Temă de casă
REȚELE DE CALCULATOARE ȘI INTERNET

Rețele de boți

Andrei CIORAN
Master IISC, An 2

Cuprins

- Introducere
- Istorie
- Tipuri de botnet-uri
- Metode de gestiune a botnet-urilor
- Metode de răspândire
- Motivație
- Concluzii

Malware - Introducere(1)

Diferite termene cum ar fi virus, vierme, troienii, rootkit, și altele au fost stabilite pentru a clasifica diferitele tipuri de malware:

- **Virușii** - virus de calculator este un program de calculator care se poate reproduce [1] și răspândi de la un calculator la altul.
- **Viermii** - spre deosebire de un virus de calculator, un vierme nu are doar capacitatea de a se copia la diferite medii, dar este, de asemenea, capabil să se răspândească în mod activ[2].
- **Troienii** - un cal troian ascunde rutine de malware pretinzând că ar fi software legitim.Pretinzând să au un scop legitim, acestea păcălesc utilizatorul să instaleze software-ul sau să execute codul care conține calul troian, software ce încarcă apoi rutine încorporate malware.

Malware - Introducere(2)

- **Spyware** - este un termen generic pentru software-ul scris cu intenția de extragere de date.
- **Keylogger** - înregistrează intrările de la tastatură, în scopul de a captura parole
- **Sniffere** -Instrumentele provenind din domeniul analizei de rețea, care au fost găsite utile într-un context rău intenționat, fiind folosite pentru a trage cu urechea la traficul din rețea, în scopul de a obține parole
- **Rootkit** - este o colecție de instrumente care ajuta dezvoltatorii să prevină anumite rutine și procese de a fi detectate sau dezactivate. Ideea din spatele unui rootkit este de a asigura prezența continuă a proceselor proprii sau pentru a menține accesul la un sistem remote

Malware - Evoluție

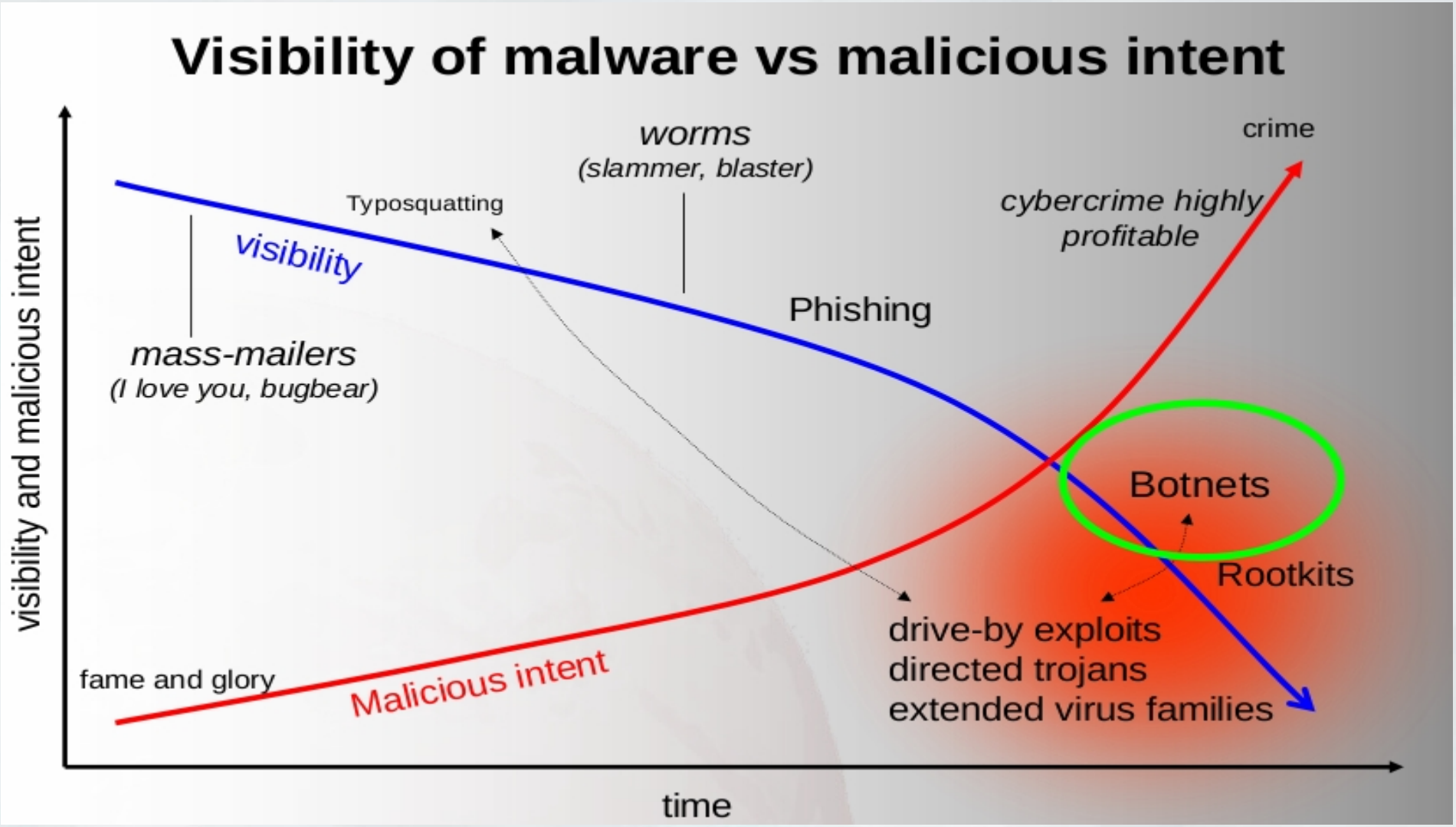


Figura 1 – Evolutia malware-ului[3]

