XSS férgek és vírusok

Bucsay Balázs
http://www.rycon.hu/
earthquake[at]rycon[dot]hu
BB$HT

XSS jelentése

- XSS avagy Cross Site Scripting
- Injektálás fajta
- Sebezhető oldalba HTML-JavaScript... fecskendezése
- non-perzisztens, és perzisztens XSS-ek

Vírusok

- Fertőzött alkalmazások, új alkalmazásokat fertőznek meg
- Emberi beavatkozás szükséges
- Pl: mydoom

Férgek

- Saját magától terjed
- Emberi beavatkozás nem feltétlen szükséges
- Pl: botnetek kliens részei

~ Oday exploitok

- ActiveX exploitok:
  - hetente kijön kb 1db
- XDP exploitok:
  - régen jellemzőbbek voltak, de manapság is találnak
  - Flash nyelvre jellemző

Ki- és Felhasználhatóság 1/4

- Manapság szinte minden webszervíz sebezhető XSS-re
- Nincs Web 2.0 XSS nélkül :)
- Legnagyobb szociális hálókban is, levelező kliensekben is léteznek sebezhetőségek.

Ki- és Felhasználhatóság 2/4

- Bármilyen kód szúrható az oldalba (XSS)
- A kód marad vagy sem (non-./perzisztens)
- Cookie lopás, session hijacking, exploitálás
- Bármit meg lehet tenni a böngészőkkel

Ki- és Felhasználhatóság 3/4

- Minden Web 2.0 alkalmazás igényli a JavaScriptet
- Minél nagyobb egy alkalmazás, annál bonyolultabb, annál könnyebb benne hibát találni
- Beépített függvények megkönnyítik a férgek írását

Ki- és Felhasználhatóság 4/4

- Webes, bináris botnetek építése
- Spammelés
- Egyéb pénzkereseti lehetőségek

Fertőzés és terjeszkedés

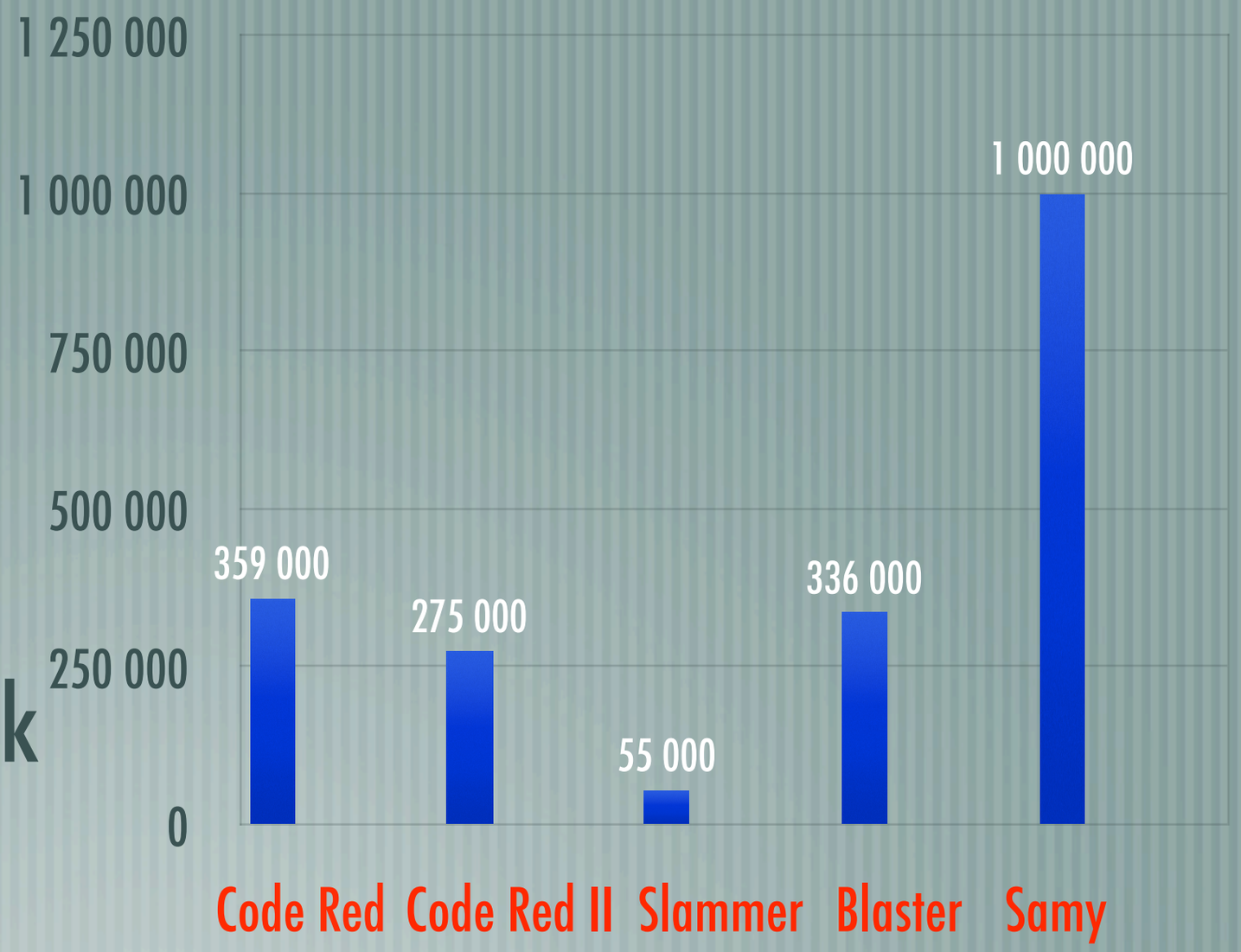
- Lépések:
  - 1. a web szolgáltatás megfertőzése
  - 2. felhasználó megnézi az oldalt
  - 3. felhasználónál lefut a kód és az 1. lépésre ugrik

Fiktív példa

- Szociális hálózat:
  - adatlap vagy üzenetküldés sebezhető
  - adatlapot megfertőzzük, más felhasználó megnézi
  - lefut a kód nála, és megfertőzi a saját adatlapját
  - 3. személy megnézi az egyik fertőzött adatlapot és...
  - 4. személy megnézi az ...

Terjedés gyorsasága

Szokatlan sebességgel, hihetetlen gyorsan terjednek



Kivitelezés

- Ezeket a férgeket/vírusokat nagyon rövid idő alatt meg lehet írni, 10 perces munka lényegi payload nélkül.
- JavaScript és HTML tudás szükségeltetik, esetleg még más.

Féreg/vírus felépítése

- Két részből áll:
  - propagáló kód
  - payload (hasznos teher)

Proof Of Concept 1/2

- Külső file.

Eltávolítás

- Nem a felhasználók dolga
- A web-szervíz a fertőzött, így a backend-ekből kell kiírtani a férget
- Egy időben kell ezt megtenni, hogy ne tudjon közben is terjedni

Védekezés

- XSS ellen kell védekezni
- Minden User-inputot (felhasználó által adott értékeket) ellenőrizni és átalakítani, esetleg szűrni kell.

Proof Of Concept 2/2

- Megírt üzenetküldő rendszer bemutatása, rajta egy XSS Worm demonstrálása.

Köszönöm a figyelmet!

Bucsay Balázs - http://www.rycon.hu