SECURITY 2011

19. ročník konference o bezpečnosti v ICT

DoS útoky včera, dnes a zítra

Tomáš Vobruba, Michal Drozd

AEC, spol. s r.o.

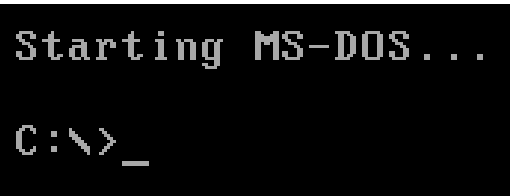
Přehled

DENIAL OF SERVICE

- DoS
  - Typy útoků
  - Aplikační útoky z pohledu OWASP
- Příklady táhnou – electronic warfare
  - WikiLeaks
  - Cpost.cz
  - Twitter
- DDoS
  - Vylepšený DoS
  - Fabulace moderního typu útoků
  - Motivace

DoS – co říká Wiki?

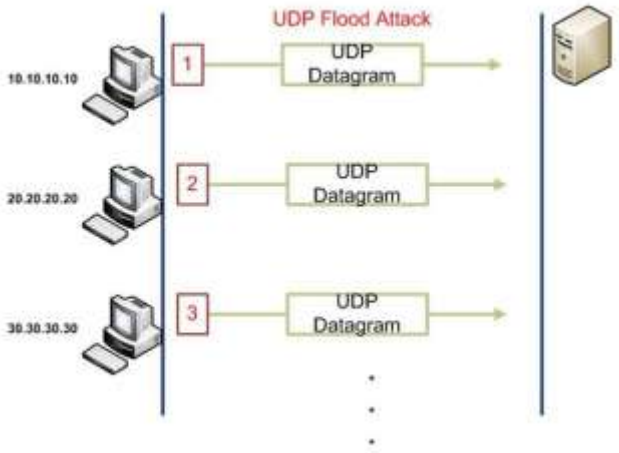
- **Denial of Service** nebo též **Distributed Denial of Service** je technika útoku na internetové služby nebo stránky, při níž dochází k přehlcení požadavky a pádu nebo minimálně nefunkčnosti a nedostupnosti pro ostatní uživatele.
- Cíle takového útoku jsou v zásadě dva:
  - Vnucení opakovaného resetu cílového počítače
  - Narušení komunikace mezi serverem a obětí tak, aby jejich komunikace byla buď zcela nemožná, nebo alespoň velmi pomalá.

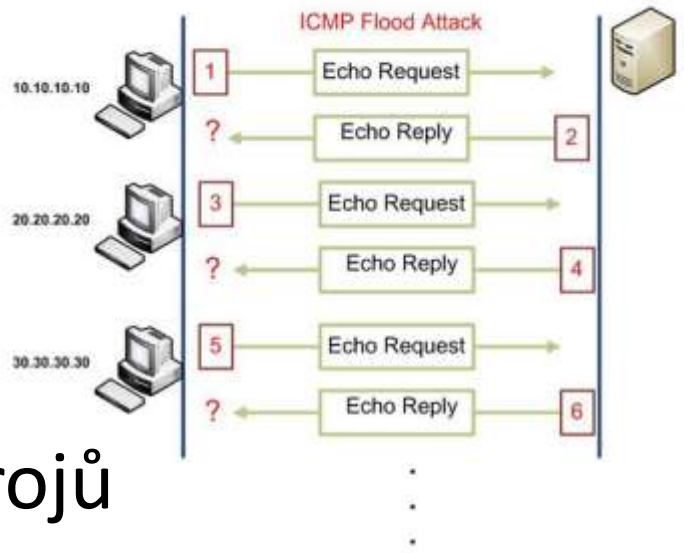


Zdroj - http://cs.wikipedia.org/wiki/Denial_of_Service

Typy útoků

- Síťové
  - SYN Flood
  - UDP Flood
  - ICMP Flood
  - Land Attack
  - Teardrop Attack

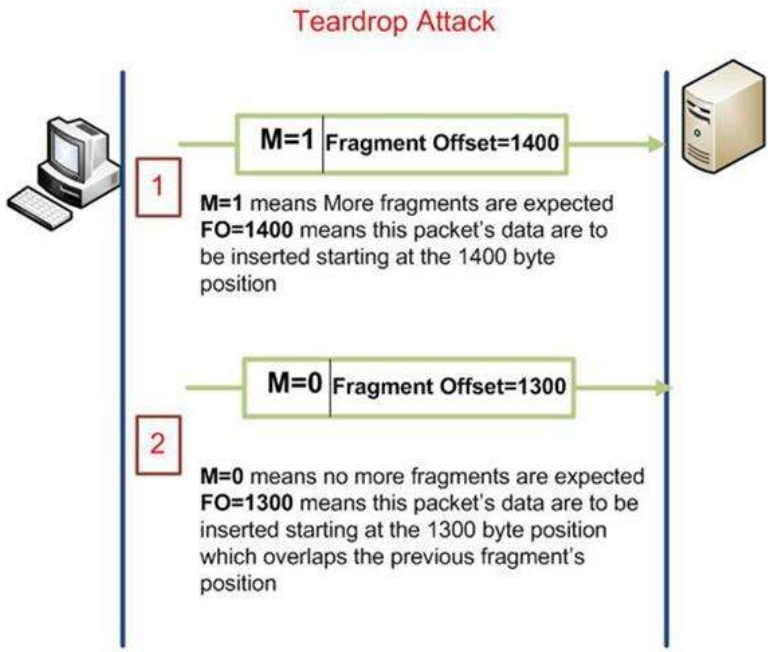




- Aplikační
- Cílem je obvykle vyčerpání zdrojů

Ping of death a Teardrop

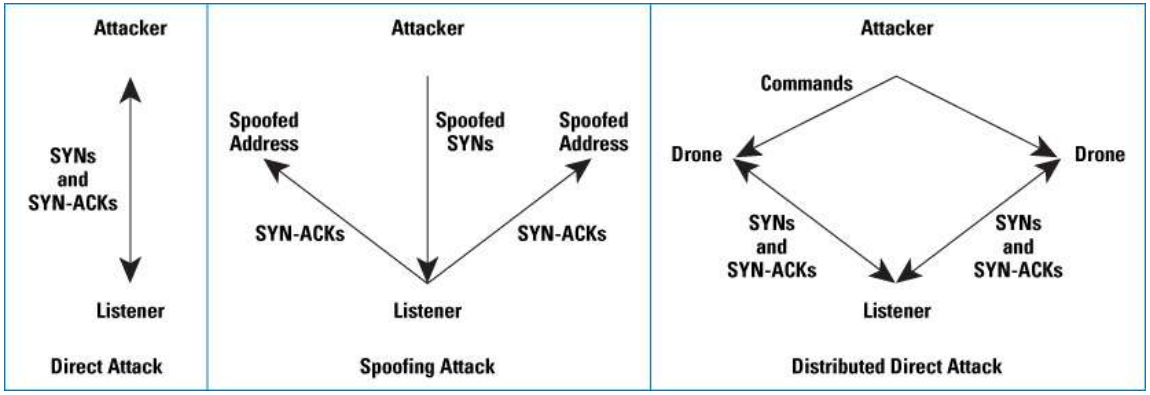
- Teardrop a ping of death jsou cíleny na programovou chybu v operačních systémech.
- Ping of death využíval chyby, kdy systémy neuměly zpracovat pakety větší než 65 536 bajtů. V případě, že systém přijal paket o větší velikosti, došlo ke zhroucení systému

