Carl Patterson

Ping Chung

Privacy and Internet Security

April 2019

Malware and Vulnerabilities: Why swift updates are important

Picture this scenario a user is on their laptop or PC, that happens to have Windows 10 installed, doing whatever it is users do, when something pops up on their screen. The computer is saying that it is time to save all documents and shutdown or restart so that it can install some updates. The user ignores this and click it away; they don’t have time to install those pesky updates. A few hours later the user wakes their PC from sleep mode and tries to log in, but it does not work, the screen shows some text that shows instructions on how to buy bitcoins to get their now encrypted files back: they got hit with ransomware.

The above scenario plays out multiple times a day, this is how many people treat updates for their computers. It is not exclusive to Windows users either, I have met multiple MACOS users that simply refuse to install updates and then wonder why they have advertisements popup on their screen every five minutes and I am sure there are stories out there of Linux sysadmins that neglect to install updates for fear it may interfere with critical systems to the business. Many people see security measures as a hindrance to convenience and to them the latter is more important. This is the reason Microsoft decided to force updates on Windows 10 because many users ignore them and then complain when they end up with some type of malware on their PC. According Kaspersky Labs malware “refers to a type of computer program designed to infect a legitimate user's computer and inflict harm on it in multiple ways.”

It is often stated that Windows has the biggest market share of all the major operating systems, according to statcounter.com Windows boasts a 79.46% market share on desktops worldwide, as of March 2019, and 70.45% in the United States. The rest of the worldwide market is shared by MacOS at 14.35%, Linux at 1.7%, Chrome OS at 1.28% and Unknown is 3.2%. These statistics do not paint the full picture however because as mentioned earlier businesses use computers as well and this only tells us of personal use.

Linux dominates the market share for web servers, according to [www.w3cook.com](http://www.w3cook.com), has over 95% market share among the most popular one million websites and 68.2% of the ten thousand most popular websites from the same list. For cloud servers there are no definitive statistics, but according to Dan Price from [www.makeuseof.com](http://www.makeuseof.com), Linux has a 92% share of all instances on Amazon EC2, with windows holding the remaining 8%. In 2017 it was reported that of the top 500 supercomputers in the world 498 of them were using Linux while the remaining two used AIX (Price). On the Mobile side of things, Android, which is based on the Linux kernel, controls 75.33% of the mobile market with its closest competitor being iOS at 22.4% as of March 2019 (statcounter.com).

All the above statistics show that regardless of what operating system you decide to use, it will always be very important to secure computers for both personal and for business use. Both Windows and Linux are extremely popular choices for operating systems and that means that attackers see them both as excellent targets because they could steal data that they would love to get their hands on, which is why they constantly search for vulnerabilities to exploit. A vulnerability is defined by the book Data and Computer security: dictionary of standards concepts and terms as “a weakness in the physical layout, organization, procedures, personnel, management, administration, hardware or software that may be exploited to cause harm to the ADP system or activity.” Regardless of what industry, the size of the business, hackers will attack in order to find some valuable data to sell or to steal money.

According to breachlevelindex.com, the social media industry saw the most data stolen in 2018 a massive 56.18% of all data breaches. The top three is closed off by “other” at 20.14% and hospitality at 10.60%. Data breaches also cost a lot of money, an average of “$3.86 million” according to Rob Sobers. A study done by IBM Corporation in 2018 placed the average cost of a data breach in the US at $7.91 million dollars. The study also shows that the average time it takes a company to discover that they have been breached is 197 days. It goes on to say that companies that discover data breaches in 30 days or less will save on average 1 million dollars compared to other companies.

Aviva Zacks writes that, in 2018 there were a total of 812.67 million malware infections recorded up from 12.40 million in 2009, that is 65.54 times more in just eleven years. This shows the need for securing our computers is always getting more and more important. The once thought-to-be bulletproof MacOS even saw a 165% increase in malware from 2009 to 2018, suggesting that it was only protected by its smaller market share; as it grew popular crackers decided that it was now worth the effort to target (Zacks).

