Garmin outage caused by confirmed WastedLocker ransomware attack

bleepingcomputer.com/news/security/garmin-outage-caused-by-confirmed-wastedlocker-ransomware-attack/

Sergiu Gatlan

By
Sergiu Gatlan

- July 24, 2020
- 12:57 PM
- 1

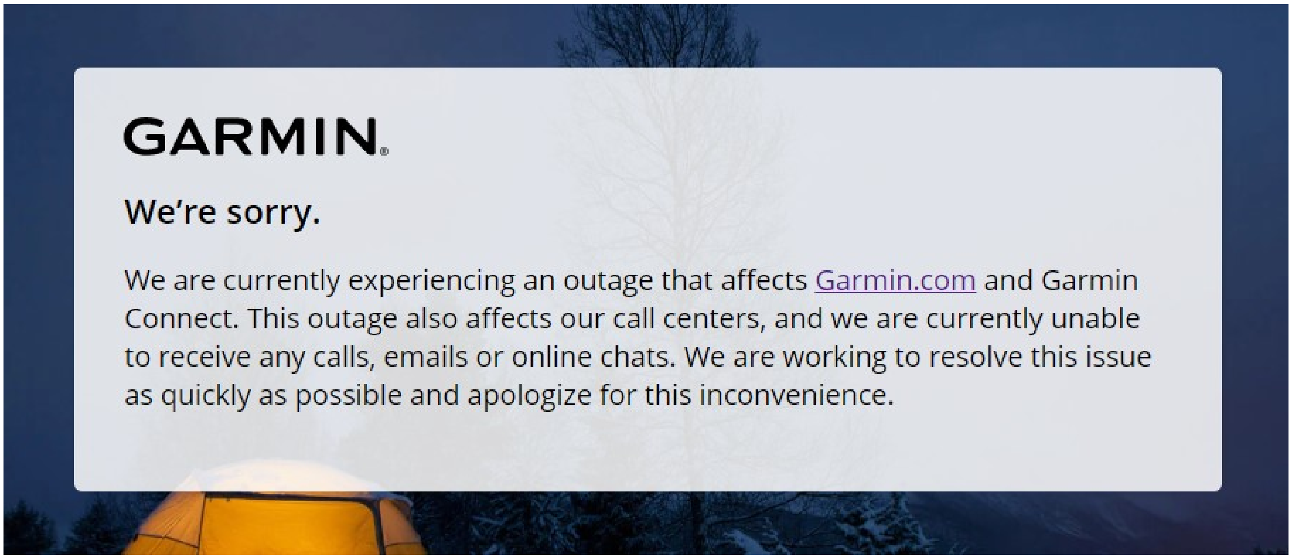
08/01/20 Update: Sources had told BleepingComputer that Garmin paid the ransomware. Today, in a new article we describe how we obtained the WastedLocker decryptor acquired by Garmin and a restoration package created by their IT department.

Wearable device maker Garmin shut down some of its connected services and call centers on Thursday following what the company called a worldwide outage, now confirmed to be caused by a WastedLocker ransomware attack.

Garmin's product line includes GPS navigation and wearable technology for the automotive, marine, aviation, marine, fitness, and outdoor markets.

"We are currently experiencing an outage that affects Garmin.com and Garmin Connect," an outage update notification published on the company's newsroom says.

"This outage also affects our call centers, and we are currently unable to receive any calls, emails or online chats. We are working to resolve this issue as quickly as possible and apologize for this inconvenience."



GARMIN.

We're sorry.

