

The Future of Zombie Infestation on Seventh Generation Video Game Systems

Jim O'Gorman

jameso@elwood.net

<http://www.elwood.net/>

Introduction

Botnets, zombies, and malware have been pervasive in the computing press for the last few years, and with good reason. While numbers on the growth of botnets are always reported differently¹ (numbers such as a 34% increase in 2007 over 2006² and over \$20 million in losses³ are common) the general consensus is botnets and zombies are one of the largest threats facing the Internet users today⁴.

Botnets are being run as a profit making venture⁵. As such, any development put forward in professional botnets have expected ROI targets, with a desire to create as many newly infected zombie hosts as possible. In this paper we will explore the conditions required for zombie infestation to occur on a computing device and the likelihood of seventh generation video game systems being targeted for infection.

For more information on the history of zombies and botnets, there are many sources online which contain very complete histories^{6 7}. For information on how to get involved in the fight against botnets, the ShadowServer⁸ project is highly suggested.

Conditions for a Zombie Infestation

As with any infestation, the proper conditions are required for the infection to take root. In the case of a zombie host, the malware author must consider four factors in evaluating the attractiveness of the target platform. These factors are:

Attractiveness of target = Size of install base x Uniformity of platform x Ease of exploitation x Utility of system

Defined, these variables are:

Size of install base - A platform must be of adequate size to justify the effort required for development. This is one of the reasons that in the past Microsoft Windows has been the most targeted platform. Recently, Apple's OS X has had malware released which could lead to a zombie infection⁹, leading many to speculate this was a trial run on testing OS X as a zombie platform. It is no accident this coincides with the platform's recent gains in market share¹⁰.

Uniformity of platform - There has to be a reasonable expectation that the install base will have similarly configured systems and/or installed applications. Often this

will mean default applications or configurations that are expected by common popular services. Windows Media Player, Microsoft Office, web browsers and common browser plugins (flash, adobe acrobat, etc.) are often targeted in such manner¹¹. Widespread applications and configurations provide creators with a known environment to target¹².

Ease of exploitation - The infection process must be adequately simple to prevent errors from occurring during the infection process. A complex infection process has more points to go wrong, reducing the number of infected hosts which will be harvested. In recent history, this has led to social engineering attacks being heavily involved in most malware infections. What this translates into is the system is only as secure as the user is clever enough to not be tricked into taking actions which would be adverse to the users' interest.

Utility of system - There has to be a degree of usefulness of the system to an attacker after infection. This may be computing power for distributed computing efforts, sensitive data stored on the infected host, bandwidth for distributed denial of service attacks, or the ability to infect other more attractive systems.

Combined, these factors determine the attractiveness of a target host to botnet harvesters. A single variable being low does not mean the target will be unattractive. For instance, a low install base platform may still be an attractive target if the ease of exploitation is high enough to capture a large enough percentage of the overall number of installed units.

Seventh Generation Video Game Systems

At this point, seventh generation video game systems appear to be the most attractive alternative computing platform for botnet expansion. It is expected that an attempt to harvest these devices as a botnet platform will be made in 2008.

The current make up of seventh generation video game systems have significant differences from previous generations. The Microsoft Xbox 360 (360), Sony Playstation 3 (PS3) and Nintendo Wii (Wii) all have storage mediums (with the sole exception of the low end 360 arcade edition model shipped in late 2007) and some form of network access (wireless of the Wii, wireless and gigabit Ethernet for the PS3, and Ethernet for the 360) out of the box. Computing power on the PS3 and 360 systems rival many desktop computer systems.

These seventh generation systems are equipped with many traditional PC features such as hard drives and USB ports. And in many cases, the systems do not turn "off" in the traditional sense, but rather go to a passive "standby" mode. While in this mode the Wii will periodically poll a proprietary online service to check for messages sent to the unit.

Plugging the merits of these systems into our earlier model:

Size of install base - As of September 2007¹³, there has been sales of over 7 million 360s, nearly 5 million Wiis, and just over 2 million PS3s. Early numbers from November 2007 indicate a traditional seasonal uptick in sales, with numbers out of Japan indicating a large increase in PS3 sales¹⁴.

