James Rollins
ICTN 4040-601
Term Paper
Dr. Phil Lunsford
Mrs. Constance Boahn
April 10, 2015

How the Lizard Squad Took Down Two of the Biggest Networks in the World

During the 2014 Christmas holidays, millions of people all over the world were subjected to an unwanted gift. They sat down to play their new video game or watch a streaming movie on their Microsoft X-Box or Sony PlayStation, only to find that the online services of their respective system was unavailable. The blackout lasted for a couple days in Microsoft's case, but the Sony service was down for more than a week. Microsoft's X-Box Live and the Sony PlayStation Network had been successfully disabled by the Lizard Squad; a globally organized group of hackers, who had publicized their intentions on social media such as Twitter and Facebook for weeks prior to the attack.

X-Box Live and the PlayStation Network are world-wide online gaming and digital media delivery services. They provide a framework of connectivity for users to connect to one another for multiplayer video games, as well as streaming movies, music, and television programming. Some of the streaming services both networks provide are Netflix, the NFL Network, and proprietary music streaming applications. As of December 2014, X-Box Live had 48 million subscribers and the PlayStation Network reported 110 million subscribers (BBC News, 2014). Both services offer a limited free subscription and a full featured paid subscription.

X-Box Live is available in 42 countries around the world (Wikipedia, 2015) and the PlayStation Network is available in 70 countries (Wikipedia, 2015).

A Distributed Denial of Service (DDoS) attack is the process of flooding servers and/or firewalls with requests with the intention of making the devices unable to serve legitimate user requests. The most simple of these attacks are SYN floods and Conn floods. Whether the server being attacked fails, or the firewall in front of it fails, the result is the same – the network is unable to serve its customers (Holmes, 2015). Over 80% of modern DDoS attacks are HTTP floods (Holmes, 2015). The hackers' requests in HTTP floods look like legitimate HTTP requests and are passed through the router to the targeted server. The overwhelming number of requests, sometimes in the millions, cripple the server's ability to answer the real requests. These numbers are achieved by the hackers through the use of botnets. Botnets are created when a user's PC is infected with a distributed piece of malware that allows the hacker to gain control of the device. Once the device is under the hacker's control, it becomes a "zombie" and is added to the botnet as a whole. The hacker can then direct his zombies to attack any target he chooses with a nearly endless stream of illegitimate data. Personal home routers are also becoming targets of attackers as in the case of the Lizard Squad's attack on X-Box Live and the PlayStation Network (Brandom, 2015). The average botnet size reported in 2011 was about 20,000 devices per network. However there are botnets containing 10 to 15 million compromised clients (Holmes, 2015).

The Lizard Squad is a group of black hat hackers who claim responsibility for several DDoS attacks over the past few years with the most publicized being the attack on X-Box Live and the PlayStation Network. Most of their attacks center on online gaming web sites, but they have also claimed responsibility for attacks on the government of North Korea and Malaysia Airlines (Wikipedia, 2015). The group claimed that its reason for taking down Microsoft and Sony's networks were to expose security weaknesses in the services. They posted freely about the impending attack in the weeks leading up to Christmas on various social media sites such as Facebook and Twitter. In a December 2014 interview with Business Insider an unidentified member of the Lizard Squad offered some more insight into the reasons for the attack. He said the project started “for laughs” before the group decided to officially claim the attack was to force the companies to upgrade the security on the networks. They chose Christmas because it would allow them to affect the largest group of customers. The hacker also offered some revealing information about the levels of security on the two networks. He claimed that Microsoft had the most lax security – “almost nothing”, but Sony’s security measures were more robust and took some time to get around (Smith, 2014). The group said they would keep the networks down as long as they wanted to. The end of the attack came when MegaUpload founder Kim Dotcom offered the group vouchers for content hosting services on his site equaling roughly $30,000.00 (Krebs on Security, 2014). Also possibly leading to the end of the attack were efforts by another hacker group called the Finest Squad. The Finest Squad managed to hack Twitter accounts and websites belonging to members of the Lizard Squad. They then published pictures and names of some of the Lizard Squad members online. For a hacker the revelation of his identity is one of the worst things that can happen. This could lead to arrest, or reprisals from the people he has attacked. It has never been made known how the Finest Squad hacked into the social media accounts. The Finest Squad also revealed how the Lizard Squad perpetrated the DDoS attack using tools that cost as little as $300.00 (Cook, 2014).