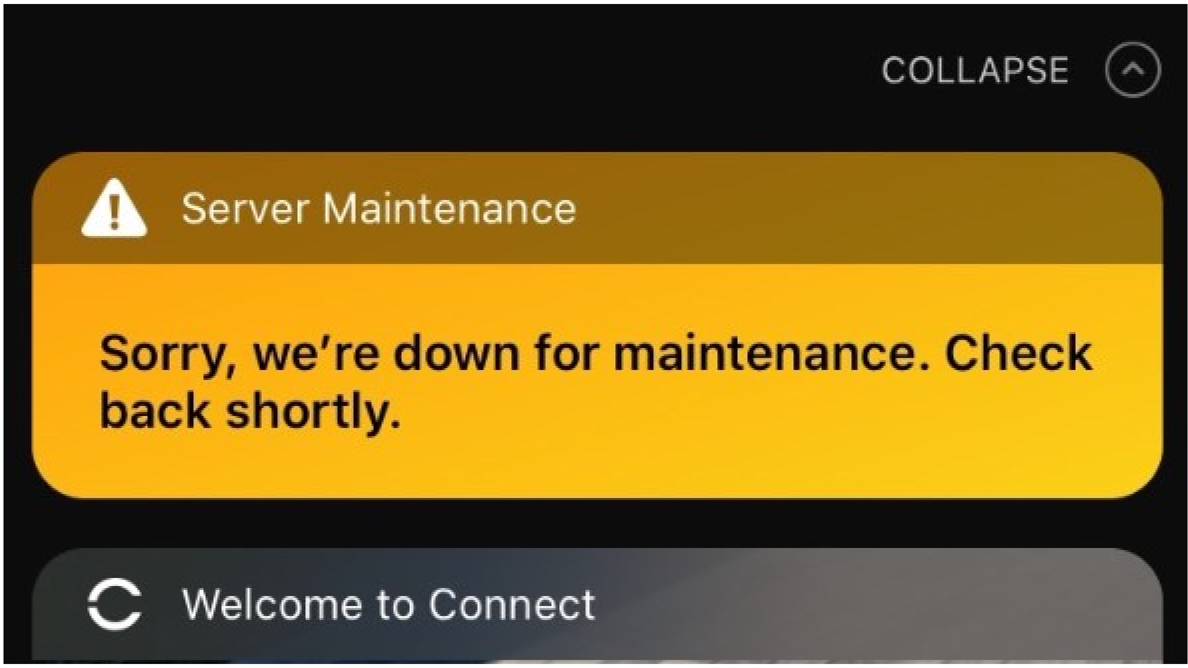
We are currently experiencing an outage that affects Garmin.com and Garmin Connect. This outage also affects our call centers, and we are currently unable to receive any calls, emails or online chats. We are working to resolve this issue as quickly as possible and apologize for this inconvenience.

While Garmin didn't mention it in their outage alert, multiple flyGarmin services used by aircraft pilots are also down, including the flyGarmin website and mobile app, Connext Services (weather, CMC, and position reports) and Garmin Pilot Apps (Flight plan filing unless connected to FltPlan, account syncing, and database concierge).

inReach satellite tech (Service Activation and Billing) and Garmin Explore (Explore site and Explore app sign) used for location sharing, GPS navigation, logistics, and tracking through the Iridium satellite network are also down.

The company's Indian branch first tweeted about some servers being shut down due to planned maintenance nine hours ago that would limit the performance of the Garmin Express, Garmin Connect mobile, and website.

Four hours later, Garmin's main Twitter and Facebook accounts shared the same outage message (1, 2) about the incident impacting Garmin Connect services, including the mobile app and the website, with its call centers also being down due to the outage.



Server Maintenance

Sorry, we're down for maintenance. Check back shortly.

Welcome to Connect

Garmin Connect down for maintenance

> This outage also affects our call centers, and we are currently unable to receive any calls, emails or online chats. We are working to resolve this issue as quickly as possible and apologize for this inconvenience. (2/2)
>
> — Garmin (@Garmin) July 23, 2020

