

Criminals in the Cloud: Past, Present, and Future

Jim Lippard

Sr. Product Manager, IT Security

EarthLink Business



secureworld expo

is your world secure?

Agenda

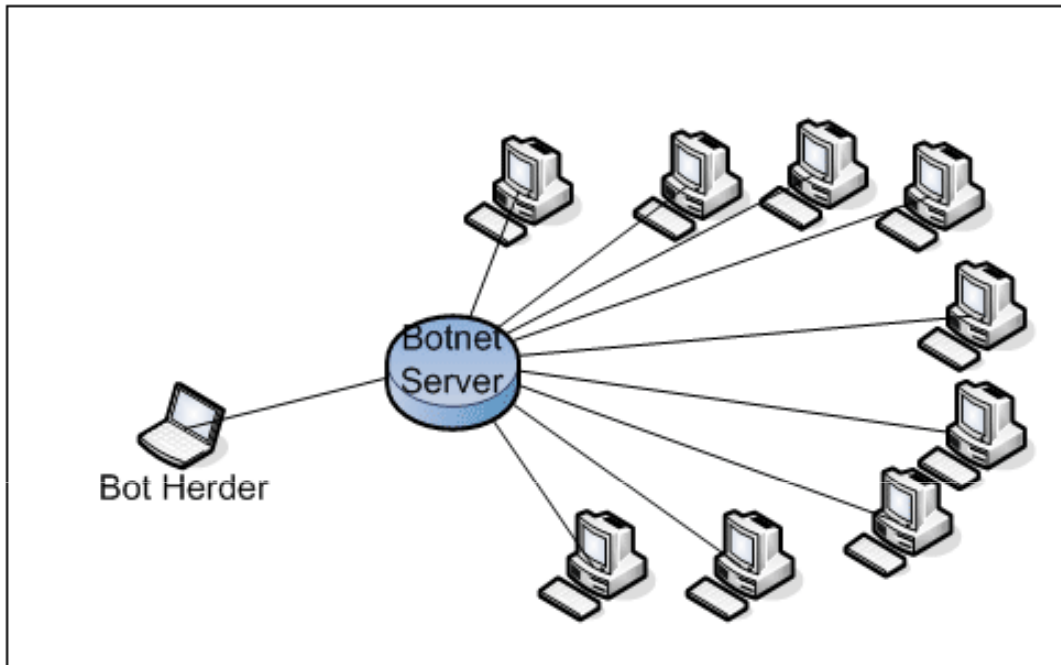
- What is a botnet?
- Bot Lifecycle
- Botnet Ecosphere
- Botnet History & Evolution
- Defense
- Offense
- Future
- Q&A



What is a botnet?

