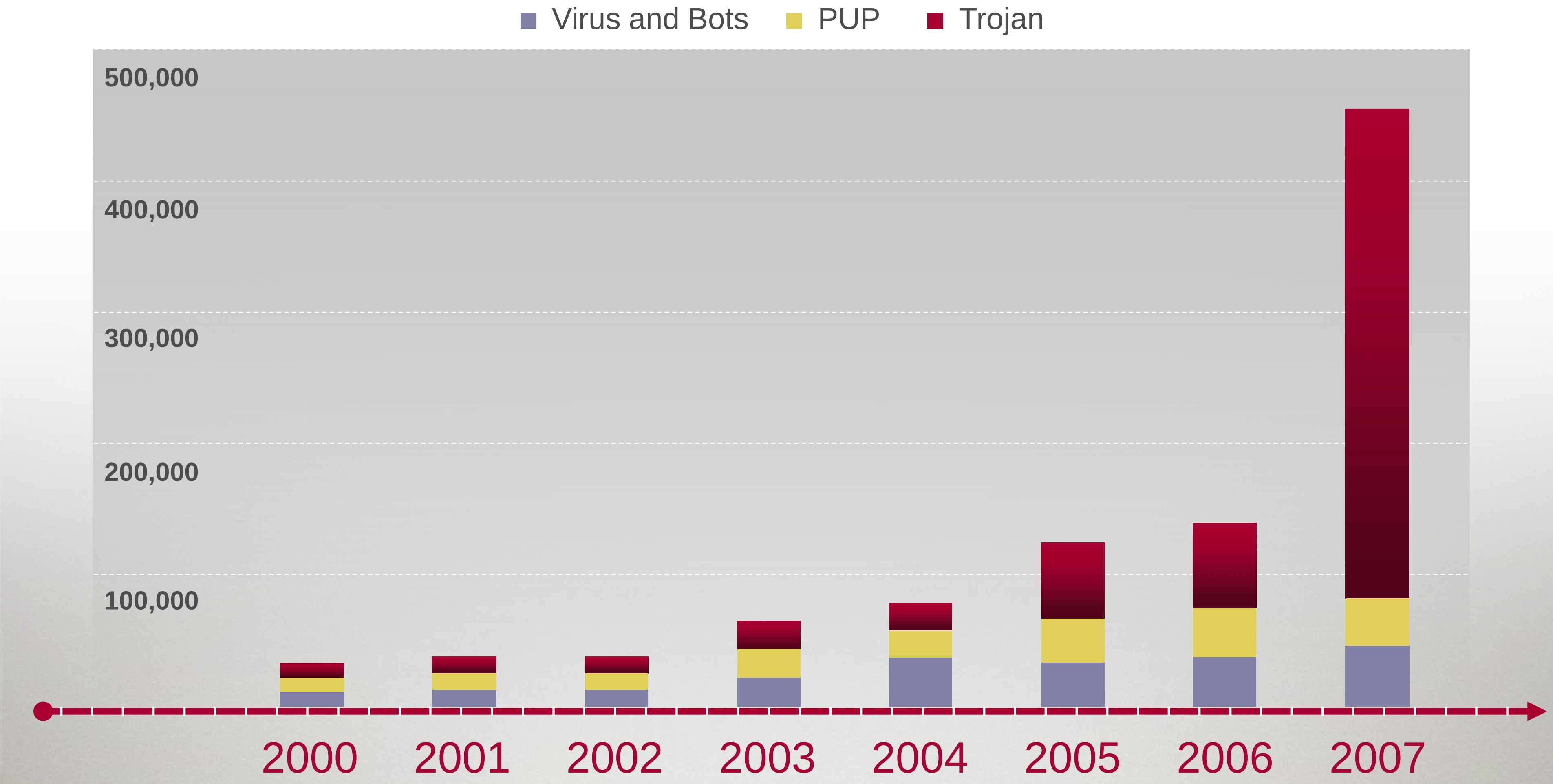
Malicious World

McAfee Labs Research

Toralv Dirro
McAfee Labs EMEA Security Strategist

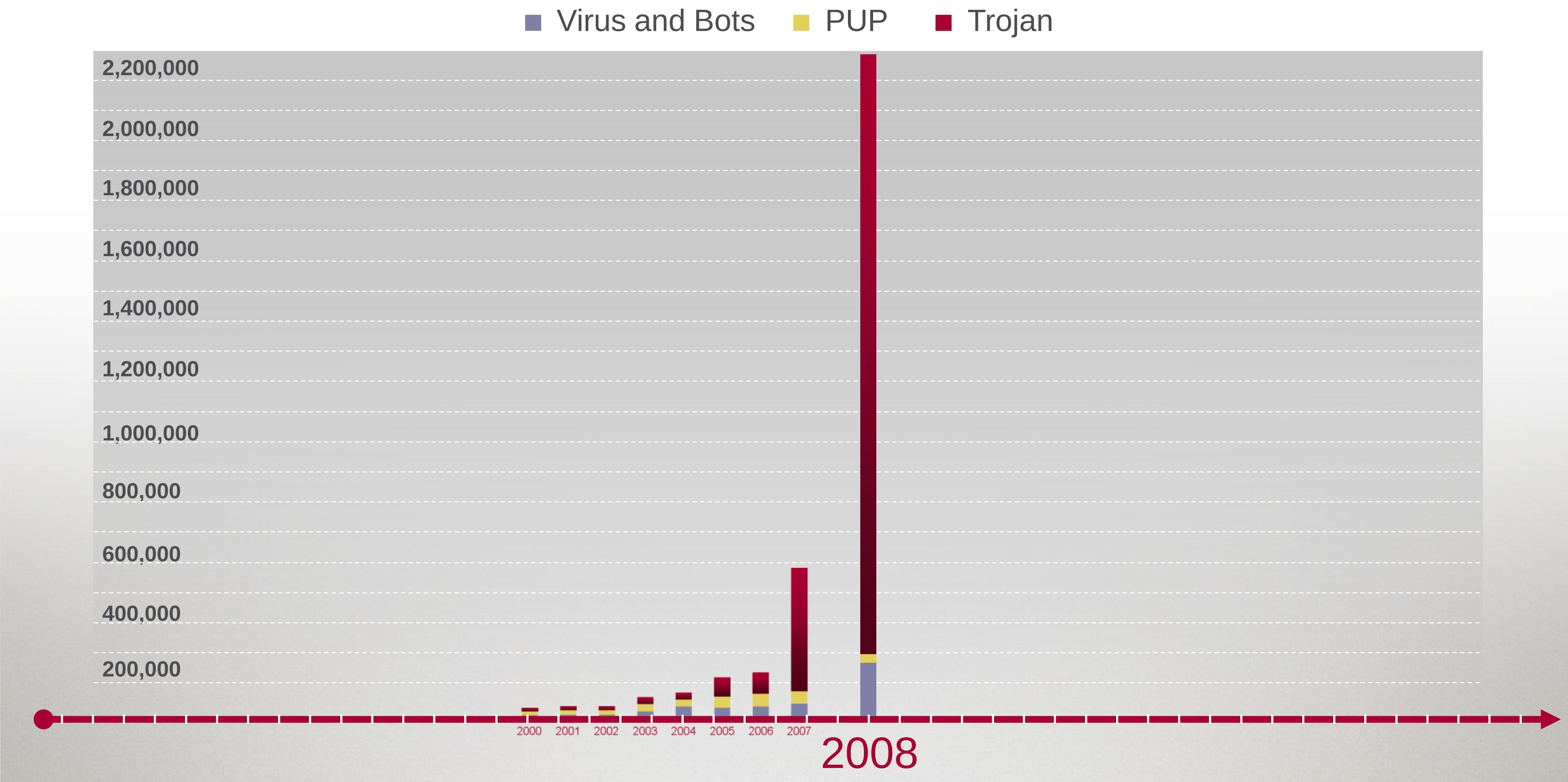
Cyber Crime Altering Threat Landscape



Malware Growth (Main Variations)

Source: McAfee Labs

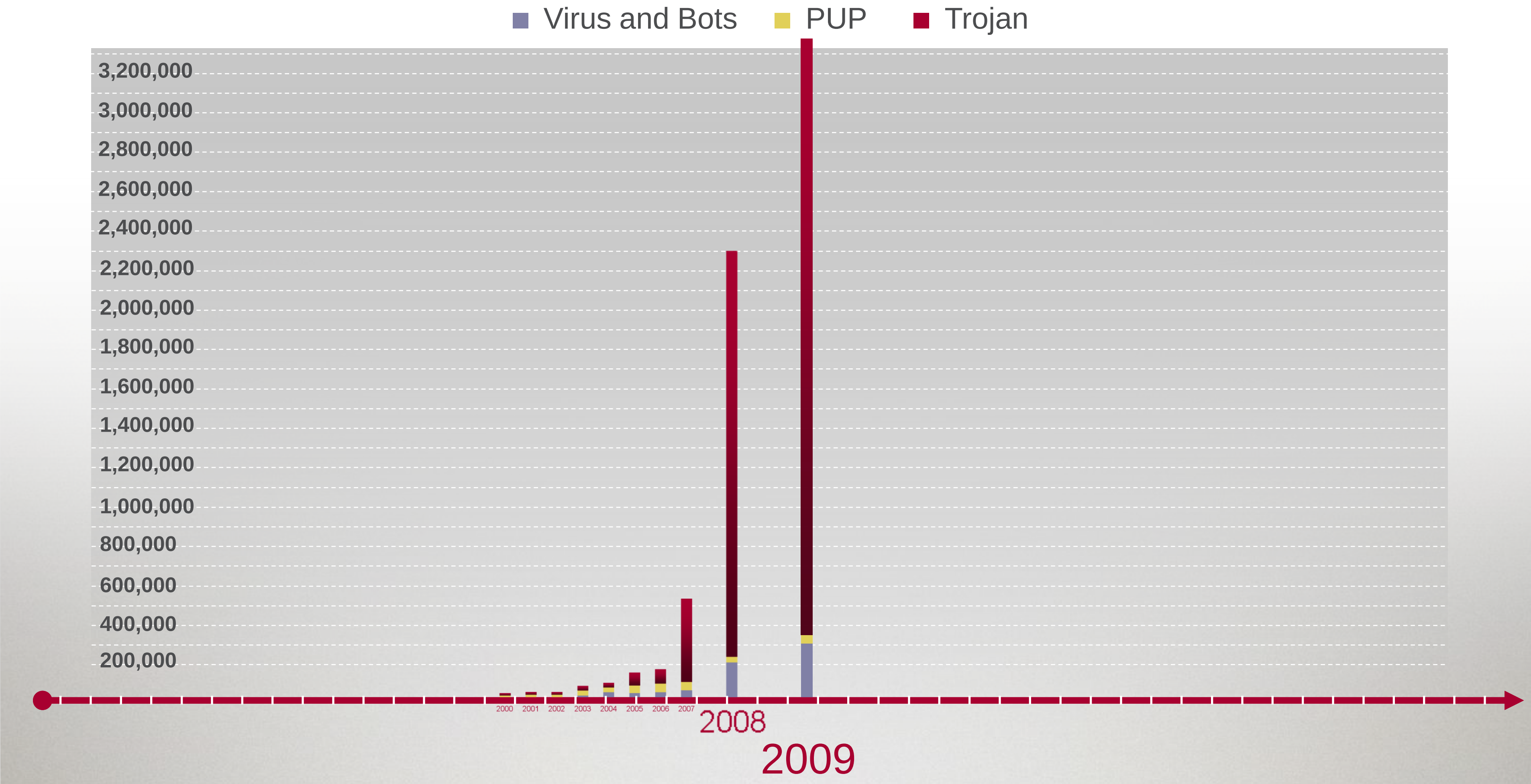
Cyber Crime Altering Threat Landscape



Malware Growth (Main Variations)