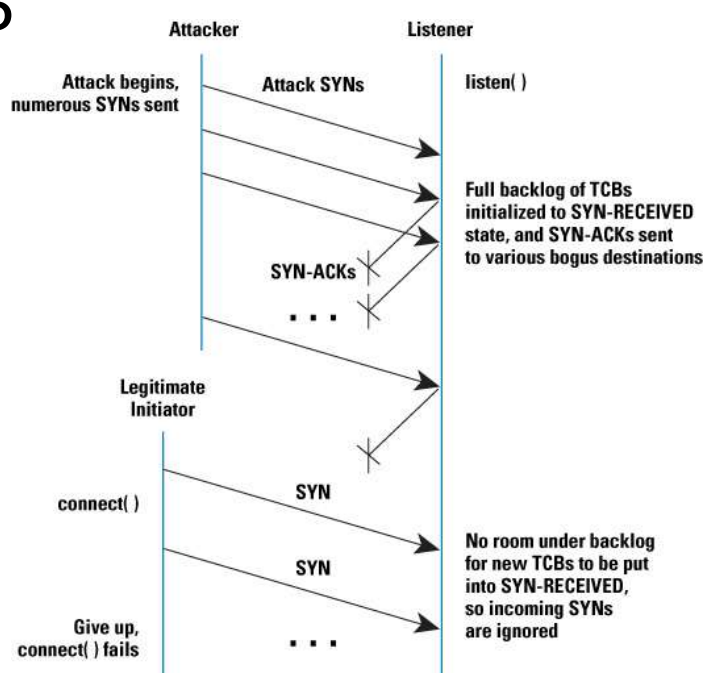


./teardrop 10.10.10.10 192.168.1.2 –p 80 –n 10000

Síťové útoky

- **SYN Flood** *./hping -a 10.10.10.10 -p 80 -S 192.168.133.143 -i u1*
  - je příkladem DoS útoku na zdroje serveru. Při tomto útoku je posláno velké množství paketů s příznakem SYN a podvrženou zdrojovou IP adresou.



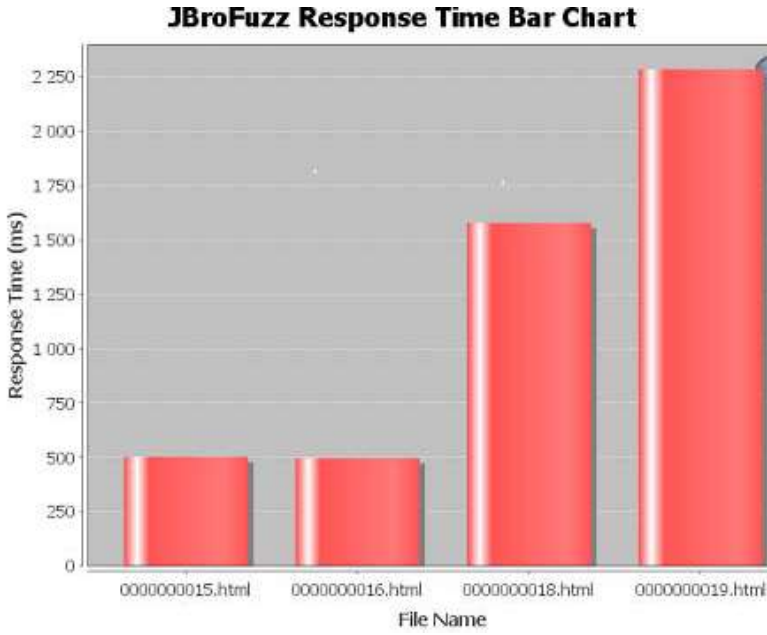


Aplikační útoky

- V podstatě, cílem DoS útoku v prostředí webových aplikací, mohou být:
  - **systémové zdroje** – chybou ve webové aplikaci může dojít k vyčerpání systémových zdrojů (diskové místo, RAM, strojový čas, …)
  - **samotná aplikace** – chyby v implementaci nebo návrhu mohou zanést chyby, které mohou způsobit např. buffer overflow (jazyky, kde má sám programátor na starosti správu paměti)
  - **uživatel** – útok na uživatele zapříčiní, že oprávněný uživatel se nemůže přihlásit do systému
  - **databáze** – mnoho databází je citlivých např. na SQL Injection, což umožní modifikovat strukturu databáze a služba na ní postavena je vyřazena z provozu

Aplikační útoky

- Chyby velikosti session a její uvolňování **(OWASP-DS-008)**
- Chyby SQL **(OWASP-DS-001)**



Běžný SQL dotaz vytvořený v MS Visual Studio vypadá takto:

SELECT * FROM [zipcode] WHERE ([city] LIKE '%' + @city + '%')

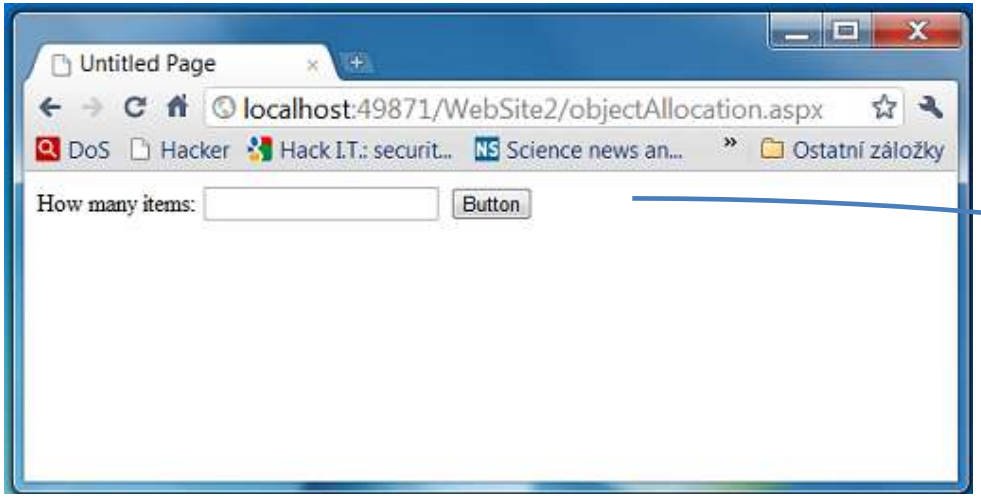
Wildchar SELECT dotazy:

- %_[aaaaacccvbbaaaa[! -z]@$!_%

%_[aaaabbbbbbbbbccaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa[! -z]@$!_%

Aplikační útoky

- Webová aplikace bez kontroly horní meze alokovaných objektů v C# (**OWASP-DS-004)**



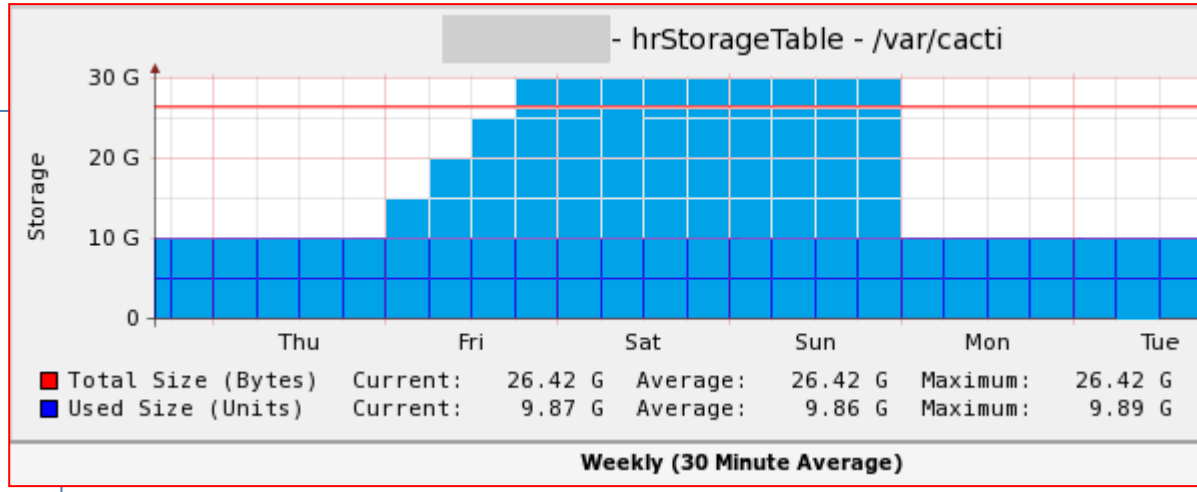

```
protected void btnAllocate_Click(object sender, EventArgs e)
{
if (txtNum.Text != string.Empty)
{
myGreatObj[] obj = new myGreatObj[Convert.ToUInt32(txtNum.Text)];
lblResult.Text = "It was created " + Convert.ToUInt32(txtNum.Text) + "
object(s).";
}}
```

