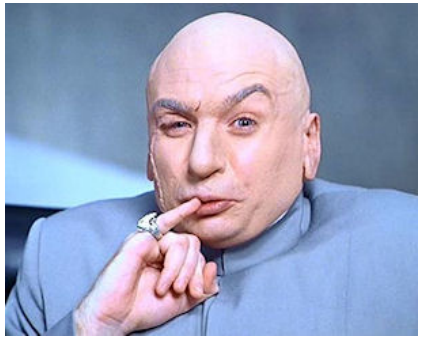
In the Cloud Security

Greg Day
Principal Security Analyst EMEA
AVERT member
July 28, 2009

The Tsunami



- Decades of threats, surely we have a handle on this?

- Estimated in excess $1trillion loss through Cybercrime and data loss in 2008

  McAfee Unsecured Economies Report 2009

- Q1 2009 - 12 million new IP's zombied since January! 50 percent increase since 2008

  McAfee Quarterly threat Report Q1 2009

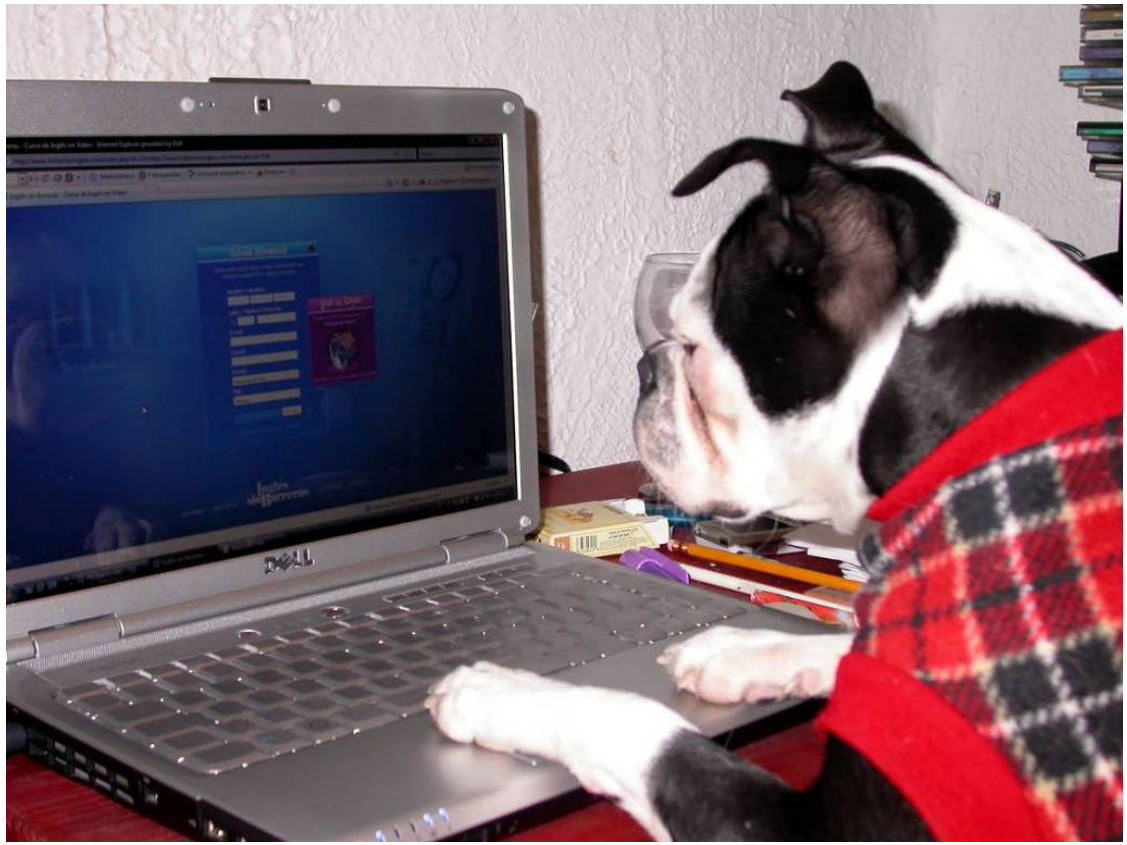
- Koobface - more than 800 new variants in March 09!

  McAfee Quarterly threat Report Q1 2009

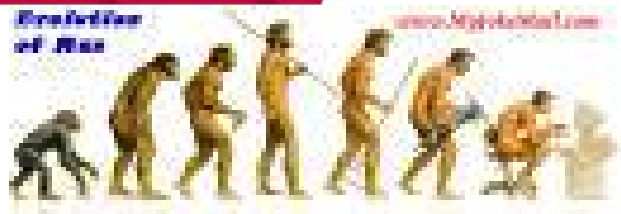
Understand the motivation, to understand the methodology

Source: Chat Interview with the Dream Coders Team, the developers of MPack
http://www.robertlemos.com/2007/07/23/mpack-interview-chat-sessions-posted/

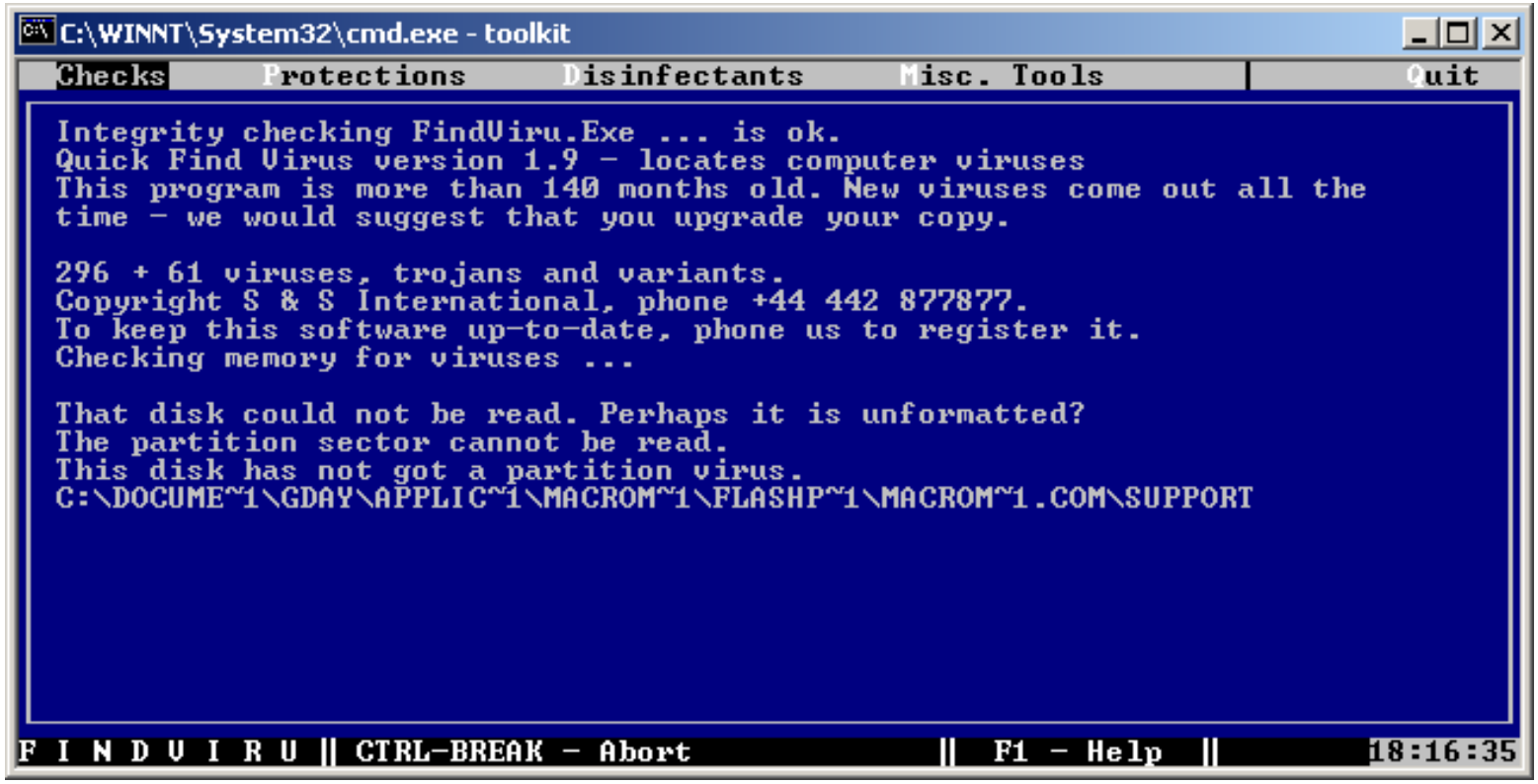
Today anyone can be a cyber criminal!



Over 20 years of Anti-Virus

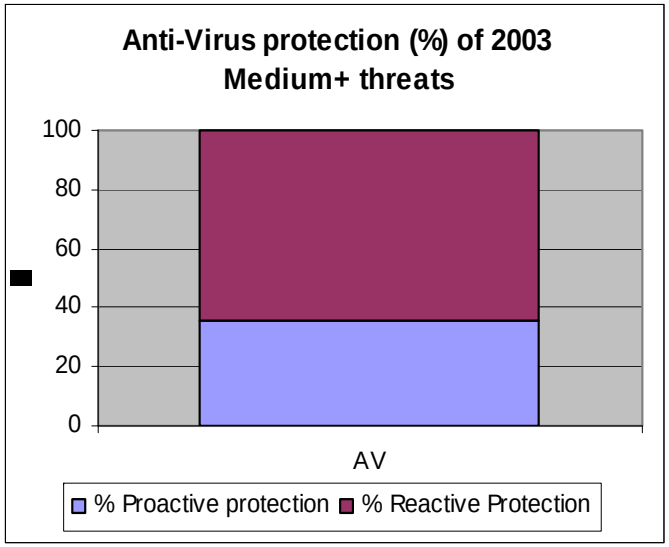


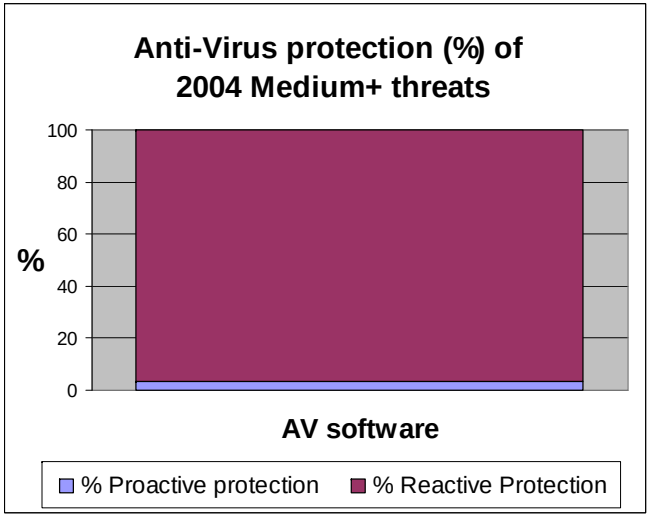
- Dr Solomon's Anti-virus from 1990



- Looking for string match against known malware

The age old question - Is anti-virus dying?





- 1991 : Michelangelo : 6 months ?
- 1997 : WM/Cap : 2 months ?
- 1999 : WM/Melissa : 1 Day ?
- 2000 : VBS/Loveletter : 4 hours ?
- 2001 : CodeRed/Nimda : 1 hour ?
- 2003 : Slammer : 3 mins ?
- 2008 : Mass Web compromises : secs ?