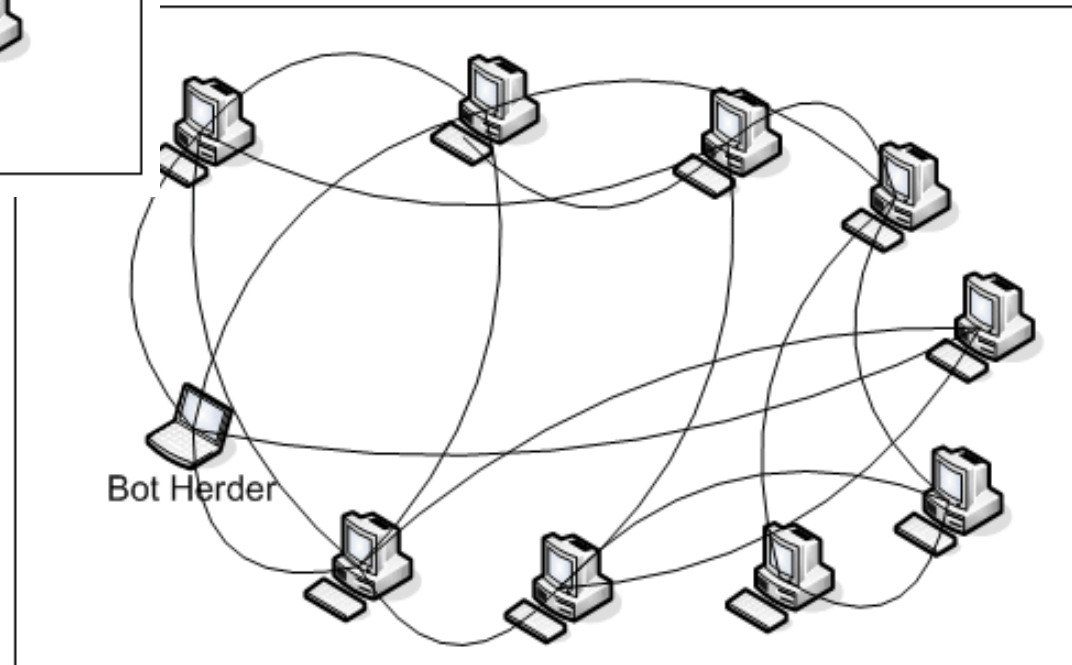


What is a botnet?



Traditional C&C

P2P C&C



What is a botnet?

Two general purposes of using botnets:

- Provide layers of separation/insulation between criminal actors and criminal acts.
- Provide a cloud computing platform for a wide variety of functions.

Neither requires that there be anything of interest on victim computers.



Bot Lifecycle

- Infection
- Control
- Commands
- Detection
- Notification
- Removal
(repeat)



Botnet Ecosphere

Social context: Botnets are created by human agents to achieve some purpose.

Usually:

1. Create botnet.
 2. ???
 3. Profit!
- What's step 2?
 - Do all of these steps need to be done by the same people?
 - Who are these people?



Botnet Ecosphere

Some roles for division of criminal labor:

- Exploit/exploit pack developer
- Botmaster/admin (manages botnet)
- Seller (drives traffic to exploit sites, paid per infection)
- Spammer (sender)
- Sponsor (spam ad buyer)
- Phisher
- Carder (trades in card data/makes counterfeits)
- Cashier (takes out cash)
- Reshippers (stolen good/cash laundering--WFH/GTJ)



Botnet Evolution: Overview

The convergence of DDoS tools, IRC bots, P2P software, worms, and SaaS = modern botnets

- **Early 1990s: IRC channel bots** (e.g., eggdrop, mIRCscripts, ComBot, etc.).
- **Late 1990s: Denial of service tools** (e.g., Trinoo, Tribal Flood Network, Stacheldraht, Shaft, etc.). Peer-to-peer file sharing tools.
- **2000: Merger of DDoStools, worms, and rootkits** (e.g., Stacheldraht+torakit+Ramen worm; Lion worm+TFN2K).
- **2002: IRC-controlled bots implementing DDoS attacks.**
- **2003: IRC-controlled bots spread with worms and viruses, fully implementing DDoS, spyware, malware distribution activity. First P2P bots (Sinit, WASTE).**
- (Dave Dittrich, "Invasion Force," *Information Security*, March 2005, p. 30)
- **2003-present: Botnets used as a criminal tool for extortion, fraud, identity theft, computer crime, spam, and phishing.**



Botnet Evolution: History

- **Dec. 1993:** Eggdrop bot - Non-malicious, occasionally abused (Supported linking multiple bots by 1999)
- **April 1998:** GTbot variants - Based on mIRC, malicious bots
- **1999:** Sub7 trojan - Pretty Park worm, IRC listeners
- **May 1999:** Napster - Non-malicious file sharing, hybrid P2P & client-server
- **March 2000:** Gnutella - Non-malicious file sharing, decentralized P2P
- **April 2002:** SDbot variants - Malicious bot with IRC client. Code made widely available.



Botnet Evolution: History

Aug 2002-Sep 2003: Sobig variants - Botnet used by Ruslan Ibragimov's send-safe spam operation



Botnet Evolution: History

- **Oct 2002:** Agobot variants - (500+ by 2008), malicious bot w/modular design
- **Apr 2003:** SpyBot variants - Derived from Agobot
- **May 2003:** Nullsoft WASTE - Encrypted P2P network. Removed from distribution by AOL
- **Sep 2003:** Sinit - P2P trojan, found peers via crafted DNS packets to random IPs, exchanged peer lists when found
- **Nov 2003:** Kademlia - P2P distributed hash table



Botnet Evolution: History

Feb 14, 2004: FBI takedown of Foonet and “DDoS Mafia.”

