

# Ransomware – ako sa brániť



Maroš Barabas, AEC s.r.o.

# Ransomware

- Malware, zbraň, business model
- Som zašifrovaný, čo so mnou?
- Keď zaplatím, dostanem svoje dáta späť?
- Mýtus. Kým neuvidím, neuverím, netýka sa ma to ...



97.25

Percentage of phishing  
emails delivering ransomware

**... o pár dní neskôr ...**

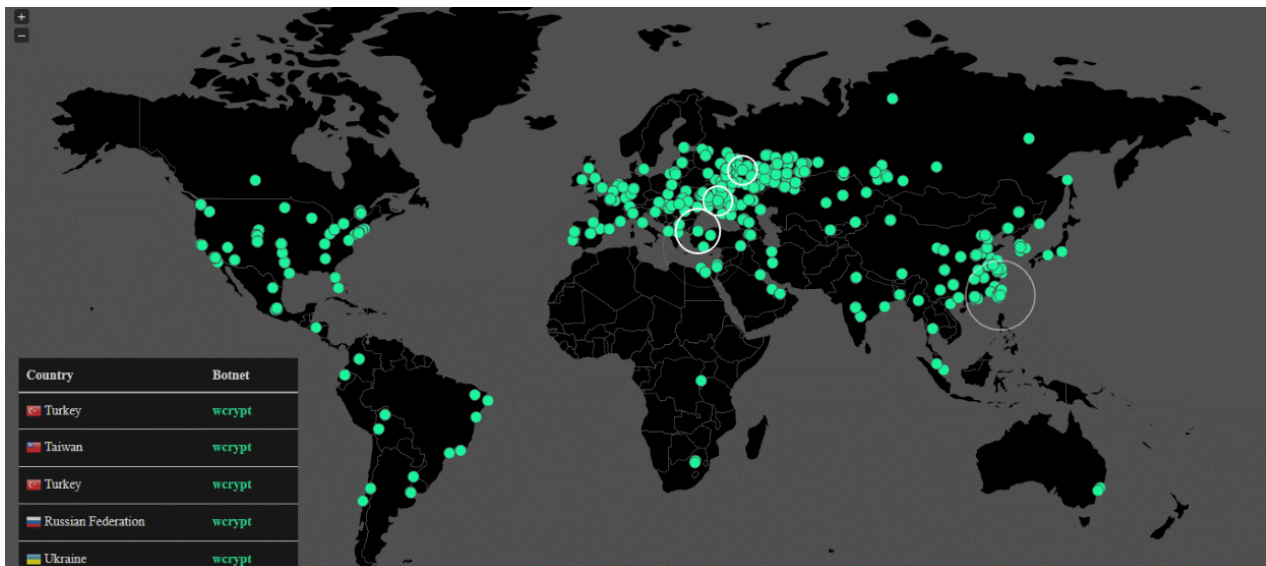


# Ransomware – vektory útoku

- **Phishing** – otvorenie prílohy, kliknutie na link (15 rokov bez obrany)
- **Kliknutie** na podvrhnutú reklamu
- **Zraniteľnosť** sieťovej služby
- **Stiahnutie** programu/aplikácie z nedôveryhodného zdroja
- **Iné zdroje** (USB, chyba prehliadača, deti, ...)

