Kriptovīrusi

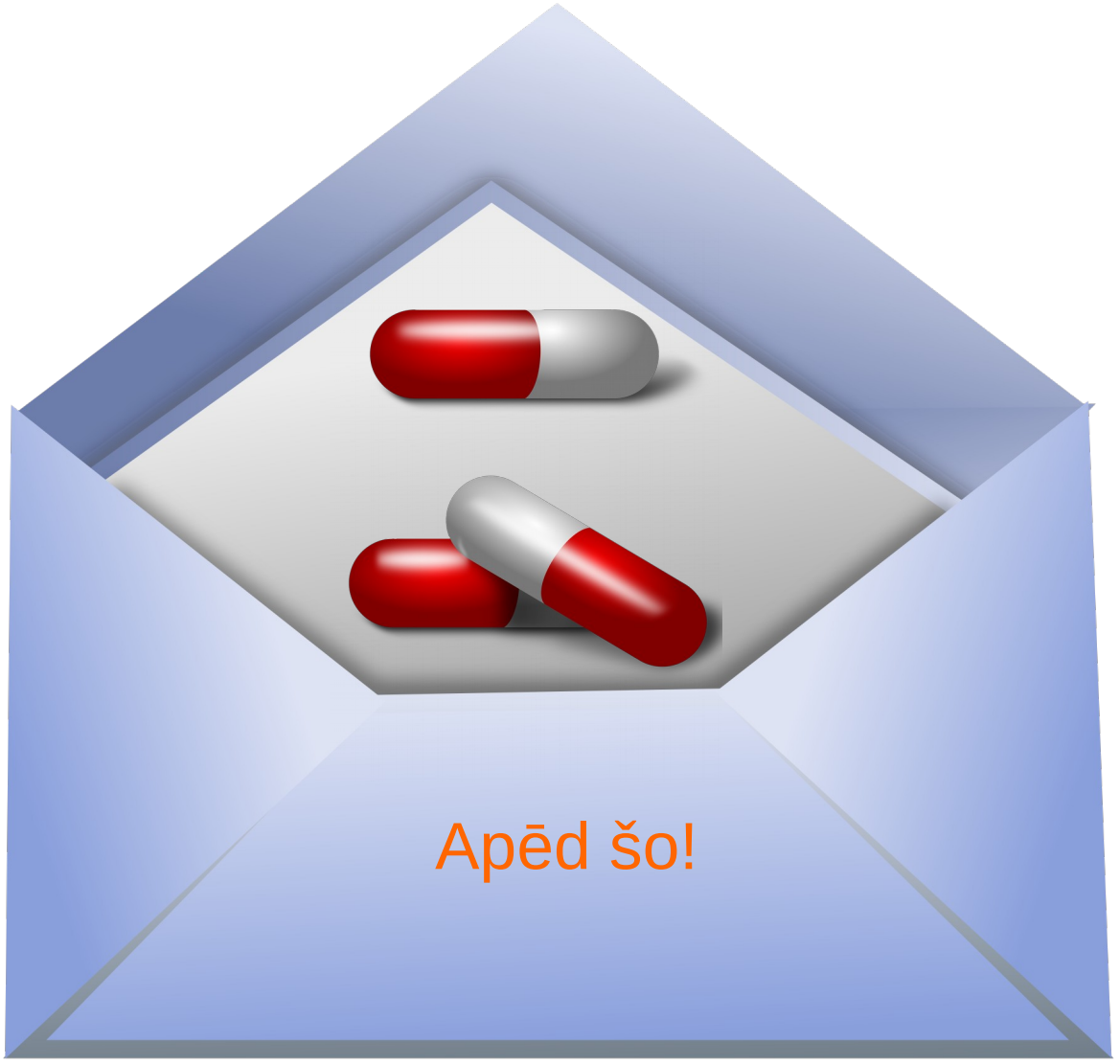
Esi Drošs 11.12.2017, Kārlis Podiņš, CERT.LV

