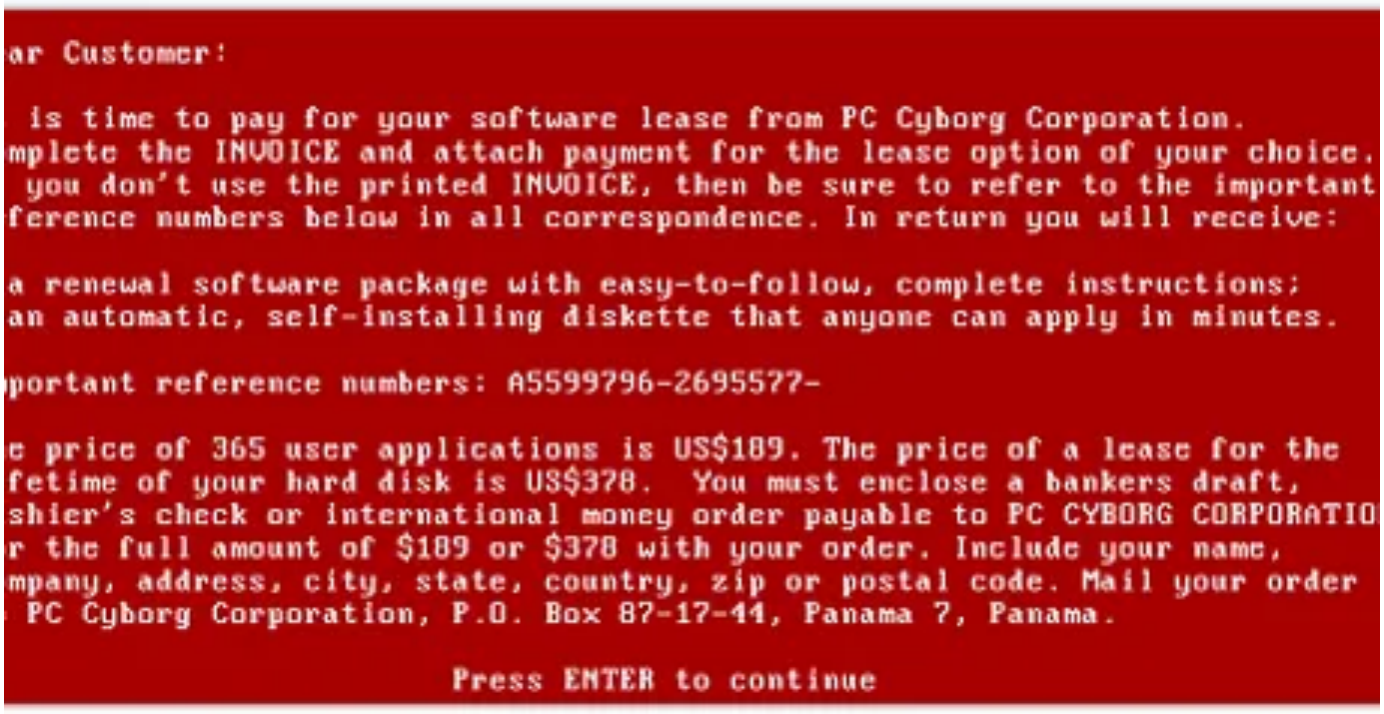
Hacker gang behind Garmin attack doesn't have a history of stealing user data

There's a high probability that Garmin user data might be safe, after all.

Written by **Catalin Cimpanu,** Contributor on July 28, 2020

Image: rottonara

/ executive guide



Ransomware: One of the biggest menaces on the web

Everything you need to know about ransomware: how it started, why it's booming, how to protect against it, and what to do if your PC's infected.

Read now

Read now

Wearables and GPS tracker maker Garmin suffered a ransomware attack last week after a hacker gang breached its internal network and encrypted the company's servers.

The attack caused a five-day outage for the company, during which time, users feared that the hackers might have also stolen their personal details along with geolocation history from the Garmin's servers.

The practice of stealing data before encrypting the victim's network has become widespread today among ransomware gangs, who often use the stolen data into coercing victims into paying the ransom demand.

However, three cyber-security firms who spoke with *ZDNet* this week have said that the hacker group suspected of being behind the Garmin hack is one of the rare groups who don't engage in this particular practice and has no history of stealing customer data before encrypting files.

Attack linked to EvilCorp gang

Known as EvilCorp, this hacker group operates out of Russia, and two of the gang's members have been indicted by US officials last December for operating the Dridex malware botnet.