Uniformity of platform - A uniform configuration is a key selling feature for developers to release software for these systems. While both the 360 and PS3 are sold in different retail configurations, the base firmwares of all three platforms are uniform across the systems. New to this generation of video game systems, an upgradeable firmware demonstrates the maturity of the platforms. Slight differences in firmware revisions and minor hardware differences are the only deviations that can be expected. As a whole, video games systems have been one of the most widely used alternative computing devices with uniform base configurations.

Ease of exploitation - This varies per system. The 360 has access to a closed online network (XBox Live), yet does allow interaction between XBox Live users and MSN Messenger. The Wii has access to an Internet based purchasing venue, a version of the Opera web browser, and the ability to send Internet e-mail to a Wii system (w+Wii Number@wii.com). The PS3 has an embedded web browser, access to an Internet based purchasing venue, and the ability to operate as wireless access point for Playstation Portable systems (PSP). Video game system users would be particularly vulnerable to social engineering bases attacks due to the lack of past attacks on the systems.

Utility of system - Through the use of the Internet based purchasing venue, there is opportunity to access credit card information via a compromised video game system. For the PS3 and 360, the level of computing power would be an attractive addition to a botnet. Systems could be utilized in distributed denial of service attacks, or the generation of spam messages.

Based on this, it is worth further investigating the possibility of zombie infection of the Wii and PS3 due to the number of vectors for possible attack on the systems. For now, the most likely vector of attack on the 360 remains the use of the MSN Messenger product. Widespread attack targeting the 360 via this vector is unlikely.

Wii

The high end of sales of the Wii is unknown at this point. To date, the Wii has sold as quick as the units are manufactured. Many believe the Wii will have the largest market share of all seventh generation systems as soon as the manufacturing process can generate the units. Further, the Wii has attracted many non-traditional video game system buyers. These consumers do not have set expectation of usage of a video game system, increasing the odds of a successful social engineering attack.

As previously stated, the Wii has access to an Internet based shopping channel. Consumers are able to store money within this system that attackers could possibly target. Beyond that, the possibility of running a rogue access point, distributed denial of service, or utilizing the system for spam e-mail generation remain. Overall, the CPU power on the Wii platform does not offer attractive capabilities for an attacker.

Attack vectors are numerable on the Wii. The possibility of a browser based attack against the Opera browser exists. A rogue access point attack would be possible. The most likely vector would be the use of Internet based e-mail. An attacker that is able to find an exploit of the Wii's e-mail handling code could possibly sustain a brute force e-mail attack against the Wii namespace. If the attack is as such to run rogue code delivered through this attack, the possibility to infect the system with a zombie would be high.

Ease of exploitation through this method would be rather low at this point. Very little work has been done in the public area on reverse engineering the Wii platform, providing attackers with a limited base of information to build from. However, the widespread nature of the Wii system will increase its attractiveness to attackers over the course of 2008.

PS3

The PS3 has the potential to be the most interesting platform to attackers, with its limited install base being the only negative point in targeting the platform for botnet harvesting. The PS3 remains the most expensive seventh generation video game system and is currently the slowest selling system. There has been recent reports of the PS3 outselling the Wii in Japan, and recent changes in advertising strategy for the system are expected to increase sales. If this has any affect on US based sales remains to be seen, however the sales deficit remains high regulating the PS3 to the lowest selling seventh generation video game system for the foreseeable future.

Despite this, the PS3 offers the most utility as a zombie host. The computing power of the PS3 can be demonstrated by the platforms use within the Folding@Home project. Currently in December of 2007, the PS3 is contributing 1088 teraflops to the effort¹⁵. Non PS3 platforms have a cumulative output of 218 teraflops within the effort.

This utility in mathematical operations has been recently demonstrated in the use of the PS3 to conduct brute force attacks on passwords¹⁶. In this attack, the PS3 has demonstrated the ability to conduct 1.4 billion cycles per second, compared to a high end Intel based chip operating at 15 million cycles per second¹⁷. This ability to conducted proven high speed mathematical calculations coupled with the demonstrated distributed computing power of the platform is a very attractive offering in a botnet platform.

A further demonstration of the PS3's ability to compute mathematical functions is the November 30th prediction of the 2008 US presidential election winner¹⁸. This project

is less to do with the true output of the US presidential election, and more focused on hashing collisions within MD5. In the project, it was determined that a single PS3 is equivalent to roughly 30 standard PCs in a cluster in the hashing operations that were conducted.

