Sigurnosne prijetnje na Internetu

Mreže kompromitiranih računala (engl. Botnets)

Mihael Orsag, 22. siječnja 2025.

Pregled predavanja

- Pitanja za ispite
- Motivacija
- Što je mreža kompromitiranih računala?
- Životni ciklus mreže kompromitiranih računala
  - Troškovi
- Izvori novčane dobiti
- Zaključak

Pitanja za ispite

- Nabrojite barem tri stadija životnog ciklusa mreže kompromitiranih računala
- Nabrojite barem tri izvora novčane dobiti koje pruža mreža kompromitiranih računala
- Nabrojite barem tri motivacije za izradu mreže kompromitiranih uređaja
- Na koji način se radi marketing mreže kompromitiranih računala?
- Koja je najpopularnija metoda širenja mreže kompromitiranih računala?

Motivacija

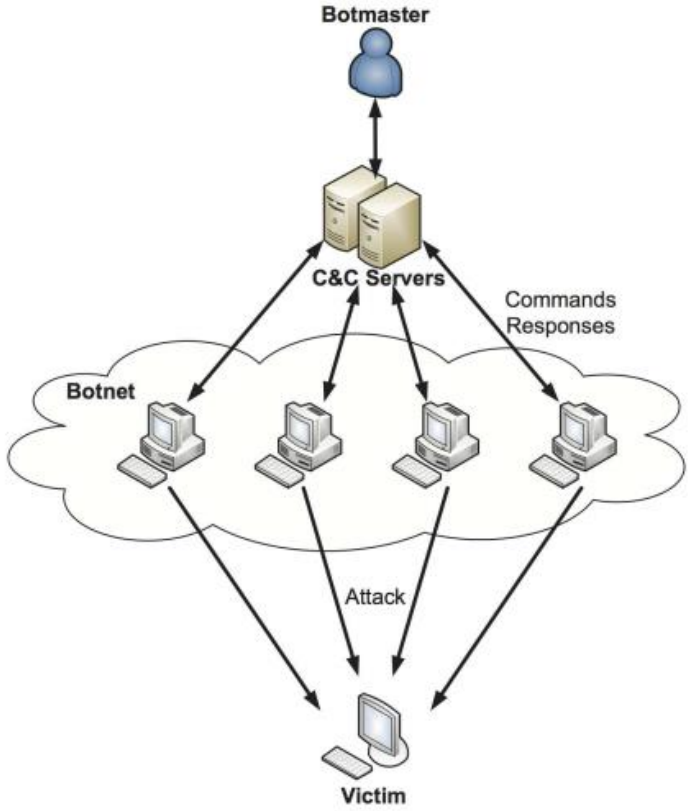
- Završili smo fakultet i želimo profitirati od proteklih 5 godina boli u leđima, neprospavanih noći, traumatičnih iskustava i silnog prikupljenog znanja
- Jesu li mreže kompromitiranih računala dobra opcija?

Motivacija

- Radimo za tvrtku koja se specijalizira u obrani protiv mreža kompromitiranih računala
- Želimo doznati kako najbolje možemo pružati svoje usluge, odnosno štititi naše korisnike
- Ako znamo kako mreže kompromitiranih računala funkcioniraju, lakše ih možemo ugasiti

Što je mreža kompromitiranih računala?

- engl. *Botnet*
- Grupa računala povezanih internetom
- Kontrolira ih *botmaster*
- Zašto su korisni?
  - Transfer vlasništva
    - Ogromna količina dostupnih resursa ovisno o uređajima

