

Adatbiztonság III.

Buday Gergely

2010. december 1.

1 Cyber attacks

Cyber ...

- Cyber crime: üzleti érdek
- Cyber terrorism: rombolás
- Cyber war: országok között zajlik

Botnet business

- Botnet: saját "vezérlő" szoftverrel ellátott, megtámadott gépek hálózata
- bot: a vezérlő program
- el kell rejteni őket, hogy a víruskeresők ne találják meg
- a bot terjesztése: spam küldésével, fórumra küldéssel, facebookon, valamint worm-szerű ön-terjesztéssel
- fórumon: itt egy érdekes videó, csak egy speciális kodek kell hozzá, töltsd le

Hogyan keresnek pénzt botnettel?

- DDos támadással
- Bizalmas adatok megszerzésével
- Spam küldésével
- Adathalászattal
- Trójai programok terjesztésével

DDos támadások

- 2009 január: támadás a GoDaddy.com webszolgáltató ellen
- Majdnem 24 óráig elérhetetlen volt a szolgáltató által tárolt sok ezer honlap
- 2007 február: támadás az internet root névszerverei ellen
- Ára: 50\$-tól több ezer dollárig (24 órás támadás)
- a shadowserver.org szerint 2008-ban 190.000 DDos támadást hajtottak végre, 20 millió dollárt bevételezve (nincs benne a zsarolás, amit nem tudunk becsülni)

Bizalmas információ lopása

- Amit az ember a saját gépén tárol: bankkártya-szám, üzleti információ, jelszavak
- bankszámlaszám: 1-től 1500 dollárig
- "carder" - bankkártya-hamisítók
- Brazil bűnözők 4.74 millió dollárt hívtak le pc-kről szerzett információkkal
- E-mail címek gyűjtése
- 1 millió e-mail cím 20 dollártól 100-ig terjed
- Ugyanennyi címre e-mail küldés 150 dollártól 200-ig terjed

Adathalászat

- A szervereket nagyüzemben gyártják, de védeni kell őket a bezárás ellen
- Botnetekkel néhány percenként lehet IP-címet váltani egy domain névhez
- "fast flux" szolgáltatás
- Havi díj: 1000-2000 dollár

Spam

- A Kaspersky Lab szerint a spam 80%-át botnetek küldik
- Viagra, másolt órák, online kaszinók
- 2008-ban 780 millió dollár bevételt értek el a spammelők

Search Engine Optimisation (SEO) Spam

- Page ranking
- Botnetekkel feljebb lehet tornázni a honlapunkat a keresési listán
- Egyik szempont: hány link mutat a honlapunkra

Adware, malware

- Épp egy autós magazint olvasunk, amikor hirtelen feljön egy ablak, ami autóalkatrészeket kínál
- Nem installáltunk semmit. De nem is kell: a botnet üzemeltetői gondoskodtak erről.
- J K Shiefer 2007-ben havi 14000 dollárt keresett: egy 250000 gépet tartalmazó botnettel 10000 gépre installált szoftvereket.

Klikkeléses csalás

- A hirdető cégek klikkelés alapján fizetnek
- Botnettel egyszerű csalni
- Google AdSense: a vevők a Google-nek fizetnek a klikkelésért
- A Google más webszajtokon is hirdeti ezt a céget, fizetve minden klikkelésért.
- Nehéz bíróság elé citálni ezért valakit
- A Click Forensics szerint a klikkelések 16-17%-a hamis, és ezek harmada botnetek által generált.
- Ez kb. 33 millió dollárt jelentett 2008-ban.

Botnetek bérlése és kereskedése

- Marx: áru - pénz - áru
- botnet - pénz - botnet