McAfee
An Intel Company

Malware Trends 2011

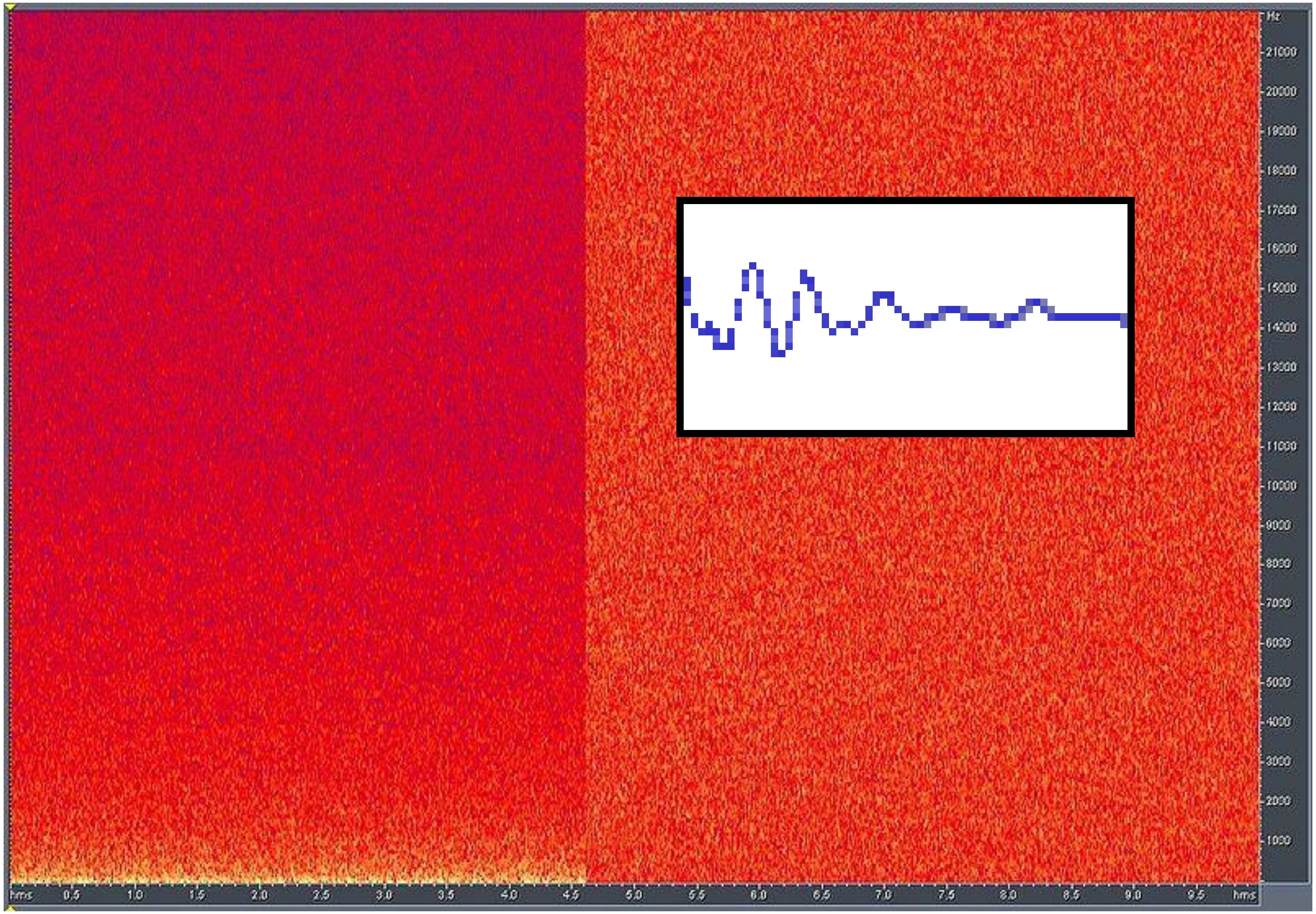
From cybercrime to nation-state sponsored espionage

Toralv Dirro
McAfee Labs EMEA Security Strategist

January 9, 2012

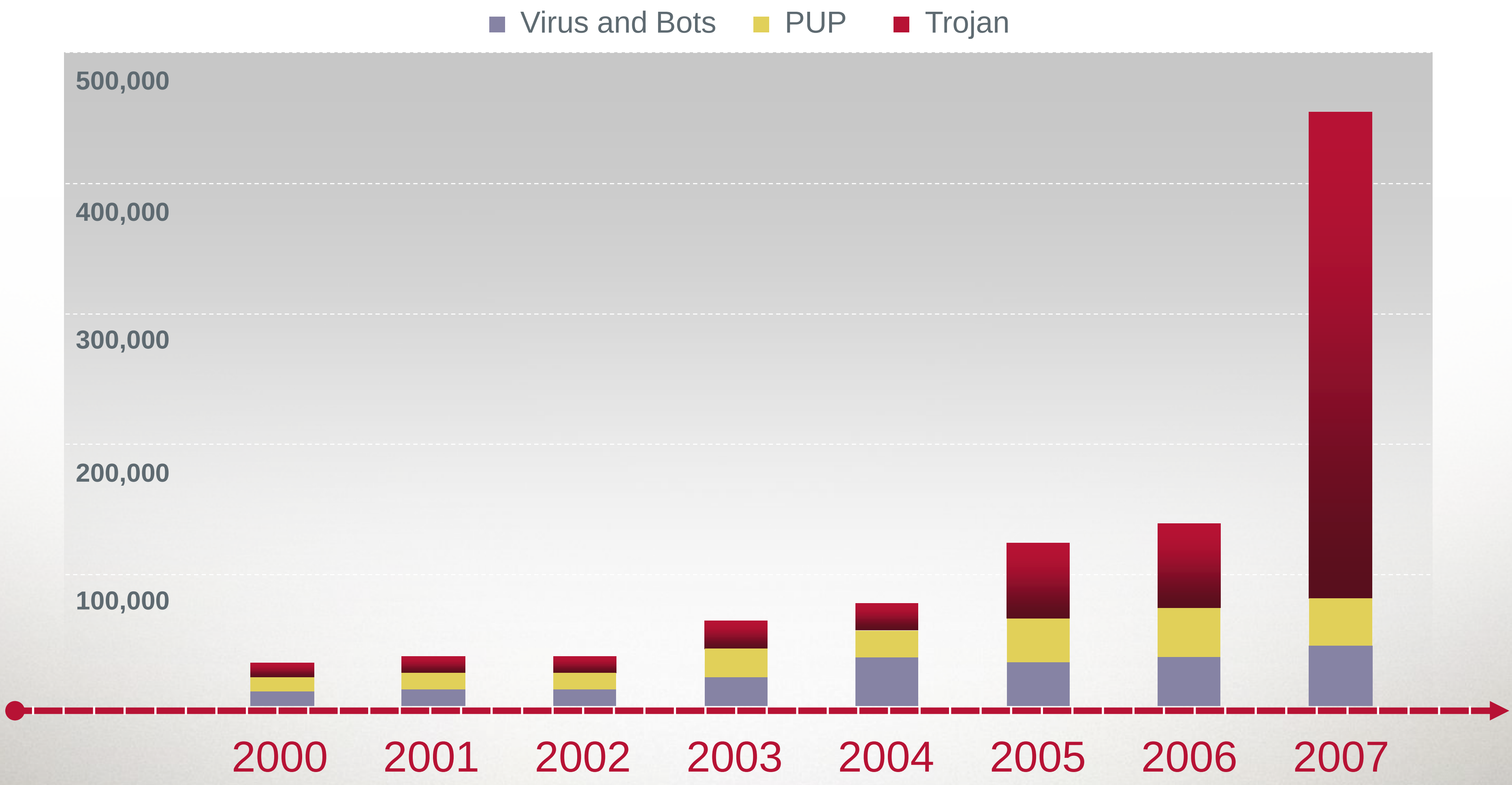
SAFE NEVER SLEEPS.

...or about Noise and Signal



White/pink poise picture copyright: http://en.wikipedia.org/wiki/User:Lenilucho

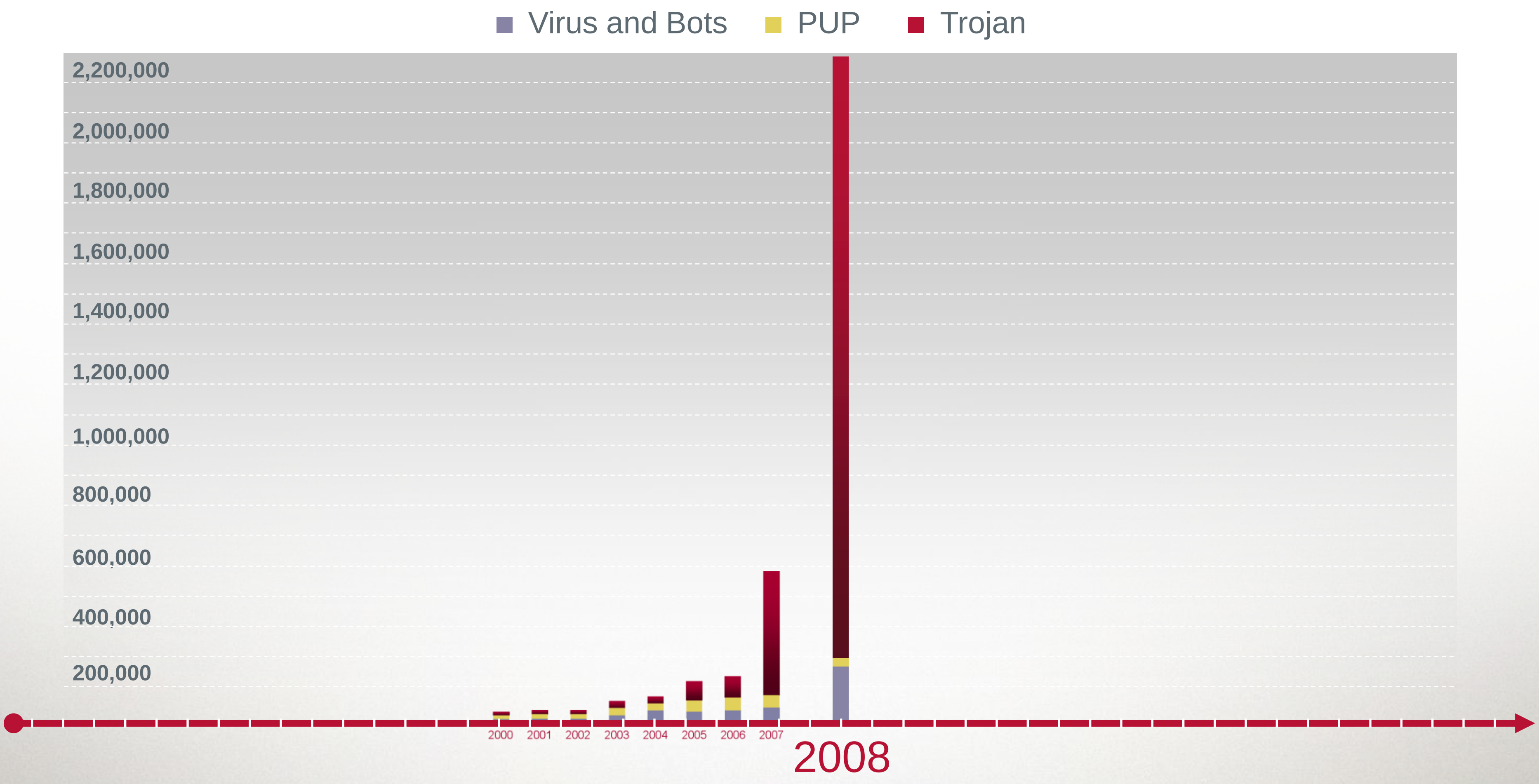
Noise



Malware Growth (Main Variations)