From Elephant to Chameleon
How threats have changed

Evolution of threats

McAfee

Method

2001 – CodeRed & Nimda (u[illegible]se security vulnerabilities)

2002 – Klez & [illegible] (Droppers)

2003 – Slamm[illegible]peed), Slapper (Unix, directed attack)

Speed

Volume

Early proactive techniques

Heuristics (behavioural analysis)

- Positive & Negative analysis
- Protection against new file and/or macro viruses
- Checks for virus like characteristics
- Block execution of possible virus code (OAS)
- No cleaning as no exact match
- Tangible sample to send to virus lab

Speed…

The blended/zero day attack, bought the new solutions

McAfee

Sniffer - Local, Ethernet (Line speed at 10 Mbps) - [Snif2: Decode, 275/5833 Ethernet Frames]

File Monitor Capture Display Tools Database Window Help

Default

No.	Source Address	Dest Address	Summary	Len (Bytes)	Rel. Time
264	0010A4EBD7A6	Broadcast	ARP: C PA=[10.1.1.10]BART PRO=IP	60	0:00:00.56
265	Bart	0010A4EBD7A6	ARP: R PA=[10.1.1.10]BART HA=Bart PRO=IP	60	0:00:00.56
266	HOMER	BART	ICMP: Echo	106	0:00:00.56
267	BART	HOMER	ICMP: Echo reply	106	0:00:00.56
268	HOMER	BART	TCP: D=135 S=1462 SYN SEQ=3480113163 LEN=0 WIN=16384	62	0:00:00.56
269	BART	HOMER	TCP: D=1462 S=135 SYN ACK=3480113164 SEQ=1052707216 LEN=0 WI	62	0:00:00.56
270	HOMER	BART	TCP: D=135 S=1462 ACK=1052707217 WIN=17520	60	0:00:00.56
271	HOMER	BART	MS/DCE: RPC(V5.0) Bind	126	0:00:00.56
272	0010A4EBD7A6	Broadcast	ARP: C PA=[10.1.1.11] PRO=IP	60	0:00:00.56
273	0010A4EBD7A6	Broadcast	ARP: C PA=[10.1.1.12] PRO=IP	60	0:00:00.56
274	BART	HOMER	MS/DCE: RPC(V5.0) Bind Ack	114	0:00:00.57
275	HOMER	BART	MS/DCE: RPC(V5.0) Request	1514	0:00:00.57
276	HOMER	BART	MS/DCE: RPC Continuation of frame 275; 244 Bytes of data	298	0:00:00.57
277	0010A4EBD7A6	Broadcast	ARP: C PA=[10.1.1.13] PRO=IP	60	0:00:00.57
278	BART	HOMER	TCP: D=1462 S=135 ACK=3480114940 WIN=17520	60	0:00:00.57
279	0010A4EBD7A6	Broadcast	ARP: C PA=[10.1.1.14] PRO=IP	60	0:00:00.57
280	0010A4EBD7A6	Broadcast	ARP: C PA=[10.1.1.15] PRO=IP	60	0:00:00.57
281	0010A4EBD7A6	Broadcast	ARP: C PA=[10.1.1.16] PRO=IP	60	0:00:00.57
282	0010A4EBD7A6	Broadcast	ARP: C PA=[10.1.1.17] PRO=IP	60	0:00:00.57
283	0010A4EBD7A6	Broadcast	ARP: C PA=[10.1.1.18] PRO=IP	60	0:00:00.58
284	0010A4EBD7A6	Broadcast	ARP: C PA=[10.1.1.19] PRO=IP	60	0:00:00.58
285	0010A4EBD7A6	Broadcast	ARP: C PA=[10.1.1.20] PRO=IP	60	0:00:00.58
286	0010A4EBD7A6	Broadcast	ARP: C PA=[10.1.1.21] PRO=IP	60	0:00:00.58
287	0010A4EBD7A6	Broadcast	ARP: C PA=[10.1.1.22] PRO=IP	60	0:00:00.59
288	0010A4EBD7A6	Broadcast	ARP: C PA=[10.1.1.23] PRO=IP	60	0:00:00.59
289	0010A4EBD7A6	Broadcast	ARP: C PA=[10.1.1.24] PRO=IP	60	0:00:00.59
290	0010A4EBD7A6	Broadcast	ARP: C PA=[10.1.1.25] PRO=IP	60	0:00:00.59
291	0010A4EBD7A6	Broadcast	ARP: C PA=[10.1.1.26] PRO=IP	60	0:00:00.60
292	0010A4EBD7A6	Broadcast	ARP: C PA=[10.1.1.27] PRO=IP	60	0:00:00.60
293	0010A4EBD7A6	Broadcast	ARP: C PA=[10.1.1.28] PRO=IP	60	0:00:00.60
294	0010A4EBD7A6	Broadcast	ARP: C PA=[10.1.1.29] PRO=IP	60	0:00:00.60
295	0010A4EBD7A6	Broadcast	ARP: C PA=[10.1.1.30] PRO=IP	60	0:00:00.60

```
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP:       000. ....    = routine
```

Sniffer - Local, Ethernet (Line speed at 10 Mbps) - [Snif2: Decode, 275/5833 Ethernet Frames]

File Monitor Capture Display Tools Database Window Help

No.	Source Address	Dest Address	Summary	Len (Bytes)	Rel. Time	Delta T
264	0010A4EBD7A6	Broadcast	ARP: C PA=[10.1.1.10]BART PRO=IP	60	0:00:00.565	0.0
265	Bart	0010A4EBD7A6	ARP: R PA=[10.1.1.10]BART HA=Bart PRO=IP	60	0:00:00.566	0.0
266	HOMER	BART	ICMP: Echo	106	0:00:00.566	0.0
267	BART	HOMER	ICMP: Echo reply	106	0:00:00.566	0.0
268	HOMER	BART	TCP: D=135 S=1462 SYN SEQ=3480113163 LEN=0 WIN=16384	62	0:00:00.567	0.0
269	BART	HOMER	TCP: D=1462 S=135 SYN ACK=3480113164 SEQ=1052707216 LEN=0 WI	62	0:00:00.567	0.0
270	HOMER	BART	TCP: D=135 S=1462 ACK=1052707217 WIN=17520	60	0:00:00.567	0.0
271	HOMER	BART	MS/DCE: RPC(V5.0) Bind	126	0:00:00.567	0.0
272	0010A4EBD7A6	Broadcast	ARP: C PA=[10.1.1.11]PRO=IP	60	0:00:00.568	0.0

```
MS/DCE RPC: Call ID                          = 229
MS/DCE RPC: Allocation Hint                  = 0x00000690
MS/DCE RPC: Presentation Context Identifier  = 0x0001
MS/DCE RPC: Operation Number                 = 4
MS/DCE RPC: [ 1436 bytes Stub Data ]
MS/DCE RPC:
```

```
00000380: 00 00 0e 00 ff ff 68 8b 0b 00 02 00 00 00 00 00  ....ÿÿh▌........
00000390: 00 00 00 00 00 00 86 01 00 00 00 00 00 00 86 01  ......▌.......▌.
000003a0: 00 00 5c 00 5c 00 46 00 58 00 4e 00 42 00 46 00  ..\.\.F.X.N.B.F.
000003b0: 58 00 46 00 58 00 4e 00 42 00 46 00 58 00 46 00  X.F.X.N.B.F.X.F.
000003c0: 58 00 46 00 58 00 46 00 58 00 9d 13 00 01 cc e0  X.F.X.F.X.▐...Ìà
000003d0: fd 7f cc e0 fd 7f 90 90 90 90 90 90 90 90 90 90  ý▐Ìàý▐▐▐▐▐▐▐▐▐▐▐▐
000003e0: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ▐▐▐▐▐▐▐▐▐▐▐▐▐▐▐▐
000003f0: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ▐▐▐▐▐▐▐▐▐▐▐▐▐▐▐▐
00000400: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ▐▐▐▐▐▐▐▐▐▐▐▐▐▐▐▐
00000410: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ▐▐▐▐▐▐▐▐▐▐▐▐▐▐▐▐
00000420: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ▐▐▐▐▐▐▐▐▐▐▐▐▐▐▐▐
00000430: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ▐▐▐▐▐▐▐▐▐▐▐▐▐▐▐▐
00000440: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ▐▐▐▐▐▐▐▐▐▐▐▐▐▐▐▐
00000450: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ▐▐▐▐▐▐▐▐▐▐▐▐▐▐▐▐
00000460: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ▐▐▐▐▐▐▐▐▐▐▐▐▐▐▐▐
00000470: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ▐▐▐▐▐▐▐▐▐▐▐▐▐▐▐▐
00000480: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ▐▐▐▐▐▐▐▐▐▐▐▐▐▐▐▐
00000490: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ▐▐▐▐▐▐▐▐▐▐▐▐▐▐▐▐
000004a0: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ▐▐▐▐▐▐▐▐▐▐▐▐▐▐▐▐
000004b0: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ▐▐▐▐▐▐▐▐▐▐▐▐▐▐▐▐
000004c0: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ▐▐▐▐▐▐▐▐▐▐▐▐▐▐▐▐
000004d0: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ▐▐▐▐▐▐▐▐▐▐▐▐▐▐▐▐
000004e0: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ▐▐▐▐▐▐▐▐▐▐▐▐▐▐▐▐
000004f0: 90 90 90 90 90 90 90 90 90 90 90 90 eb 10 5a 4a  ▐▐▐▐▐▐▐▐▐▐▐▐ë.ZJ
00000500: 33 c9 66 b9 76 01 80 34 0a 99 e2 fa eb 05 e8 eb  3Éf¹v.▌4.▌âúë.èë
00000510: ff ff ff 70 61 99 99 99 c3 21 95 69 64 e6 12 99  ÿÿÿpa▌▌▌Ã!▌idæ.▌
00000520: 12 e9 85 34 12 d9 91 12 41 12 ea a5 9a 6a 12 ef  .é▌4.Ù´.A.ê¥▌j.ï
00000530: e1 9a 6a 12 e7 b9 9a 62 12 d7 8d aa 74 cf ce c8  á▌j.ç¹▌b.×▌ªtÏÎÈ
00000540: 12 a6 9a 62 12 6b f3 97 c0 6a 3f ed 91 c0 c6 1a  .¦▌b.kó▌Àj?í´ÀÆ.
00000550: 5a 9d de 7b 70 c0 c6 c7 12 54 12 df bd 9a 5a 48  Z▐Ü{pÀÆÇ.T.ß¼▌ZH
```

Decode | Matrix | Host Table | Protocol Dist. | Statistics

For Help, press F1

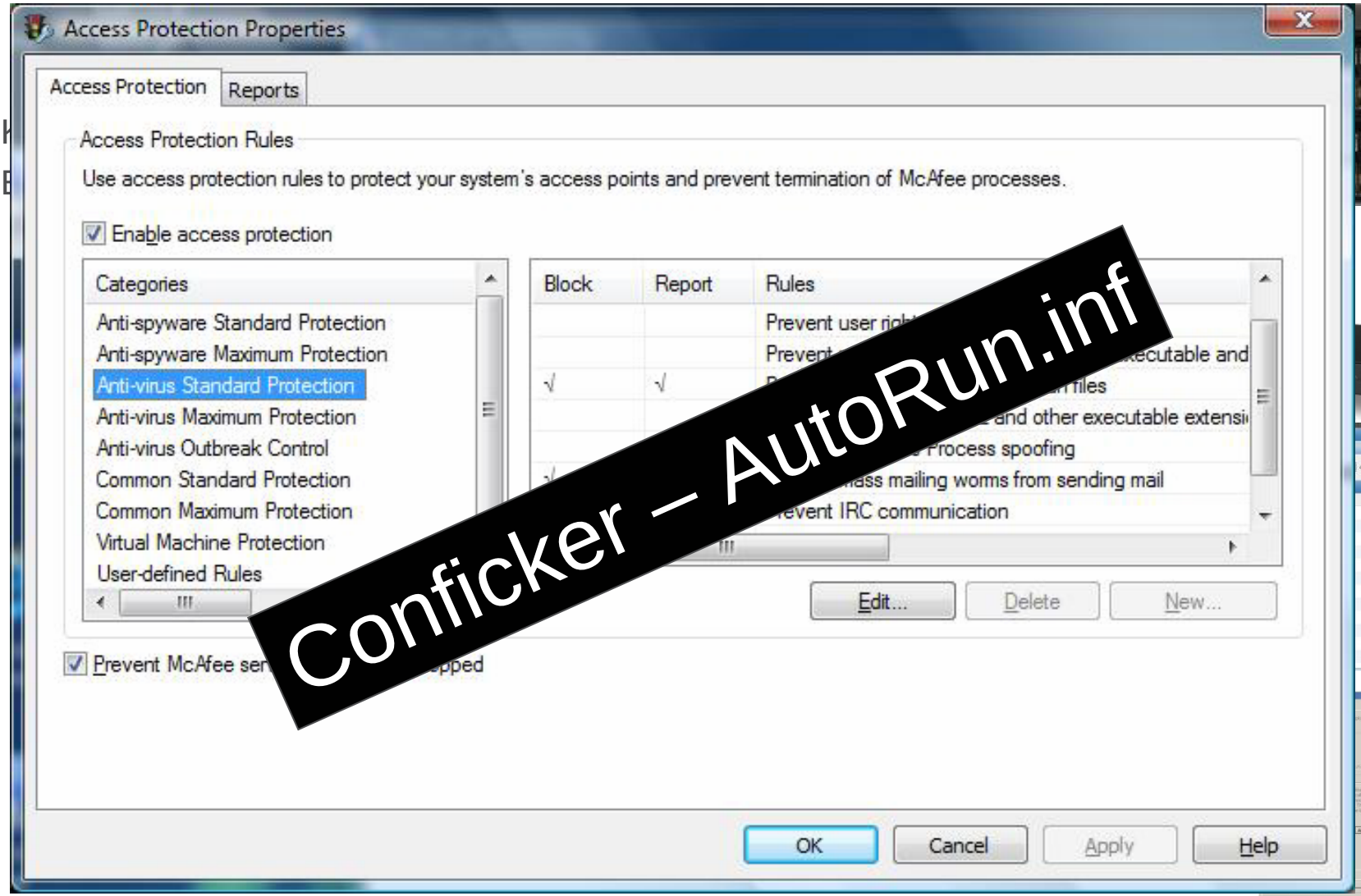
You can see the RPC data is packed with repetitive no operation (NOP) data to exceed the buffer limit, which causes the overflow.
This known vulnerability allows arbitrary code be to run with local system privileges.