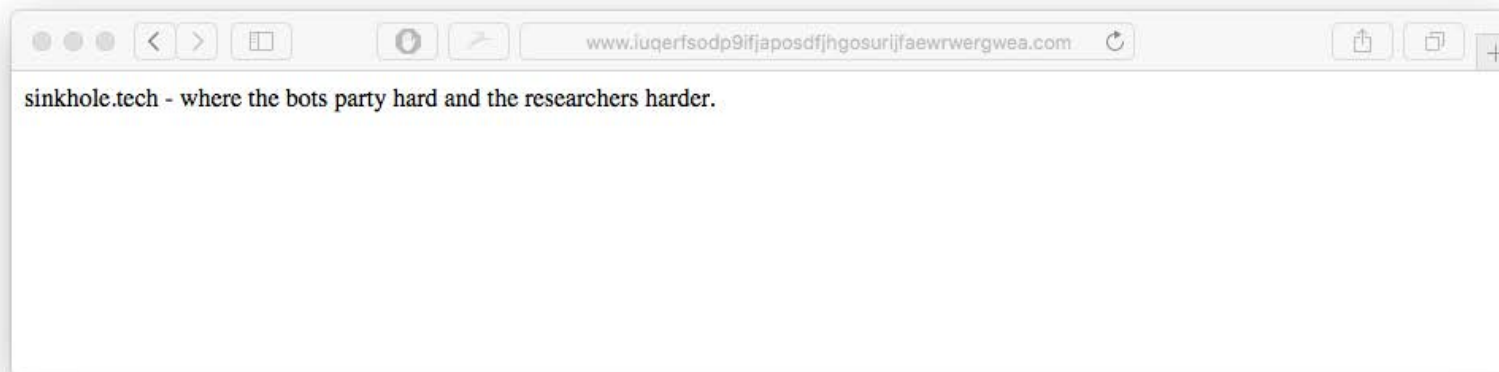


# WannaCry (12.5.2017)



*Živá mapa [intel.malwaretech.com/WannaCrypt.html](http://intel.malwaretech.com/WannaCrypt.html)*

- Exploit na SMB (TCP 445)
- Technika obchádzania Sandbox tech. (Necrus DNS check)
- Naobsahuje C&C call-back
- Nehoda alebo profesionalita?
- Používa SMBv1 i SMBv2



# WannaCry (12.5.2017)



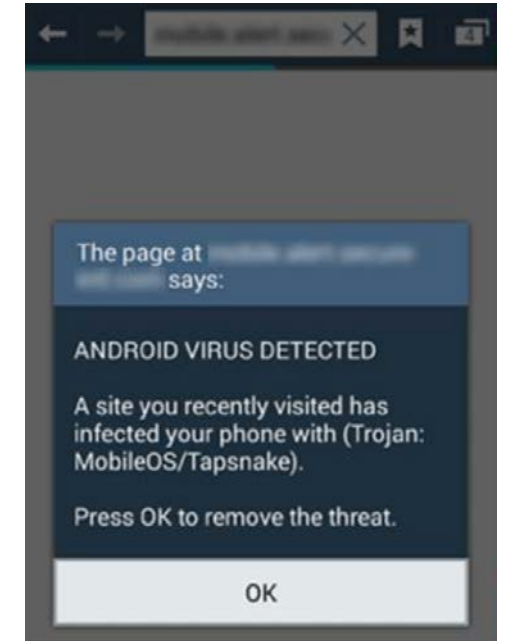
- MS17-010 SEC vydáný 14. 3. 2017 (Critical)
- 12.5 – za menej ako 2h infikovaných 50 tis. systémov
- 13.5 – Microsoft vydáva záplaty i pre WinXP
- 14.5 – druhý variant, iná doména, znova kill-switch
- 14.5 – tretí variant – bez domény

# State of the Art

- **Viac ako 10 rokov** (Reveton -> CryptoLocker -> CryptoWall -> Locky -> Cerber -> WannaCry)
- Prvý ransomware identifikovaný v r. 1989 ako súčasť trojanu AIDS
- 24/7 podpora, call-centrá, platobné brány
- 400% zvýšenie útokov ransomware (report 2016)
- **Neschopnosť ochrany .. zdanlivá?**

