

# Impact of Botnets on the Health of Internet

**S.C. Leung**

CISSP CISA CBCP

[scleung@hkcert.org](mailto:scleung@hkcert.org)



# Agenda

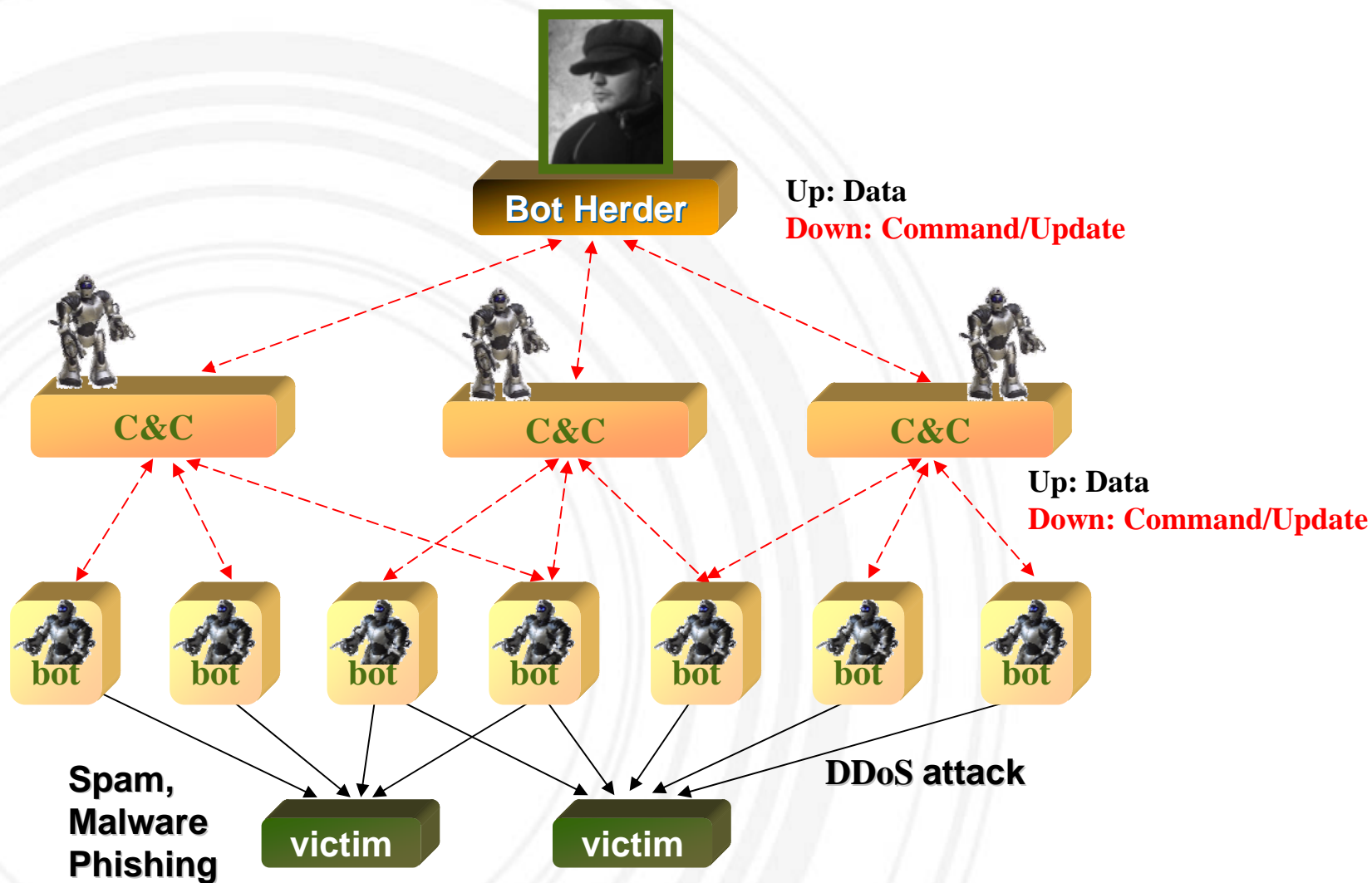
- What are Botnets? Why do Botnets exist?
- Impacts of Botnets
- Takedowns of Botnets
- Defense against Botnets

The background features a series of concentric, semi-transparent circles in shades of light gray and white, centered on the left side. A solid green horizontal bar spans the width of the slide, positioned below the text. The overall design is clean and modern.

