FACULTY OF SCIENCE & TECHNOLOGY
Department of Computing & Informatics
Forensic Computing & Security

Computer Fundamentals

Paul-David Jarvis
s5115232@bournemouth.ac.uk

Ransomware & Microprocessors

Table of Contents

Cyber Threat

Ransomware

Ransomware is a malicious program that once installed will stop the user from being able to access their system and encrypt their folders. Users have to pay a ransom to receive a key that will be able to decrypt their files. This payment is usually through bitcoin so it can't be traced.

The most recent and most infamous ransomware attack was the worldwide cyberattack known as 'The WannaCry ransomware attack' The attack happened in May 2017 and targeted computers running a Microsoft Windows Operating System. The ransomware was WannaCry

The creators of WannaCry and the perpetrators of The WannaCry ransomware attack are currently unknown. There are several reports that state that the attack was more of an opportunistic and random attack rather an attack that was created to target the big companies that fell victim. The ransom was extremely low which further suggests that it wasn't planned. Some suggest that WannaCry was developed by government agencies due to the other popular malicious program that also exploited Microsoft vulnerabilities, called EternalBlue which was developed by the National Security Agency. WannaCry uses the exploit found by EternalBlue in Microsoft's software and Operating Systems. They released a patch that would fix this exploit however not everybody updated to the new patch released by Microsoft which left them vulnerable.

The reason why WannaCry was so devastating was because the second version of WannaCry had the ability to act like a worm, this means that not only can WannaCry infect your personal computer, it can also attack every computer on your network that is vulnerable and infected.

WannaCry was estimated to have spreaded to more than 200,000 computers across 150 countries, infecting huge organisations such as the NHS and causing damage ranging from hundreds of millions to billions of dollars. The reason why this ransomware caused this much damaged was because it is not possible to decrypt it without the key. You are only able to get your files back is by restoring a backup or paying the $300 ransom. If the user has not paid the ransom, after 7 days, it will begin to erase the computer files.

There are several methods that can help prevent these types of attacks. The first and most important step is to make sure you have adequate protection. Anti-viruses that feature real-time protection such as Malwarebytes or Kaspersky will detect malware and other malicious programs and will quarantine then remove them.

The second step is to create backups of your data on a regular basis. The best way to protect these backups are by external devices such as a USB thumb drive, the reason is that if you had your backups stored online then they could also be compromised.

Another step is to make sure that you have updated your computer to the latest version. WannaCry took advantage of zero days in Microsoft software. The reason why we should update is when Microsoft discovers a zero day they would instantly work on patching it so on this occasion WannaCry wouldn't be able to use it to spread.

Shortly after the attack, Andrien Guinet, a cyber security researcher from Quarkslab, found that prime numbers from memory weren't being erased after WannaCry encrypted the user's files. This means that these numbers can be used to generate a public and private key. A decryption tool, WanaKiwi, was released that tries to find these prime numbers and generate the two keys to help users to decrypt their files so they won't have to pay the ransom. However, WanaKiwi might not be able to help if the user rebooted their computer and if the memory was overwritten by any other process.

Darien Huss, a network engineer, discovered that WannaCry has one or two "kill switches" built into the ransomware. Meaning that if the kill switch requirements are met then the WannaCry will stop spreading. WannaCry will search for an unregistered domain with a bunch of random letters and numbers, if this domain was found then it will activate the kill switch. Shortly after the developer of WannaCry updated his ransomware to stop this kill switch.

Microprocessors

Evolution of Microprocessors

Microprocessors on the most fundamental level is a big electronic circuit with hundreds of million little switches which are either on or off (1s or 0s). Fast electronic switches are needed, and the key is a semiconductor which is part conductor like copper which allows electricity to flow through extremely easily and part insulator like plastic which stops any electricity flowing through, this in-between state is what allows them to be switched easily. Semiconductors were first discovered at the Royal Institution by Michael Faraday during his experimentation with silver sulphide in 1833. The microprocessor is the brain of the computer. It's responsible for executing several instructions by fetching them, decoding them and then executing those instructions.

The CPU has multiple features like their clock speed or cores. Every CPU has a clock speed, this is the number of instructions that they can process. For example, A CPU with a clock speed of 4.0GHz can process 4 billion instructions a second. The more cores a CPU has means it can

manage more instructions. A CPU with 4 cores can manage 4 times the instructions which drastically improves their performance.