Click in this box to continue

Proactive behavioural protection (HIPS, NIPS, FW, Whitelisting etc…)

McAfee

- K
- E



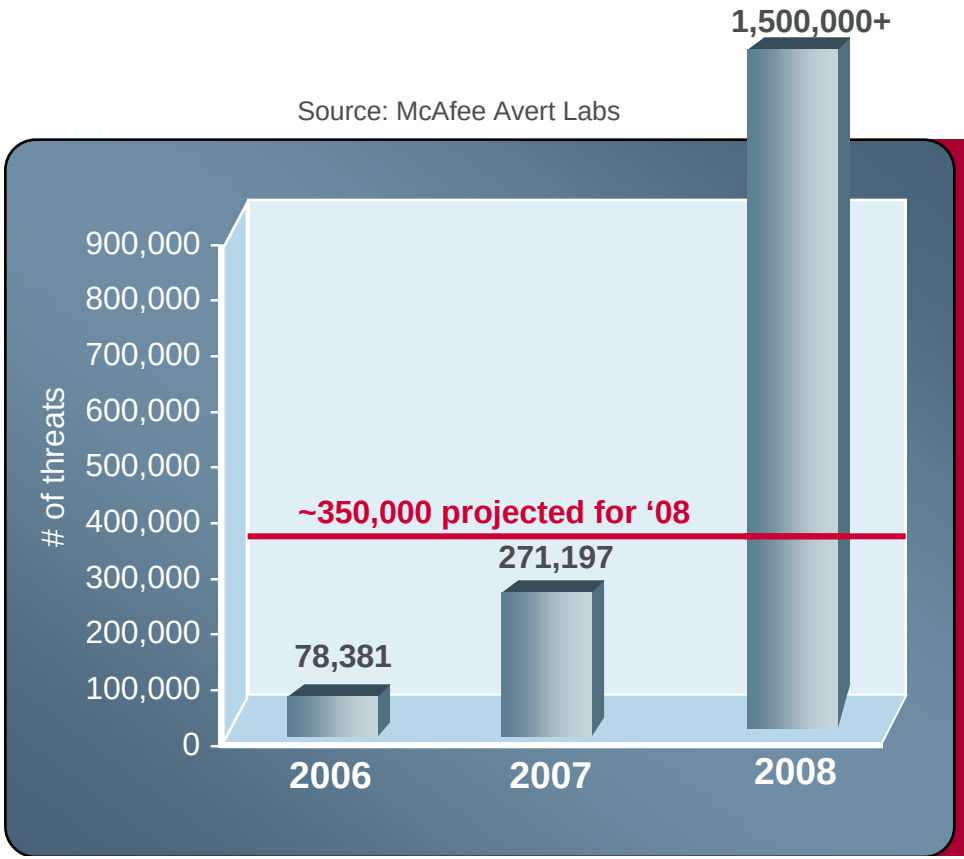
Proactive Behavioural Controls - limitations

- What did I really stop?
- Did it stop all of the attack?
- What else could it have done?

- We still want to identify the threat
- We sometimes need to clean up

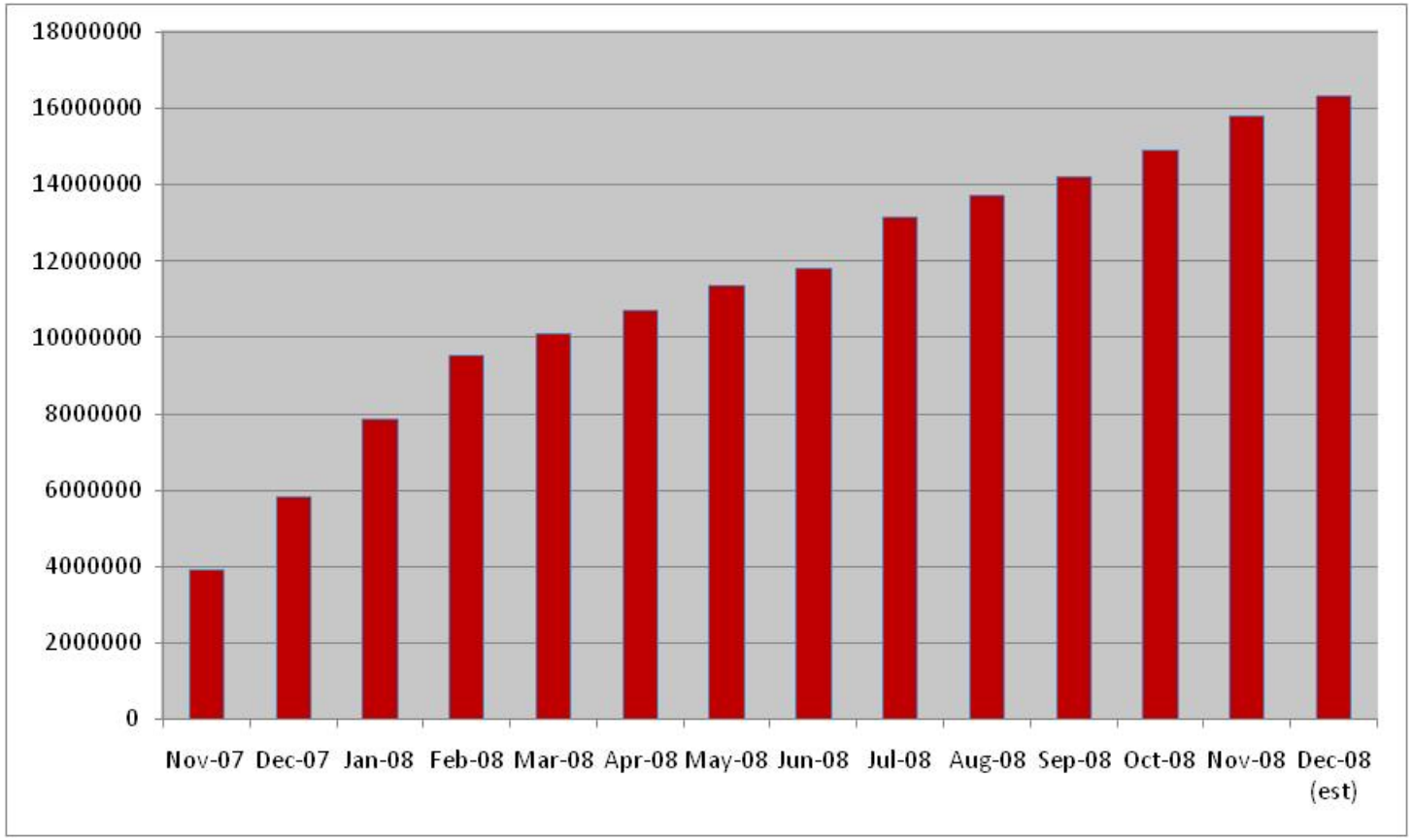
- Assumes clean at point of install

Volume…



- 246% growth from 2006 to 2007
- 400%+ growth projected for 2008
- 2008 exceed projections

The Great Zoo: McAfee Known Malware Samples



Count of dirty samples/hashes in the McAfee zoo

Shark – Compliable multi system back door Trojan
Now anyone can be a cyber criminal!

u have!

ntrol!

he keylogger

al processes
ted systems
me!

Buy the deployment tools

McAfee

orum/index.php?s=f20642e07e39acb14b6d0b6c880538dd&showtopic=5640&st=0&p=40031&#entry40031

We are proud to present a browser vulnerability test kit - the **Sploit25** exploit pack.

The pack consists of 5 sploits:

- **IE MDAC** - the everpresent sploit, provides the main infection of old IE 6
- **IE Snapshot** - a unique script, infects IE 6 and 7
- **FF Embed** - an exploit for ancient FireFoxes
- **PDF** - the famous private Acrobat Reader sploit
- **PDF vis** - in our pack *two* PDFs cowork and show an all-right infection rate

According the results of tests done by administration, the infection hitrate is *13% to 30%* depending on traffic types and countries. Tests were held using 7 different types of traff from different sellers, the infection rate **averages to 25%**.

Sploit25 contains a comfortable single-file 150 kb installer which creates all the files and prepares the pack for its job. The pack has a nice no-frills design and convenient statistics.

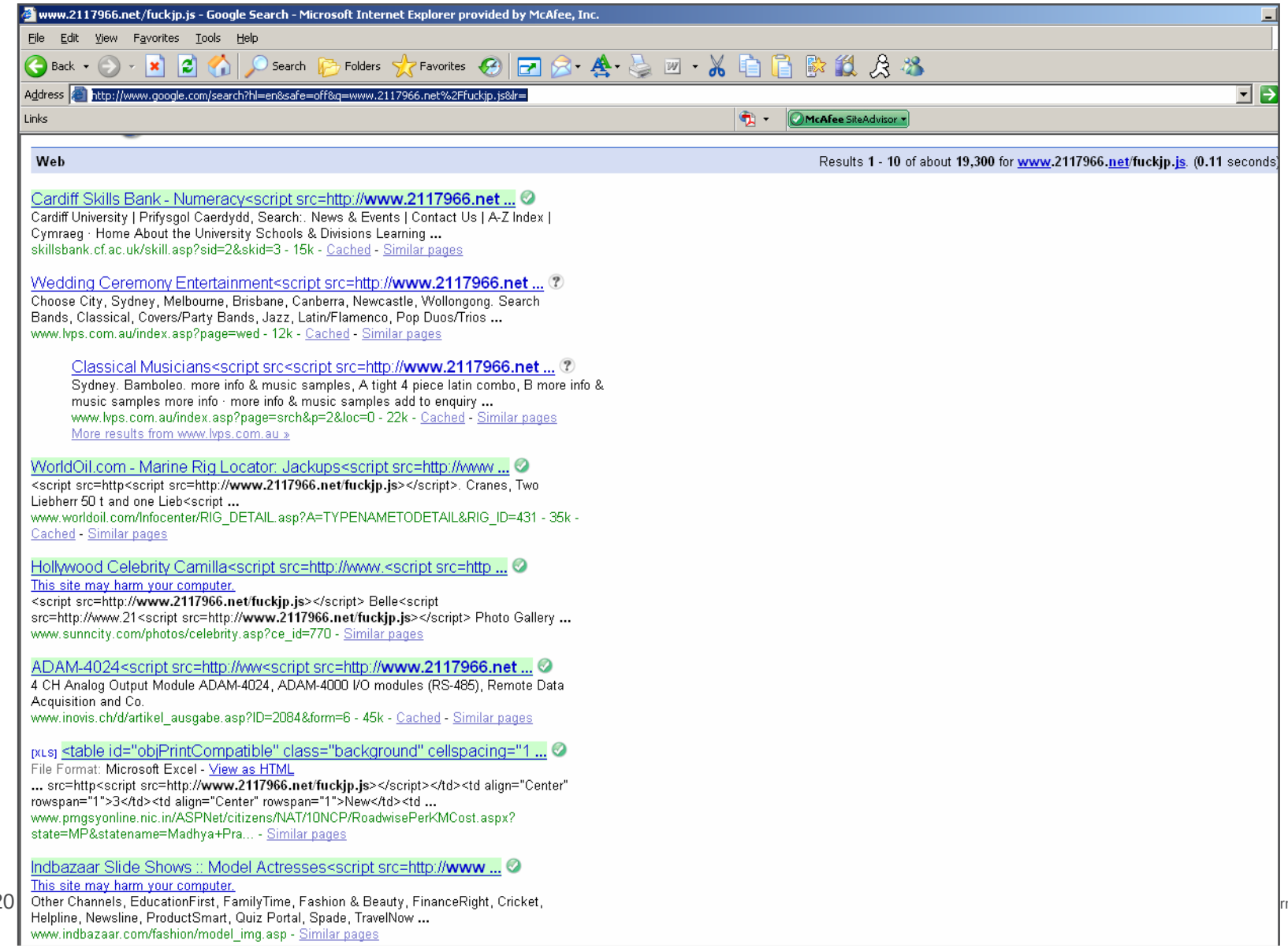
The updates and AV cleans are included in the support. Additionally, you get a discount on significantly new sploits.

The pack is bound to the domain and the IP, all the sploits are bound to an URL. If you try to resell, decode, remove the boundaries, you will lose all the support, updates and guarantees.