Botnet-uri - Istorie

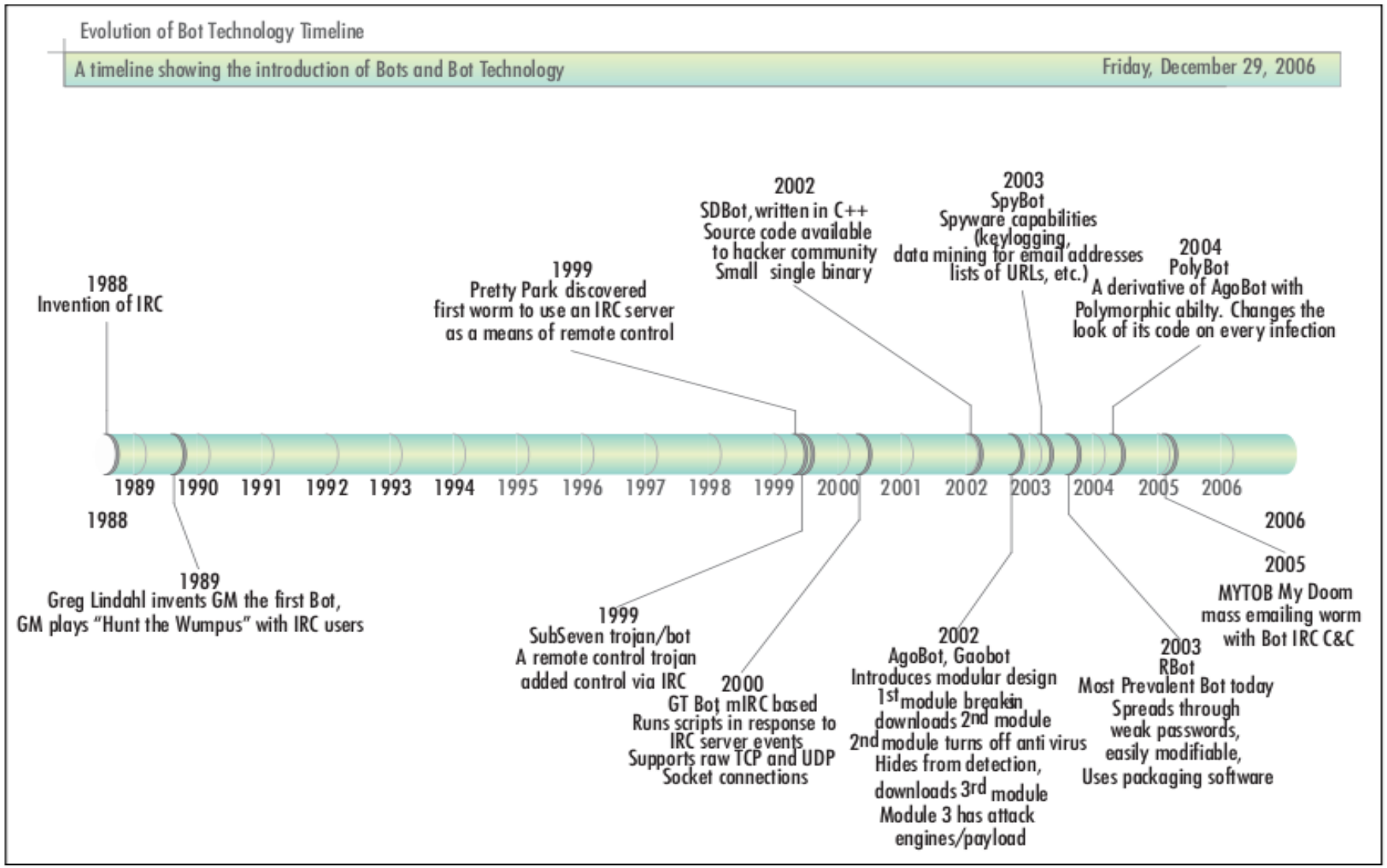
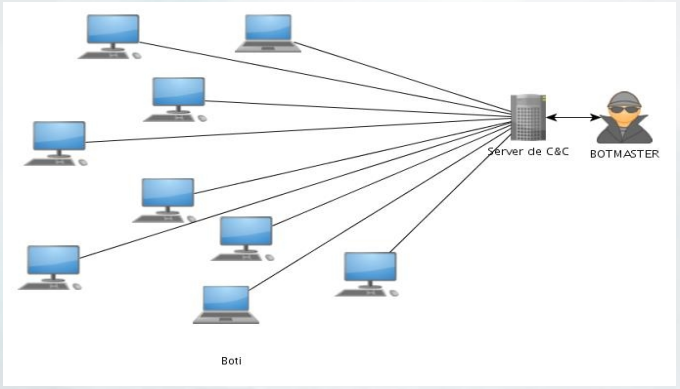