The increase in attacks led many programmers to begin specializing in securing systems and devices. These security researchers spend their days looking for bugs that can be exploited and do their best to produce security patches before the crackers can get to them. Many Companies even have what they call a bug bounty program where they pay white hat hackers who find bugs in their products and report them along with a fix. Companies that do this include RedHat, Tesla, AT&T, Microsoft, Apple, Amazon Web services, GitHub, United Airlines and Facebook. Thomas Claburn wrote in theregister.co.uk that a survey was done to find just how much money can be made from white hat hacking:

According to the survey, approximately 12 per cent of hackers using HackerOne earn at least $20,000 annually from bug bounties, about 3 per cent make more than $100,000, and 1.1 per cent are making more than $350,000. So the majority of bug hunters rely on other income sources.

This shows us that these big companies take their security seriously enough and pay accordingly when they receive some help. One company, Google has even went as far as employing a team of computers scientists whose job it is to find bugs and vulnerabilities, not in Google’s products but instead the products of Google’s competitors. Whenever they discover a weakness, they notify the developers of its discovery and urge them to work on fixing it. Project Zero will then wait a certain number of days, if the exploit is not fixed by then, they release it to the public to force the company to fix the vulnerability. The team is named Project Zero, after the term zero-day exploit (Osborne).

A zero-day exploit is defined on us.norton.com as “a newly discovered software vulnerability. Because the developer has just learned of the flaw, it also means an official patch or update to fix the issue hasn’t been released.” A vulnerability that is either unknown to or not yet patched by the developers of the means that anyone with knowledge of its existence can take full advantage of that without anyone knowing until it is too late or unless they were discovered by and intrusion detection system. Norton’s website says ‘zero-day” means the developers have zero days to get the issue fixed assuming it was already discovered by malicious attackers.

An example of a serious Linux zero-day exploit that was discovered in recent times was the OpenSSL bug called Heartbleed (CVE-2014-0160). Heartbleed only affected Linux because other operating systems like Windows, have their own implementation of SSL that was not susceptible to this bug. TLS/SSL is used to secure data being transported across the internet. It prevents hackers from stealing our credit card information when we make purchases, passwords and usernames, instant messages and our video calls.

Heartbleed bug was a weakness in the way OpenSSL checks to see if a connection is still active even if there was no recent activity. In an article for csoonline.com, Josh Fruhlinger wrote that in order to check the connection either the server or client will send “an encrypted piece of data” to the other and the other party, whose job is to reply with the same piece of data (up to 64 KB) in size, this is called a heartbeat. The problem with this feature is that the length of the message was not actually checked to ensure that it was the same. This means that the server could specify a message of 64KB and send one 20KB in length instead. The client will allocate 64kb of memory for the message but only receive 20KB.

When the client sends the message back it sends 64KB of data to the server, 20 of which is the message and the rest will be whatever data that happens to be sitting in memory waiting to be overwritten. Memory that has been deallocated is not cleaned, to reduce wasting CPU cycles, so whatever data that happened to be stored there before will still be there. An attacker could wind up getting back a piece of data that was stored in memory as a private key or usernames and passwords, meaning they now had access to a database or server or someone’s account. A report from Reuters in 2014 stated Heartbleed was the reason hackers stole the data of “about 4.5 million patients of hospital group Community Health Systems Inc.” The Canada Revenue Agency was also attacked using the Heartbleed vulnerability in 2014, according to Pete Evans, 900 citizens had their social insurance numbers stolen from a government database. After Heartbleed was discovered, developers created a fix for it in version 1.0.1 to prevent any further damage and data loss.

One example of a bug found by Project Zero is the Windows 10 bug (discovered in 2017) that allows a cracker to remotely execute code on their victim’s computer(s) (Osborne, Charlie, ZDNet). The bug was given the common vulnerabilities and exposures (CVE), defined by the NVD Database as “a dictionary that provides definitions for publicly disclosed cybersecurity vulnerabilities and exposures,” number: CVE-2017-0290. The vulnerability was found in Microsoft’s security programs that are installed on Windows, specifically the Microsoft Malware Protection Engine (MsMpEng) (Osborne).