Aplikační útoky

- Zapisování dat na pevný disk

(OWASP-DS-006)

```
try
{
// Bad data format
}
catch (Exception ex)
{
logToFile(ex.Message + ";" + txtInput.Value,
logFile);
}
```




```
Servlet failed with Exception
org.apache.wicket.protocol.http.PageExpiredException: Invalid URL
    at org.apache.wicket.protocol.http.request.CryptedUrlWebRequestCodingStrategy.onError(CryptedUrlWebRequestCodingStrategy.java:308)
    at org.apache.wicket.protocol.http.request.CryptedUrlWebRequestCodingStrategy.onError(CryptedUrlWebRequestCodingStrategy.java:321)
    at org.apache.wicket.protocol.http.request.CryptedUrlWebRequestCodingStrategy.decodeURL(CryptedUrlWebRequestCodingStrategy.java:293)
    at org.apache.wicket.protocol.http.request.CryptedUrlWebRequestCodingStrategy.decode(CryptedUrlWebRequestCodingStrategy.java:118)
weblogic.servlet.internal.WebAppServletContext$ServletInvocationAction.run(WebAppServletContext.java:3496)
    at weblogic.security.acl.internal.AuthenticatedSubject.doAs(AuthenticatedSubject.java:321)
    at weblogic.security.service.SecurityManager.runAs(Unknown Source)
    at weblogic.servlet.internal.WebAppServletContext.securedExecute(WebAppServletContext.java:2180)
    at weblogic.servlet.internal.WebAppServletContext.execute(WebAppServletContext.java:2086)
    at weblogic.servlet.internal.ServletRequestImpl.run(ServletRequestImpl.java:1406)
    at weblogic.work.ExecuteThread.execute(ExecuteThread.java:201)
    at weblogic.work.ExecuteThread.run(ExecuteThread.java:173)
org.apache.wicket.WicketRuntimeException: Unable to decrypt the text ' . ^SMB ~^_p`M :^O '
```

Aplikační útoky

- Chybné uvolňování prostředků (**OWASP-DS-007**)

```
try
{
myConnection.Open();
reader = myCommand.ExecuteReader();
myDataGrid.DataSource = reader;
myDataGrid.DataBind();
}
catch(Exception ex)
{
// Catches and logs the exception
}
finally
{
reader.Close();
myConnection.
```

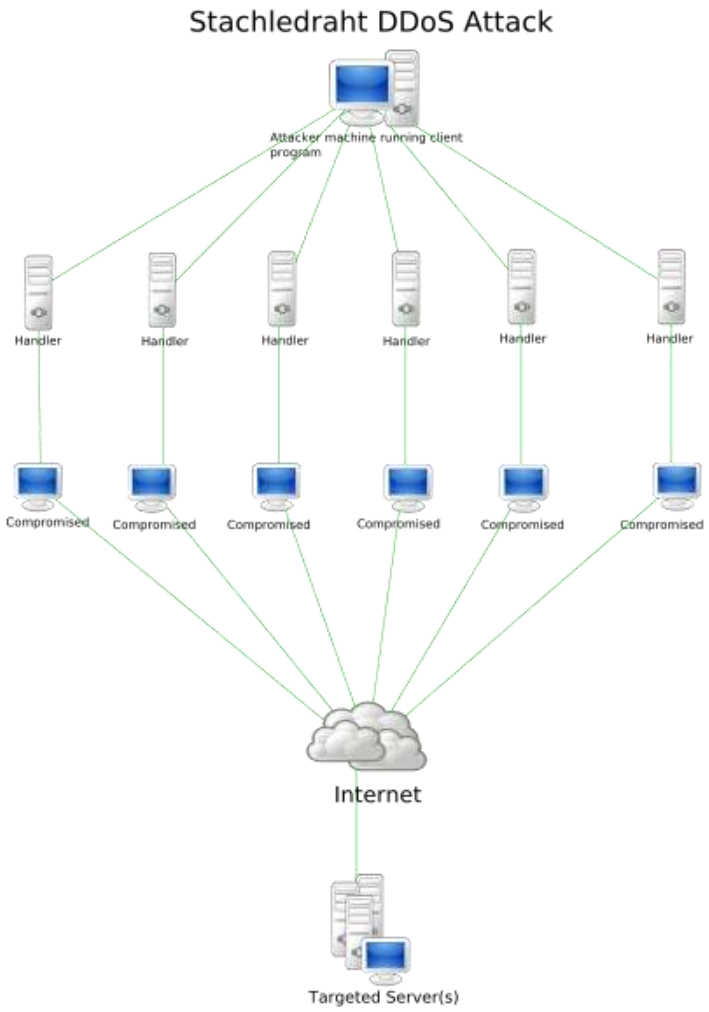
```
class Worker implements Executor {
...
public void execute(Runnable r) {

try {
...
}
catch (InterruptedException ie) {
// postpone response
Thread.currentThread().interrupt();
}
}
public Worker(Channel ch, int nworkers) {
...
}
protected void activate() {
Runnable loop = new Runnable() {
public void run() {
try {
for (;;) {
Runnable r = ...;
r.run();
}
}
catch (InterruptedException ie) {
...
}}
};
new Thread(loop).start();
}}
```

Nejsou nastaveny limity.
Útočník je schopen vyčerpat zdroje velmi rychle.

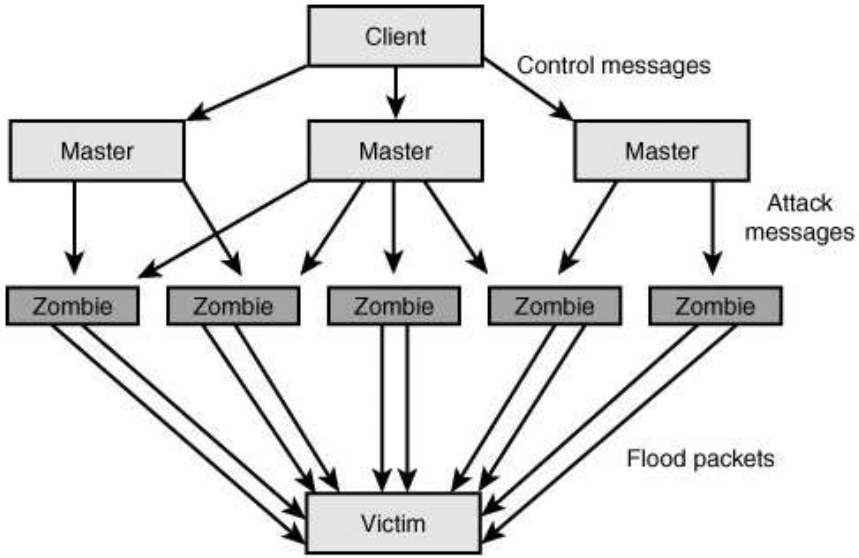
DDoS

Speciálním případem DoS je DDoS. DDoS (Distributed DoS) má stejný cíl jako obyčejný DoS, ale je veden prostřednictvím velkého počtu útočících stanic, které zpravidla bývají součástí botnetu a jsou označovány jako zombie