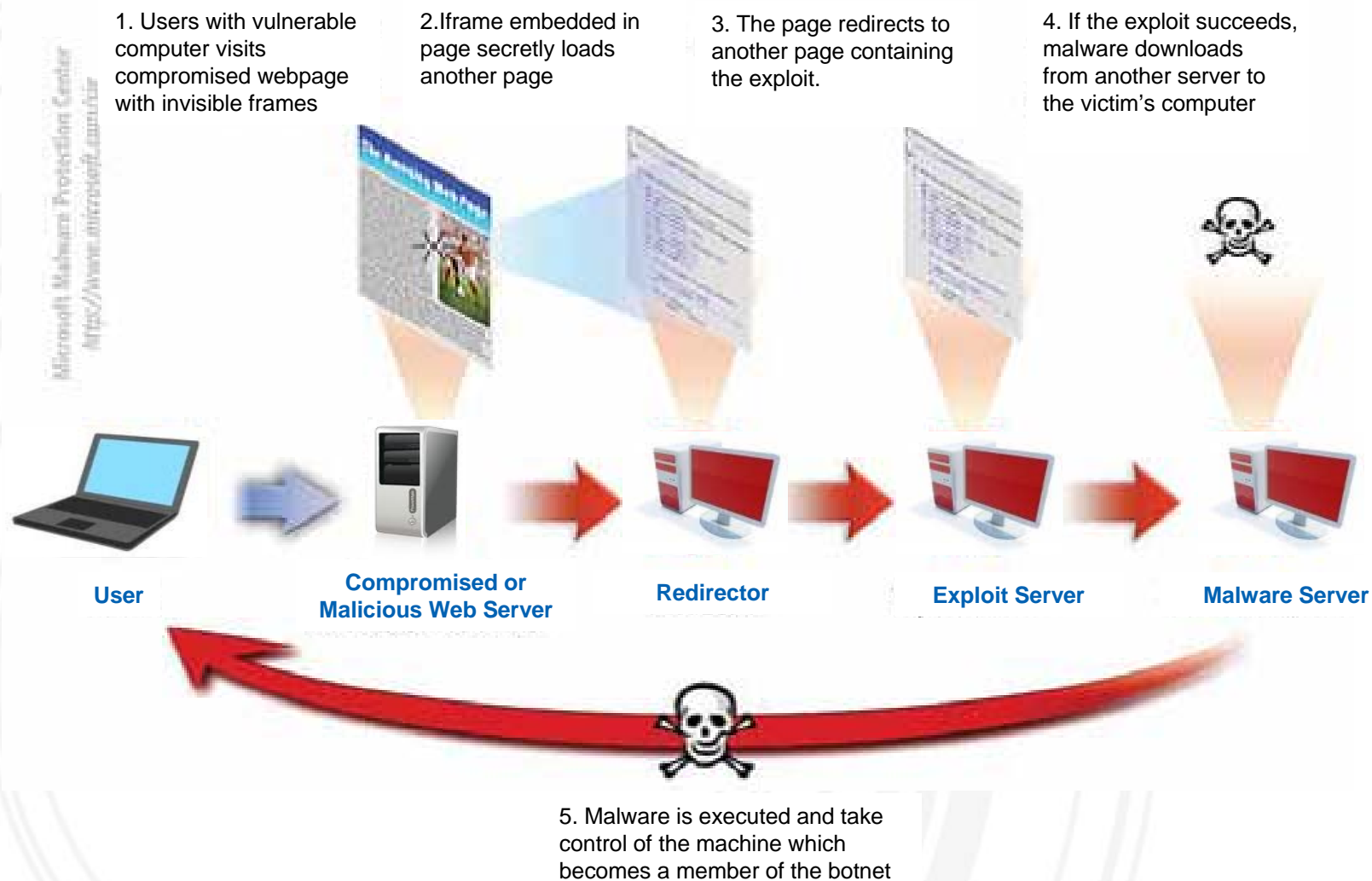
# **What are Botnets? Why do Botnets exist?**

# Botnet (roBot Network)

= infrastructure of controlled victim computers (bots)



# The Making of a Bot



# Botnet is “Crime as a Service”

- Botnet = Launchpad of cyber crimes provided by bot herders for services like
  - Hosting: phishing, spam
  - Application service: identity theft, click fraud, DDoS
  
- Reference:
  - Microsoft Security Intelligence Report 2010 on botnet
    - <http://www.microsoft.com/security/sir/default.aspx>



76services.com (closed in 2009)

The background features a series of concentric, semi-transparent circles in shades of light gray and white, centered on the left side. A solid green horizontal bar spans the width of the image, positioned below the text. The overall aesthetic is clean and modern.

# **Impact of Botnets**



中韓印俄百電腦攻陷港交所  
幕後黑手未明 引5措施昨成功防禦

【明報專訊】本報獲悉，前日令港交所「披露易」網站癱瘓導致7隻股  
 停牌、連累股民帳面損失逾2000萬元的海外黑客攻擊，相信源自中國大陸、韓國、印度及俄羅斯等多國數以百計的「傀儡電腦」，但警方仍未  
 認誰是幕後主腦。而黑客昨日再度攻擊披露易網站，但因港交所按警方  
 議及時加裝「過濾裝置」，成功阻截攻擊。為防再遭黑客癱瘓網站引發  
 牌，港交所引入5項新措施。

Hackers Penetrate Nasdaq Computers

Article    Stock Quotes    Comments

Email    Print    Save    Tweet    A    A

By DEVLIN BARRETT

Hackers have repeatedly penetrated the computer  
 Stock Market during the past year, and federal inve  
 perpetrators and their purpose, according to people

The exchange's trading platform—the part of the sy

NEWS

London Stock Exchange May  
 Have Been Hacked Last Year

By Doug Aamoth on February 1, 2011





# DDoS

- Political motivated
  - Estonia 2007-May
  - Georgia 2008-July (814Mbps)
  - Korea 2009-Oct
  - Burma 2010-Nov (10-15 Gbps)
  - Amazon 2010-Dec
  - Malaysia 2011-Jun
- Financial motivated
  - Korean gambling site extortion 2011
  - German gambling site extortion 2011