Source: McAfee Labs

Cyber Crime Altering Threat Landscape

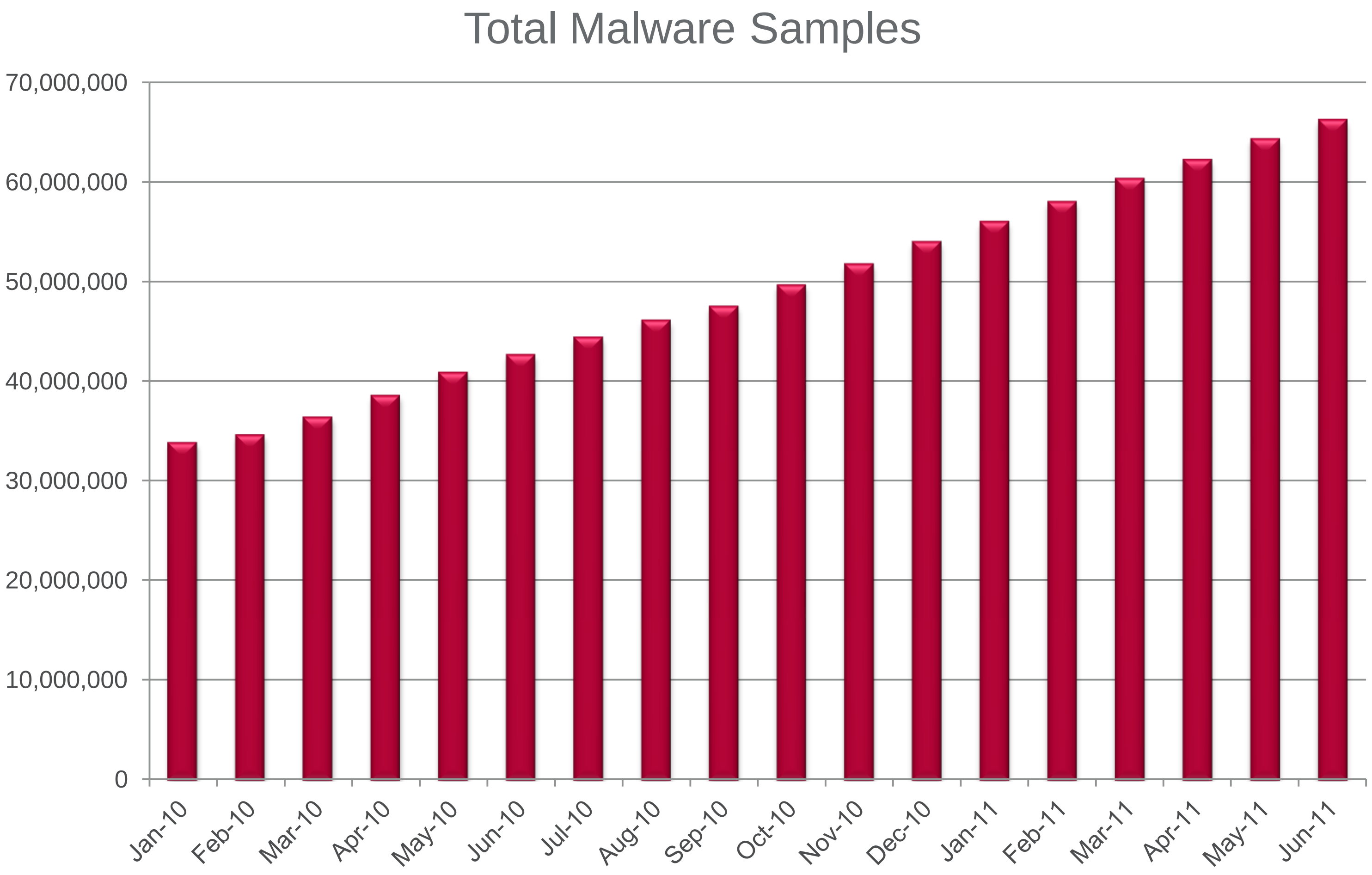


Malware Growth (Main Variations)

Source: McAfee Labs

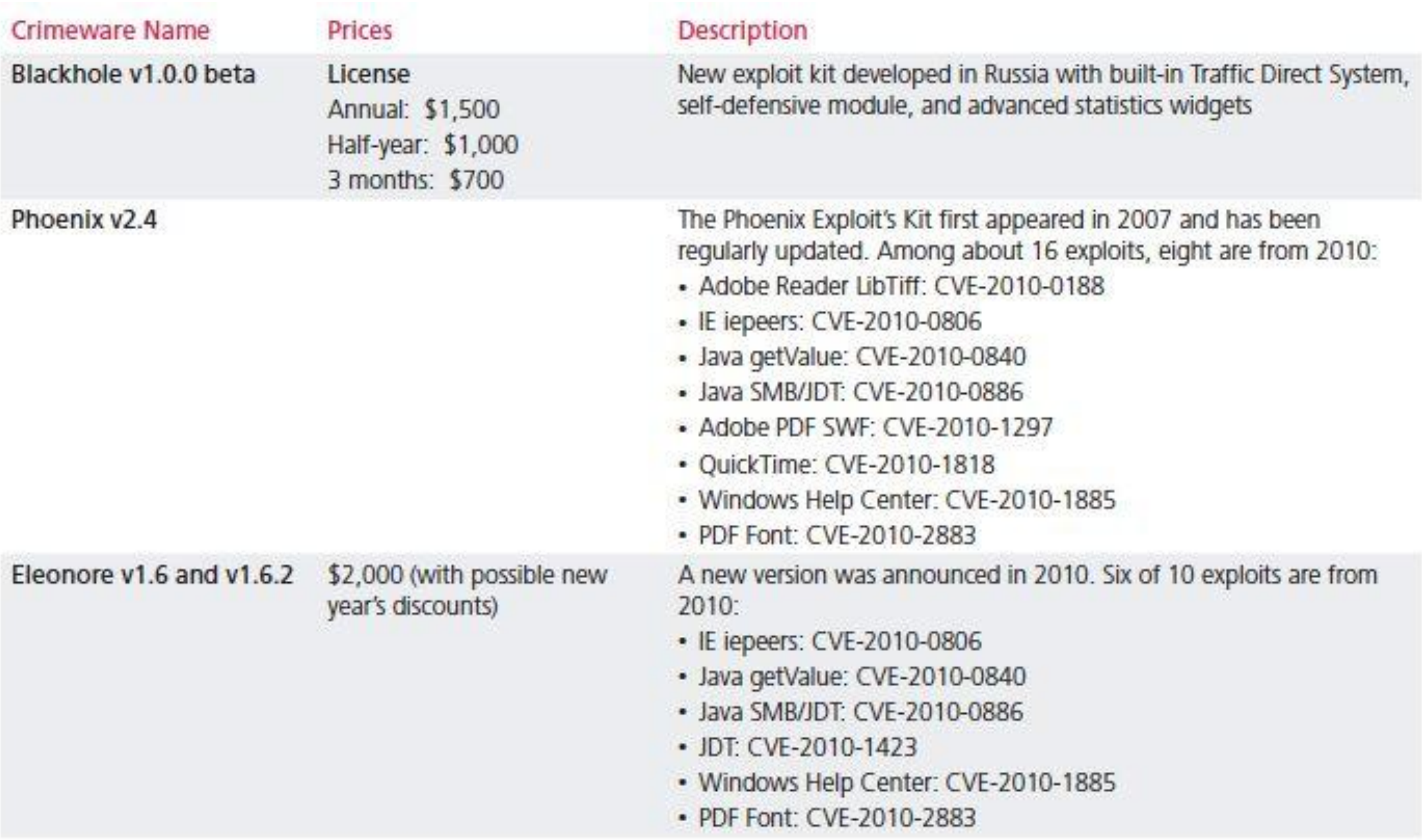
Key Trend: Malware Growth Continues

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

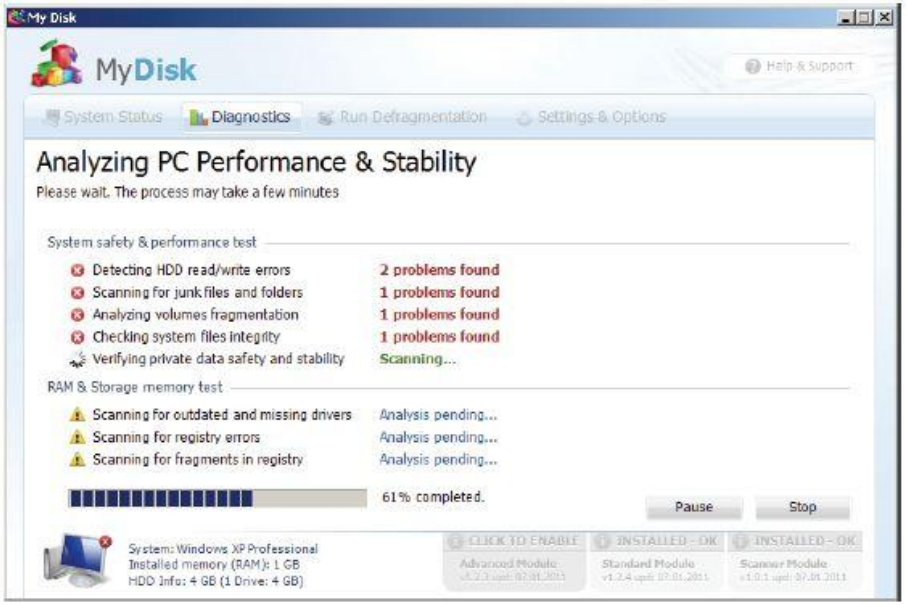
Trojan and Exploit Kits easily available



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.



Analyzing PC Performance & Stability

Please wait. The process may take a few minutes

System safety & performance test

- Detecting HDD read/write errors — 2 problems found
- Scanning for junk files and folders — 1 problems found
- Analyzing volumes fragmentation — 1 problems found
- Checking system files integrity — 1 problems found
- Verifying private data safety and stability — Scanning...

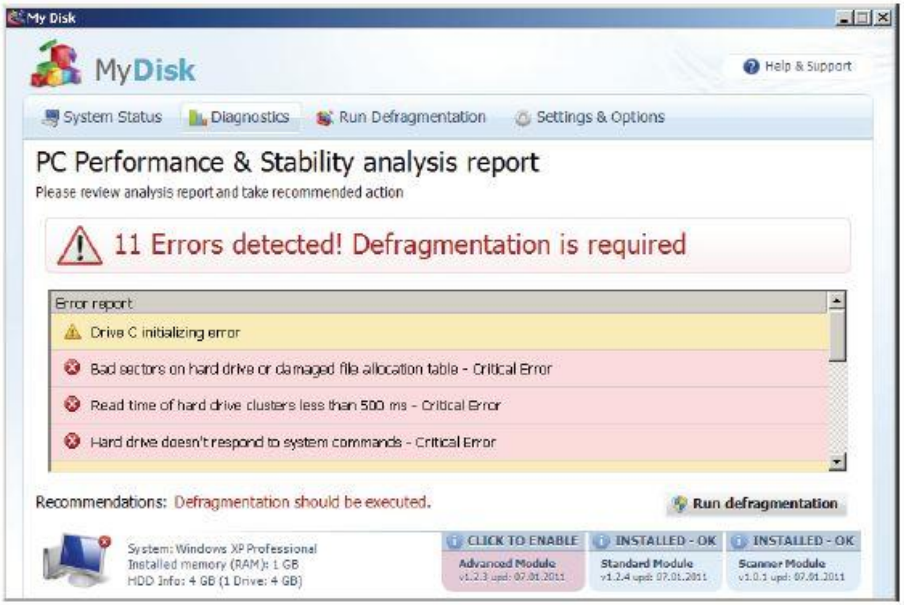
RAM & Storage memory test

- Scanning for outdated and missing drivers — Analysis pending...
- Scanning for registry errors — Analysis pending...
- Scanning for fragments in registry — Analysis pending...

61% completed.

System: Windows XP Professional
Installed memory (RAM): 1 GB
HDD Info: 4 GB (1 Drive: 4 GB)

Advanced Module v1.2.3 upd: 07.01.2011 | Standard Module v1.2.4 upd: 07.01.2011 | Scanner Module v1.0.1 upd: 07.01.2011



PC Performance & Stability analysis report

Please review analysis report and take recommended action

11 Errors detected! Defragmentation is required

Error report

- Drive C initializing error
- Bad sectors on hard drive or damaged file allocation table - Critical Error
- Read time of hard drive clusters less than 500 ms - Critical Error
- Hard drive doesn't respond to system commands - Critical Error

Recommendations: Defragmentation should be executed.

System: Windows XP Professional
Installed memory (RAM): 1 GB
HDD Info: 4 GB (1 Drive: 4 GB)

Advanced Module v1.2.3 upd: 07.01.2011 | Standard Module v1.2.4 upd: 07.01.2011 | Scanner Module v1.0.1 upd: 07.01.2011

