



2007 Top 10 Malicious Code Trends

Author:

Neelay S. Shah
Senior Software Security Consultant
Foundstone Professional Services



Table of Contents

Abstract 3

Top 10 Trends 4

Summary 7

Future..... 7

About Foundstone Professional Services..... 8

References 9

Abstract

Today's information landscape wherein most of the information is stored, processed and exchanged in digital form presents malware (viruses, trojans, worms, rootkits, adware etc.) authors with an increasingly growing opportunity to employ malicious code effectively for financial gain by stealing online banking credentials, sensitive personal information leading to identity theft or sensitive intellectual property that could be sold to a competitor. To add to this, the weak presence and enforcement of information security laws in a majority of the developing countries allows the malicious code authors to operate at will. As such writing and distributing malicious code is a booming business today with a large underground economy developing around it.

Over the years, malicious code authors have become smarter and found new and effective ways to infect and exploit more and more users. At the same time malicious code is now being developed with more sophisticated techniques to avoid detection and being quarantined by the typical anti-virus / anti-malware solutions.

This paper focuses and details the trends that were observed in the evolution of malicious code over the course of 2007. We identify the growth of different categories of malicious code, the means used to propagate malicious code and geographic as well as sector-wise distribution of malicious code over the past year. The paper concludes with what you can expect in the coming year.

Top 10 Trends

1. *Trojans and Worms Infections Continued to Rise(1),(2)*

The number of Trojan and Worm infections as well as the number of new Trojans and worms identified continued to increase in 2007. Trojans have become the vehicle of choice for malicious code writers because they are typically stand-alone malicious executables that reside on the victims' system and then wait for the attacker's command to do further damage. Trojans do not spread as quickly as worms, which are typically self-replicating; hence Trojans allow for a more focused attack, allowing the attackers to pick and choose his / her victims.

Nuwar (also known as the Storm Worm) was one of the most widely reported malicious code family in 2007. Numerous variants of the same worm were also released and it actually managed to build one of the largest P2P botnet ever, which it used for listening for new commands, download and install more malicious executables.

2. *Online Gaming and Virtual World Threats Increased(1),(2)*

Malicious code specifically written to target online games continued to rise steadily throughout the last year. Targeting online games is not only attributed to its growing popularity, which is now estimated to have almost 217 million unique visitors but also to the nature of the online games which now act as virtual worlds allowing the users to trade their virtual items with other gamers in exchange for real world currency.

Most of the trojans and worms targeted towards online games are keyboard loggers which stealthily capture the account credentials when the user launches the game and then submits the same to the malicious attacker via email or a web request.

PWS-Zhengtu Trojan which collects user credentials and information for users of the Chinese game Zhengtu and PWS-Lineage which steals user information for the Lineage II game were some of the most widely reported Trojans targeting online games during the past year.

3. *Parasitic Crimeware Comes of Age(1)*

2007 marked the emergence of parasitic crimeware: malicious code which typically runs as a key-logger and collects the user's sensitive and confidential information such as credit card number or online bank

account details. Crimeware uses parasitic code (malicious code which attaches to the executables on the system and executes as part of those executables) to harvest the information.

Grum was one example of the parasitic crimeware that resurfaced and was widely seen last year, which spread by luring the users to download a fake version of Internet Explorer 7.0.

Fujack was another parasitic crimeware widely observed last year which spread through network shares and external storage devices like USB keys.

4. Instant Messaging Malicious Code Continued to Increase(1)

Malicious code targeting instant messaging clients continued to rise considerably over the last year. The number of vulnerabilities reported against the popular instant messaging applications such as AIM, Yahoo Messenger, and MSN Messenger almost doubled in the past year.

Exploit-YIMCAM was one of exploit codes released last year that exploited the Yahoo Instant Messenger Webcam ActiveX control vulnerability. *StealthChatMon* was another worm that was seen in 2007 which captured the user conversations for popular instant messaging clients like Yahoo, MSN and Skype.

5. Adware Started to Decline(1)

Adware infections actually began to decline gradually in 2007. The US government crackdown against purveyors of ad-serving software has had a positive effect. The combination of lawsuits, better defenses, and the negative connotation associated with this form of advertising helped to continue the decline of adware.

6. Mobile Attacks Failed to Takeoff(3),(4)

Mobile malware attacks continued to remain steady and did not take off dramatically last year as was predicted by security experts. This is due to the fact that the mobile devices are still not a financially attractive target for attackers. It is still rare to find users who use their mobile phones for checking their financial accounts or storing sensitive data such as credit cards which appeal to attackers.

Viver was one of the new malware seen in the wild for Symbian platform. This Trojan is similar to the popular *J2ME / RedBrowser Trojan* and sends out an SMS to a premium numbers charging the mobile users for the SMS.

7. Number of New Rootkits and Polymorphic Viruses Continued to Increase(5)

Rootkits are essentially malware which use extremely sophisticated stealth techniques to hide themselves from being detected. The number of new rootkit variants that were observed almost doubled to 7,235 in the first half of 2007 as compared to those observed in 2006. Similarly, polymorphic viruses, which are typically encrypted with a different key per infection also continued to rise due to their alluring property of evading signature-based detection.