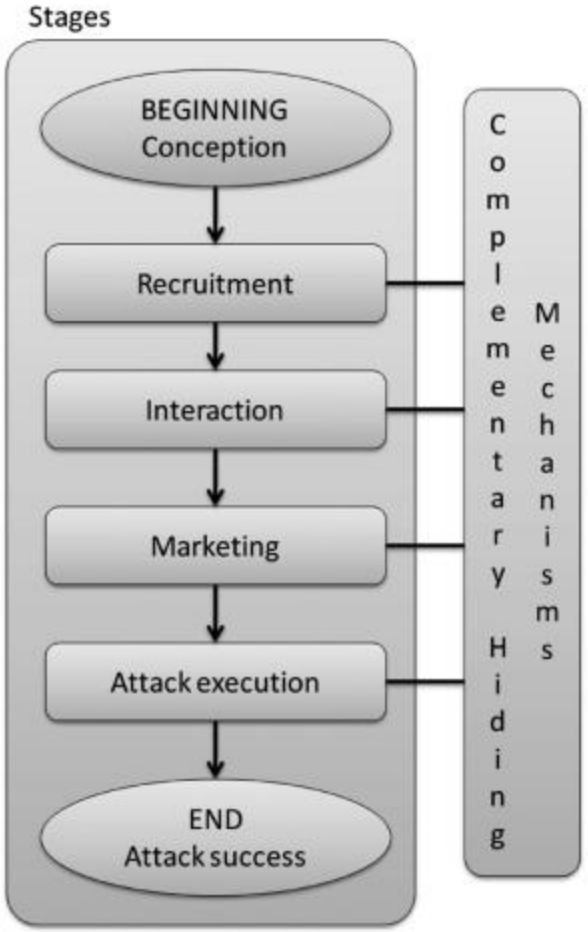


Slika 1: Tipična mrežna arhitektura mreže kompromitiranih računala [2]

Životni ciklus[4]

- Koncepcija
- Dizajn
- Stvaranje botneta
- Interakcija
- Marketing
- Izvršavanje napada
- Uspješan napad

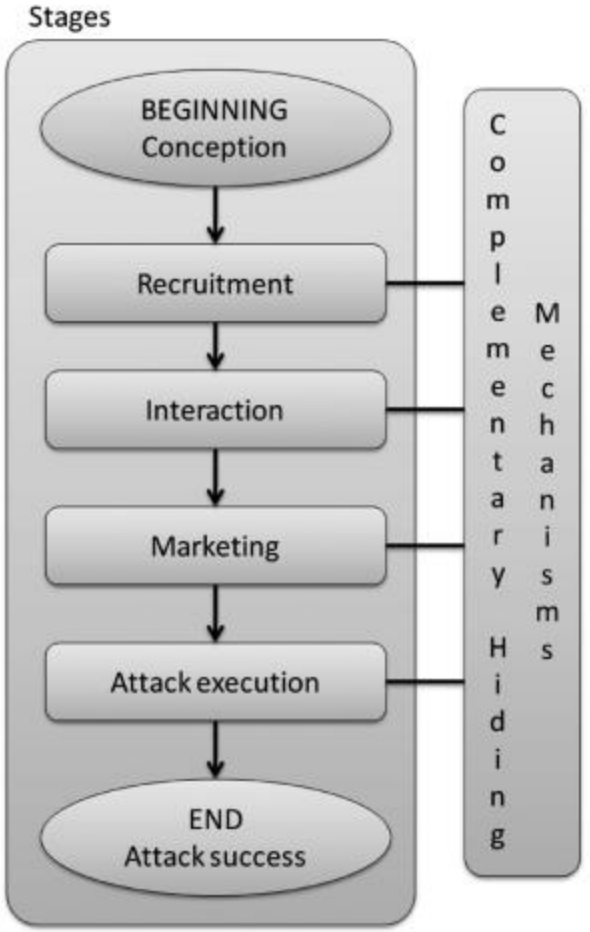
- Obično se više stadija događa istovremeno (npr. dok se botnet gradi izvode se napadi i radi marketing)



Slika 2: Botnet life-cycle [4]

Koncepcija[4]