FOCUS 09
Anatomy of a scareware company

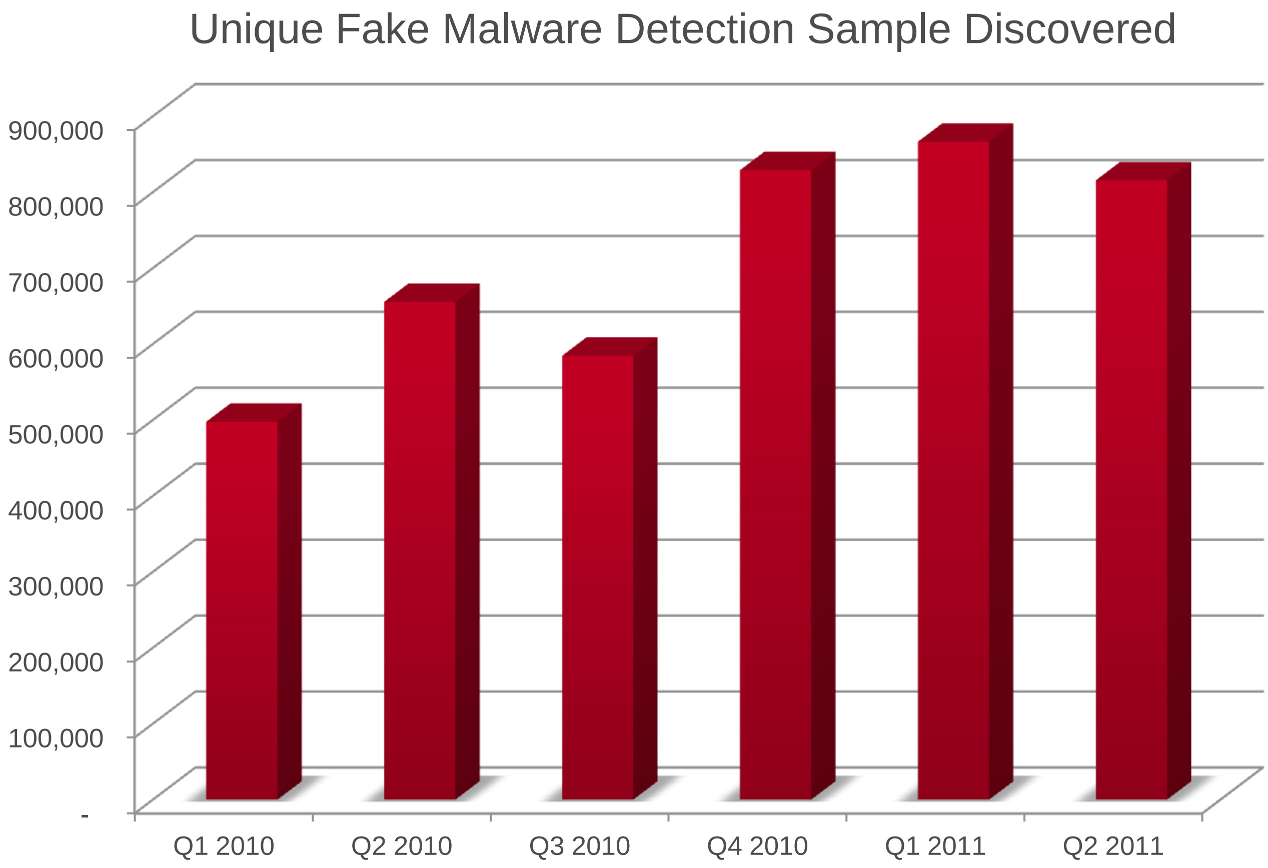
Using more than 63 gigabytes of information culled from querying the company's own portal servers and other publicly available data, McAfee Labs Researchers, unearthed some astonishing operational details including the following:

- 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.

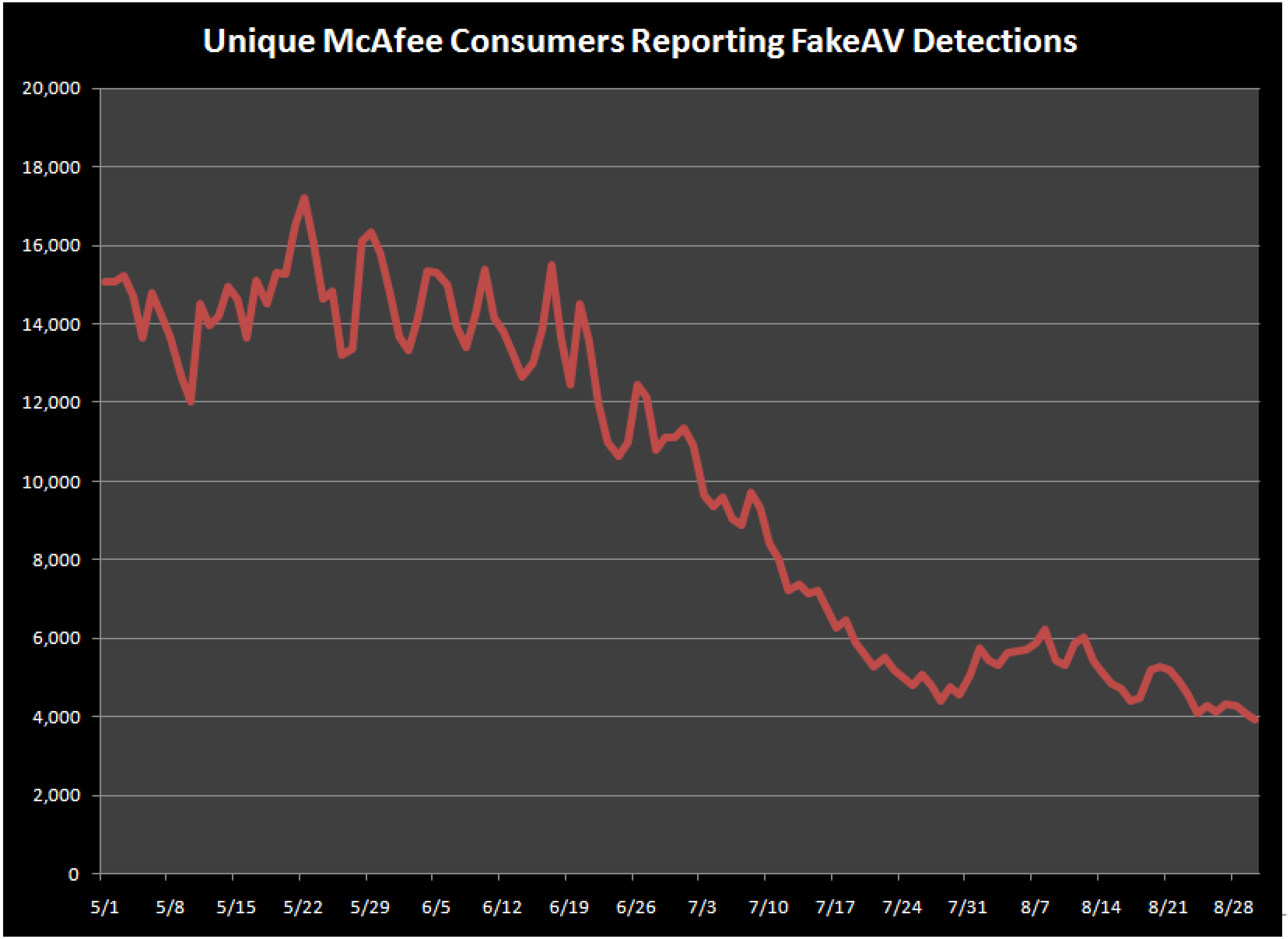


And then the money stopped flowing...