Confirmed WastedLocker ransomware attack

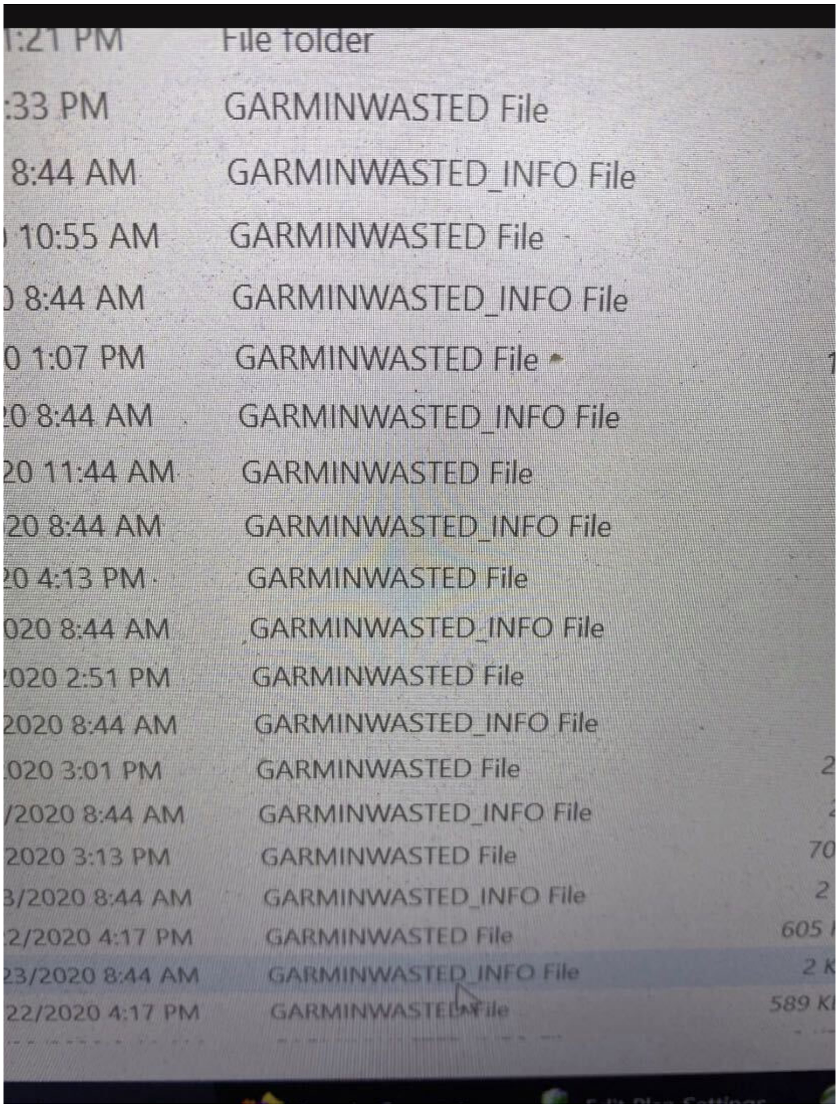
A source close to the Garmin incident response and a Garmin employee confirmed to BleepingComputer that the WastedLocker ransomware attacked Garmin.

A Garmin employee told BleepingComputer that they first learned of the attack when they arrived at their office on Thursday morning.

BleepingComputer was told that the Garmin IT department had tried to remotely shut down all computers on the network as devices were being encrypted, including home computers connected via VPN.

After being unable to do so, employees were told to shut down any computer on the network that they had access to.

In a photo of a Garmin computer with encrypted files shared with BleepingComputer, you can see that the **.garminwasted** extension was appended to the file's name, and ransom notes were also created for each file.



```
:21 PM          File folder
:33 PM          GARMINWASTED File
8:44 AM         GARMINWASTED_INFO File
) 10:55 AM      GARMINWASTED File
) 8:44 AM       GARMINWASTED_INFO File
0 1:07 PM       GARMINWASTED File               1
20 8:44 AM      GARMINWASTED_INFO File
20 11:44 AM     GARMINWASTED File
20 8:44 AM      GARMINWASTED_INFO File
20 4:13 PM      GARMINWASTED File
020 8:44 AM     GARMINWASTED_INFO File
2020 2:51 PM    GARMINWASTED File
2020 8:44 AM    GARMINWASTED_INFO File
020 3:01 PM     GARMINWASTED File               2
/2020 8:44 AM   GARMINWASTED_INFO File          2
2020 3:13 PM    GARMINWASTED File               70
3/2020 8:44 AM  GARMINWASTED_INFO File          2
2/2020 4:17 PM  GARMINWASTED File               605
23/2020 8:44 AM GARMINWASTED_INFO File          2 K
22/2020 4:17 PM GARMINWASTED File               589 KI
```

Source: BleepingComputer

As part of this company-wide shutdown, the employee told us that Garmin did a hard shutdown of all devices hosted in a data center as well to prevent them from possibly being encrypted.