# Zásady slušného správania

- **Paranoja** – zdĺhavá duševná porucha charakterizovaná bludnými predstavami



# Zásady slušného správania

- Archivácia – zálohovať, archivovať, kontinuálne, inkrementálne

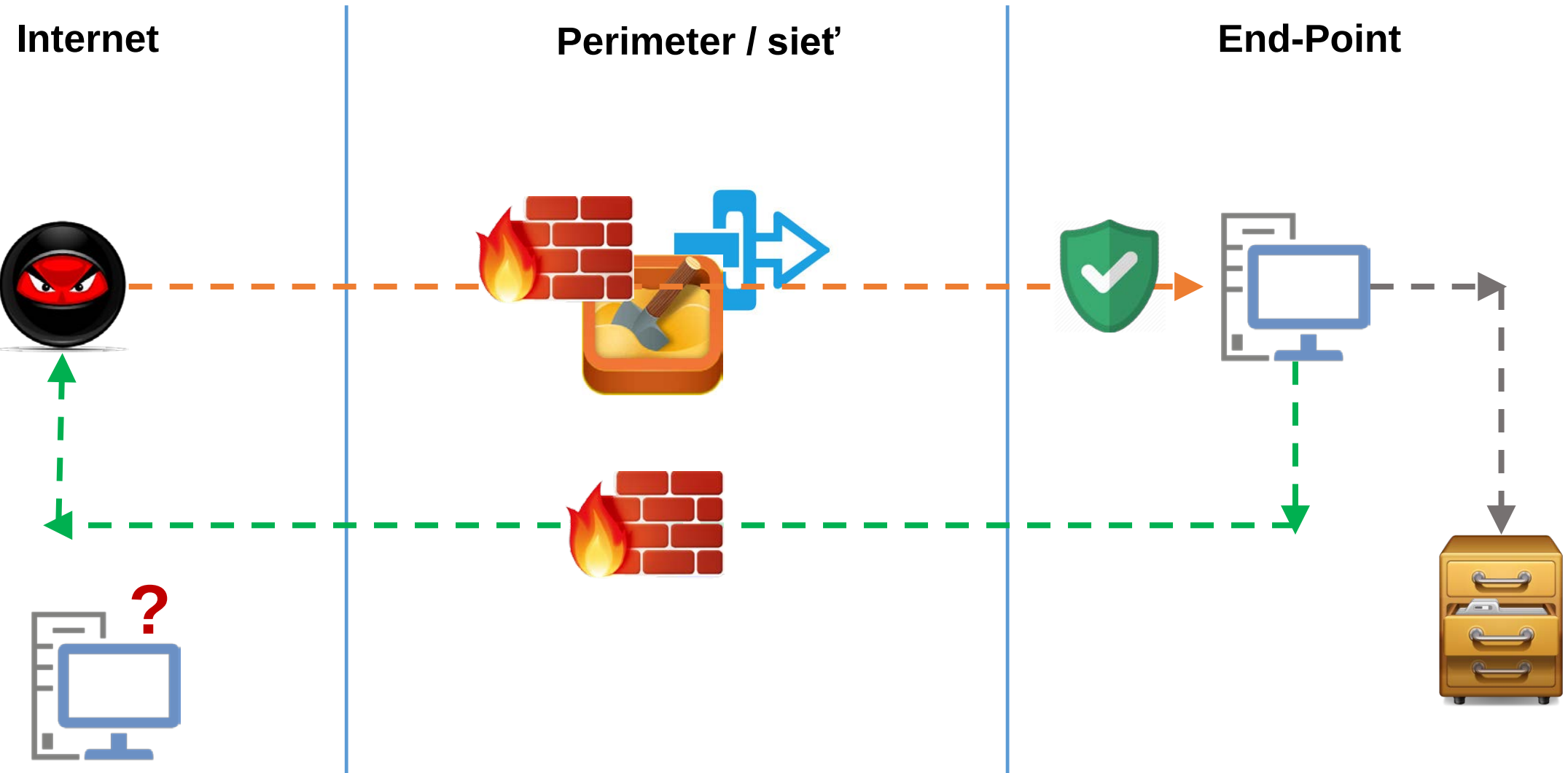
```
set extIP to do shell script "ifconfig en0 | grep 'inet ' | awk -F ' ' '{print $2}' | sed 's/\\.[0-9]*$//'"
if extIP = "██████████" then
  try
    mount volume "smb://██████████"
  end try
  do shell script "hdiutil attach -mountpoint /Volumes/Backup/ /Volumes/mbarabas/Backup.sparsebundle"
end if
```

- Best-practise

- Aktualizácie
- Least privilege
- Minimalizácia „attack-surface“
- Vyžadovanie bezpečnostného minima
- Kontrola



# Detekcia



# Detekcia – sieťová úroveň

- **NGFW** – základný kameň sieťovej bezpečnosti (IPS, AppControl, URL filtering, ...)
- **Web/Email brána, SPAM filter** – bižutéria?
- **Sandbox** – často jediná ochrana voči pokročilému malware
- **Správna segmentácia** – zabránenie lokálnemu šíreniu

# Detekcia – end-point úroveň

- **Signatúry** – účinné voči známemu malware
- **Heuristické metódy** – účinné voči novým vzorkám
- **Real-Time Monitoring**
- **Zálohovanie a obnova**



***O chvíľu: Ransomware v praxi***

*Peter Stančík, vedúci Awareness tímu, ESET*

# Zaujímavosti z histórie

- **Honeypoty** – šifrovanie sieťových diskov
- **Obnoviť alebo zaplatiť?** Otázka na Business
- **Popcorn Time** – ušetri za odporúčanie 😊

## Security



### Ransomware scum offer free decryption if you infect two mates

Friends don't infect friends with ransomware ... until it saves them \$770

11 Dec 2016 at 22:57, [Darren Pauli](#)



Ransomware scum are suggesting that victims infect their friends instead of paying for decryption keys.

my monthly income only 400dollar... you really wanna do this on me? :(

[See More](#)



thundercrypt@tuta.io

9:29 PM



To: qwe uio

[Details](#)

No, we don't. Frankly speaking, our Taiwanese campaign seems to be a total failure. Apparently, we have largely overestimated income of the population of your country.