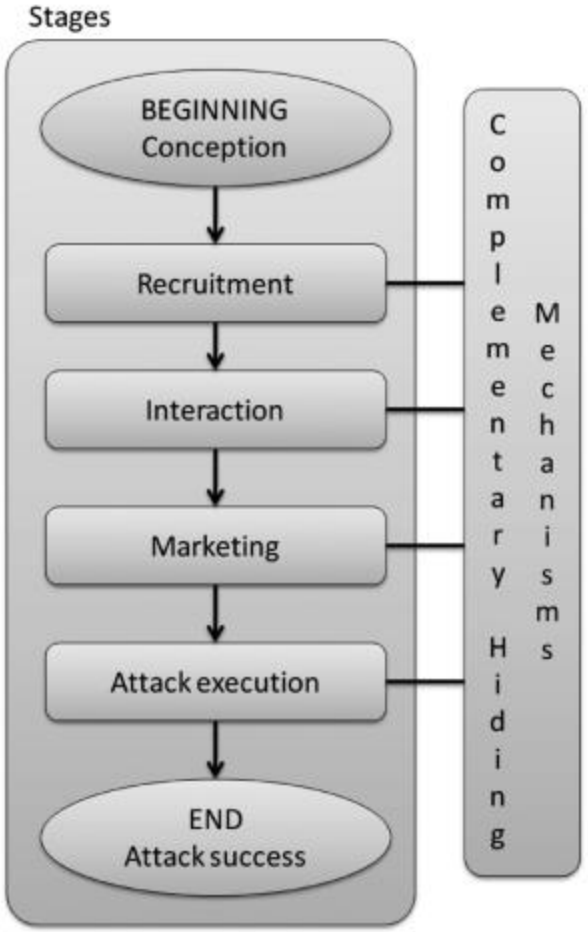
- Motivacija
  - Ego
  - Reputacija
  - **Novac**
    - Primarni
  - Viša svrha
  - Socijalni status



Slika 2: Botnet life-cycle [4]

Stvaranje botneta[4]

- Skeniranje interneta za ranjivim uređajima
  - Mirai botnet
- Drive-by-download
- Pay-per-install
  - najpopularniji



Slika 2: Botnet life-cycle [4]

Stvaranje botneta - troškovi[3]

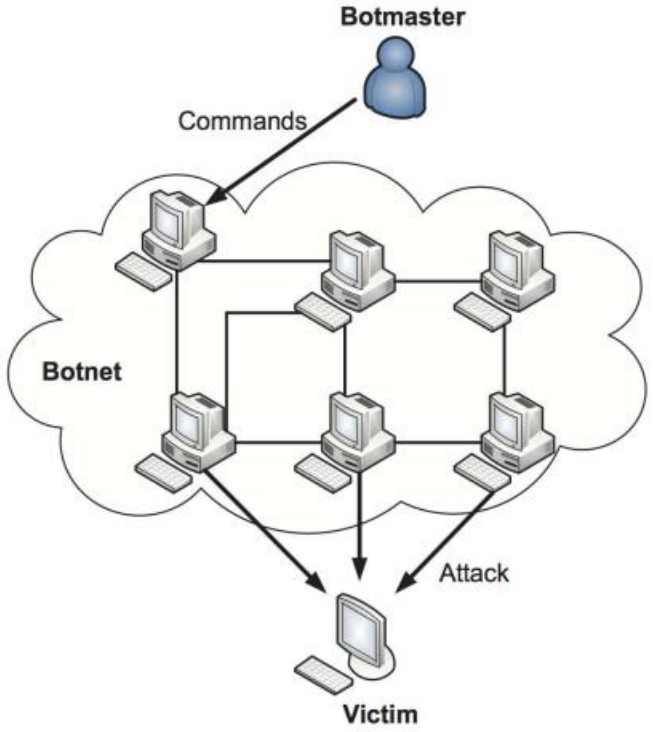
- Skeniranje Interneta
  - 2^32 x 1 minuta = 8171 godina
- Drive-by-download
  - Potrebne infrastruktura za posluživanje stranica
- Pay-per-install
  - $7 - $180 po 1000 instalacija
  - ~$0.0935 po instalaciji
  - Konstantan trošak - dinamičnost botneta