This company-wide shutdown is what caused the global outage for Garmin Connect and other connected services.

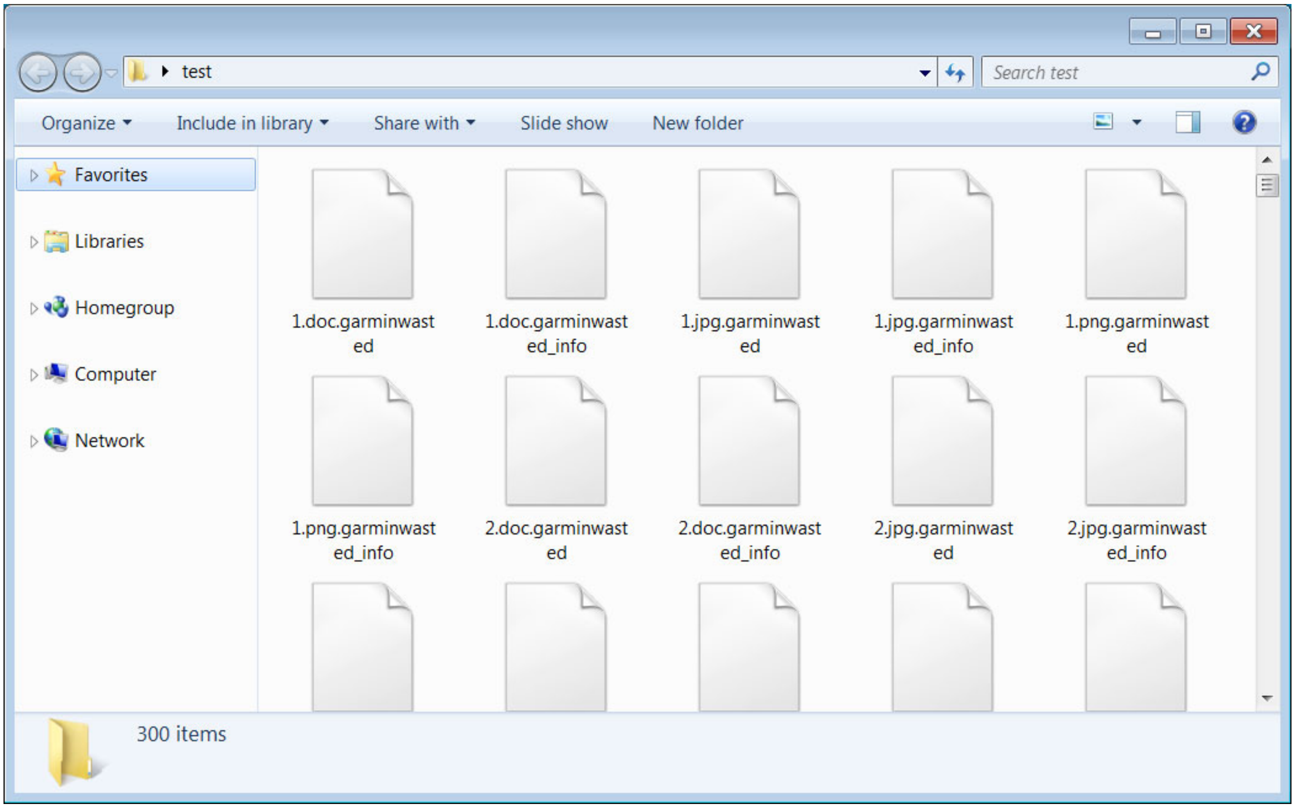
iThome also published a report on a Garmin internal memo earlier about a 'virus' attack affecting the company's internal IT servers and databases that caused Garmin Taiwan factories to shut down production lines for two days (on July 24 and 25th).

If you work at Garmin or know someone working there with first-hand information on this incident, you can confidentially contact us on Signal at +16469613731.

After further research, BleepingComputer found the same WastedLocker ransomware sample used in the attack on Garmin.