Saturs

- Petya
- notPetya
- maybePetya

Petya

- Infekcijas vektors – izpildāmais fails epastā
  - Lokālā administratora tiesības
    - Yes, I agree – click click click
- MBR pārrakstīšana – pirmā programmatūra (software)
- MFT šifrēšana
- Bitcoin izpirkums par atslēgu
- Mīnusi
  - Datņu saturs nemainīts, daļu iespējams atgūt
- Plusi
  - Pilnīga paralīze
  - Nav problēmu ar šifrēšanas slēpšanu – on-the-fly atšifrēšanu

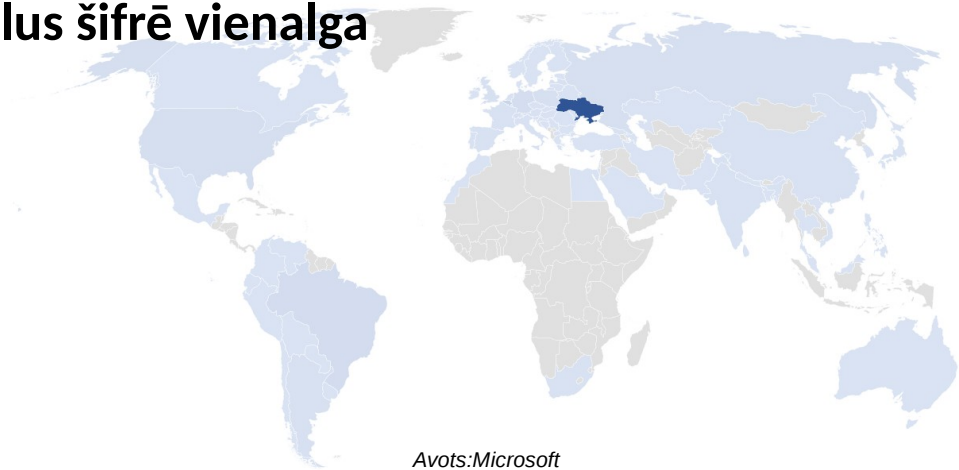

Apēd šo!

Mischa

- **Petya + Mischa = ❤**
- **Mischa = datņu līmeņa šifrēšana**
  - **Ja netiek pie lokālā administratora tiesībām**
- **80. gadu tehnoloģijas + bitcoin monetizācijai**

notPetya

- Modificēts Petya+Mischa
- Sākotnēji izplatās caur *backdoor* Ukrainā izmantotā grāmatvedības programmatūrā
- Tālāka izplatīšanās pa lokālo tīklu ar SMB ievainojamībām un pass-the-hash
  - Tārps
- MFT šifrēšana
- Failu līmeņa šifrēšana
- Specifiska uzvedība atrodot AV produktus – failus šifrē vienalga
  - Kaspersky
  - Symantec
- Bitcoin izpirkums par šifrēšanas atslēgu
  - Atšifrēšana nav paredzēta



Avots:Microsoft

notPetya - secinājumi

- Supply Chain izmantošana uzbrukuma mērķēšanai
  - lokāli izmantota programmatūra
    - Arī vieglākais ceļš - ticams, ka vairāk caurumu
- Win10 iebūvētie mehānismi veiksmīgi pasargā
  - Ir jēga izmantot pēdējo versiju
  - Ukrainas gadījumā nepasargātu
- Infekcijas sākumā pēc VirusTotal datiem tikai 2 produkti klasificē kā ļaundabīgu
  - AV – aizsardzība pret vakardienas apdraudējumiem
  - VirusTotal nevar izmantot AV salīdzināšanai – konfigurācija

