Seznamte se - botnety

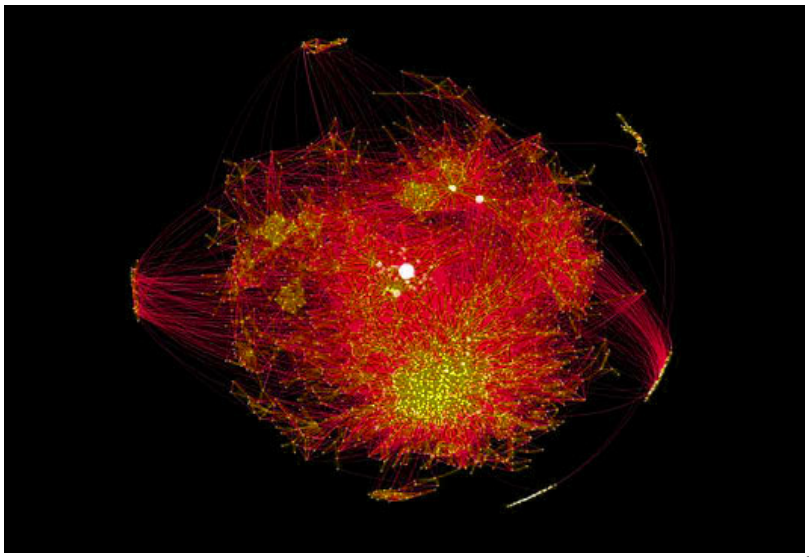
Vložil/a RubberDuck [1], 14 Listopad, 2012 - 23:00

- Unsorted [2]

Pojem botnet se v posledních několika letech stal každodenním pojmem. Tak každodenním, že už mu jen málokdo přikládá nějaký vyšší význam. Ale víme, co to skutečně botnet je, jaká je jeho historie a k jakým účelům je využíván? V následujícím článku se pokusím podat základní informace.

Pod pojmem botnet chápeme skupinu počítačů, tzv. botů, jenž podléhají příkazům nadřazeného počítače, tzv. řídícího a kontrolního centra (Command & Control Center). Boti se podle nastavení přihlašují k C&C, kde dostávají konkrétní příkazy, a ty následně vykonají. Jinými slovy, jedná se o aplikaci typu klient/server s vlastním komunikačním protokolem a vlastní sadou příkazů, přičemž samotný klient/bot může být trosjký kůň, červ nebo vir.

Na začátku všeho byly trojské koně. Programy tvořené klientskou a serverovou částí. Útočník zasílal koníkovi příkazy a on poslušně odpovídal. S postupujícím časem začalo být ovládání klasických trosjkých koní časově poměrně náročné. Důvod je jednoduchý: Tyto aplikace byly schopné v jediný okamžik komunikovat pouze s jedním cílem. V reakci na tento nedostatek se začaly objevovat první nesmělé pokusy o vytvoření multiklientských trojských koní. O prvním skutečném botnetu takovém, jak ho známe dnes, se začalo veřejně mluvit nejspíš na začátku roku 2004 v souvislosti s botnetem Bagle (první studie zabývající se myšlenkou sítě počítačů ovládaných z jediného místa je však mnohem starší - konkrétně z roku 1989). Šířil se v podobě červa otevírajícího backdoor na předefinovaném portu. Jeho hlavním cílem bylo rozesílání spamu. Téměř určitě lze ale předpokládat, že první skutečné botnety existovaly již před rokem 2004. Jen se o nich nevědělo nebo byly objeveny mnohem později.



[3]
Grafické znázornění celého botnetu může být občas úchvatné

V současné době se velmi často setkáváme s botnety využívajícími IRC servery jako C&C. Ve většině případů zakládají na PHP botovi z roku 2008. Princip získávání nových botů je pak velmi triviální. Botnet operátor na IRC kanále čeká na připojení dostatečného počtu botů. Následně jim zasílá dorky a boti, v kombinaci s vyhledávači typu google, hledají potenciálně zneužitelné webové systémy a pokoušejí se je exploitovat. Pokud se to podaří, pokusí se zapsat a uložit na web svou kopii a spustit ji. Pokud i s tímto uspěje, bot se následně přilásí na IRC server a je připraven přijímat příkazy. Tito boti kromě webových aplikací rovněž zkoušejí slabá hesla u FTP a SSH aplikacích na nalezených