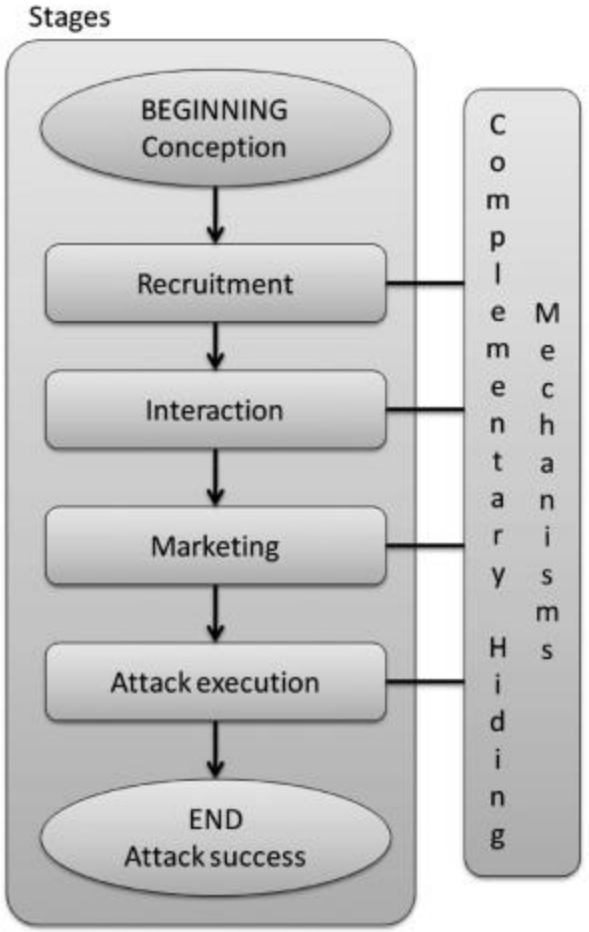
Stvaranje botneta - troškovi[3]

- Zlođudni program je prije svega program
  - Potrebno vrijeme i novac za razvijanje
- ~$59 po satu ~ $10384+ mjesečno
  - Prije nego li botnet uopće postoji i ima priliku pokriti troškove
- Gotovi paketi – ZeuS, Mirai
  - $700, $30

Dizajn[4]

- Arhitektura
  - Centralizirana
    - Postoje C^2 serveri
  - Decentralizirana
    - Svako kompromitirano računalo je i C^2 server
  - Hibridna
    - Podmreže kompromitiranih računala
- Protokol
  - Različite kompleksnosti

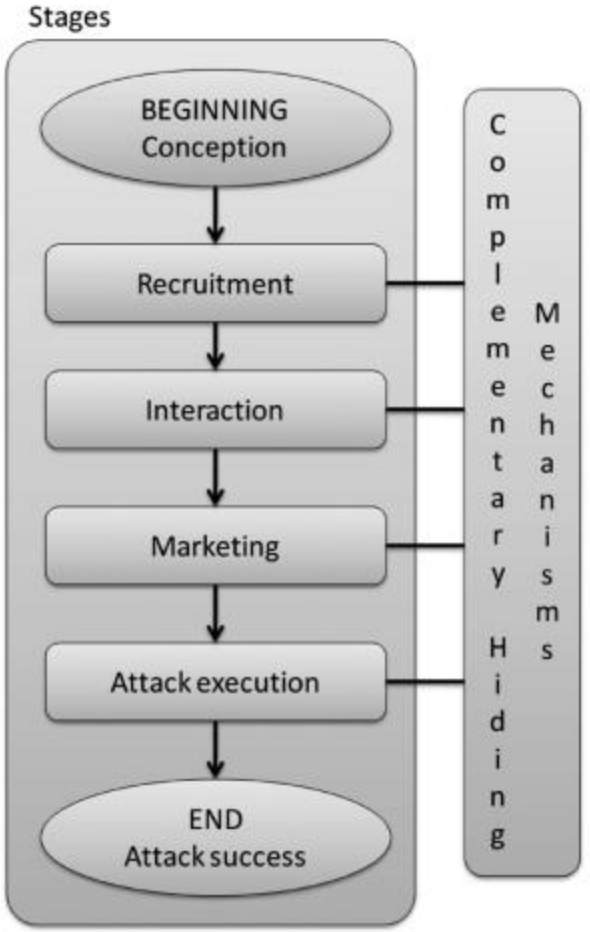




Slika 2: Botnet life-cycle [4]