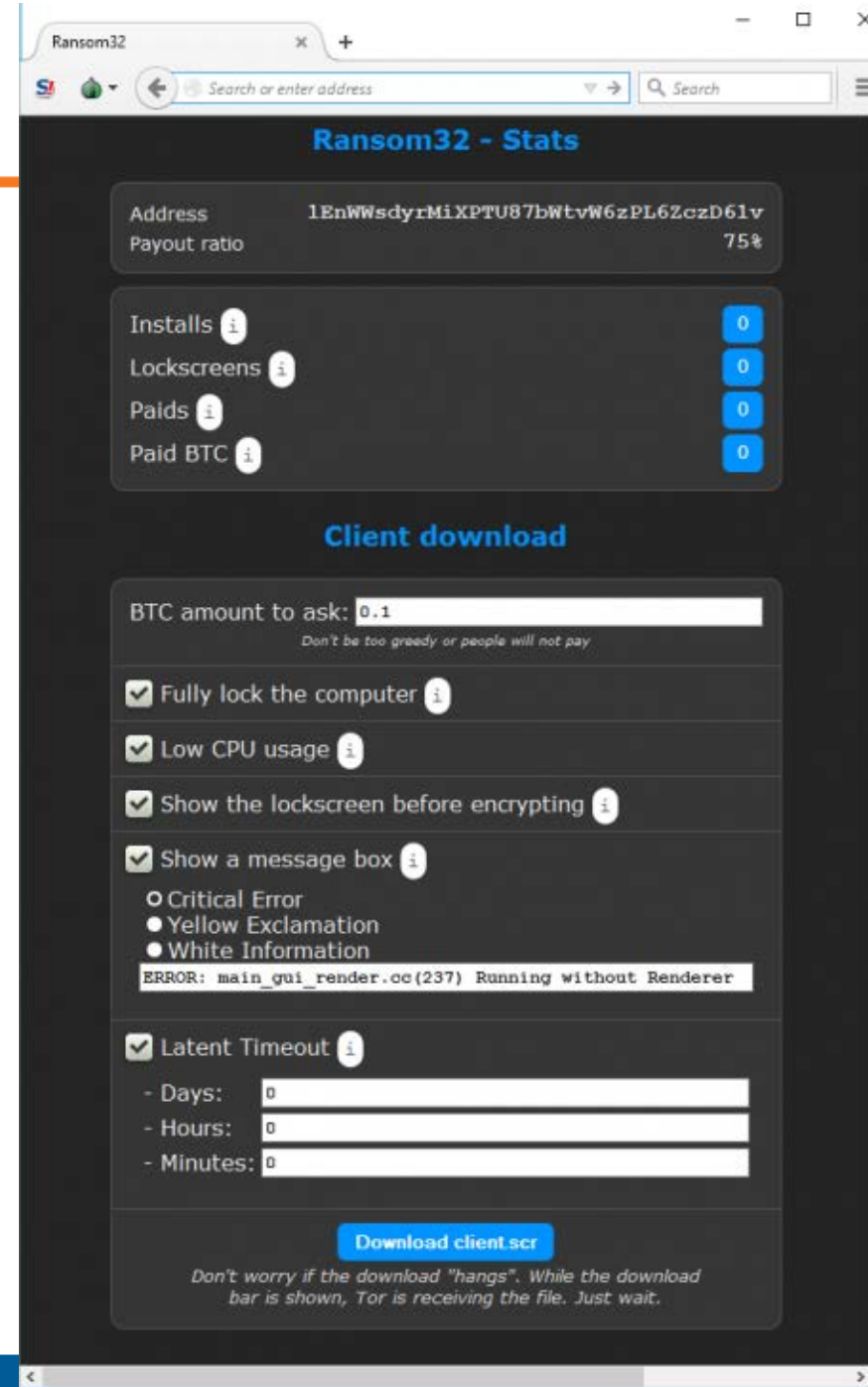
Soooo, ok. You don't have to pay now, we've switched ThunderCrypt to decryption mode for your computer. Therefore, as soon as our server establishes connection with your computer, the decryption should start automatically. If it doesn't, let us know.

P. S. But if you indeed liked something about ThunderCrypt and would like to donate us a few cups of coffee, always feel free to do so:

# Budúcnosť?

- Ransomware as a service (RaaS)?
- Vydieranie 2.0 – útok na povest'
- Advanced ransomware?
- Open-source ransomware?
  - Zeus – 20 derivátov po zverejnení

*... Paying the ransom should always be the last resort ... but sometimes ... the only sensible business decision left is to pay the criminals ...*



# Ďakujeme za pozornosť

Maroš Barabas

AEC s.r.o.

Maros.Barabas@aec.sk

