Nedávné kybernetické útoky v ČR a ve světě

„Český ransomware“

- Malware, který se šíří zřejmě přes nakažené webové stránky (pro MS Windows systémy)
- Po infikování PC jej zablokuje a vyžaduje zadání kódu, který je nutné koupit
  - Cca EUR 100
- Tváří se jako varování Policie ČR, které upozorňuje na nelegální SW v počítači a platbu uvádí jako pokutu za jeho používání
  - Psychologický efekt – každý má v PC nějaký nelegální SW :-)

„RansomWare“

- Bylo zachyceno několik verzí tohoto SW
  - Jedná se nadnárodní aktivitu, směřující někam do Ruska
  - MW má několik skinů, které jsou upravovány podle cílových uživatelů (jazyk, místní zvyklosti policie, …)
  - Poslední česká verze byla velmi přesvědčivá
    - Někteří uživatelé přicházeli zaplatit pokutu přímo na služebny ČP :-)

„RansomWare“

- Velká vlna šíření byla zaznamenána na začátku roku
- Česká Policie případ aktivně řeší(la)
  - spolupráce s evropskými partnery
  - Centralizovaná evidence a vyšetřování všech případů
- CESNET CSIRT prováděl forenzní analýzu malware

Český ddos týden

- 4. až 7. března vlna ddos útoků na české weby
- Velmi cílená na mediální efekt, se znalostí českého prostředí
  - Pondělí: weby médií (idnes.cz, ...)
  - Úterý: seznam.cz
  - Středa: Velké banky
  - čtvrtek: Mobilní operátoři
- Dvě vlny každý den
  - 9-11 a 14-16 hod.
- Nikdo se k útokům nepřihlásil, motivaci neznáme

Český ddos týden - realizace

- „Ranní“ vlna využívala TCP SYN flood
  - Předstírané a nedokončené pokusy o ustavení TCP spojení
  - Vyčerpání TCP stacku na straně aplikací neumožní ustavit legitimní spojení
  - Zdrojová adresa podvržená (nicméně útok pocházel zřejmě z více strojů)
- Odpolední vlna založena na packet reflection
  - Pokus o TCP spojení s náhodným uzlem v Internetu s podvrženou zdrojovou adresou (vedoucí na cíl útoku)
- Útoky negenerovaly velké objemy dat
  - Někdy stačilo 80-120 Mbps, max. zřejmě kolem 1Gbps
  - Přesto úspěšné, v řadě případů „odešla“ předřazená infrastruktura (load-balancing, firewally)

Ddos proti Spamhaus-u

- Spamhaus je organizace, spravující seznamy spammerů
- Masivní útok ddos na servery Spamhaus a později CloudFlare (dodavatel ddos ochran pro Spamhaus)
  - Útoky začaly 16.3 a trvaly déle než týden
- V největší vlně generoval útok toky 300Gbps
  - Problémy i pro London Internet Exchange, cca hodinové snížení propustnosti
    - Reálně zpomalení celého Internetu

SpamHaus - realizace

- Velké toky generovány pomocí techniky DNS amplification
  - DNS odpověď je výrazně větší než dotaz (proto „amplification“)
  - Na světě existuje spousta otevřených DNS resolverů (navíc zpravidla na „tlustých“ linkách)
  - Pomocí padělané zdrojové adresy lze zahltit linku k oběti
- K útoku přispěly:
  - Otevřené DNS resolvery (zvýšení toků, až 1:10)
  - Ignorovaná doporučení na routovací politiky, zejm. http://tools.ietf.org/html/bcp38 (znemožnění podvrhnout IP adresu)

SpamHaus - realizace

- Vedle masivního síťového ddosu i podvržení aplikačního serveru
- Pomocí techniky BGP hijacking přesměřování routování IP adresy jednoho ze serverů na podvržený stroj
  - Stroj na každý dotaz ohledně IP adresy tvrdil, že IP je na seznamu spammerů

SpamHaus - dozvuky

- Podezření z útoků padá na „šedý“ server-hosting, který se dostal na seznam spammerů
  - CyberBunker, Nizozemí
- 25.4. ve Španělsku zatčen Sven Kamphuis (z CyberBunker), zřejmě bude obviněn kvůli „unesení“ IP adresy SpamHausu
- Už 26.4. se objevilo prohlášení podporující S.K. a hrozící dalšími útoky
  - http://pastebin.com/qzhcE1nVh