Price:
Sploit pack build - 2500 wmz
Rebuild to a new domain - 2000 wmz
Rebuild to a new domain if the old domain is in malware list - 50 wmz
Rebuild to a new subdomain if the old domain is in mallist - free

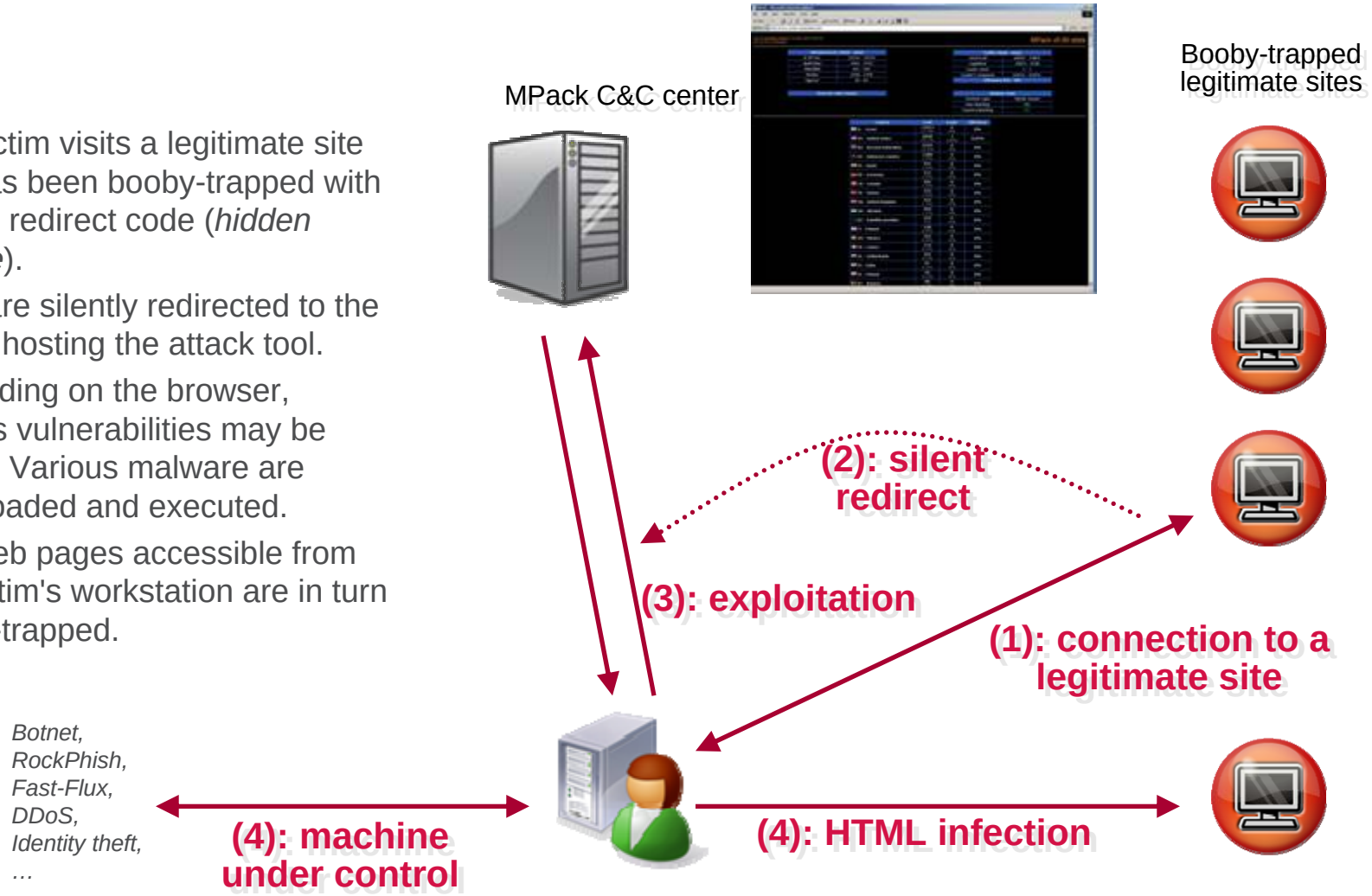
Contacts: icq

Mass infection of public web pages globally (13 March 08)

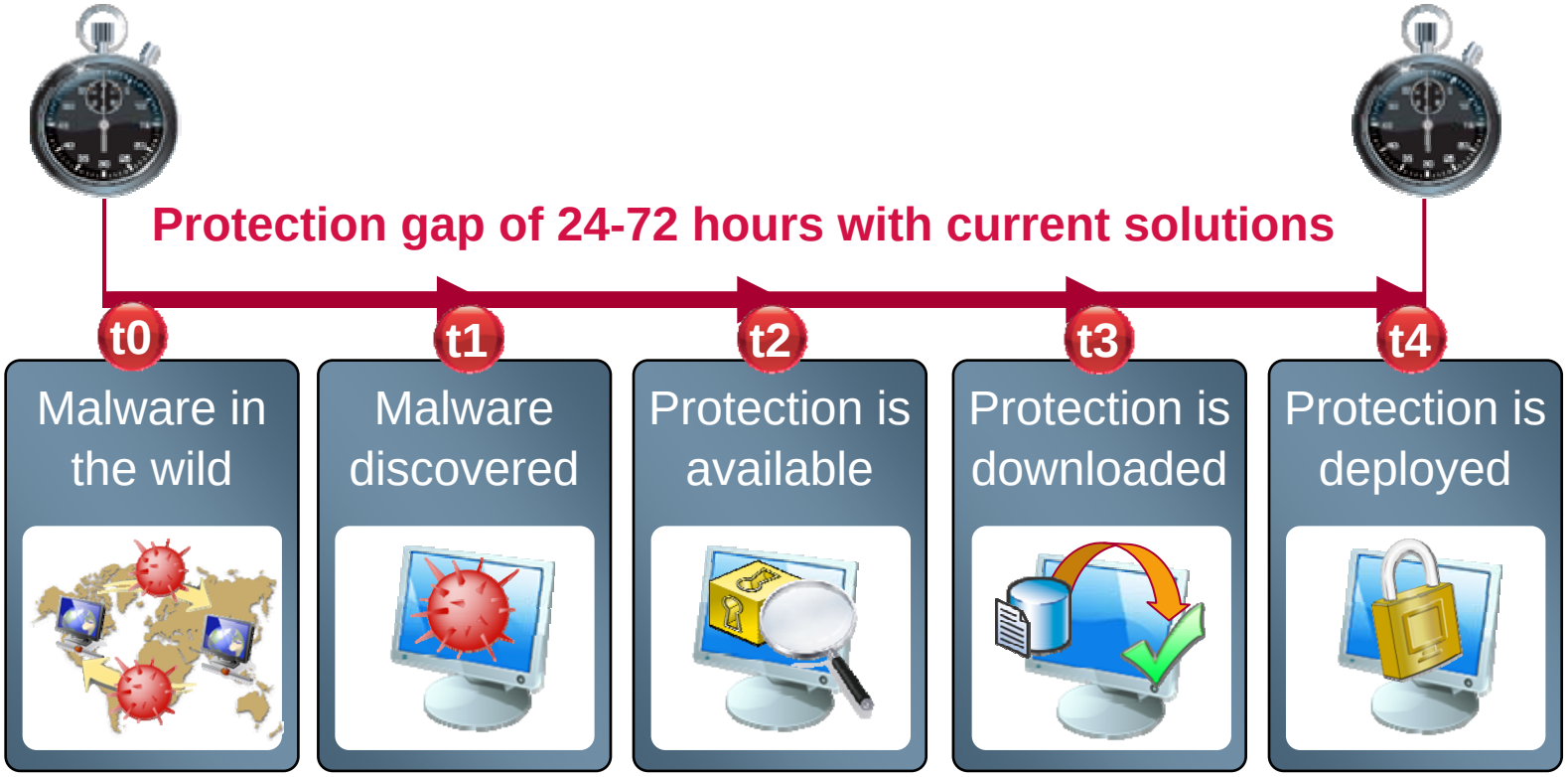


Example: IFrame & MPack

1. The victim visits a legitimate site that has been booby-trapped with hidden redirect code (*hidden iFrame*).
2. They are silently redirected to the server hosting the attack tool.
3. Depending on the browser, various vulnerabilities may be tested. Various malware are downloaded and executed.
4. The web pages accessible from the victim's workstation are in turn booby-trapped.



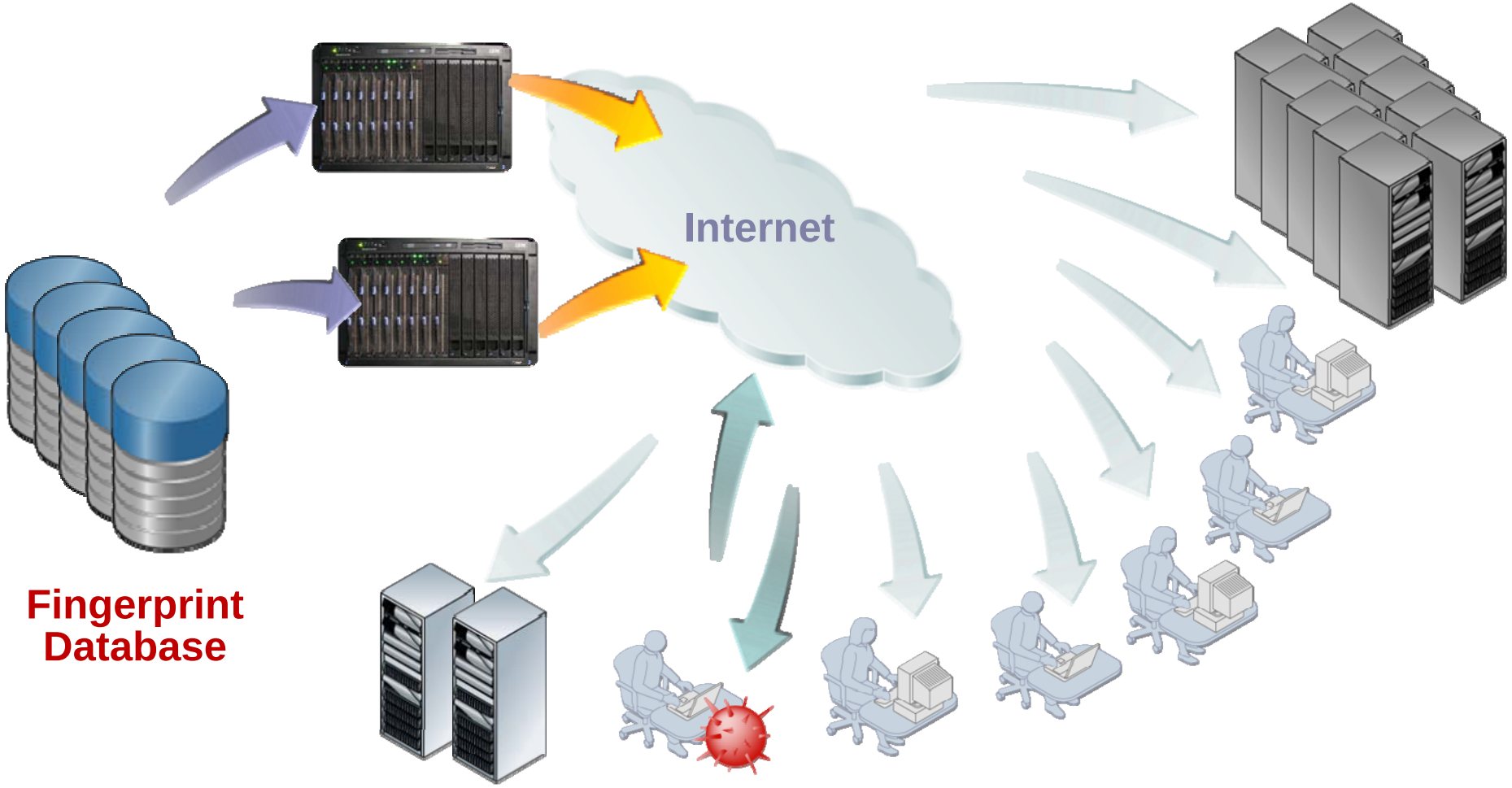
Regular “Protection Gap”



Security in the Cloud

McAfee

Next Gen “In the cloud” detection



What is “in the Cloud scanning”?

End-node reporting

Very little system overhead

Meta-data

In the cloud security - Blocking what we already know!