Zhelatin was one of the most popular rootkits seen last year that spread via email. Once the victim downloaded and allowed the rootkit to execute, it would install itself as a driver and turn off the security program installed on the machine to avoid being detected.

8. Malicious Code Propagation Trend(2)

Email attachment was one of the most common propagation mechanisms for malicious code in the past year being responsible for almost half of all malicious code distribution. The success rate of propagating malicious code via email attachments was limited since most enterprises today have up-to-date security products installed to scan and block malicious code being sent to the corporate mail server. File sharing through Common Internet File Sharing Protocol (CIFS) and Peer to Peer protocols were the other popular propagation mechanisms.

9. Geographic Trends(6),(7)

Malicious code infections found in developing countries continued to grow at a faster rate than the developed countries throughout the first half of 2007. This could be attributed to a number of factors such as:

- The deployment of security products is far wider in developed countries than in developing countries.
- The user awareness and education around computer safety and privacy is also more prevalent in developed countries.
- Many of the developing countries have weak legislative controls and the difficulties of international cooperation make them an ideal target for malicious code authors.

In Asia Pacific, Mongolia was seen to have the highest infection rate followed by Thailand and Macau SAR. Albania had the highest infection rate in Europe followed by Turkey and Romania. In the Americas, Dominican Republic had the highest infection rate followed by Brazil and Honduras. Finally, in Middle East and Africa, Bahrain had the highest infection rate followed by Egypt and Iraq.

10. Sector Trends(7)

The Education sector was the most exposed sector to malicious code with one in every 56.86 emails containing malicious code itself or having links to websites with malicious code. Following the education sector were the Chemical / Pharmaceutical sector (one in every 75.38 emails); Wholesale sector (one in every 85.21 emails); Retail sector (one in every 91.80 emails); and Accommodation/Catering industry (one in every 95.50 emails) containing either malicious code itself or links to malicious code.

Summary

2007 saw the continued rise of trojans and worms and in fact even saw the biggest botnet to date in the form of the Nuwar worm. Numerous variants of the same were released throughout the year and continue to infect more systems worldwide. Crimeware authors who target sensitive and confidential user information, such as their online banking credentials and credit card numbers, turned to parasitic malware during 2007. Malicious code targeting online games continued to gain prominence as more and more users start playing them and the games themselves start dealing with real world currencies. Mobile malware and attacks as predicted by many security experts, more or less failed to take off dramatically.

Future

Malicious code specifically written to target online games and virtual worlds are expected to rise as are attacks targeting instant messaging clients. VOIP attacks and threats are expected to grow considerably as the number of VOIP users continue to increasing exponentially. The trend of compromising popular websites including those for social networking and then using them to distribute malware is also expected to rise through the next few years. Finally with the election season being intense in the United States, fake fundraising and supporter emails are increasingly likely to be used to distribute malware.

Individuals should make sure to surf the web more responsibly and keep away from potentially malicious websites and submitting their credentials to phishing sites. Additionally they should be running up-to-date versions of anti-virus, anti-malware and desktop firewall solutions on their systems to mitigate the threat of being compromised while surfing the web.

About Foundstone Professional Services

Foundstone® Professional Services, a division of McAfee, Inc., offers expert services and education to help organizations continuously and measurably protect their most important assets from the most critical threats. Through a strategic approach to security, Foundstone identifies and implements the right balance of technology, people, and process to manage digital risk and leverage security investments more effectively. The company's professional services team consists of recognized security experts and authors with broad security experience with multinational corporations, the public sector, and the US military.

References

1. **McAfee Inc.** McAfee Avert Labs Top 10 Threat Predictions for 2008. [Online]
http://www.mcafee.com/us/local_content/white_papers/threat_center/wp_avert_predictions_2008.pdf.
2. **Symantec.** Symantec Internet Security Threat Report Trends for January – June 07. [Online]
http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf.
3. **McAfee Inc.** Revisiting the Crystal Ball: Updating Our 2007 Predictions. [Online]
<http://www.avertlabs.com/research/blog/index.php/2007/06/18/revisiting-the-crystal-ball-updating-our-2007-predictions/>.
4. **F-Secure.** State of Cellphone Malware in 2007 . [Online]
<http://www.usenix.org/events/sec07/tech/hypponen.pdf>.
5. **McAfee Inc.** Rootkits, Part 1 of 3: the Growing Threat. [Online]
http://www.mcafee.com/us/local_content/white_papers/threat_center/wp_akapoor_rootkits1_en.pdf.
6. **Microsoft.** Microsoft Security Intelligence Report – January through June 2007. [Online]
<http://www.microsoft.com/downloads/details.aspx?FamilyId=4EDE2572-1D39-46EA-94C6-4851750A2CB0&displaylang=en>.
7. **MessageLabs.** MessageLabs Intelligence: 2007 Annual Security Report. [Online]
http://www.messagelabs.com/mlireport/MLI_2007_Annual_Security_Report.pdf.