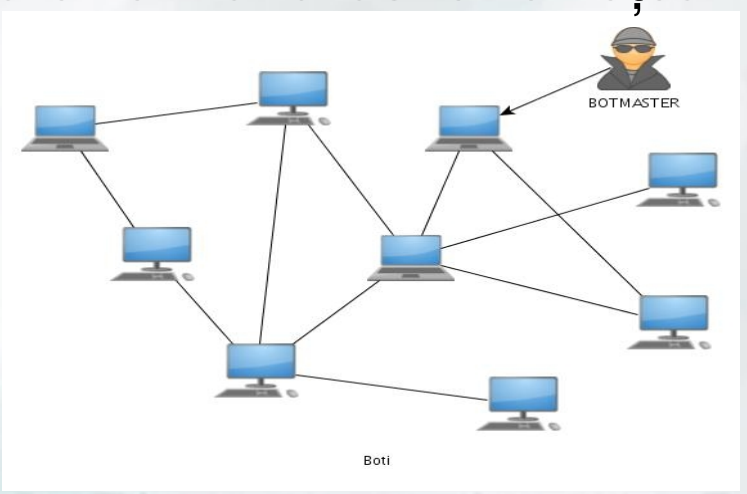
Figura 2 – Istoria botnet-urilor[4]

Botnet-uri - Introducere

O definiție modernă a bot-ului este un concept avansat de software rău intenționat care încorporează, de obicei, unul sau mai multe aspecte ale malware-ului prezentat, pentru înmulțire și integrare într-un sistem, oferind funcționalitatea compromisă a sistemului atacatorului.

O caracteristică definitorie a boților este faptul că, după ce compromite cu succes sistemul gazdă, se conectează la un server central sau alte mașini infectate formând astfel o rețea. Această rețea este numită un botnet.





