ASA

Risk Consultants

Research Note

Malware Analysis: A Look Into the Past and Future

By: Devin Luco

Copyright © 2012, ASA Institute for Risk & Innovation

Keywords: Malware, Virus, Storm Worm, Cyber Threats, Cyber Protection

Abstract – This research note defines malware and distinguishes between the different types that users are exposed to today. It is important to keep up-to-date on malware issues since it affects millions of users and costs billions of dollars every year. By looking at the 2007 Storm Worm case, it will give a deeper understanding of why it is important to be cautious when using computers or mobile devices. Most importantly, this note ends with basic steps on how to protect against malware threats in the future.

ASA

Risk Consultants

What is Malware?

Malware, also known as malicious software, is any code or program that is used to gain access to, collect personal information from, or interrupt the functionality of a private computer. Usually people make the mistake of grouping all malware as "computer viruses." However, there are many different types of malware including Trojan horses, worms, viruses, spyware, and adware.

Trojan Horses – Just as the name implies, Trojan horses conceal themselves as a harmless program but when executed, unleashes a malicious code that damages the operating system of a computer.[1] Often, Trojans are sent via email using misrepresenting messages to manipulate the recipient into opening the program.[2]

Worms – This malicious code has the ability to replicate and distribute itself through networks. Depending on the type of worm, it can replicate with or without user execution. Due to its replicating nature, worms use a vast amount of system resources sometimes resulting in a denial-of-service (making a network service unavailable to its' intended users).[3]

Viruses – Unlike worms, viruses replicate themselves by latching onto a host program or file and spread once the user executes the host.[4] Viruses damage software, hardware, and computer data.

Spyware – Spyware is best known as tracking software. Usually users download this without knowing because it is packaged within another program that the user actually wants.[5] Once installed, Spyware tracks and gathers sensitive information without the user's knowledge. The owner of the spyware can sell the personal information or use it for his/her own malicious purposes.

Adware – Adware is software that displays advertisements to the user.[6] This type of software is usually more of an annoyance for those that are affected. However, some Adware invades a user's privacy with an added tracking function.

Why is it Important?

So why should we care? Malware has been around for many years. Despite anti-virus software protections, malware still infects countless computers across the globe every year. According to a 2010 survey by Symantec, 286 million different types of malware accounted for 3 billion attacks on users.[7] The study also showed high vulnerability for threats on social networking sites, where information on profiles

are used for attacks.[8] Attackers target social networking users by linking to malicious sites where they are exposed and exploited.[9] This vulnerability is alarming considering Facebook, one of the most popular social networking sites in the world, just reached one billion users in October 2012. Meaning approximately one-seventh of the world's population could potentially be vulnerable to attacks.

As technology continues to advance, attackers become more sophisticated and find new ways to cause threats. Currently in our society, we are seeing a migration of users from computers to mobile devices. According to a 2012 survey by Pew Research Center, 44% of U.S. adults own a smartphone, and 18% own a tablet.[10] With the increasing number of mobile users, security threats become more accessible and prevalent. Mobile users usually download lots of applications from Apple's App Store or Android's Marketplace, which is where malware could possibly be hiding. Google announced in the past that they had to remove several malicious applications, most of them Trojans.[11]

Whether the malware attacks are through computers or mobile devices, it is very costly for consumers. 71 million consumers in the U.S. alone lost $20.7 billion to cybercriminals.[12] Consumers worldwide lost

$110 billion from malware attacks during the same time period of July 2011 to July 2012.[13]

Storm Worm, considered one of the top 10 worst computer viruses of all time,[14] affected millions of users around the world. By looking at this historical example, we can further our understanding of how malware affects computers and networks, why it spreads so quickly, and how to protect ourselves from future threats.

A Historical Case: The "Storm Worm" Trojan

Storm Worm is a family of Trojan viruses that started infecting Windows based computers in late January 2007.[15] Similar to malware in the past, Storm Worm was sent to computers via email messages with an accompanying attachment. The email would contain a subject line about a natural disaster that occurred. An example of a Storm Worm email subject line would be, "230 dead as storm batters Europe."[16]

The main trap of Storm Worm is the fact the subject line seems real. By using a subject line that describes a natural disaster, recipients are prone to open the email and attachment. The body of the email usually directs the recipient to open the attachment to learn more about the story.[17] Social engineering, a manipulation tactic that takes advantage of human's trusting nature, is the main strategy in this

attack. Recipients are trusting the email is legitimate based on the emotional aspect and real nature of the story. Once the file is opened, the infected computer becomes part of a botnet.[18] A botnet describes a group of computers that have been compromised. The hacker can later use and communicate with other compromised computers for malicious purposes without the original owner's knowledge.[19] The Storm Worms botnet was much harder to track and destroy because it did not use a centralized server. Instead each infected computer acted as a host and was only a section of the entire botnet network.[20]

The Storm Worm is much more complex than other malware. It has several different components:

- A backdoor that allows hackers access for gathering personal information[21]
- The ability to turn computers into spam-bots to generate and post spam to others[22]
- The installation of a peer-to-peer network that allows communication between other infected computers in the botnet[23]
- The ability to gather email address information to spread the virus virtually[24]

- The ability to update and invite other malware programs to download[25]
- A rootkit, which disguises the Trojan[26]

How to Protect Yourself?