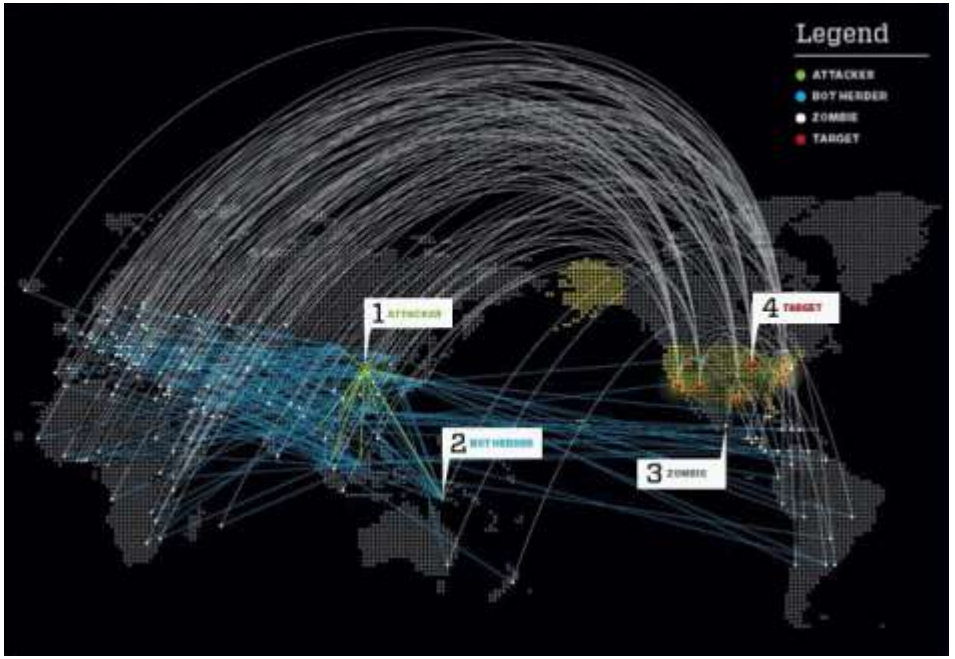
Zdroj - http://cs.wikipedia.org/wiki/Denial_of_Service



BotNety



Struktura DoS útoku pomocí botnetu



V současné době je termín nejvíce spojován s malware, kdy botnet označuje síť počítačů infikovaných speciálním software, který je centrálně řízen z jednoho centra. Botnet pak provádí nežádoucí činnost, jako je rozesílání spamu, DDoS útoky a podobně.
Příkladem poslední doby je červ Conflicker
(http://spectregroup.wordpress.com/2010/04/15/dark-clouds-for-rent/)

Příklady táhnou

Wikileaks down

- Klasický DDoS útok.
- Rychlost útoku byla 500Mbps
- Útok šel proti DNS serverům

Wikileak Xerxes Dos Attack

Want to have a look at the tools which Jester (the one who did a Ddos distributed denial of service) attack ag
Here you go :

Xerxes in Action

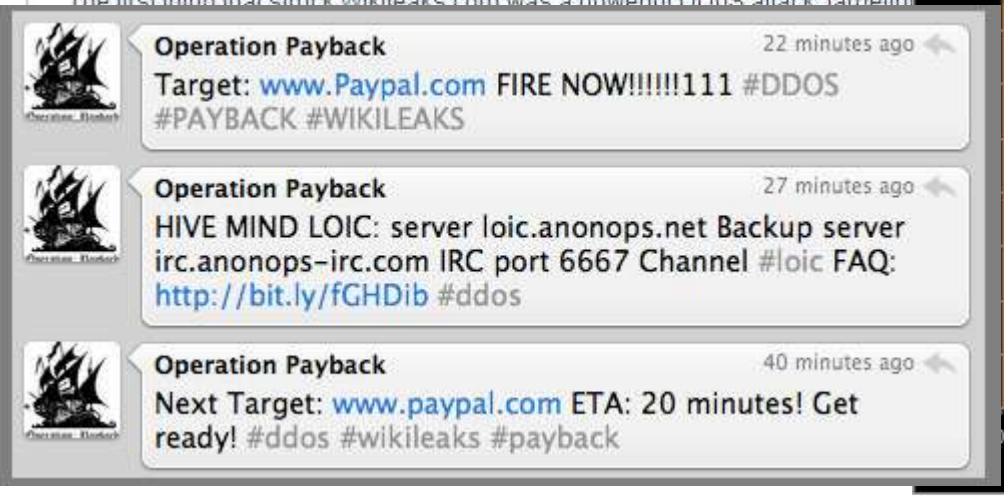
The tool used to Ddos Wikileak

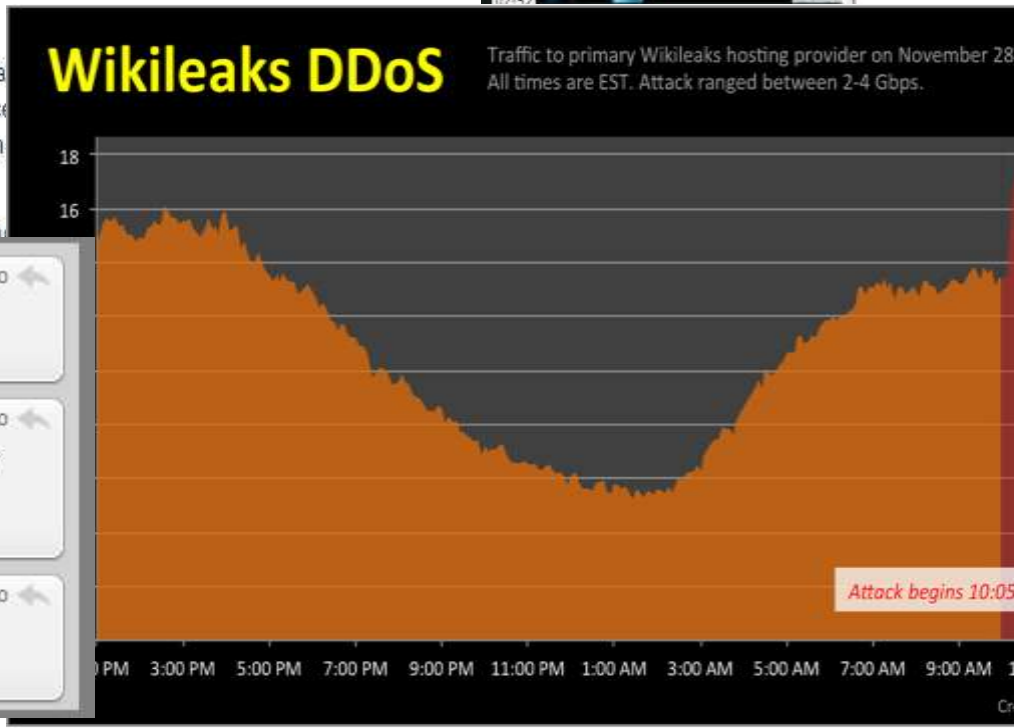
WIKILEAKS.COM HIT BY DDOS ATTACK AND DNS SERVER FIRE

DDoS Attack Quickly Rocketed Traffic to 500Mbps

February 2008 - Wikileaks.com, a Web site that leaked "anonymous, untracea
experiencing hard times. The Web site suffered a Distributed Denial of Servic
restraining order. All of these strikes came after the Web site had leaked som
trust structures in the Cayman Islands.

The first thing that struck Wikileaks.com was a powerful DDoS attack, targetin





Wikileaks - Xerxes

Twitter down

- Poslední vlna útoků je spojována s Wikileaks

Denial-of-Service Attack Knocks Twitter Offline (Updated)

By Eliot Van Buskirk, evolver.fm August 6, 2009 | 10:06 am

Twitter was shut down for hours Thursday morning by what it described as an "ongoing" denial-of-service attack, silencing millions of Tweeters. It was the first major outage the service has suffered in months and possibly the first ever due to sabotage. The outage appeared to begin mid-morning, EST, and affected users around the world. After about three hours, the service was coming back online in fits and starts (updated).

The first official word about the outage came in a terse statement on Twitter's status blog: "Site is down — We are determining the cause and will provide an up

twitter

Login Join Twitt

DDOS attack now exceeding 10 Gigabits a second.

6:06 AM Nov 30th, 2010 via web

Retweeted by 100+ people

wikileaks

WikiLeaks

Twitter Service Status

Visit site » Check other services »

Current Status SHARE

Up

Having trouble with Twitter?