Botnet-uri - Arhitectura centralizată

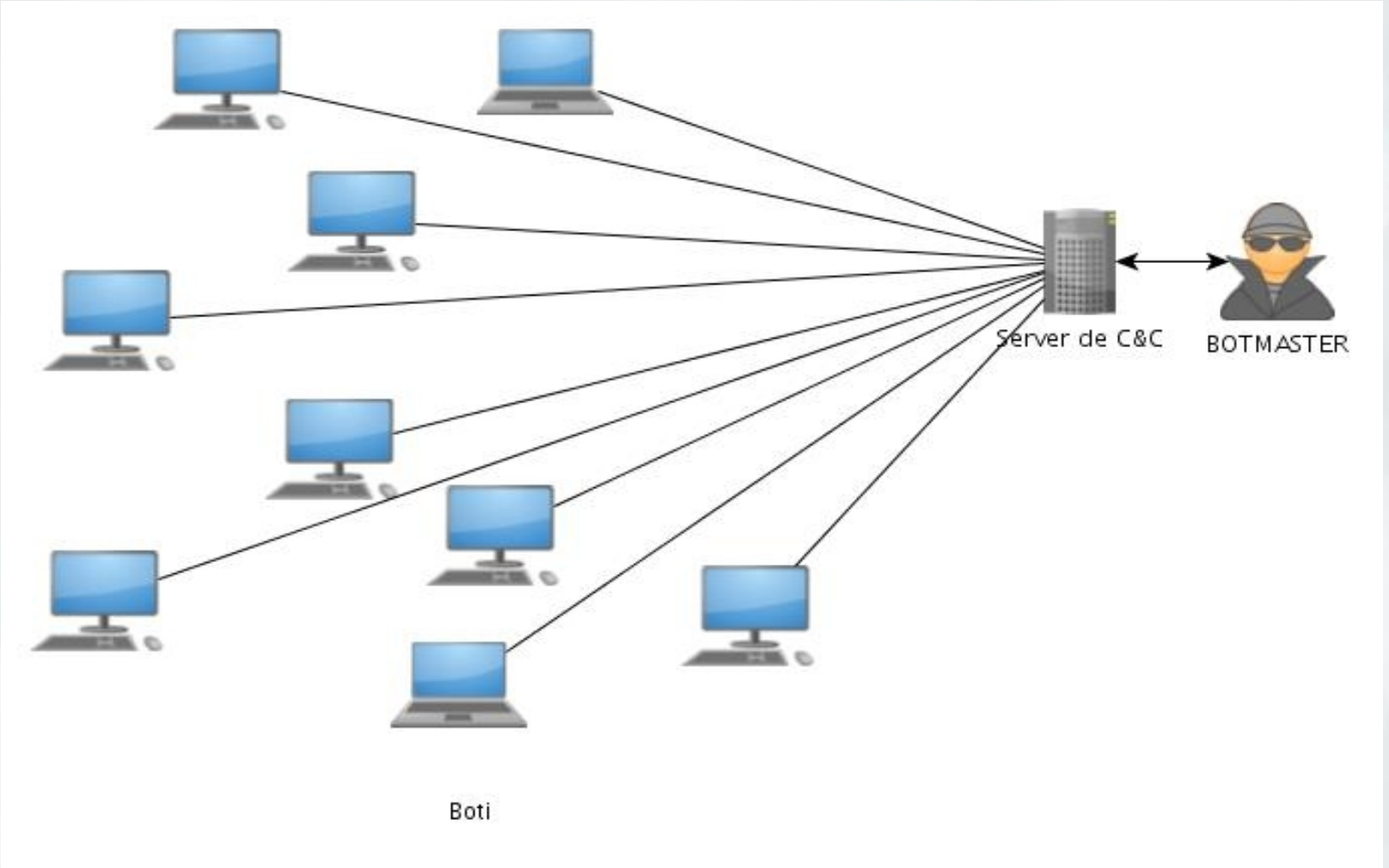


Figura 3– Botnet cu arhitectura centralizată

Botnet-uri - Arhitectura descentralizată

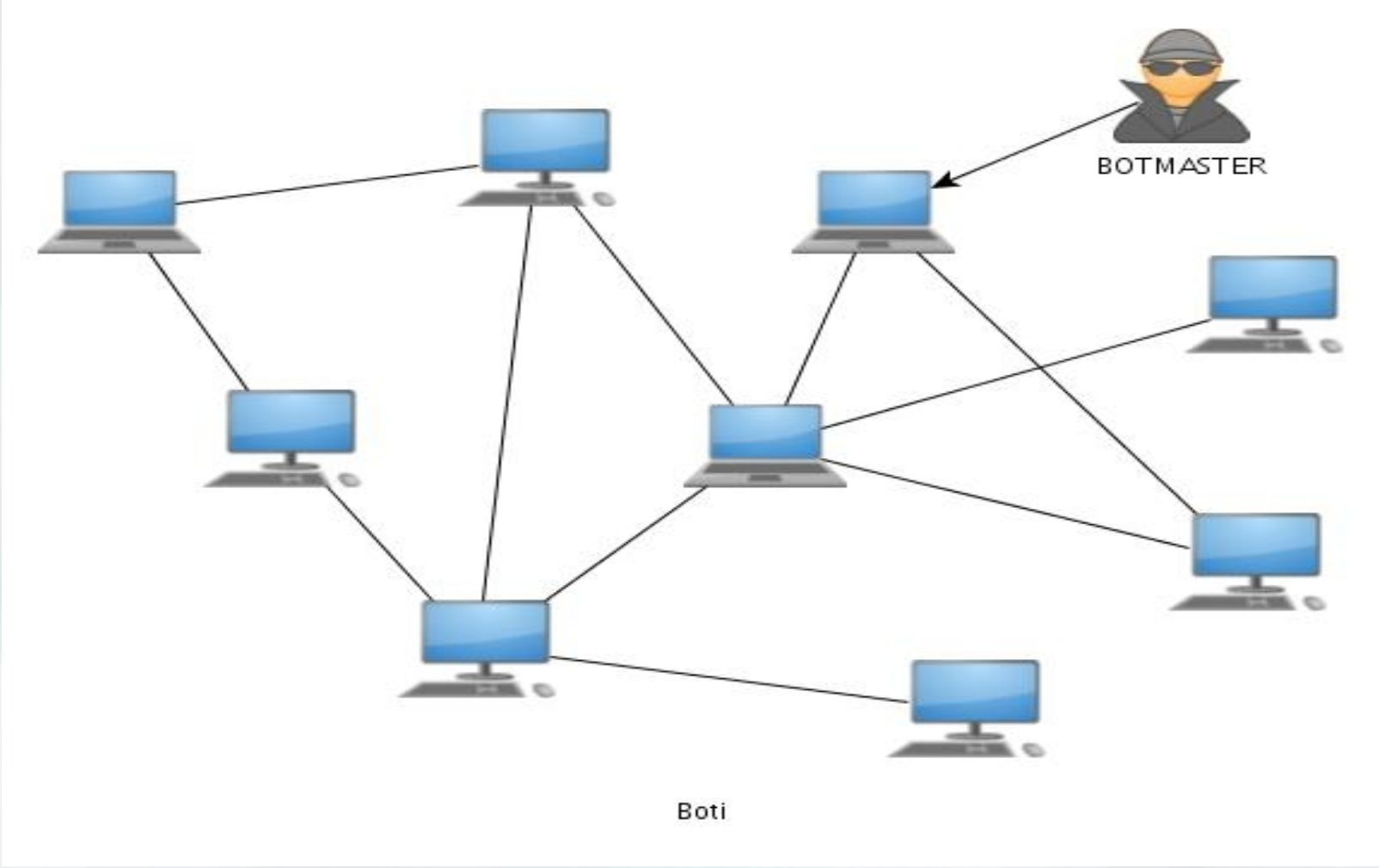