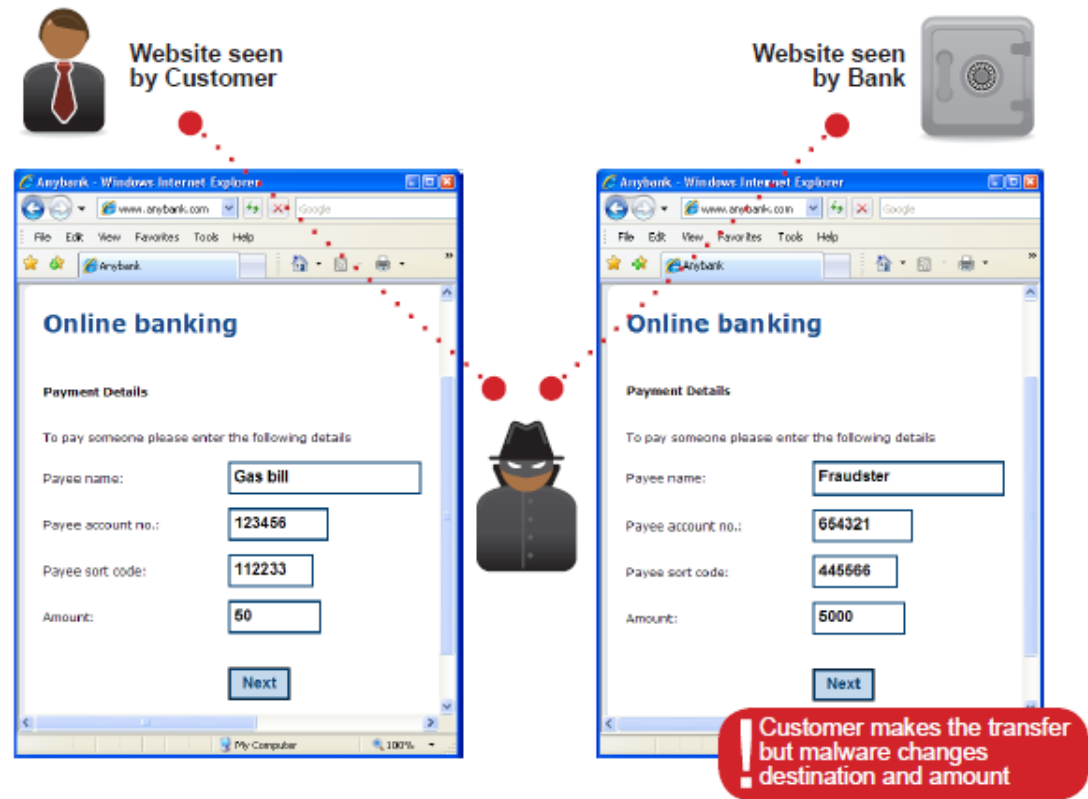
# Botnet targeting Banks

## ▪ Zeus Botnet

- steals banking information by Keylogging and Form Grabbing
- administration UI features:
  - Screenshot (save to html without image)
  - Fake redirect (redirect to a prepared fake bank webpage)
  - **Html inject** (hijack the login session and inject new field)
  - :
  - **Log the visiting information of each banking site**, record the input string (text or post URL)
- Sold at USD400-700 depending on features, with version upgrade

# Man-in-the-Browser

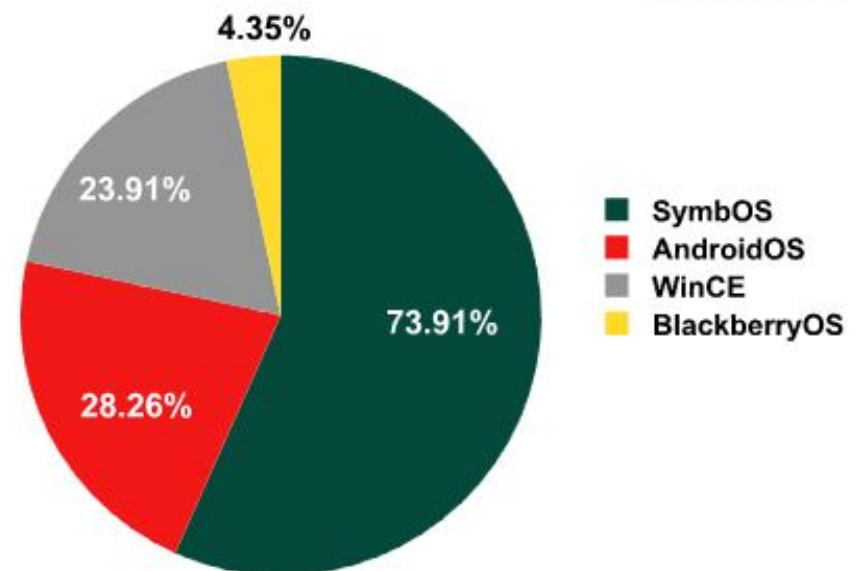
- Hackers' dream: breaking two factor authentication
  - Intercept transaction
    - Install software/plugin inside the browser, hook major OS and web browser APIs and proxying data
  
- Change amount and change destination to attacker account and send to the bank
  
- Change the display to user as if his transaction was executed
  - Calculate the “should be amount” and rewrites the remaining total to screen



Source: [www.cronto.com](http://www.cronto.com)

# Zeus in the Mobile

- ZitMo (reported in Sep-2010)
  - Zeus ver 2.0, Man in the mobile (Mitmo)
  - Installed in mobile devices – Symbian, Android, WinCE and BlackBerry
  - Sniff all the SMS messages that are being delivered.
    - Designed to steal one-time password (OTP) sent via short-text (SMS) message
    - What if you use mobile banking with OTP via SMS?!