DDoS tool of choice: Agobot

Creator: Axel “Ago” Gembe of Germany, was indicted in 2008.

WANTED
BY THE FBI

COMPUTER INTRUSION
SAAD ECHOUAFNI



Alias: Jay R. Echouafni

DESCRIPTION

Date of Birth Used:	June 23, 1967	Hair:	Black
Place of Birth:	Morocco	Eyes:	Green
Height:	5'10"	Sex:	Male
Weight:	200 pounds	Race:	White (North African)
NCIC:	W966352802	Nationality:	Moroccan
Occupation:	Unknown		
Scars and Marks:	Echouafni has a mole on his right cheek.		
Remarks:	Echouafni speaks English and French and may have fled to Morocco.		

CAUTION

Saad Echouafni, head of a satellite communications company, is wanted in Los Angeles, California for allegedly hiring computer hackers to launch attacks against his company's competitors. On August 25, 2004, Echouafni was indicted by a federal grand jury in Los Angeles in connection with the first successful investigation of a large-scale distributed denial of service attack (DDoS) used for a commercial purpose in the United States. In a DDoS, a multitude of compromised systems attack a single target causing a sustained denial of service for its customers. The investigation, codenamed Operation Cyberflam, was initiated in 2003 when a large-digital video recorder vendor based in Los Angeles reported a series of crippling denial of service attacks that effectively halted its business for nearly two weeks. That business, as well as others both private and government in the United States, were temporarily disrupted by these attacks which resulted in losses ranging from \$200,000 to over \$1 million.

SHOULD BE CONSIDERED ARMED AND DANGEROUS

IF YOU HAVE ANY INFORMATION CONCERNING THIS PERSON, PLEASE CONTACT YOUR LOCAL FBI OFFICE OR THE NEAREST AMERICAN EMBASSY OR CONSULATE.

Robert S. Mueller III
ROBERT S. MUELLER, III
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION
UNITED STATES DEPARTMENT OF JUSTICE
WASHINGTON, D.C. 20535
TELEPHONE: (202) 324-3000

I Los Angeles Field Office | July Fugitives | Fugitives I



Botnet Evolution: History

Mar 2004: Phatbot - P2P bot using WASTE

bot.command runs a command with system()
bot.unsecure enable shares / enable dcom
bot.secure delete shares / disable dcom
bot.flushdns flushes the bots dns cache
bot.quit quits the bot
bot.longuptime If uptime > 7 days then bot will respond
bot.sysinfo displays the system info
bot.status gives status
ot.rndnick makes the bot generate a new random nick
bot.removeallbut removes the bot if id does not match
bot.remove removes the bot
bot.open opens a file (whatever)
bot.nick changes the nickname of the bot
bot.id displays the id of the current code
bot.execute makes the bot execute a .exe
bot.dns resolves ip/hostname by dns
bot.die terminates the bot
bot.about displays the info the author wants you to see
shell.disable Disable shell handler
shell.enable Enable shell handler
shell.handler FallBack handler for shell
commands.list Lists all available commands
plugin.unload unloads a plugin (not supported yet)
plugin.load loads a plugin
cvar.saveconfig saves config to a file
cvar.loadconfig loads config from a file
cvar.set sets the content of a cvar
cvar.get gets the content of a cvar
cvar.list prints a list of all cvars
inst.svcdel deletes a service from scm
inst.svcadd adds a service to scm
inst.asdel deletes an autostart entry
inst.asadd adds an autostart entry
logic.ifuptime exec command if uptime is bigger than specified
mac.login logs the user in
mac.logout logs the user out
ftp.update executes a file from a ftp url
ftp.execute updates the bot from a ftp url
ftp.download downloads a file from ftp
http.visit visits an url with a specified referrer
http.update executes a file from a http url
http.execute updates the bot from a http url
http.download downloads a file from http

