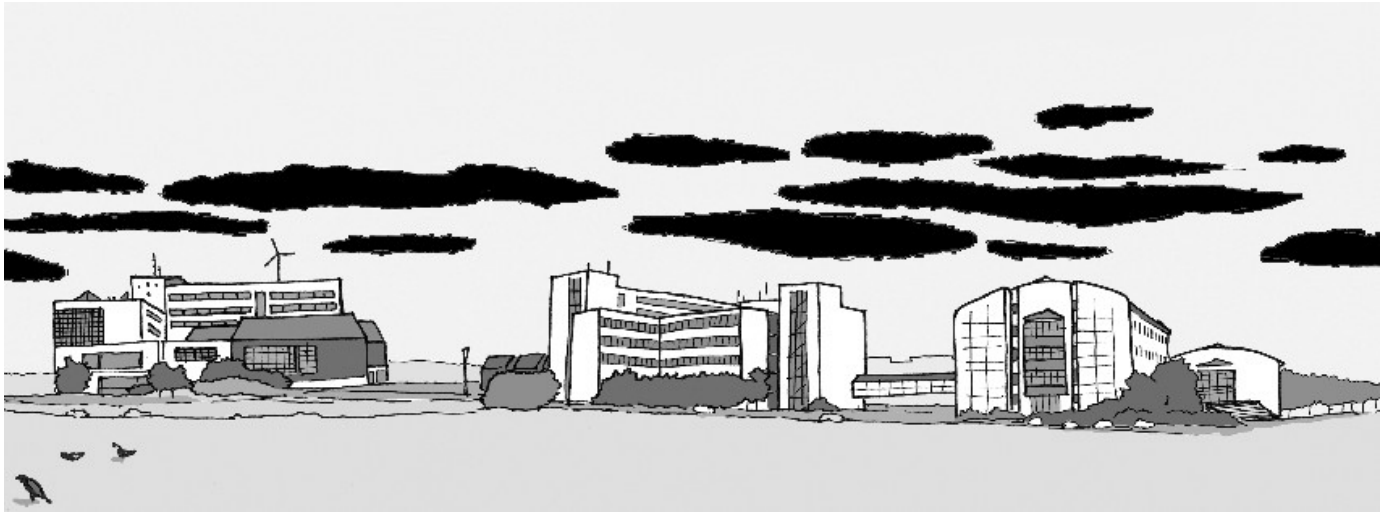
Trnitá cesta Crypt0l0ckeru

Aleš Padrta

Úvodní slovo

- 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 zužitkuje 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@studiomazzottiecruciani.it>
Komu: ■■■■■■■■■■@■■■.zcu.cz

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

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

Se srdecným pozdravem,
Martin Veselý

s.fr>

Kompletní informace:
https://dl.dropboxusercontent.com/s/xjbju2tx1k1ruq8/439937.zip?dl=0

Vážíme si vaší práce.