Occurrences of ZitMo across mobile platforms. Source: KSN data  
2011-July

# Botnet is all about Money

TODAY @ PCWORLD

## Hackers Use Frequent Flyer Miles as Currency

By John P. Mello Jr., PCWorld

8-Aug-2011



Unsatisfied with stealing bank account information from their victims, cybercriminals steal frequent flyer miles, too. The miles are used as currency among some of the miscreants, according to a report released today by the malware fighters at the [Kaspersky Lab](#).

"In one IRC [Internet Relay Chat] message, a cybercriminal was selling access to a Brazilian botnet that sends spam in exchange for 60,000 miles, while, in another message, air miles were offered for stolen credit cards," Kaspersky analyst Vyacheslav Zakorzhevsky wrote in the company's monthly malware statistics report.

"This coincides with our predictions for 2011 in which we stated that cybercriminals would be interested in all kinds of information and ready to steal absolutely everything," he added.

[http://www.pcworld.com/article/237480/hackers\\_use\\_frequent\\_flyer\\_miles\\_as\\_currency.html](http://www.pcworld.com/article/237480/hackers_use_frequent_flyer_miles_as_currency.html)

## Bitcoin Hack Story

30-June-2011



Bitcoin - first attempts to create a real-world currency with no governments, no central banks, and no rules

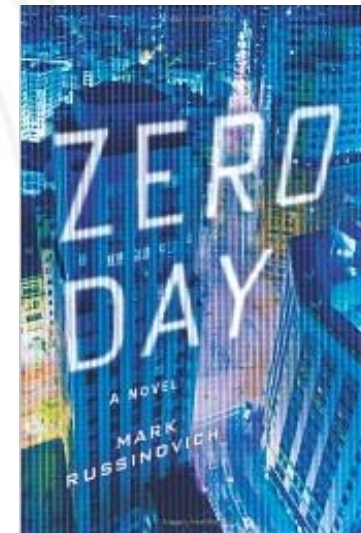
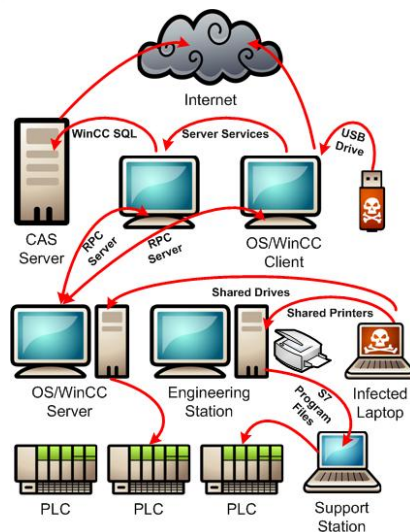
<http://www.security-faqs.com/the-bitcoin-hack-story.html>

# Botnet: Hacking Made Easy

- Hacktivist groups: Anonymous and Lulzsec groups used botnet to attack
  - Anonymous attacked businesses that refused to service Wikileaks
    - DDoS attacks against Amazon, PayPal, MasterCard, Visa and the Swiss bank PostFinance, in retaliation for perceived anti-WikiLeaks behavior.
    - DDoS Malaysian, US, Turkey governments
  - Lulzsec
    - DDoS and US government websites
    - Hack into Sony, Nintendo, Mastercard, Paypal
    - Was believed to hack into 18 Italian university and disclose database on Internet on revenge of another hacker (based in Italy)'s disclosure of Lulzsec members

# Botnet – more than Money → Critical Infrastructure

- Stuxnet - attacks to Critical Infrastructure
  - Found to be designed to search for Siemens program logic controllers of accelerators
  - First rootkit in SCADA. Botnet successful getting into SCADA network of Iranian nuclear plant!
- State sponsored cyber attacks surface?



Mark Russinovich, creator of the SysInternal Suite, wrote a novel describing terrorists attempting to bring down a nation's critical infrastructure with a worm

# Are you exposing your vulnerability?

## ISC Diary

Refresh Latest Diaries

### Controlling a Cisco IOS device from an IRC channel

Published: 2011-08-06,  
Last Updated: 2011-08-07 00:06:14 UTC  
by Manuel Humberto Santander Pelaez (Version: 1)  
Rate this diary:

3 comment(s)

**You need to look at your vulnerabilities, besides external threats, to secure yourself.**

- <http://isc.sans.edu/diary.html?storyid=11332>

#### **Cisco devices are more intelligent than before.**

- Cisco IOS now has a scripting language
- Cisco devices have storage for the IOS image and the configuration files
- Cisco IOS now supports event manager
- Cisco devices are all network connected

What if the programming language is used to perform something nasty within the device that may compromise the entire network?