The vulnerability gives crackers the ability to execute code remotely by having Microsoft defender scan a “specially crafted file”, which would give them complete control over an infected system, due to the amont of privilege the MsMpEng has. According to the Project Zero team the bug can be taken advantage of simply by sending an email to the victim, showing that the bug could be exploited by creating a worm to spread the special file to unsuspecting victims. Another similar Windows exploit was discovered by Kaspersky labs and Qihoo 360, CVE-2018-8174. This bug resided in the Vbscript engine and allows attackers to execute code on the victim’s machine. It can be exploited through internet explorer or Microsoft Word documents (Kovacs, Eduard).

Fortunately, these bugs were reported and patched before any serious damage was done, but this was not the case in 2017 when the WannaCry ransomware began spreading across the globe causing a lot of chaos in multiple industries and many large companies. WannaCry was made possible thanks to a leaked National Security Agency (NSA) tool. The agency had known about the exploit, located in the Microsoft Server Message Block (Matt Burgess), as Ellen Nakashima wrote in the Washington Post, for five years. According to Nakashima agency officials contemplated reporting the bug to Microsoft but in the end, they kept it secret, naming the tool EternalBlue. When the company was hacked many of its hacking tools were stolen, including EternalBlue, and released to the public, where it became the catalyst for the creation of WannaCry (Nakashima).

As mentioned earlier WannaCry is categorized as ransomware which is defined by McAfee as “Malware that employs encryption to hold a victim’s information at ransom.” Meaning the victim’s files are encrypted by the ransomware and they are forced to pay in order to get their data back. The malware spread across the globe and created problems in countries like Spain, Russia, USA, England, China, Germany and India. Some global companies and organizations were also hit including the Indian state police, FedEx, the Russian central bank, UKs National Health Service, Americas Homeland Security department and automaker Nissan.

Luckily for us the creators of WannaCry left a loose end in the design of the software. A security researcher from the UK, Marcus Hutchins discovered that the malware had a built-in “kill switch”. Hutchins noticed that WannaCry would periodically try to contact a specific URL before it began to encrypt files (Fruhlinger). Hutchins noticed that the URL was not registered and decided to register the hostname. Once the it was up, WannaCry decrypted the encrypted files and became inactive; saving many from needing to pay to regain access to their data.

The key detail about the WannaCry situation is that the affected machines were not up-to-date with their security patches, else they would not have been affected, because Microsoft had already released a security patch for the vulnerability (MS17-010) before the ransomware began making its rounds. This was another example of companies being lax when it comes to installing updates that cost some of them millions of dollars.

In most cases, vulnerabilities are usually found at the operating system or userspace level, but they can also exist below those levels as well. The Specter and Meltdown bugs was found in code that runs on the CPU which is at the hardware level, which is below both userspace and operating system level. Specter is a group of vulnerabilities, three in total: a “branch target injection” (CVE-2017-5715), “bounds check bypass” (CVE-2017-5753) and a “speculative bounds bypass” (CVE-2017-3639) (Apple). Meltdown (CVE-2017-5754) is described as “rogue data cache load” that allows a user process to read kernel memory and according to Apple, has the “most potential to be exploited.” Apple describes the Specter exploits as “difficult to take advantage of from a locally running program”, however they can be exploited in a web browser with a running JavaScript process.

Specter was a bug in the code for speculative execution. Usenix.org defines it as a technique used in computing to preempt what files or data a process may need from disk. The processor uses time that would otherwise be spent idling to run different simulations in order to try and predict what the process will need next (usenix.org). If the speculation is successful, it passes that data to the process, saving time. If it failed, then no time was lost because only idle CPU cycles were used. An attacker looking to take advantage of Specter would need to force speculative execution. Paul Kocher & Co, states that the methods for taking advantage of Specter “should not have been executed under correct program execution.” Specter allows an attacker to force the CPU to leak data that would be secure under normal circumstances by forcing controlling the speculative execution (Kocher).

