Malware World 2010

Beware the Predators

Toralv Dirro
McAfee Labs EMEA Security Strategist

$70mio International Cybercrime Ring Busted

- October 1st 2010: Operation Trident Breach
  - Investigations began in May 2009
  - 60 criminals charged, 10 arrested
  - International Partnership with SBU and other authorities
    - The Federal Bureau of Investigation, including the New York Money Mule Working Group, the Newark Cyber Crime Task Force, the Omaha Cyber Crime Task Force, the Netherlands Police Agency, the Security Service of Ukraine, the SBU, and the United Kingdom's Metropolitan Police Service participated in the operation.
  - The cyber thieves targeted small- to medium-sized companies, municipalities, churches, and individuals, infecting their computers using a version of the Zeus Botnet. The malware captured passwords, account numbers, and other data used to log into online banking accounts. This scheme resulted in the attempted theft of $220 million, with actual losses of $70 million from victims' bank accounts

FOCUS 09
Anatomy of a scareware company

Using more than 63 gigabytes of information culled from querying the company's own portal servers and other publicly available data, Dirk Kollberg, from McAfee Labs, unearthed some astonishing operational details including the following:

- Innovative Marketing used more than 34 different production servers in less than six months and used as many as six different servers at a time to infect, advertise and sell their illicit wares.
- In one 10-day stretch, the company received more than 4 million download requests, meaning that at least 4 million people tried to buy the worthless applications.
- Internal documents report that the URLs used to hawk the scareware are only valid for 15 minutes, making it all but impossible for federal, state or international law enforcement agencies to yank the offending URLs before they've moved on to new addresses.
- It used multiple customer call centers, including at least one in Poland and one in India, to service unsuspecting customers calling via VoIP connections to buy, remove or question the need for the unnecessary scareware. And, believe it or not, they recorded and saved these bogus customer service calls. More incredibly, 95 percent of callers exited were "happy" when the call concluded.
- Because they needed an extensive network of ISPs to pull off the scam, Innovative Marketing kept detailed spreadsheets with all the ISPs pertinent data including price, location and, most telling, a column that rate the ISPs "abuseability"—essentially an assessment of which ISPs would play ball and not ask questions as they went about their business.
- The company added a whopping 4.5 million order IDs, essentially new purchases, in 11 months last year. With most of the phony applications selling for $39.95, that's more than $180 million in less than a year.

http://www.internetnews.com/security/article.php/3842936/McAfee+FOCUS+09+Anatomy+of+a+Scareware+Scam.htm

FTC vs. Innovative Marketing

„ The FTC succeeded in persuading a U.S. federal judge to order Innovative Marketing and two individuals associated with it to pay $163 million it had scammed from Americans. Neither individual has surfaced since the government filed its original suit more than a year ago. But Ethan Arenson, the FTC attorney who handled the case, warned: "Collection efforts are just getting underway.""

(Source: Reuters)

Price Estimates for Credit and Debit Card Dumps

Dumps are information electronically copied from the magnetic stripe on the back of credit and debit cards. Prices for these data vary, depending on the inclusion of the card's PIN.

Credit and Debit Card Dumps	Estimate of Prices (without PIN, with PIN) in U.S. Dollars							
	United States		European Union		Canada, Australia		Asia	
Visa Classic	15	80	50	150	30	150	50	150
MasterCard Standard		90		140		150	60	140
Visa Gold/Premier	30	100	70	160	35	160	120	150
Visa Platinum		110		170		170	150	170
Purchasing/Signature	35	120	100		40		100	
Business/Corporate	45	130		170		175	150	170
Infinite			130	190	45	200		190
MasterCard World		140						
AMEX Green	20							
AMEX Red			40					
AMEX Gold	40		70					
AMEX Platinum	50							

The Malware Market

Trojan and Exploit Kits easily available

Exploit Kits (Release)	Prices in U.S. Dollars	Description
Zombie Infection Kit (July)	1,000	New Russian kit contains at least 10 package exploits, including: • Windows Help Center (HCP) CVE-2010-1885 • Java Web Start Argument Injection CVE-2010-0886
Phoenix v2.3r (August)	2,200	The Phoenix Exploits Kit first appeared in 2007 and receives regular updates. Today it includes 15 exploits, with 5 from 2010: • Adobe Reader LibTiff CVE-2010-0188 • Java SMB CVE-2010-0746 • IE iepeers CVE-2010-0806 • Adobe PDF SWF CVE-2010-1297 • Windows Help Center (HCP) CVE-2010-1885
CrimePack v3.1.3 (July)	400	CrimePack appeared in 2009. Among 14 exploits, 4 are from 2010: • IE iepeers CVE-2010-0806 • Java getValue CVE-2010-0840 • JRE toolkit cmd exe CVE-2010-1423 • Windows Help Center (HCP) CVE-2010-1885
SpyEye v1.2 (April)	Kit for 500–1,000	Created by Gribodemon, v1.0 came to market in December 2009. Version 1.2 is a serious Zeus competitor.
Zeus	Kit for 3,000–4,000. Must include add-ons and plug-ins from 500–10,000	The most important news this quarter is the appearance of Zitmo (Zeus in the Mobile). We also saw the first samples of v2.1.

Zeus: Development of a Trojan Kit

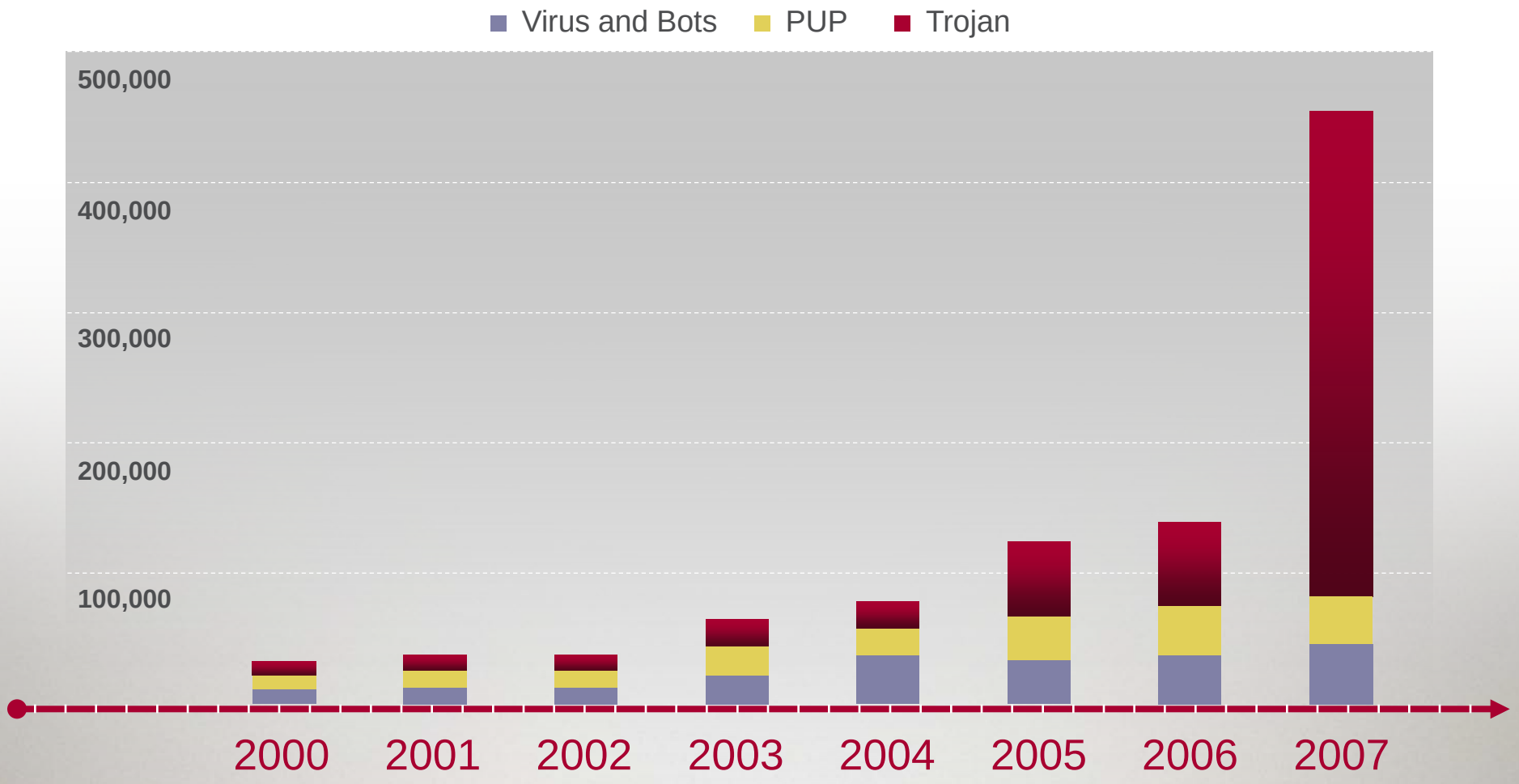
Date	Version	Comments
2006	V1.0.0.0	
JUN 2008	V1.0.3.7	
AUG 2008	V1.0.6.8	
NOV 2008	V1.0.6.9	
	V1.0.6.27	
	V1.1.0.0	
NOV 2008	V1.1.1.0	
20 DEC 2008	V1.2.0.0	RC4 encryption / BackConnect function Price: 3000$ / 4000$
30 DEC 2008	V1.2.1.0	Price: 3000$
	V1.2.1.2	
	V1.2.1.4	
	V1.2.1.6	
	V1.2.1.10	
11 MAR 2009	V1.2.2.0	
	V1.2.2.1	
28 MAR 2009	V1.2.3.0	
02 APR 2009	V1.2.4.0	
	V1.2.4.2	
	V1.2.4.6	
27 MAY 2009	V1.2.5.0	
	V1.2.5.1	
04 JUN 2009	V1.2.6.0	
	V1.2.6.1	
22 JUN 2009	V1.2.7.0	Ability to disable the phishing filter in IE7, IE8
	V1.2.7.5	
	V1.2.7.7	
	V1.2.7.10	
	V1.2.7.11	
	V1.2.7.15	
	V1.2.7.16	
	V1.2.7.19	**FireFox Form Grabber module** **Price: 1500$ / 3500$**
	V1.2.7.21	
05 OCT 2009	V1.2.8.0	
	V1.2.8.1	
11 OCT 2009	V1.2.9.0	
17 OCT 2009	V1.2.10.0	Jabber real time notification
	V1.2.10.1	
NOV 2009	V1.2.11.0	Hardware locking