# Shodan: expose online devices

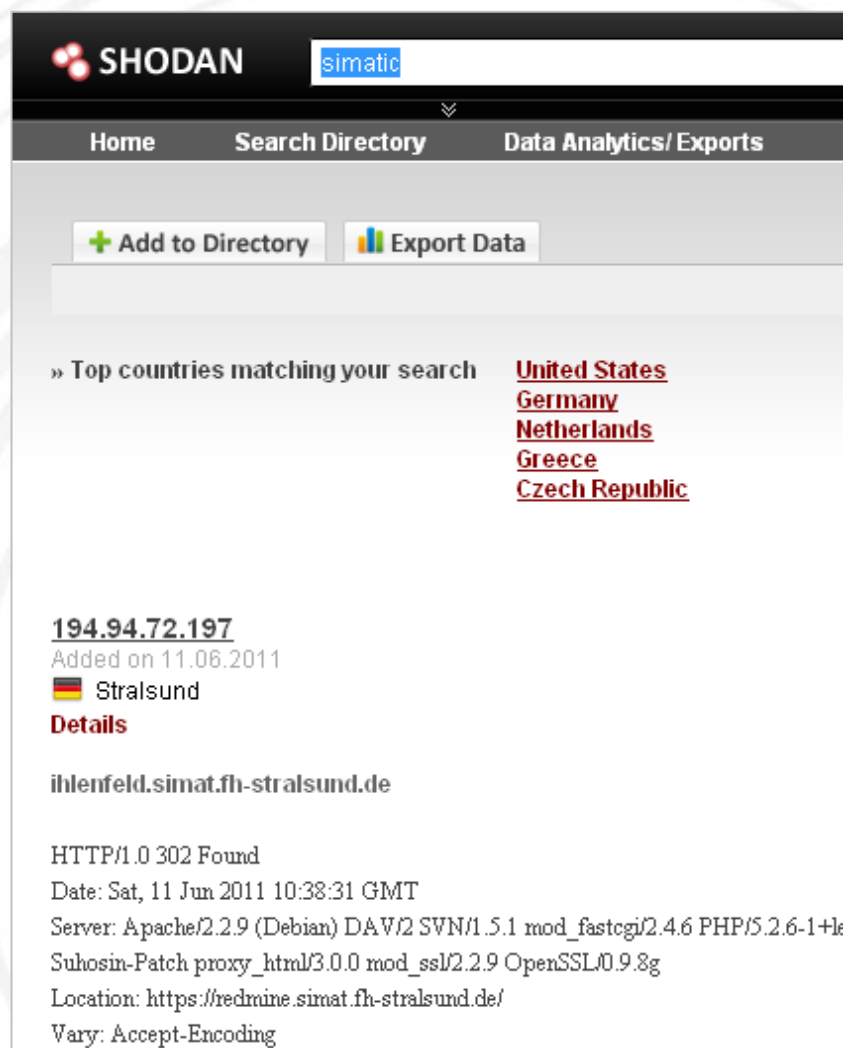
- <http://www.shodanhq.com>



The screenshot displays the Shodan website interface. The main banner reads "EXPOSE ONLINE DEVICES." followed by a list of device types: "WEBCAMS. ROUTERS. POWER PLANTS. IPHONES. WIND TURBINES. REFRIGERATORS. VOIP PHONES." Below this are buttons for "TAKE A TOUR" and "FREE SIGN UP". A "Popular Searches" section is visible, listing various search queries and their results. The search results are as follows:

Date	Search Query	Description
15 MAR 10	Webcam	best ip cam search I have found yet.
14 JAN 10	default password	Finds results with "default password" in the banner; the named defaults might work
13 AUG 10	dreambox	dreambox
14 JAN 10	cisco-ios last-modified	Finds Cisco-IOS results that do not require any authentication ;-)
20 JAN 10	netgear	user: admin pass: password
10 SEP 10	Snom VOIP phones with no authentication	A list of Snom phone management interface without authentication
11 JAN 10	Router w/ Default Info	Routers that give their default username/ password as admin/1234 in their banner.
29 NOV 10	Dreambox	Dreambox

# Shodan: expose online devices



SHODAN

Home Search Directory Data Analytics/ Exports

[+ Add to Directory](#) [Export Data](#)