Report an Issue

Status information updated 4 minutes ago Refresh automatically

Status History

Up

Down

24 hours ago 12 hours ago 6 hours ago 3 hours ago Now

Resources API Business Help Jobs Terms Privacy

twitter

WikiLeaks

@wikileaks

BUĎME SILNÍ

SPOLEČNĚ OTEVŘEME STÁT

10. 2. 2011, 15:35

RSS

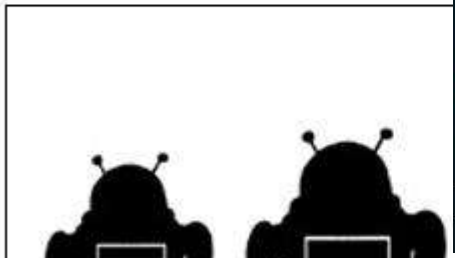
PIRÁTSKÉ NOVINY

M“ — ČESKÝ ROZHLAS

mní předání utajovaných a cenzurovaných
korupce a organizovanému zločinu v České

Pirátská strana pod DDoS útokem - Upřesnění

Aktualizováno | Je to tak, i serv
probíhajících bojů. Ve čtvrtek
opakovaně nedostupné, což vy
fungovaly, na to, co se děje). V
útoku, který nám jako pravděp
technického odboru.



JS LOIC

No need to download, install or setup anything - just click the button, sit and enjoy the show.

Step 1. Select your target:

URL:

https://www.paypal.com:443/

For current target see: http://anonops.net/

Step 2. Ready?

IMMA CHARGING MAH LAZER

Optional. Options

Requests per second: 10

Append message:

Attack status:

Requested: 22

Succeeded: 22

Failed: 0

We need your help in support of wikileaks leave this page firing as long as you can. Don't worry if requests show as failed.

Česká Pošta

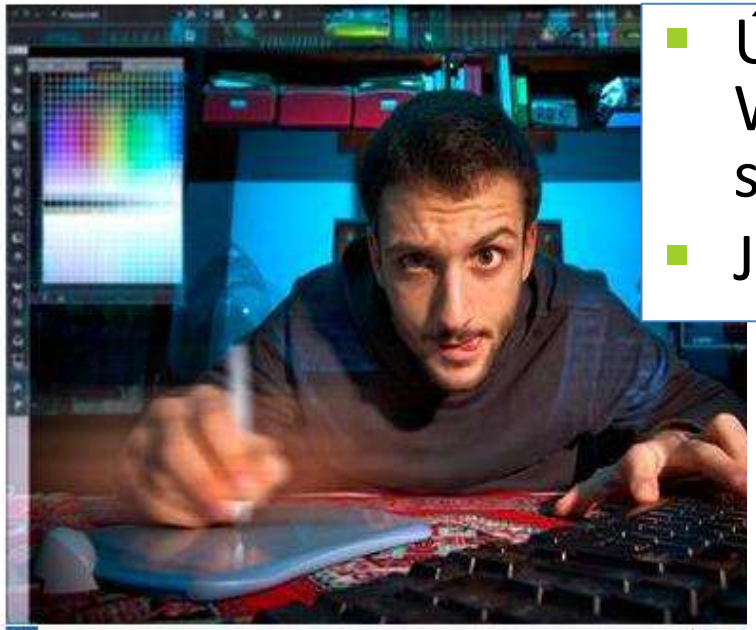


foto: S

Česká pošta čelí útoku hackerů. V oh jsou balíky s vánočními dárky

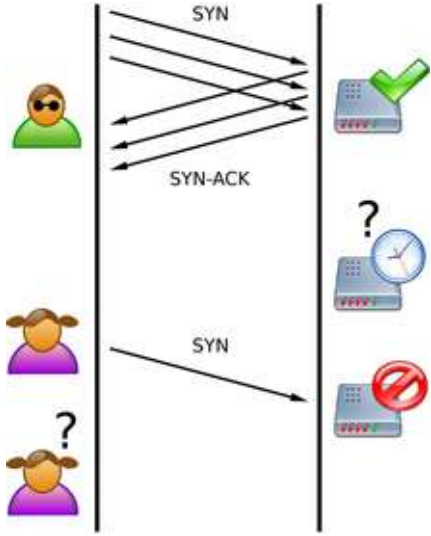
Exkluzivně 9. prosince 2010 19:10, aktualizováno 10.12. 9:08

PRAHA - Rozsáhlý útok hackerů postihl vnitřní systém Če pošty. Internetoví piráti podle informací Lidových novin na část internetových stránek firmy, jejímž prostřednictv podávají on-line hromadné objednávky.

Desítky specialistů pošty i jejích dodavatelských IT firem se v s době horečně snaží útok, trvající od čtvrtečního rána, zastavit. Hromadná podání on-line, na které hackeři útočí, využívají sto například internetových obchodů, které poštou v současné pře nákupní horečce posílají tisíce balíků denně.

- Útok následoval v lavině DoS útoků vůči Wikileaks, PayPal a České piratské straně.
- Jednalo se o jednoduchý SYN Flood útok

Služba je nyní mimo provoz a zatím není jasné, kdy bude obnovena. Kvůli pracem na zastavení hackerského útoku jsou občas mimo provoz celé internetové stránky České pošty. Tiskový mluvčí České pošty Ivo Mravinac problémy pošty potvrdil. "Na webovou adresu aplikace podání on-line **přicházejí tisíce fiktivních požadavků z dynamicky se měnících adres, které v důsledku zapříčiní nedostupnost systému.** Způsobuje to potíže našim firemním zákazníkům, je to velmi nepříjemné i pro poštu, prosinec je standardně obdobím největšího růstu balíkových podání," uvedl Mravinac.



Fiktivní příkazy shazující systém pošty, je jich i šest tisíc za minutu, generují roboti nasazení právě hackery. "Protože zatím všechny okolnosti nasvědčují tomu, že by se jednat o **útok hackerů, pravděpodobně podáme trestní oznámení na neznámé pachatele,"** dodal mluvčí pošty.

Podle informací Lidových novin pracovníci pošty zkoumají i možnost, že by se mohlo je útok zorganizovaný některou konkurenční přepravní firmou. Česká pošta totiž v uplyn měsících navýšila svůj podíl na trhu balíkové přepravy, jejích služeb například v dalek míře, než dřív, využívají internetové obchody. "Proč k tomu dochází nevíme, pokud se potvrdí, že se jedná o hackerský útok, musí jeho původ zjistit policie," dodal Mravinac.

#&@!! .. ??? Motivace ??? .. !! #&@

Son of GhostNet: China-based hacking targets India government

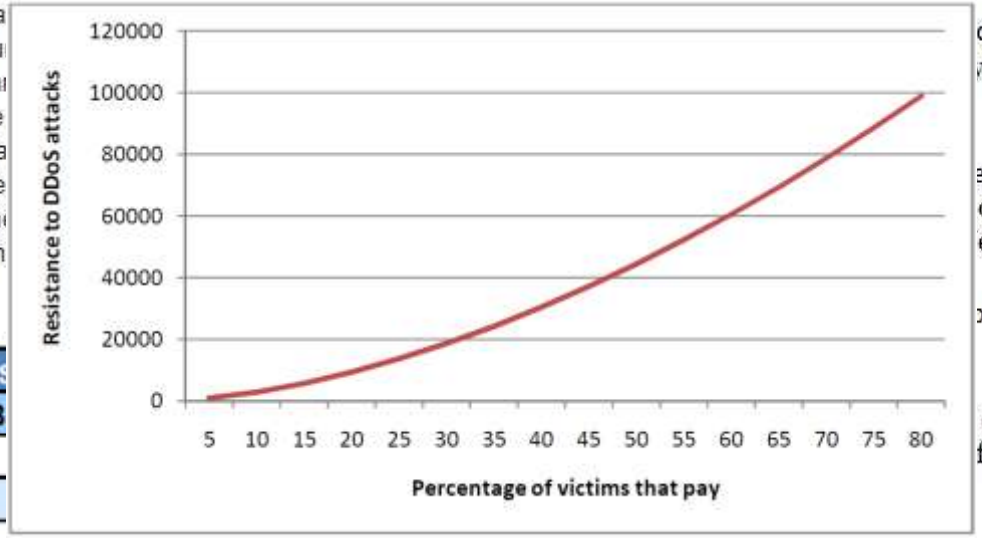
By John Timmer | Last updated 10 months ago

The people who uncovered GhostNet, an extensive cyber espionage network that targeted the Tibetan exile community, are back with a an infected machine that was fou investigation, an international tea uncovered a completely separate targeted the Indian government, a classified documents that had be hackers. By reconstructing the n able to trace things back to the h Chengdu, China.

