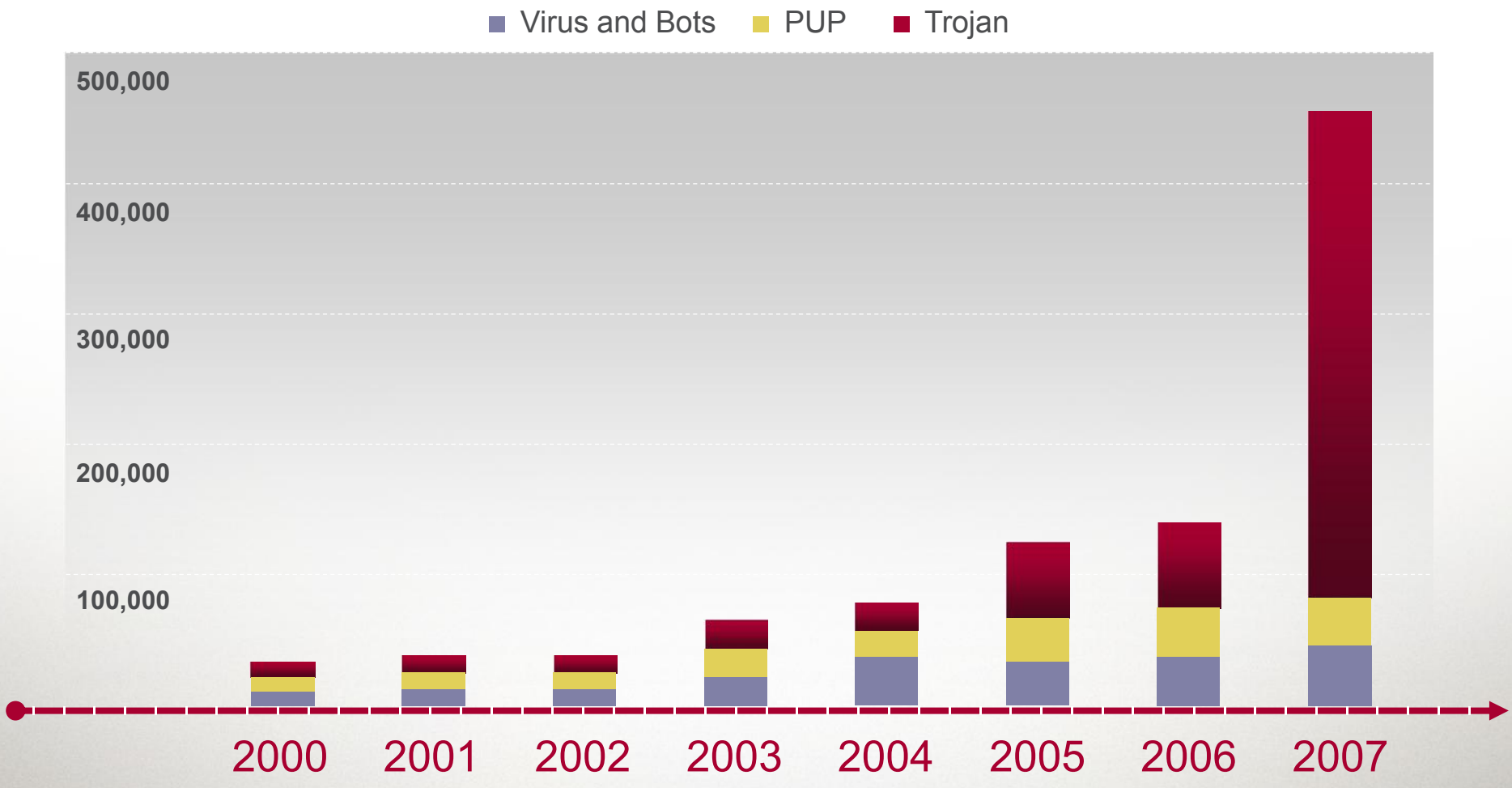
Evolving Threats, Evolving Technology

McAfee Labs Research

Toralv Dirro
McAfee Labs EMEA Security Strategist

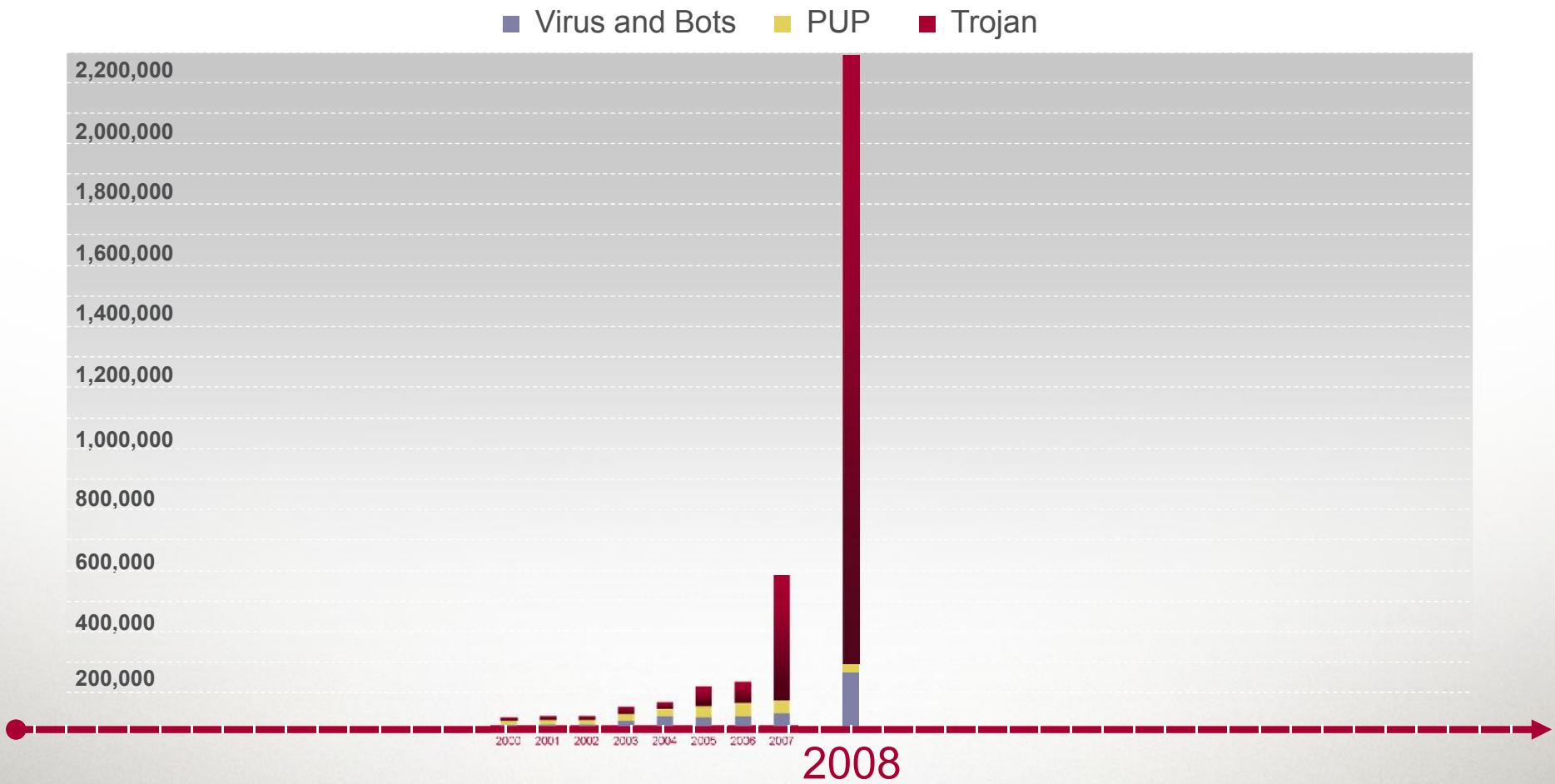