rsl.logoff logs the user off
rsl.shutdown shuts the computer down
rsl.reboot reboots the computer
pctrl.kill kills a process
pctrl.list lists all processes
scan.stop signal stop to child threads
scan.start signal start to child threads
scan.disable disables a scanner module
scan.enable enables a scanner module
scan.clearnetranges clears all netranges registered with the scanner
scan.resetnetranges resets netranges to the localhost
scan.listnetranges lists all netranges registered with the scanner
scan.delnetrange deletes a netrange from the scanner
scan.addnetrange adds a netrange to the scanner
ddos.phatwank starts phatwank flood
ddos.phaticmp starts phaticmp flood
ddos.phatsyn starts phatsyn flood
ddos.stop stops all floods
ddos.httpflood starts a HTTP flood
ddos.synflood starts an SYN flood
ddos.udpflood starts a UDP flood
redirect.stop stops all redirects running
redirect.socks starts a socks4 proxy
redirect.https starts a https proxy
redirect.http starts a http proxy
redirect.gre starts a gre redirect
redirect.tcp starts a tcp port redirect
harvest.aol makes the bot get aol stuff
harvest.cdkeys makes the bot get a list of cdkeys
harvest.emailshttp makes the bot get a list of emails via http
harvest.emails makes the bot get a list of emails
waste.server changes the server the bot connects to
waste.reconnect reconnects to the server
waste.raw sends a raw message to the waste server
waste.quit
waste.privmsg sends a privmsg
waste.part makes the bot part a channel
waste.netinfo prints netinfo
waste.mode lets the bot perform a mode change
waste.join makes the bot join a channel
waste.gethost prints netinfo when host matches
waste.getedu prints netinfo when the bot is .edu
waste.action lets the bot perform an action
waste.disconnect disconnects the bot from waste



Botnet Evolution: History

- **2003:** Rbot - Uses encryption to evade detection
- **2004:** Polybot - Adds polymorphism
- **Mar 2006:** SpamThru - P2P bot
- **Apr 2006:** Nugache - P2P bot, distributed via trojaned downloads on freeware sites. Author arrested Sep 2007.
- **2006-2011:** Rustock - Major spammer. Atrivo takedown Sep 2008, McColo takedown Nov 11, 2008.
- **Jan 2007-late 2008:** Storm/Peacomm trojan - P2P; massive spammer. RBN connection? 20% of spam in 2008.
- **2007:** Srizbi - Used Mpack, Reactor Mailer, bypassed host firewall. Similar to Rustock. Was largest botnet for a time. McColo.



