.05.2019
16	R0776	kramski	25.03.2020	08:31:48	-wx----	1	kramski	Domain Users	7930056	11.07.2018	12:30:29.3345988000	10.12.2018	16:45:57.5881352000	11.07.2018
17	R0776	kramski	25.03.2020	08:31:48	-wx----	1	kramski	Domain Users	3398856	11.07.2018	12:31:02.8967609000	10.12.2018	16:45:57.6505372000	11.07.2018
18	R0776	kramski	25.03.2020	08:31:48	-wx----	1	kramski	Domain Users	2555592	11.07.2018	12:30:59.6880451000	10.12.2018	16:45:57.6973387000	11.07.2018
19	R0776	kramski	25.03.2020	08:31:48	-wx----	1	kramski	Domain Users	9478	12.02.2019	22:40:22.0000000000	03.04.2019	16:44:27.3133214000	03.04.2019
20	R0776	kramski	25.03.2020	08:31:48	-wx----	1	kramski	Domain Users	9487	12.02.2019	22:40:22.0000000000	03.04.2019	16:44:27.3173214000	03.04.2019
21	R0776	kramski	25.03.2020	08:31:48	-wx----	1	kramski	Domain Users	9487	12.02.2019	22:40:22.0000000000	03.04.2019	16:44:27.3223214000	03.04.2019
22	R0776	kramski	25.03.2020	08:31:48	-wx----	1	kramski	Domain Users	2363392	14.08.2018	08:37:56.7214390000	14.08.2018	08:37:56.7214390000	18.01.2019
23	R0776	kramski	25.03.2020	08:31:48	-wx----	1	kramski	Domain Users	125733	16.10.2019	08:40:21.6670839000	16.10.2019	08:40:21.6670839000	16.10.2019
24	R0776	kramski	25.03.2020	08:31:48	-wx----	1	kramski	Domain Users	1198055	18.07.2017	16:56:24.4603995000	18.07.2017	16:56:32.5708915000	10.12.2018
25	R0776	kramski	25.03.2020	08:31:48	-wx----	1	kramski	Domain Users	1840655	13.02.2019	12:11:21.0932272000	13.02.2019	12:15:04.1756272000	13.02.2019
26	R0776	kramski	25.03.2020	08:31:48	-wx----	1	kramski	Domain Users	5095286	13.02.2019	12:12:43.3832272000	13.02.2019	12:15:04.2224272000	13.02.2019
27														
28														
29														

Suchen

Tabelle 1 von 1 Standard Deutsch (Deutschland) Mittelwert; Summe: 0 100 %

Funde

R0776-kramski-20200325-083148-listing.tsv - LibreOffice Calc

Datei Bearbeiten Ansicht Einfügen Format Vorlagen Tabelle Daten Extras Fenster Hilfe