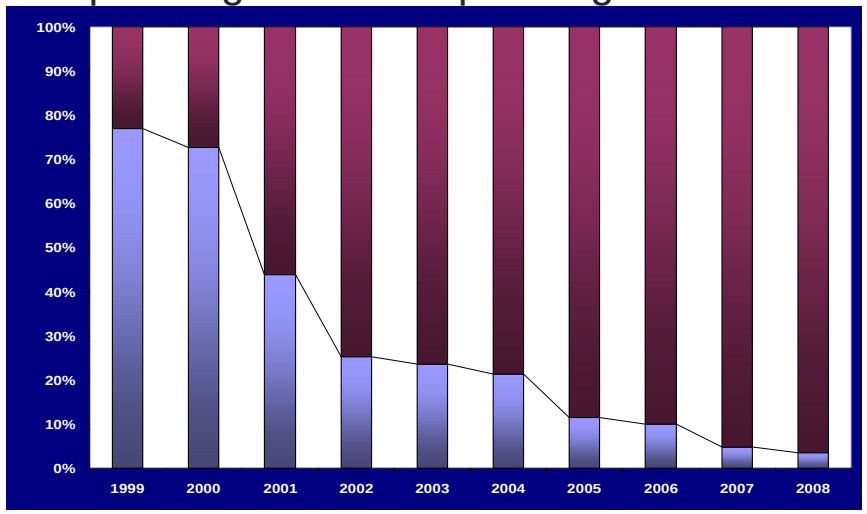
Non-replicating malware is static

And some replicating is static too (e.g. worms)

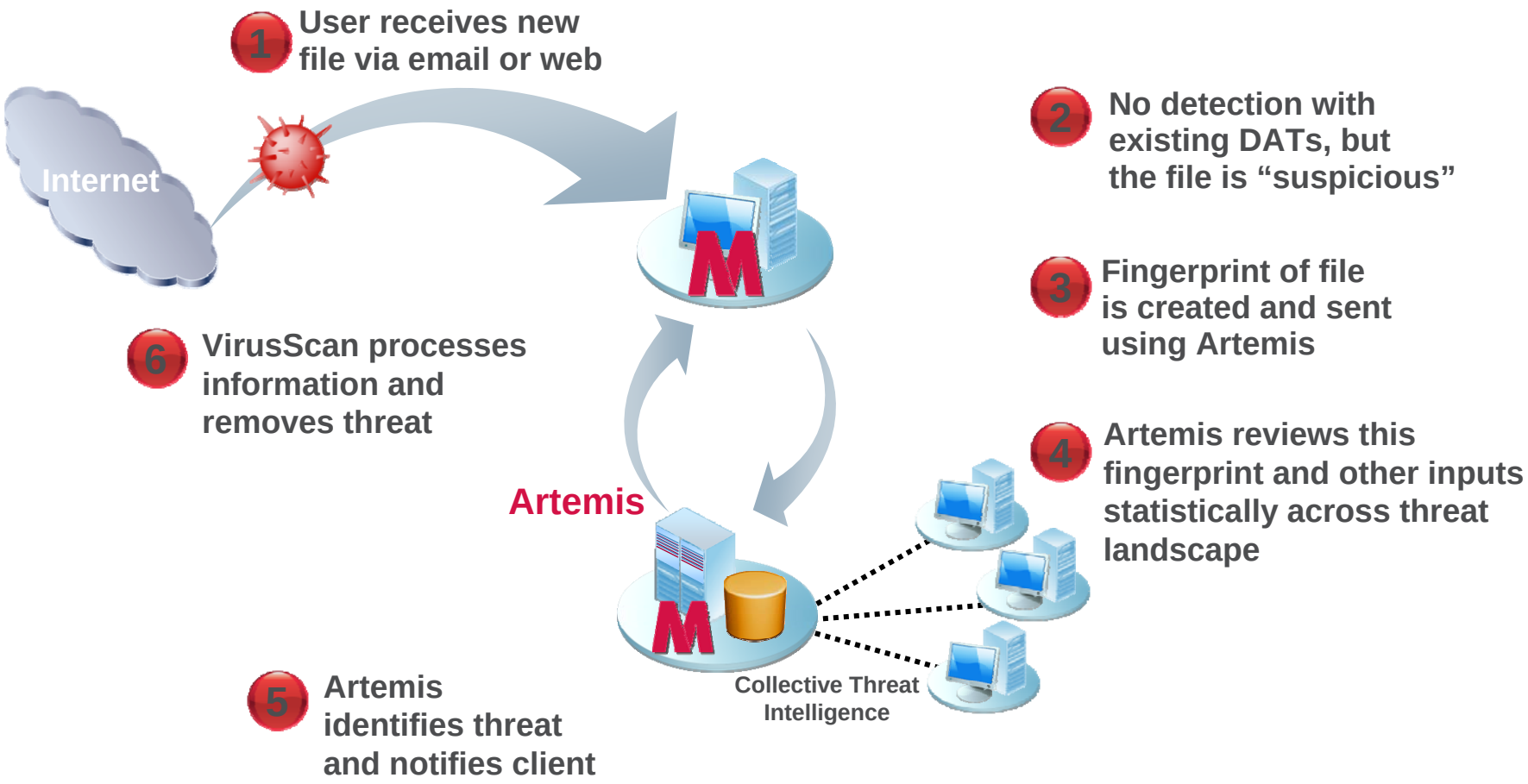
Can be detected with a fingerprint (MD5,SHA-1,SHA-2, etc.)

Black List of fingerprints

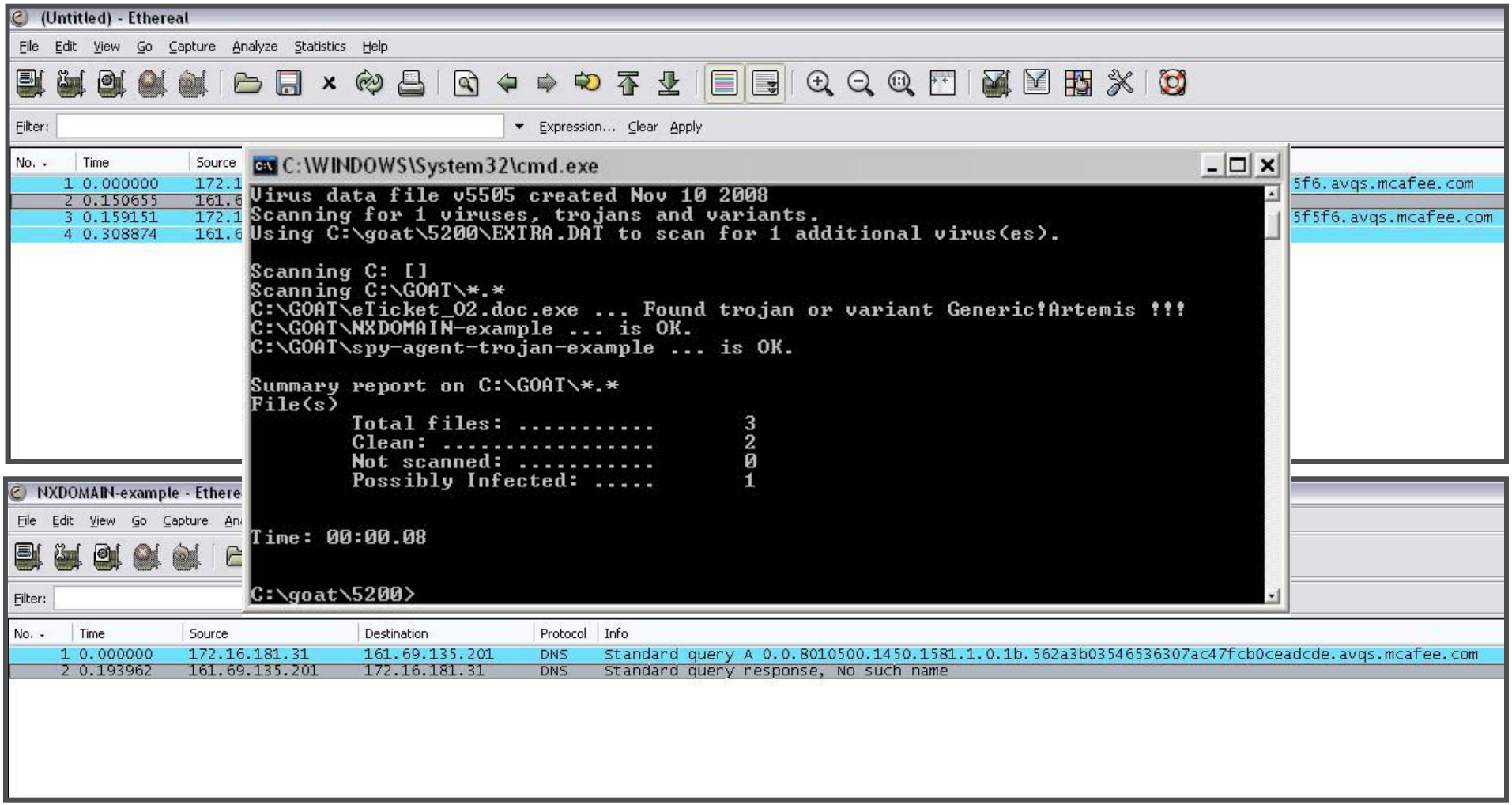
Replicating vs Non-Replicating Malware



How does in the Cloud anti-virus work?



In the Cloud in action



In the cloud security - Identifying what we don't know!

McAfee

Software may be deemed "suspicious" based on
Observed behaviours
Source
Detections by other products

Behaviours, sources, detections can be assigned a weight

Based on the resulting weight, software may be classified as "suspicious" with different degrees of certainty

Closing the loop

McAfee

McAfee
McAfee Avert Workflow (1.2.484)

Dashboard | Malware | Reports | Configuration

Analyst | Researcher | Downloads | Available

4902838	WebImmune	[redacted]	1	1	0		16 Oct 21:38:43	Solved	handled by automation					

Samples — Page 1 of 1 (1 items)

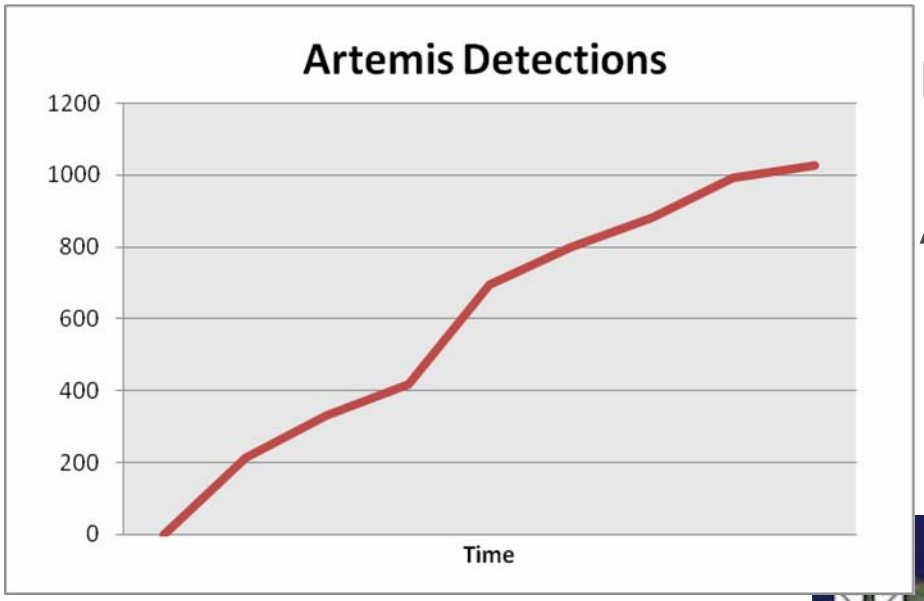
MD5	Filename	Owner	Occurrences	Status	Assignor	Detections
3a14ba03fcd9de0d13bc25886a404889	statement_jan-oct.doc.exe	[redacted]	1-15-15	closed	[redacted]	AI 3/12 .-----MM-N--.- RA 3 MNA SAC spy-agent.bw DET spy-agent.bw

Take Sample | Assign Sample | Unassign Sample | Junk | Resolve | Raiden Update

Page 1 of 1 (1 items)

4902646	Non_Escalated	FW: [SPAM-McAfee]Account data	[redacted]	1	1	0		16 Oct 18:38:11	Solved	handled by automation				
4902602	WebImmune		[redacted]	1	1	0		16 Oct 18:09:06	Solved	handled by automation				
4902586	PO Q_P0	Statement_JAN-OCT.doc.exe	[redacted]	1	1	0		16 Oct 17:55:33	Solved	handled by automation				
4902511	PO Q_P0	sample	[redacted]	1	1	0		16 Oct 17:04:08	Solved	handled by automation				

Malware case study – Spy-Agent.bw



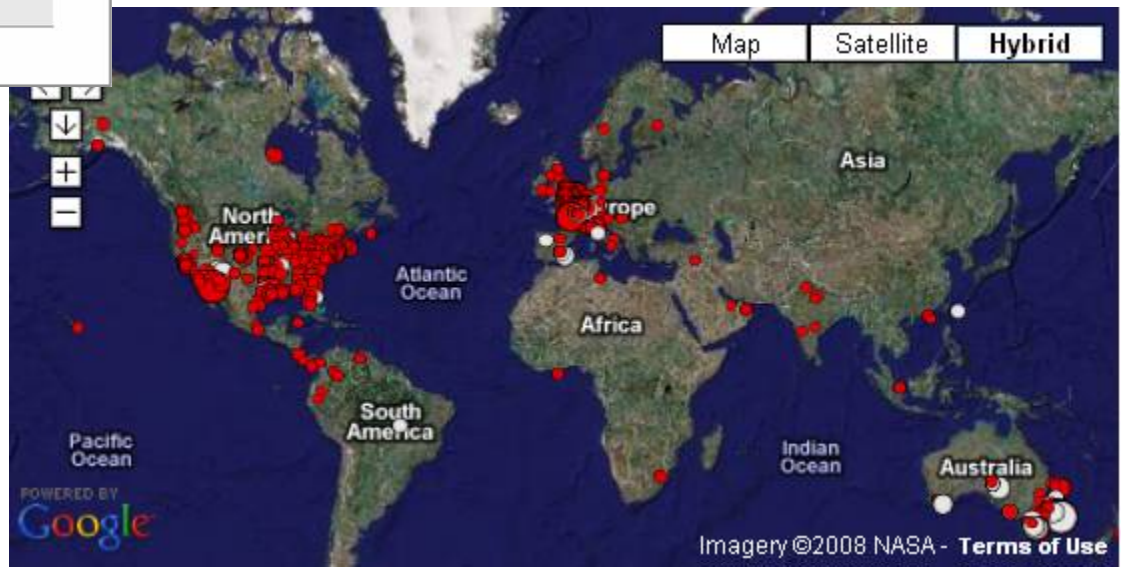
First seen

- 15th October 2008, 22:24:28

Auto-blacklisted

- 15th October 2008, 22:57:01

Artemis clients sent fingerprints ~2 hours before regular submission saw the file



