Kórház a vírus szélén

A zsarolóvírusok trendjei és behatolásuk a fősodorba

Bolcsó Dániel

Index.hu

Zsarolóvírus / Ransomware

Típusok

- Locker (ORFK, NNI)
- Cryptoware

Terjedés

- Csatolmány
- Fertőzött oldal
- Fertőzött hirdetés

Népszerű fajták

Top 3*

- Teslacrypt (58,43%)
- CTB-Locker (23,49%)
- Cryptowall (3,41%)

Slágerek

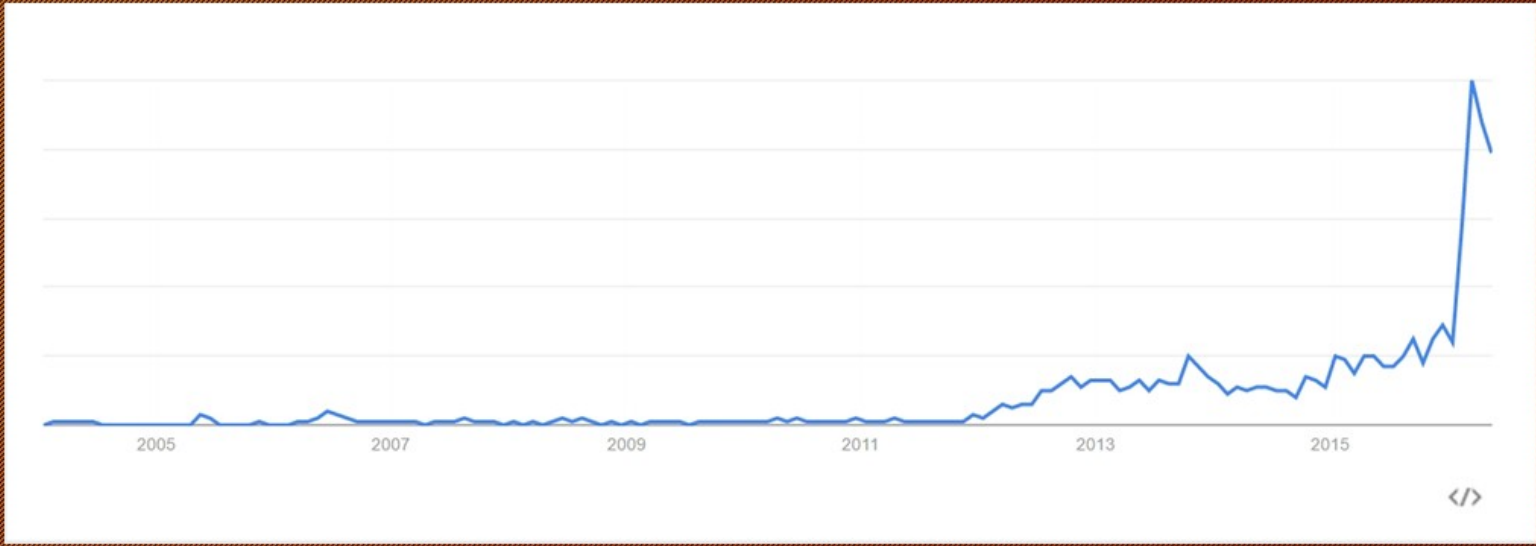
- Locky (február, macro, számla)
- Petya (március, macro, önéletrajz)
- SamSam (március, JBoss alkalmazásszerver)

*Kaspersky, 2016. Q1

Halad a korral

- Bitcoin
- Bittorrent, mobilplatformok
- Okosautók, IoT?
- RaaS: Ransomware as a Service – a felhasználóbarát kiberbűnözés

Betörés a mainstreambe



A figyelem okai

Elszaporodás, további növekedés*

- Csak a legutóbbi negyedévben: 2846 új ransomware-típus (+14%)
- Az ismert támadások száma: +30%

Látványosabb incidensek >>> közintézmények

*Kaspersky, 2016. Q1

Kórházi esetek

- **Hollywood Presbyterian Medical Center**

  Los Angeles, február, Locky, 17 ezer dollár

- **Medstar-kórházak**

  március, SamSam

- **Február-március**

  Kalifornia, Kentucky, Indiana, Kanada, Németország, Új-Zéland...

Magyarország

- **Csolnoky Ferenc Kórház,** Veszprém

  Locky

- **Erzsébet Kórház,** Zirc

  TeslaCrypt

- **stb**

A kórház mint ideális célpont

- Kritikus infrastruktúra
- Érzékeny adatok
- Élet-halál, időérzékenység
- Nagyobb fizetési hajlandóság
- Nagy közérdeklődés + könnyebben kiderül
- IT-problémák

Ransomware <3 kórházak?

- IT-problémák máshol is
- Általában cégek, szervezetek hálózatai, területi lefedettség
- Magáncégek: könnyebb eltitkolni

Más példák

- **SamSam:** videojátékosok, építőipar
- **Petya:** HR-cégek
- **Egyházi intézmények** (hillsborói plébánia, 570 dollár)
- **Iskolák** (Dél-Karolina, 10 ezer dollár; magyar gimnázium, Locky)
- **Önkormányzatok** (Plainfield, N.J., március)
- **Fehér Ház** (belső figyelmeztetés, május)

Fizetés?

- Közvetlen fejlesztési forrás
- Pozitív visszacsatolás, sikeres üzleti modell
- Nem biztos az adatvisszaállítás
- Utófertőzés, botnet
- Viszont: a szolgáltatáskiesési idő, az adatpótlás költségei

Miért egyre népszerűbb?

- Nagy megtérülés
  - Olcsó
  - Gyakran bejön
  - Könnyű mutálni
- Egyre könnyebb műfaj
- Nagy visszhang

Védekezés

- A vírusirtó nem ismeri fel
- Whitelisting
- Viselkedéselemzés
- Folyamatos ellenőrzés szimulálása
- Adaptív védekezés, IT-biztonság mint szolgáltatás

Megelőzés

- Elkülönített, rendszeres biztonsági mentés
- Frissítések
- Többrétegű vírusvédelem
- Világos policy-k (hozzáférés, jogosultságok)
- Továbbképzés, tájékoztatás!

+ **Média**

Köszönöm a figyelmet!