Cost of hiring DDoS		
Price ($)	Duration (h)	B
20	2	
30	6	
50	12	45
70	24	45
75	24	100
250	24	1000
100	24	1000
600	168	1000
900	24	4750
5500	168	4750
1000	24	4750
6000	168	4750
400	5	5000

U.S. Military's Elite Hacker Crew

John Lasker 04.18.05



dable hacker posse: a super-secret,
to launch bloodless cyberwar against ene

e Armed Services Committee hearing last
or Stratcom, disclosed the existence of a u
etwork Warfare, or JFCCNW.

uld best be described as the world's most

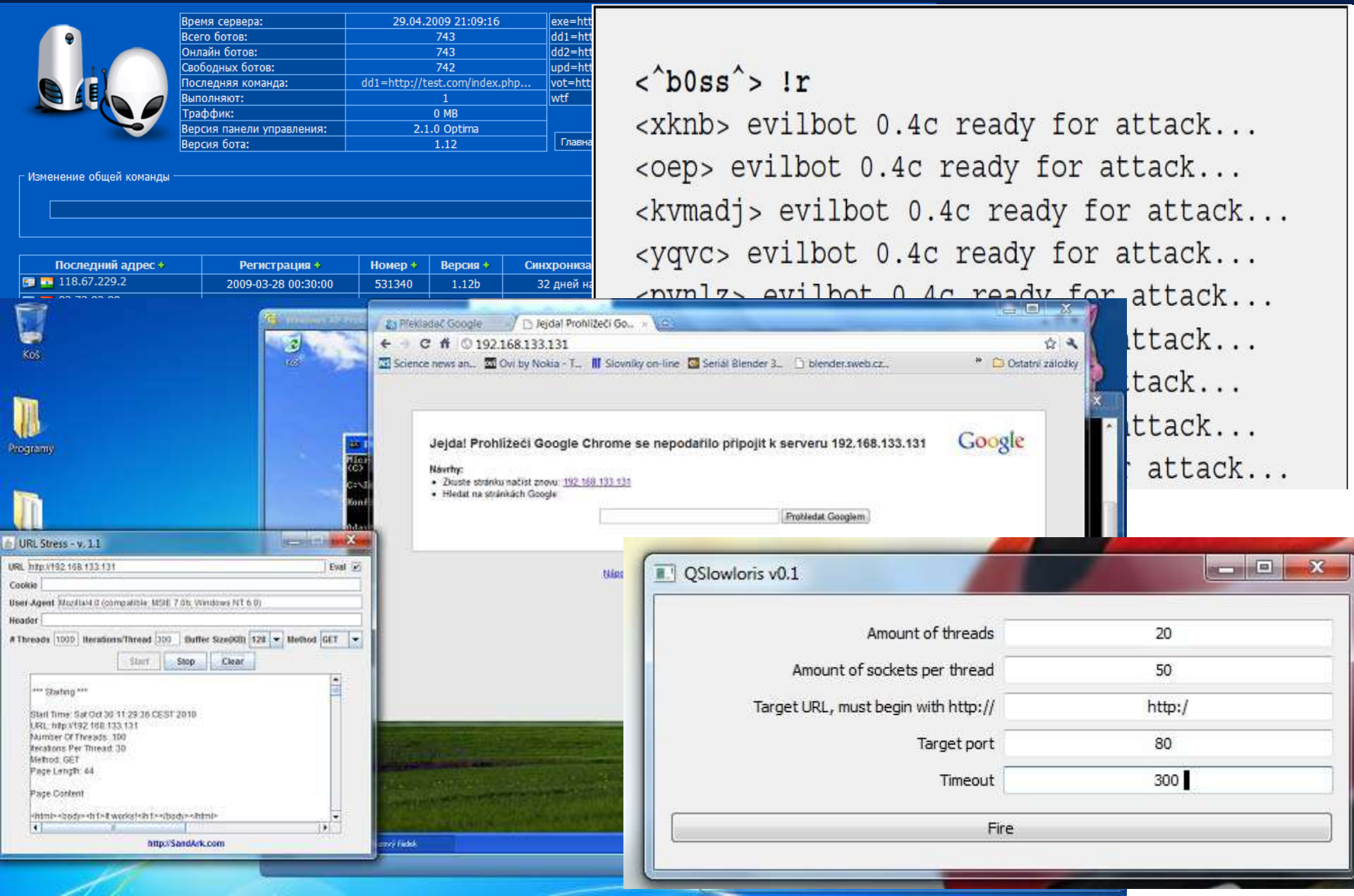
of Defense networks. The unit is also
f Computer Network Attack, or as some

Chinese cyberespionage network runs across 103 nations

By Joel Hruska | Last updated March 30, 2009 10:05 AM

The existence and operation of massive, coordinated, government-affiliated online espionage networks is typically the province of television or the silver screen, rather than the subject of research. In the real world, even a direct link between online and offline action (Russia's invasion of Georgia and the simultaneous online attacks against that country are a good example) is not enough to automatically prove that the government behind the one is automatically behind the other. We've covered the rise of hacktivism previously on Ars; as more citizens come online, we'll undoubtedly see more of this type of crowdsourced aggression in the future.

Nástroje veřejně dostupné

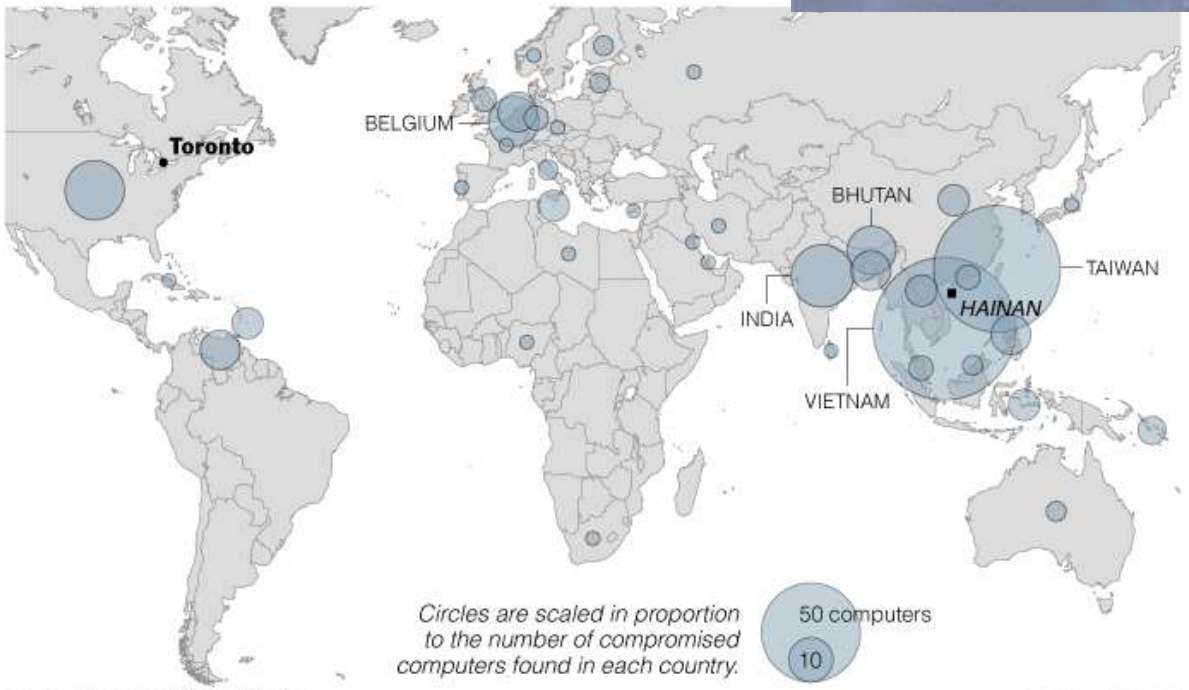


Botnety

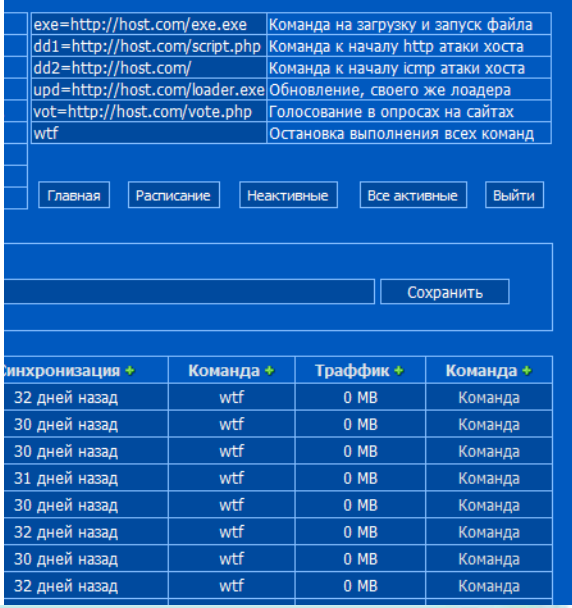
- Nástroje veřejně známé
- Dostupné za peníz