Date	Version	Comments
NOV 2009	V1.2.12.0	
22 NOV 2009	V1.3.0.0	TAN grabber removed / Winlicense packer / OK for Vista and 7 / VNC Prices: 3000$ / 6000$: Zeus Kit 1500$: Backconnect module 2000$: Mozilla Grabber 500$: Jabber IM plugin 10000$: VNC module
	V1.3.1.1	
	V1.3.1.2	
	V1.3.1.10	
	V1.3.2.1	
	V1.3.3.0	
	V1.3.3.6	
	V1.3.4.0	
DEC 2009	v1.3.4.1	
	V1.3.3.5	
DEC 2009	V1.4.0.0	Randomized filenames / Polymorphism / OK for FireFox Price: about 16k $
11 JAN 2010	V1.3.2.0	
	V1.3.2.1	
JAN 2010	V1.3.4.2	
JAN 2010	V1.4.1.0	
	V1.3.4.3	
	V1.3.4.4	
APR 2010	V2.0.0.0	Stolen data saved in the Registry
MAI 2010	v2.0.0.1	
	V2.0.1.1	
JUL 2010	V2.0.2.1	
	V2.0.3.1	
	V2.0.4.0	
JUN 2010	V2.0.5.0	Price: 500$
JUL 2010	V2.0.6.1	
JUL 2010	V2.0.6.2	
JUL 2010	v2.0.6.3	
JUL 2010	V2.0.6.5	
AUG 2010	**V2.0.7.0**	
	V2.0.7.4	
	V2.0.8.0	
	V2.0.8.7	
	V2.0.8.9	
SEPT 2010	V2.1.0.0	New config style
	V2.1.0.6	
	V2.1.0.7	

Mergers and Accquisitions: SpyEye & Zeus

Date	Version	Comments
29 DEC 2009	v1.0	Price: 500 WMZ (USD 500)
8 JAN 2010	v1.0.1	
10 JAN 2010	v1.0.2	
13 JAN 2010	V1.0.6	
27 JAN 2010	V1.0.65	CC Autofil module. Formgrabber with built-in keylogger. Web Control Panel
4 FEB 2010	V1.0.7	Zeus Killer Module
8 FEB 2010	v1.0.72	
14 FEB 2010	v1.0.75	
26 FEB 2010	v1.0.8	Webinjects capability using Zeus format. Price: 1000 WMZ (USD 1000)
19 MAR 2010	v1.0.9	Price for the FTP-Backconnect module for new customers : 333 WMZ (USD 333)
28 MAR 2010	v1.1	Price for the Firefox Injection module : 500 WMZ for old customers and 1000 WMZ for new ones (USD 500 / USD 1000)
11 AVR 2010	v1.2	
14 JUL 2010	v1.2.4	
11 AUG 2010	?	Basic package: 1000 WMZ Injects for FF: + 1000 WMZ SOCKS plugin: +750 WMZ
?	V1.2.50	
?	V1.2.57	Price: 400$
?	V1.2.60	Price: 500$
?	V1.2.80	Price: 650$
10 OCT 2010		Posts on various forum are removed by the author (gribodemon/harderman)
13 OCT 2010		Harderman announces he succeeds Slavik (the ZeuS author) who quits the scene. All clients who bought the software from Slavik will be serviced from him. In another conversation, Harderman says the two malware families(SpyEye & Zeus) will soon be merged into one powerful Trojan.
NOV 2010		Rumor said that old customers of SpyEye will have to pay $4000 more to have continuity in the new Zeus project. Old Zeus customers will have 30% discount. SpyEye is dead.

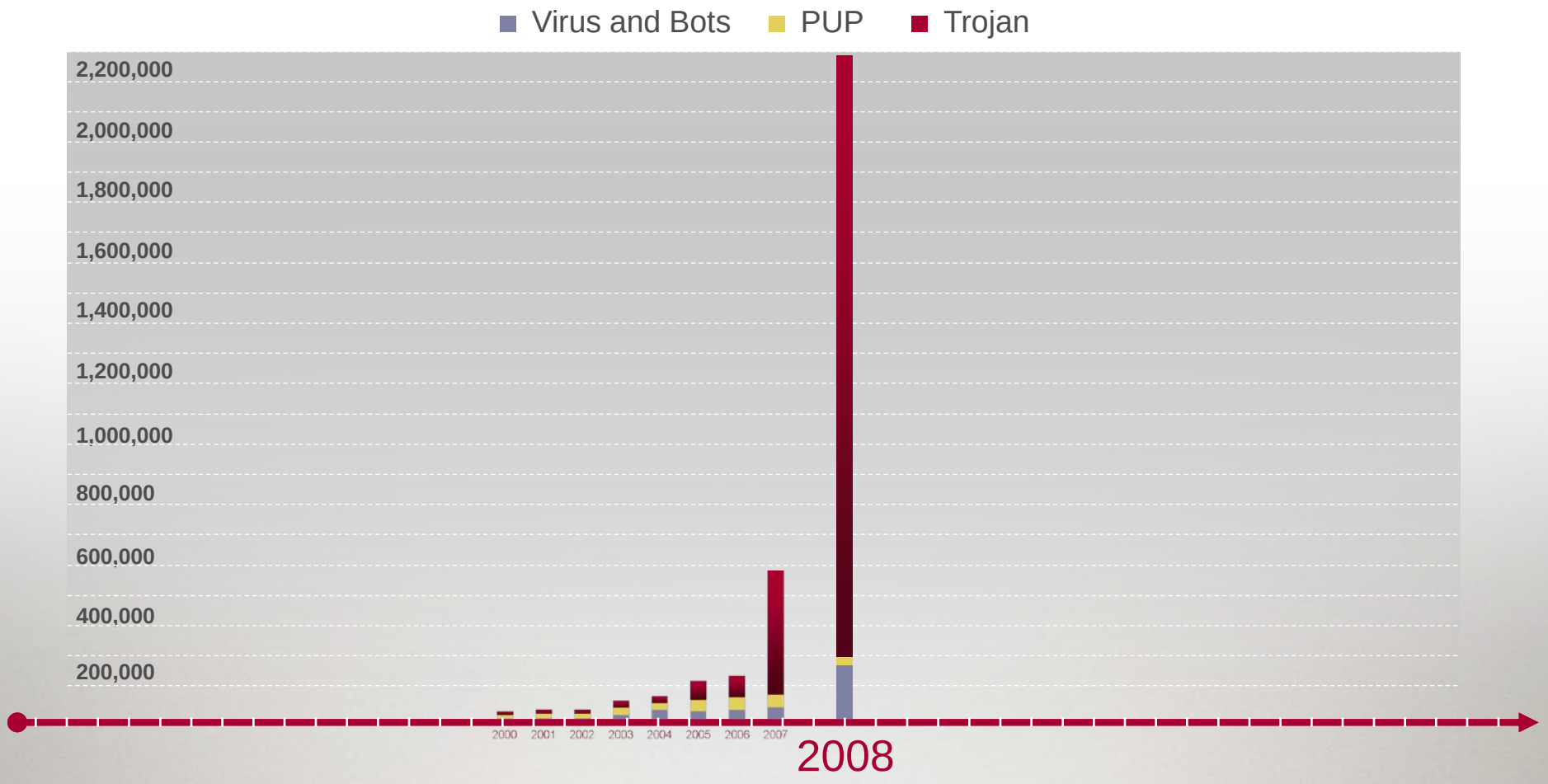
Cyber Crime Altering Threat Landscape



Malware Growth (Main Variations)