Although computing users are exposed to millions of threats every day, there are some easy steps we can take to protect ourselves from malicious software:

For both business and personal users:

1. Being educated in the different types and the possible damage that can be caused is the first step to protecting yourself from such threats. Reading websites, such as http://www.securityfocus.com/, regularly will help keep you current on malware and vulnerability trends.
2. Do not open any suspicious emails. Remember, malware can access email address books to distribute itself through email. So advise your colleagues, friends, and families to be cautious with opening attachments as well.

For business users:

1. Encourage the development of a risk management process. Having a strong risk management methodology will help

employees identify controls that are vulnerable to threats, develop plans for mitigating exposure, and develop recovery plans if affected by malware.

2. Restrict employees' access to buildings, networks, servers, and workstations. Implement access privileges that require employees to enter user ids and passwords.

For personal users:

1. Update your operating system, browser, and anti-virus software. This will ensure that your machine is prepared to identify the latest malware threats that are circling through the network.
2. Install malware removal software. This will come in handy if a worm or Trojan bypasses your anti-virus software.
3. For mobile protection, remember to investigate and research applications before you download. Be sure to take notice of the developer name and pricing information; compare it to what you are seeing in the application store for any discrepancies.[27]

Conclusion

As we have seen, malware can disguise itself in many shapes and forms. Malware can be a minor nuisance as adware or spyware. It can also be very damaging and costly as Trojans, worms, or viruses.

Although we can never be 100% safe, by analyzing and learning from past malware occurrences, we can be proactive in preventing and responding to future attacks.

ASA

Risk Consultants

References

[1] "Strategies for Managing Malware Risks." *Microsoft*. 18 Aug. 2006. Web. 6 Nov. 2012. <http://technet.microsoft.com/en-us/library/cc875818.aspx>

[2] Microsoft, n. pag.

[3] Microsoft, n. pag.

[4] Microsoft, n. pag.

[5] Microsoft, n. pag.

[6] Microsoft, n. pag.

[7] Oran, Olivia. "Symantec Reports Rise of Malware in Mobile." *TheStreet*, *Inc*. 4 May 2010. Web. 7 Nov. 2012. <http://www.thestreet.com/story/11073235/1/symantec-reports-rise-of-malware-in-mobile.html>

[8] Oran, n. pag.

[9] Oran, n. pag.

[10] Mitchell, Amy, Tom Rosenstiel, and Leah Christian. "Mobile Devices and News Consumption: Some Good Signs for Journalism." *State of the Media.org*. n.d. Web. 8 Nov. 2012. <http://stateofthemedia.org/2012/mobile-devices-and-news-consumption-some-good-signs-for-journalism/>

[11] Claburn, Thomas. "Google Removes Malicious Android Apps." *InformationWeek Security.* 2 Mar. 2011. Web. 9 Nov. 2012. <http://www.informationweek.com/security/vulnerabilities/google-removes-malicious-android-apps/229300051>

[12] Osborne, Charlie. "Cybercrime Costs U.S. Consumers $20.7 billion." *CNET*. 5 Sept. 2012. Web. 8 Nov. 2012. <http://news.cnet.com/8301-1009_3-57506216-83/cybercrime-costs-u.s-consumers-$20.7-billion/>

[13] Osborne, n. pag.

[14] Strickland, Jonathan. "10 Worst Computer Viruses of All Time." *HowStuffWorks*. n.d. Web. 6 Nov 2012. <http://computer.howstuffworks.com/worst-computer-viruses10.htm>

[15] Kawamoto, Dawn. "'Storm Worm' Rages Across the Globe." *CNET*. 19 Jan. 2007. Web. 30 Oct. 2012. <http://news.cnet.com/storm-worm-rages-across-the-globe/2100-7349_3-6151414.html >

[16] Kawamoto, n. pag.

[17] Kawamoto, n. pag.

[18] Landesman, Mary. "What is the Storm Worm?" *About*.com, n.d. Web. 30 Oct 2012. <http://antivirus.about.com/od/virusdescriptions/a/stormworm.htm>

[19] Landesman, n. pag.

[20] Landesman, n. pag.

[21] Landesman, n. pag.

[22] Landesman, n. pag.

[23] Landesman, n. pag.

[24] Landesman, n. pag.
[25] Landesman, n. pag.
[26] Landesman, n. pag.
[27] Jeffers, David. "Protect Your Smartphone from Mobile Malware." *PC World.* 27 Mar. 2012. Web. 8 Nov. 2012. <http://www.pcworld.com/article/252235/protect_your_smartphone_from_mobile_malware.html>