Source: McAfee Labs

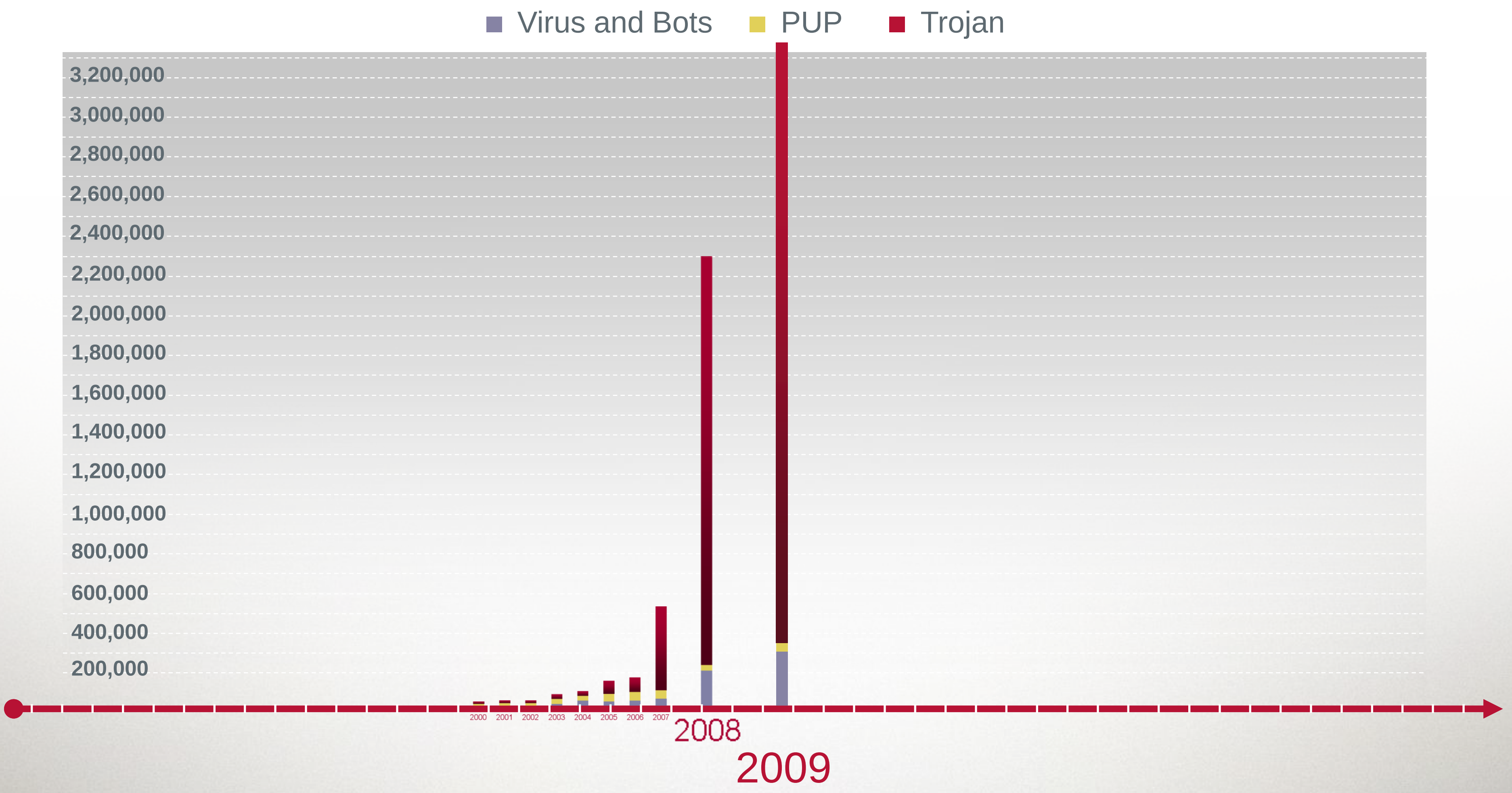
Noise



Malware Growth (Main Variations)

Source: McAfee Labs

Noise

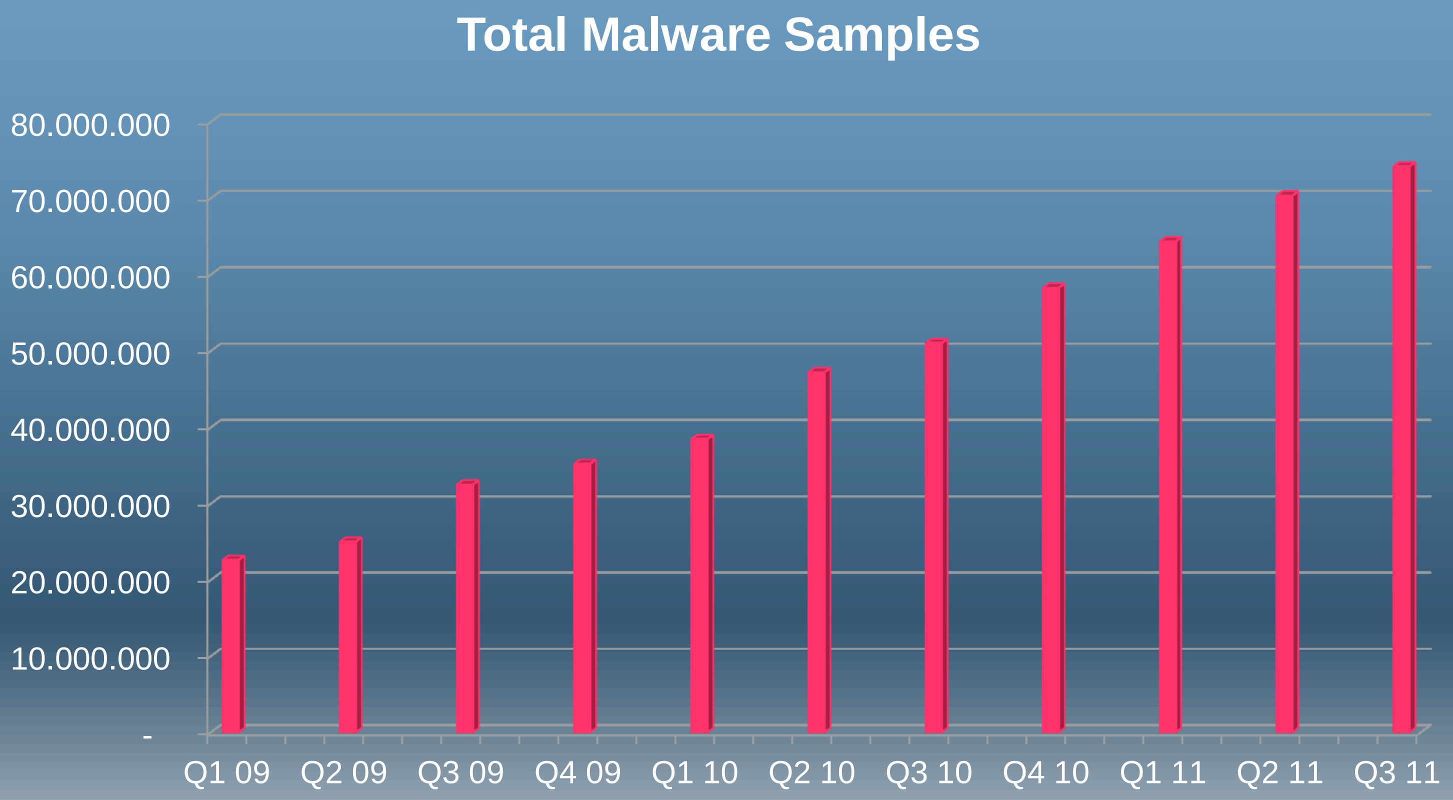


Malware Growth (Main Variations)

Source: McAfee Labs

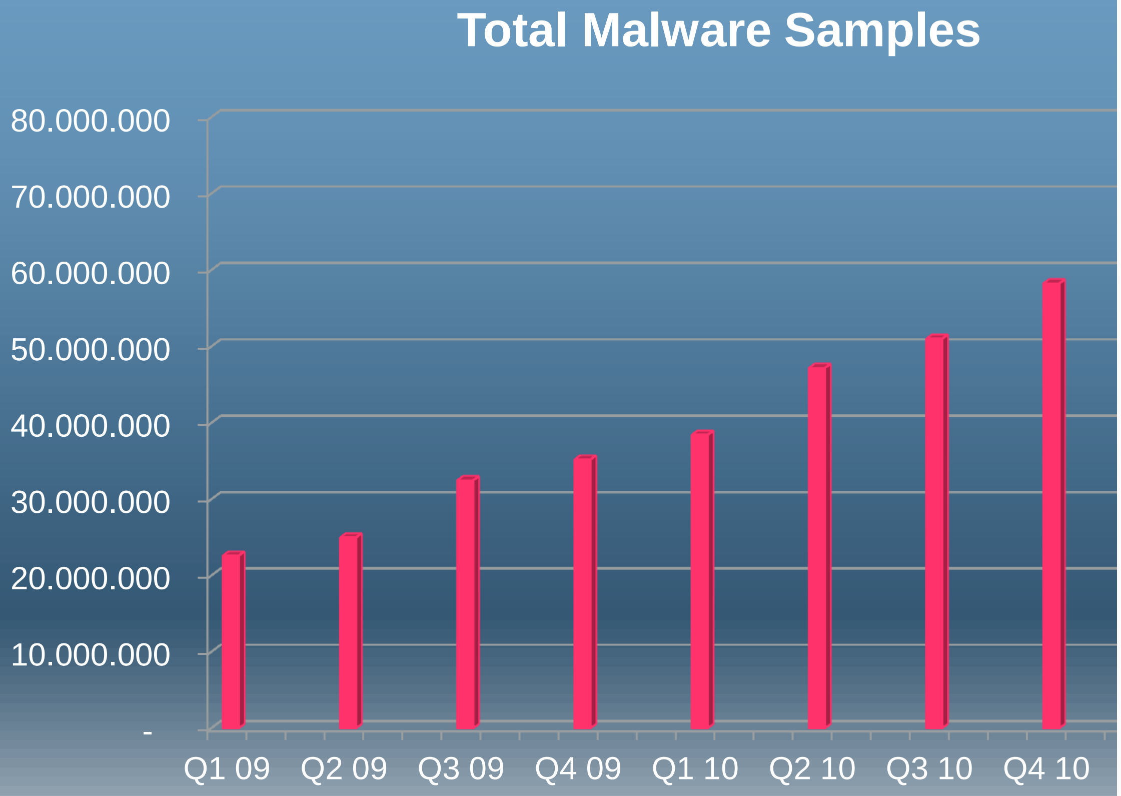
Noise: Malware Growth Continues

The growth in the number of new malware samples slowed ~20% in Q3 (typically its slowest quarter), but even at the Q3 rate of growth the number of distinct malware samples in the McAfee zoo will exceed 75m by year's end.

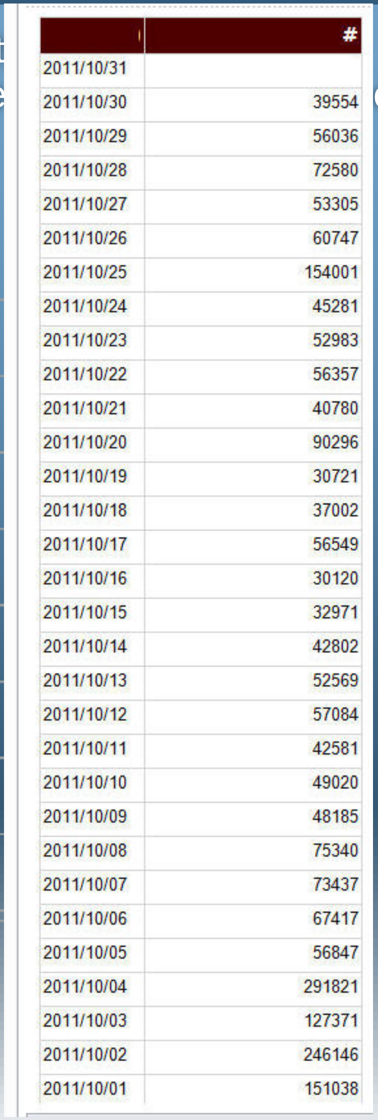


Noise: Malware Growth Continues

The growth in the number of new malware samples slowed ~20% in Q3 (t quarter), but even at the Q3 rate of growth the number of distinct malware e zoo will exceed 75m by year’s end.