Source: McAfee Labs

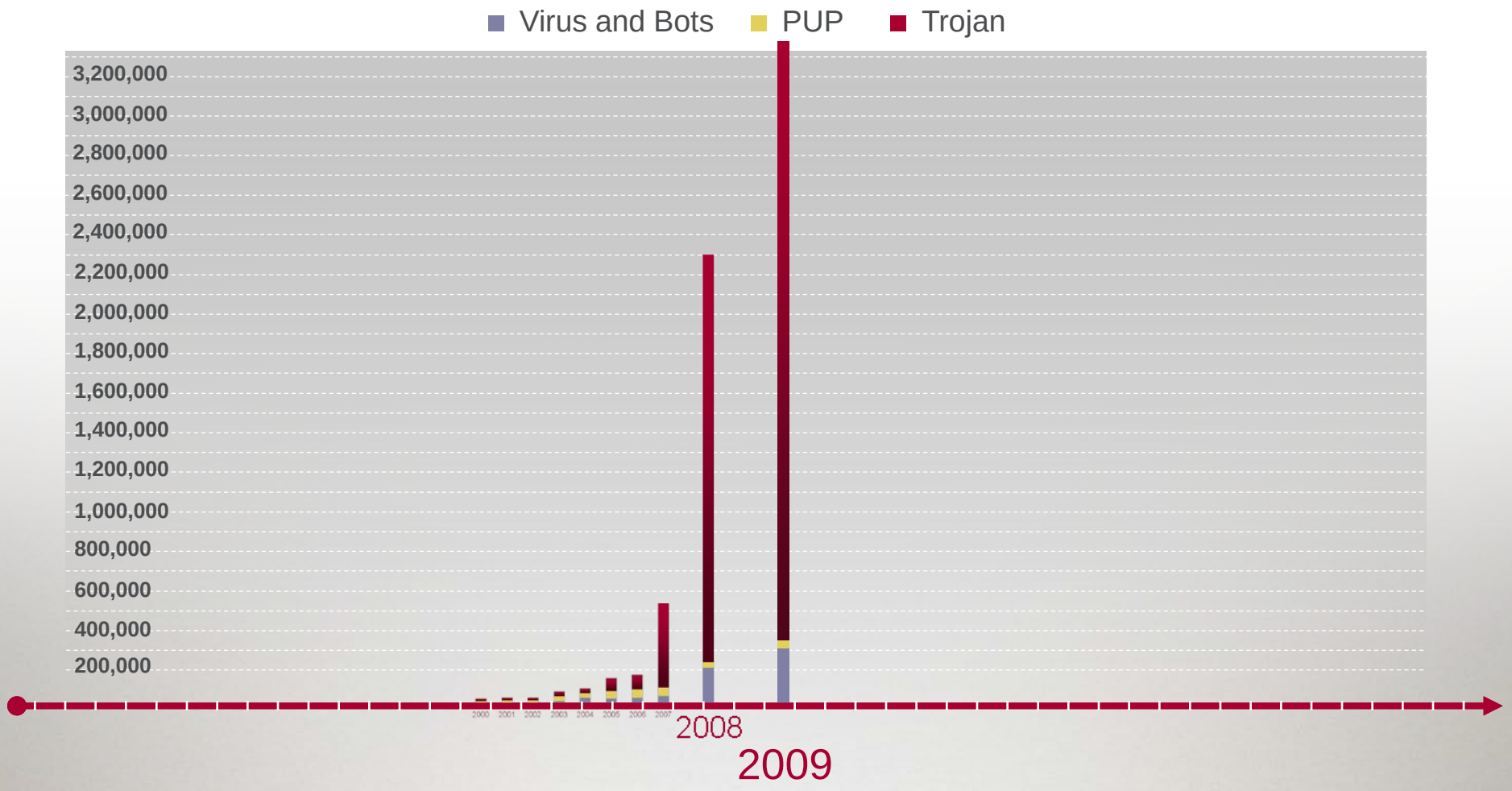
Cyber Crime Altering Threat Landscape



Malware Growth (Main Variations)

Source: McAfee Labs

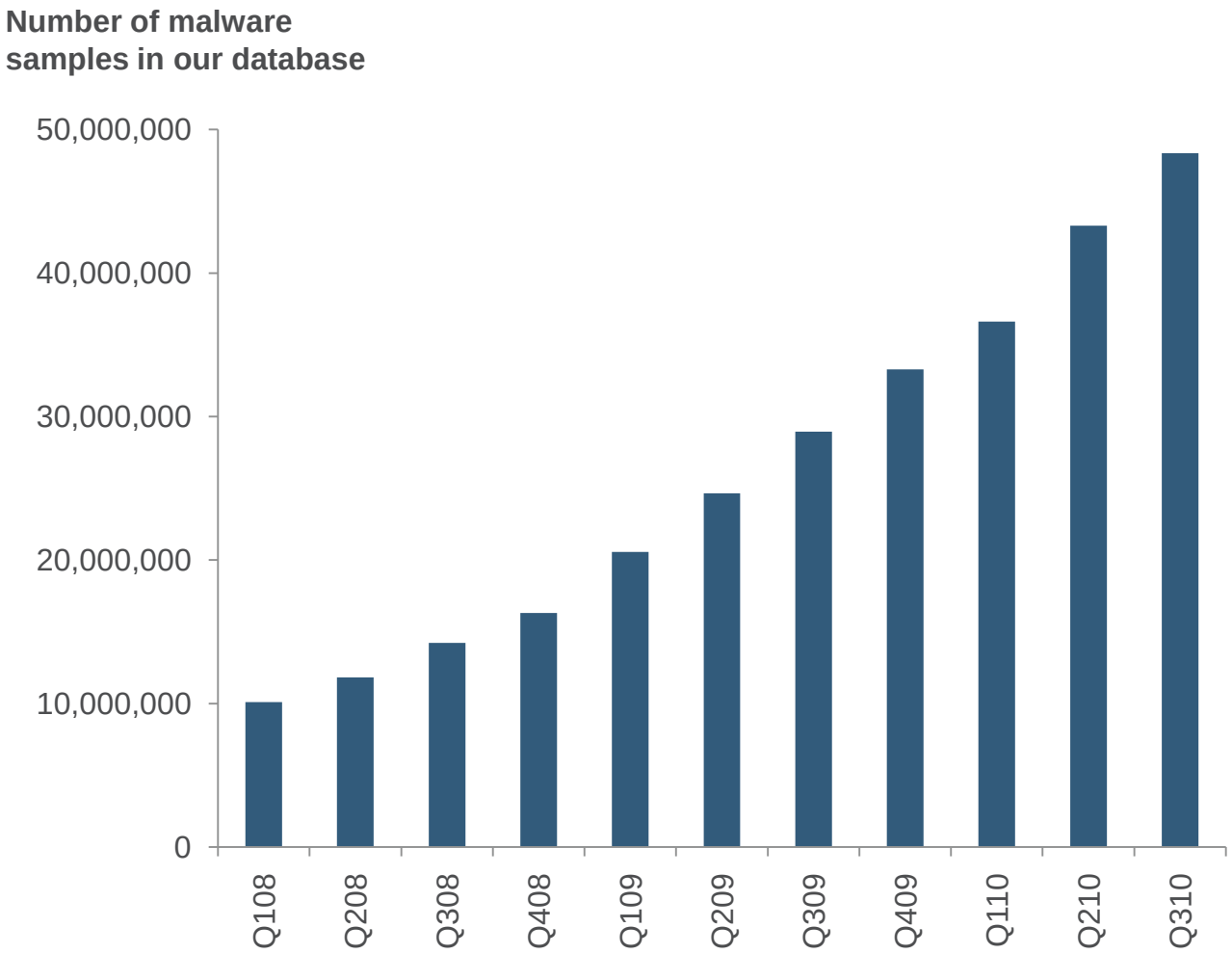
Cyber Crime Altering Threat Landscape



Malware Growth (Main Variations)

Source: McAfee Labs

Malware still growing strong ☹



New pieces of malware per day:

2007: 16,000
2008: 29,000
2009: 46,000

Q1/2010: 40.000
Q2/2010: 55.000

Q3/2010: **60.000**

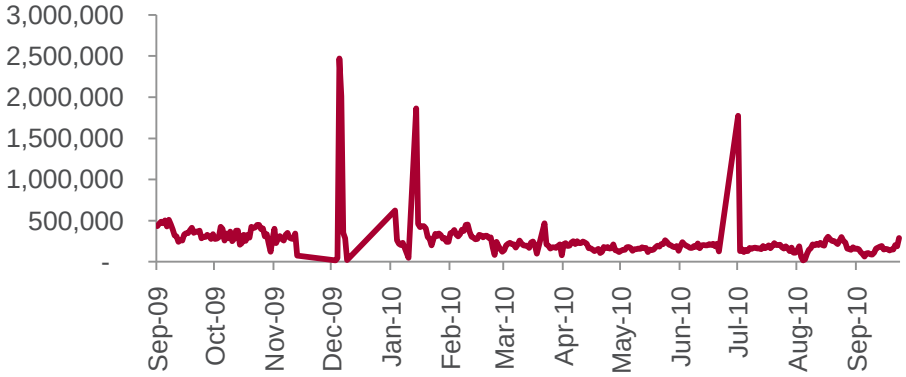
Top 10 Malware Globally

1) Generic! Atr
   Generic removable-device malware
2) Generic.dx
   Generic downloaders and Trojans
3) W32/Conficker.worm!inf
   Removable-device Conficker worm
4) FakeAlert-FakeSpy!env.a
   Legitimate-looking fake anti-virus scam
5) Exploit-CVE2008-5353
   A JRE exploit that downloads a Trojan
6) GameVance
   Online gaming software that collects stats anonymously
7) Generic PUP.x
   General-purpose potentially unwanted programs
8) Adware-Hotbar.b
   Adware program
9) Exploit-ByteVerify
   Java applet Trojan
10) Adware-URL.gen
    Adware program

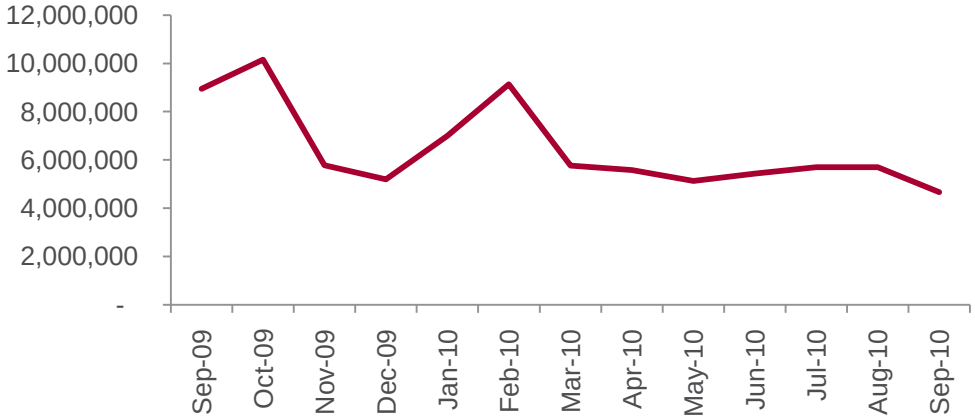
Two notable adware programs have joined the top ten list, both spread via malicious websites.

Botnet Infections Held Steady

Overall Botnet Infections Per Day

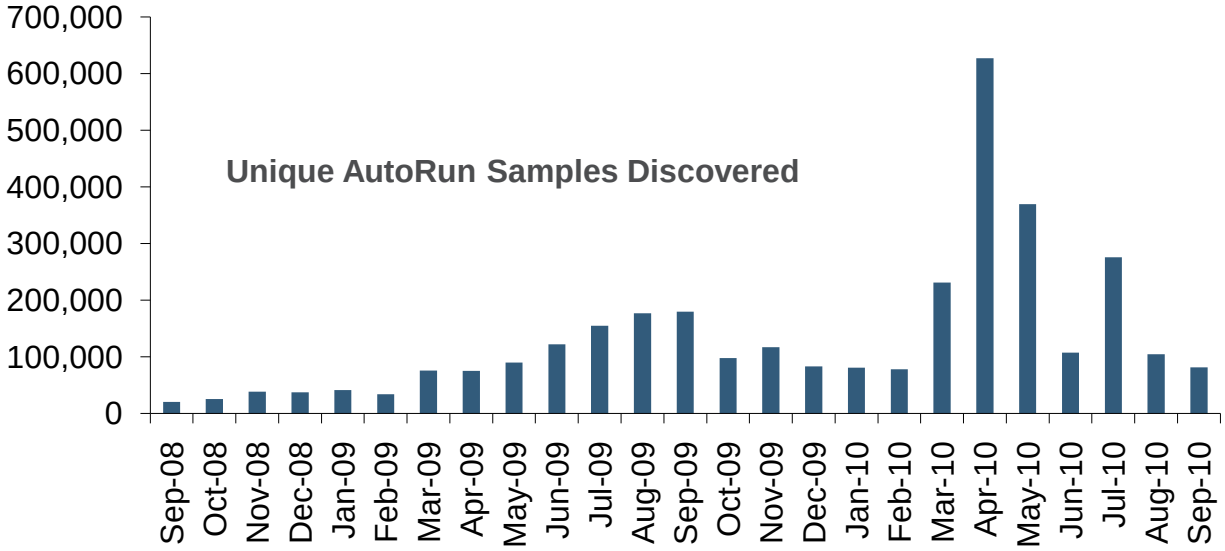


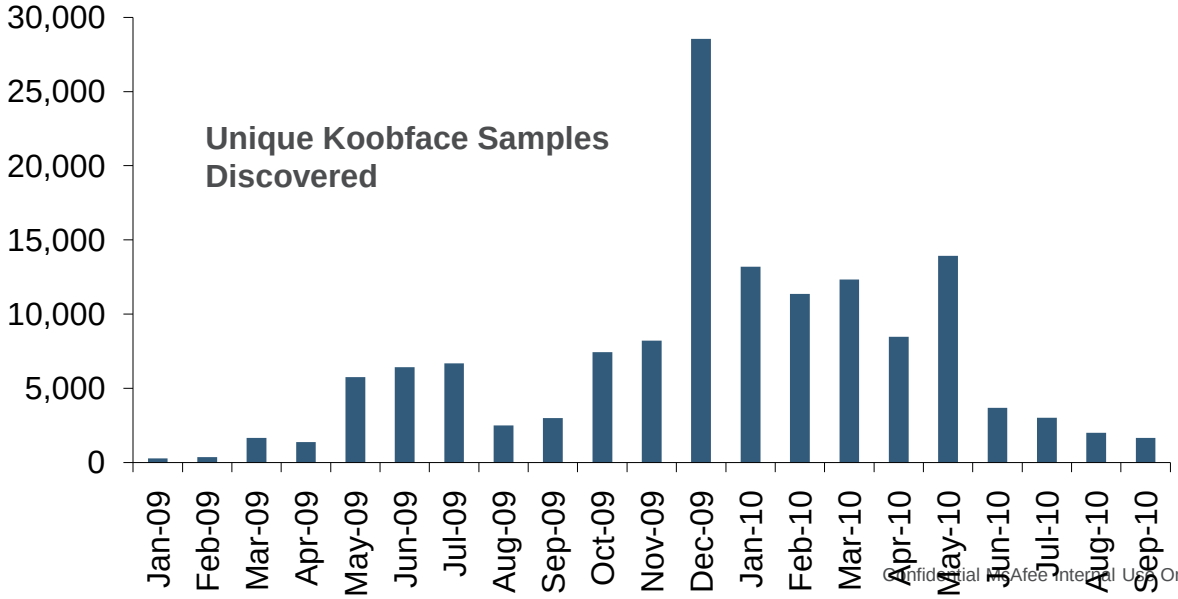
Overall Botnet Infections Per Month



We have seen new botnet infections hold steady at around six million per month.