Figura 4 – Botnet cu arhitectura descentralizată

Botnet-uri – Fast-flux Services Networks

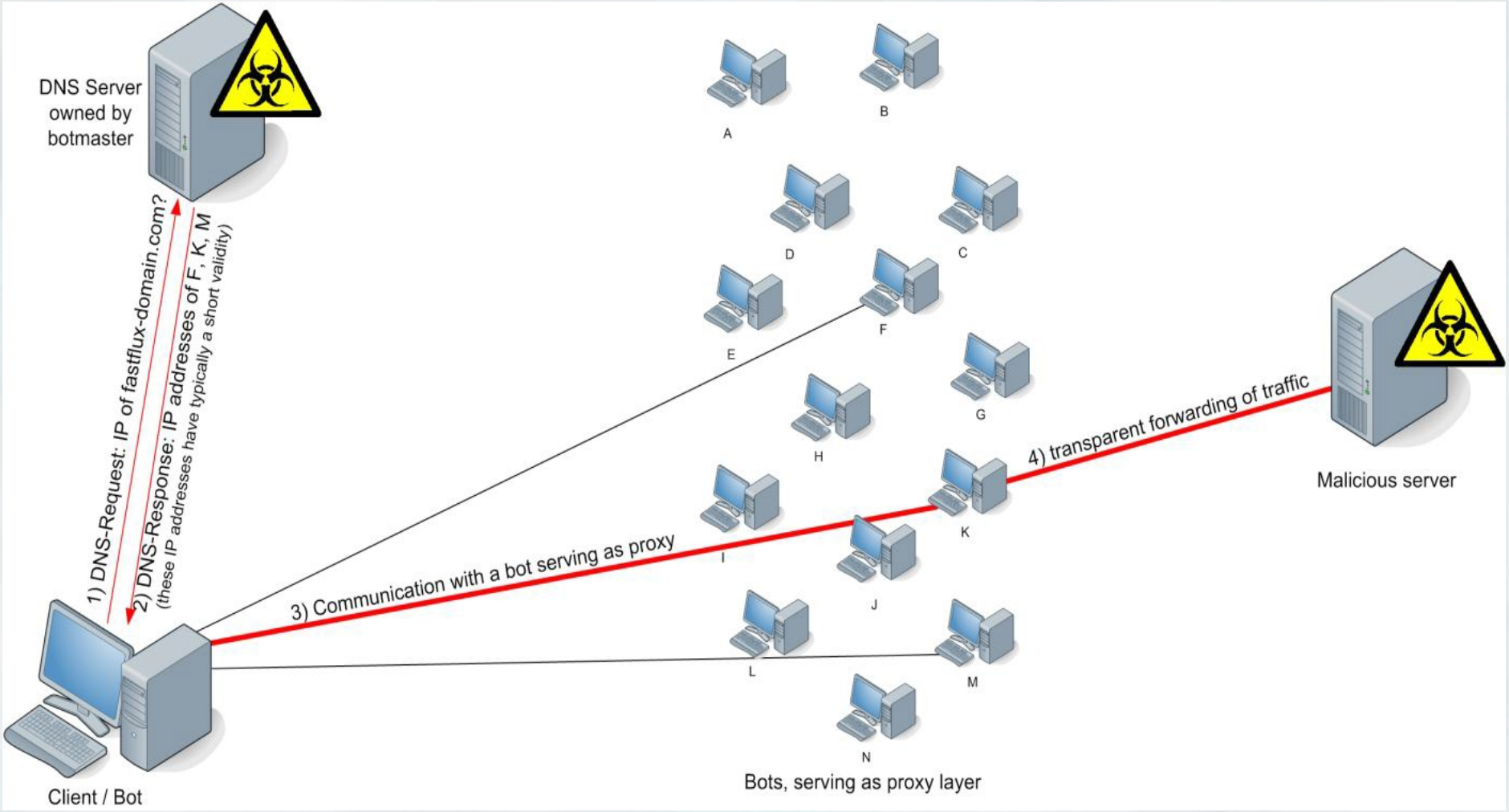


Figura 5 – FFSN – exemplu de functionare[5]