However, while the group's malware centerpiece is the vast Dridex botnet, the group has also been tied to ransomware operations.

EvilCorp's first forays into the ransomware scene happened in 2016 when the group started distributing the Locky and Bart strains, which they mass-spammed across the internet, targeting home consumers.

Circa 2017, as the ransomware landscape evolved from targeting regular users to attacking companies, the EvilCorp gang also changed their ways with the times and launched BitPaymer, a new ransomware strain they used exclusively in attacks against high-profile targets, such as enterprises, government networks, or

against high-profile targets, such as enterprises, government networks, or healthcare organizations.

But the software landscape evolves, and sometimes code becomes inefficient or malware detections get better. As such, earlier this year, EvilCorp evolved again. The actual reasons are unknown, but according to reports from Fox-IT, Malwarebytes, SentinelOne, and Symantec, around May 2020, the EvilCorp gang started replacing BitPaymer with a newer and better ransomware strain called WastedLocker.

This newer WastedLocker version has been identified as the ransomware that encrypted Garmin's network, according to Garmin employees who spoke with *ZDNet* and to many other news outlets.

No data theft in past BitPaymer and WastedLocker attacks

Yesterday, Garmin formally admitted to suffering a ransomware attack in SEC 8-K filings and a public press release. A particular sentence from the press release caught our eye.

"We have no indication that any customer data, including payment information from Garmin Pay™, was accessed, lost or stolen."

Since Garmin's formal announcement yesterday, *ZDNet* has reached out to cyber-security firms that are known to provide incident response services for ransomware attacks.

In interviews this week, security researchers from Coveware, Emsisoft, and Fox-IT have told *ZDNet* that, historically, they have not seen evidence of user data theft during past BitPaymer and WastedLocker attacks.

"Bitpaymer did not have a history of data exfiltration," Bill Siegel, CEO of Coveware, a company that does incident response and even handles ransomware payments negotiations, told *ZDNet*.

Siegel said the same thing stands for BitPaymer's replacement, WastedLocker; with Emsisoft and Fox-IT confirming Siegel's assessment from their own experience

Emsisoft and Fox-IT confirming Siegel's assessment from their own experience, and the Malwarebytes report claiming the same thing.

"In the WastedLocker cases we were involved in, we didn't see any indication of data being stolen," Emsisoft Chief Technical Officer Fabian Wosar told us in an online chat.

"We have not seen them [EvilCorp] stealing customer data to specifically use to force victims to pay," Frank Groenewegen, Chief Security Expert at Fox-IT, also told *ZDNet* in a phone call.

However, Groenewegen doesn't rule out the fact that some data exfiltration might have taken place, in some form or another.

The Fox-IT exec says that EvilCorp often steals data from a company's network, but this usually includes content such as manuals, employee lists, Active Directory credential dumps, and various other.

The hackers scour this information for details that may aid the EvilCorp hackers in moving laterally across a network and deploying their ransomware to as many computers as possible.

This data could contain small portions of personal information, the Fox-IT exec warns. Furthermore, since logs are usually deleted or encrypted, many companies can't tell right away if user data was stolen.

Nevertheless, EvilCorp is nowhere near the same category as some other ransomware gangs. Groups like Maze, REvil, Ako, CLOP, and others are widely known today to steal huge swaths of data from the networks they hack, data they threaten to publish on "leak sites" to force victims to pay huge ransomware decryption fees.

EvilCorp stole some user data in the past, long ago

But Groenewegen warns that if EvilCorp hasn't visibly stolen data to use in extortions in past BitPaymer and WastedLocker attacks, this doesn't mean they aren't doing it right now, or won't do it in the future.

The Fox-IT exec says that EvilCorp is more than capable of exfiltrating data, referring to older attacks.

"Before they started to focus on deploying ransomware, they used to target payment processors to steal debit/credit card data," Groenewegen said. The EvilCorp gang then turned around and sold this data on carding forums for a profit.

However, based on what the three security firms have told *ZDNet*, currently, Garmin user data appears to be safe, based on the group's past modus operandi.

Of course, this article is not definitive in its assessment, and just speculative analysis of the Garmin incident based on past EvilCorp attacks and the expertise of those involved in respective incident responses.

Europol's top hacking ring takedowns



/ security

How to find and remove spyware from your phone

The best VPN services: How do the top 5 compare?

How to find out if you are involved in a data breach -- and what to do next

The 5 best browsers for privacy: Secure web browsing

How to delete yourself from search results and hide your identity online

Editorial standards