- 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...



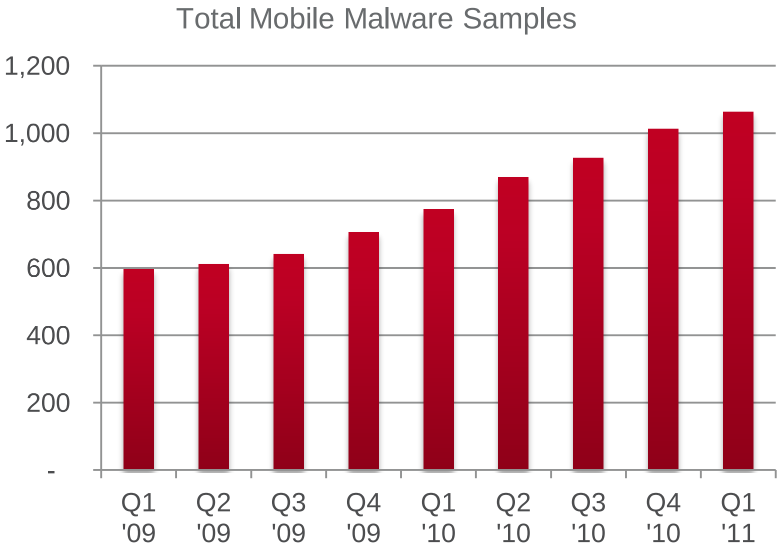
$70mio International Cybercrime Ring Busted

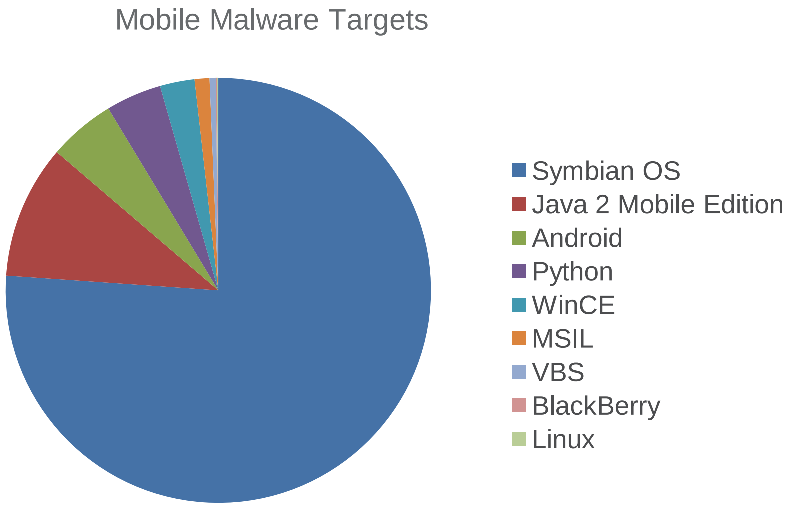
- October 1st 2010: Operation Trident Breach
  - Investigations began in May 2009
  - 60 criminals charged, 10 arrested
  - International Partnership with SBU and other authorities
    - The Federal Bureau of Investigation, including the New York Money Mule Working Group, the Newark Cyber Crime Task 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

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.

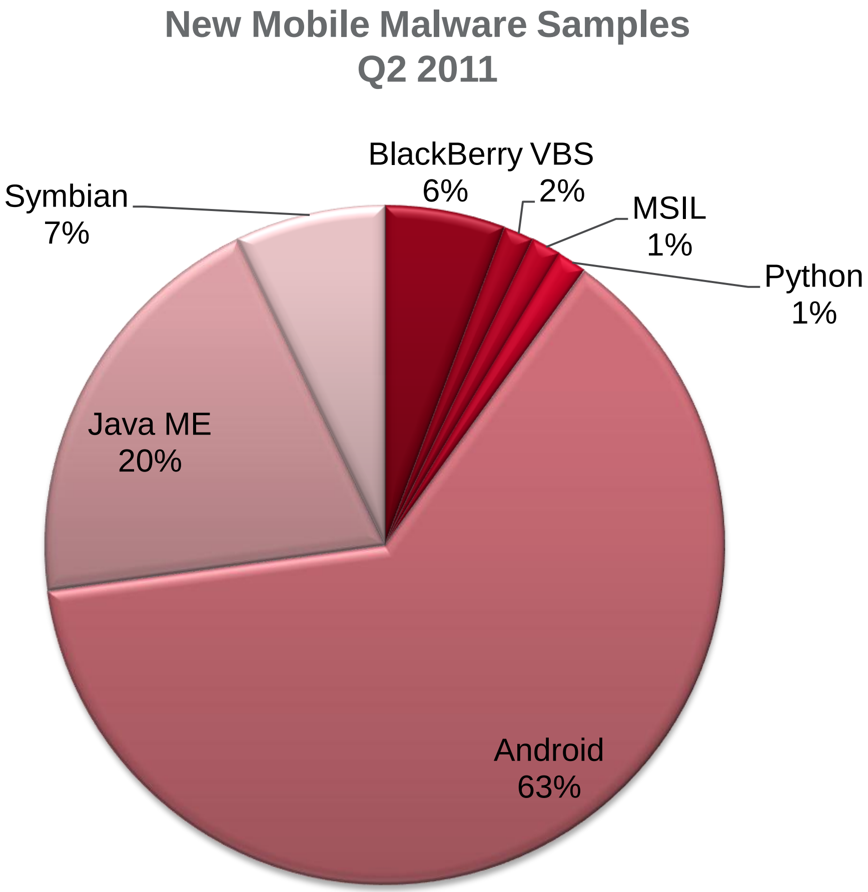
The mobile attack strategies are starting to mirror the approaches historically used to attack PC operating systems. A maliciously altered application obtains root access and then “connects” the device to a botnet-like command center, which issues subsequent instructions to extract data from the device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