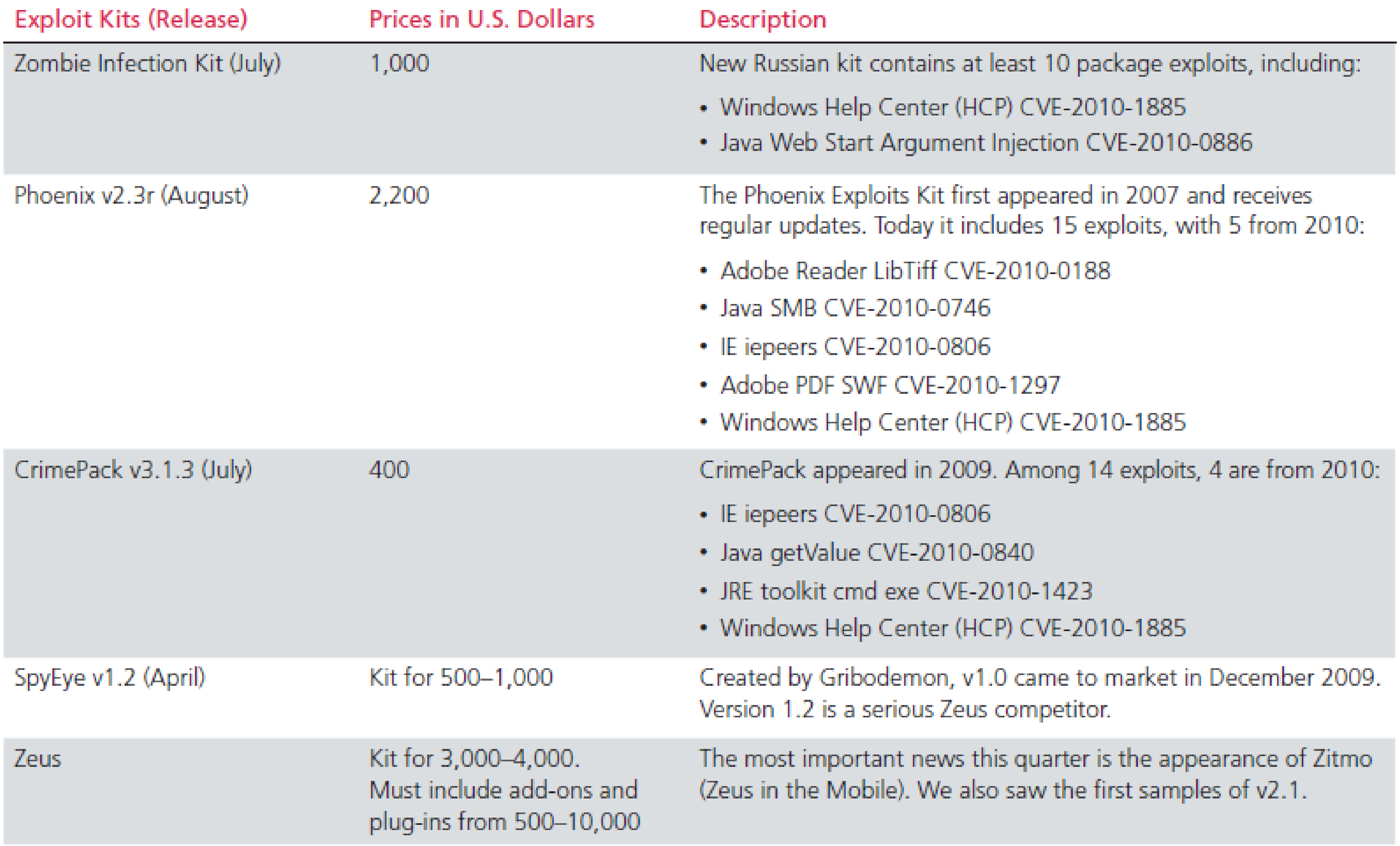


Artemis New Hashes By Day October 2011



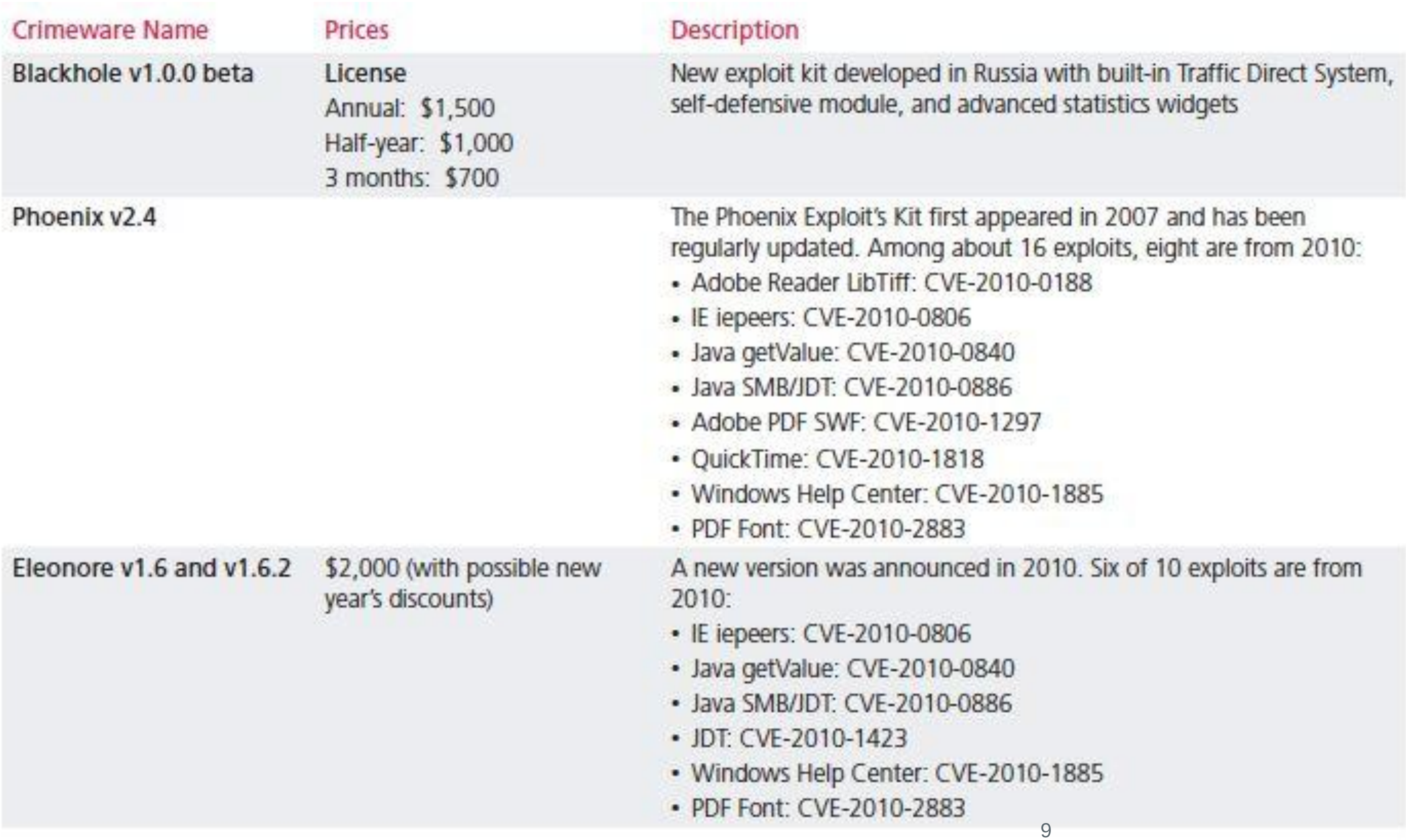
	#
2011/10/31	
2011/10/30	39554
2011/10/29	56036
2011/10/28	72580
2011/10/27	53305
2011/10/26	60747
2011/10/25	154001
2011/10/24	45281
2011/10/23	52983
2011/10/22	56357
2011/10/21	40780
2011/10/20	90296
2011/10/19	30721
2011/10/18	37002
2011/10/17	56549
2011/10/16	30120
2011/10/15	32971
2011/10/14	42802
2011/10/13	52569
2011/10/12	57084
2011/10/11	42581
2011/10/10	49020
2011/10/09	48185
2011/10/08	75340
2011/10/07	73437
2011/10/06	67417
2011/10/05	56847
2011/10/04	291821
2011/10/03	127371
2011/10/02	246146
2011/10/01	151038

Highly Sophisticated Noise



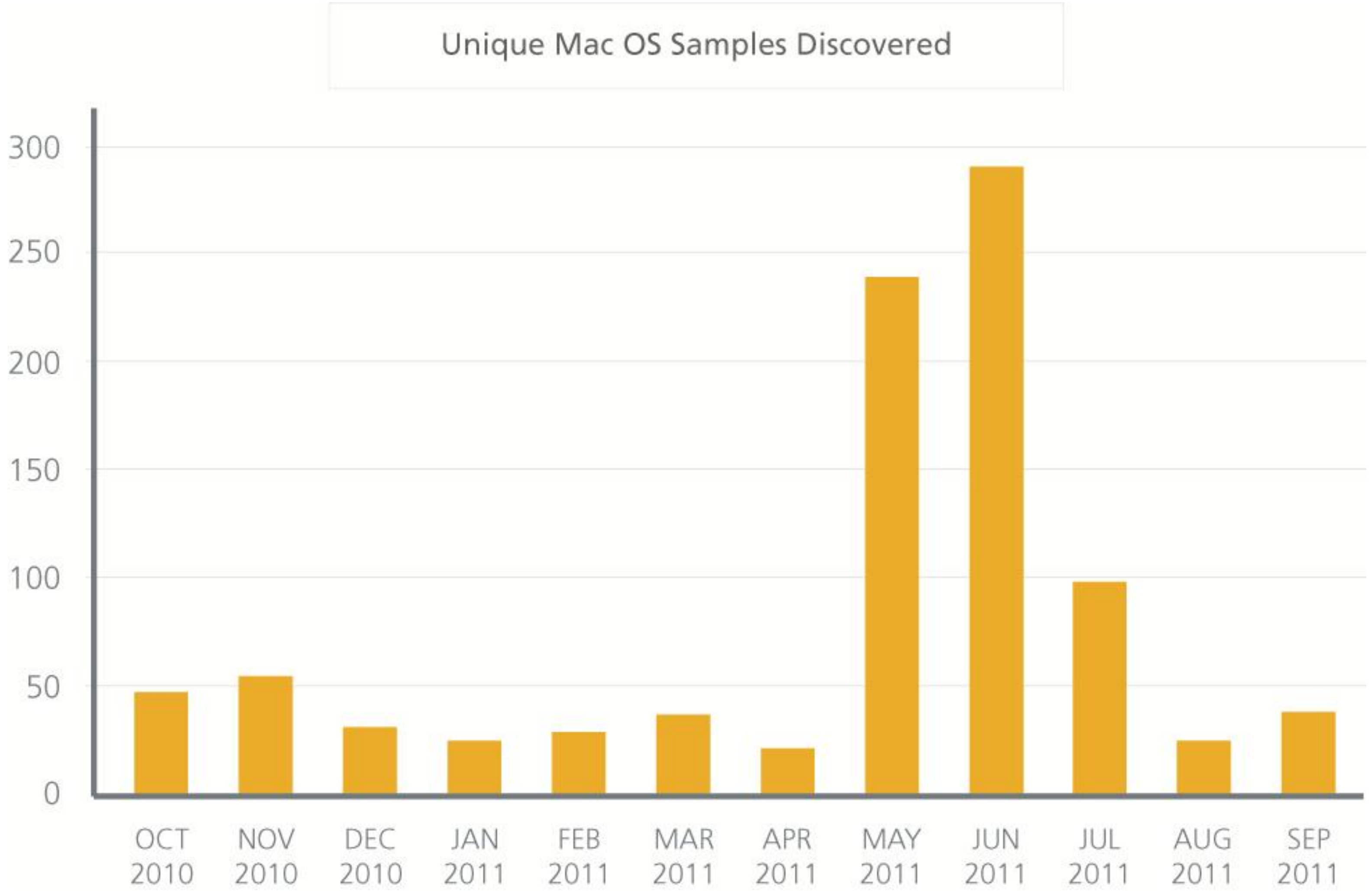
Exploit Kits (Release)	Prices in U.S. Dollars	Description
Zombie Infection Kit (July)	1,000	New Russian kit contains at least 10 package exploits, including: • Windows Help Center (HCP) CVE-2010-1885 • Java Web Start Argument Injection CVE-2010-0886
Phoenix v2.3r (August)	2,200	The Phoenix Exploits Kit 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.

