It is a great post about the cyber threats, Aldo. It pointed out the example for the losses on the commonly identified threats. The hackers seek for the system vulnerabilities to achieve their own purpose, which could often result in a financial cost.

One of the new ransomwares, eCh0raix, targets network-attached storage (NAS) including QNAP and Synology (Ruchna, Haozhe & Zhibin, 2021). It targets the devices exposed to the public internet network and plants a backdoor account for attacking actions like file encryption. Although the related NAS vendors can provide fix and recovery tools for the related vulnerabilities (Network & Security, 2021), this ransomware keeps various updates from September 2020 up till now August 2021 which became an ongoing offensive and defensive cyber warfare.

Nevertheless, some ethical hackers are ‘hack for good’. Some of the large organizations offer bug hunting to award ethical hackers like Google offered Vulnerability Rewards Program (VRP). Over the past 10 years since 2010, this program awarded nearly $30 million in total for 2,022 researchers, which found a total of 11,055 bugs (Jan, 2021).

Cyber security is never-ending cyber warfare, it is important for companies to invest with a suitable strategy to prevent the impact during this war.

Reference:

Ruchna, N., Haozhe, Z. & Zhibin, Z. (2021) New eCh0raix Ransomware Variant Targets QNAP and Synology Network-Attached Storage Devices. *Unit 42*. Available from:

<https://unit42.paloaltonetworks.com/ech0raix-ransomware-soho/>

[Accessed 19 Aug 2021].

Network & Security – Security (2021) What should I do when found nas is encrypting my files by 7z?. *Support*. Available from: <https://www.qnap.com/en/how-to/faq/article/what-should-i-do-when-found-nas-is-encrypting-my-files-by-7z> [Accessed 19 Aug 2021].

Jan, K. (2021) A new chapter for Google’s Vulnerability Reward Program. *Google Security Blog.* Available from: <https://security.googleblog.com/2021/07/a-new-chapter-for-googles-vulnerability.html> [Accessed 19 Aug 2021].