Botnet-uri – Botnet cu locomoție

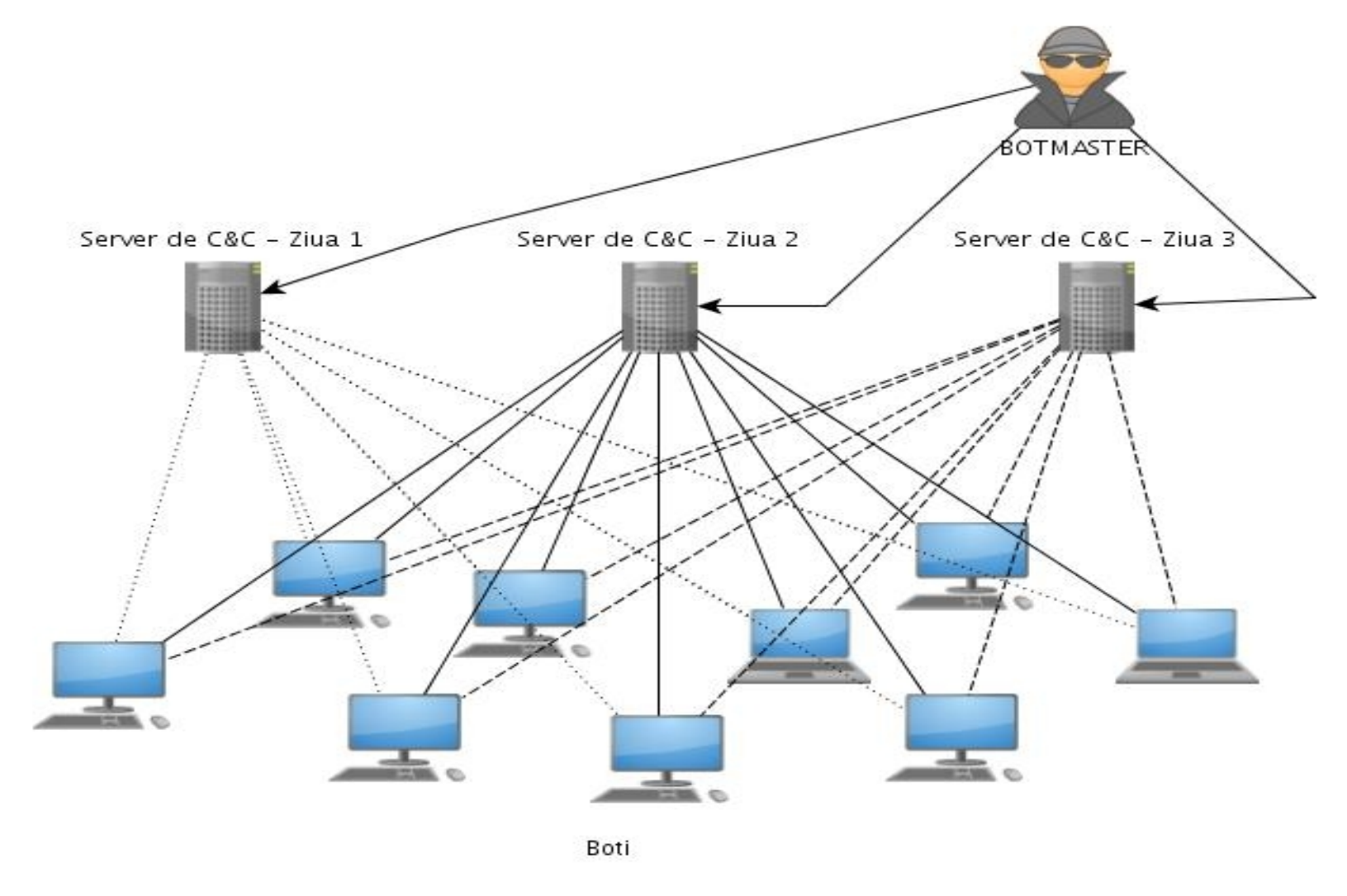


Figura 6 – Exemplu de rețea cu locomoție

Botnet-uri – Metode de răspândire

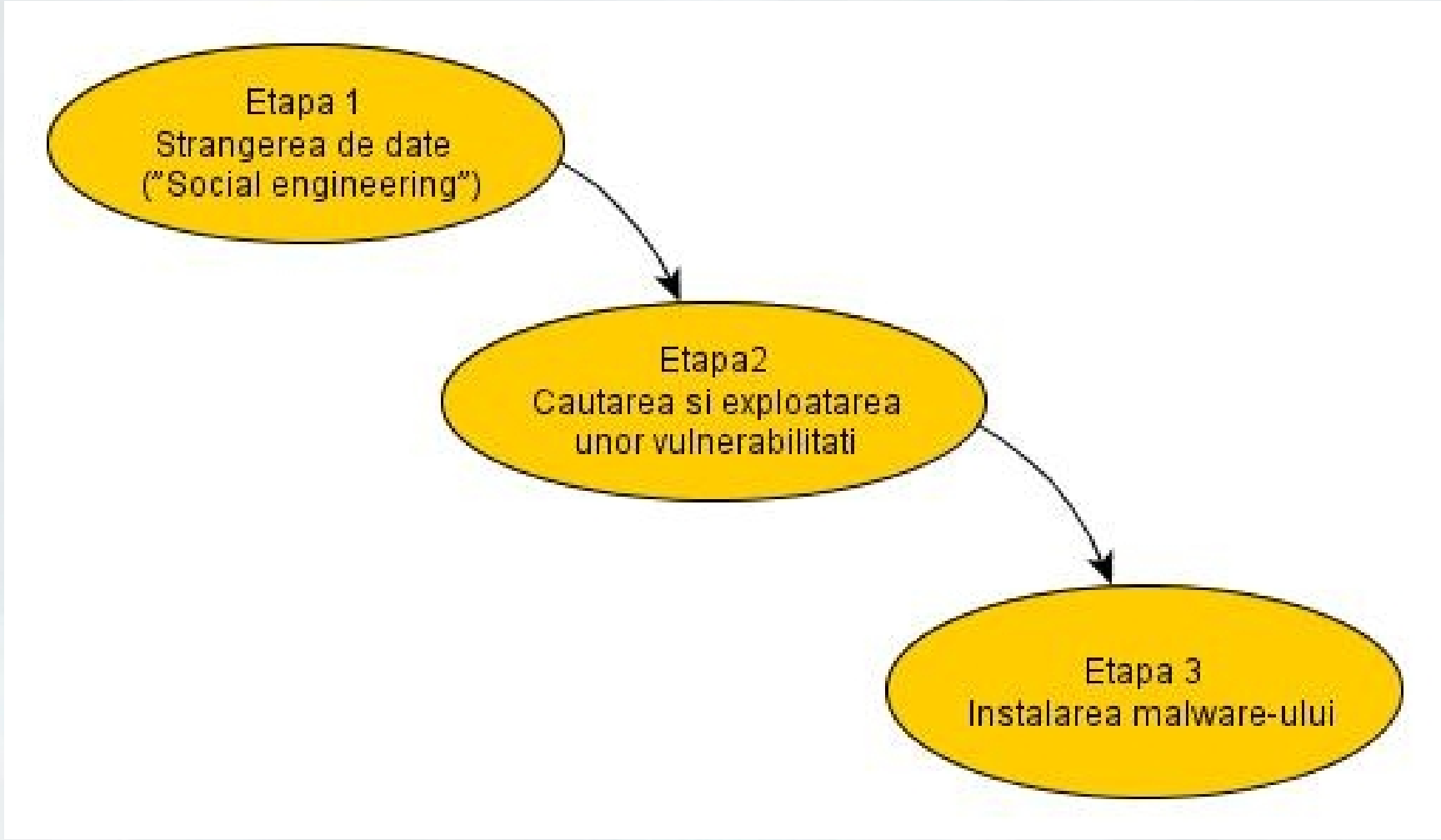


Figura 7 – Etapele răspândirii unui malware

Botnet-uri - Contactarea serverului de C&C

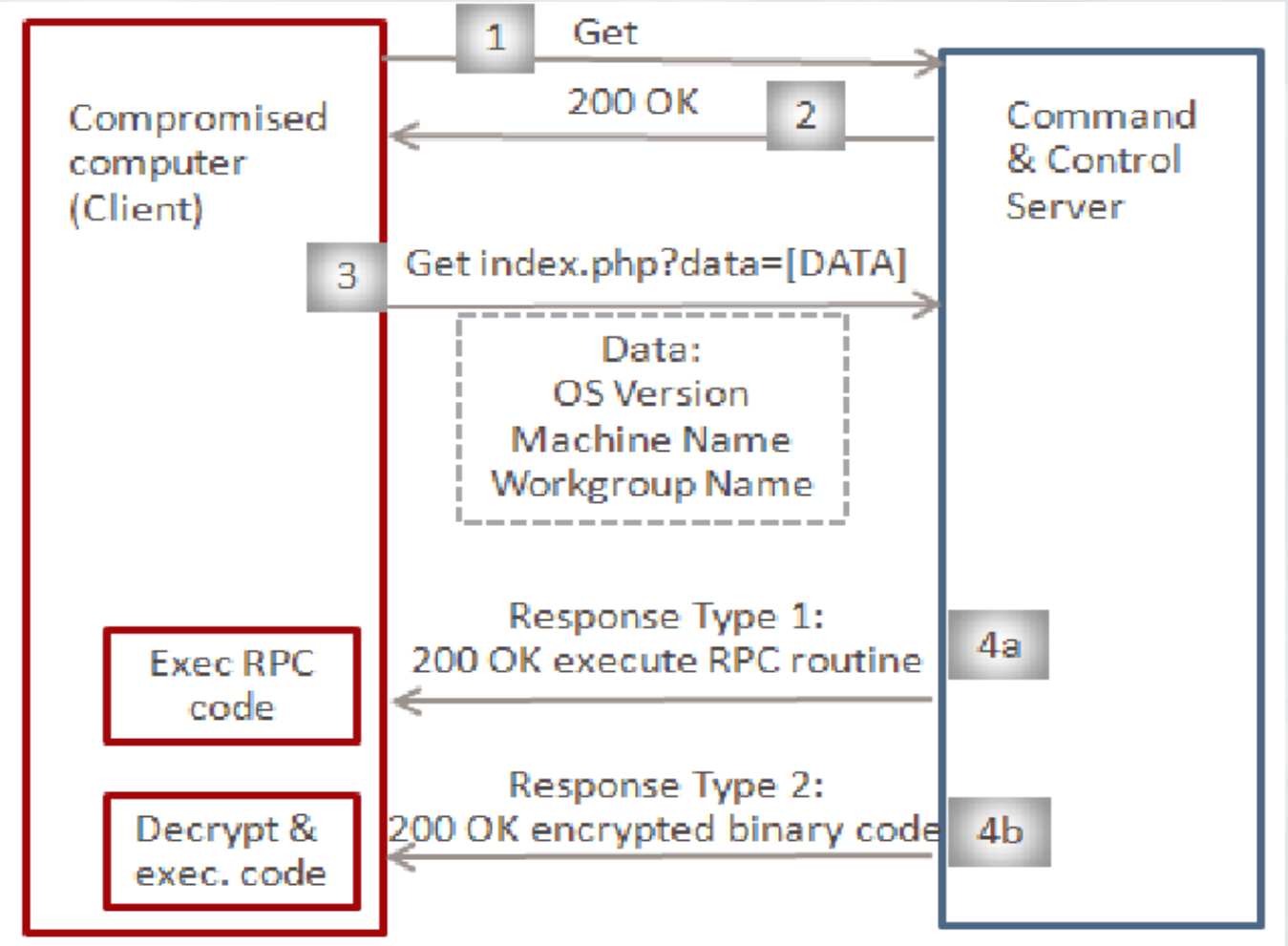


Figura 8 – Un model de contactare a serverului de comanda si control[7]

Botnet-uri - Motivație

Furtul de identitate - extragerea automată a datelor de utilizator și a acreditărilor din sistemele infectate. Obiective-cheie includ parole pentru diferite servicii cum ar fi conturi de e-mail, magazine online, platforme bancare sau platforme de social networking

Trimiterea de e-mail-uri nesolicitate - Una dintre cele mai populare utilizări ale botnet-urilor

Fraudarea click-urilor- Un alt mod de monetizarea a botnet-urilor este prin ceea ce se numește fraudarea click-urilor

Atacuri de tip DDOS (Distributed Denial Of Service)- Botnet-urile constau de obicei în număr atât de mare de sisteme controlate de la distanță încât lățimea lor de bandă cumulată poate ajunge la mai mulți GB de trafic pe secundă. Acest lucru permite botmaster-ilor să pornească atacuri împotriva site-uri web.