Interakcija[4]

- Komunikacija s C2 serverima
- Registracija novih računala
  - Proces kroz koji se inficirani uređaj pridružuje botnetu
  - Dinamička
    - Prikupljanje informacija za prijavu od neutralne treće strane
  - Statička
    - Informacije za prijavu su instalirane zajedno s zlćudnim kodom



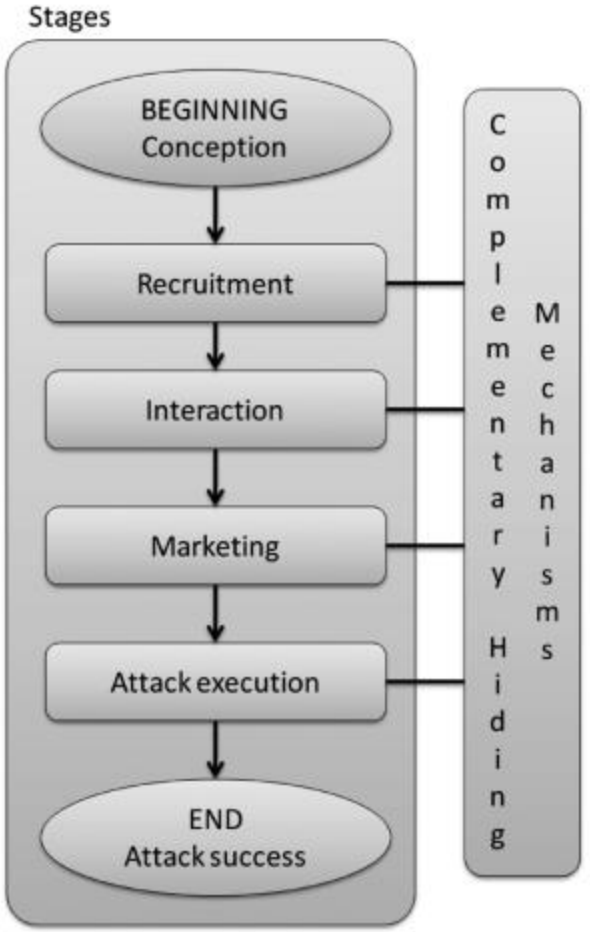
Slika 2: Botnet life-cycle [4]

Interakcija - troškovi[3]

- Komunikacija s C2 serverima
  - Domain flux
    - više desetaka domena tjedno koje se koriste za komunikaciju između botova i C2 servera
    - $10 - $20 godišnje za .com i .net
    - $1 - $10 godišnje za novije poput .shop i .club

Marketing[4]

- Reklamiranje činjenice da mreža kompromitiranih računala postoji i koje usluge nudi
  - Može biti samo prodaja
- Obično preko *darkweb* foruma, no moguće i preko "legitimnih" usluga
  - Booteri