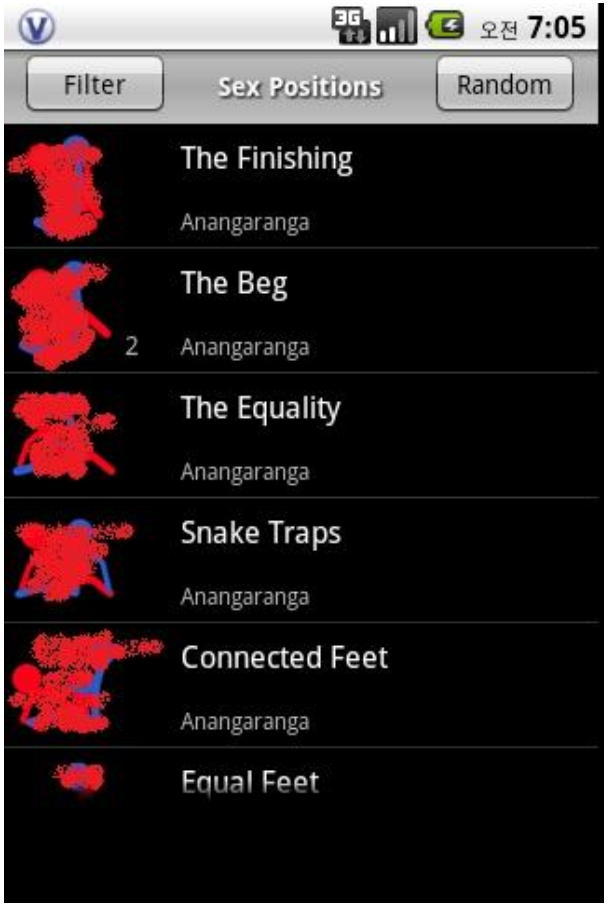


Mobile Crimeware

“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



The Finishing
Anangaranga

The Beg
2 Anangaranga

The Equality
Anangaranga

Snake Traps
Anangaranga

Connected Feet
Anangaranga

Equal Feet

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

Recent Examples

- Android/Jmsonez.A is a version of a calendar app that doesn’t quite work as intended. No matter when the program is launched, it displays the calendar for January 2011. If the user tries to change the month to a future date, the malware begins sending SMS messages to a premium-rate number. Android/Jmsonez.A also monitors the inbox for confirmation SMS messages from the premium-rate service to avoid detection.

- The Android/DroidKungFu family is similar to Android/DrdDream; it also uses a pair of root exploits to maintain itself on a device. The exploits are actually identical to those used by the Android/DrdDream except they have been encrypted with AES. These variants can also load URLs and install additional software and updates .

Recent Examples

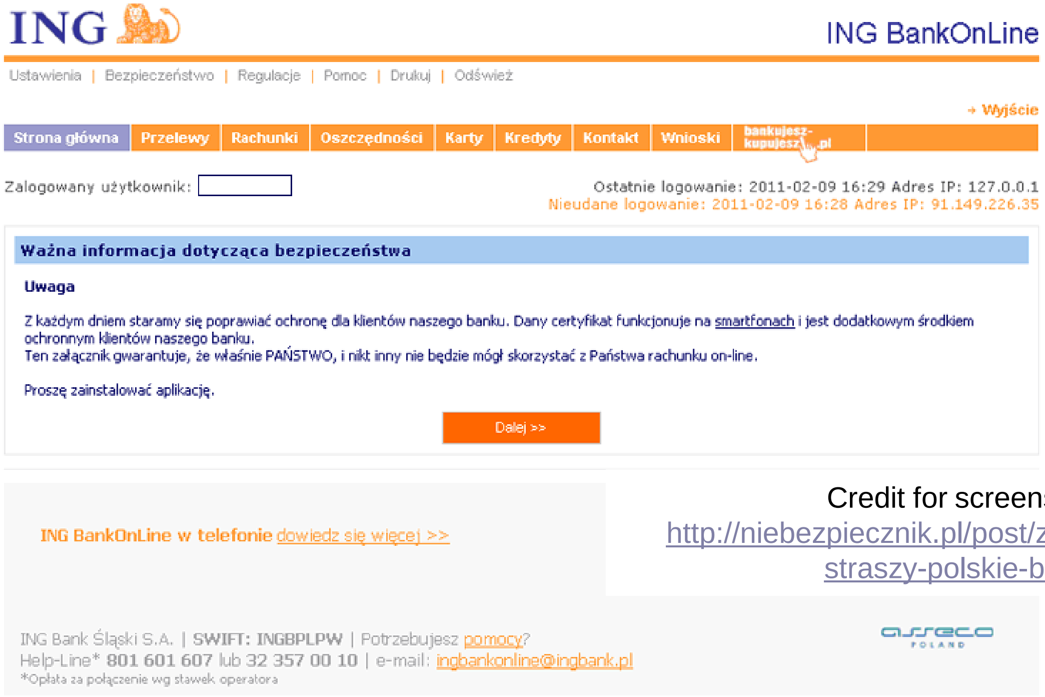
- Android/Toplank.A pretends to be a multiuser update to the popular Angry Birds game. The malware sends sensitive information (international mobile subscriber identity, the list of permissions granted to the malware, etc.) to the attacker and can download an additional Android app to an infected device. The new app provides a backdoor to the attacker, who can then add and delete bookmarks, browser history, and shortcuts. The attacker can also download further software.

- Mobile crimeware authors are continuing their tricks with SymbOS/Zitmo.C and BlackBerry/Zitmo.D, which are simple SMS forwarders. The authors have already compromised victims’ PCs with advanced malware, so it appears that they are doing only the bare minimum on mobile platforms to enable their attacks

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.



Zalogowany użytkownik:

Ostatnie logowanie: 2011-02-09 16:29 Adres IP: 127.0.0.1
Nieudane logowanie: 2011-02-09 16:28 Adres IP: 91.149.226.35

Ważna informacja dotycząca bezpieczeństwa

Uwaga

Z każdym dniem staramy się poprawiać ochronę dla klientów naszego banku. Dany certyfikat funkcjonuje na smartfonach i jest dodatkowym środkiem ochronnym klientów naszego banku.
Ten załącznik gwarantuje, że właśnie PAŃSTWO, i nikt inny nie będzie mógł skorzystać z Państwa rachunku on-line.

Proszę zainstalować aplikację.