Meltdown is a side channel attack that allows hackers to bypass the memory isolation built into the CPU. The attack circumvents the “supervisor bit” that controls how the memory of user and kernel processes are isolated (Moritz Lipp & Co). When an attacker uses this exploit, they gain access to everything stored in memory at that point in time. This “memory dump” can contain sensitive data like keys, passwords and usernames.

Specter and Meltdown received patches very quickly, however this came at a cost to performance. Speculative execution was created to increase performance so patching that issue either changed the features in a way that made it slower or turned some features off completely. Some early reports stated that there was a 30% decrease in performance (Fruhlinger). Later Benchmarks revealed that the performance loss was anywhere between 5% and 10%. Ganesh T.’s benchmarks revealed that the performance reductions depended on the type of process. Steven J and Vaughan-Nichols reported that “highly cached random memory” will show anywhere from 8 to 19 percent performance loss. Database analytics will see 3 to 7 percent loss in performance, high performance computing will lose 2 to 5 percent and accelerator technologies that do not rely on the CPU, for example the GPU, will see less than 2 percent. While it is good that fixes for these exploits were swiftly created, there are many devices that are unable to receive the patches, for example, embedded devices and internet-of-things.

All the above information shows us that it is imperative to be on our toes all the time and just how important installing updates, especially security patches, are in today’s world where computers are used in every aspect of life. From banking to schools, transportation to infrastructure, retail to healthcare every major industry in the world utilizes computers for one reason or another. All these computers need to be properly secured and monitored in order to prevent malicious attackers from either destroying or stealing critical data for their own benefit.

Works Cited

Burgess, Matt. “Everything You Need to Know about EternalBlue – the NSA Exploit Linked to Petya.” *WIRED*, WIRED UK, 29 June 2017, www.wired.co.uk/article/what-is-eternal-blue-exploit-vulnerability-patch. Accessed 30 Apr. 2019.

“CVE-2017-0290.” *CVE*, cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0290. Accessed 29 Apr. 2019.

Claburn, Thomas. “Hehe, Still Writing Code for a Living? It's 2018. You Could Be Earning x3 as a Bug Bounty Hunter.” *The Register® - Biting the Hand That Feeds IT*, The Register, 17 Jan. 2018, www.theregister.co.uk/2018/01/17/bug\_bounties\_pay/. Accessed 28 Apr. 2019.

“Desktop Operating System Market Share United States Of America.” *StatCounter Global Stats*, gs.statcounter.com/os-market-share/desktop/united-states-of-america. Accessed 27 Apr. 2019.

“Desktop Operating System Market Share Worldwide.” *StatCounter Global Stats*, gs.statcounter.com/os-market-share/desktop/worldwide/2019. Accessed 27 Apr. 2019.

Evans, Pete. “RCMP Says It Asked Revenue Canada to Delay Announcing Stolen SINs | CBC News.” *CBCnews*, CBC/Radio Canada, 15 Apr. 2014, www.cbc.ca/news/business/heartbleed-bug-rcmp-asked-revenue-canada-to-delay-news-of-sin-thefts-1.2609192. Accessed 29 Apr. 2019.

Finkle, Jim. “U.S. Hospital Breach Biggest Yet to Exploit Heartbleed Bug: Expert.” *Reuters*, Thomson Reuters, 20 Aug. 2014, www.reuters.com/article/us-community-health-cybersecurity/u-s-hospital-breach-biggest-yet-to-exploit-heartbleed-bug-expert-idUSKBN0GK0H420140820. Accessed 29 Apr. 2019.

Fruhlinger, Josh. “Spectre and Meltdown Explained: What They Are, How They Work, What's at Risk.” *CSO Online*, CSO, 15 Jan. 2018, www.csoonline.com/article/3247868/spectre-and-meltdown-explained-what-they-are-how-they-work-whats-at-risk.html. Accessed 30 Apr. 2019.

Fruhlinger, Josh. “What Is WannaCry Ransomware, How Does It Infect, and Who Was Responsible?” *CSO Online*, CSO, 30 Aug. 2018, www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html. Accessed 30 Apr. 2019.