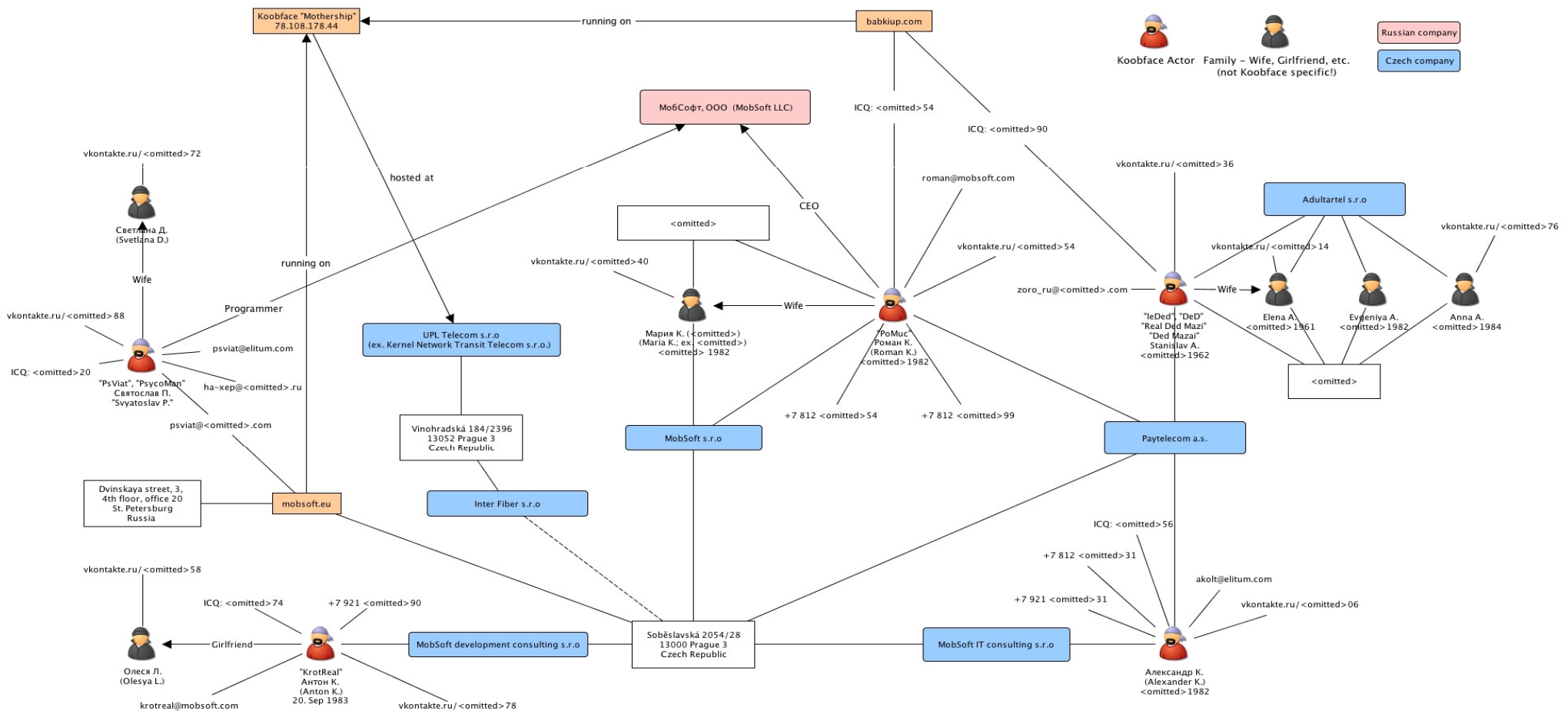
Botnet Evolution: History

- **2007:** Cutwail trojan - Rootkit, DDoS and spam bot. 1.5M-2M bots. C&C taken down when ISP 3FN was taken down by the FTC on June 4, 2009.
- **2007-2012:** Zeus - financial info stealer, variants of software sold for \$500-\$15K. Still prevalent. Configs stored in AWS EC2, use of Google, Twitter, Facebook.
- **2008-2009:** Torpig/Anserin - Financial info stealer. Includes Mebroot rootkit. UCSB researchers temporarily controlled for 10 days in 2009.
- **Nov. 2008:** Conficker worm - Variants A-E, end action of A-D was to update to subsequent versions; disabled Windows update and AV. Variant E (Apr 2009) installed Waledac spambot and SpyProtect scareware. Massive propagation (10.5M+). On May 3, 2009, variant E deleted itself and left C.



Botnet Evolution: History

Dec 2008: Koobface - Social network C&C, had Mac version. Click fraud, scareware sales. Gang exposed in NY Times.



Botnet Evolution: History

- **2009:** Grum/Tedroo -Spammer, generated 26% of spam in March 2010.
- **Mar 2009:** Coreflood - Info stealer, taken down Apr 2011 (FBI w/ISC).
- **Apr 2009:** Waledac - Spammer. 1% of spam volume. Microsoft takedown of C&C domains Feb. 2010, spam domains Sep. 2010.
- **May 2009:** Bredolab trojan - Botnet. 30M bots, 143 C&C seized by Dutch police Oct. 25, 2010, Armenian suspect arrested.
- **2009:** Aurora - Google attacked.
- **2009:** Mariposa (Spain) - Info stealer, spam, DDoS. Taken down by Spanish police (w/Panda Security), Dec 23. 8-12M bots.
- **Apr 2010:** Storm 2 - Minus P2P



Botnet Evolution: History

2011: DNSChanger - Esthost/Rove Digital, redirected 6 million people to malicious websites, 4M bots. Nov 8: 100 servers seized in U.S., 6 Estonians arrested.