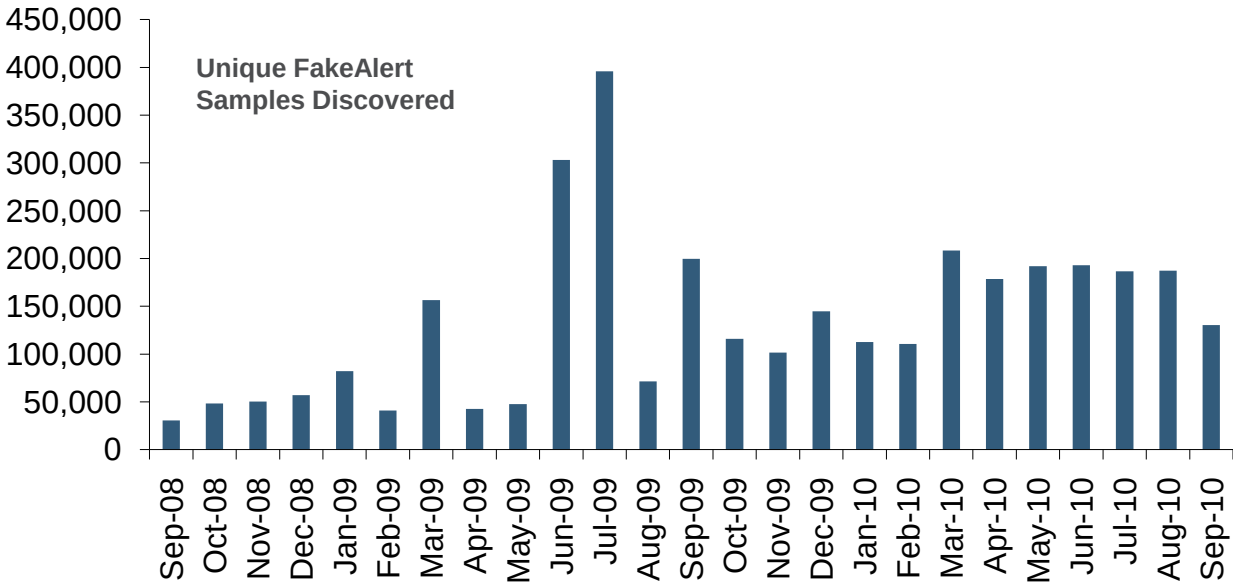
AutoRun And Koobface Level Off

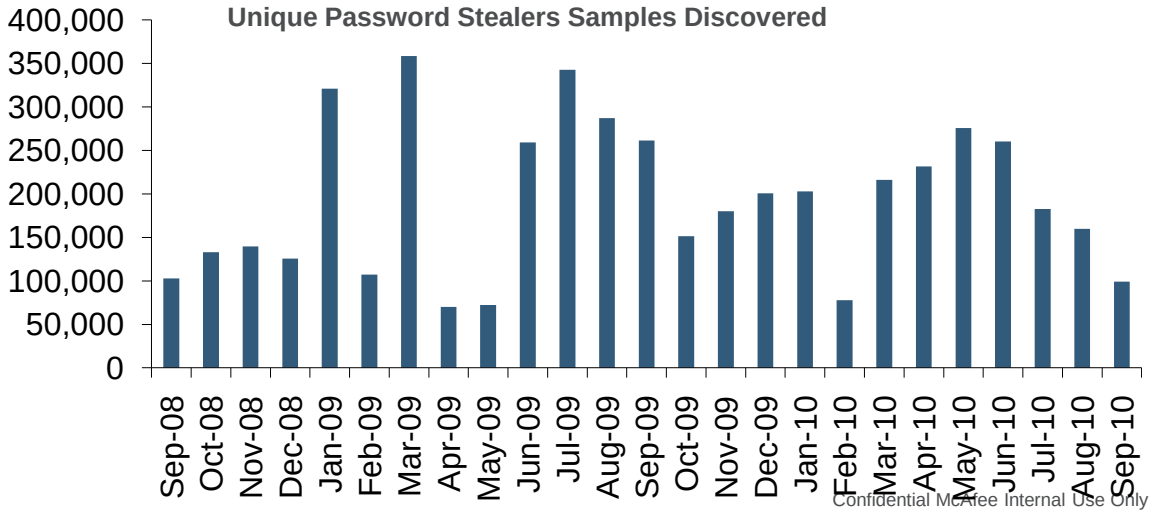




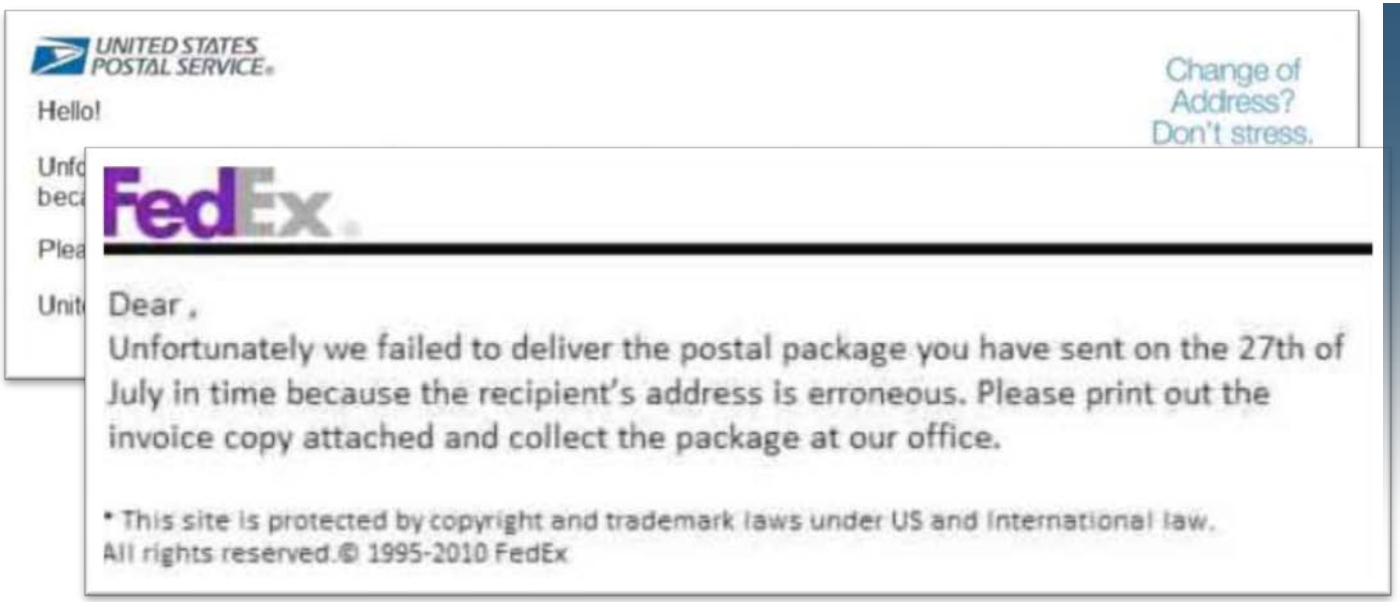
Fake Security Software Peaked in ’09

But Remains High for This Lucrative Form of Cybercrime



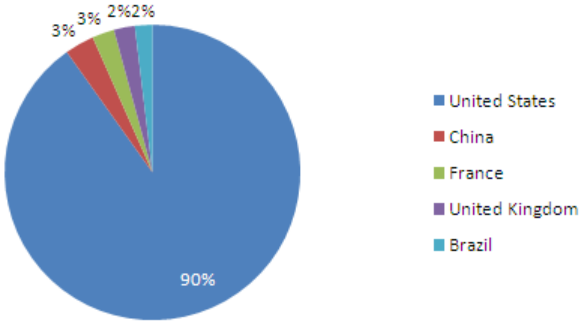


Zeus Is In a Class All By Itself

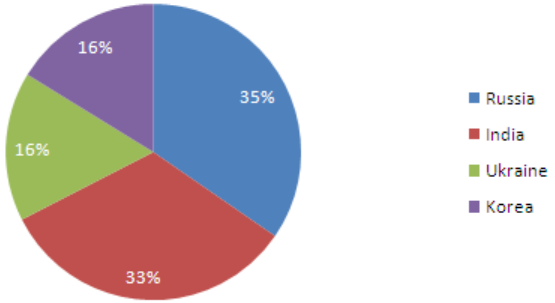


Zeus (Zbot or PWS-Zbot) is spread via download or phishing sites. Some Zeus campaigns switched from text to graphics in emails to avoid anti-spam technologies.