notPetya

Avots: Financial Times

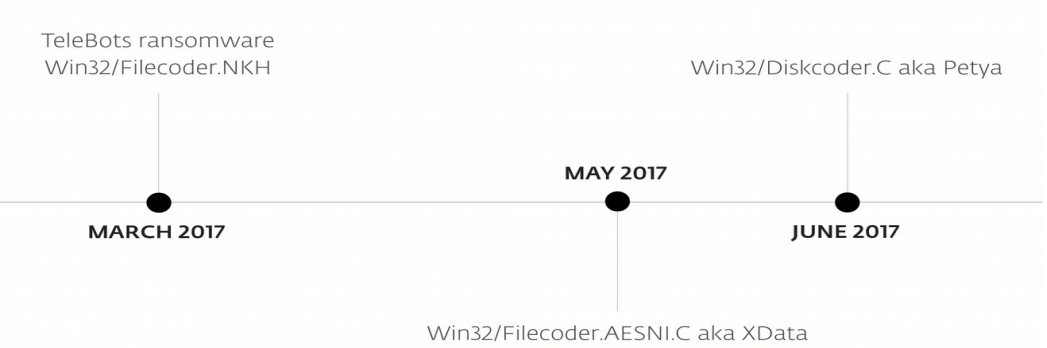
Collateral damage - Maersk

- Maersk = 1/5 pasaules kravu apjoma
- Ietekme 4 valstīs
- 200..300M$ zaudējumi

- Upuri arī Merck, FedEx

NotPetya – skats no putna lidojuma

- Supply chain attack
- Kritiskā infrastruktūra
- Šifrējošā vīrusa piesegs
- Win un Linux
- MEDoc izmantots gan maijā, gan jūnij..
  - 1x – nejaušība, 2x – likumsakarība?
- "...we are reasonably confident towards it being Russia" FireEye
- 27.jūnijs – notPetya
- 28.jūnijs – Ukrainas konstitūcijas diena



Avots: ESET

Wannacry

- Šifrējošais vīruss
- Tālāka izplatīšanās pa lokālo tīklu ar SMB
- Piedēvēts Ziemeļkorejas aktivitātēm (Symantec)
- NHS UK, Telefonica, FedEx, Deutshe Bahn
- 300.000 iekārtu
- Izpirkums 130 k$
  - bitcoin maciņa ienākumus iespējams izsekot

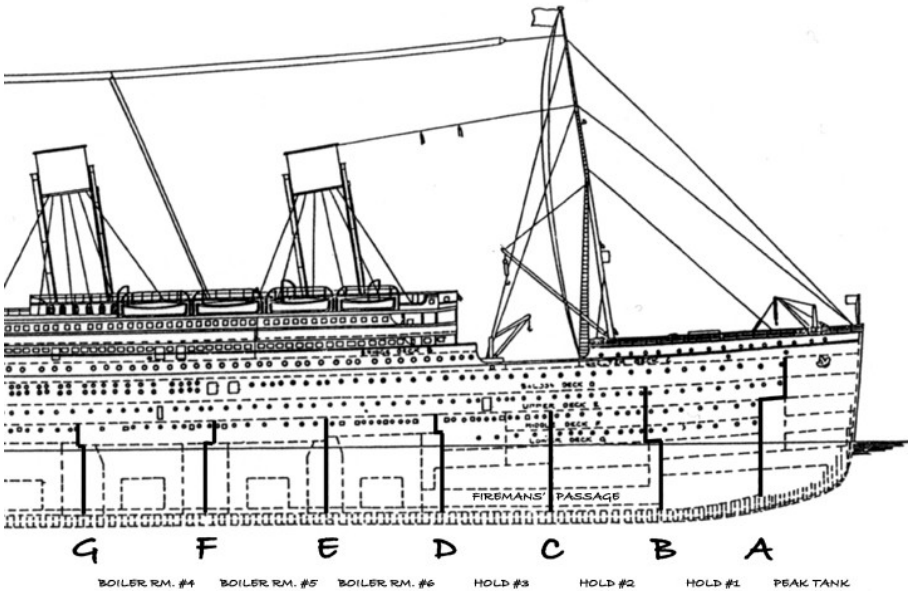
Apkopojums

	Valsts	**Noziedzība**
Izpirkums	Wannacry	Petya
Zaudējumi+morāle	notPetya	?

Problēmas un risinājumi

- Ārējs audits uz rakstīšanas tiesībām
- Problēmas personalizācija
  - Līdz šim pārāk bieži infekcija = problēma citiem

- Tiesību ierobežošana
- Lietotāju izolācija
- Baltie saraksti



Bulkheads & Compartments in the Bow Section


Paldies!