BUNDESPOLIZEI
NATIONAL CYBER CRIMES UNIT
ACHTUNG!!!

Achtung!!!

Das Betriebssystem wurde im Zusammenhang mit Verstößen gegen die Gesetze der Bundesrepublik Deutschland gesperrt!

Es wurde folgender Verstoß festgestellt: Ihre IP-Adresse lautet mit dieser IP wurden Seiten mit pornografischen Inhalten, Kinderpornografie, Sadomasochismus und Gewalt gegen Kinder aufgerufen. Auf Ihrem Computer wurden ebenfalls Videodateien mit pornografischen Inhalten, Elementen von Gewalt und Kinderpornografie festgestellt!

Es wurden auch Email in Form von Spam, mit terroristischen Hintergründen, verschickt. Diese Sperrung des Computers dient dazu, Ihre illegalen Aktivitäten zu unterbinden.

Um die Sperrung des Computers aufzuheben, sind Sie dazu verpflichtet eine Strafe von 100 Euro zu zahlen. Sie haben zwei Möglichkeiten die Zahlung von 100 Euro zu leisten.

1) Die Zahlung per Ukash begleichen

Dazu geben Sie bitte den erworbenen Code in das Zahlungsfeld ein und drücken Sie anschließend auf OK (haben Sie mehrere Codes, so geben Sie Diese einfach nacheinander ein und drücken Sie anschließend auf OK).

2) Die Zahlung per Paysafecard begleichen

Dazu geben Sie bitte den erworbenen Code (gegebenfalls inkl. Passwort) in das Zahlungsfeld ein und drücken Sie anschließend auf OK (haben Sie mehrere Codes, so geben Sie Diese einfach nacheinander ein und drücken Sie anschließend auf OK).

Bitte das System Fehler melden, so müssen Sie den Code per Email erstattung@center.bundeskriminalamt.de versenden.

Ukash Wo kann ich Ukash kaufen?

Es gibt unzählige Möglichkeiten, Ukash zu erwerben, z.B. in Geschäften, Kiosken, per Geldautomat, online oder über eine E-Wallet (elektronische Geldbörse). Nachstehend finden Sie eine Liste, aus der hervorgeht, wo Sie in Ihrem Land Ukash erwerben können.

Tankstellen - jetzt auch erhältlich befolgenden Tankstellen: Agip, Avia, Esso, OMV, Qi und Westfalen.

Esso, Agip, Avia, OMV, Qi, Westfalen, Esso

Ebay - Kaufen Sie Ukash in vielen tausend Supermärkten oder Cash-Shops, in denen Sie dieses Logo sehen.