A1 f_x Σ = COMPUTERNAME

	O	P	Q	R
1	AccessTime	Name	RelPath	MD5sum
2	16:51:42.6066747000	Get32.exe	AppData/Local/Apps/2.0/NGB1QA48.NXM/92CGJK0X.M47/micr...exe_1975b8453054a2b5_0010.0	699cfc000e743fc67726d7ade39197
3	16:51:13.9192067000	psping.exe	AppData/Local/Apps/2.0/NGB1QA48.NXM/92CGJK0X.M47/micr...exe_1975b8453054a2b5_0010.0	dce4801c688e0567c025ae57785ff66f
4	16:51:13.8880049000	CalCheck.exe	AppData/Local/Apps/2.0/NGB1QA48.NXM/92CGJK0X.M47/micr...exe_1975b8453054a2b5_0010.0	404b1af996b9745a33f747aea0c7e17d
5	16:51:13.8724040000	mrmapi.exe	AppData/Local/Apps/2.0/NGB1QA48.NXM/92CGJK0X.M47/micr...exe_1975b8453054a2b5_0010.0	2b09abefdc84d46d10c2a83b0870f3d4
6	16:51:13.9036058000	CalCheck.exe	AppData/Local/Apps/2.0/NGB1QA48.NXM/92CGJK0X.M47/micr...exe_1975b8453054a2b5_0010.0	b89e04782913276215b3a9f4c3e44a75
7	16:51:13.9036058000	mrmapi.exe	AppData/Local/Apps/2.0/NGB1QA48.NXM/92CGJK0X.M47/micr...exe_1975b8453054a2b5_0010.0	377ebcfcfd36b08865fff053b1f81d45
8	16:51:14.1376193000	Microsoft.Sara.exe	AppData/Local/Apps/2.0/NGB1QA48.NXM/92CGJK0X.M47/micr...sara_31bf3856ad364e35_0010.0	d3c7318e78e2a681a14014ae8121df87
9	16:51:42.6066747000	Get32.exe	AppData/Local/Apps/2.0/NGB1QA48.NXM/92CGJK0X.M47/micr...tion_1975b8453054a2b5_0010.0	699cfc000e743fc67726d7ade39197
10	16:51:14.1376193000	Microsoft.Sara.exe	AppData/Local/Apps/2.0/NGB1QA48.NXM/92CGJK0X.M47/micr...tion_1975b8453054a2b5_0010.0	d3c7318e78e2a681a14014ae8121df87
11	16:51:13.9192067000	psping.exe	AppData/Local/Apps/2.0/NGB1QA48.NXM/92CGJK0X.M47/micr...tion_1975b8453054a2b5_0010.0	dce4801c688e0567c025ae57785ff66f
12	16:51:13.8880049000	CalCheck.exe	AppData/Local/Apps/2.0/NGB1QA48.NXM/92CGJK0X.M47/micr...tion_1975b8453054a2b5_0010.0	404b1af996b9745a33f747aea0c7e17d
13	16:51:13.8724040000	mrmapi.exe	AppData/Local/Apps/2.0/NGB1QA48.NXM/92CGJK0X.M47/micr...tion_1975b8453054a2b5_0010.0	2b09abefdc84d46d10c2a83b0870f3d4
14	16:51:13.9036058000	CalCheck.exe	AppData/Local/Apps/2.0/NGB1QA48.NXM/92CGJK0X.M47/micr...tion_1975b8453054a2b5_0010.0	b89e04782913276215b3a9f4c3e44a75
15	16:51:13.9036058000	mrmapi.exe	AppData/Local/Apps/2.0/NGB1QA48.NXM/92CGJK0X.M47/micr...tion_1975b8453054a2b5_0010.0	377ebcfcfd36b08865fff053b1f81d45
16	12:22:48.5935399000	MailStoreClient.exe	AppData/Local/MailStore Client Launcher/11.1.0.13498-ee55486122cb9c56aa11d6d6ff3c3475571d	8202238b6a4290770e2e61bc07150900
17	12:13:33.7322724000	MailStoreMapiClient_x64.exe	AppData/Local/MailStore Client Launcher/11.1.0.13498-ee55486122cb9c56aa11d6d6ff3c3475571d	1d646375c21c0ff54674a8697166d5f9
18	12:13:33.6846491000	MailStoreMapiClient_x86.exe	AppData/Local/MailStore Client Launcher/11.1.0.13498-ee55486122cb9c56aa11d6d6ff3c3475571d	4bae0691512ce11b7b1bc6cd1a1eb10
19	16:44:27.3113214000	ldap.bat	AppData/Local/Temp/jetty-0.0.0.0-8074-onepoint.war_-any-7644675788614491259.dir/webapp/scr	8836b7d4b4ed97825cf3dd81b56fee68
20	16:44:27.3163214000	repExport.bat	AppData/Local/Temp/jetty-0.0.0.0-8074-onepoint.war_-any-7644675788614491259.dir/webapp/scr	e38f8a1631a303ae8e5855453426c5bd
21	16:44:27.3203214000	repImport.bat	AppData/Local/Temp/jetty-0.0.0.0-8074-onepoint.war_-any-7644675788614491259.dir/webapp/scr	9694d6cf961d7f51f8b3e6769fa2958a
22	08:04:11.5097661000	LibreOffice_6.1.0_Win_x64_helppack_de.msi	AppData/Local/Temp/update/misc/LibreOffice_6.1.0_Win_x64_helppack_de.msi	289c68ea442da48dfb0feb92ab6213b
23	11:10:38.2841724000	Un_A.exe	AppData/Local/Temp/~nsu.tmp/Un_A.exe	b0b1122d224ed17397225d359c28458e
24	14:39:54.1234437000	unins000.exe	AppData/Roaming/UBitMenu/unins000.exe	8abffdf55ef2e06249cb0ba3bfcc8d8b
25	12:15:04.1444272000	YUMI-2.0.6.3.exe	Programme/YUMI/YUMI-2.0.6.3.exe	d859a06aadcfca077fd5c5f468f02e
26	12:15:04.1756272000	YUMI-UEFI-0.0.1.2.exe	Programme/YUMI/YUMI-UEFI-0.0.1.2.exe	9386ddde46d267379ba99abb9a86eaaaf
27				
28				
29				

R0776-kramski-20200325-083148-listing

Suchen Alle suchen ☐ Formatierte Anzeige ☐ Groß- und Kleinschreibung beachten ☐

Tabelle 1 von 1 Standard Deutsch (Deutschland) Mittelwert; Summe: 0 100 %

cut und sort

Alle Listings dublettenfrei ausgeben

Da die Listing-Dateien wiederholt erzeugt werden, und auch rechnerübergreifend die EXEs bestimmt mehrfach auftreten, brauchen wir zunächst eine Befehlskette, die alle gefundenen EXEs mit Rechner, Pfad und MD5sum ausgibt, aber MD5sum zur Dublettenbereinigung nutzt (Rechner und Pfad sind also in diesen Ausgaben oft nur noch als exemplarisch zu verstehen):

```
$ cut -f 1,17,18 *-listing.tsv | sort -t$'\t' -k 3 -u | tail
[...]
```