Cyber Crime Altering Threat Landscape



Malware Growth (Main Variations)

Source: McAfee Labs

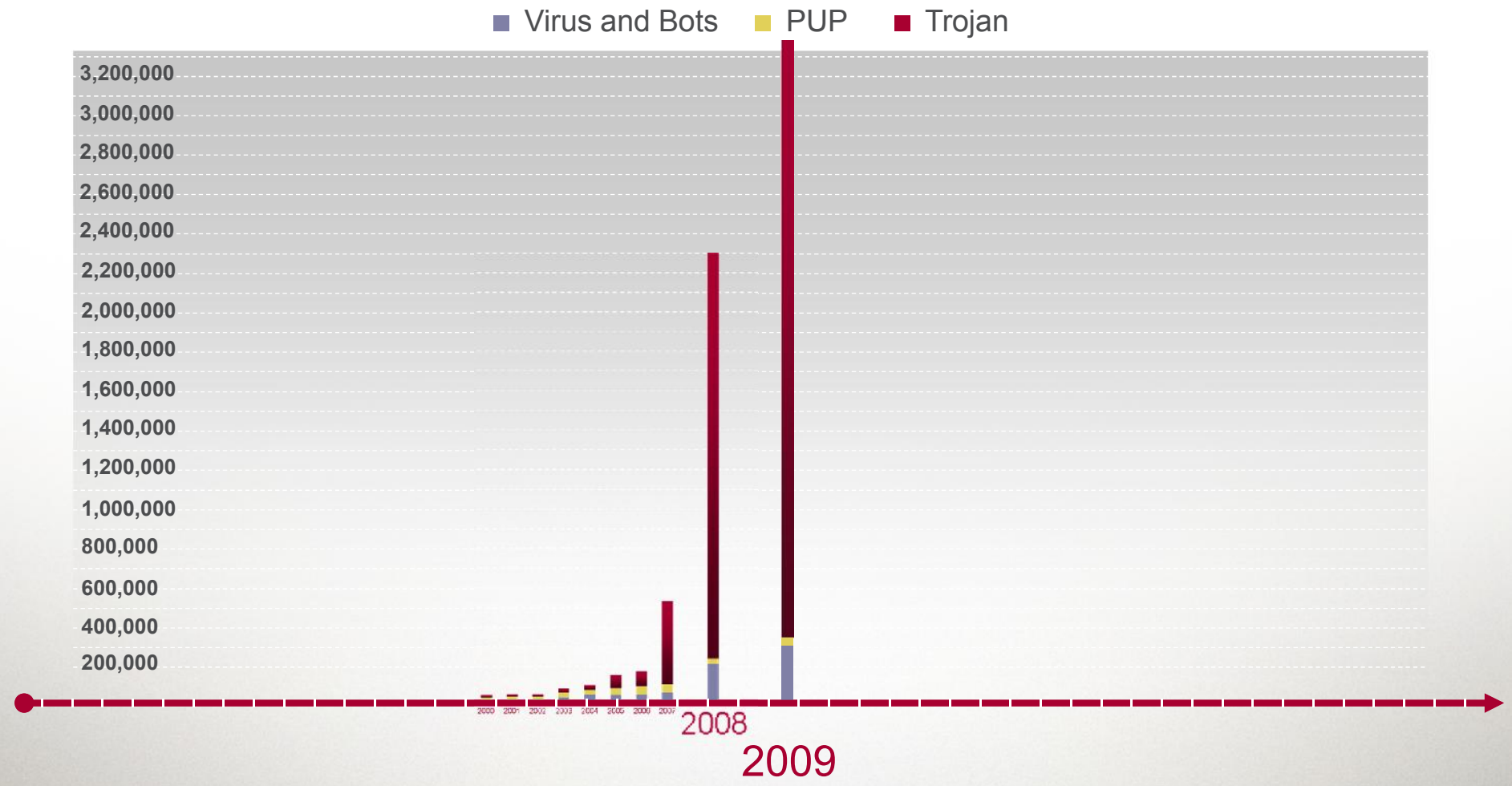
Cyber Crime Altering Threat Landscape



Malware Growth (Main Variations)

Source: McAfee Labs

Cyber Crime Altering Threat Landscape

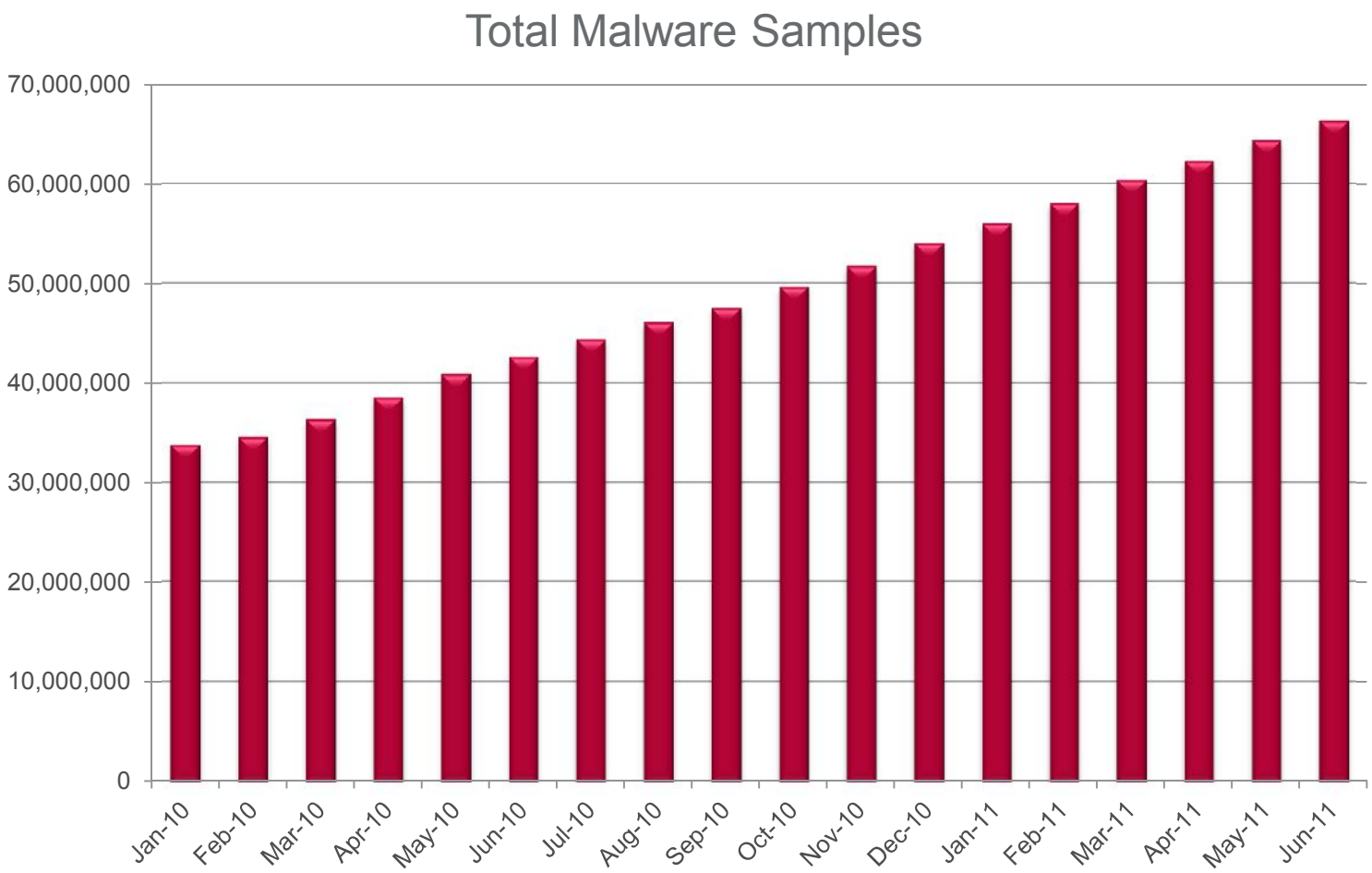


Malware Growth (Main Variations)

Source: McAfee Labs

Key Trend: Malware Growth Continues

The growth in the number of new malware continues unabated. McAfee Labs identifies approximately 55,000 pieces of new malware each day. At its current pace the total number of malware samples in the McAfee "zoo" will reach 75 million by the end of 2011 For the first six months of 2011 new malware detections increased 22% over same period in 2010.