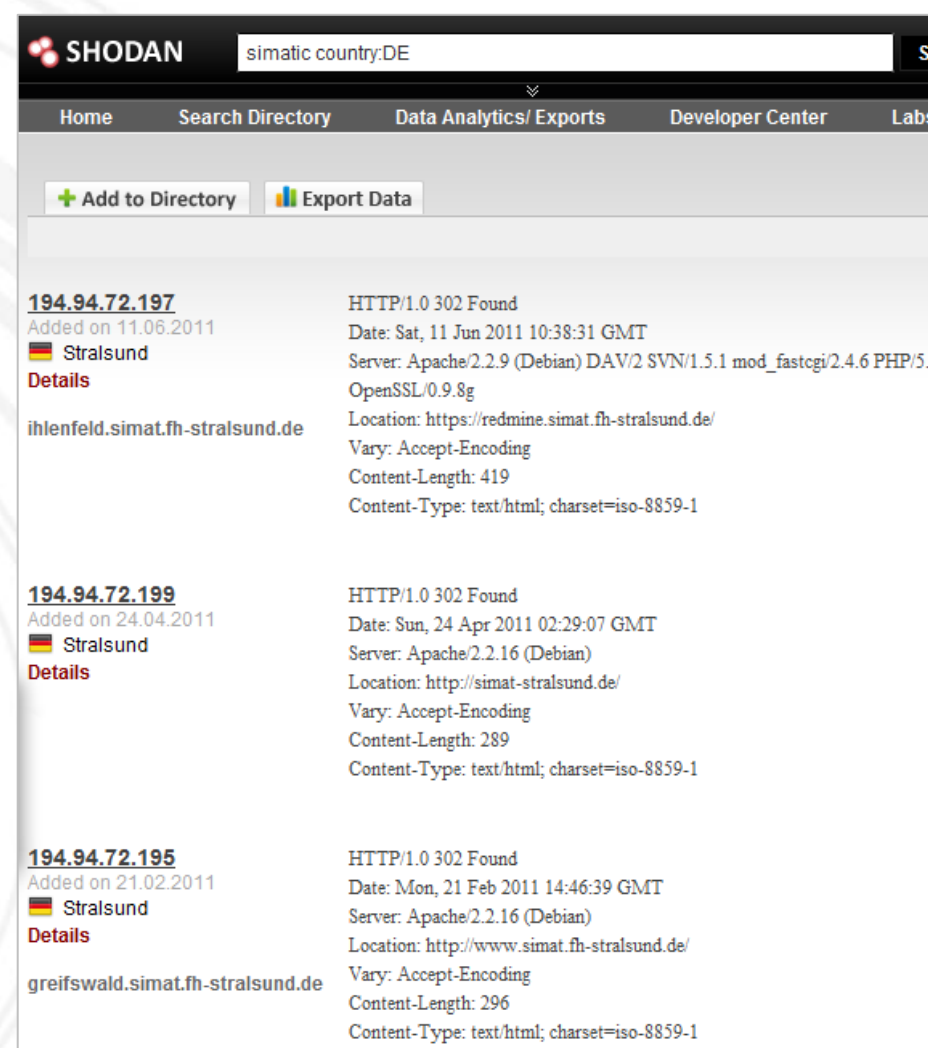
» Top countries matching your search

- [United States](#)
- [Germany](#)
- [Netherlands](#)
- [Greece](#)
- [Czech Republic](#)

**194.94.72.197**  
Added on 11.06.2011  
🇩🇪 Stralsund  
[Details](#)

ihlenfeld.simat.fh-stralsund.de

HTTP/1.0 302 Found  
Date: Sat, 11 Jun 2011 10:38:31 GMT  
Server: Apache/2.2.9 (Debian) DAV/2 SVN/1.5.1 mod\_fastcgi/2.4.6 PHP/5.2.6-1+le  
Suhosin-Patch proxy\_html/3.0.0 mod\_ssl/2.2.9 OpenSSL/0.9.8g  
Location: https://redmine.simat.fh-stralsund.de/  
Vary: Accept-Encoding



SHODAN

Home Search Directory Data Analytics/ Exports Developer Center Labs

[+ Add to Directory](#) [Export Data](#)

**194.94.72.197**  
Added on 11.06.2011  
🇩🇪 Stralsund  
[Details](#)

ihlenfeld.simat.fh-stralsund.de

HTTP/1.0 302 Found  
Date: Sat, 11 Jun 2011 10:38:31 GMT  
Server: Apache/2.2.9 (Debian) DAV/2 SVN/1.5.1 mod\_fastcgi/2.4.6 PHP/5.2.6-1+le  
OpenSSL/0.9.8g  
Location: https://redmine.simat.fh-stralsund.de/  
Vary: Accept-Encoding  
Content-Length: 419  
Content-Type: text/html; charset=iso-8859-1

**194.94.72.199**  
Added on 24.04.2011  
🇩🇪 Stralsund  
[Details](#)

ihlenfeld.simat.fh-stralsund.de

HTTP/1.0 302 Found  
Date: Sun, 24 Apr 2011 02:29:07 GMT  
Server: Apache/2.2.16 (Debian)  
Location: http://simat-stralsund.de/  
Vary: Accept-Encoding  
Content-Length: 289  
Content-Type: text/html; charset=iso-8859-1

**194.94.72.195**  
Added on 21.02.2011  
🇩🇪 Stralsund  
[Details](#)

greifswald.simat.fh-stralsund.de

HTTP/1.0 302 Found  
Date: Mon, 21 Feb 2011 14:46:39 GMT  
Server: Apache/2.2.16 (Debian)  
Location: http://www.simat.fh-stralsund.de/  
Vary: Accept-Encoding  
Content-Length: 296  
Content-Type: text/html; charset=iso-8859-1

The background features a series of concentric, semi-transparent circles in shades of light gray and white, centered on the left side. A solid green horizontal bar spans the width of the image, positioned below the text. The text is centered horizontally within the white space above the bar.

# **Takedown of Botnets**

# Cat & Mice Game

## ▪ Mice side

- Stealthy bots
- Bulletproof Hosting
- Fastflux (changing DNS response)
- Cross jurisdiction

C&C == Achilles' heel  
isolate them → undirected  
bots will sit idle

## ▪ Cat side

- Research bot infrastructure (Vendor, academia)
- Collaborative Takedowns (Police, ISPs, web forums)
- Proactive Discovery (security researchers, HKCERT)

# Waledac

- Impact
  - 1M bots
- open a back door, steal personal information
  - turn bots into web server, web proxy, DNS and spam template relays
  - Billions of spams
- Major web server service
  - Pharmacy
  - serving malware



# Waledac Botnet

- Spreading by
  - **Spam** emails employ social engineering extensively
    - contain link to **iFrame embedded malicious website**, tricking user to install the malware
- Author = Creator of Storm botnet (which overwhelmed the Internet back in 2007)
- Has sound infrastructure

## uses Nginx web server

### HTTP Response Header

Name	Value
HTTP Status Code: HTTP/1.1 200 OK	
Server:	nginx/0.8.5
Date:	Tue, 11 Aug 2009 09:48:18 GMT
Content-Type:	text/html
Connection:	keep-alive
Content-Length:	174
Last-Modified:	Tue, 11 Aug 2009 09:48:02 GMT
Accept-Ranges:	bytes

## uses Double Fast Flux DNS

The **DNS records** are changing all the time

The **DNS servers** are changing all the time

# Waledac

- Operation b49 (2010-Feb)
  - Microsoft, FBI
  - take 277 domain names used by botnet communication offline
  - **Secret court order** to avoid bot herder to set up new domains
  
- Result
  - Botnet taken down
  
- <http://arstechnica.com/microsoft/news/2010/02/judges-restraining-order-takes-botnet-cc-system-offline.ars>