Ease of exploitation on the PS3 is directly affected by the fact it is the most open of the seventh generation video game platforms. This is reflected in the base hardware on the system which includes user replaceable IDE hard disk¹⁹, CF memory, SD memory, memory stick, Bluetooth, WiFi, Gigabit Ethernet, and USB 2.0.

Knowledge of the utilization of the system is much easier to come across on the PS3, in part due to the level of documentation available through the PS3 Linux project²⁰. As an example of the level of developer information available, developers have recently obtained the use of the PS3 video card through the use of open code under PS3 Linux²¹ using no propriety drivers. While an attack such as forcing a remote PS3 to install Linux is not realistic, the knowledge derived of the low level functioning of the system that can be obtained through study of the PS3 Linux project could assist with exploit development.

Possible infection vectors on the PS3 include the Playstation Network (PSN), and various online play options available. Exploits of online games are well known on traditional computing systems²², these are normally designed to affect in-game play. The possibility of exploitation of these online games to a lower level may be possible. The depth of verification the PS3 conducts when authenticating with the PSN is unknown, making DNS spoofing and rogue access points a possible attack vector.

As part of the PSN, there is the ability to create "friends" and send messages between systems. The use of these messages for various attacks, including social engineering attacks, remains to be seen.

The use of the web browser for attacks is the most likely vector for an attack to take place against the PS3. Browser based attacks are well known, and the possibility of an attack involving a site downloading software and manipulating the user into installing software is high. This is the same model of attack used by many botnet harvesters, and efficient techniques are well known. There is indication that Sony has taken steps that anticipate this sort of attack, as indicative of optional filtering software within later firmware revisions²³.

Conclusion

With the amount of money at stake in the operation of a successful botnet, zombie infestations will continue to increase. The conditions that affect the attractiveness of a system to botnet harvesters are the size of install base, the uniformity of the platform, the ease of exploitation, and the utility of system.

Currently, seventh generation video game systems are at high risk of botnet harvesting due to the computing power of the systems (in the case of the PS3, a specialized sought after form of computing), a large and growing install base, and a highly uniform platform. Of the seventh generation systems the Wii and PS3 are potentially the most attractive targets due to the delivery vectors offered by the openness of the systems.

¹ <http://www.shadowserver.org/wiki/pmwiki.php?n=Stats.BotCounts>

² <http://blog.wired.com/27bstroke6/2007/08/even-the-hacker.html>

³ <http://www.fbi.gov/page2/nov07/botnet112907.html>

⁴ <http://www.sans.org/top20/>

⁵ <http://www.first.org/conference/2006/papers/ianelli-nicholas-slides.pdf>

⁶ http://pages.cs.wisc.edu/~pb/botnets_final.pdf

⁷ <http://www.honeynet.org/papers/bots/>

⁸ <http://www.shadowserver.org/wiki/pmwiki.php>

⁹ <http://www.intego.com/news/ism0705.asp>

¹⁰ <http://www.fastcompany.com/magazine/121/all-eyes-on-apple.html>

¹¹ http://www.sans.org/top20/2007/press_release.php

¹² <http://cryptome.org/cyberinsecurity.htm>

¹³ <http://kotaku.com/gaming/sales-charts/a-look-back-at-the-years-npd-sales-320210.php>

¹⁴ <http://money.cnn.com/news/newsfeeds/articles/newstex/AFX-0013-21361220.htm>

¹⁵ <http://fah-web.stanford.edu/cgi-bin/main.py?qtype=osstats>

¹⁶ <http://www.smh.com.au/news/security/playstation-a-hackers-dream/2007/11/26/1196036813741.html>

¹⁷ <http://www.pcworld.com/article/id,140064-c,gameconsoles/article.html>

¹⁸ <http://www.win.tue.nl/hashclash/Nostradamus/>

¹⁹ <http://www.ps3fanboy.com/2007/11/28/video-ps3-hard-drive-replaced-in-minutes/>

²⁰ http://en.wikipedia.org/wiki/Linux_for_PlayStation_3

²¹ http://www.ps3news.com/PlayStation3/PS3_GPU_Use_in_Linux_Video_available/

²² [http://en.wikipedia.org/wiki/Exploit_\(online_gaming\)](http://en.wikipedia.org/wiki/Exploit_(online_gaming))

²³ http://www.reghardware.co.uk/2007/11/16/ps3_trend_micro/