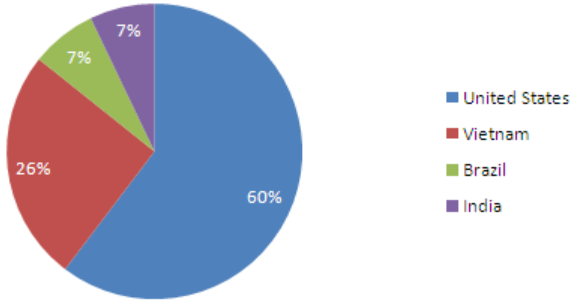
USPS Zeus Campaign



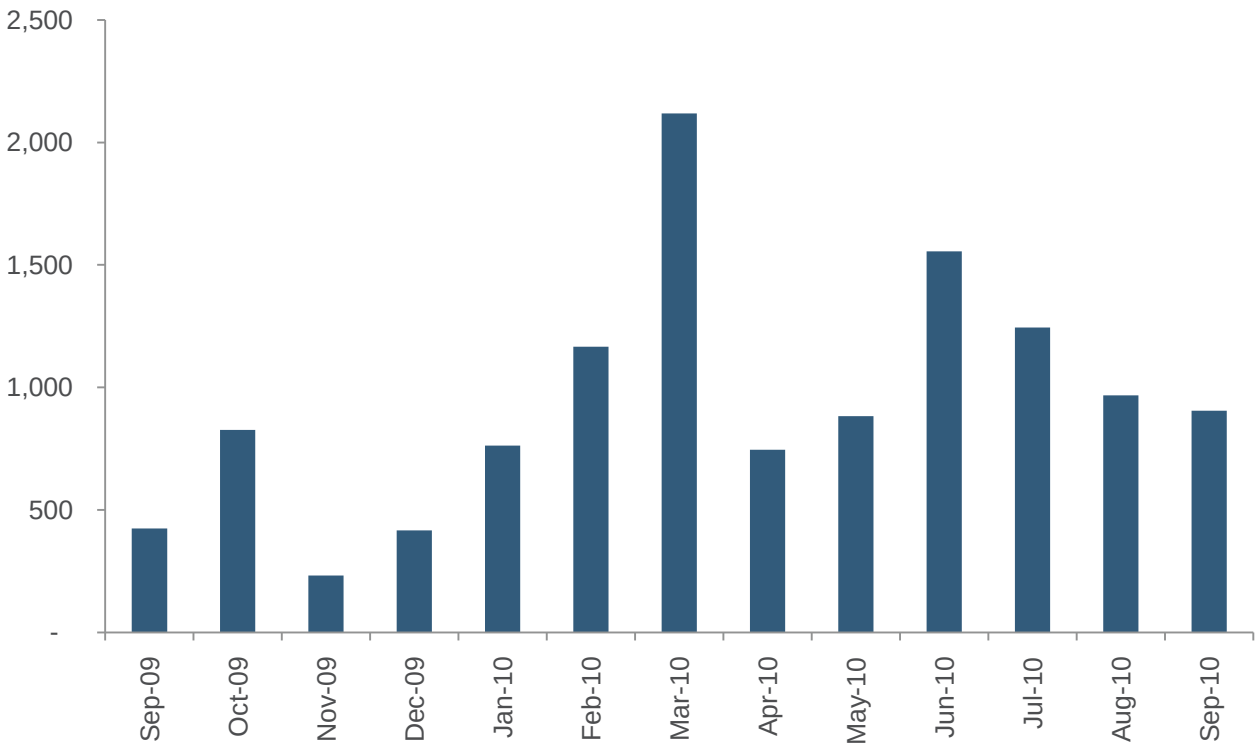
SSA Zeus Campaign



eFax Zeus Campaign



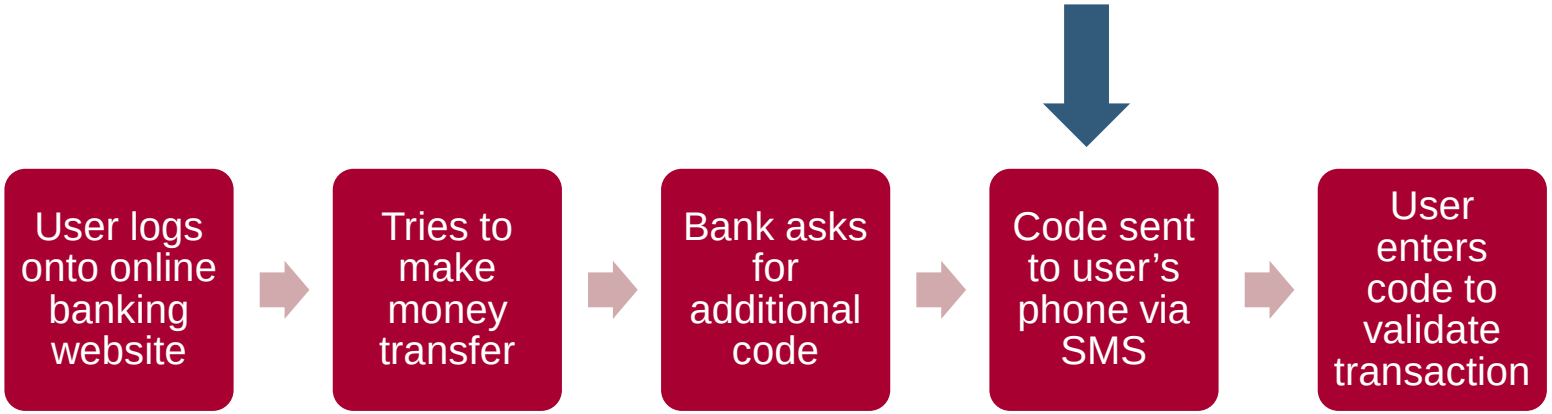
Websites Hosting Zeus



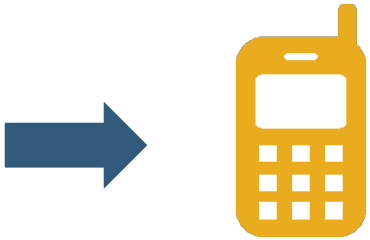
McAfee Labs is finding URLs dedicated to hosting Zeus.

Zeus Goes Mobile

Zeus intercepts so it can validate its own transactions



Then Zeus can send a message to the user's phone directing them to a malicious website



Cybercriminals Are Optimizing Their Threats for Search Engines

This quarter's most poisoned search topics:

- Haiti earthquake
- Chile earthquake/Hawaii tsunami warning
- Toyota recall
- Apple iPad
- 2010 NCAA bracket/March Madness
- Tiger Woods apology
- Shamu attack/Florida shark attack
- Olympic luge tragedy
- Groundhog Day
- U.S. Health Care Reform Bill

And They Go Where We Go!

60% of Top Google Search Terms Returned Malicious Sites in the First 100 Results

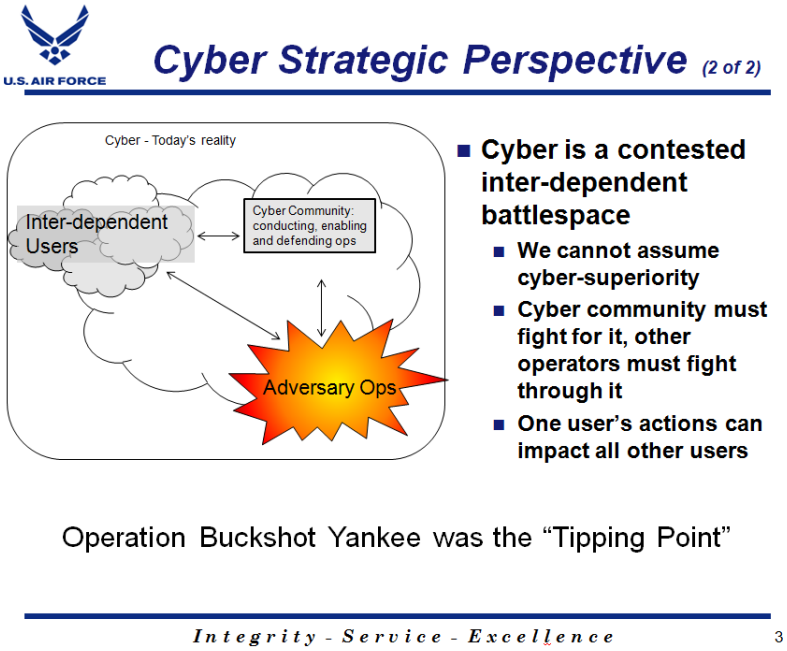
Web/Domain Reputation

Top 15 Website Categories	Number of Sites
Malicious Sites	14,475,580
Residential IP Addresses	6,040,787
Spam URLs	4,085,439
Pornography	2,815,319
Content Servers	2,511,339
Business	2,510,899
Phishing	1,474,321
Parked Domains	1,215,048
Travel	1,140,018
Anonymizers	997,863
Online Shopping	979,092
Real Estate	873,159
Instant Messaging	842,263
Government/Military	829,381
Marketing/Merchandising	826,286

Number of sites categorized in our Web- and Domain Reputation Services.

Targeted Attacks

- A senior Pentagon official reveals details of a previously-classified malware attack he considers *“the most significant breach of U.S. military computers ever.”*
  - Deputy Defense Secretary William J. Lynn III explains that in 2008, a flash drive believed to have been infected by a foreign intelligence agency uploaded malicious code onto a network run by the military's Central Command.
  - *"It was a network administrator's worst fear: a rogue program operating silently, poised to deliver operational plans into the hands of an unknown adversary."*
  - The incident led to a massive Pentagon response operation called *"Operation Buckshot Yankee"* aimed at purging infected systems of the malware and preventing something similar from happening again.



Source: http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain

Targeted Attacks

- Targeted Attacks and Advanced Persistent Threats (APT)

- Attackers have lots of Ressources
  - 0-Days
  - Customized Malware
    - But Ghost Net used of-the shelf Malware

- High Social Engineering Factor
  - Attachments with supposedly relevant information for the receipient
  - Links to supposedly relevant information
  - Email, Social Network Messages, IM

- Low Distribution to stay under the radar

Stuxnet: Under the Hood

- Discovered in July 2010 by VirusBlokAda company in Minsk, Belarus
- First seen in Iran, Indonesia, India – now spread worldwide
- Targets Siemens WinCC and SIMATIC Process Control System (PCS7)
- Using four 0-day vulnerabilities plus Conficker (MS08-067)
  - Shortcut icon vulnerability (CVE-2010-2568/MS10-046) – affecting every version of Windows since Windows 2000 (even Win95)
  - Design flaw in Print Spooler (MS10-061/CVE-2010-2729)
  - Two privilege escalations exploits [win32k.sys]
- A user opens a folder that contains the .lnk template files (.pif files also vulnerable)
- Rootkit drivers signed with valid certificates (Realtek and Jmicron)
- UPX packed, XOR encoded everywhere
- Once loaded, queries Siemens database with known default password
- Connected to C&C servers, sending sensitive data
- Manipulating the database to control the HMI output and manipulating the PLC's

Stuxnet: a Targeted Attack Runs Rampant

Stuxnet, the first malware targeting industrial control systems, threatens critical infrastructure.