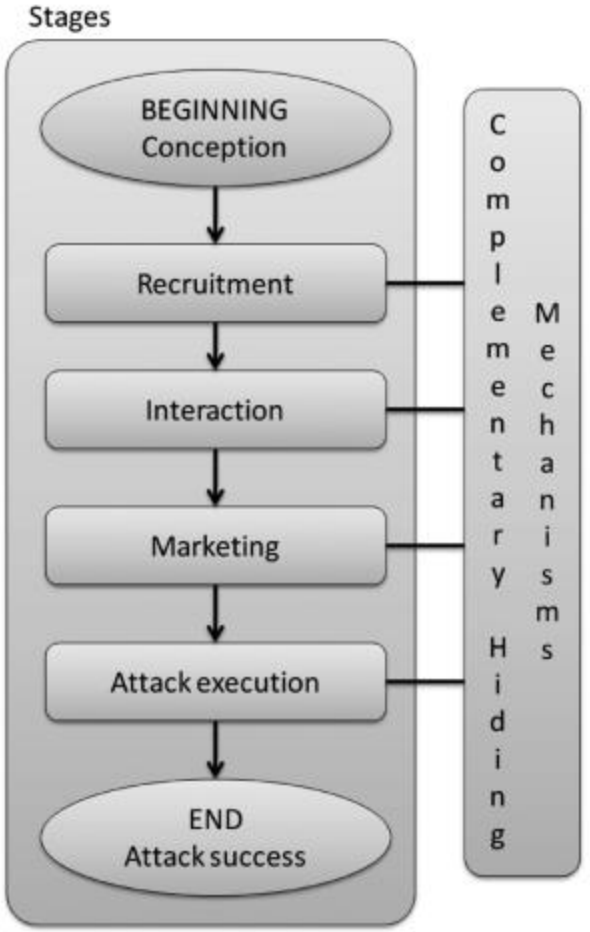
Slika 2: Botnet life-cycle [4]

Marketing - troškovi[3]

- Minimalni
- Potrebno je jedino vrijeme
- Na što se više različitih stranica oglas pojavi, veće su šanse da će se pojaviti zainteresirani korisnici

Izvođenje napada[4]

- Botmaster preko C&C servera šalje botovima informacije o napadu (meta, parametri napada, …)



Slika 2: Botnet life-cycle [4]

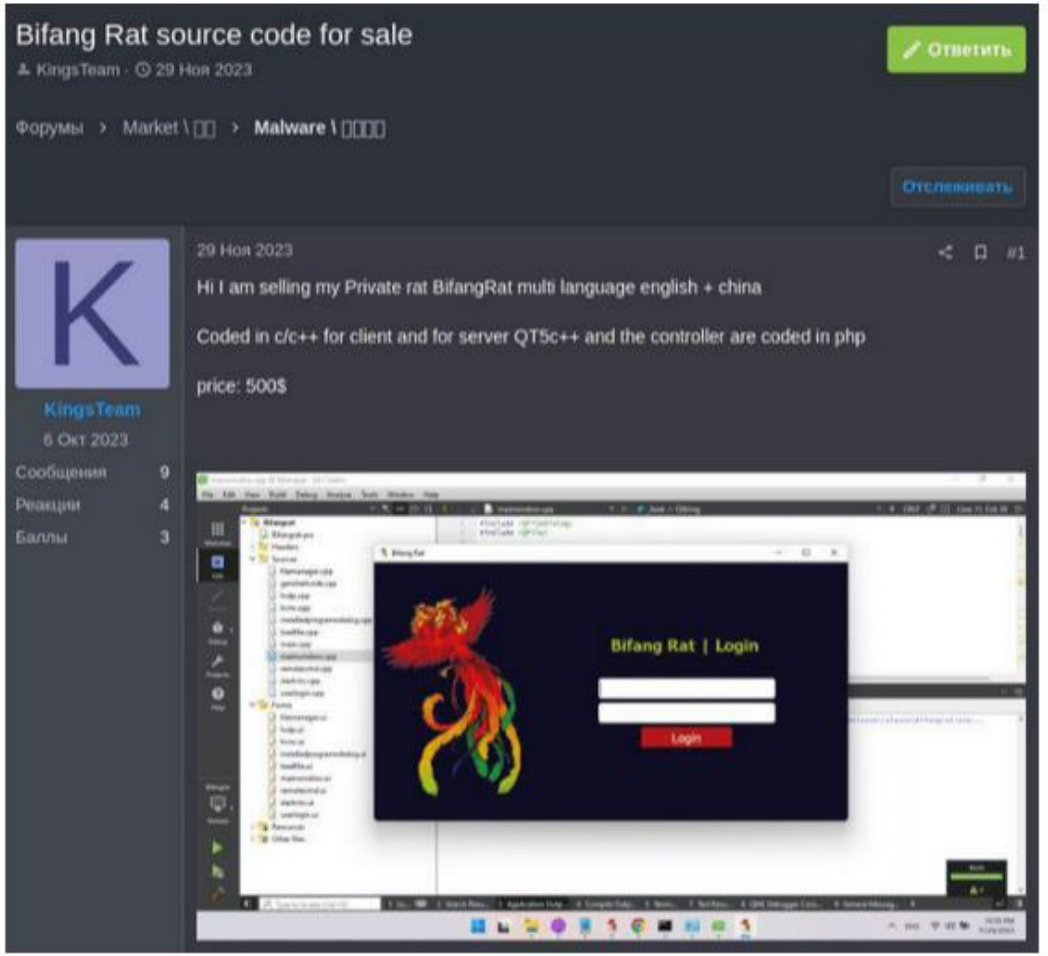
Dugoročni troškovi[3]