Security & privacy

Example:

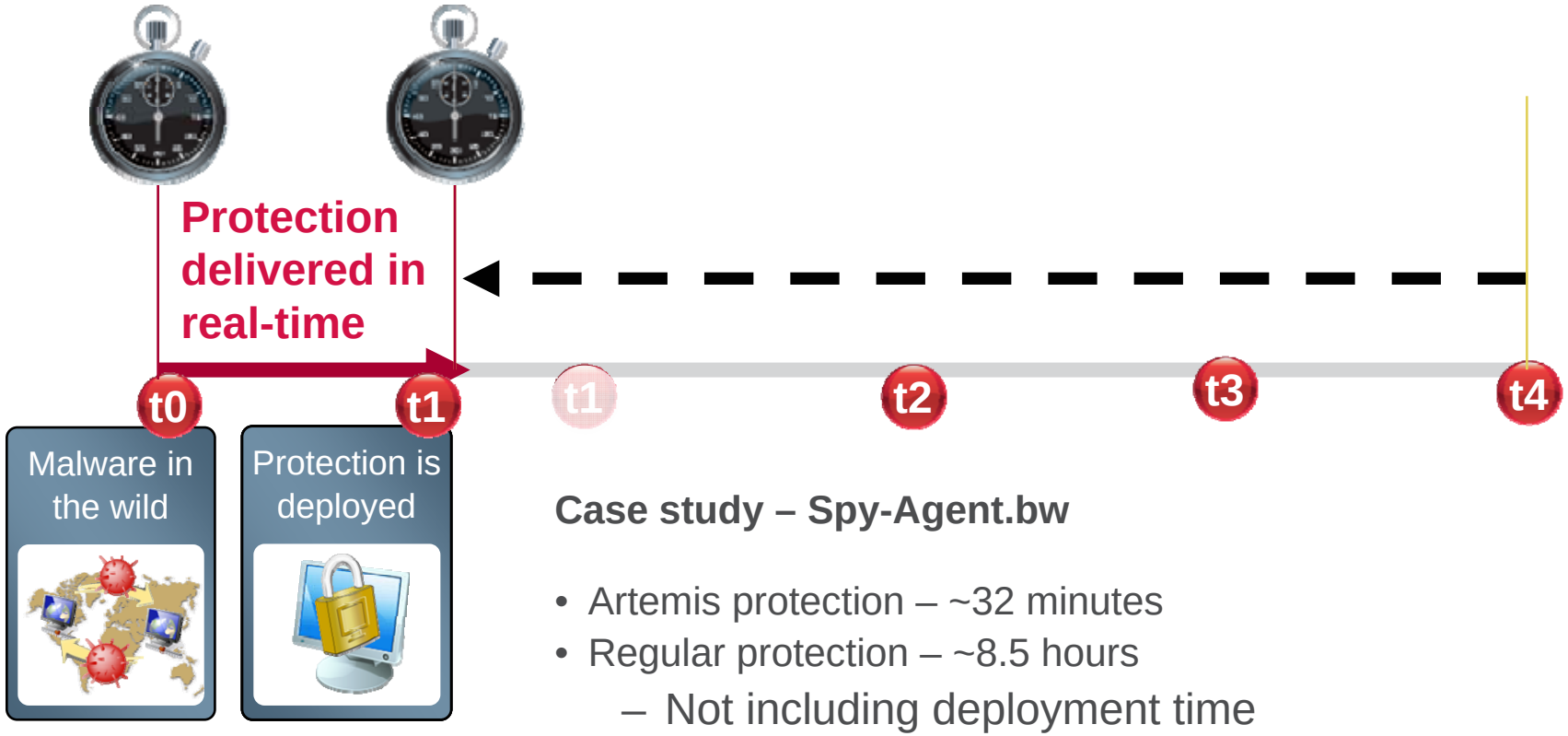
U0B6gKhbtiZCoxyh0IneADS/RShS8iRCBSEvwfjekG/q4yDRg
qEUXjHWKvnrySGa6QMdftrlpl5pAdJvOUAcNcvCjKvpIfsxv8q
Bk4uRQQ60r5StRCXOpiA0Qy3fKmLRUZyNq1EyjLLPKgJDZI
0nqHhRWX+TDgPgXRfW9wD06qE

Cryptographically strong actionable responses

Query specific

Immune to replay attacks

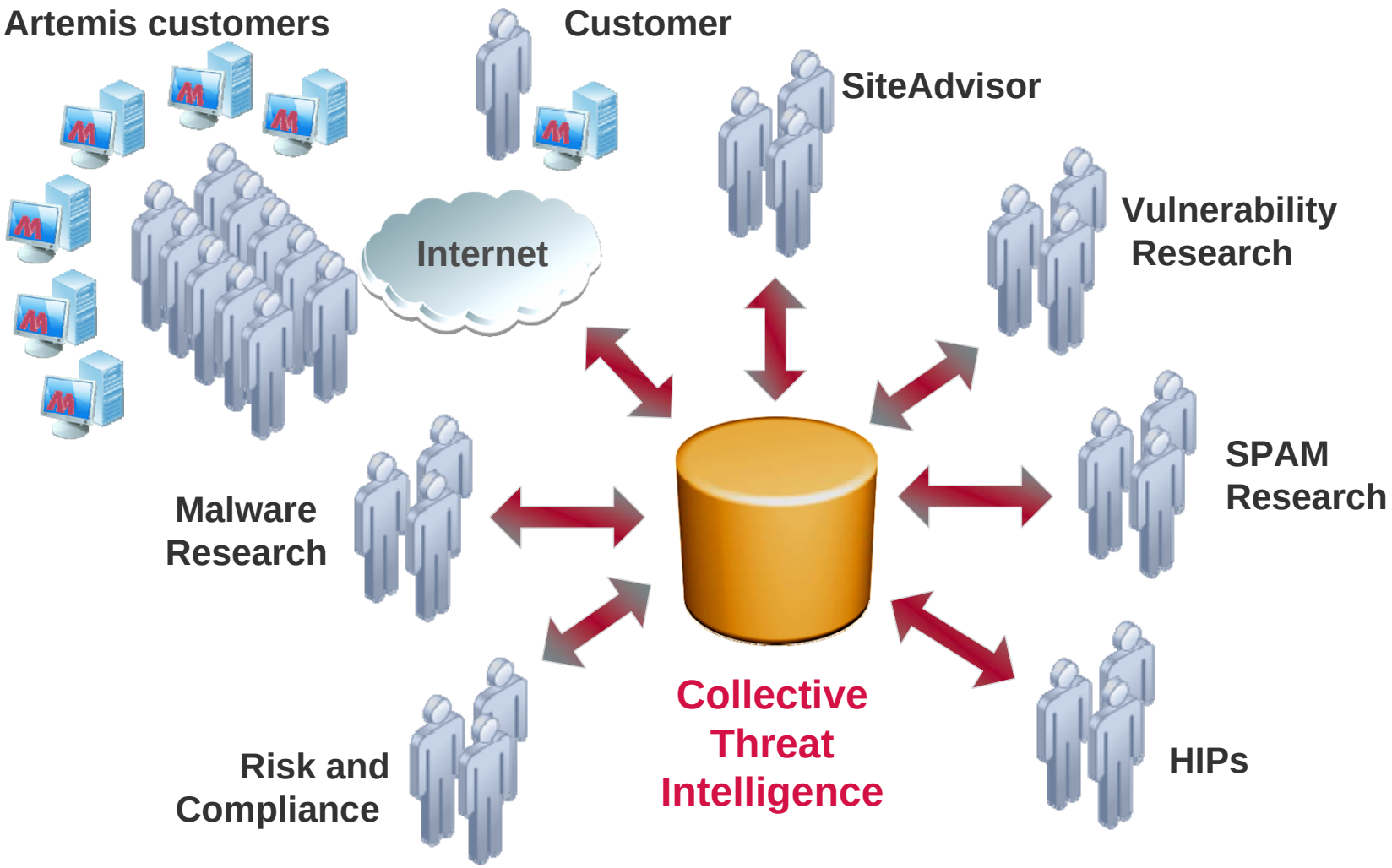
Cloud security compressed “Protection Gap”



Case study – Spy-Agent.bw

- Artemis protection – ~32 minutes
- Regular protection – ~8.5 hours
  - Not including deployment time

I was blind, but now I see



Taking it to the next level

Collaborative Global Intelligence

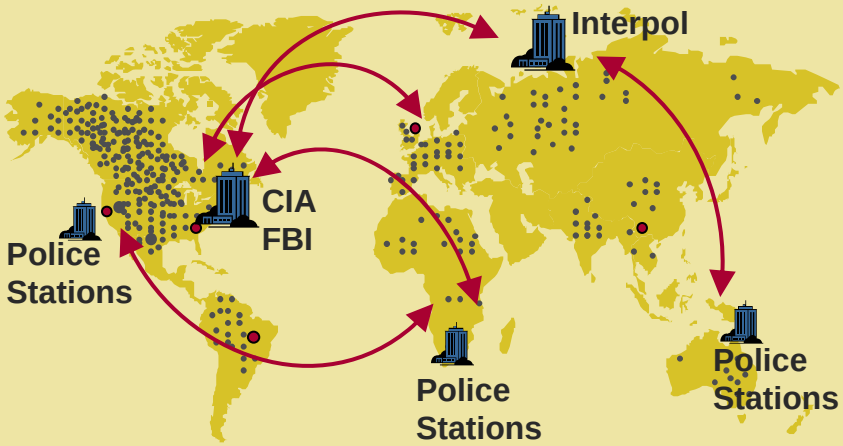
McAfee

Physical World

Intelligence Agents

Deploy agents: Officers around the globe *(MI5, MI6, FBI, CIA, Interpol.)*
Global intelligence system: Share intelligence information. (e.g. criminal history, global finger printing system)

Results
Effective - Accurate detection of offenders
Pro-active - Stop them from coming in the country



Cyber World

Intelligence Probes

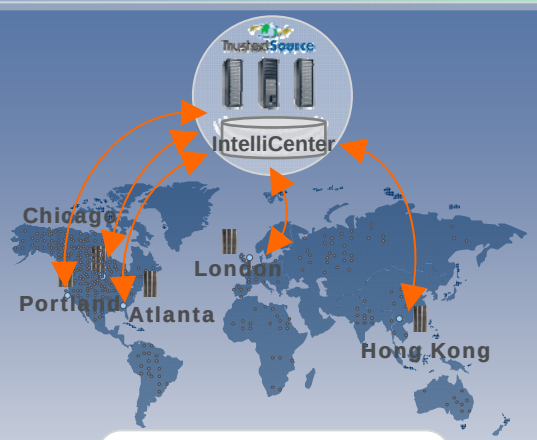
Deploy security probes: Around the globe *(firewall, email gateways, web gateways)*
Global intelligence system: Share cyber communication info.
(e.g.: hackers, spammers, phishers)

Results
Effective - Accurate detection of bad IPs, domains
Pro-active - Deny connection to intruders to your enterprise