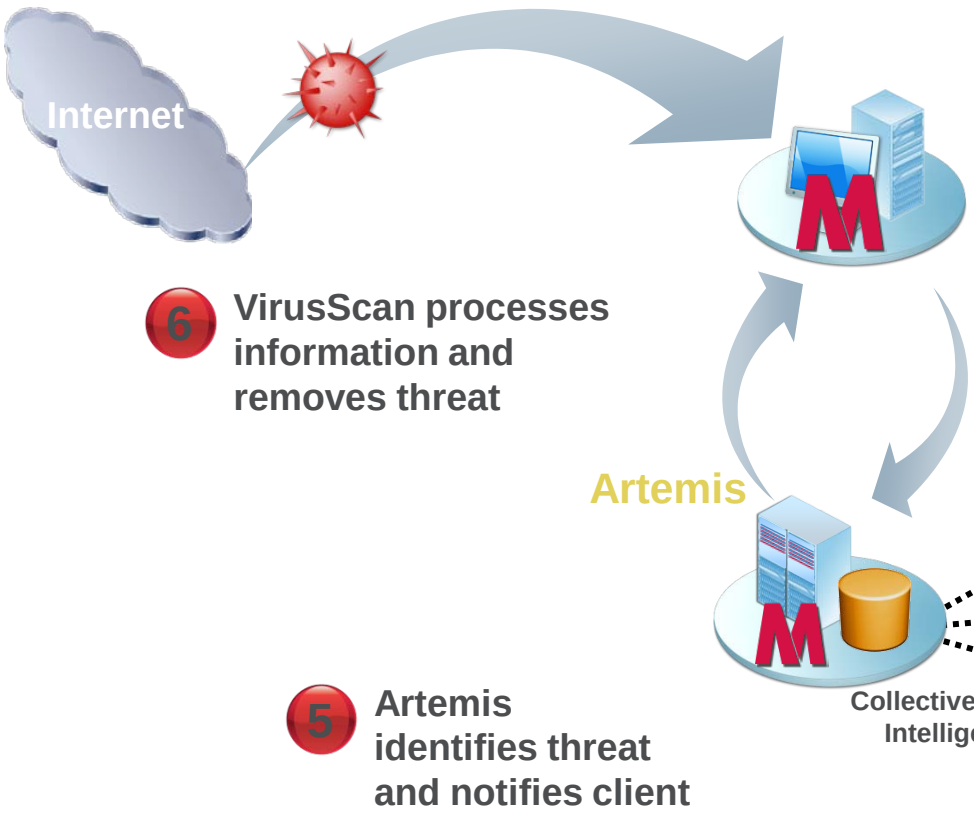
Protection Catching Up: „Cloud Security“

About that In-The-Cloud Security Thingie...

- „Invented“ 3 years ago

- Implemented one way or the other by most major AV vendors
  - And noone really documents what exactly they are doing

So this is how it works



About that In-The-Cloud Security Thingie...

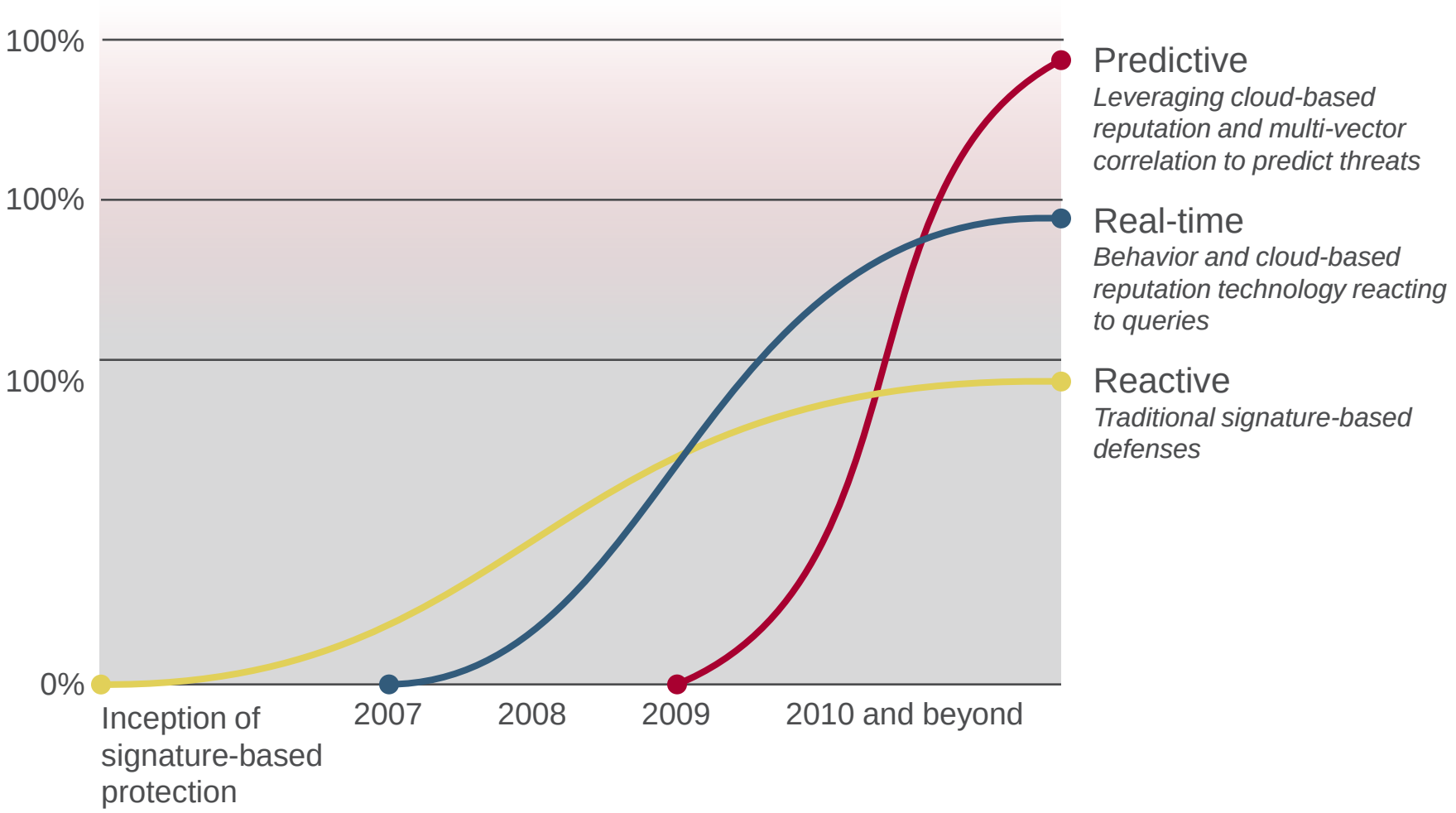
- „Invented“ 3 years ago
- Implemented one way or the other by most major AV vendors
  - And noone really documents what exactly they are doing
- So it‘s basically a file reputation service
  - Comparable to what has been done in other areas long ago
    - AntiSpam
    - Domain Reputation
- Major benefit: Detection Speed (near real-time)
  - And it makes products look great in any test against collections (>99.9%)

Problems of that Cloud Security Thingie...

- True Serverside Polymorphism
  - Needs more metadata than just fingerprint

- Detection only available when online
  - Outbreak situation, Gateway down -> Detection gone ☹

Evolution of Threat Detection



Threat Intelligence Feeds

Correlation of various Reputation Feeds

Malware

- IP addresses distributing
- URLs hosting malware
- Mail/spam including it
- Botnet affiliation
- IPS attacks caused

Domain/URL

- Mail/spam sending activity
- Web access/referer activity
- Malware hosting activity
- Hosted files
- Popups
- Affiliations
- DNS hosting activity

IP address

- Botnet/DDoS activity
- Mail/spam sending activity
- Web access activity
- Malware hosting activity
- Network probing activity
- Presence of malware
- DNS hosting activity
- Intrusion attacks launched

IPS attacks/vulnerabilities

- IP addresses of attackers
- Vulnerability utilized
- Botnet affiliation
- Malware responsible

Lots of data to correlate

Queries

- 2.5B Malware Reputation Queries/Month
- 20B Email Reputation Queries/Month
- 75B Web Reputation Queries/Month
- 2B IP Reputation Queries/Month
- 300M IPS Attacks/Month
- 100M Ntwk Conn Rep Queries/Month
- **100+ BILLION QUERIES**

Nodes

- Malware: 40M Endpoints
- Email: 30M Nodes
- Web: 45M Endpoint and Gateway Users
- Intrusions: 4M Nodes
- **100+ MILLION NODES, 120 COUNTRIES**