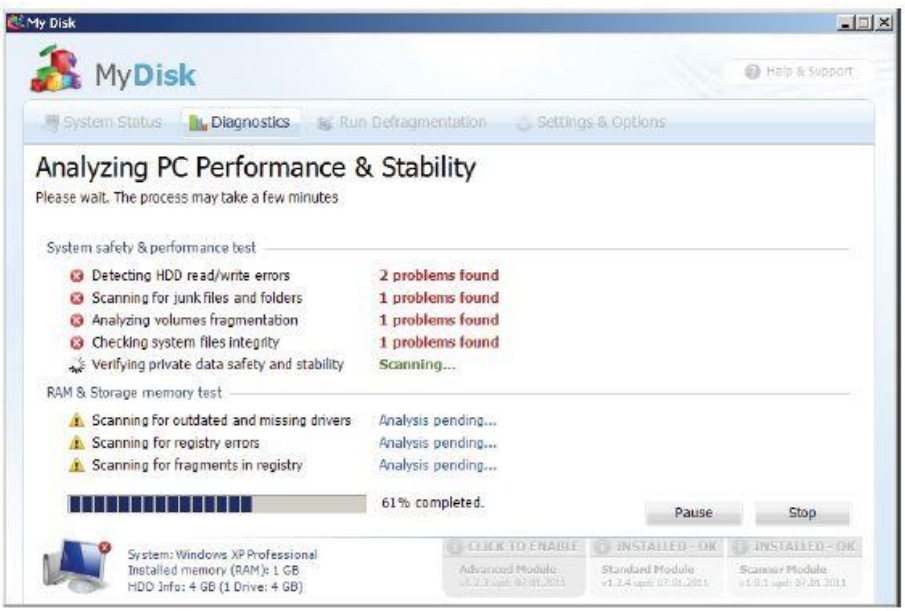
The Malware Market

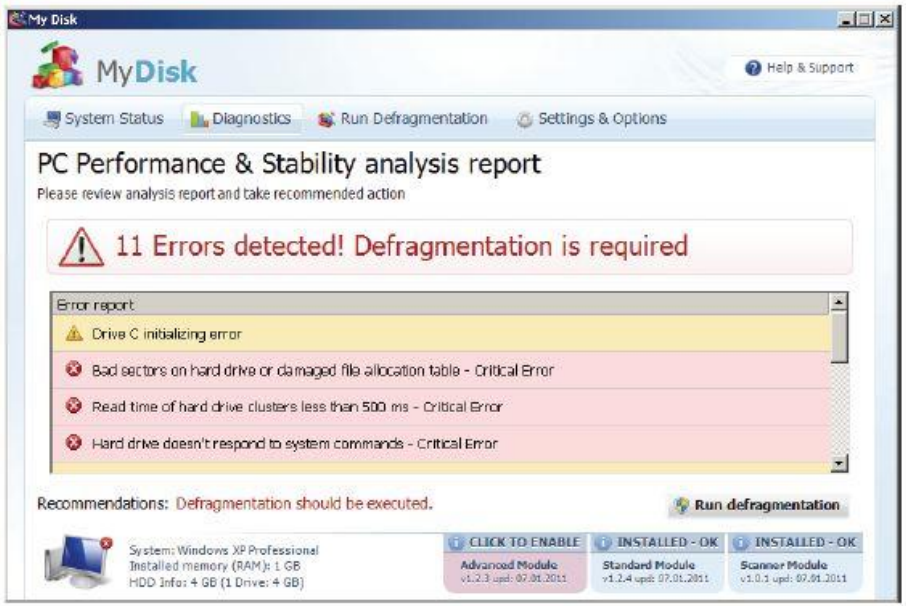
Trojan and Exploit Kits easily available

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

Fake Malware

Cybercriminals and scammers have long used fake security products—known as fake or rogue AV—to scam users out of their money. Now, rogue applications are shifting from security products toward system and disk utilities.





FOCUS 09
Anatomy of a scareware company

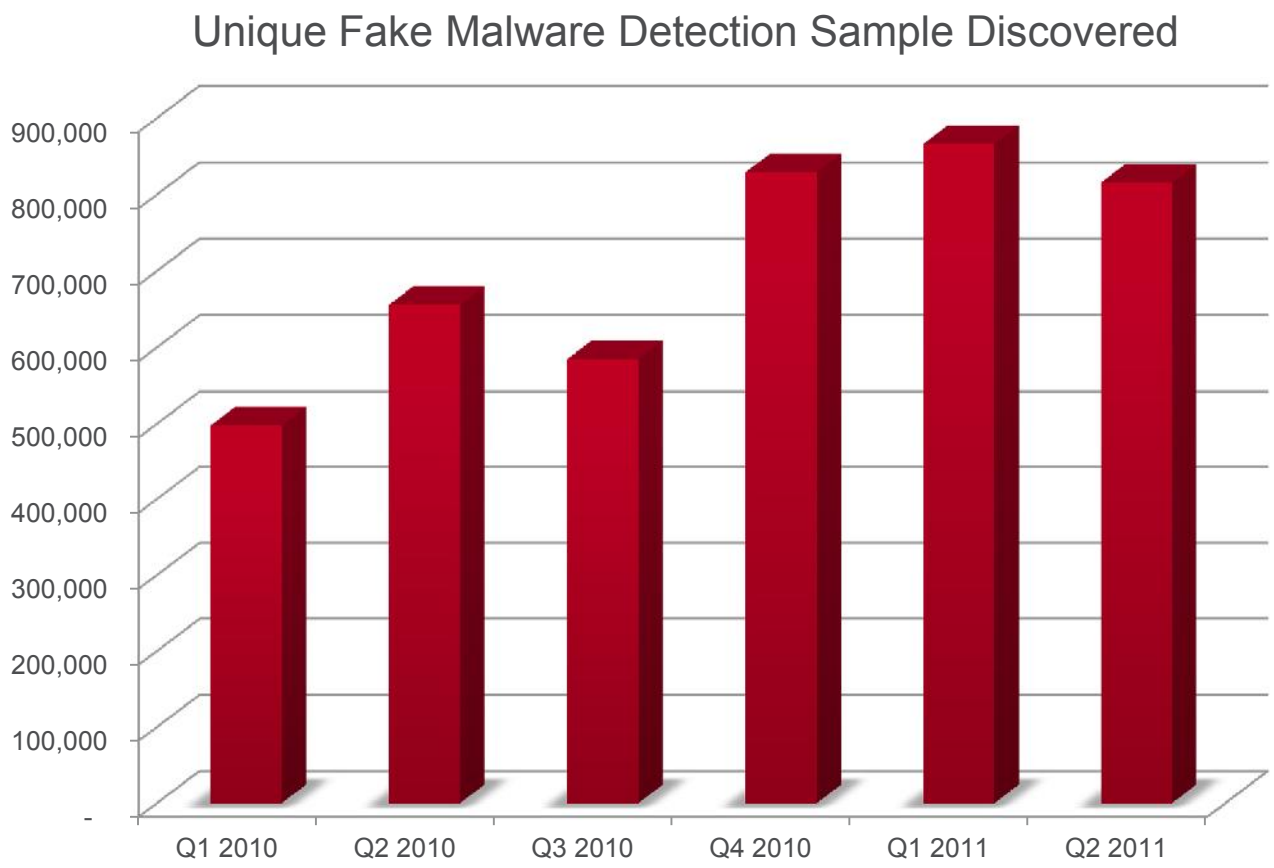
Using more than 63 gigabytes of information culled from querying the company's own portal servers and other publicly available data, McAfee Labs Researchers, unearthed some astonishing operational details including the following:

- 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

Decline in Fake Malware Detection Software

Fake anti-virus, also known as bogus or rogue security software, declined modestly following two quarters of growth. While this has historically been a very profitable scam, this decline reflects the issues perpetrators started to have in Q2 accessing transaction clearing infrastructure.

