Jameson Walter

CS 356 System Security

9/5/2002

Garmin Hack

In July of 2020, the Garmin fitness company was hacked by a Russian Group know as Evil Corp. Their goal was to use a ransomware tool, WasteLocker, to make large parts of the company's software and tools unusable. WasterLocker is a tool that can encrypt large chucks of data and render it useless until the ransom is paid or is decrypted. (Adler) Customers were the first to notice the problem and pointed out the issues to Garmin. Within four days, Garmin announced they had my hacked. (Barrett) Evil Corp demanded 10 million dollars to free the software, which was eventually paid. This attack could spark an onslaught of attacks because the ransom was paid so quickly. It is likely now that hacker groups will target more fortune 500 companies in the future. As said by Graham Cluley, "…the more companies that pay a ransom, the more the criminals are likely to launch similar attacks in the future. At the same time, you may [feel like paying] the criminals if you feel your company cannot survive any other way." More and more companies will likely fall fate to this difficult decision in the future.

Works Cited

Adler, Seth. “Incident of the Week: Garmin Pays $10 Million to Ransomware Hackers Who Rendered Systems Useless.” *Cyber Security Hub*, 28 Mar. 2022, https://www.cshub.com/attacks/articles/incident-of-the-week-garmin-pays-10-million-to-ransomware-hackers-who-rendered-systems-useless.

Barrett, Brian. “The Garmin Hack Was a Warning.” *Wired*, Conde Nast, 1 Aug. 2020, https://www.wired.com/story/garmin-ransomware-hack-warning/.