Highly Sophisticated Noise

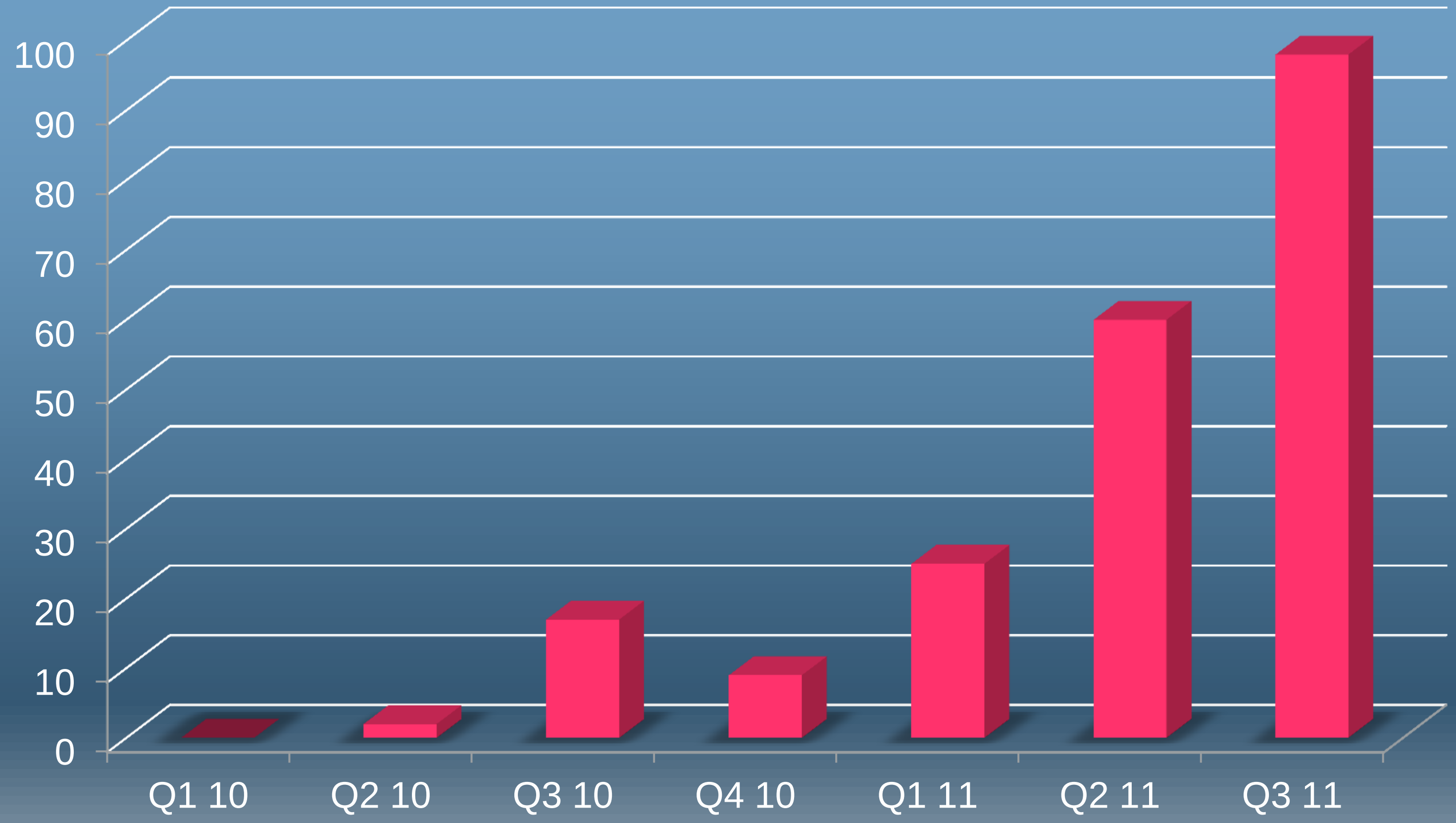


Crimeware Name	Prices	Description
Blackhole v1.0.0 beta	**License** Annual: $1,500 Half-year: $1,000 3 months: $700	New exploit kit developed in Russia with built-in Traffic Direct System, self-defensive module, and advanced statistics widgets
Phoenix v2.4		The Phoenix Exploit's Kit first appeared in 2007 and has been regularly updated. Among about 16 exploits, eight are from 2010: • Adobe Reader LibTiff: CVE-2010-0188 • IE iepeers: CVE-2010-0806 • Java getValue: CVE-2010-0840 • Java SMB/JDT: CVE-2010-0886 • Adobe PDF SWF: CVE-2010-1297 • QuickTime: CVE-2010-1818 • Windows Help Center: CVE-2010-1885 • PDF Font: CVE-2010-2883
Eleonore v1.6 and v1.6.2	$2,000 (with possible new year's discounts)	A new version was announced in 2010. Six of 10 exploits are from 2010: • IE iepeers: CVE-2010-0806 • Java getValue: CVE-2010-0840 • Java SMB/JDT: CVE-2010-0886 • JDT: CVE-2010-1423 • Windows Help Center: CVE-2010-1885 • PDF Font: CVE-2010-2883

Mac OS

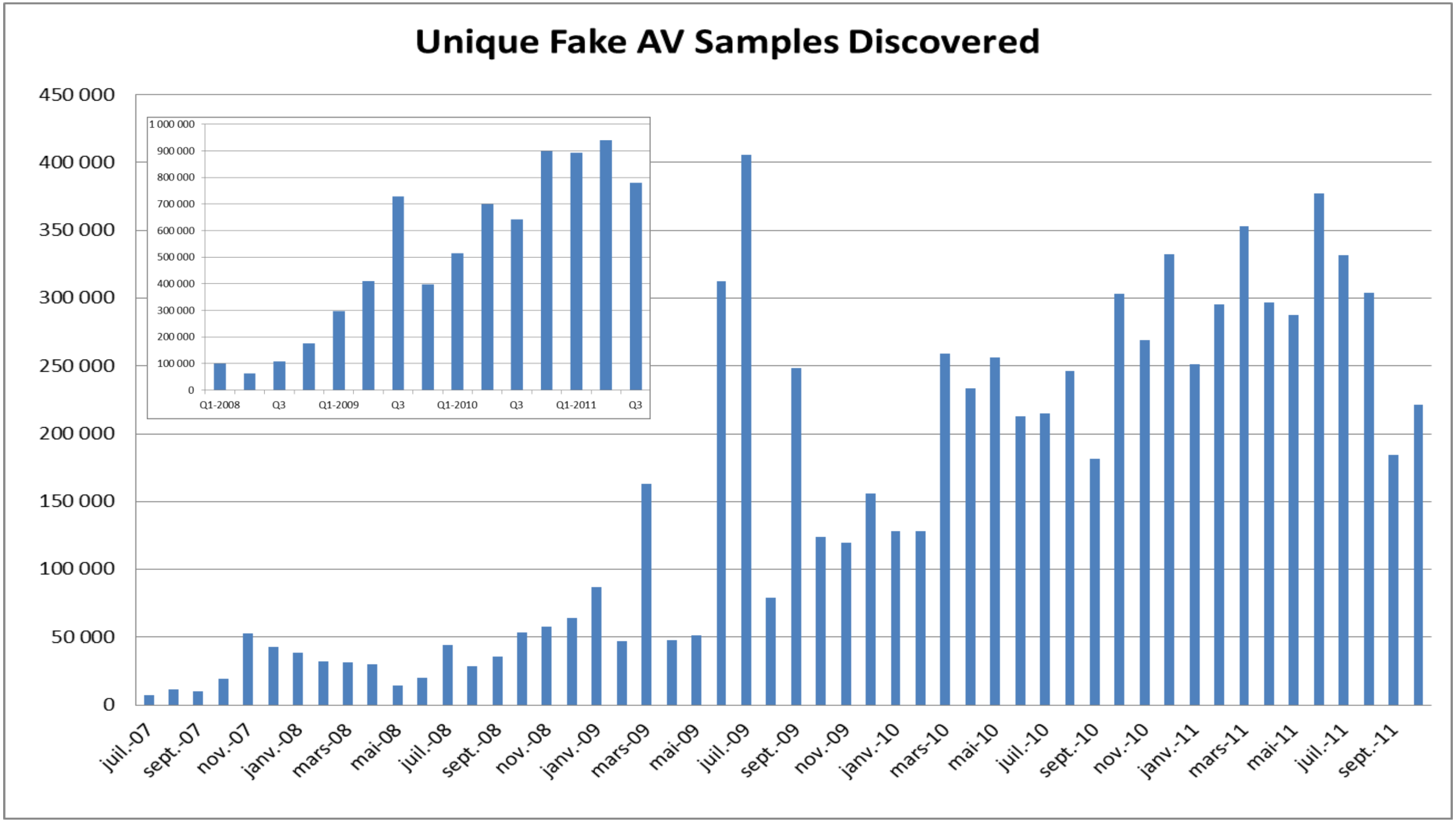

Unique Mac OS Samples Discovered
300
250
200
150
100
50
0
OCT 2010
NOV 2010
DEC 2010
JAN 2011
FEB 2011
MAR 2011
APR 2011
MAY 2011
JUN 2011
JUL 2011
AUG 2011
SEP 2011

Android Malware by Quarter



FakeAlert/Scareware – Multi 100mio Business

McAfee An Intel Company



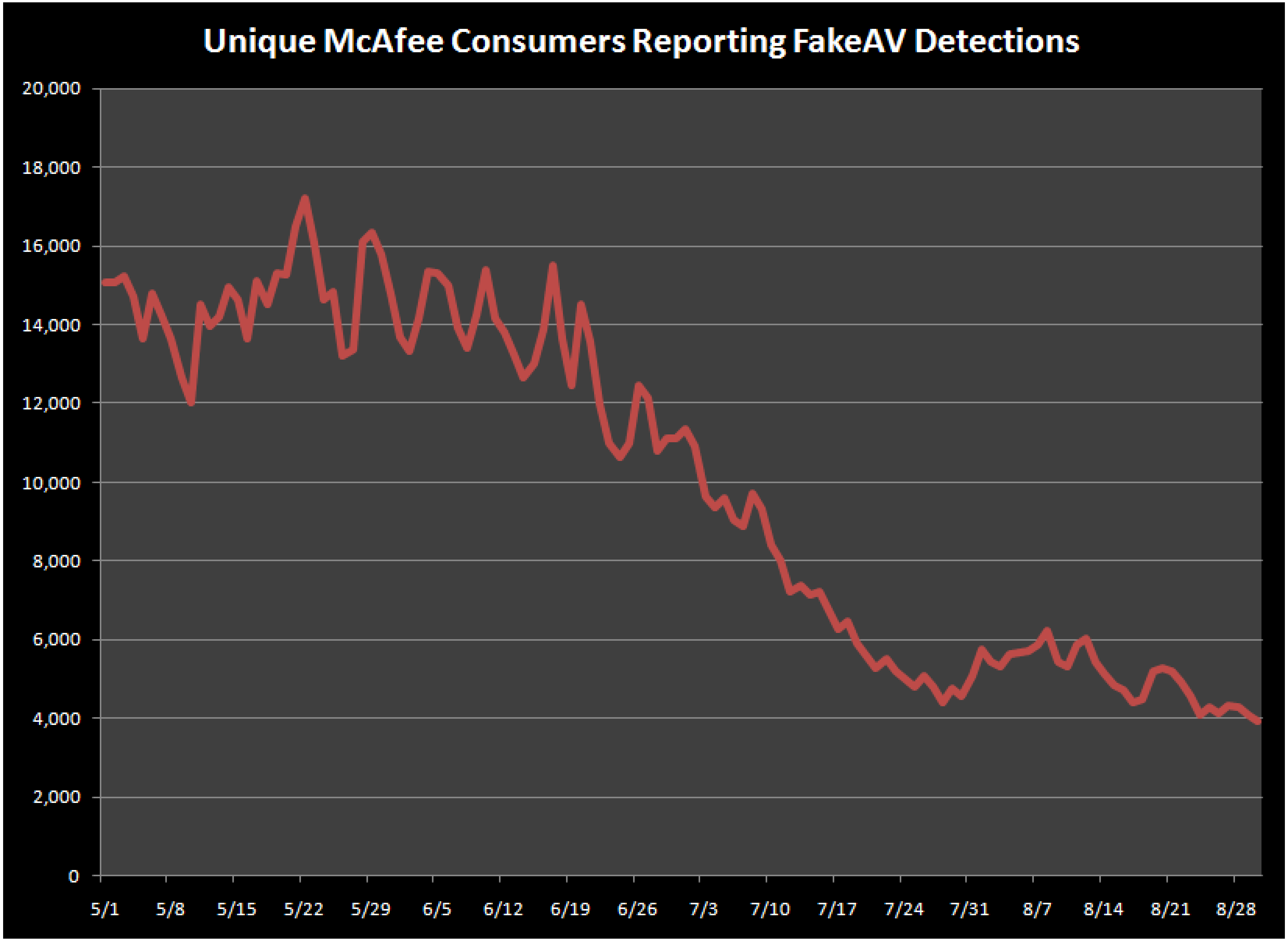
FakeAlert is the McAfee name for rogue anti-spyware or anti-viruses which are considered as malware (Trojan sub-family). Also known as scareware.

And then the money stopped flowing...

- Several companies in the Fake Malware (aka FakeAlert, Fake-AV, Scareware) market experienced difficulties to process credit card transactions of their victims

- Subsequently their Affiliates stopped installing/distributing

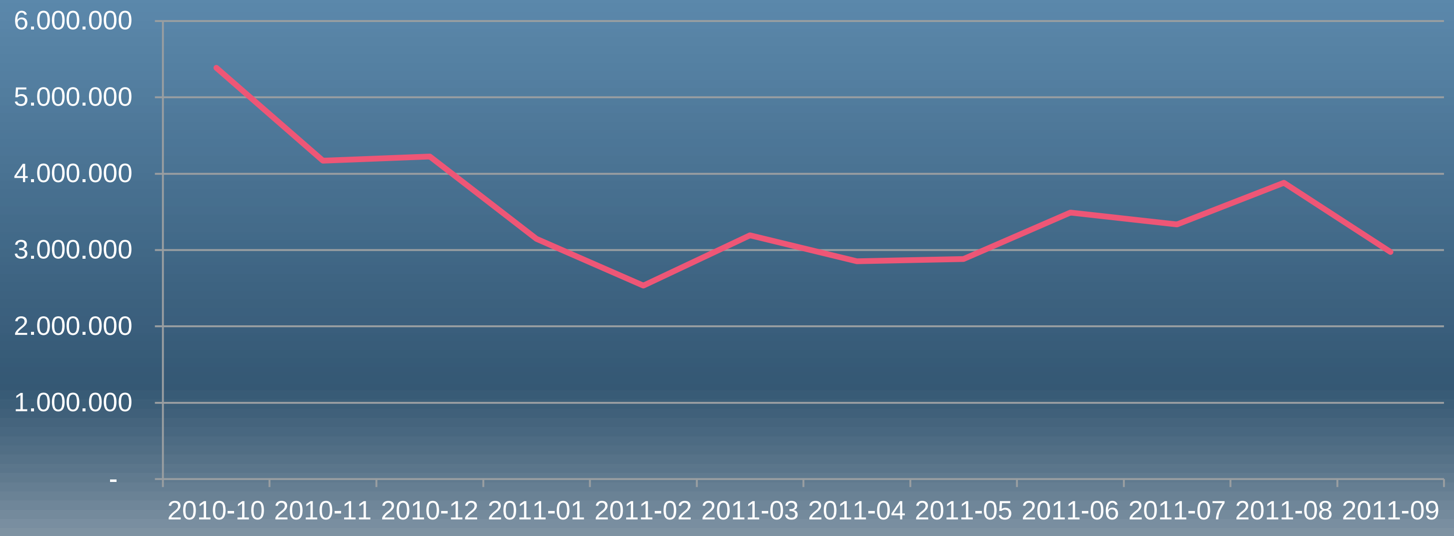
And then the money stopped flowing…



Botnet Infections Recover

The botnet “service providers” did their best to replace the Rustock & Bredolab nets lost to carrier actions in the last year. However, as the current trend is to build out smaller botnets with distributed command & control, progress has been uneven. Overall, botnet infection numbers are essentially unchanged since the beginning of the year.