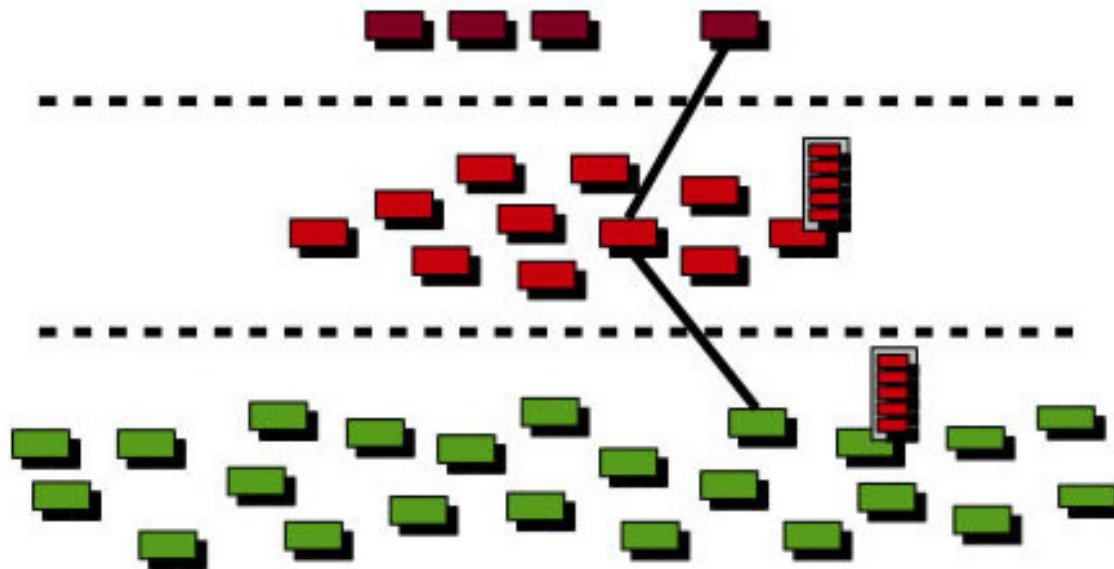
Ukash

paysafecard

Figure 1. Police Trojan displays this image, which differs per country

Botnet Evolution: History

2011: Kelihos/Hlux/Waledac 2.0 - P2P botnet similar to Waledac. 3-tier design: controllers, routers, workers. Spam, MacDefender scareware. Taken down Sep 26, 2011 by Microsoft.

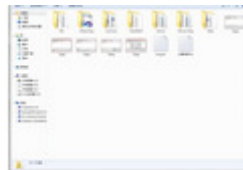


Botnet Evolution: Present Day

2011- 2012: Darkshell - DDoS botnet & buyable kit.



DarkShell.




DarkShell.














DarkShell.



Vip1.34 Edition

 [Download the update statistics](#)

 [official products DarkShell local version	122	11-28
 [official products] DarkShell Professional (VIP)	130	11-24
 [official] DarkShell free version	124	11-24
 The official products] Vip1.34, updated version	181	09-05
 [software] (-DDOS) denial of server attack detection	71	08-25
 Official Product] Vip1.33	152	08-24
 [official products] BETA1.2 version update	173	08-17
 Official Product] Vip1.32	104	08-15
 Official Product] DarkShell.Source	273	08-06
 Official Product] DarkShell.BETA	355	08-06
 Official Product] DarkShell.VIP	209	08-06

软件总数: 11个软件

今日更新: 0个软件

下载总数: 1894人次

[[浏览软件详细列表](#)]

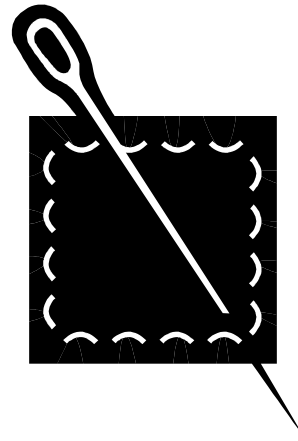
Botnet Evolution: Present Day

Feb 2012: Flashback trojan - Exploits Java flaw. Mac botnet 655K+ strong. Deletes itself if ClamXav is installed.