Global Intelligence, Local Protection

McAfee

GLOBAL DATA MONITORING



Ownership
- Whois
- Zone files
- Trademark

Content
- Images
- Text
- Links

Behavior
- Social networks
- Persistence
- Longevity

AUTOMATED ANALYSIS

10 Billion Enterprise Messages Analyzed per Month

Dynamic Computation Of Reputation Score

IP | Domain | URL | Image | Message

Bad → Good

REAL-TIME PROTECTION PLATFORMS

Edge / Firewall
- Traffic Shaping
- Attack Blocking

Web Gateways
- Anti-Malware
- Anti-Spoofing

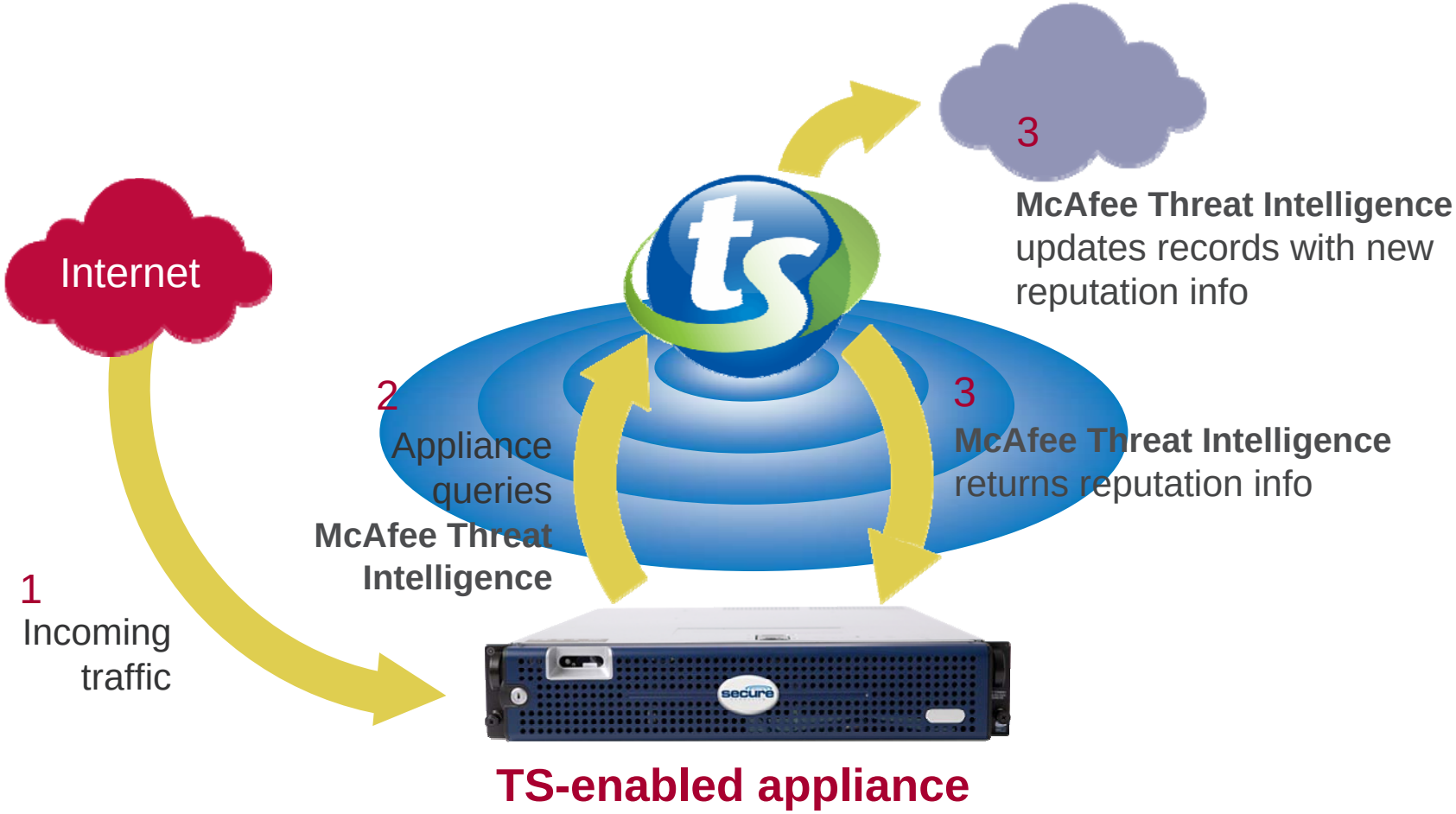
Messaging Gateways
- Outbreak Detection
- Anti-Spam

Identity Fraud Applications
- Anti-Phishing
- Zombie Alerts

Global Data Monitoring is Fueled by the Network Effect of Real-Time Information Sharing from Thousands of Gateway Security Devices around the World

Intelligence: How It All Works….

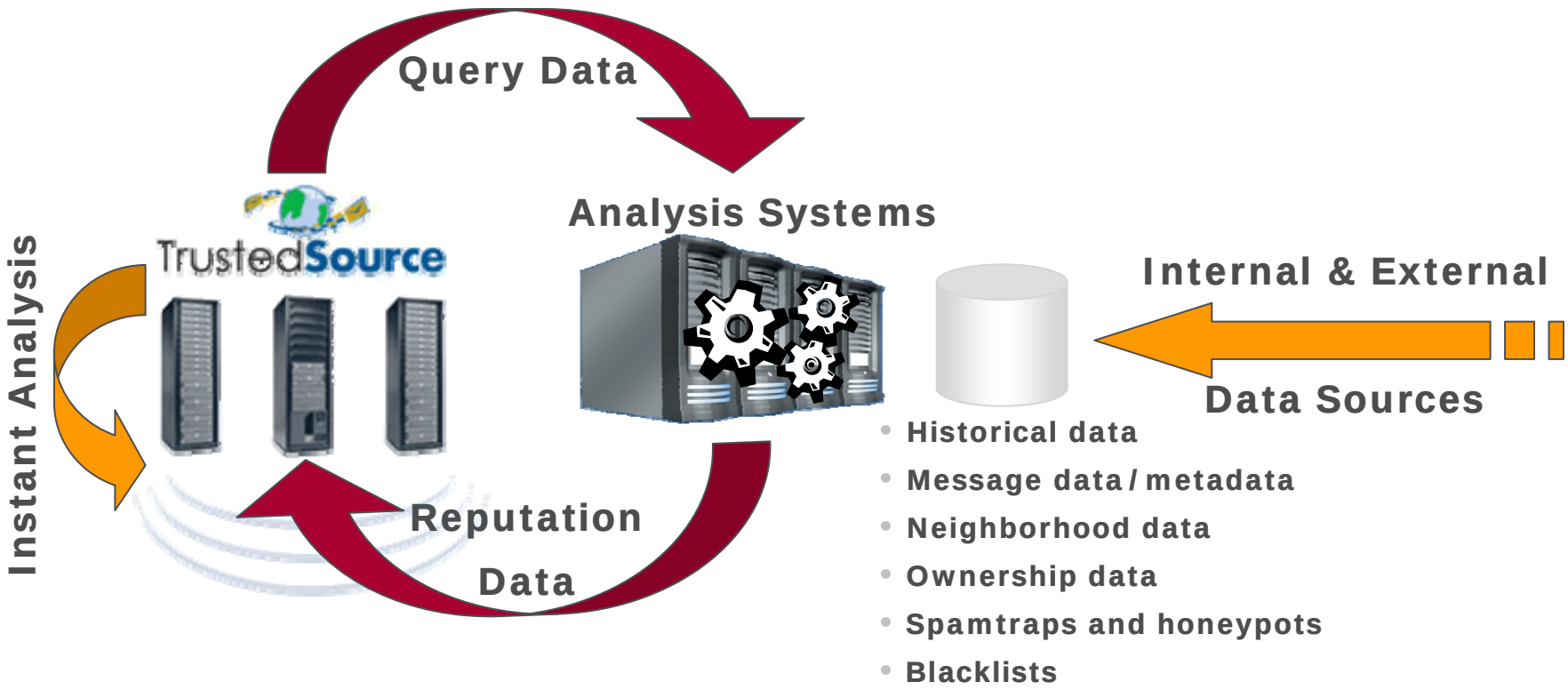
This entire process happens constantly, every second, 7x24x365



TS-enabled appliance

Responder Architecture

- Legacy protocol based on customized DNS servers
- Enhanced proprietary protocol (UDP over SSL)

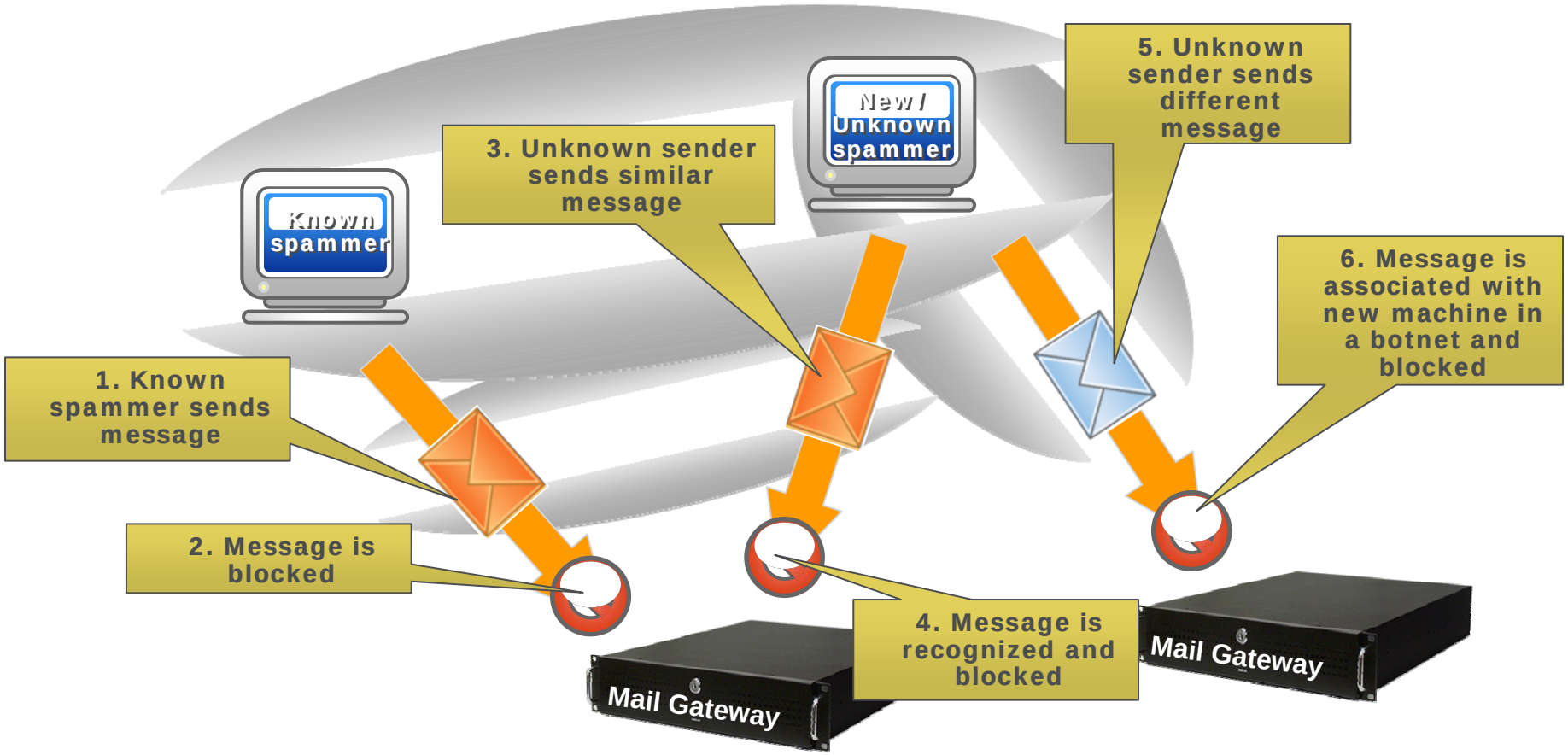


What does it monitor?

- Email
  - IP Reputation
  - Message Reputation
- Web
  - URL Categories
  - Web Reputation
- Intrusion/FW
  - IP/Protocol Reputation
  - Geo-Location
  - IPS Attack Vector Correlation