- Najveća komponenta cijene programa
  - Održavanje
    - Što botnet duže postoji, to je kompleksniji te treba više vremena za njegovo održavanje
    - Ranjivosti se uklanjaju i nastaju
      - Potrebno inkorporirati u zlćudni kod

- $59 po satu – 4 sata dnevno ~ $62000 godišnje

Izvori novčane dobiti

- Jednokratni
  - Prodaja mreže kompromitiranih računala
  - Prodaje se kod
  - Cijene od $99 do $10,000
    - Ovisno o veličini mreže



Slika 4: Oglas za prodaju koda mreže kompromitiranih računala [6]

Izvori novčane dobiti[3]

- Ponavljajući
  - *DDoS*
  - *Crawling*
  - *Scraping*
  - *Spam*
  - *Fast-flux hosting*
  - *Search engine spam*

Izvori novčane dobiti[3]

- DDoS
  - Stresseri/Booteri
  - $50 - $x000 dnevno ovisno o veličini

- *Scraping*
  - Email adrese koje se koriste pri *spam* kampanjama
  - $20 - $100 po milijun adresa

Izvori novčane dobiti[3]

- *Spam*
  - $150 - $200 po milijun email adresa

- *Data harvesting*
  - Prikupljanje podataka s kompromitiranih računala
  - $7 - $15 po korisničkom računu
  - $10 - $20 po 1000 podataka o kreditnim karticama