# Rustock

- Impact
  - 1M bots
  - 40B spam emails per day (Symantec: 50% of spams) - selling software, drugs ... counterfeit.
  - Advanced fee fraud - use Microsoft trademark to lure people into lottery scams
  
- Operation b107 (2011-Mar)
  - Microsoft + FireEye + law enforcement + Pfizer (pharmaceutical) + University of Washington
  - Involved CERTs (CNCERT/CC) & ISPs around the world
  - **Microsoft alleged**, “unlawful intrusion, intellectual property violations and dissemination of unsolicited bulk email to the injury of Microsoft and the public.”
  - Court orders to seize computers C&C
  - **Sinhole** to track live bots
  
- Result
  - Spamhaus.org : Spam by Rustock virtually disappeared
    - [http://www.norman.com/security\\_center/security\\_center\\_archive/2011/spam\\_botnet\\_rustock\\_beheaded/](http://www.norman.com/security_center/security_center_archive/2011/spam_botnet_rustock_beheaded/)



# Bredolab

## ■ Impact

- Millions of bots
- spam

## ■ Operation (2010-Oct)

- Dutch authorities and hosting provider WebLease
- Install C&C server,
  - distribute a program to infect bots, redirect it to a website giving information how to disinfect their computers.
  - Reported that 100K PCs visiting that website
- [http://www.pcworld.com/businesscenter/article/208888/dutch\\_law\\_enforcement\\_takes\\_down\\_the\\_bredolab\\_botnet.html#tk.mod\\_rel](http://www.pcworld.com/businesscenter/article/208888/dutch_law_enforcement_takes_down_the_bredolab_botnet.html#tk.mod_rel)

# Coreflood

- Impact
  - 2M machines
  - Send spam, steal credentials and other personal and financial information
  
- Operation (2011-Apr)
  - ISC + FBI + DOJ
  - DOJ and the FBI issued warrants for and seized five "command and control" servers
  - **ISC installed their C&C** → and send KILL command to bots (but bot reinstalled after PC reboot). C&C recorded every bot's IP address and ISPs informed users.
  - **Microsoft updated MSRT** to remove Coreflood malware.
  
- Result
  - <http://arstechnica.com/security/news/2011/04/doj-fbi-set-up-command-and-control-servers-take-down-botnet.ars>

# Botnets fight back

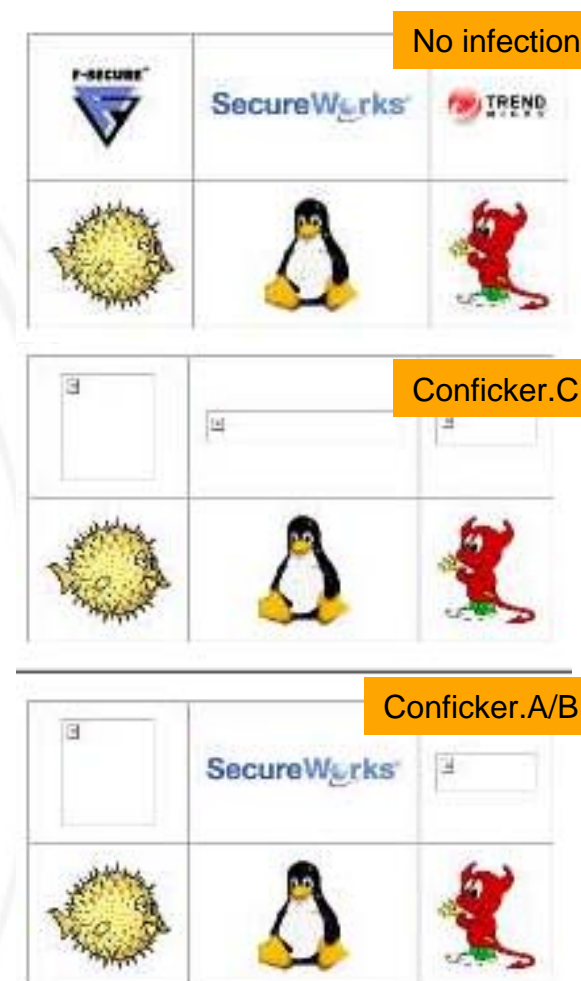


# Conficker – a model for sustainable botnet

- Designed to survive in **disaster** - **What if the C&C are taken down?**
  - Conficker.B - Domain generation for malware update
    - Active since Nov 2008, generating 250 domains/day in 5 TLDs for update
  - **Conficker's natural predator: the Conficker Working Group**
    - ICANN, domain registries and IT industry collaborated to pre-empt Conficker
      - Pre-register domains
      - Redirect traffic to sinkholes to study the behaviours
  - Conficker.C improved
    - Starting Apr 1, 2009, generating 50,000 domains/day in 116 TLDs; uses 500 in random (Some are existing domains) → making it harder to preempt the domains
    - improved authentication and encryption → so you cannot infiltrate into Conficker.C botnet easily
    - uses P2P for update as well – peers can update each other with the right authentication
    - Blocks more security vendors web site

# Collaborative Effort Works!

- Conficker Working Group lead a concerted effort ([www.confickerworkinggroup.org](http://www.confickerworkinggroup.org))
  - ICANN organized all registries to pre-empt the registration, handle affected domains
  - Researches generated the list of generated domain and affected domains to provide transparency
  - Some worked out an EyeChart for easy detection
  - Security vendors developed detection and removal tools
  