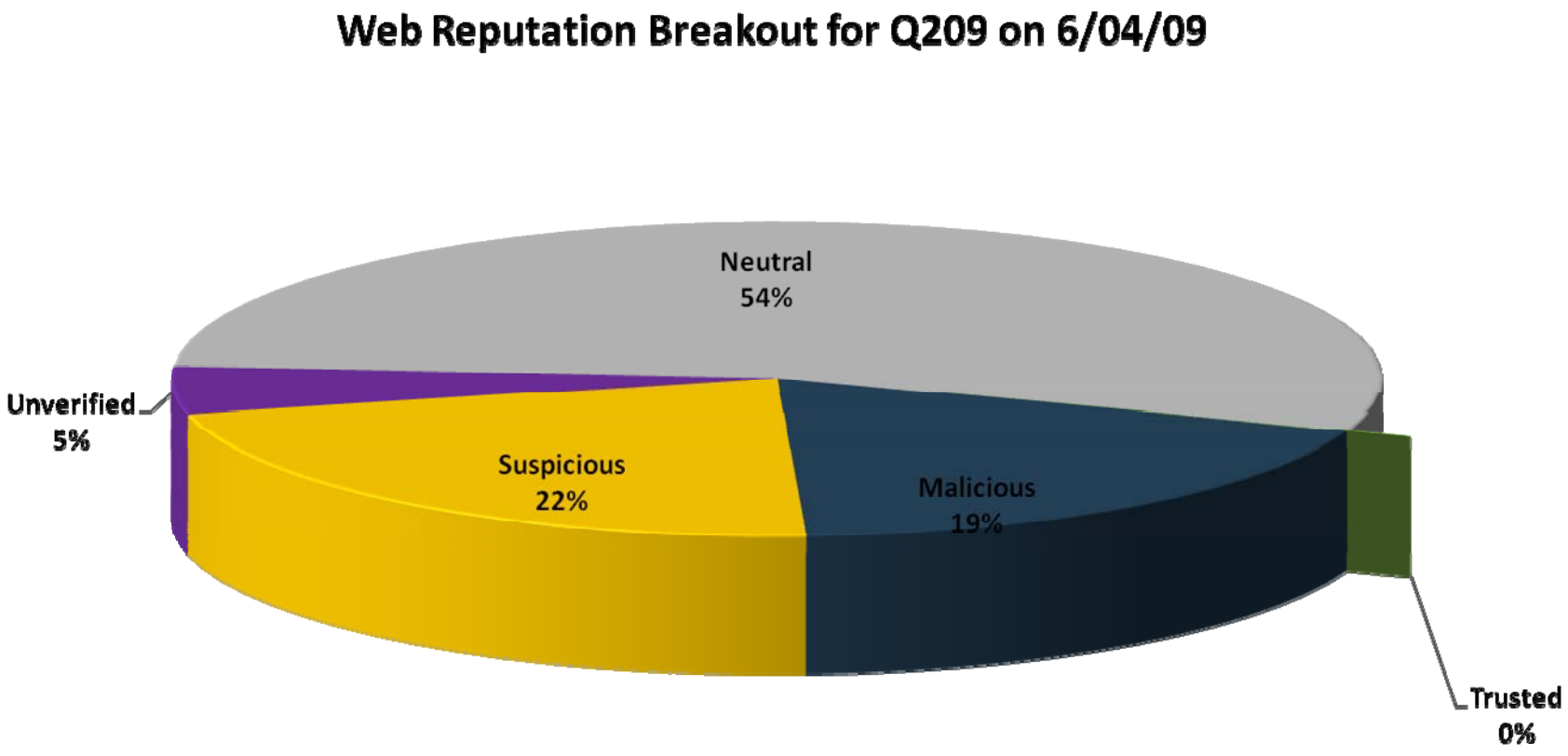
Dimensions		Connection Reputation	Content Reputation
Other	Hack Attack	Hacker sites	DoS, DDoS, misc other attacks
Web	Active Content Malware	Compromised or malicious web sites or URLs	ActiveX, Java, VB code from infected web sites
Email	Virus Phishing Spam	Zombies, Botnets, other sources	Image spam, Virus, worms, Trojans
		IP Domain URL	Attachment Image Message

Message Reputation



Allows Reputations to Move Across Identities and Protocols

TS Web Reputation Breakout



Building Web Reputation

TrustedSource for Web

Raw Data

- TrustedSource for Email
- Domain Registrations
- WHOIS data
- WebWasher classifiers
- SmartFilter categories
- Web access logs
- Malware URLs
- Phishing URLs
- Spam URLs
- Fortune 1000 websites
- Blacklists
- Whitelists

Analysis

- Correlation Mapping (Joint Conditional Mapping)
- Support Vector Machine classification of all parameters
- Parked Domain Identifier
- Neighborhood Classification
- Real-Time Classifier
- GEO Location
- Host information:
  - DNS
  - WHOIS
  - OS
  - Webserver
  - Certificate information

Reputation Service

Size

- 75 Million Hosts

Precision

- More Precise (-180 - +180)
- Identified zombies, malware, suspicious

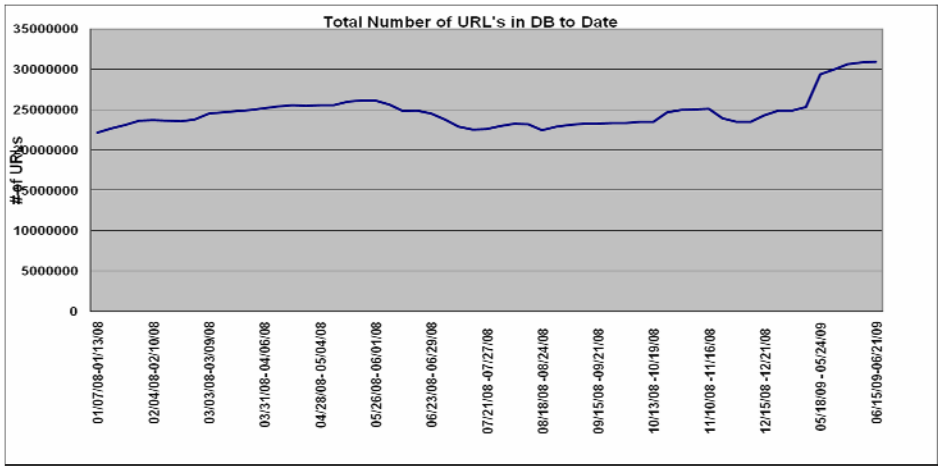
Reputation Range

-180 — +180

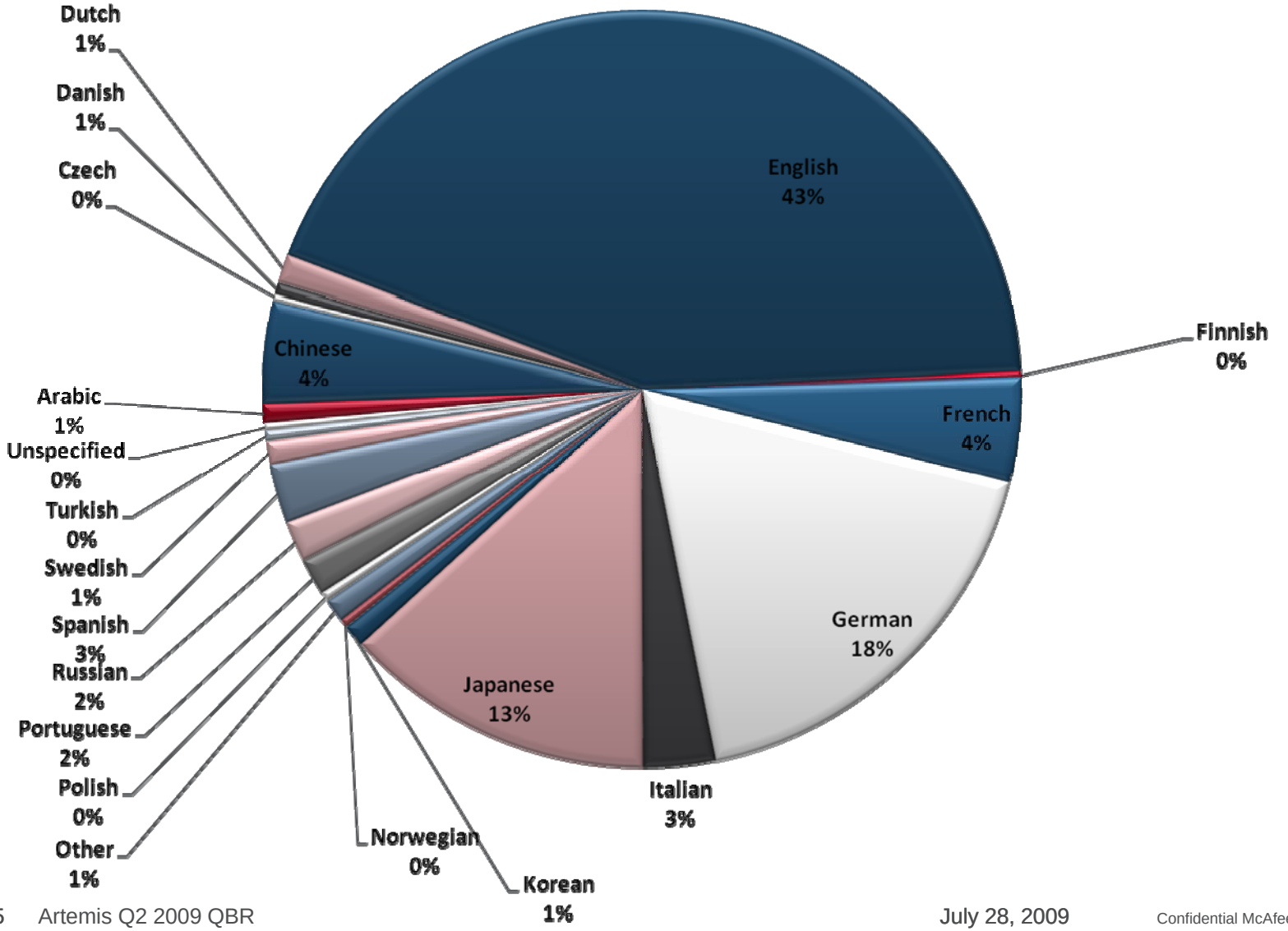
Bad — Suspicious — Good

TrustedSource Web Database

- Category-based filtering + reputation based filtering = best protection available
- 96 URL categories
- TrustedSource global intelligence augments numerous categories such as Spam, Malicious Sites, Phishing, Hacking/Computer Crime
- Reputation-based filtering for today's Web 2.0 threats
  - Provides an additional layer of security
  - Malicious sites, Spyware, Hacking, P2P, IM and more
- 31+ Million URLs (contains IPs, HTTP and HTTPS URLs)
- Automated proactive and reactive URL gathering systems
- Human review of URLs by multi-lingual/cultural Web Analysts
  - Global coverage (language and regions)
- Real-time updates

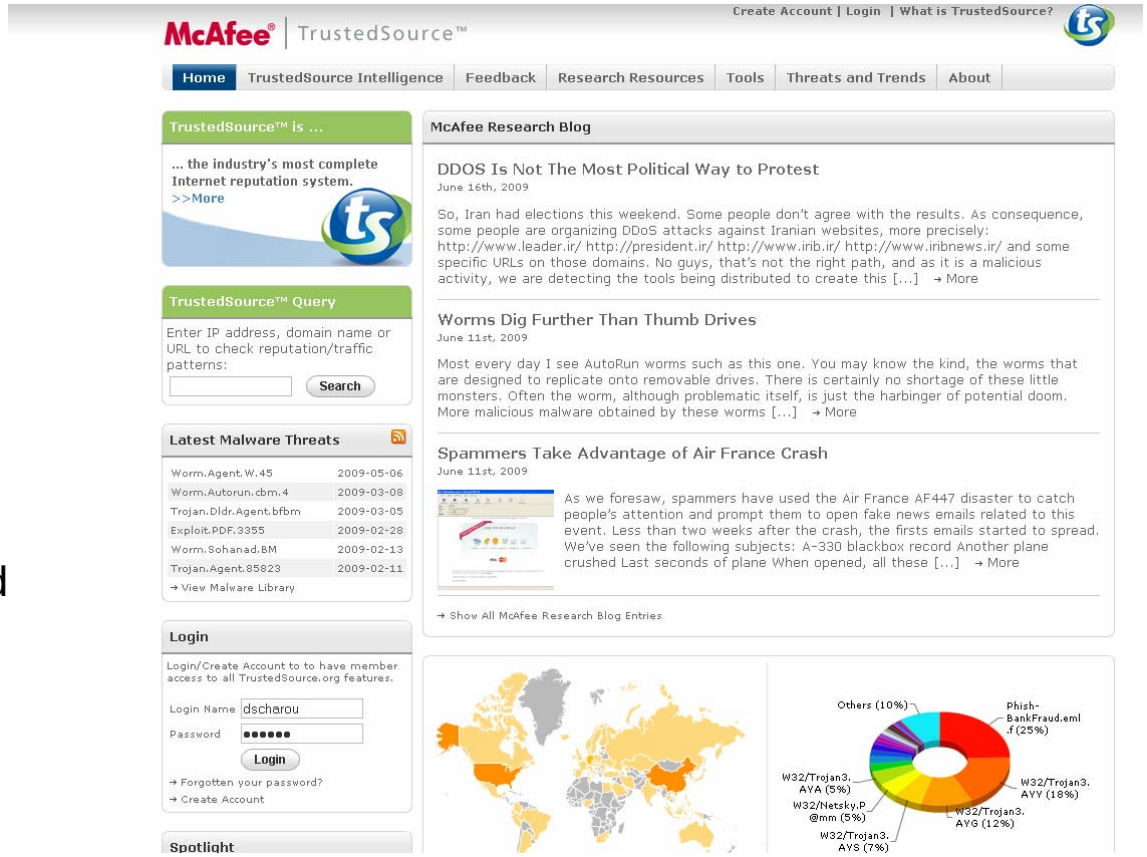


TS Web Language breakout



www.TrustedSource.Org

- Public Portal
- View reputations for domains, IP addresses or URLs
- Sending patterns of the senders
- Analytical information:
  - country of origin
  - network ownership
  - hosts for known senders within each domain
- Snapshot of global email trends, including a map illustrating country of origin for email attacks
- Graphs displaying overall email and spam volume trends
- ROI Calculator
- ZombieMeter
- Domain Health Check
- Latest malware threats
- Blogs from experts
- Top spam senders



McAfee®

Greg_Day@McAfee.com

0100011101110010011001010110011101011111010001000110000101111001010000000100
1101011000110100000101100110011001010110010100101110011000110110111101101101