ING BankOnLine w telefonie dowiedz się więcej >>

ING Bank Śląski S.A. | SWIFT: INGBPLPW | Potrzebujesz pomocy?
Help-Line* 801 601 607 lub 32 357 00 10 | e-mail: ingbankonline@ingbank.pl
*Opłata za połączenie wg stawek operatora

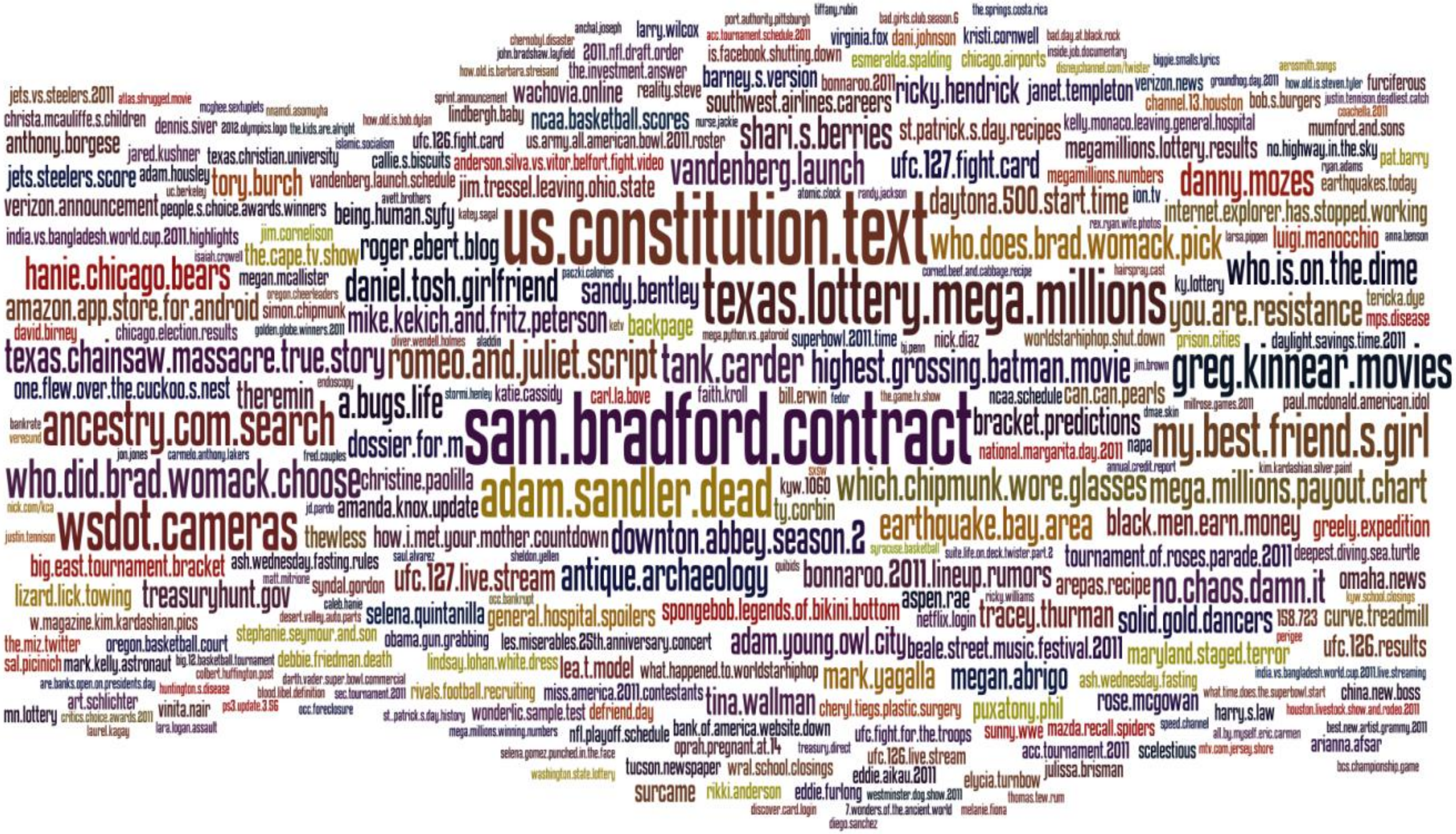
Credit for screenshot:
http://niebezpiecznik.pl/post/zeus-straszy-polskie-banki/

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.

February 2011

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).



Targeted Attacks

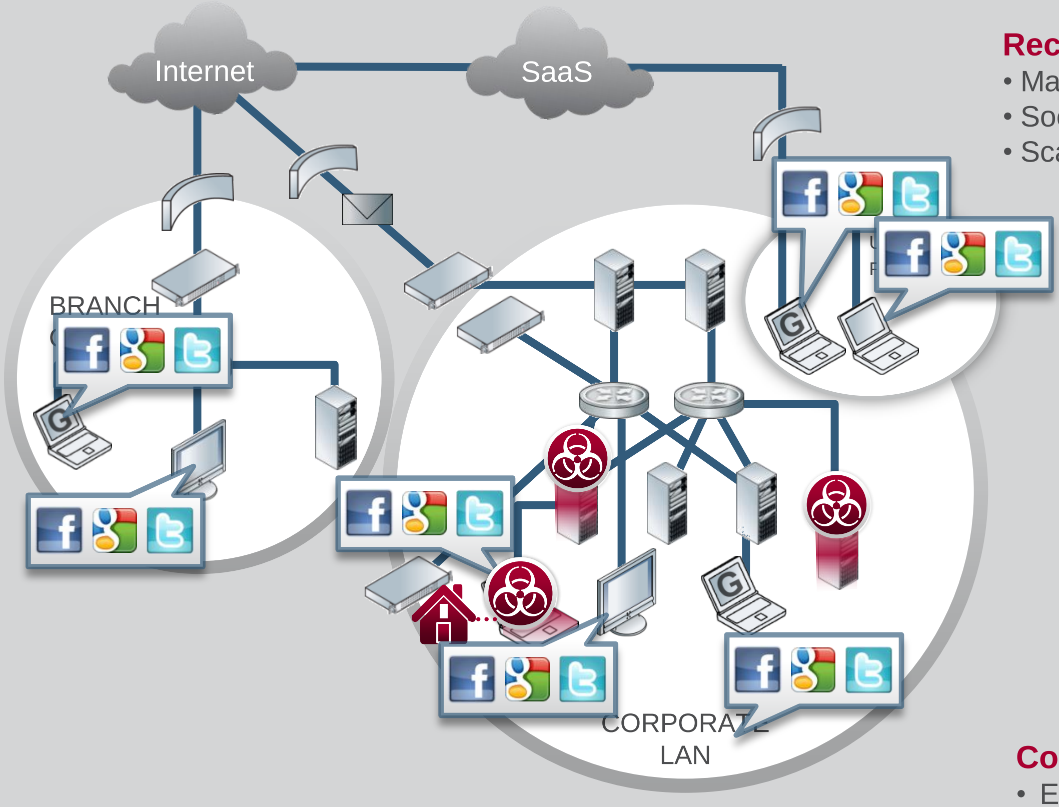
- Targeted Attacks and Advanced Persistent Threats (APT)

- 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

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

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®