Global Botnet Infections per Month



Global Malware Vision

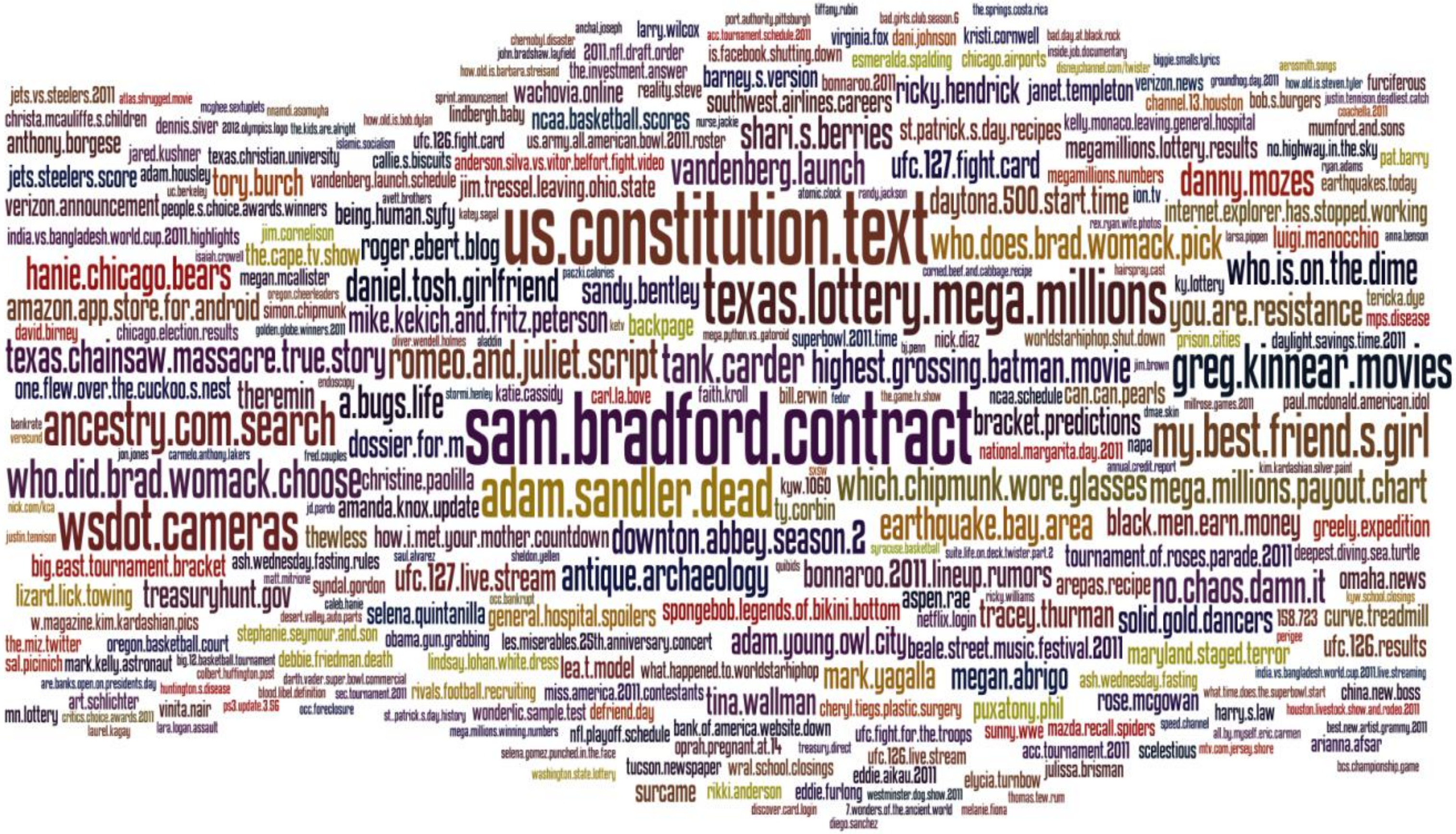
McAfee
An Intel Company

	End of 2007 (cumulative)	End of 2008 (cumulative)	End of 2009 (cumulative)	End of 2010 (cumulative)	Added in			
					Q1-2011	Q2-2011	Q3-2011	October
Malware (families) (DAT related)	358,000	484,000	594,000	655,400	+1,820	+1,040	+1 764	+1736
Autorun (Collection)	230,000	680,000	2,000,000	5,000,000	+710,000	+470,000	+460,000	+170,000
Exploits (Collection)	220,000	510,000	830,000	1,700,000	+140,000	+550,000	+140,000	+61,000
FakeAV, Scareware (Collection)	150,000	600,000	2,500,000	5,200,000	+900,000	+960,000	+820,000	+220,000
PassWord Stealers (Collection)	1,400,000	3,500,000	7,000,000	10,700,000	+1,000,000	+780,000	+880,000	+260,000
Rootkits (Collection)	170,000	680,000	1,700,000	2,900,000	+570,000	+510,000	+300,000	+80,000
Malware Zoo (Collection)	5,800,000	16,300,000	33,300,000	54,200,000	+6,900,000	+5,200,000	+4,700,000	+1,600,000

Note: The methods to count vary from company to company, comparison is not easily possibly!!

Black SEO

Of the top 100 results for each of the daily top search terms: 1.2% of search results this quarter led to a malicious site, down from 3.3% last quarter. 49% of the terms led to malicious sites (down from 51%). On average, each of these poisoned result pages contained more than two malicious links (down from five).



Most Dangerous Celebrities 2011

1. **Heidi Klum**
   - Klum, the former Victoria’s Secret model and current producer of “Project Runway” moved up from No. 10 on last year’s list to No. 1 today. **Searching for Klum results in nearly a one in ten chance of landing on a risky site**.
2. **Cameron Diaz**
   - 2010’s Most Dangerous Celebrity fell to second place, with searches resulting in slightly fewer risky sites this year. She has most recently been in the spotlight with her 2011 movies “Bad Teacher” and “The Green Hornet.”
3. **Piers Morgan**
   - A new addition to the top ten list, Morgan is also the most dangerous male celebrity. He is best known as the host of “Piers Morgan Tonight,” taking over for Larry King, a winner of the “Celebrity Apprentice,” and one of the judges on “America’s Got Talent.”

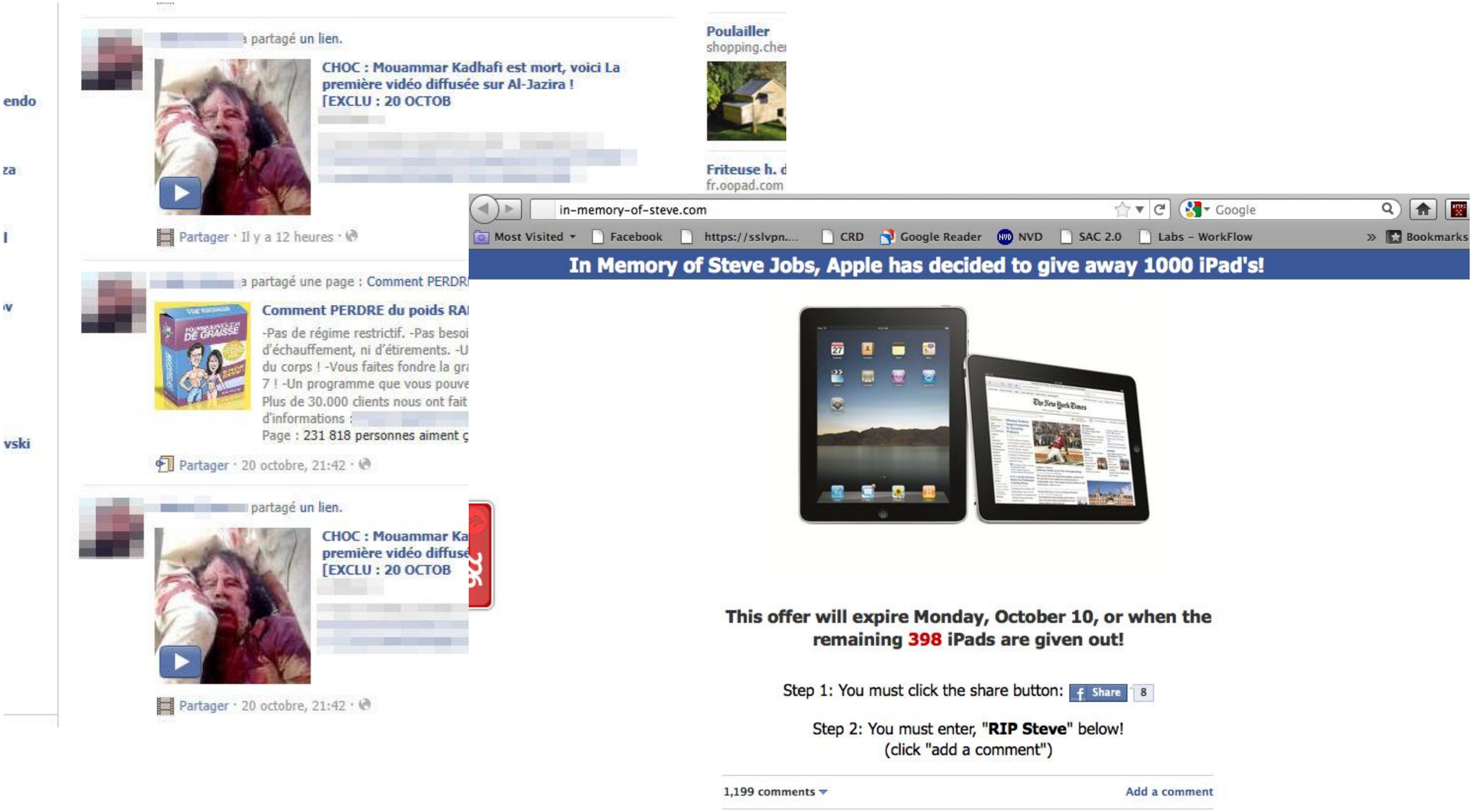
And Mass SQL Injections

- Benign legitimate websites becoming dangerous over night
  - Sometimes takes weeks/months to discover and mitigate

- „Just recently we have seen a spike in the number of incidents associated with LizaMoon infections we documented a while back. We have recorded approximately 6.3 million websites infected by malware as part of this SQL injection attack.“
  - Source: http://www.stopthehacker.com/2011/08/24/lizamoon-all-over-again/

Scam

Scammers profit from Steve Jobs and Kadhafi' Deaths



endo

za

l

w

vski

[redacted] a partagé un lien.

CHOC : Mouammar Kadhafi est mort, voici La première vidéo diffusée sur Al-Jazira ! [EXCLU : 20 OCTOB

Partager · Il y a 12 heures ·

[redacted] a partagé une page : Comment PERDR

Comment PERDRE du poids RA

-Pas de régime restrictif. -Pas besoi d'échauffement, ni d'étirements. -U du corps ! -Vous faites fondre la gr 7 ! -Un programme que vous pouve Plus de 30.000 clients nous ont fait d'informations :

Page : 231 818 personnes aiment ç

Partager · 20 octobre, 21:42 ·

[redacted] partagé un lien.

CHOC : Mouammar Ka première vidéo diffusé [EXCLU : 20 OCTOB

Partager · 20 octobre, 21:42 ·

Poulailler
shopping.che

Friteuse h. d
fr.oopad.com

In Memory of Steve Jobs, Apple has decided to give away 1000 iPad's!

This offer will expire Monday, October 10, or when the remaining 398 iPads are given out!

