Fatatíska úlfsins: Þróun spilliforrita gegn netvörnum

Finnbogi Finnbogason CTO
13. nóvember 2024

Veiruvarnir í meira en 30 ár!

- Lykla-Pétur - Friðrik Skúlason
- Starfandi síðan 1993
- Stórasta veiruvarnarvélin í heimi
- 400.000.000.000 skrár daglega

1993 FRISK SOFTWARE INTERNATIONAL

2012 CYREN

2023 varist

…

"Never let a good crisis go to waste.“
- Winston Churchill

Hvað eru “umbúðir”?

T1027 - *Obfuscated Files or Information*

https://attack.mitre.org/techniques/T1027/

Þekkt spilliforrit

Innvafið ➔ Óþekkt !

Umbúðir eru hagkvæmar!

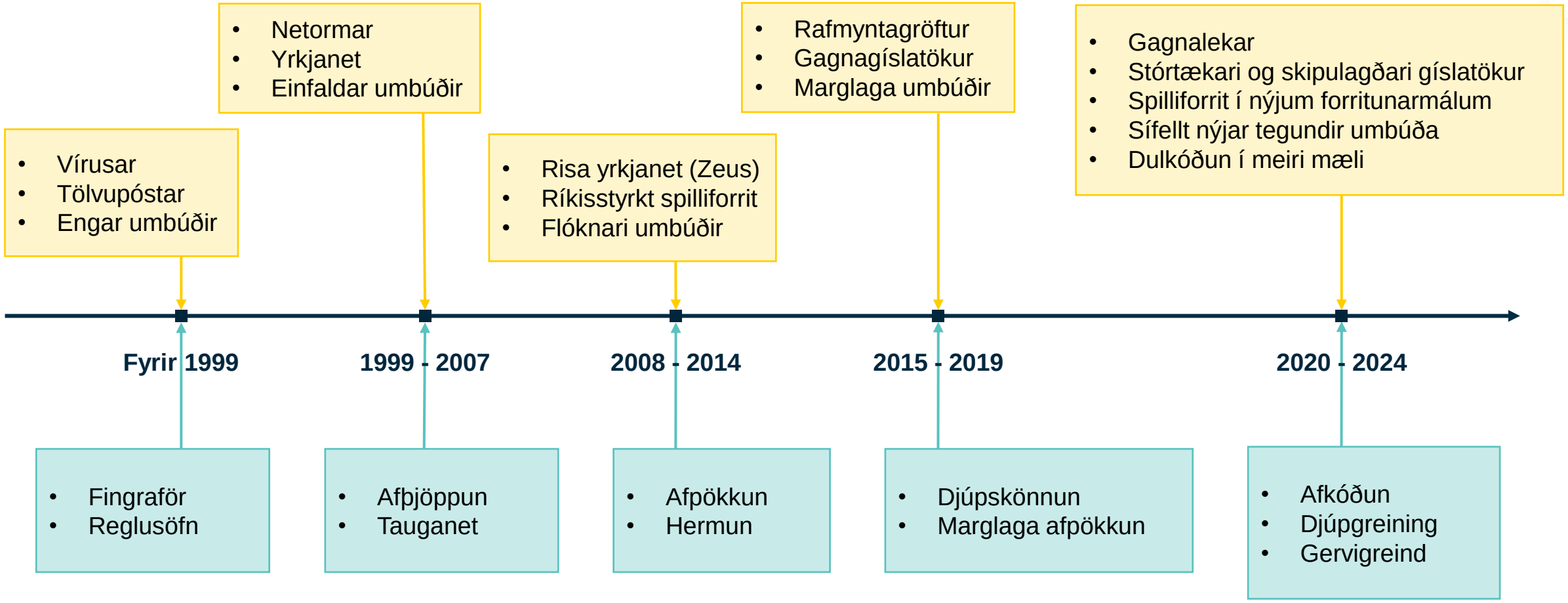
Af hverju?