The Vast Reach of 'GhostNet'

Researchers have detected an intelligence gathering operation involving computers. Below, the locations of 347 of the compromised machines, m diplomatic and economic government offices of South and Southeast As



Ruská scéna



Работаем со всеми проектами независимо от тематики!

В онлаин практически круглосуточно!

Основные типы атак: (http/icmp/syn/upd)

Наши цены самые доступные на рынке DDoS(a)
Цена составляет от 80$ в сутки!

Конечная цена зависит от сложности заказа и определяется многими параметрами (предполагаемый срок атаки, ширина канала атакуемого сервера, хитрые Админны и т.д.).

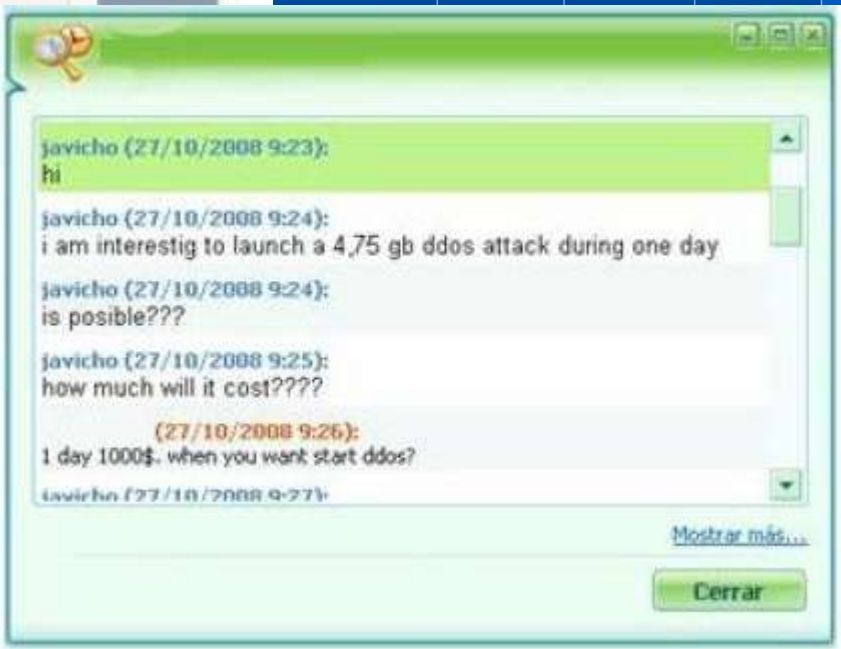
Индивидуальный подход к каждому клиенту

При больших заказах скидки

Постоянным клиентам скидки

Предоставляем тест 10 мин (Только серьезным клиентам)

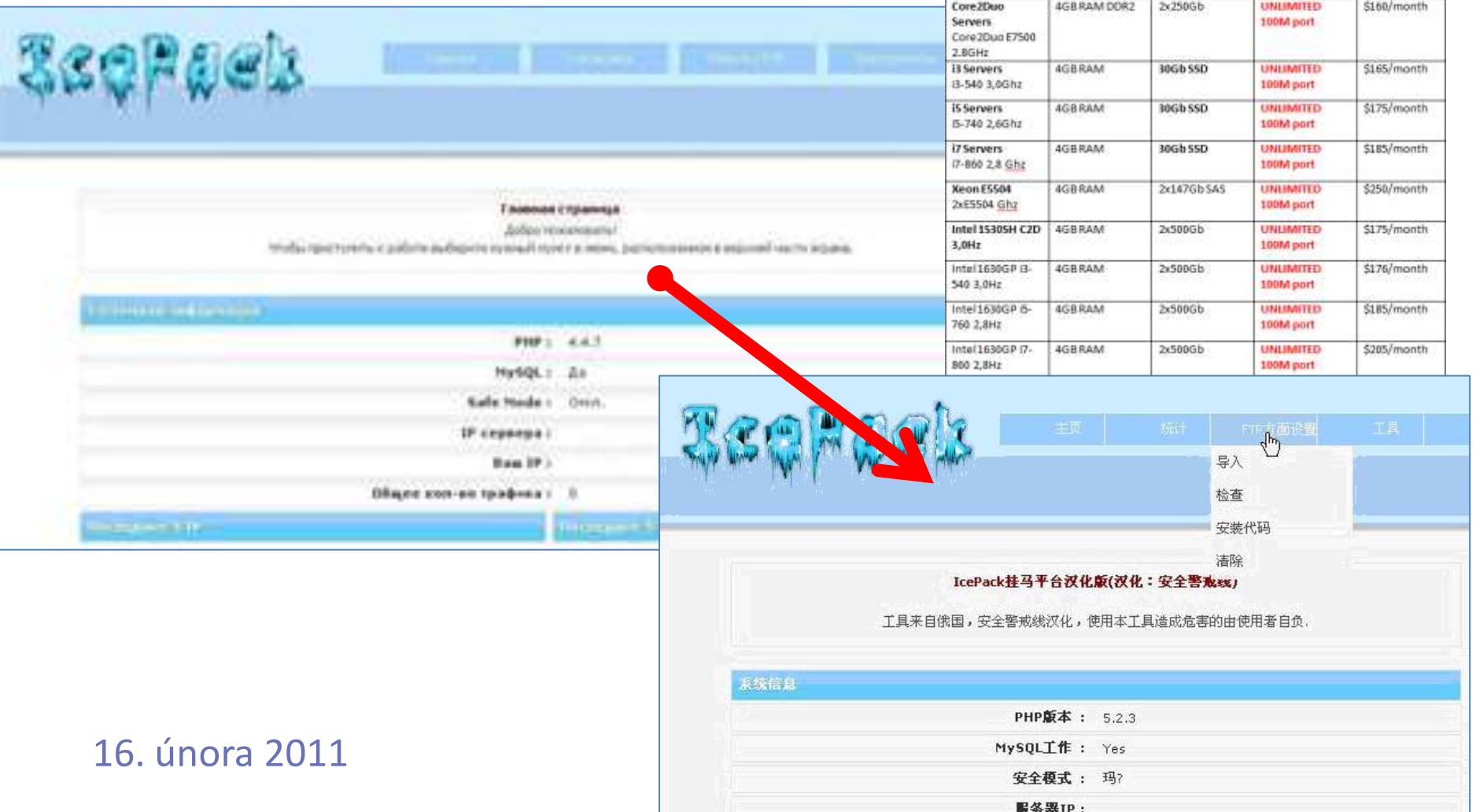
Тольно в нашем сервере Вы получите БОНУС флуд мобильного,стационарного телефона в подарок.Если нужна услуга отдельного флуда любого телефона то можно заказать стоимость договорная пишите сервис на вышом уровне!



Ruská scéna

- Příkladem je stormbotnet
  - game4.exe – Denial of Service tool

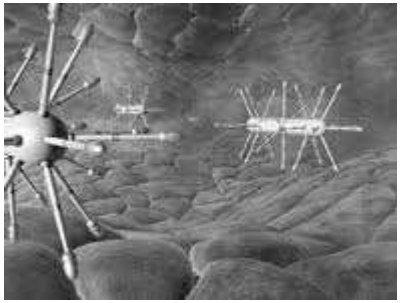
SERVER SPECIFICATION	DEDICATED RAM	HARD DISK	BANDWIDTH	PRICE/ORDER NOW
Atom Server Atom D510	2GB	160Gb	UNLIMITED 100M port	$68/month
P4 Server P4-2,8Ghz	2GB	2x160Gb SATA	UNLIMITED 100M port	$75/month
Core2Duo Servers Core2Duo E7500 2.8GHz	4GB RAM DDR2	2x250Gb	UNLIMITED 100M port	$160/month
i3 Servers i3-540 3,0Ghz	4GB RAM	30Gb SSD	UNLIMITED 100M port	$165/month
i5 Servers i5-740 2,6Ghz	4GB RAM	30Gb SSD	UNLIMITED 100M port	$175/month
i7 Servers i7-860 2,8 Ghz	4GB RAM	30Gb SSD	UNLIMITED 100M port	$185/month
Xeon E5504 2xE5504 Ghz	4GB RAM	2x147Gb SAS	UNLIMITED 100M port	$250/month
Intel 1530SH C2D 3,0Hz	4GB RAM	2x500Gb	UNLIMITED 100M port	$175/month
Intel 1630GP i3-540 3,0Hz	4GB RAM	2x500Gb	UNLIMITED 100M port	$176/month
Intel 1630GP i5-760 2,8Hz	4GB RAM	2x500Gb	UNLIMITED 100M port	$185/month
Intel 1630GP i7-860 2,8Hz	4GB RAM	2x500Gb	UNLIMITED 100M port	$205/month



16. února 2011

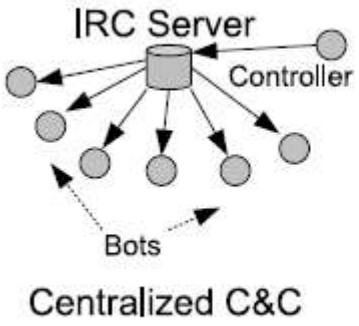
Coby kdyby…

- Metoda KISS (Keep It Simple, Stupid)
- Základem je generovat polymorfistický kód
- Kód šířený formou síťového červa s šířením pomocí metody půlení intervalu. (metoda nanobotů)
  - Každý zdroj infekce si drží databázi napadených cílů a předává ji dál
- Generování škodlivého malware na menší počet strojů – žádná globální infekce
  - Toto je pak velmi těžko zachytitelné AV společnostmi
  - Využití pouze těch strojů, které mají dostatečný výkon a rychlou linku
  - Žádné komerční prostředí - pouze broadbandy
- Kombinování typu útoků
  - Nejzákladnější využití klasického GET /index.html HTTP/1.0

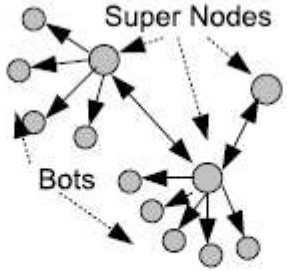


Coby kdyby…

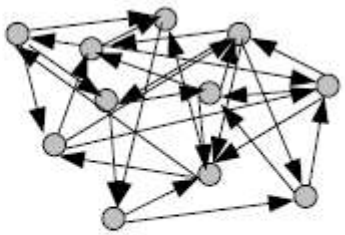
- Pokud se zjistí, že se jeden vypne, předá tuto informaci dalšímu
- Řízeno http reverzní proxy s dynamickým redirektorem.
- Neexistuje master botnetové skupiny – každý může dělat mastera
  - Forma řízení podobná multicast skupinám, pouze na úrovni HTTPS

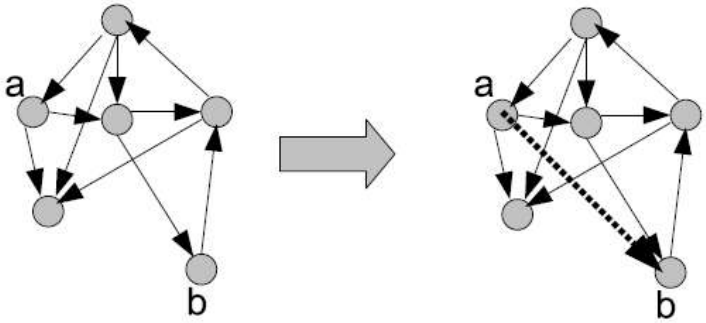


Centralized C&C



Super Node C&C


A Possible RDP C&C

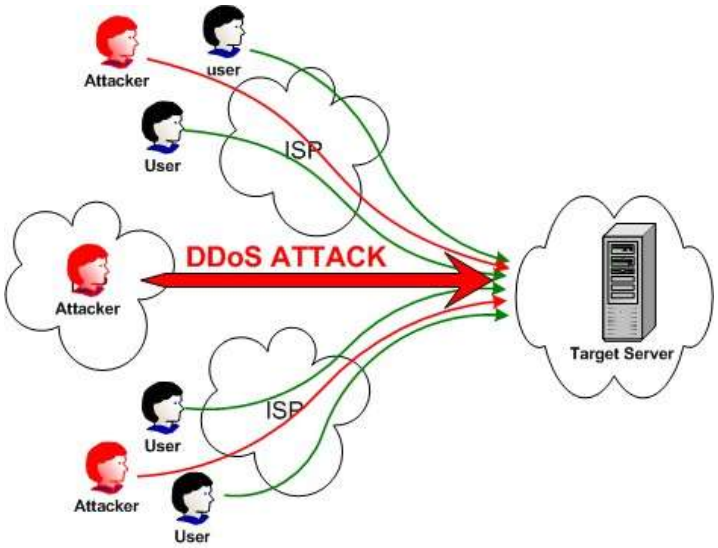


http://www.computersecurityconference.com/2008/CSC2008-Norman.pdf

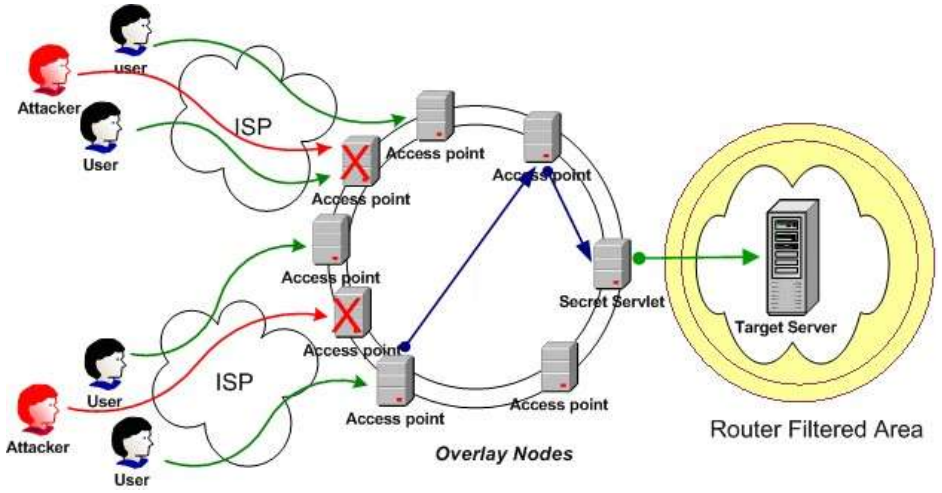
Obrana?

- Velmi těžký úkol
- Základní síťové útoky jsou popsány a většina firewallů se jim umí bránit
- Aplikační útoky dokážou předejít metodologie vývoje jako je:
  - performance testing
  - správný sizing
- Přesto proti botnetům a DDoS není možné se bránit. Je možné se v podstatě jenom vyplatit

Obrana?



Existují i hw prostředky a obchodní nabídky globálních poskytovatelů



SECURITY 2011

19. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Tomáš Vobruba

AEC, spol. s r.o.

tomas.vobruba@cleverlance.com