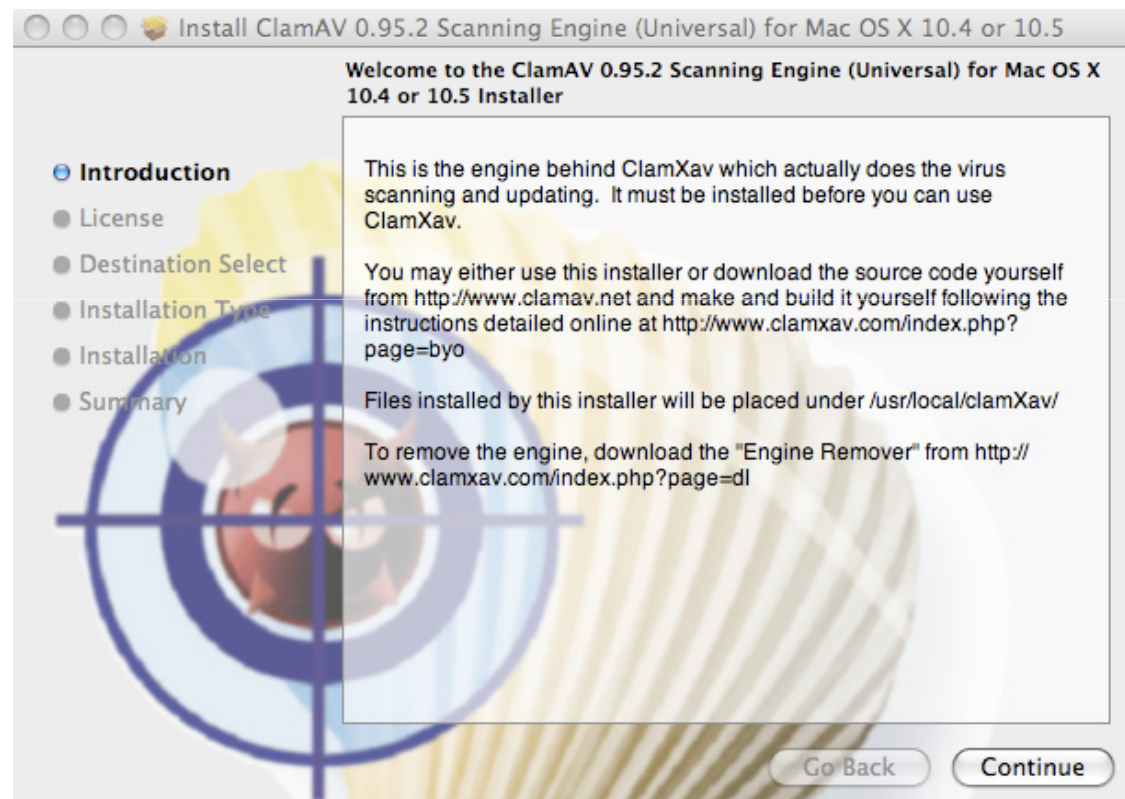
Defense

- Patch.



Defense

Mac users: It's time for AV.



Defense

Filter

- Outbound traffic
- Web content filtering
- Application control
- Identity awareness
- Intrusion prevention
- Data leak prevention
- Web application firewall



Defense

Monitor

- Signs of bots often show up in web and DNS requests
- Monitor user login activity; 30% of breaches use stolen credentials
- Log and alert/review
- You need an incident response plan



Defense

- Report
- Collaborate



Offense

- Track
- Takeover
- Takedown
- Arrest & Prosecute



FBI:

May 22, 2001: Operation Cyber Loss – 62 arrests

May 16, 2002: Operation E-Con – 50 arrests

Nov 20, 2003: Operation Cyber Sweep – 125 arrests

Feb 14, 2004: Operation Cyber Slam – Foonet DDoS

May 20, 2004: Operation SLAM-Spam - 50 targets

Jun 13, 2007: Operation Bot Roast – 3 arrests

Nov 29, 2007: Operation Bot Roast II – 3 indictments

Sep 30, 2010: Operation Trident Beach – 5 Ukraine arrests, Zeus partial takedown

Apr 2011: Coreflood takedown (w/ISC)

Nov 8, 2011: Operation Ghost Click – 6 Estonians arrested for DNSChanger. (w/Trend Micro)

Microsoft Digital Crimes Unit:

Feb 22, 2010: Operation b49, Waledac C&C takedown (w/Shadowserver, Symantec)

Oct 27, 2010: Operation b49, Waledac spam takedown

Mar 16, 2011: Operation b107, Rustock takedown (w/FireEye)

Sep 26, 2011: Operation b79, Kelihos/Waledac 2.0 takedown; civil suit vs. Dominique Alexander Piatti.

Mar 23, 2012: Operation b71, Zeus takedown (w/F-Secure)

CrowdStrike:

Mar 29, 2012: Kelihos v2 takedown (w/SecureWorks, HoneyNet Project, Kaspersky)



Future

- Macs as targets
- Social networks as delivery mechanism
- Mobile as target
- More indirect attacks (CAs, RSA, Sophos)
- Competing legal agendas:
 - Global Online Freedom Act (GOFA) HR 3605
 - Cyber Intelligence Sharing and Protection Act (CISPA) HR 2523
- A decline in the use of large botnets except as “stepping stones”



Q&A

Any questions?

Jim Lippard

Sr. Product Manager, Security

EarthLink Business

jlippard@corp.earthlink.com

Twitter: @lippard