R07xx	AppData/Local/Programs/Git/usr/bin/tsort.exe	fe08e5bd1b23c701c0a15cf919915300
R07xx	AppData/Local/Programs/Git/cmd/start-ssh-pageant.cmd	fe57499d10c5fd319bce323aac321f71
R07xx	eclipse/java-2019-03/eclipse/eclipse.exe	feb4a634a99bcf7c2efc8e06a6ab300f
R07xx	AppData/Local/Programs/Git/usr/bin/recode-sr-latin.exe	fed01249a8319aa9a5936cab7cfe9175
R07xx	AppData/Local/atom/app-1.40.1/resources/app/apm/node_modules/.bin/npm.cmd	fe57499d10c5fd319bce323aac321f71
		fe57499d10c5fd319bce323aac321f71
COMPUTERNAME	RelPath	MD5sum

"cut -f 1,17,18" gibt nur die Felder (Spalten) 1,17 und 18 der Listings aus. "sort -t\$'\t' -k 3 -u" sortiert nach dem dritten Feld (also MD5sum) und unifiziert die Daten auch gleich danach (ähnlich "uniq").

cut und sort

Whitelist anlegen

Wir schreiben zunächst ALLE gefundenen EXEs temporär in die entstehende produktive Whitelist:

```
$ cut -f 1,17,18 *-listing.tsv | sort -t$'\t' -k 3 -u | cut -f 2,3 > whitelist.tsv
```

```
AppData/Local/Programs/Opera [...] aller_helper_64.exe 011250e5a67c08e08dbb7ea9a67ae5ce
AppData/Local/Programs/Git/usr/bin/dd.exe 116b36c2f6698a1d8fa5fc7a9f8ce9f
```

[...]

Nun können wir whitelist.tsv in Excel öffnen und manuell durchsehen. Dabei ist es praktischer, zuerst nach RelPath zu sortieren (Spalte A). Vor dem Speichern müssen wir aber wieder nach MD5sum (Spalte B) aufsteigend sortieren.

Wir speichern weiterhin im .tsv-Format, aber Excel schreibt die .tsv-Dateien leider mit MS-DOS-Line-Ends. Die müssen wir nach jedem Speichern wieder in Unix-Line-Ends zurückverwandeln, sonst kann grep die Pattern nicht korrekt verarbeiten:

```
$ dos2unix whitelist.tsv
```

grep

Unbekannte ausführbare Dateien finden

Wir benutzen "grep", um gegen die Whitelist zu prüfen. "grep -f FILE" liest die Suchpattern, die man finden will, aus einer Datei. Sie werden alle ver-odert, wenn diese Datei mehrere Zeilen hat. "grep -f-" liest hier allerdings nicht aus einer echten Datei, sondern von Standard-Input, in das wir die MD5sums der Whitelist hinein pipen. "-v" negiert die Such-Logik zu "finde NICHT", "-h" unterdrückt die Ausgabe der Dateinamen. Der Rest wieder wie oben.

```
$ cut -f 2 whitelist.tsv | grep -v -h -f- *-listing.tsv | cut -f 1,17,18 |  
  sort -t$'\t' -k 3 -u | less
```

[...]

```
R07yy  AppData/Local/Temp/FadeTop.exe acf3005db376c65dd1d8f760e11bfbe1
```

```
R07xx  AppData/Local/Temp/chocolatey/chocInstall/tools/chocolateyInstall/  
helpers/functions/Uninstall-ChocolateyPackage.ps1  
ade09904c2662ac40641a2d45a05435a
```

```
R07xx  AppData/Local/Temp/chocolatey/chocInstall/tools/chocolateyInstall/  
helpers/chocolateyScriptRunner.ps1      aeca272d5d86530bda42290c319f16a3
```

grep

Whitelist erweitern

Die unbekannten Einträge sichern wir zur Begutachtung und als Kandidaten für eine Erweiterung der Whitelist:

```
$ cut -f 2 whitelist.tsv | grep -v -h -f *-listing.tsv | cut -f 1,17,18  
| sort -t$'\t' -k 3 -u | cut -f 2,3 > whitelist-kandidaten.tsv
```

Nun können wir whitelist-kandidaten.tsv in Excel öffnen, durchsehen und hoffentlich alle Zeilen in whitelist.tsv übernehmen.

Das war's, bleibt gesund!

Kein Emotet, kein COVID-19!



CC-BY-NC 4.0

Heinz Werner Kramski-Grote

Kramski@web.de

<https://creativecommons.org/licenses/by-nc/4.0/legalcode.de>