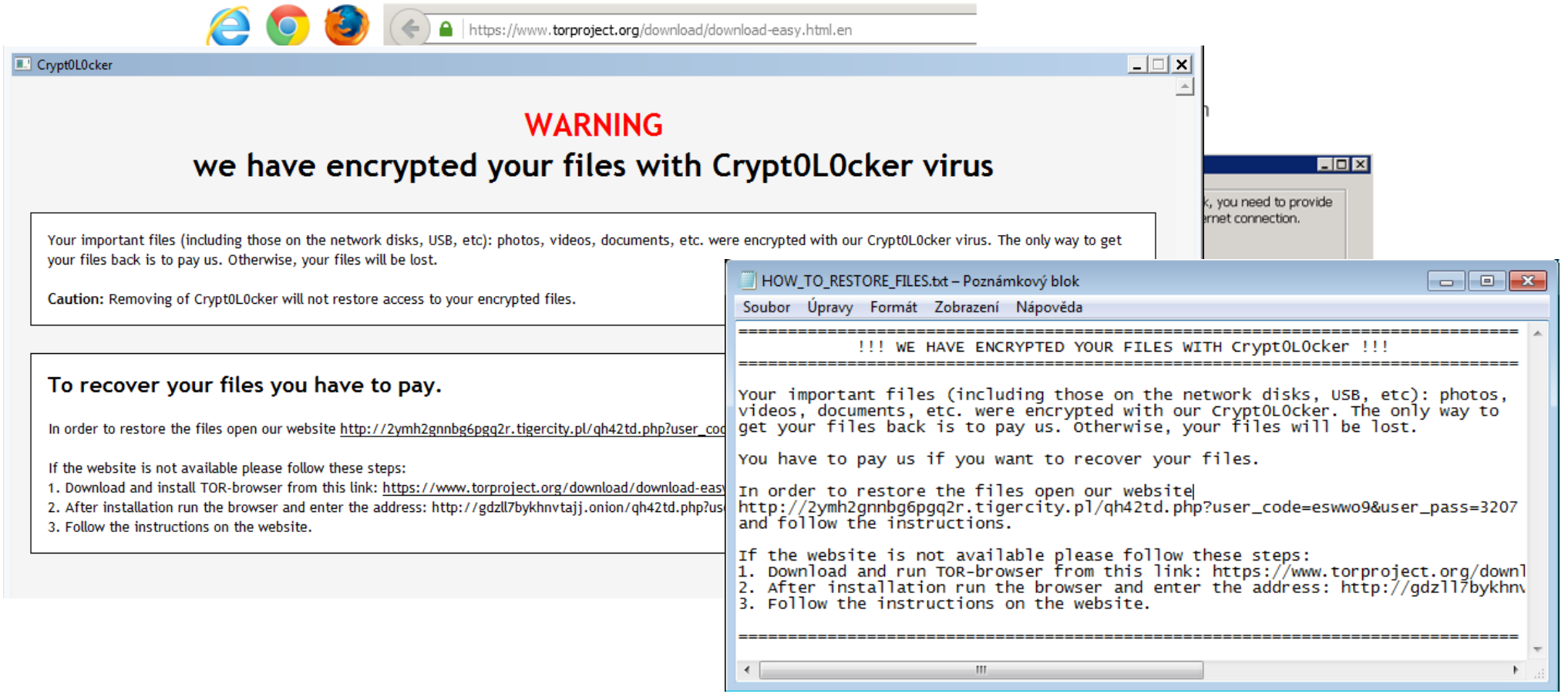
S pozdravem,
Jakub Krejcí

… 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



Forenzní laboratoř

Dějství II: Analýza

Cíle analýzy

- 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 charakeristiky indikující otevření souboru?
  3. Jak lze zablokovat činnost malware?
- Rychlost je klíčová
  - Průběžné sdělování nalezených informací

Analýza – od e-mailu k ransomware

- 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

Analýza – od e-mailu k ransomware

- Analýza javascriptu
  - Deobfuskace
    - 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

Analýza – od e-mailu k ransomware

```
$ 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");
...
```

Analýza – od e-mailu k ransomware

- 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 – od e-mailu k ransomware

- 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

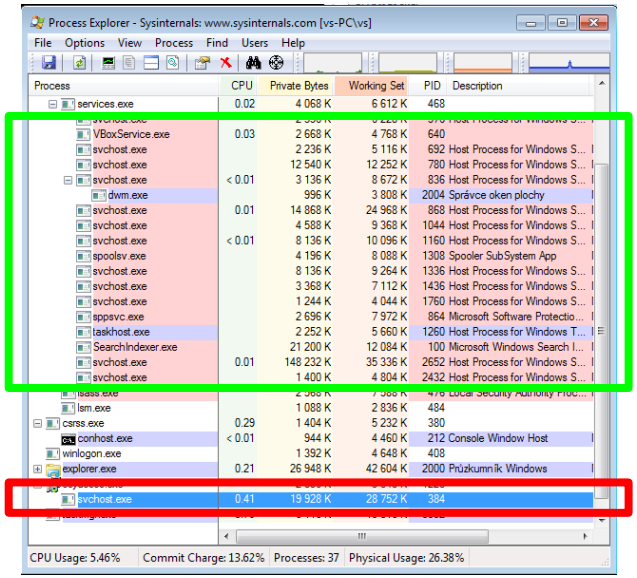
Analýza – od e-mailu k ransomware

- Výsledky dynamické analýzy
  - Potvrzení modifikovaného NSIS instalátoru
  - Využívání lokálního tempu aktuálního uživatele
  - Vytvoření procesu svchost.exe
    - Code injection
    - Crypt0l0cker
  - Úložiště

    `C:\ProgramData\`
    `C:\ProgramData\<random>\`
  - Persistence

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

    Spouštěn je opět „NSIS instalátor“

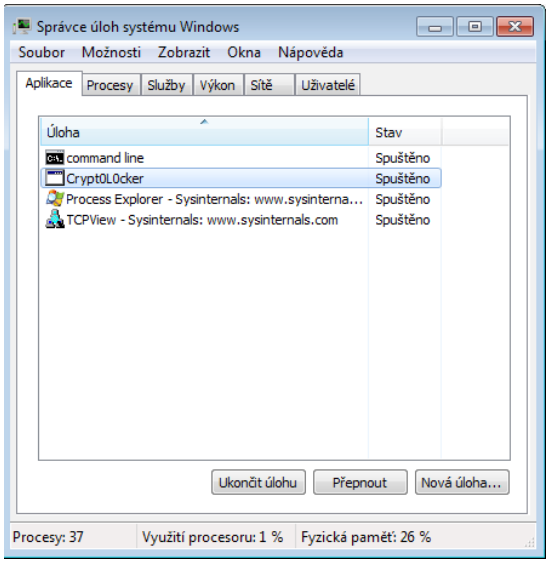


Analýza – od e-mailu k ransomware

- 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 javacsriptem, který po spuštění stáhne další součásti malware z webu. Jde o první krok vedoucí k instalaci ransomware Crypt0l0cker.
2) Jaké jsou lokální a síťové charakeristiky 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)

Odpovědi na otázky

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

Forenzní laboratoř

Dějství III: Využití informací

Reakce a prevence

- 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

Forenzní laboratoř CESNET

- Služby forenzní laboratoře
  - Analýza bezpečnostních incidentů (reakce)
    - Analýza zařízení
    - Analýza malware
    - …
  - Penetrační a zátěžové testy (prevence)
    - Simulace reálných útočníků

      => možnost na chyby reagovat včas
  - Doplňkové služby
    - Konzultace
    - Školení, semináře, workshopy
    - Obnova dat
    - …

Nejbližší workshop

- 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