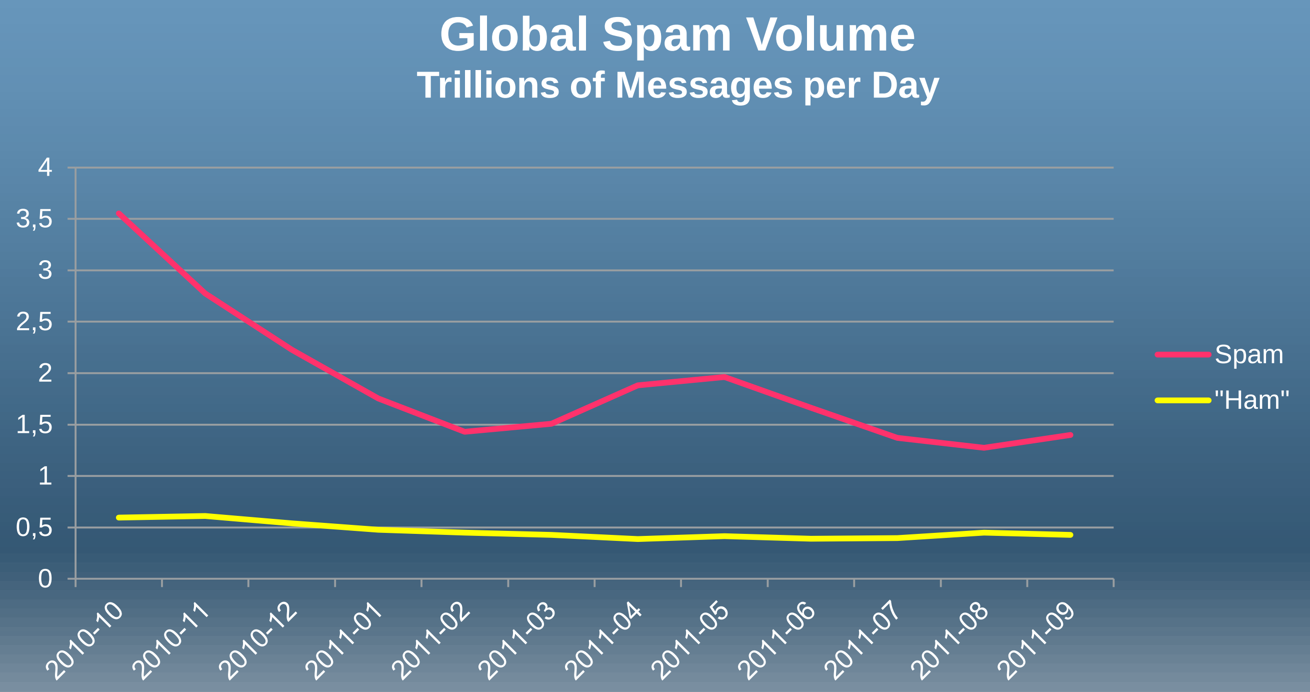
Step 1: You must click the share button: Share 8

Step 2: You must enter, "**RIP Steve**" below!
(click "add a comment")

1,199 comments ▾ Add a comment

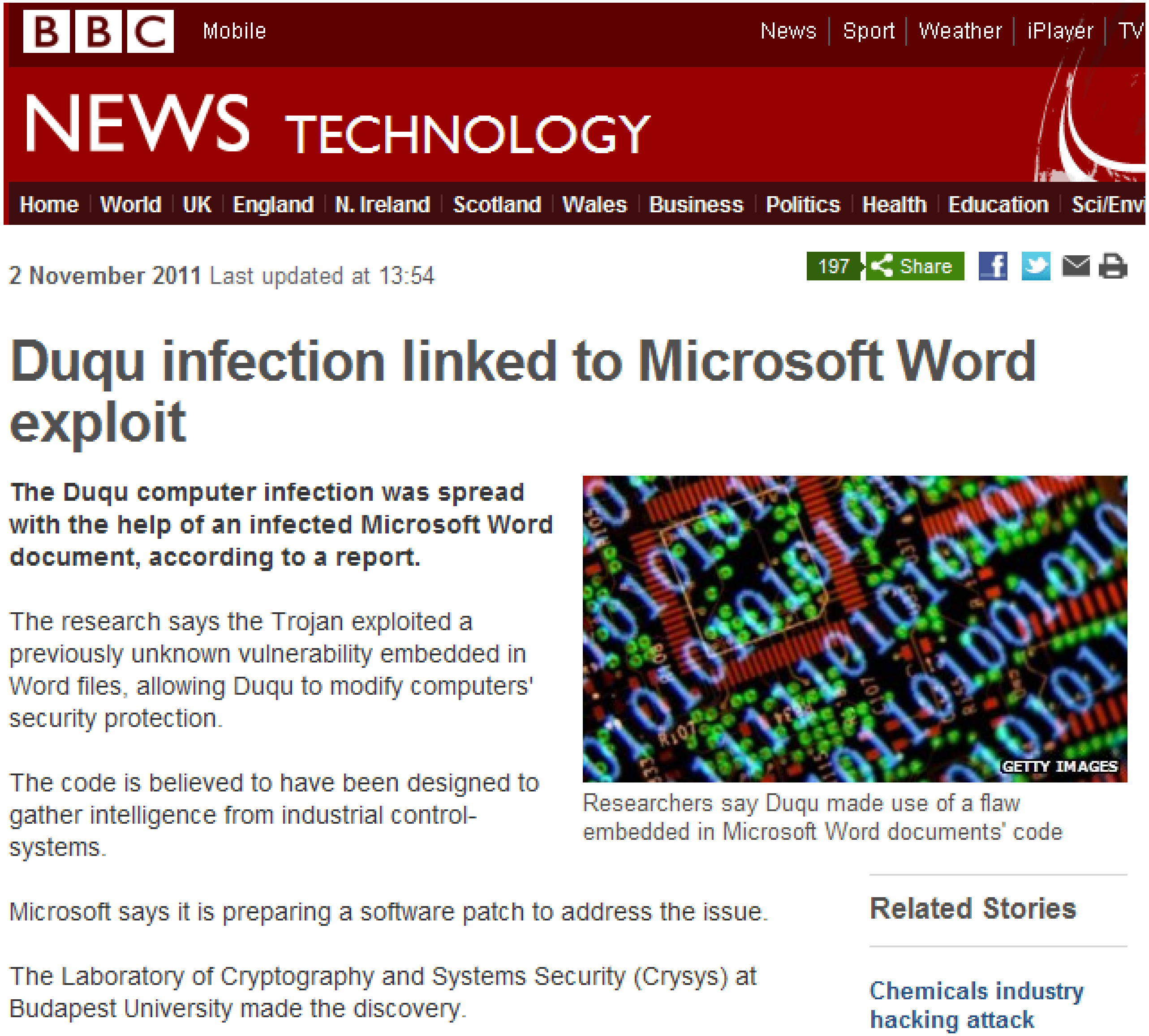
Noise

Global spam volume was essentially flat in the second half of 2011. Current daily spam volume is now at a level not seen since 2007. There are signs that many spammers have abandoned their volume mailing activity due to lack of cost effective botnet services and the greater response rates and profitability available from targeted, low volume spear phishing attacks.



Signal

McAfee
An Intel Company



BBC
Mobile
News | Sport | Weather | iPlayer | TV
NEWS TECHNOLOGY
Home | World | UK | England | N. Ireland | Scotland | Wales | Business | Politics | Health | Education | Sci/Envi
197
Share
GETTY IMAGES

2 November 2011 Last updated at 13:54

Duqu infection linked to Microsoft Word exploit

The Duqu computer infection was spread with the help of an infected Microsoft Word document, according to a report.

The research says the Trojan exploited a previously unknown vulnerability embedded in Word files, allowing Duqu to modify computers' security protection.

The code is believed to have been designed to gather intelligence from industrial control-systems.

Researchers say Duqu made use of a flaw embedded in Microsoft Word documents' code

Microsoft says it is preparing a software patch to address the issue.

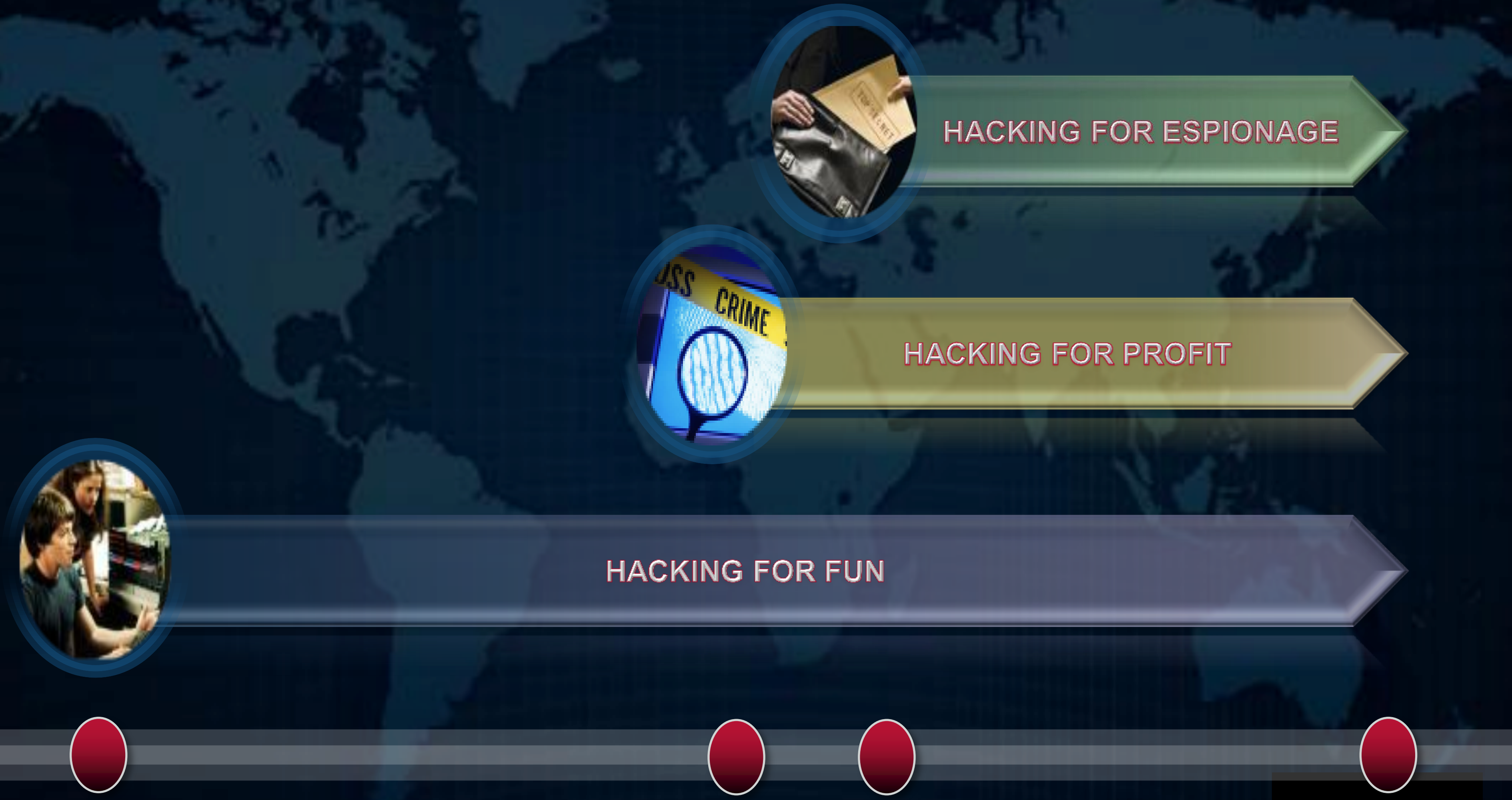
The Laboratory of Cryptography and Systems Security (Crysys) at Budapest University made the discovery.