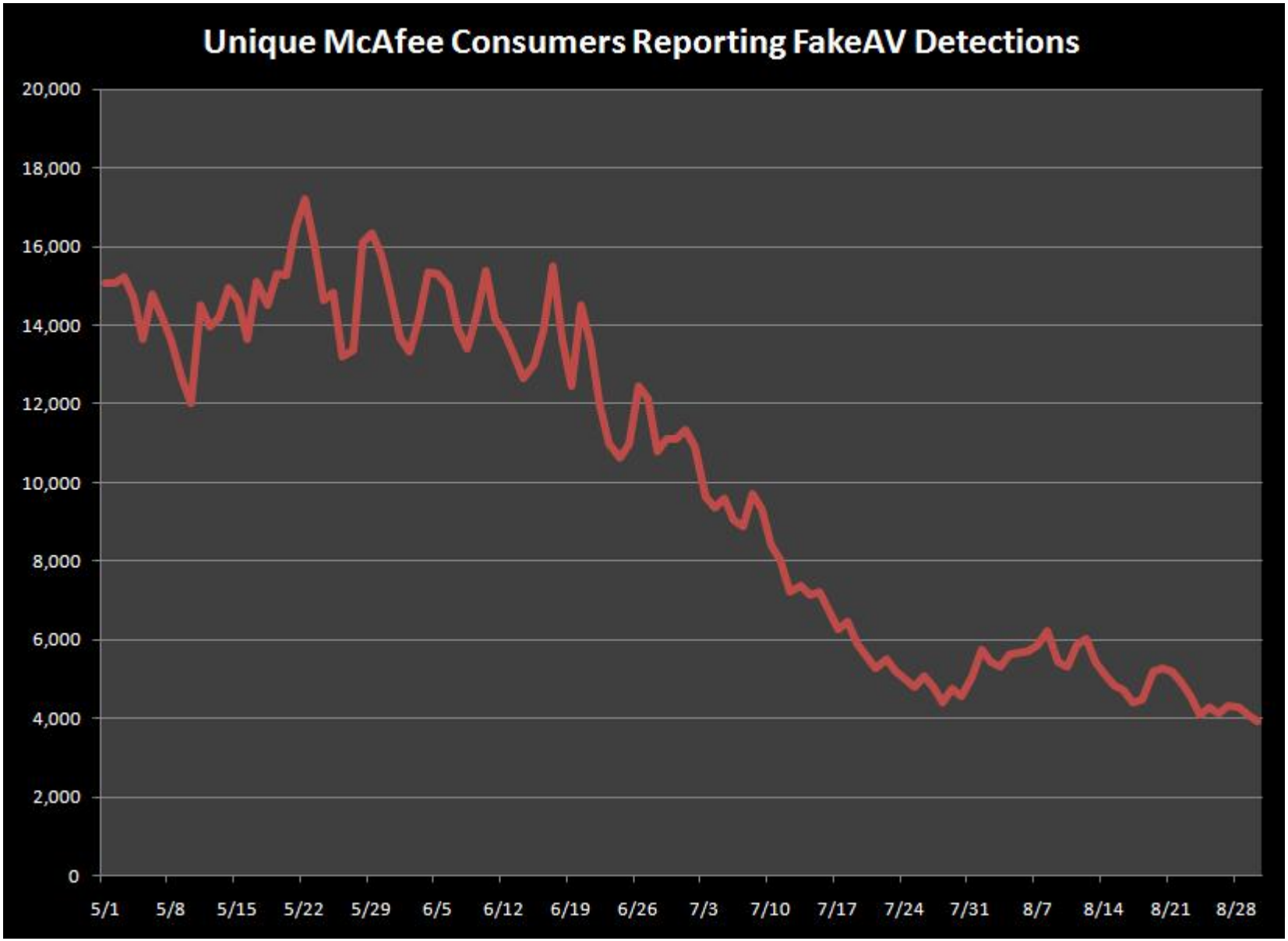


And then the money stopped flowing...

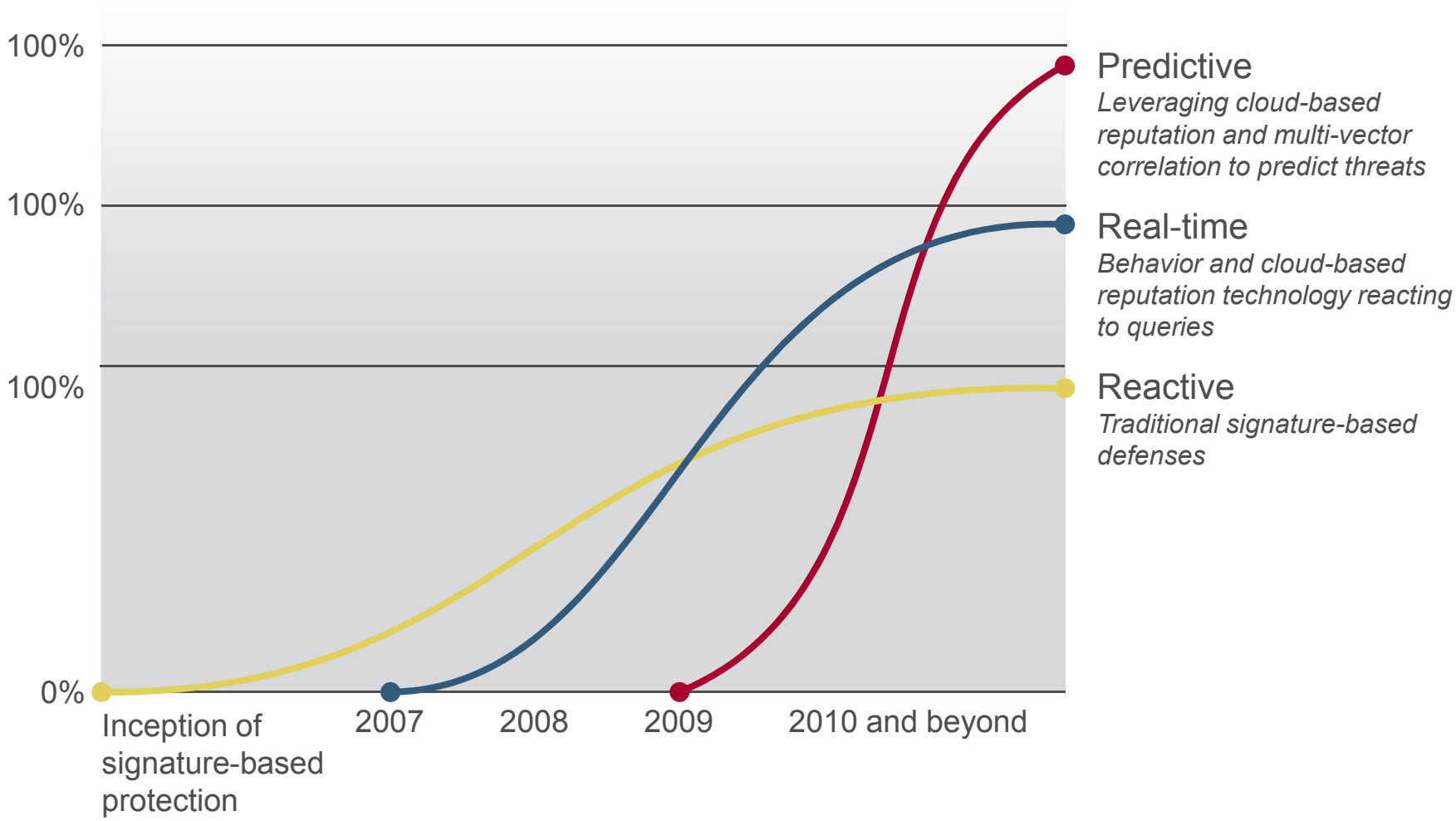
- Several companies in the Fake Malware (aka FakeAlert, Fake-AV, Scareware) market experienced difficulties to process credit card transactions of their victims

- Subsequently their Affiliates stopped installing/distributing

And then the money stopped flowing...