Botnet-uri - DDoS

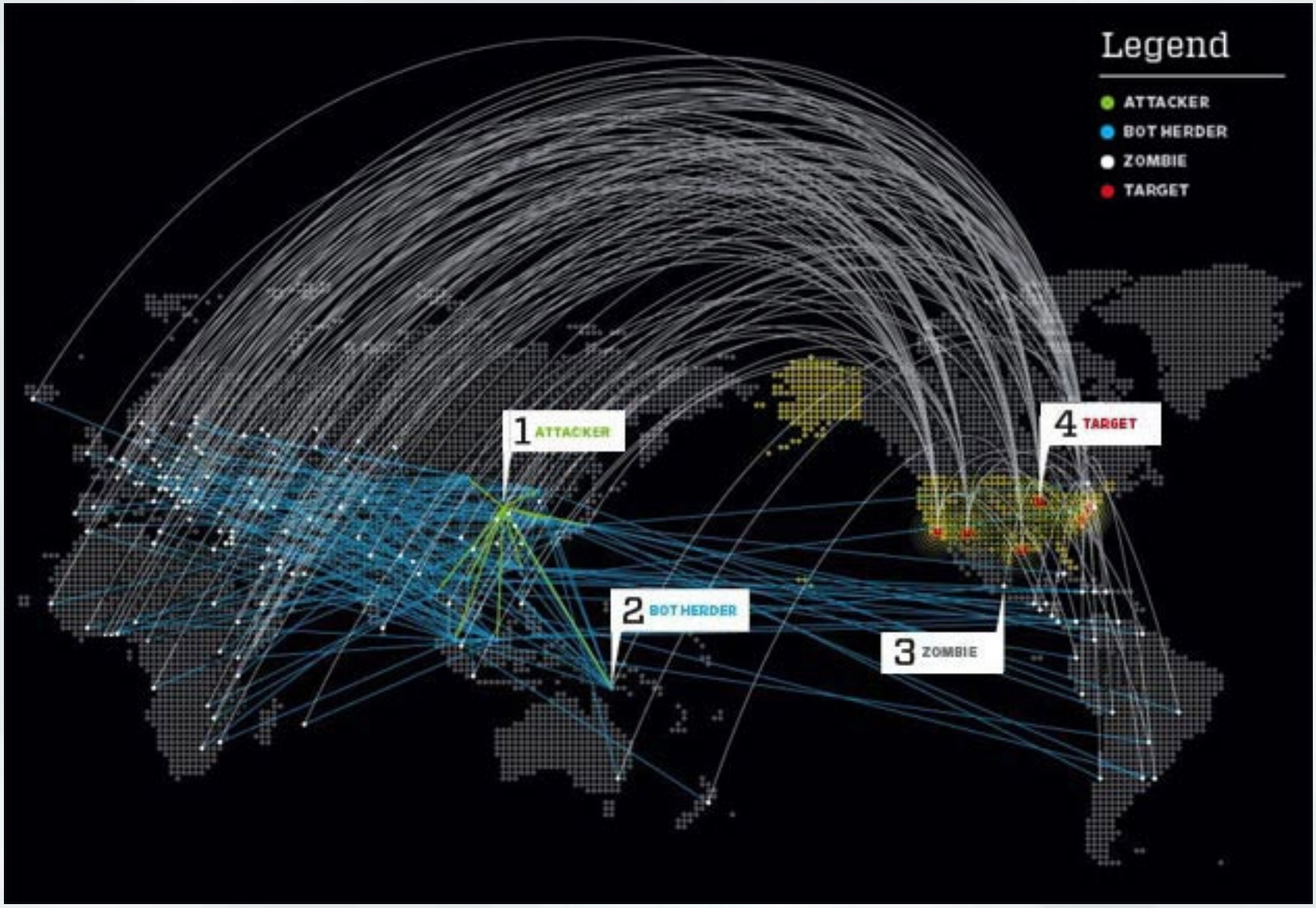


Figura 9 – Exemplu de atac DDoS[6]

Concluzii

Comercializarea de boți deschide piața botnet pentru botmaster-ii fără cunoștințe tehnice avansate. Acesta poate servi, de asemenea, ca un punct de intrare pentru părți cu interesele politice, ce pot folosi botnet-urile ca instrument de influență politică sau de terorism

Disponibilitatea tot mai mare a accesului la Internet mobil duce la creșterea posibilității ca smartphone-urile să fie compromise pe o scară largă. Smartphone-urile sunt atractive pentru infractori din cauza creșterii capacității de calcul și a capacității de a se conecta la Internet.

În ultima vreme a fost observată o rată ridicată a apariției de noi versiuni, lucru posibil prin conceptele de polimorfism și metamorfism. O tendință observată în ultimii ani este faptul că aceste modificări de cod sunt efectuate numai pe serverele de malware, ascunzându-se astfel mecanismele exacte de modificare de către cercetătorii din firmele de securitate.

Bibliografie

[1]Dr. Solomon's Virus Encyclopedia, 1995, ISBN 1897661002, Abstract at http://vx.netlux.org/lib/aas10.html

[2]Jussi Parikka (2007) "Digital Contagions. A Media Archaeology of Computer Viruses", Peter Lang: New York. Digital Formations-series. ISBN 978-0-8204-8837-0, p. 19

[3] Douwe Leguit, Manager Knowledge Center GOVCERT.NL, BOTNETS

[4] Botnets: The Killer Web App, Craig Schiller, Jim Binkley, Gadi Evron, David Harley, Carsten Willems, Tony Bradley, Michael Cross

[5] Botnets: Measurement, Detection, Disinfection and Defence, Daniel Plohmann, Elmar Gerhards-Padilla, Felix Leder, ENISA, 2007

[6] http://www.wired.com/politics/security/magazine/15-09/ff_estonia_bots

[7] http://www.symantec.com/connect/blogs/w32stuxnet-dossier