Fruhlinger, Josh. “What Is the Heartbleed Bug, How Does It Work and How Was It Fixed?” *CSO Online*, CSO, 13 Sept. 2017, www.csoonline.com/article/3223203/what-is-the-heartbleed-bug-how-does-it-work-and-how-was-it-fixed.html. Accessed 29 Apr. 2019.

Gemalto. “Data Breach Statistics by Year, Industry, More.” *Breach Level Index*, breachlevelindex.com/. Accessed 28 Apr. 2019.

Longley, Dennis, et al. *Information Security: Dictionary of Concepts, Standards and Terms*. Stockton Press, 2014.

“Microsoft Patches Two Windows Zero-Day Vulnerabilities.” *SecurityWeek*, www.securityweek.com/microsoft-patches-two-windows-zero-day-vulnerabilities. Accessed 29 Apr. 2019.

“Mobile Operating System Market Share Worldwide.” *StatCounter Global Stats*, gs.statcounter.com/os-market-share/mobile/worldwide. Accessed 27 Apr. 2019.

Nakashima, Ellen, and Craig Timberg. “NSA Officials Worried about the Day Its Potent Hacking Tool Would Get Loose. Then It Did.” *The Washington Post*, WP Company, 16 May 2017, www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82\_story.html. Accessed 29 Apr. 2019.

Osborne, Charlie. “Microsoft Releases Emergency Patch for 'Crazy Bad' Windows Zero-Day Bug.” *ZDNet*, ZDNet, 9 May 2017, www.zdnet.com/article/microsoft-releases-emergency-patch-for-crazy-bad-windows-zero-day-bug/. Accessed 29 Apr. 2019.

Price, Dan. “The True Market Shares of Windows vs. Linux Compared.” *MakeUseOf*, 27 Mar. 2018, www.makeuseof.com/tag/linux-market-share/. Accessed 27 Apr. 2019.

S, Ganesh T. “Meltdown & Spectre: Analyzing Performance Impacts on Intel's NUC7i7BNH.” *RSS*, AnandTech, 23 Mar. 2018, www.anandtech.com/show/12566/analyzing-meltdown-spectre-perf-impact-on-intel-nuc7i7bnh/4. Accessed 30 Apr. 2019.

Sobers, Rob. “56 Must Know Data Breach Statistics for 2019.” *Inside Out Security*, 10 Apr. 2019, www.varonis.com/blog/data-breach-statistics/. Accessed 30 Apr. 2019.

Sydny ShepardJul 17, 2018. “The Average Cost of a Data Breach.” *Security Today*, securitytoday.com/articles/2018/07/17/the-average-cost-of-a-data-breach.aspx. Accessed 30 Apr. 2019.

“What Is Malware?” *McAfee*, www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-malware.html. Accessed 30 Apr. 2019.

“Zero-Day Vulnerability: What It Is, and How It Works.” *Official Site*, us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html. Accessed 29 Apr. 2019.

*Reactive Cost-Benefit Analysis*, www.usenix.org/legacy/publications/library/proceedings/usenix03/tech/fraser/fraser\_html/node17.html. Accessed 30 Apr. 2019.

*Usa.kaspersky.com*, usa.kaspersky.com/resource-center/definitions/zero-day-exploit. Accessed 29 Apr. 2019.

Paul Kocher and Jann Horn and Anders Fogh and Daniel Genkin and Daniel Gruss and Werner Haas and Mike Hamburg and Moritz Lipp and Stefan Mangard and Thomas Prescher and Michael Schwarz and Yuval Yarom. “Specter Attacks: Exploiting Speculative Execution”, 40th IEEE Symposium on Security and Privacy, 2018.

Moritz Lipp and Michael Schwarz and Daniel Gruss and Thomas Prescher and Werner Haas and Anders Fogh and Jann Horn and Stefan Mangard and Paul Kocher and Daniel Genkin and Yuval Yarom and Mike Hamburg. “Meltdown: Reading Kernel Memory from User Space”, 27th Security Symposium (USENIX Security 18), 2018.