Overtime microprocessors have changed from the very first microprocessor, Intel 4004, to the modern processors such as an Intel Core i9. There are now many more transistors on a single CPU then thought to be possible back when Federico Faggin helped produce the first CPU when he led the research and development project.

The next breakthrough that helped the evolution of microprocessors was with the invention of a transistor. This is a very fast electronic switch with zero moving parts. We use a voltage to switch an electric current off or on. This can switch faster than it takes light to travel only a few millimeters.

The next significant breakthrough was the development of an integrated circuit (IC), This is a piece of silicon built on transistors. With the rapidly development of microprocessors, we will see processors with millions of transistors on their chips and this is by making the transistors smaller and smaller. It was discovered that the smaller the transistor, the faster it was. The positive side to this was that the smaller the transistors, the more you can fit onto a single piece of silicon which would cost less to produce. Gordon Moore, the co-founder of Fairchild semiconductors and Intel released an observation that would be later known as Moore’s Law where the number of transistors is doubling.

In 1971, Intel introduced their first ever single chip microprocessor, the intel 4004. Invented by Federico Faggin, Ted Hoff and Stan Mazor. This single chip CPU has a clock speed of 740 KHz, 2,300 transistors, a single core and is 4-bit. The modern-day processors such as Intel's latest 8th generation, Core™ processors such as their i9, i7, i5 and i3s can have anything from 4 to 18 cores, clock anything from 2GHz to roughly 5GHz and can have from 700 million transistors to a couple of billion. In comparison, that is roughly 4.9 million more KH, 3.9 billion more transistors and 17 additional cores.

References

Cyber Threat

En.wikipedia.org. (2018). *WannaCry ransomware attack*. [online] Available at: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack [Accessed 4 Oct. 2018].

En.wikipedia.org. (2018). *EternalBlue*. [online] Available at: https://en.wikipedia.org/wiki/EternalBlue [Accessed 4 Oct. 2018].

Malwarebytes. (2018). *Ransomware - What Is It & How To Remove It*. [online] Available at: https://www.malwarebytes.com/ransomware/ [Accessed 4 Oct. 2018].BBC News. (2017). *Global manhunt for WannaCry creators*. [online] Available at: https://www.bbc.co.uk/news/technology-39924318 [Accessed 4 Oct. 2018].

Malware Wiki. *WannaCry*. [online] Available at: http://malware.wikia.com/wiki/WannaCry [Accessed 4 Oct. 2018].

Microsoft.com. (2017). *Ransom:Win32/WannaCrypt threat description - Windows Defender Security Intelligence*. [online] Available at: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom:Win32/WannaCrypt [Accessed 4 Oct. 2018].

Curtis, S. (2017). *Who is behind the NHS cyber attack crippling hospital trusts across the UK?*. [online] mirror. Available at: https://www.mirror.co.uk/tech/who-behind-nhs-cyber-ransomware-10410865 [Accessed 4 Oct. 2018].

Microprocessor

Business Casual, 2017. Intel: The Godfather of Modern Computers [video, online]. YouTube. Available from: https://www.youtube.com/watch?v=szaWnH-8OeQ [Accessed 28 September 2018]

Tech Tators, 2018. Evolution of Intel | History of Intel (1971-2018) [video, online]. YouTube. Available from: https://www.youtube.com/watch?v=TqOCC65HkCQ [Accessed 28 September 2018]

Techquickie, 2015. Coding Communication & CPU Microarchitectures as Fast As Possible [video, online]. YouTube. Available from: https://www.youtube.com/watch?v=FkeRMQzD-0Y [Accessed 28 September 2018]

Chris Bishop, 2008. Lecture 1 - Breaking the speed limit [video, online]. The Royal Institution. Available from: http://www.rigb.org/christmas-lectures/watch/2008/hi-tech-trek/breaking-the-speed-limit [Accessed 28 September 2018]

Intel. *Intel | Data Center Solutions, IoT, and PC Innovation*. [online] Available at: https://www.intel.co.uk/content/www/uk/en/homepage.html [Accessed 28 Sep. 2018].