- HKIRC, HKCERT, Police and OGCIO
  - Check affected domains in April list for suspicious content
  - Put idle domains in close observation
  - Exchange intelligence on the progress
  - Coordinate with CNCERT/CC on an HK IP address owned by a mainland web hosting provider



# Conficker – a model for sustainable Botnet

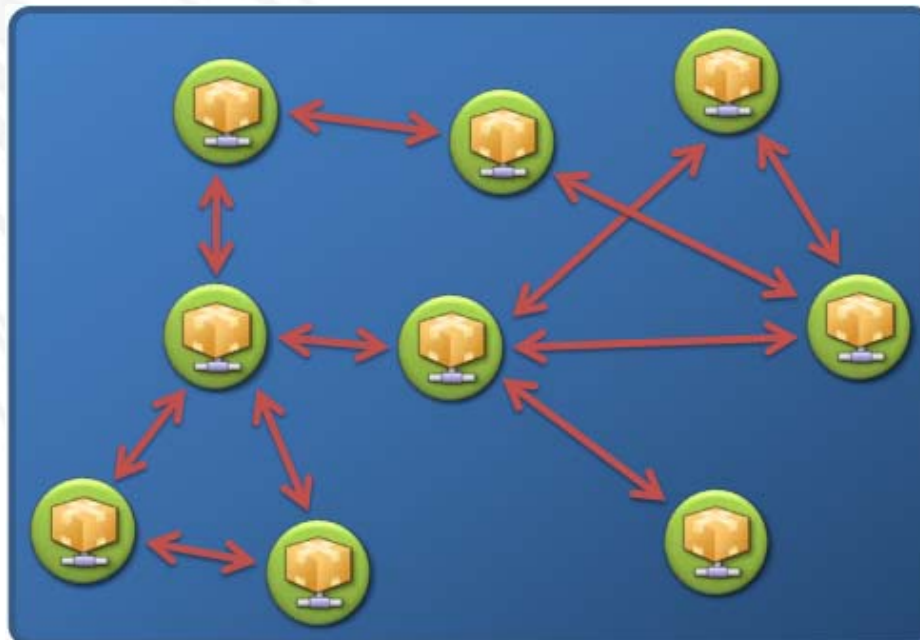
- Everyone watching the domain generation, but nothing happened there
  
- Conficker has dual update mechanisms
  - domain generation
  - P2P
  - Conficker took the liberty to use any one at any time → succeeded to evolve by P2P channel
  
- We still have a long way to close it down.

# Communication Topology

- Centralized, hierarchical



- Distributed, P2P



# TDL-4 / TDSS family (Allureon) – hard to destroy



- Impact
  - 4M bots, including 64bit Windows
  - Spam, DDoS, proxy (have a Firefox proxy plugin)
  - Spread via file sharing and porn sites. Creates DHCP server and gives out malicious DNS servers → sites serving malware
- TDL-4 will remove AV, and other rootkits
- Infect MBR to load on every reboot → subverting driver signing in Win7
- Encrypt filesystem. Hook the File I/O -- whenever the disk sector of rootkit is accessed it returns fake content → hiding the malware
- Encrypt communication
- Use P2P communication without relying on C&C
- Monitor the MBR and rootkit system objects. If not found → reinfect the system



The background features a series of concentric, semi-transparent circles in shades of light gray and white, centered on the left side. A solid green horizontal bar spans the width of the page, positioned below the main title. The overall aesthetic is clean and modern.

# **Success Factors in Botnet Takedowns**

# Success Factors in Botnet Takedown

- Collaboration efforts from
  - Law enforcement and government entities
  - CERT
  - ISPs, OSP, ...
  - Security researchers, Academia
- Creative disruption tactics
  - Sharing of intelligence
  - Speed up takedown
  - Preempt future attacks
  - Use Sinkhole to get information of bots. Find out bot machines left before they join another botnet. They are vulnerable. They may be leaking data
  - Solve legal issues

**WE NEED YOU!**

# Success Factors in Botnet Takedown

## ▪ Be proactive

- new bots and variants come out fast → malware signature model is outdated → PCs infected faster than being detected
- Millions of bot machines are left. They are vulnerable. They may be leaking data.
  - CERTs and ISPs must find them out and clean them, before they join new botnets

**WE NEED YOU!**

- Microsoft promoted a global PC infection response system
  - a system that can scan and quarantine compromised systems to protect the rest of the Internet is one way to avoid the rampant spread of malware.

The background features a series of concentric, semi-circular arcs in shades of light gray and white, centered on the left side. A solid green horizontal bar spans the width of the image, positioned below the text. The overall design is clean and modern.

# **Defense against Botnets**

# Defense against Botnet at client side

- 3 Baseline Defense is necessary but not insufficient
  - Protection from malware
  - Personal Firewall
  - Update patches → this is more and more important



- Secunia Personal Software Inspector  
[http://secunia.com/vulnerability\\_scanning/personal/](http://secunia.com/vulnerability_scanning/personal/)

- Install Microsoft Malicious Software Removal Tool (MSRT)
- Use newer and secure browsers (Chrome 12, FF 5, IE 9)

## Defense against Botnet at server side

- Install minimum modules on server. Do not use it to browse Internet
- Keep patching update
- Protect from web attacks
  - Application Firewall
  - See **SQL Injection Defence Guideline** published by HKCERT
- McAfee promoted offensive defense
  - organizations to use common hacker techniques to test their own software and websites before the bad guys do.



# Q & A

[www.hkcert.org](http://www.hkcert.org)