Related Stories

Chemicals industry hacking attack

Source: http://www.bbc.co.uk/news/technology-15554361

Historic Stages of Cyber Attacks



HACKING FOR ESPIONAGE

HACKING FOR PROFIT

HACKING FOR FUN

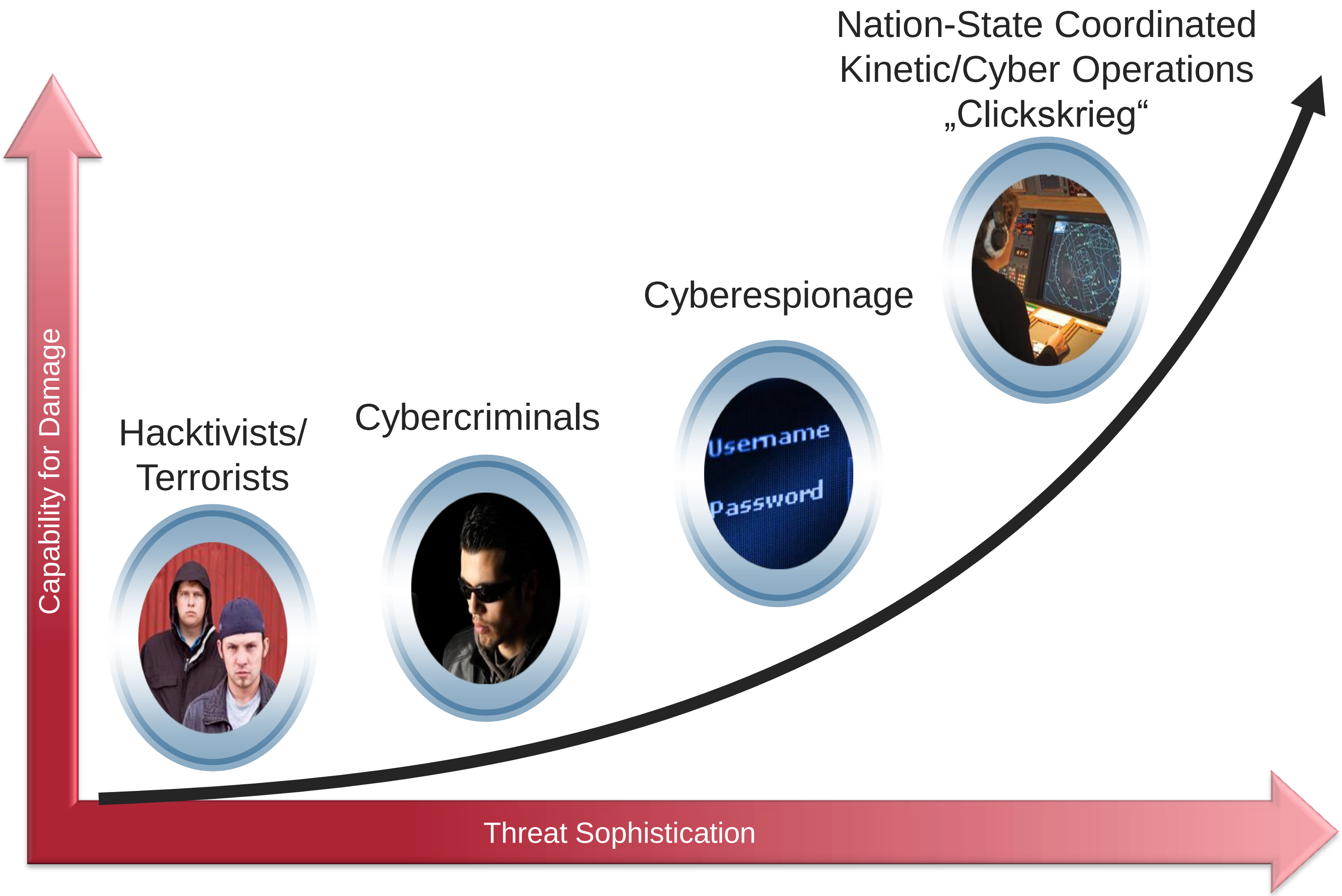
Mid-1980’s

2003

2005

Today

Classification of Attackers



Nation-State Coordinated
Kinetic/Cyber Operations
„Clickskrieg"

Cyberespionage

Cybercriminals

Hacktivists/
Terrorists

Capability for Damage

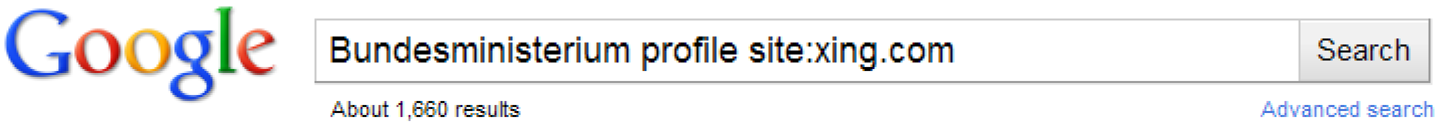
Threat Sophistication

The Old SECURITY Model

Is BROKEN

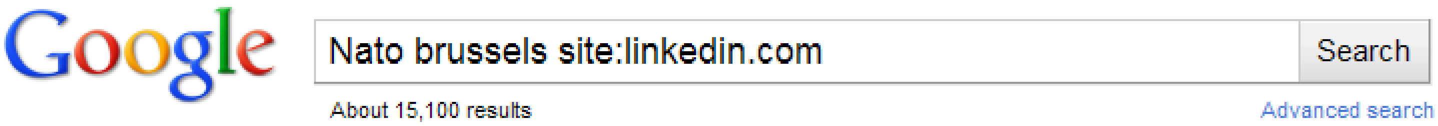
You, and You Alone ARE THE TARGET

Successful Social Engineering made easy


Bundesministerium profile site:xing.com

About 1,660 results

About 1,660 results


Nato brussels site:linkedin.com

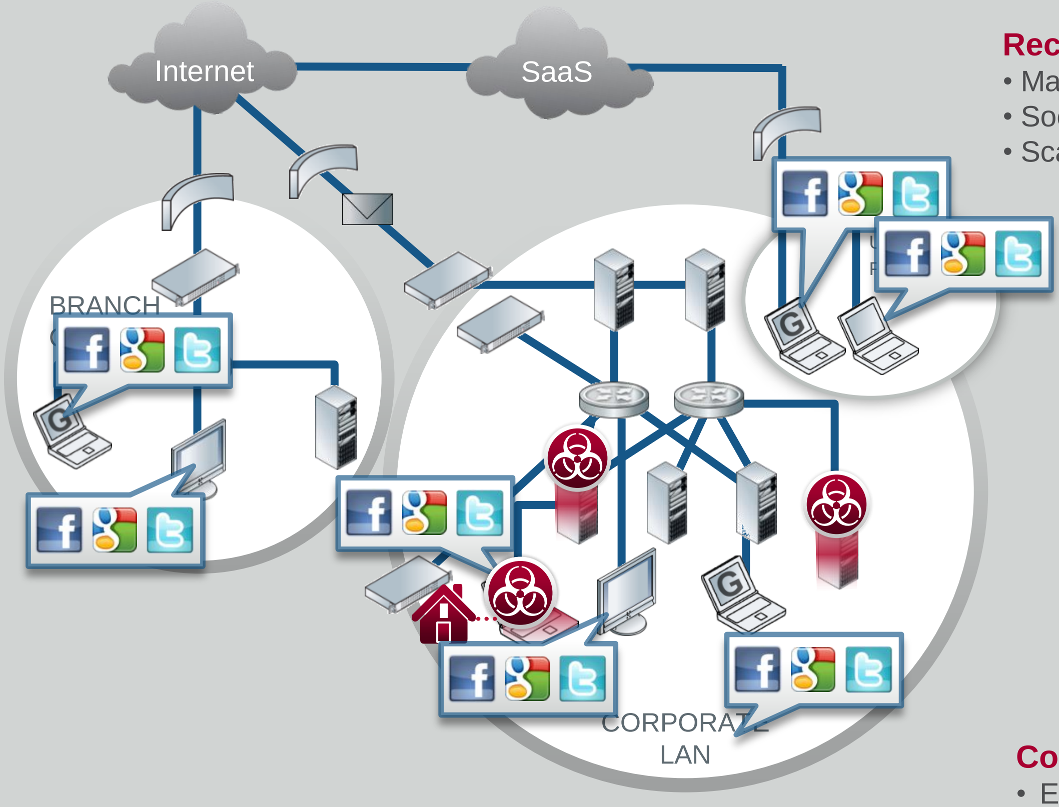
About 15,100 results

About 15,100 results

Checking on some of the results quickly led to Facebook profiles, Twitter accounts (some with Twitter location enabled) and FourSquare

Patterns Indicative of Night Dragon & Many APTs

McAfee
An Intel Company



Reconnaissance

- Map org chart (Identify attack targets)
- Social reconnaissance (acquire email, IM, etc.)
- Scan for vulnerabilities (web server/OS/DNS/network, etc.)

Social Engineering Targeted Malware

- Phishing email (malicious PDF, DOC, etc. w/shellcode)
- Candy drops around blgd (Thumb drives, DVD's)
- Gain physical access (impersonate cleaning crew, etc.)

Establish Covert Backdoor

- Command execution on target
- Gain elevated user privileges, Inject additional Malware
- Laterally move within network & establish backdoors

Establish Command & Control Infrastructure

- Install system admin tools (Keyloggers, Trojans, etc.)
- Establish encrypted SSL tunnel
- Utilize a remote administration tool (RAT)

Complete Objectives

- Ex-filitrate Intellectual Property, Trade Secrets
- Install Trojans in source code
- Control critical systems

Maintain Persistence

- Revamp Malware to avoid detection
- Utilize other attack methods to maintain presence
- Continue monitoring networks, users, data

Why should organisations care about APTs?

Attackers

- Malicious Insiders / Ex-Employees
- Unscrupulous Competitors
- Nation States
- Terrorist / Activists Organizations

Motives

- Political—maintain internal stability
- Economic—stealing intellectual property
- Technical—access to source code
- Military—identify weaknesses to defeat superior military forces

Targets

- Organizations w/ critical IP
- Critical Infrastructure
- Federal Government
- DoD contractors

Goals

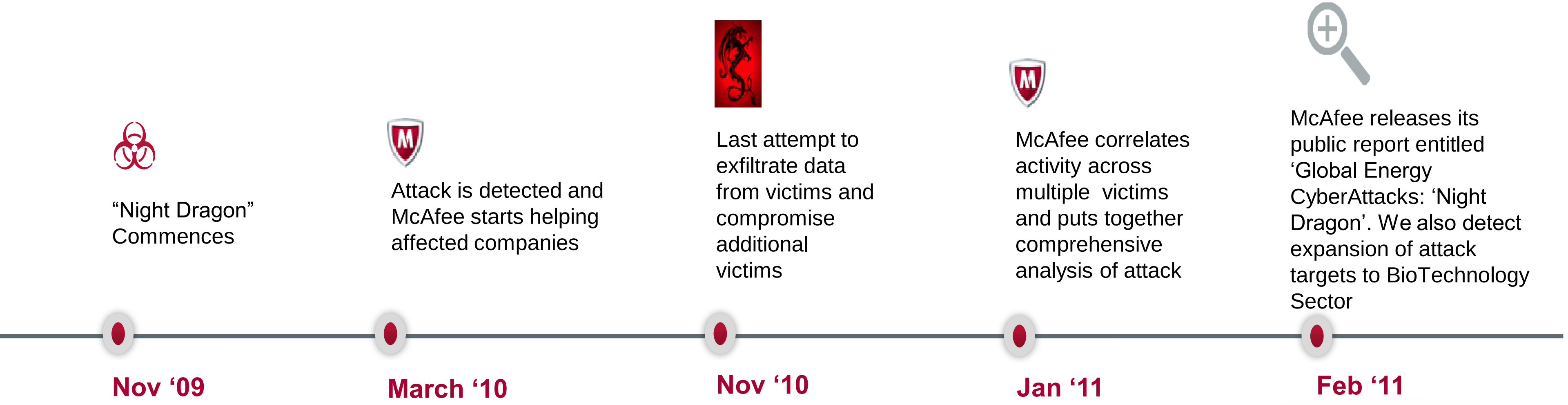
- Establish network foothold
- Stealth intrusion, backdoors
- Ex-filtrate sensitive data
- Leave no traces

IF YOU HAD A COMPROMISED SYSTEM STEALING DATA, HOW WOULD YOU KNOW?

Operation NIGHT DRAGON

Signal

‘Night Dragon’ Intrusions



Nov ‘09
“Night Dragon” Commences

March ‘10
Attack is detected and McAfee starts helping affected companies

Nov ‘10
Last attempt to exfiltrate data from victims and compromise additional victims

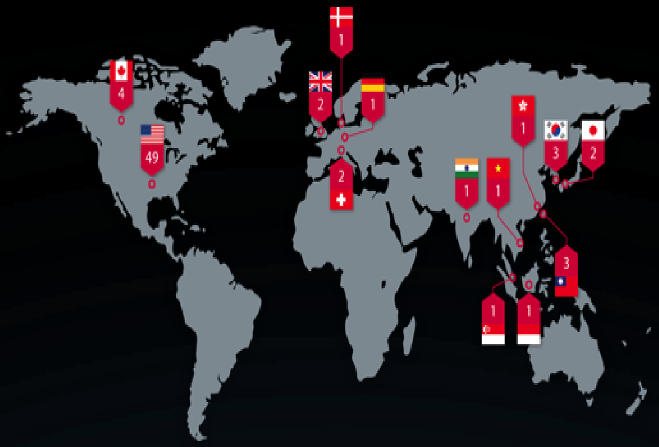
Jan ‘11
McAfee correlates activity across multiple victims and puts together comprehensive analysis of attack

Feb ‘11
McAfee releases its public report entitled ‘Global Energy CyberAttacks: ‘Night Dragon’. We also detect expansion of attack targets to BioTechnology Sector

- Named by McAfee in January 2011 and investigated since early 2010
- Long-term targeted attack against major multi-national oil & gas and bio-technology companies
  - 7 confirmed victims, >dozen suspected and are being investigated
- Gigabytes of documents exfiltrated related to:
  - Sensitive oil/gas field bidding projects
  - Oil discoveries
  - Industrial control settings of SCADA systems
- Attribution to Chinese actors

OPERATION SHADY RAT

The Entire Western Economy is Owned



22

U.S. Federal Gov.	6
U.S. State Gov.	5
U.S. County Gov.	3
Canadian Gov.	2
South Korean Gov.	1
Vietnam Gov.	1
Taiwan Gov.	1
U.S. Gov. Contractor	1
United Nations	1
Indian Gov.	1

6

Construction/ Heavy Industry	3
Steel Industry	1
Energy	1
Solar Power	1

13

Electronics Industry	3
Computer Security	2
Information Technology	2
Satellite Communications	2
News Media	2
Information Services	1
Communications Technology	1

