The Garmin Hack
February 2, 2025
Katie Taylor | CS 356

Garmin was hit by a massive ransomware attack on July 23, 2020. This attack brought many of the services offered by Garmin to a halt. The attackers, the Russian cybercrime group Evil Corp, used ransomware called WastedLocker. Unlike ransomware, which steals data and information in the victim's databases, WastedLocker encrypts the infected host's files and holds them hostage until a ransom is paid. WastedLocker is considered destructive because once those files are locked, they are completely useless until, as just stated, the victim pays the attackers their ransom demand (Pantazopoulos et al., 2020). This is what happened to Garmin. Garmin Services like Garmin Connect, flyGarmin, Strava, and in Reach were all affected essentially overnight. This caused issues for customers with wearable devices, and even some airplanes that utilized Garmin software (Adler, 2020). The malware encrypted their internal systems, which caused these crucial services to shut down. The first sign of this attack was when workers started sharing photos of their encrypted workstations (Terranova Security, 2023). After the files were locked, EvilCorp demanded a ransom of $10,000,000 to restore access to the files. It's widely believed that Garmin paid the ransom. It's believed that a third-party negotiator, a security firm in New Zealand, was hired by Garmin. This company would have acted as the liaison to lawfully pay the $10,000,000 ransom to avoid breaking any sanction laws in the U.S. (Adler, 2020). While it's not been confirmed, it's also believed that this attack was orchestrated through social engineering attacks, as it's a common way these data breaches occur. Social engineering is when the attacker fools or misleads a target to obtain sensitive information or even permits the attacker access to systems and data (ClearBridge, 2022).

Sources:

1. Adler, S (2020). Incident of the week: Garmin pays $20 million to ransomware hackers who rendered systems useless. Cyber Security Hub. Retrieved from https://www.cshub.com/attacks/articles/incident-of-the-week-garmin-pays-10-million-to-ransomware-hackers-who-rendered-systems-useless
2. ClearBridge (2022). 3 things to learn from Garmin's ransomware attack. ClearBridge. Retrieved from https://clearbridge.io/3-things-to-learn-from-garmin-ransomware-attack/
3. Terranova Security (2023). 6 things to learn from the Garmin security breach. Terranova Security. Retrieved from https://www.terranovasecurity.com/blog/garmin-security-breach#:~:text=In%20Garmin%27s%20case%2C%20the%20malware,share%20photos%20of%20encrypted%20workstations
4. Pantazopoulos, N., Antenucci, S., & Sandee, M. (2020). WastedLocker: A new ransomware variant developed by the Evil Corp group. Nccgroup. Retrieved from https://www.nccgroup.com/us/research-blog/wastedlocker-a-new-ransomware-variant-developed-by-the-evil-corp-group/