Honda investigates possible ransomware attack, networks impacted

bleepingcomputer.com/news/security/honda-investigates-possible-ransomware-attack-networks-impacted/

Ionut Ilascu

By
Ionut Ilascu

- June 8, 2020
- 11:55 AM
- 1

Computer networks in Europe and Japan from car manufacturer giant Honda have been affected by issues that are reportedly related to a SNAKE Ransomware cyber-attack.

Details are unclear at the moment but the company is currently investigating the cause of the problems that were detected on Monday.

Trouble confirmed, likely SNAKE ransomware

The company has confirmed to BleepingComputer that its IT network is not functioning properly but declined to provide more information regarding the nature of the issue as an investigation is ongoing.

“Honda can confirm that there is an issue with its IT network. This is currently under investigation, to understand the cause,“ a company representative told us.

From what is known at this point, the issues have not influenced the Japanese production or dealer activities. Furthermore, the company spokesperson said that there is no impact on Honda customers.

“In Europe, we are investigating to understand the nature of any impact” - Honda

While the Japanese car manufacturer is tight-lipped about these events, a security researcher named Milkream has found a sample of the SNAKE (EKANS) ransomware submitted to VirusTotal today that checks for the internal Honda network name of "mds.honda.com."

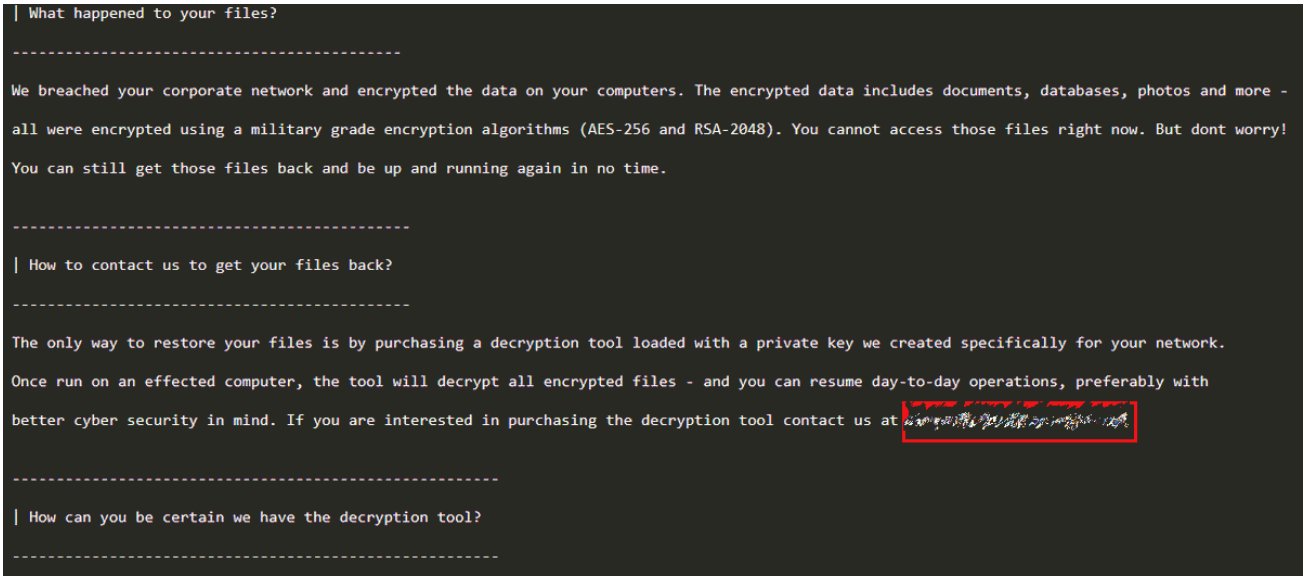
When BleepingComputer tried to analyze the sample, the ransomware would start and immediately exit without encrypting any files.

The researcher states that this is because the ransomware tries to resolve the "mds.honda.com" domain, and failing to do so, will terminate the ransomware without encrypting any files.

Security researcher Vitali Kremez has also told BleepingComputer that in addition to the mds.honda.com check, it also contains a reference to the U.S. IP address 170.108.71.15.

This IP address resolves to the 'unspec170108.amerhonda.com' hostname.

The reference to this IP address and the internal hostname check are very strong indicators that today's network outages are being caused by a SNAKE ransomware attack.



Snake Ransom note dropped by sample found today
credit: milkream

It is unclear how many systems are affected but Snake is known to steal data before deploying the encryption routine. In a statement to BleepingComputer on Tuesday, Honda says that they can "confirm that there is no information breach at this point in time."

"Work is being undertaken to minimise the impact and to restore full functionality of production, sales and development activities. At this point, we see minimal business impact" - Honda representative

BleepingComputer reached out to the SNAKE ransomware operators, and while they did not admit to the attack, they did not deny it either.

"At this time we will not share details about the attack in order to allow the target some deniability. This will change as time passes," the SNAKE operators told BleepingComputer.

Open database leaks sensitive info

If this proves to be an intrusion from an unauthorized party, it would be a significantly different security incident than what the company had to deal with last year when misconfigured databases exposed sensitive information on the public internet.

At the end of July 2019, security researcher Justin Paine found an unsecured ElasticSearch database containing information on about 300,000 Honda employees across the world, including the CEO.

Apart from personally identifiable information, the database instance included details about machines on the network, like the version of the operating system, hostnames, and patch status.

According to Paine's research, a table called "uncontrolledmachines" listed systems on the internal network that did not have security software installed.

"If an attacker is looking for a way into Honda's network knowing which machines are far less likely to identify/block their attacks would be critical information. These "uncontrolled machines" could very easily be the open door into the entire network," Paine said

Another open ElasticSearch database belonging to Honda was discovered on December 11 last year by security researcher Bob Diachenko. The records were unprotected on the public internet and included data about customers in North America.

The database was from a data logging and monitoring server for telematics services. It included full names, email addresses, phone numbers, postal addresses, vehicle make and model, as well as its identification number (VIN).

The company estimated that about 26,000 unique consumer-related records were exposed due to the misconfigured database.

Update 6/8/20: Added information about a Honda IP address in the ransomware executable and a statement from the SNAKE ransomware operators.

Update 6/9/20: Added details from a second statement from Honda about the risk of information breach and the impact on business.

This is a developing story

Related Articles:

BlackCat/ALPHV ransomware asks $5 million to unlock Austrian state

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

SpiceJet airline passengers stranded after ransomware attack

- Honda
- Ransomware
- Snake

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.

- Previous Article
- Next Article

Comments

woody188 - 1 year ago

-
-

I have heard that production was impacted at some plants in the USA. They had just resumed production at some of these plants due to COVID-19 shut downs only to have to shut down again a week later due to this attack. Not that there isn't a glut of vehicles anyhow...

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: