eSafe®

EXTREME CAPACITY. MAXIMUM SECURITY.

Aladdin Malware Report 2006

Aladdin®

SECURING THE GLOBAL VILLAGE

Aladdin Malware Report 2006

Aladdin Knowledge Systems' Malware Report 2006 *is provided in an ongoing effort to inform and educate the public on the increasing number of Web-based threats experienced in 2006, as well as a look at likely threats to come in 2007. This comprehensive report is based on information and statistics gathered by Aladdin's Content Security Response Team (CSRT). Data contained in the report came from various sources, including automatic scanning tools which surf the Web in search of emerging threats; information provided by individual users and customers; cooperation with other antivirus technology leaders; and organizations such as Wildlist, which track and analyze "in the wild" threats.*

Malware Trends in 2006

Move to Web-based attacks redoubles

In 2006, less eMail malware was characteristic, while the growth in Web malware was enormous. In SMTP, it is easier to measure whether there is an outbreak or not. Using the Web as a measurement is much harder, but looking at Web malicious code statistics, we can see that numerous Web outbreaks occurred during 2006.

Targeted attacks grow

2006 was also characterized as the year of targeted attacks with a "mission" to infect as many machines as possible. Today, we are witnessing continuing attacks by Trojans gathering specific information from specific users with a "money-oriented mission." Today's hackers are stealing identities and information for the purpose of defrauding the general public.

Today, we are witnessing continuing attacks by Trojans gathering specific information from specific users with a "money-oriented mission."

Cybercrime attracts criminal professionals

Based on current figures and the growth of Web-based malware, it is apparent that "cybercrime" is growing and criminal organizations are starting to utilize the Web as a vehicle to gain money by stealing identities and information. For example, the Banker family of Web-based malicious code has the ability to hack into banking sites. Organized crime organizations are hiring hackers in order to acquire access to Web areas, where these types of crimes are harder to detect. In most instances, the victim does not realize that $10,000 is missing from his or her bank account, or that a large amount of money has been charged to their credit card.

Spyware gets nastier: Information theft increases in numbers and severity

Witnessed in 2006 was the sharp increase in information theft incidents and severity. In 2005, 60% of Spyware/Trojan information theft in 2005 was categorized as Reduced Threat (Commercial Information Privacy Compromise), primarily to collect browsing information and target ads accordingly. In contrast, most of the trojans and spyware variants detected in 2006 were

engaged in medium (computer and Operating System privacy compromise) to critical (end user privacy invasion and information theft privacy compromise) information theft activity.

Typical activities include creation of backdoors on infected machines, collection of personal user information, logging of keystrokes, and turning infected machines into spamming bots. Key findings of the report found that in 2006:

Over 65% of spyware detected were also engaged in Trojan activity

- Over 65% of spyware detected were also engaged in Trojan activity
- Over 30% of spyware detected were also engaged in spam activity
- Over 15% of spyware detected were also engaged in key logging activity
- Over 10% spyware detected were using rootkit techniques to evade detection

Phishers refine their techniques

2006 saw a drastic change in phishing sites: more and more phishing emails are being sent to users in order to get their account information to banking sites, eBay and more, giving hackers access to these "supposedly" secured sites. Phishing emails are becoming more professional and realistic, are incorporating elements of genuine websites for greater believability, and are using targeted messages to smaller groups for greater likelihood of success.

SpamBot networks expand

In 2006, we also saw an increase in the Bot networks, with a good example being the Warezov worm. More than 300 variants of the "old" Warezov versions and configurations are released and downloaded on a daily basis, all for one purpose: *using the infected machines to send spam.*

Exploits of vulnerabilities rise

Also noted in 2006 was a sharp increase in the amount of critical vulnerabilities turned into a zero day exploit. Many new Office vulnerabilities were exploited by malicious code (PPDropper family), IE exploits and more.

Year of the rogue

In 2006, 85% of the tests done on drive-by sites that were using zero-day exploits led to a rogue anti-spyware (spyware masquerading as anti-spyware) at the end of the rabbit hole. Rogue anti-spyware companies had a great financial year that started with the WMF exploit and continued with IE createTextRange as well as SWF, and which came to its climax with the VML and set Slice Exploits. Thousands of infected computer owners were discovered.

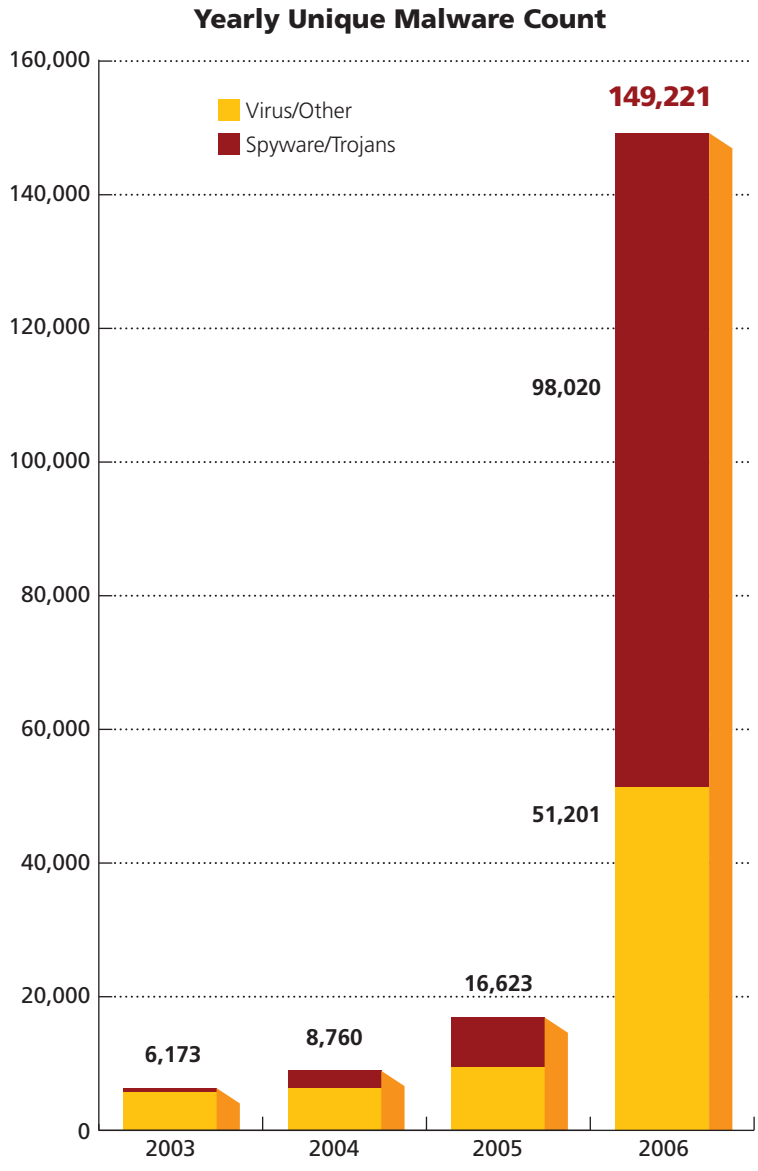
2006 Top 10 Rogue anti-spyware infections:

1	Spy Sheriff	**6**	WareOut
2	BraveSentry	**7**	Udefender
3	Spyspotter	**8**	Spyware Bomber
4	Adware remover gold	**9**	MalwareWipe
5	VirtualBouncer	**10**	TheSpyGuard

Key Malware Statistics 2006

In 2006, a total of 149,221 new instances of individual malicious code specimen were identified, representing an increase of 900% from the new malicious code identified in 2005. Growth of worms, virus and other malicious content was comparatively low based on numbers from previous years. The trend towards web-based malicious code, noted in the Aladdin 2005 Malware Report, continues to grow at an accelerating pace. In fact, the bulk of malware detected in 2006 were Web-based threats such as Spyware and Trojans, ***for an astonishing 1300% growth rate over the prior year.***

The trend towards web-based malicious code continues to grow at an accelerating pace.



2007 will bring a massive rise in targeted attacks.

What's ahead in 2007?

While it is hard to predict exactly what 2007 will bring, the Aladdin CSRT is warning organizations and users of the following potential threats:

- **Web:**
  In 2006, there was a definite increase in Web Trojans (so called spyware) able to get access to more users (like a pyramid). We believe this propagation system detected in 2006, e.g., Myspace Trojans will increase dramatically in 2007.
- **Worms:**
  We will still see worms occasionally, but not as prevalent as before. We do not believe that these worms will cause the kind of damage that the Netsky, Bagle and variants produced. Worms in 2007 will be more geographically targeted, and chances are they will quickly be detected by security products.
- **Exploits:**
  In 2006, we saw multiple cases of malicious code exploiting vulnerabilities in order to spread. With the release of IE7, Windows Vista and Office 2007, hackers will continue to search for vulnerabilities within the new versions and write malware to exploit those vulnerabilities they are certain to find.
- Profit-Driven Cyber Crime will drastically increase in 2007. We will witness more commercial organizations using drive-by methods as a "legitimate marketing tool." We will see a massive rise in targeted attacks—thousands of companies will receive threats by criminals claiming to have shell connections to computing assets.
- Information theft by Spyware and Tojans will remain a critical issue in 2007. In 2006, we witnessed the growing usage of encrypted tunnels masquerading as trusted communications. Security systems monitoring suspicious network behaviour would have to offer validation of trusted communication in order to allow organizations to work only by "trusted" communications.

Conclusion

The future holds the threat of continued growth in regards to spyware and trojans. This is especially logical when one considers the fact that most malicious code is today motivated by potential for financial gain, and not merely by the desire to cause damage. The rapid increase in Web-based attacks reflects the fact that most users, whether at home or on "secure" networks, are most vulnerable when surfing the Web. Phishing techniques now aim to lure users to websites where their computers are infected with various types of malicious code. Web surfers will have to exercise continued caution and stay informed in order to best protect themselves against online threats. Relying on reactive security systems and continually chasing updates will increasingly prove unreliable. More emphasis must be put on proactive solutions protecting against zero-day threats and targeted attacks, while keeping interaction with the user to a bare minimum in order to prevent confusion and poor security decisions.

For the latest information on spyware, viruses, worms, exploits, and other malware threats, please visit the Aladdin Content Security Response Team research portal at Aladdin.com/CSRT.

© 17/4/2006 Aladdin Knowledge Systems, Ltd. All rights reserved. Aladdin and eSafe are registered trademarks of Aladdin Knowledge Systems, Ltd. All other company and product names are trademarks or registered trademarks of their respective owners.

Aladdin
SECURING THE GLOBAL VILLAGE

For more contact information, visit: **www.Aladdin.com/contact**

North America	T: +1-800-562-2543, +1-847-818-3800	**Italy**	T: +39-333-9356711
UK	T: +44-1753-622-266	**Israel**	T: +972-3-978-1111
Germany	T: +49-89-89-4221-0	**China**	T: +86-138-18184444
France	T: +33-1-41-37-70-30	**India**	T: +919-82-1217402
Benelux	T: +31-30-688-0800	**Brazil**	T: +55-11-6106-5101
Spain	T: +34-91-375-99-00	**Japan**	T: +81-426-607-191
		All other inquiries	T: +972-3-978-1111

Printed in Israel
06998