Evolution of Threat Detection



Threat Intelligence Feeds

Correlation of various Reputation Feeds

McAfee

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**

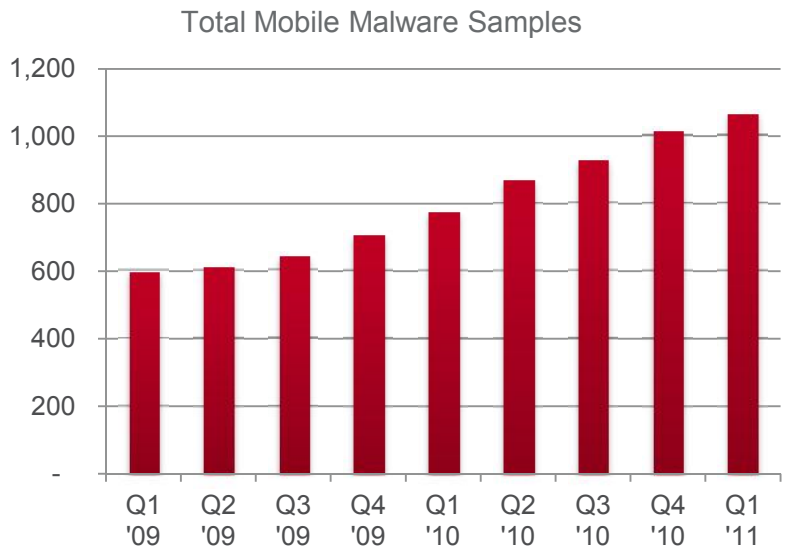
Nodes

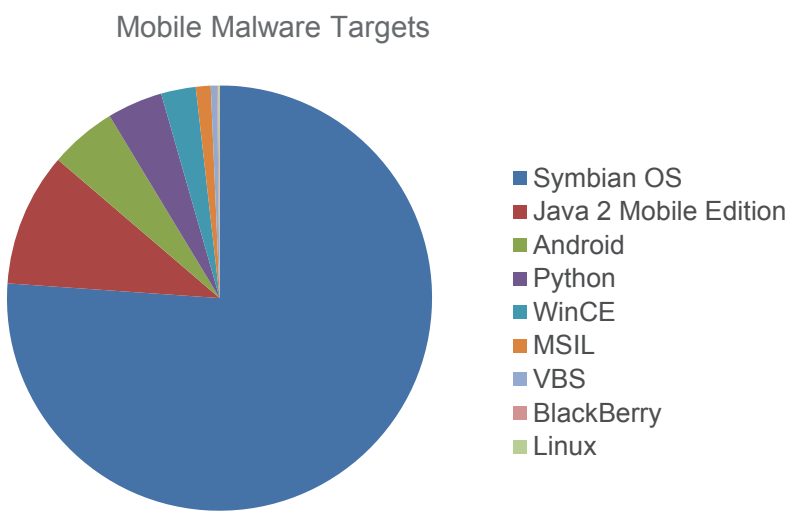
- Malware: 40M Endpoints
- Email: 30M Nodes
- Web: 45M Endpoint and Gateway Users
- Intrusions: 4M Nodes
- **100+ MILLION NODES, 120 COUNTRIES**

Q1:
Android 3rd Most Popular Mobile Target

Overall mobile malware activity growth slowed to 5% quarter over quarter, but there was a marked increase in the activity on the Android platform, which moved from the #5 most popular target to #3.

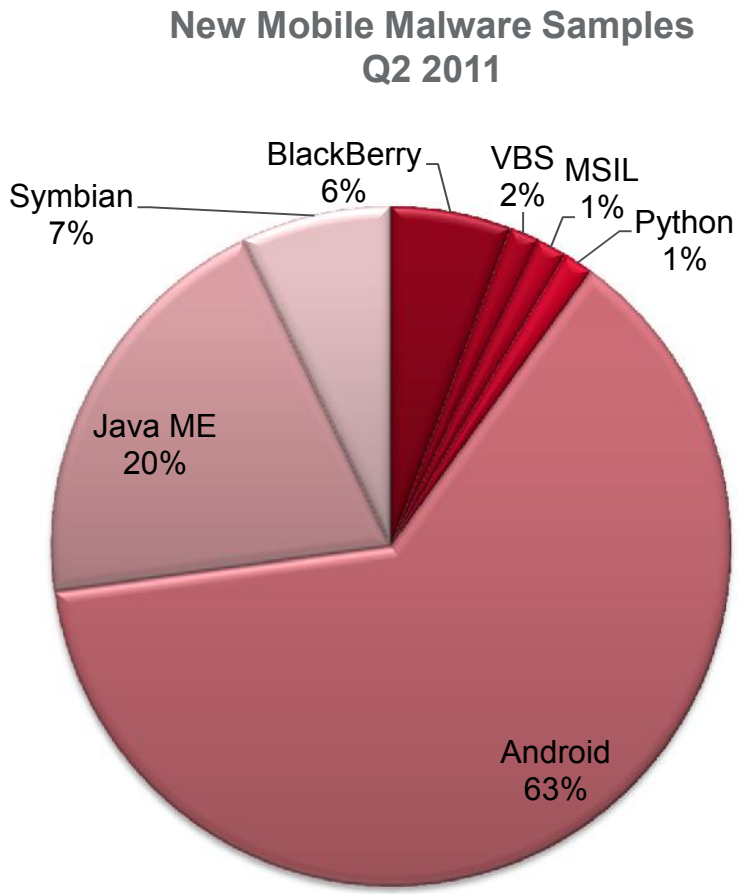
The mobile attack strategies are starting to mirror the approaches historically used to attack PC operating systems. A maliciously altered application obtains root access and then “connects” the device to a botnet-like command center, which issues subsequent instructions to extract data from the device or (over time) extend the attack to other devices.