13

Defense Contractor	13

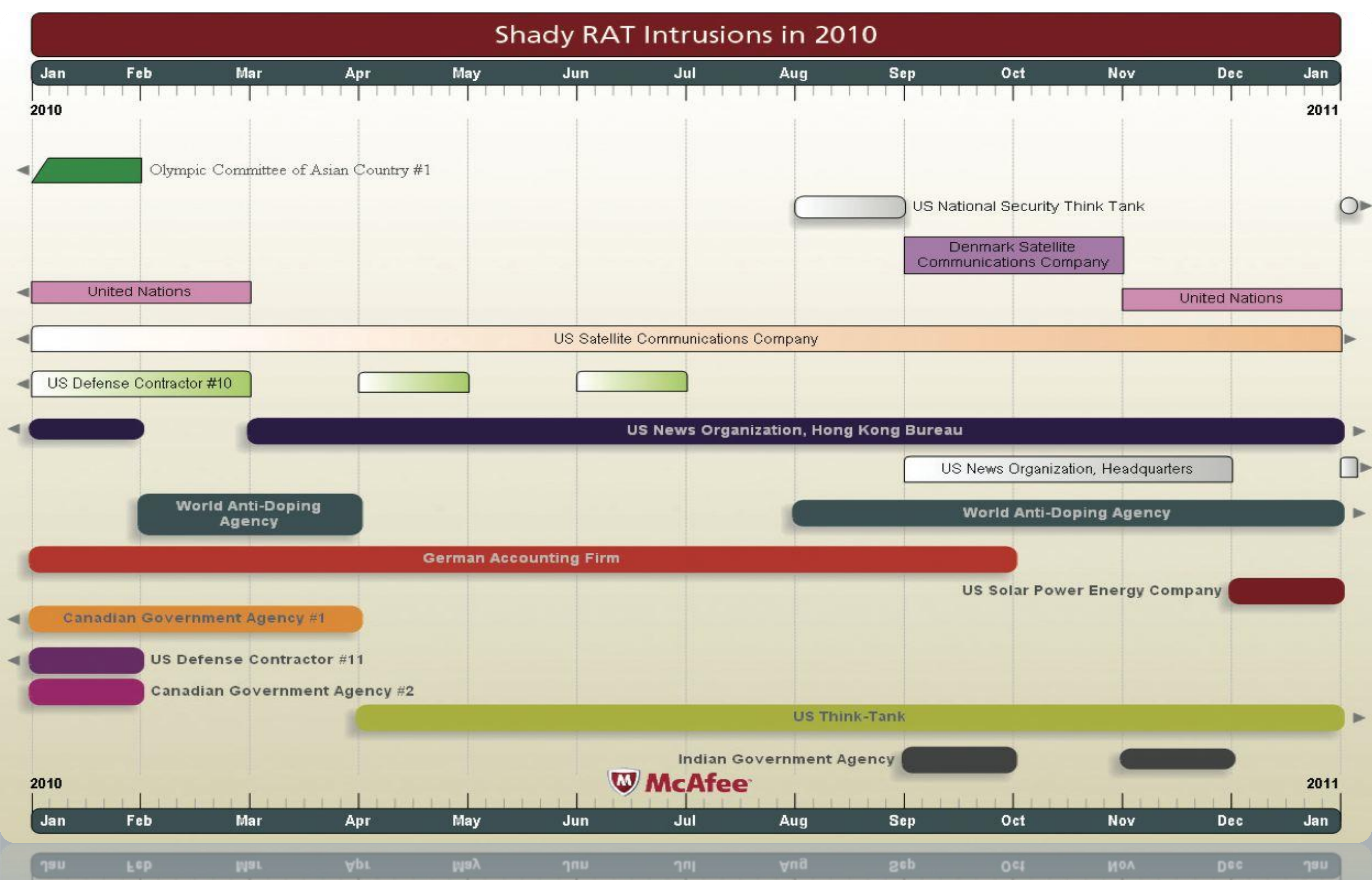
4

Real Estate	2
Accounting Industry	2
Agriculture	1
Insurance	1

12

International Sports	5
Economics/Trade	2
Think Tanks	2
International Government/ Economics/Trade	1
Political non-profit	1
U.S. National Security Non-profit	1

Operation Shady Rat



Upping the Game with Duqu?

Possibly the same group that coded Stuxnet

- Code base is closely related
  - Similar driver code used in injection techniques
  - Multiple encryption keys used
  - Rootkit Functionality
- Targeted Attacks reported in Iran, Sudan, England, US
  - Limited Reports: Austria, Hungary, Indonesia
- CA – Cmedia is in the same business district
  - Most likely generated rather than stolen

Different Goals and Functions

- Espionage
- Additional (sepperate) Keylogger Module
- No PLC functionality

Only this is interesting:

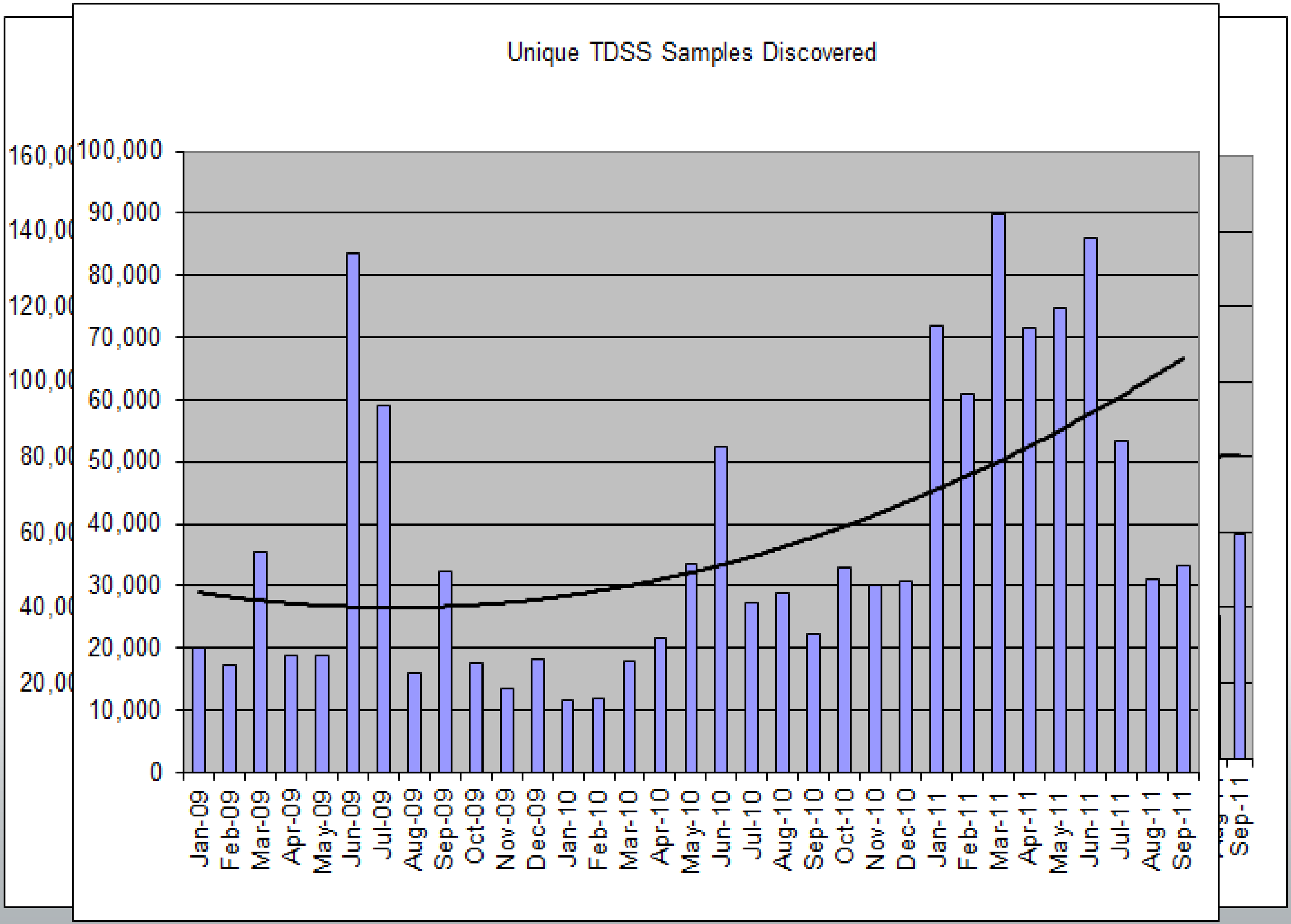
Possibly the same group that coded Stuxnet

- Code base is closely related
  - Similar driver code used in injection techniques
  - Multiple encryption keys used
  - Rootkit Functionality
- Targeted Attacks reported in Iran, Sudan, England, US
  - Limited Reports: Austria, Hungary, Indonesia
- CA – Cmedia is in the same business district
  - Most likely generated rather than stolen

Different Goals and Functions

- Espionage
- Additional (sepperate) Keylogger Module
- No PLC functionality

Increasing Use of Rootkit Technologies



BIOS Rootkits

Win32/Wador.A – A BIOS rootkit spreading in China

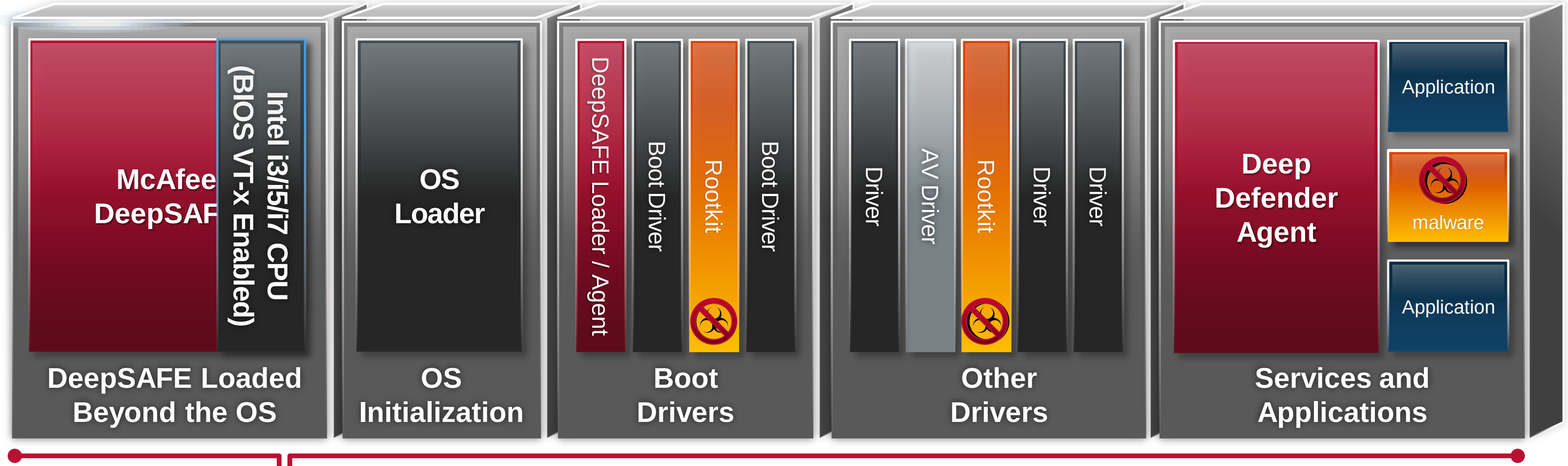
The BIOS rootkit is the most complex type of rootkit we have come across so far. It is hardware dependent, and an attacker must have extensive knowledge of the computer – including software and hardware – in order to create one. It comprises the following five components:

- BIOS ROM flasher
- Malicious BIOS ROM payload
- Infected MBR
- Infected WINLOGON.EXE/WININIT.EXE
- Protected malware code in track 0.

It is not easy to clean a computer infected with this malware, but there is some good news. First, after the destruction wreaked by CIH, many BIOS vendors started providing double BIOS in order to defend against this type of attack. Second, not many computers have AWARD BIOS installed nowadays, because more and more modern computers use EFI to interface between hardware and software. So the potential scope for this form of attack may not be very great.

Source: Virus Bulletin (October issue)

Technology Update—Stopping a Stealthy Rootkit



- Real-time kernel-level monitor of memory
- Identifies kernel-mode rootkits in real-time
- Prevents the drivers from loading
- DeepSAFE technology loads before the OS
- DeepSAFE technology informs Deep Defender of suspicious behavior

More stuff to read

- McAfee Security Journal 2011
  - http://www.mcafee.com/us/resources/reports/rp-security-journal-summer-2011.pdf
  - Featuring Chris Roberts, Jayson Street, David Kennedy
- McAfee Labs Q3 Quarterly Threats Report
  - To be released on the 22nd
- McAfee Labs Blog
  - http://blogs.mcafee.com/mcafee-labs
  - (We don‘t let marketing people touch it)
- Office of the National Counterintelligence Executive
  - http://www.ncix.gov/publications/reports/fecie_all/index.html
  - Report to Congress on Foreign Economic Collection and Industrial Espionage 2009-2011

McAfee®

An Intel Company

Toralv_Dirro@McAfee.com