serverech. Zjevným nedostatkem tohoto typu botnetu je příliš snadný přístup ke zdrojovým kódům a rovněž i snadný přístup ke kanálu.
Oblíbenější verze botnetů využívají pro komunikaci protokol HTTP. Ten je v trafficu méně nápadný a poskytuje o mnoho víc možností. Ukládáním většího množství dat počínaje a uploadem souborů konče. Kromě výše zmíněných nebo vlastních protokolů je možné se setkat i s exotickými implementacemi jako je ICQ nebo Jabber. Velmi zvláštní způsob komunikace zvolili autoři konceptu botnetu Stegobot. Zde se využívá kombinace technik steganografie a sociálních sítí umožňujících sdílet fotografie. Tyto v sobě obsahují zvláštní značky. Boti pak taková alba prochází a hledají označené obrázky. Pokud je najdou, jsou schopni z nich získat potřebné příkazy. S postupujícím čase jsou boti čím dál častěji vytvářeni modulárně a jednotlivé moduly se prodávají zvlášť. Jejich cena se v závislosti od druhu bota podstatně liší. Boti jsou programování pro userspace (Ring3), pro kernelspace (Ring0), bootkity, pro PC, chytré telefony, napříč všemi operačními systémy a pozvolna se objevují první pokusy o vytvoření botů pro síťové prvky - routery a síťové karty.

Účel botnetů je různý a záleží pouze a jen na funkcích jednotlivých botů. Botnety většinou neslouží k jedinému účelu. Celá síť je rozdělena do segmentů podle určitých parametrů botů (kapacita linky, lokace počítače, parametry počítače, velikost disku). Dříve byly nejrozšířenější spam botnety, Distributed Denial of Service a botnety určené pro směrování trafficu na konkrétní IP adresu. Později se začaly podstatněji prosazovat botnety vytvářející z cílových počítačů síť proxy serverů. V poslední době jsou nejrozšířenější tzv. bankery - boti kradoucí přihlašovací údaje do online bankovnictví, herních serverů a podobných služeb. Zvláštním typem botnetů jsou pak minery/crackery. Ty slouží k "těžbě" bitcoinů a podobných záležitostí nebo ke crackování složitějších hashů, než které zvládnou běžné online služby. Některé botnety vytváří vlastní peer-to-peer síť. Ta může sloužit například pro špionážní přenos citlivých dat z firemních sítí. U velkých sítí se některé segmenty pronajímají pro konkrétní účely.

V současné době patří mezi nejčastější prostředky distribuce botů exploitpacky [4].

[5]

Rozšíření botnetu Waledac

Zatímco dříve botnety využívali jen a jen kriminálníci, v současné době se k nim začínají připojovat i vlády a vládní organizace. Záměrem je vytvořit účinný prostředek pro případný kybernetický útok. Prvním veřejně známým představitelem botnetů tohoto typu je Duqu. Toho následoval Flame a tzv. MiniFlame. V budoucnu lze předpokládat postupný nárůst vládních botnetů.

Mezi významné představitele botnetů patří: Storm, Mariposa, BredoLab, Conficker, TDL4, ZeroAccess, Zeus, Rustock, Waledac.

Odkazy:
Storm [6]
Mariposa [7]
BredoLab [8]
Conficker [9]
TDL4 [10]

ZeroAccess [11]
Rustock [12]
Waledac [13]

URL článku: https://security-portal.cz/clanky/seznamte-se-botnety

Odkazy:
[1] https://security-portal.cz/users/rubberduck
[2] https://security-portal.cz/category/tagy/unsorted
[3] http://www.security-portal.cz/sites/default/files/botnet1.jpg
[4] http://www.security-portal.cz/clanky/seznamte-se-exploitpack
[5] http://www.security-portal.cz/sites/default/files/waled.jpg
[6] http://en.wikipedia.org/wiki/Storm_botnet
[7] http://en.wikipedia.org/wiki/Mariposa_botnet
[8] http://en.wikipedia.org/wiki/BredoLab_botnet
[9] http://en.wikipedia.org/wiki/Conficker
[10] http://en.wikipedia.org/wiki/TDL-4
[11] http://www.symantec.com/security_response/writeup.jsp?docid=2011-071314-0410-99
[12] http://en.wikipedia.org/wiki/Rustock_botnet
[13] http://en.wikipedia.org/wiki/Waledac_botnet