- Smíði flókinna spilliforrita er dýr og tímafrek
- Forðast uppgötvun á leið sinni til fórnarlamba
- Endurnýting á háþróuðum hlutum árásarinnar
- Aukin ávöxtun fjárfestingar

Helstu aðferðir

- Þjöppun
- Dulkóðun
- Umkóðun (encoding)
- Keyrslupökkun (runtime packers)

Stefnur og straumar í spilliforritum

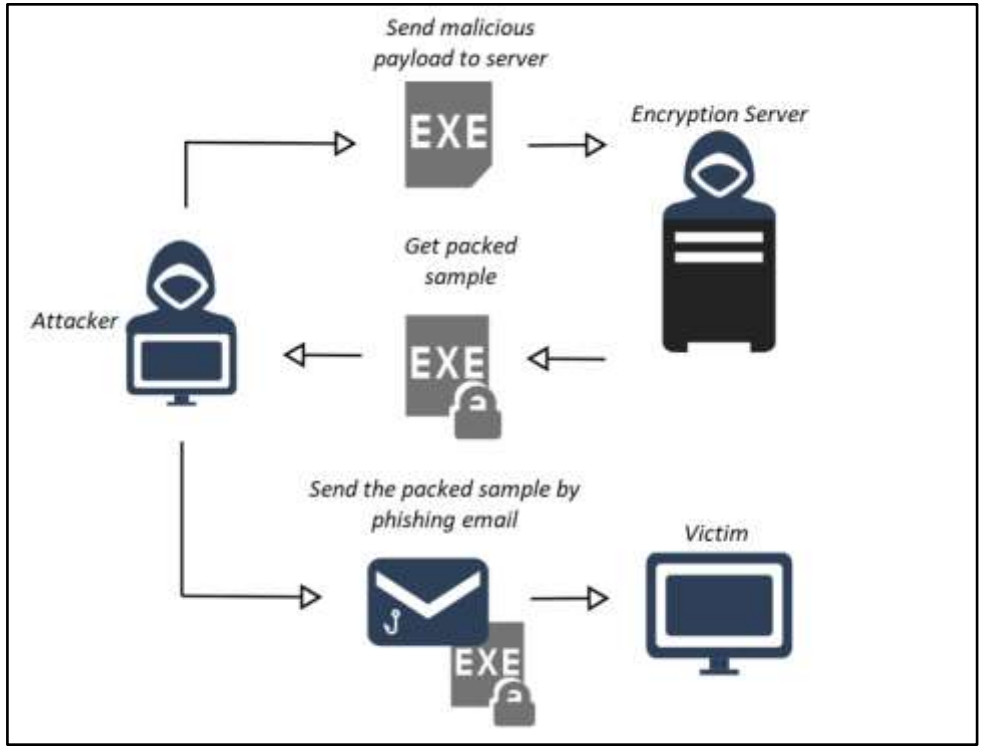


FRISK SOFTWARE INTERNATIONAL → CYREN → varist

Nýjungar stöðugt í mótun

Sauðagærurnar 2024

Packer-as-a-Service



The Hacker News

Home Cyber Attacks Vulnerabilities Expert Insights Contact

Hackers Exploit Legitimate Packer Software to Spread Malware Undetected

Jun 06, 2024 Ravie Lakshmanan

The Menace of TrickGate Packer-as-a-Service Spreading Malware Globally

Threat Level – Red | Vulnerability Report

NOVEMBER 7, 2024

Evasive ZIP Concatenation: Trojan Targets Windows Users

ARTHUR VAISELBUH, WINDOWS INTERNALS ENGINEER | PELEG CASRA, PRODUCT MARKETING MANAGER

Næstu áskoranir?

- Næsta tískubylgja er alltaf handan við hornið
- Sprenging í notkun nýrra forritunarmála
- Notkun gervigreindar til að:
  - nýsmíða eða endursmíða spilliforrit
  - framleiða flóknari umbúðir
  - sérhanna spilliforrit gegn tilteknu skotmarki

Baráttan heldur áfram…

varist

Takk fyrir!