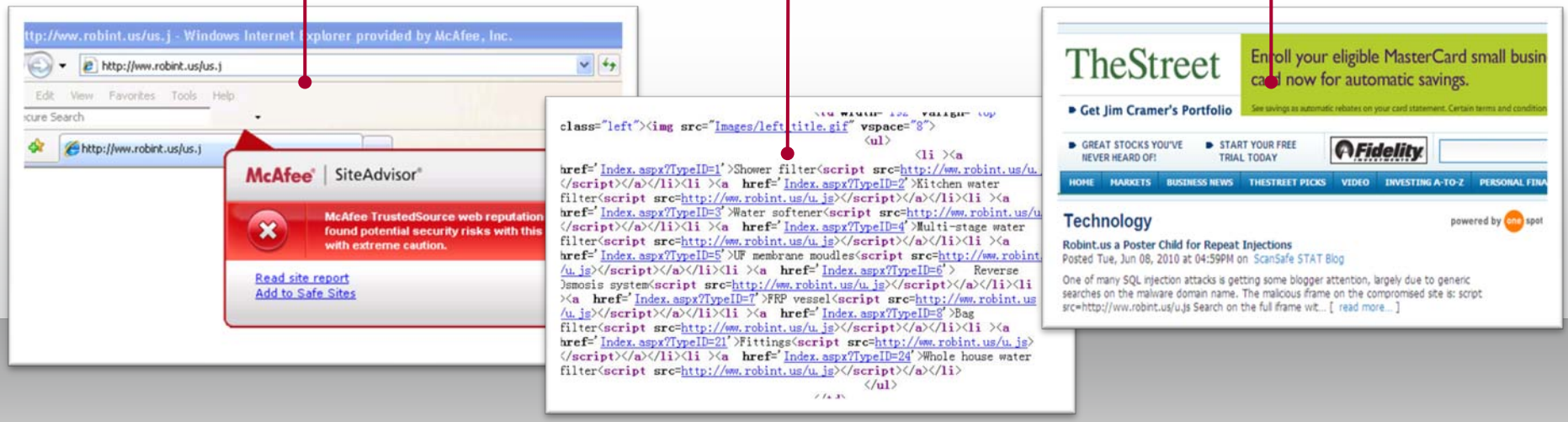
An Example

Predictive Protection Against Widespread iFrame Injection Attack

Domain Reputation flagged anomalous web behavior (registration, traffic) for URL

iFrame injection attack ran malicious javascript, responsible for downloading malicious .EXEs

Protect against this attack, even as it propagated to many thousands of websites



May 7, 2010

McAfee detects anomalous web activity; predictively adjusts web reputation

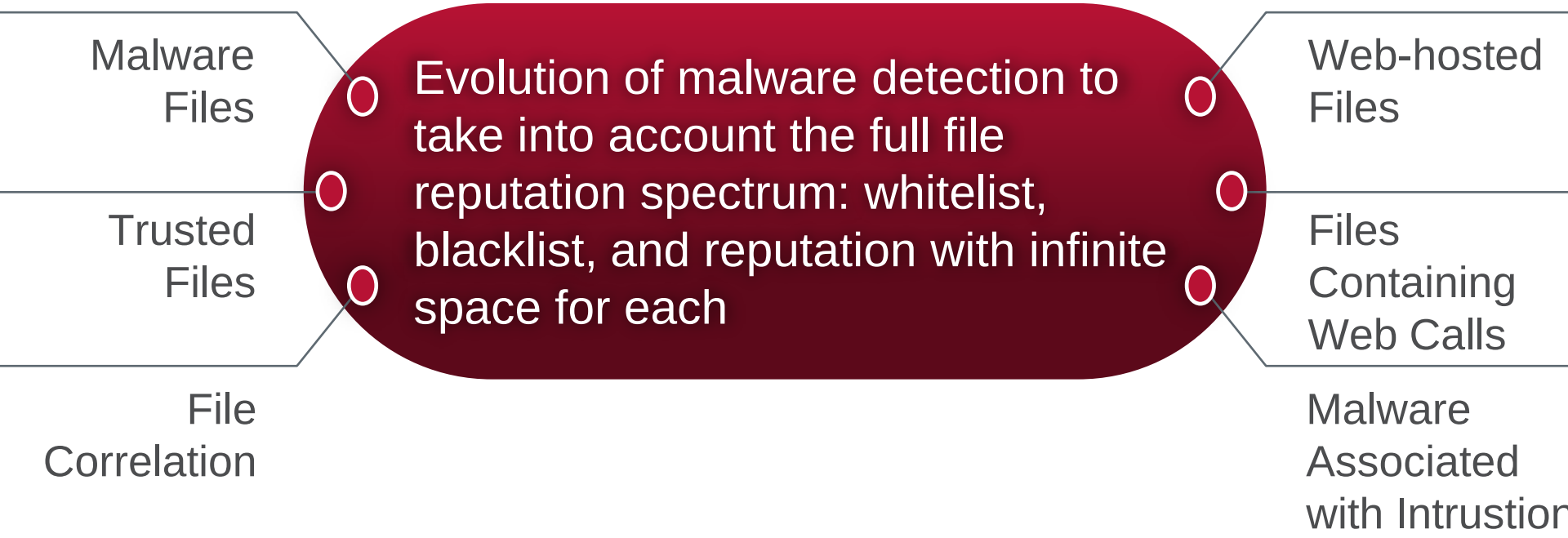
June 7, 2010

McAfee systems pick up massive iFrame injection attack; protect against attack

June 9, 2010

The media report iFrame injection attack on more than 100,000 websites hosted on IIS servers using ASP.net

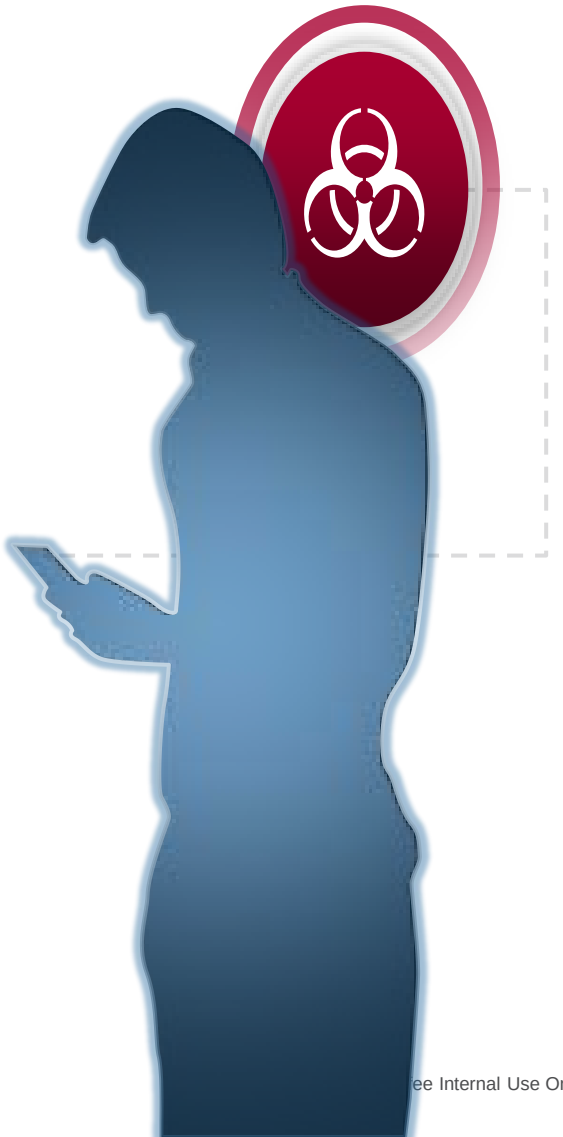
File Reputation



TWO LEVELS OF DETECTION

1

You are INFECTED
and don't know it.



TWO LEVELS OF DETECTION

2

You are INFECTED and don't know it.

Adding a Third Level of Detection

3

You are INFECTED
and don't know it…
but we DO.

Other Protections available (soon)

- Application Control / Whitelisting
  - Most secure defense against malware, even targeted attacks
  - Still scaling issues
    - Moves from dedicated devices to servers nowadays
- Advanced Behaviour Based Detection
  - Still on the horizon, gains importance with predictive detection
  - „Can you tell the difference between VNC and Netbus based on behaviour?“
- Network Based Detection of Irregular Traffic
- Cheap Trick: Mine your DNS Server for Treasure

Questions? More Info?

- Read the McAfee Labs Security Blog
  - http://www.avertlabs.com/research/blog
- Listen to the AudioParasitics Podcast
  - http://www.audioparasitics.com
- Read the Monthly Spam Report
  - http://www.mcafee.com
- Read the McAfee Quarterly Threat Report
  - http://www.mcafee.com
- Read the McAfee Security Journal
  - http://www.mcafee.com
- Watch the Stop H*Commerce Series
  - http://www.stophcommerce.com


McAfee®