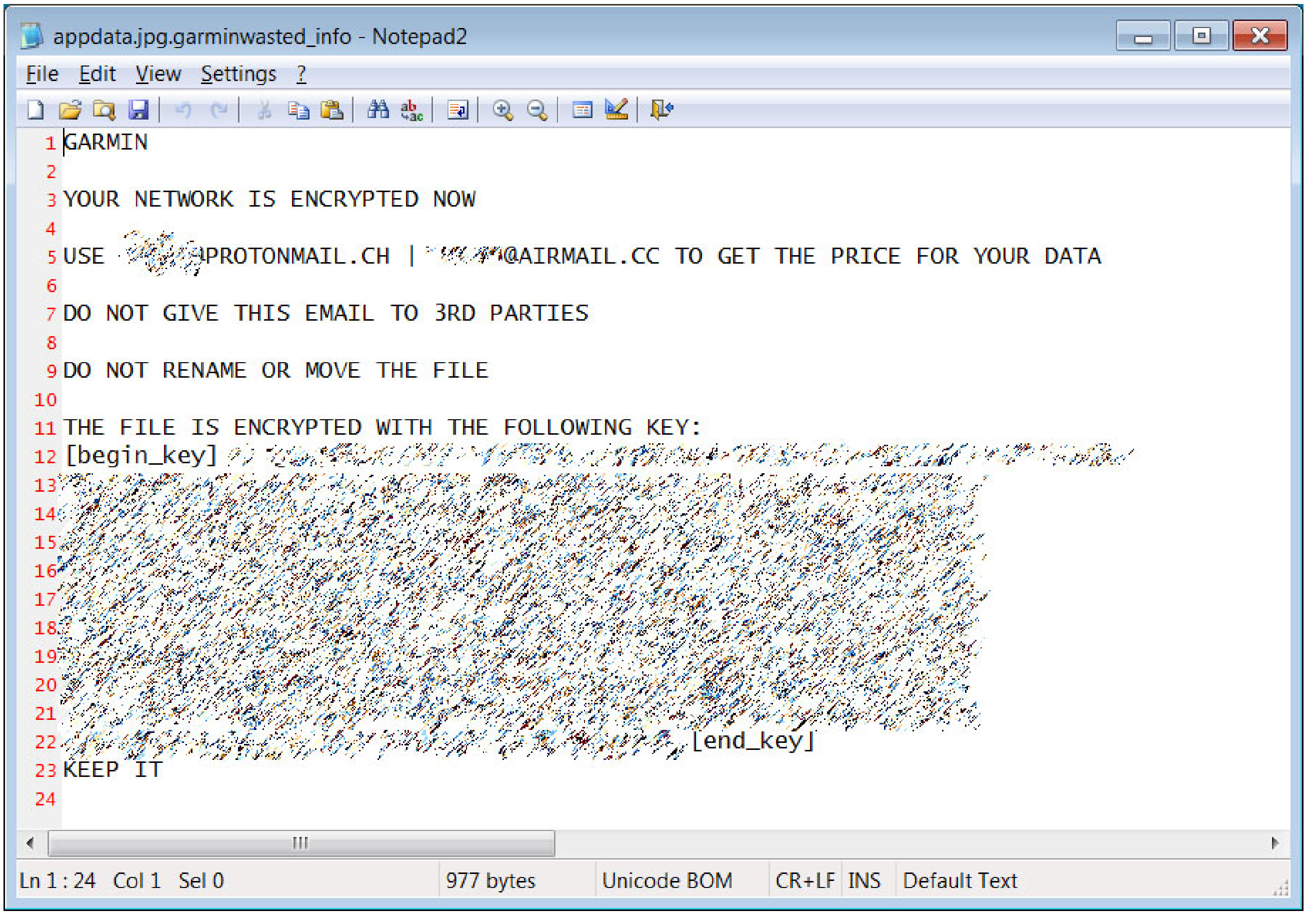
As WastedLocker samples are customized for each target, having access to the sample lets us generate the same ransom note and encrypted files as seen during the attack.

As you can see below, files encrypted with this WastedLocker sample append the same **.garminwasted** extension and create the same **garminwasted_info** ransom note as shown in the photo sent to BleepingComputer by the Garmin employee.



