Garmin’s four-day service meltdown was caused by ransomware

reader comments

82 with 58 posters participating, including story author

Share this story

GPS device and services provider Garmin on Monday confirmed that the worldwide outage that took down the vast majority of its offerings for five days was caused by a ransomware attack.

“Garmin Ltd. was the victim of a cyber attack that encrypted some of our systems on July 23, 2020,” the company wrote in a Monday morning post. “As a result, many of our online services were interrupted including website functions, customer support, customer facing applications, and company communications. We immediately began to assess the nature of the attack and started remediation.” The company said it didn’t believe personal information of users was taken.

Garmin’s woes began late Wednesday or early Thursday morning as customers reported being unable to use a variety of services. Later on Thursday, the company said it was experiencing an outage of Garmin Connect, FlyGarmin, customer support centers, and other services. The service failure left millions of customers unable to connect their smartwatches, fitness trackers, and other devices to servers that provided location-based data required to make them work. Monday’s post was the first time the company provided a cause of the

worldwide outage.

Some employees of the company soon took to social media sites to report that Garmin was taken down by a ransomware attack, which exploits vulnerabilities or misconfigurations to burrow into a company's network. Ransomware operators often spend days or weeks inside, covertly stealing passwords and mapping out network topologies. Eventually, the attackers encrypt all data and demand a ransom paid by cryptocurrency in return for the decryption key.

The aptly named Evil Corp.

Screenshots and other data posted by employees suggested the ransomware was a relatively new strain called WastedLocker. A person with direct knowledge of Garmin's response over the weekend confirmed WastedLocker was the ransomware used. The person spoke on condition of anonymity to discuss a confidential matter.

WastedLocker first came to public attention on July 10, when antimalware provider Malwarebytes published this brief profile. It said that WastedLocker attacks are highly targeted against organizations chosen in advance. During the initial intrusion the malware conducts a detailed analysis of active network defenses so that subsequent penetrations can better circumvent them.

Malwarebytes researcher Pieter Arntz wrote:

> *In general, we can state that if this gang has found an entrance into your network it will be impossible to stop them from encrypting at least part of your files. The only thing that can help you salvage your files in such a case is if you have either roll-back technology or a form of off-line backups. With online, or otherwise connected backups you run the chance of your backup files being encrypted as well, which makes the whole point of having them moot. Please note*

> *that the roll-back technologies are reliant on the activity of the processes monitoring your systems. And the danger exists that these processes will be on the target list of the ransomware gang. Meaning that these processes will be shut down once they gain access to your network.*

Once WastedLocker has taken hold in a network, demands typically range from $500,000 to $10 million. The ransomware name is derived from the extension “wasted” that’s appended to encrypted filenames, which includes an abbreviation of the victim’s name. Each encrypted file comes with its own separate file that contains a ransom note that’s customized for the specific target.

Garmin’s notice on Monday didn’t use the words ransomware or WastedLocker. The description “cyber attack that encrypted some of our systems,” however, all but definitively confirmed that ransomware of one sort or another was the cause.

According to Malwarebytes and other research organizations, the similarities between WastedLocker and an earlier piece of malware known as Dridex tied the ransomware to an organized crime group from Russia known as Evil Corp.

Late last year, federal prosecutors charged the alleged Evil Corp. kingpin Maksim V. Yakubets of using Dridex to drain more than $70 million from bank accounts in the US, UK, and other countries. On the same day prosecutors filed their 10-count indictment, the US Department of Treasury sanctioned Evil Corp. as part of a coordinated action intended to disrupt the Russian-based hacker group, which the department said had taken $100 million from organizations in 40 countries.

Citing an unnamed number of security sources, Sky News reported that Garmin obtained the decryption key. The report lined up with what the person with direct knowledge told Ars. Sky News said Garmin “did not directly make a payment to the hackers,” but didn’t elaborate. Garmin representatives

declined to provide confirmation that the malware was WastedLocker and if the company paid any sort of ransom. The Treasury's action could complicate the already difficult position of Garmin and other Evil Corp. victims by leaving them open to legal actions if they pay the crime gang for return of the encrypted data.

The sun also rises

On Monday, Garmin began slowly restoring location-based services. At the time this post went live on Ars, this page showed that Garmin Connect had returned with limited capabilities for features including Challenges & Connections, Courses, Daily Summary, Garmin Coach, Strava, Third Party Sync, Wellness Sync, and Workouts. Garmin Drive, Live Track, Activity Details and Uploads were fully restored. FlyGarmin and Garmin Pilot, which provides navigation and other services to pilots, had also come back online.

The Garmin outage underscores the major scourge that ransomware has become since it first emerged in 2013, largely as a malware novelty. Not only did ransomware last year cost US governments, health care providers, and educational institutions a combined $7.5 billion, the resulting disruptions can cause hospitals to turn away patients seeking emergency care, dangerous meddling of critical infrastructure, and hardships for millions of end users. The attack Garmin experienced gives little reason to believe law enforcement and the security industry are anywhere close to containing this growing menace.

Post updated to add details about Sky News report.

https://arstechnica.com/?p=1694603