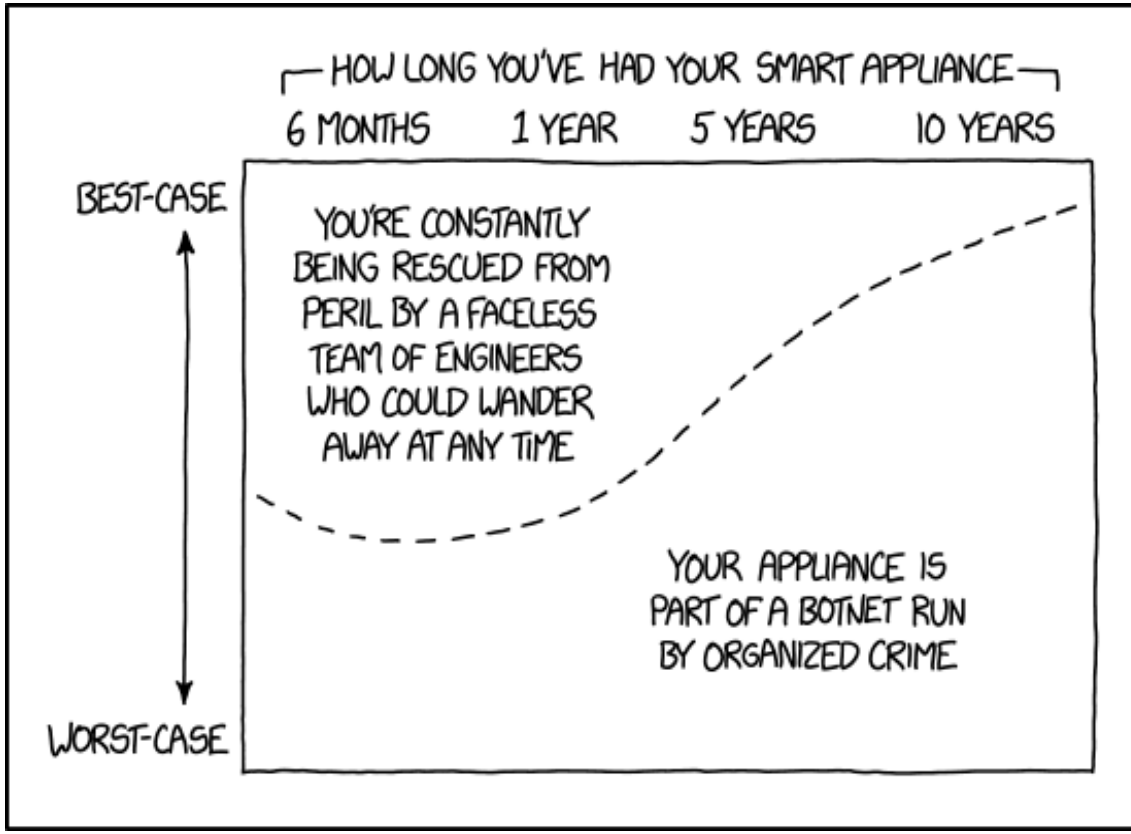
Izvori novčane dobiti[3]

- *Fast-flux* mreže
  - Posluživanje ilegalnih sadržaja preko botneta, gdje se botovi ponašaju kao posrednici
  - $1000 - $2000 mjesečno

- *Search engine spam*
  - "Namještanje" algoritma za pretraživanje/preporuku
  - Oko $300 mjesečno

Zaključak

- Botneti rastu iz dana u dan
  - Više uređaja, više mogućih članova u mreži (IoT)
- Visoka kompleksnost
  - Potrebno dobro poznavanje mreža, infrastrukture i sigurnosti
- Velik broj opcija za ostvarivanje novčane dobiti kao i visoki troškovi



Literatura

1. Bailey, Michael, et al. "A survey of botnet technology and defenses." 2009 Cybersecurity Applications & Technology Conference for Homeland Security. IEEE, 2009.
2. Mahmoud, Muhammad, Manjinder Nir, and Ashraf Matrawy. "A survey on botnet architectures, detection and defences." Int. J. Netw. Secur. 17.3 (2015): 264-281.
3. Putman, C. G. J., and Lambert JM Nieuwenhuis. "Business model of a botnet." 2018 26th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP). IEEE, 2018
4. Rodríguez-Gómez, Rafael A., Gabriel Maciá-Fernández, and Pedro García-Teodoro. "Survey and taxonomy of botnet research through life-cycle." ACM Computing Surveys (CSUR) 45.4 (2013): 1-33.

Literatura

5. Stringhini, Gianluca, et al. "The harvester, the botmaster, and the spammer: On the relations between the different actors in the spam landscape." Proceedings of the 9th ACM symposium on Information, computer and communications security. 2014.

6. Kaspersky: "Kaspersky finds botnet prices starting at $100 on dark web market". https://www.kaspersky.co.uk/about/press-releases/kaspersky-finds-botnet-prices-starting-at-100-on-dark-web-market. Pristupljeno: 21.1.2025.

Dodatna literatura

1. Bottazzi, Giovanni, and Gianluigi Me. "The botnet revenue model." Proceedings of the 7th International Conference on Security of Information and Networks. 2014.
2. Georgoulias, Dimitrios, et al. "Botnet business models, takedown attempts, and the darkweb market: A survey." ACM Computing Surveys 55.11 (2023): 1-39.

Hvala!