Ransomware gang breached CNA's network via fake browser update

bleepingcomputer.com/news/security/ransomware-gang-breached-cna-s-network-via-fake-browser-update/

Sergiu Gatlan

By
Sergiu Gatlan

- July 22, 2021
- 11:25 AM
- 0

Image: Josh Calabrese, CNA

Leading US insurance company CNA Financial has provided a glimpse into how Phoenix CryptoLocker operators breached its network, stole data, and deployed ransomware payloads in a ransomware attack that hit its network in March 2021.

Two months ago, on May 13, CNA said it began operating "in a fully restored state" after restoring the systems impacted in the attack.

As revealed in a legal notice filed earlier this month, CNA discovered the exact timeline of the ransomware attack following an investigation conducted with the help of third-party security experts hired immediately after discovering the incident.

Network breached via fake browser update

As revealed by the US insurer, the attackers first breached an employee's workstation on March 5 using a fake and malicious browser update delivered via a legitimate website.

The ransomware operator obtained elevated privileges on the system via "additional malicious activity" and then moved laterally through CNA's network, breaching and establishing persistence on more devices.

"Between March 5 and March 20, 2021, the threat actors conducted reconnaissance within CNA's IT environment using legitimate tools and credentials to avoid detection and to establish persistence," the legal notice filed with New Hampshire's Attorney General Office reveals.

"On March 20 and into March 21, 2021, the Threat Actor disabled monitoring and security tools; destroyed and disabled certain CNA back-ups; and deployed ransomware onto certain systems within the environment, leading CNA to proactively disconnect systems globally as an immediate containment measure."

Sources familiar with the attack told BleepingComputer that the Phoenix CryptoLocker encrypted more than 15,000 systems after deploying ransomware payloads on CNA's network on March 21.

BleepingComputer also learned that the ransomware operators encrypted remote workers' devices logged into the company's VPN during the attack

"Prior to deploying the ransomware, the Threat Actor copied, compressed and staged unstructured data obtained from file shares found on three CNA virtual servers; and used MEGAsync, a legitimate tool, to copy some of that unstructured data from the CNA environment directly into the threat actor's cloud-based account hosted by Mega NZ Limited," the company added.

Stolen data not sold or traded with others

As CNA further discovered, the stolen files included sensitive info (names, Social Security numbers, dates of birth, benefits enrollment, and/or medical information) belonging to employees, former employees and their dependents, and, in roughly 10% of cases, customers.

The investigation also found that the attackers only exfiltrated data to the MEGAsync account seized with the help of the FBI and Mega. Based on info provided by the cloud storage platform, the stolen CNA data was not shared outside the attackers' Mega account.

Taking into account the results of the ransomware attack investigation, CNA says that "there is no evidence that the threat actor viewed, retained or shared the exported data and, thus, no risk of harm to individuals arising from the incident."

Despite this conclusion, CNA still decided to notify impacted individuals earlier this month of a potential data breach after the March Phoenix CryptoLocker ransomware attack.

According to breach information filed by CNA with the office of Maine's Attorney General, this data breach affected 75,349 individuals.

Potential links to sanctioned cybercrime group

Based on source code similarities, Phoenix Locker is believed to be a new ransomware strain developed by the Evil Corp hacking group to avoid anctions after victims of WastedLocker ransomware no longer paid ransoms to avoid fines or legal action.

When asked by BleepingComputer about a possible connection between the sanctioned Evil Corp and Phoenix Locker, CNA said there was no confirmed link.

"The threat actor group, Phoenix, responsible for this attack, is not a sanctioned entity and no US government agency has confirmed a relationship between the group that attacked CNA and any sanctioned entity," the company said.

CNA is considered the seventh-largest commercial insurance company in the US, per stats from the Insurance Information Institute.

The insurer provides an extensive array of insurance products, including cyber insurance policies, to individuals and businesses across the US, Canada, Europe, and Asia.

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

- CNA
- Insurance
- Phoenix Cryptolocker
- Ransomware

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

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: