G Data press release 2012

Infractorii cibernetici profita de anonimat

Reteaua Tor controleaza computerele deturnate

Bucuresti (Romania) 25.09.2012 – Una dintre principalele preocupari ale infractorilor cibernetici este de a nu lasa amprente digitale pe Internet. Conform analizei efectuate de G Data Security Labs, autorii de malware izbutesc sa foloseasca reteaua globala Tor pentru intentiile lor. Atacatorii sunt operatorii botnet-urilor (administratori de botnet-uri) care folosesc servicii de anonimat pentru a ascunde comunicatia dintre serverele de control (C&C servers) si computerele infectate. G Data crede ca aceasta tactica va face mult mai dificila localizarea si clasificarea serverelor de control pe viitor.

Cum folosesc infractorii reteaua Tor?
Computerele deturnate (zombies) sunt controlate prin folosirea unei conexiuni directe la serverul de comanda si control (C&C server) sau la o platforma de comunicare P2P. Serverele C&C sunt ca niste centre de control al caror operatori obisnuiesc sa trimita comenzile catre computerele zombi. Aceasta face posibil, de exemplu, initierea si coordonarea atacurilor DDoS sau trimiterea de milioane de emailuri spam. Insa, o conexiune directa sau folosirea unei structuri P2P este foarte riscanta pentru administratori: autoritatile au timp si reusesc sa gaseasca locatiile serverelor C&C si sa le inchida. Datorita folosirii retelei Tor aceste actiuni sa se desfasoare cu dificultate pe viitor.

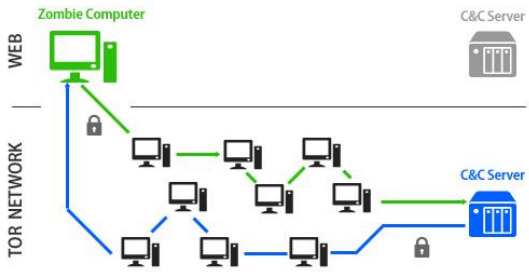

Figura 1: Acesta e modul in care atacatorii folosesc anonimatul retelei Tor pentru a controla computerele deturnate .

Ce este reteaua Tor?
Tor este o retea globala folosita de multi utilizatori pentru a naviga pe Internet in mod anonim fara a lasa niciun indiciu. Acesta serviciu nu este ilegal. Multi activisti politici arabi folosesc aceasta retea pentru a scapa din ghearele autoritatilor si de a evita sistemele de protectie web ale guvernelor.
Modul in care functioneaza reteaua Tor este simplu: utilizatorii potentiali isi lanseaza computerele ca Tunnels (releu Tor) si astfel devin unul dintre numeroasele puncte de trimitere pentru diverse servicii ale retelei Tor.
Spre exemplu, daca utilizatorul unui computer cauta o informatie pe o pagina de Internet in

browserul Tor, raspunsul catre serverul web nu este trimis direct, ci prin intermediul unui alt punct de trimitere necontorizat din retea. Asta inseamna ca este aproape imposibil de gasit adresa de IP originala a utilizatorului.

Ce este un botnet?
Un botnet este atribuit unei retele de computere conectate si infectate care este controlata de un administrator. Aceasta se intampla de obicei fara cunostinta si consensul utilizatorilor computerelor individuale care pot fi controlate de la distanta de un administrator de botneturi. Computerele infectate sunt numite zombie.

Figura 2: In trecut, serverele C&C comunicau direct cu computerele zombie.

Administratorul poate abuza de computerul victimei pentru a atinge diverse scopuri. Astfel, accesul la datele stocate in sistem si conexiunile dintre retelele de computere pot fi folosite fara ca victimele sa fie constiente de asta. Printre altele, botneturile sunt folosite pentru a lansa atacuri de suprasarcina asupra serverelor web (atacuri DoS si DDoS) si de a trimite mesaje spam.

-###-