Q2:
Android Now the #1 New Mobile Mobile Target

While Symbian remains the most attacked mobile platform in terms of total malware samples, Android has emerged as the platform experiencing the largest number of new attacks. No IOS targeted attacks were found in the wild in Q2.



Mobile Crimeware

"Geinimi": A new Trojan affecting Android devices has recently emerged in China

Geinimi is the first Android malware in the wild that displays botnet-like capabilities. Once the malware is installed on a user's phone, it has the potential to receive commands from a remote server that allow the owner of that server to control the phone.

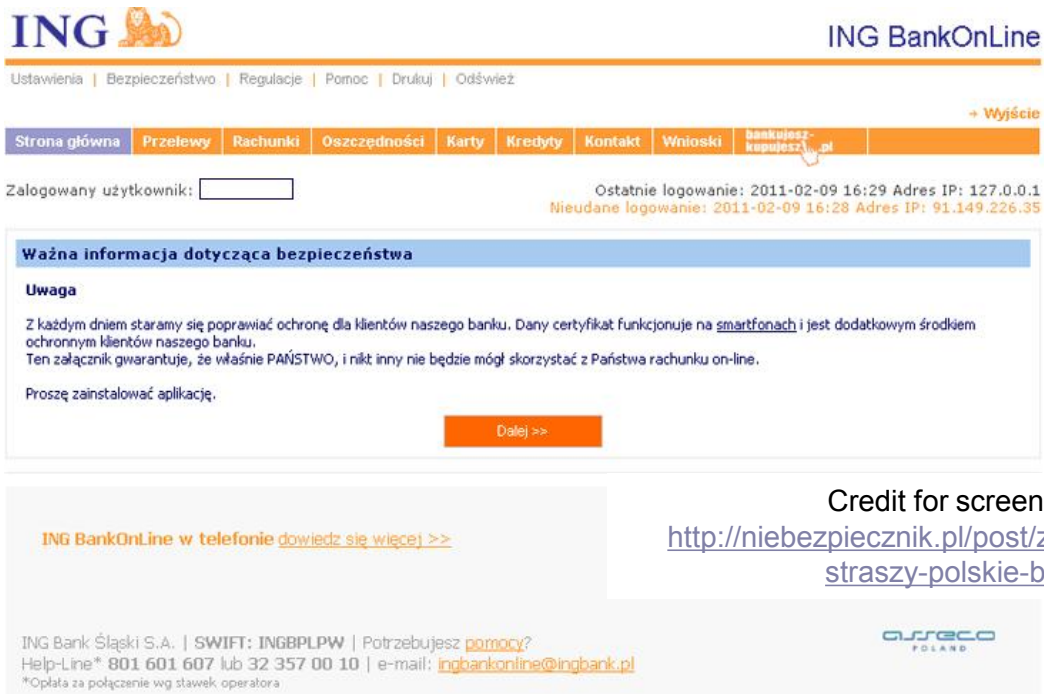
- Send location coordinates (fine location)
- Send device identifiers (IMEI and IMSI)
- Download and prompt the user to install an app
- Prompt the user to uninstall an app
- Enumerate and send a list of installed apps to the server
- Read and collect SMS messages
- Send and delete selected SMS messages
- Pull all contact information and send it to a remote server (number, name, the time they were last contacted)
- Place a phone call
- Silently download files
- Launch a web browser with a specific URL

Credit for screenshot: http://m.hauri.co.kr/info/virus_view.html?intSeq=1881&code=4

Mobile Crimeware

A variant of the ZeuS trojan is targeting the mobile phone based, two-factor authentication used by Polish ING Bank Slaski

Polish Security Consultant, Piotr Konieczny reported that operators of the Zeus botnet are attempting to reach into the mobile sphere with two new variants targeting users on Window Mobile and Symbian phones. "Zeus in the Mobile" (or Zitmo), are again attempting to authenticate bank transactions by intercepting the mTan authentication code sent to mobile devices.

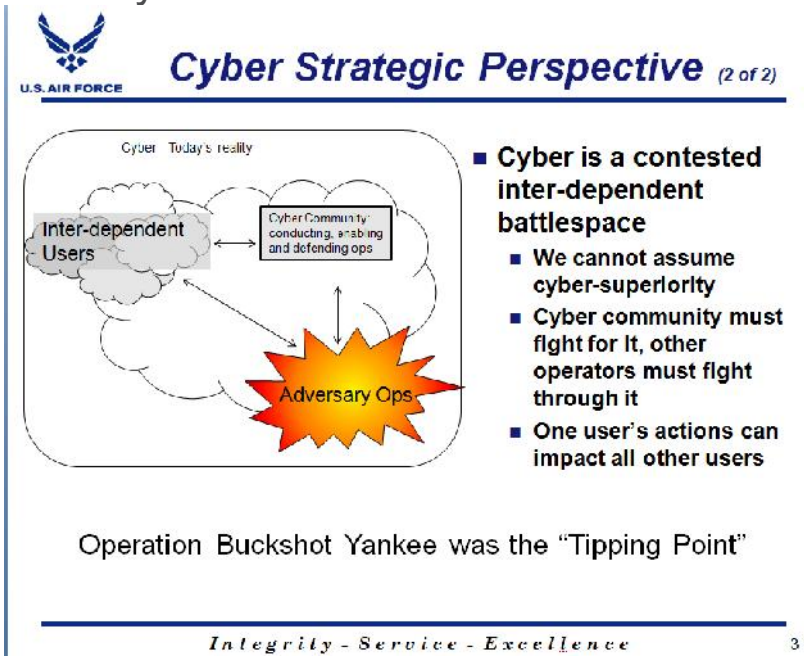


Credit for screenshot: http://niebezpiecznik.pl/post/zeus-straszy-polskie-banki/

An mTAN (mobile Transaction Authentication Number) is used by some online banking services in Europe to authorize financial transactions by sending an SMS to the customer's phone. TANs were put in to add an extra layer of security in order to complete large transactions. It is believed that Zitmo was developed to circumvent this added layer of security implemented by the banks.

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

“Night Dragon” Global Energy Cyberattacks

Late 2009

“Night Dragon” commences

Spring 2010

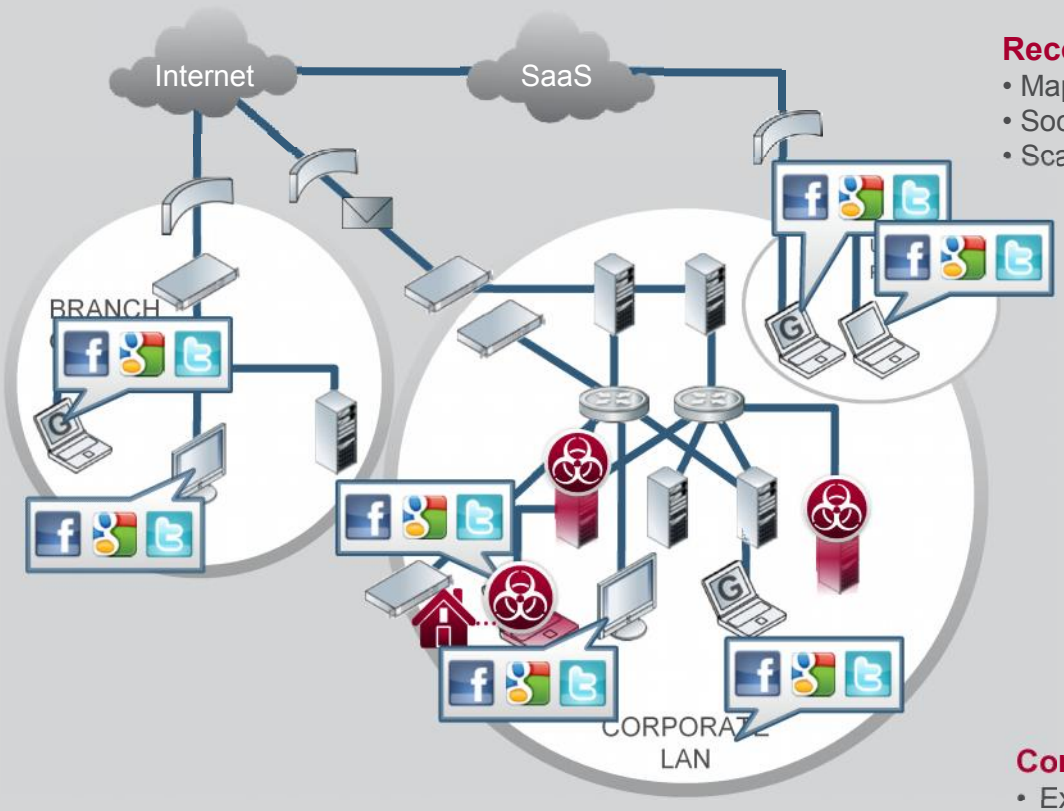
Attack is detected and McAfee starts helping affected companies

Jan 2011

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

- Named by McAfee in January 2011 and investigated since early 2010
- Long-term, targeted attack against global oil, energy and petrochemical companies
  - 5 confirmed victims, up to a dozen suspected
  - Gigabytes of documents related to oil/gas field bidding projects, oil discoveries and industrial control (SCADA) data compromised
- C&C servers and source attack traffic coming from IP addresses in China, Ireland, Netherlands

Patterns Indicative of Night Dragon & Many APTs



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

More recent examples

“The EU has reported a "serious" cyber attack on the Commission and External Action Service on the eve of a summit in Brussels, a spokesman told the BBC.”

[...]

„Details were not given but other sources compared the attack to a recent assault on France's finance ministry.” [1]

"the parliamentary computers of at least 10 federal ministers – including the Prime Minister, Foreign Minister and Defence Minister – are suspected of being hacked into in a major breach of national security."

"It is believed that several thousand emails may have been accessed", notes the paper, adding that the espionage may have been going on for more than a month. [2]

[1] Source: http://www.bbc.co.uk/news/world-europe-12840941

[2] Source: http://www.infosecurity-magazine.com/view/16940/australian-pms-emails-hacked/

And even more....

RSA

Lockheed Martin

(http://www.lockheedmartin.com/news/press_releases/2011/0528hq-secuirty.html)

Sony

Hyundai Capital Co

PBS

Several big US, European and Asian Companies/Financial Institutions

(not identified to the general public)

5 targeted attacks a day against German government systems/users

(http://www.bundestag.de/presse/hib/2011_05/2011_201/08.html)

The Chosen Few?

- Successful Attacks are hardly reported at all
  - Neither APT nor other Targeted Attacks

- It‘s fairly safe to say if
  - You possess information
  - Or have access to
- That could be of political or economic benefit for another
  - Government or
  - Competitor
- Chances are you‘re under attack

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**

SCADA, definition

- It's not a Brazilian dance. ☺

- Supervisory Control And Data Acquisition
  - ✓Large-scale, distributed remote management system for measures and controls
  - ✓Transmits and distributes critical liquids and services: water, gas, electricity, chemical products, traffic signals, etc.

  - ✓But also, in a wider sense, the industrial computer system and its local network, used within many SMBs for their production activity.

Many thanks to the French CLUSIF association which agree we use their data for this presentation

A specific context, a necessary adaptation for security systems

SECURITY TOPIC	INFORMATION TECHNOLOGY	CONTROL SYSTEMS
Anti-virus & Mobile Code Counterfeasures	Common & widely used	Uncommon and difficult to deploy
Support Technology Lifetime	3-5 Years	Up to 20 years
Outsourcing	Common & widely Used	Rarely Used
Application of Patches	Regular/Scheduled	Slow (Vendor specific)
Change Management	Regular/Scheduled	Legacy based – unsuitable for modern security
Time Critical Content	Delays are generally accepted	Critical due to safety
Availability	Delays are generally accepted	24x7x365 (continuous)
Security Awareness	Good in both private and public sector	Generally poor regarding cyber security
Security Testing/Audit	Scheduled and mandated	Occasional testing for outages
Physical Security	Secure	Very good but often remote and unmanned

(Source: INL Critical Infrastructure Protection Center, 2007)

Questions? More Info?

- Read the McAfee Labs Security Blog
  - http://blogs.mcafee.com/mcafee-labs
- Listen to the AudioParasitics Podcast
  - http://www.audioparasitics.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®