Aktuality z bezpečnosti (15.3-23.3.2017)

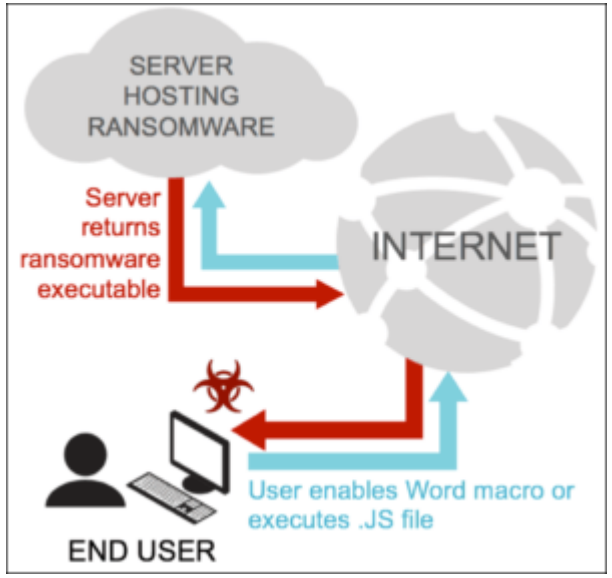
Bc. Ján Kotrady

Google a Jigsaw

- Balík voľne dostupných nástrojov pre bezpečné elektronické voľby
- DDoS ochrana
- Kontrola prístupu – 2 factor autorization
- Kontrola phisingových emailov
- Link

Cerber Ransomware

- Znovu sa začala kampaň
- JS alebo WORD makro
- Samorozbaľovanie a stiahnutie
- 500$ - 1000$
- NSIS (Nullsoft Scriptable Install System)
- Link



SAP Vulnerability

- Opravili tento mesiac najhoršiu chybu od roku 2011
- CVE-2017-6950
- Update všetkých klientov
- Útočník získa plný prístup k zariadeniu a súborom
- Niekolko
- Link

Moodle kritická chyba

- Spustiť PHP kód
- V podstate ide o SQL injection
- CVE-2017-2641
- 3.3.2 - verzia
- Link

Kritická chyba v knižnici LIBPURPLE

- Používana napr. v pidgin, adium (mac os)
- CVE-2017-2640
- Adium stále bez aktualizovania
- Link

„Hack“ windows účtu

- Použitím cmd
- Triviálne
- Admin účet
- password-less
- Video
- Link

Pwn2Own

- Firefox – opravené
- Chrome nezdolaný
- V rámci Pwn2Own sa podarilo HEAP OVERFLOW uniknúť z virtual machine
- Safari-to-root útok
- Adobe – jpeg2000 flaw heap overflow
- Ubuntu desktop exploit
- Link
- Link

Cisco

- Nájdená chyba po úniku dát z wikileaks
- Takmer všetky catalyst zariadenia s telnetom
- Približne 300 produktov
- Patch nie je k dispozícii
- CVE-2017-3881
- Link

Gmail a Yahoo

- 20 miliónov GMAIL
- 5 miliónov Yahoo
- DarkNet
- Link

MacDonald’s zraniteľnosť

- Približne 2.2 milióna
- Link

WikiLeaks zverejní firmám technické podklady

- Link

Linuxová zraniteľnosť po 10-tich rokov

- Link

Vyhrážanie sa applu

- Link
- Prístup k cloud-u

Blokovanie update od Windowsu pre nové CPU

- Link

DoubleAgent attack na Win [XP, Vista, 7, 10]

- Link(video)

Polovica android zariadení bez bezp. aktualizácií

- Link