The Lizard Squad built their botnet mainly using hacked home networking routers. This was surprisingly easy to achieve due to the fact that with the explosion of home networking, many people can set up their own networks who might not be technically savvy. They do not realize the importance of hardening these devices. In fact, many people never change the routers' default password combinations from admin/admin or root/123456. Additionally they may leave the network addressing scheme default; in most cases 192.168.1.1 or 192.168.0.1. These two changes should be the bare minimum that should be done when setting up a new home router. Other changes that should be made are modifying the SSID and setting up secure wireless connection – preferably with WPA2. The malware code that was inserted into the routers by the Lizard Squad also tried to spread itself. The code was written so that in addition to turning the host router into a zombie, it scanned the internet looking for other routers that still had the default access credentials in place and would accept incoming connections through telnet. Every time it found one, it would inject the malware, thus creating another zombie (Krebs on Security, 2015). The attack carried out on X-Box Live and the PlayStation network exemplifies why the importance of practicing hardening on home routers cannot be overstressed.

Since the attacks of Christmas 2014, Microsoft and Sony both claim to have reinforced the security on their respective online networks. They haven't released any details for obvious reasons. Perhaps they added more servers to support the service. If a section was attacked again, they could roll over to another server farm. But even that may not be enough. In 2013 Microsoft upgraded the number of servers that run X-Box Live to 300,000 units and that still wasn't enough to stop the DDoS attack (Love, 2014). Another solution may be to add stronger encryption. The encryption on these networks is not government-level or even bank-level. There is a tradeoff to be had with strong encryption however. By the very nature of the services these networks provide, too strong of an encryption algorithm could actually slow the service down, leaving dissatisfied customers. It seems that the only way to be sure these networks are safely functioning will be to wait and see if another attack occurs.

References

BBC News. (2014, December 27). *Xbox and PlayStation resuming service after attack*. Retrieved from BBC News: http://www.bbc.com/news/uk-30602609

Brandom, R. (2015, January 9). *Lizard Squad used hacked routers to take down Xbox Live and PlayStation Network* . Retrieved from The Verge: http://www.theverge.com/2015/1/9/7520415/lizard-squad-used-hacked-routers-to-take-down-xbox-live-and

Cook, J. (2014, December 26). *How A Hacker Gang Literally Saved Christmas For Video Game Players Everywhere*. Retrieved from Business Insider: http://uk.businessinsider.com/lizard-squad-hack-playstation-and-xbox-2014-12#ixzz3MwCLeR9z

Holmes, D. (2015). *The DDoS Threat Spectrum.* Seattle: F5 Networks.

Krebs on Security. (2014, December 29). *Who's in the Lizard Squad?* Retrieved from Krebs on Security: http://krebsonsecurity.com/2014/12/whos-in-the-lizard-squad/

Krebs on Security. (2015, January 9). *Lizard Stresser Runs on Hacked Home Routers*. Retrieved from Krebs on Security: http://krebsonsecurity.com/2015/01/lizard-stresser-runs-on-hacked-home-routers/

Love, D. (2014, December 30). *Why Microsoft And Sony Couldn't Stop Lizard Squad Attack Despite Warnings*. Retrieved from International Business Times: http://www.ibtimes.com/why-microsoft-sony-couldnt-stop-lizard-squad-attack-despite-warnings-1769174

Smith, D. (2014, December 26). *Why Hacker Gang 'Lizard Squad' Took Down Xbox Live And PlayStation Network*. Retrieved from Business Insider: http://www.businessinsider.com/why-hacker-gang-lizard-squad-took-down-xbox-live-and-playstation-network-2014-12

Wickipedia. (2015, March 28). *Lizard Squad*. Retrieved from Wikipedia: http://en.wikipedia.org/wiki/Lizard_Squad

Wikipedia. (2015, April 10). *Playstation Network*. Retrieved from Wikipedia: http://en.wikipedia.org/wiki/PlayStation_Network

Wikipedia. (2015, March 30). *Xbox Live*. Retrieved from Wikipedia: http://en.wikipedia.org/wiki/Xbox_Live