Files encrypted using WastedLocker sample from Garmin
Source: BleepingComputer

Furthermore, the ransom notes generated by the sample are addressed to 'GARMIN', as shown below.



```
GARMIN

YOUR NETWORK IS ENCRYPTED NOW

USE [redacted]PROTONMAIL.CH | [redacted]@AIRMAIL.CC TO GET THE PRICE FOR YOUR DATA

DO NOT GIVE THIS EMAIL TO 3RD PARTIES

DO NOT RENAME OR MOVE THE FILE

THE FILE IS ENCRYPTED WITH THE FOLLOWING KEY:
[begin_key] [redacted] [end_key]
KEEP IT
```

Garmin ransom note

Source: BleepingComputer

Reports state that the attack started in Taiwan, which coincides with the location of one of the users who uploaded the sample to VirusTotal.

BleepingComputer was told by one of the sources that the attackers are demanding a $10 million ransom.

BleepingComputer has not been able to verify this amount independently.

Evil Corp's WastedLocker ransomware

Evil Corp (aka the Dridex gang) is a Russian-based cybercriminal group active since at least 2007 known to be the ones behind Dridex malware and for using ransomware as part of their attacks including Locky ransomware and their own ransomware strain known as BitPaymer.

The U.S. Treasury Department sanctioned evil Corp gang in December 2019 after being charged for using Dridex to cause more than $100 million in financial damages.

Due to this, it is a tricky situation for Garmin if they want to pay the ransom as they would potentially be violating United States sanctions.

Since then, the hacking group has refreshed their tactics once more and are now again involved in the ransomware "business," deploying their new WastedLocker ransomware in targeted corporate attacks and asking for ransoms of millions of dollars.

Evil Corp operators also used WastedLocker ransomware to encrypt systems on Garmin's network, which has led to a significant worldwide outage of multiple services and products, including Garmin Connect, Garmin Explore, Garmin inReach, and flyGarmin.

Last month, Evil Corp was blocked from deploying WastedLocker ransomware as part of dozens of attacks against major U.S. corporations, including multiple Fortune 500 companies.

However, they did manage to compromise devices used by employees of over 30 major US private firms using fake software update alerts displayed by the malicious SocGholish JavaScript-based framework delivered through dozens of hacked U.S. newspaper websites.

07/26/20 Update: Garmin says on a page dedicated to sharing more information about the ongoing outage that they are working to restore systems and that no user data was impacted:

We are working to restore our systems as quickly as possible and apologize for the inconvenience.

Although Garmin Connect is not accessible during the outage, activity and health and wellness data collected from Garmin devices during the outage is stored on the device and will appear in Garmin Connect once the user syncs their device.

Garmin has no indication that this outage has affected your data, including activity, payment or other personal information.

Garmin also says that inReach SOS and messaging (including the MapShare website and email reply page) were not impacted by the outage and they are fully functional.

BleepingComputer has contacted Garmin for more information on this incident, but the mail bounced back as the mail servers are shut down.

Related Articles:

American Dental Association hit by new Black Basta ransomware

Costa Rica declares national emergency after Conti ransomware attacks

New Black Basta ransomware springs into action with a dozen breaches

Wind turbine firm Nordex hit by Conti ransomware attack

[Hackers use Conti's leaked ransomware to attack Russian companies](#)

- Cyberattack
- Evil Corp
- Garmin
- Outage
- Ransomware
- WastedLocker

Sergiu Gatlan

Sergiu Gatlan is a reporter who covered cybersecurity, technology, Apple, Google, and a few other topics at Softpedia for more than a decade. Email or Twitter DMs for tips.

- Previous Article
- Next Article

Comments

GrandJunction - 1 year ago

$10mn ransom, even sanctions- peanuts in comparison.

"July 21st 2020- The market expects Garmin to deliver a year-over-year decline in earnings on lower revenues when it reports results for the quarter ended June 2020. The earnings report is expected to be released on July 29, 2020. This maker of personal navigation devices is expected to post quarterly earnings of $0.38 per share in its upcoming report, which represents a year-over-year change of -67.2%."

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: