Insurance giant CNA hit by new Phoenix CryptoLocker ransomware

bleepingcomputer.com/news/security/insurance-giant-cna-hit-by-new-phoenix-cryptolocker-ransomware/

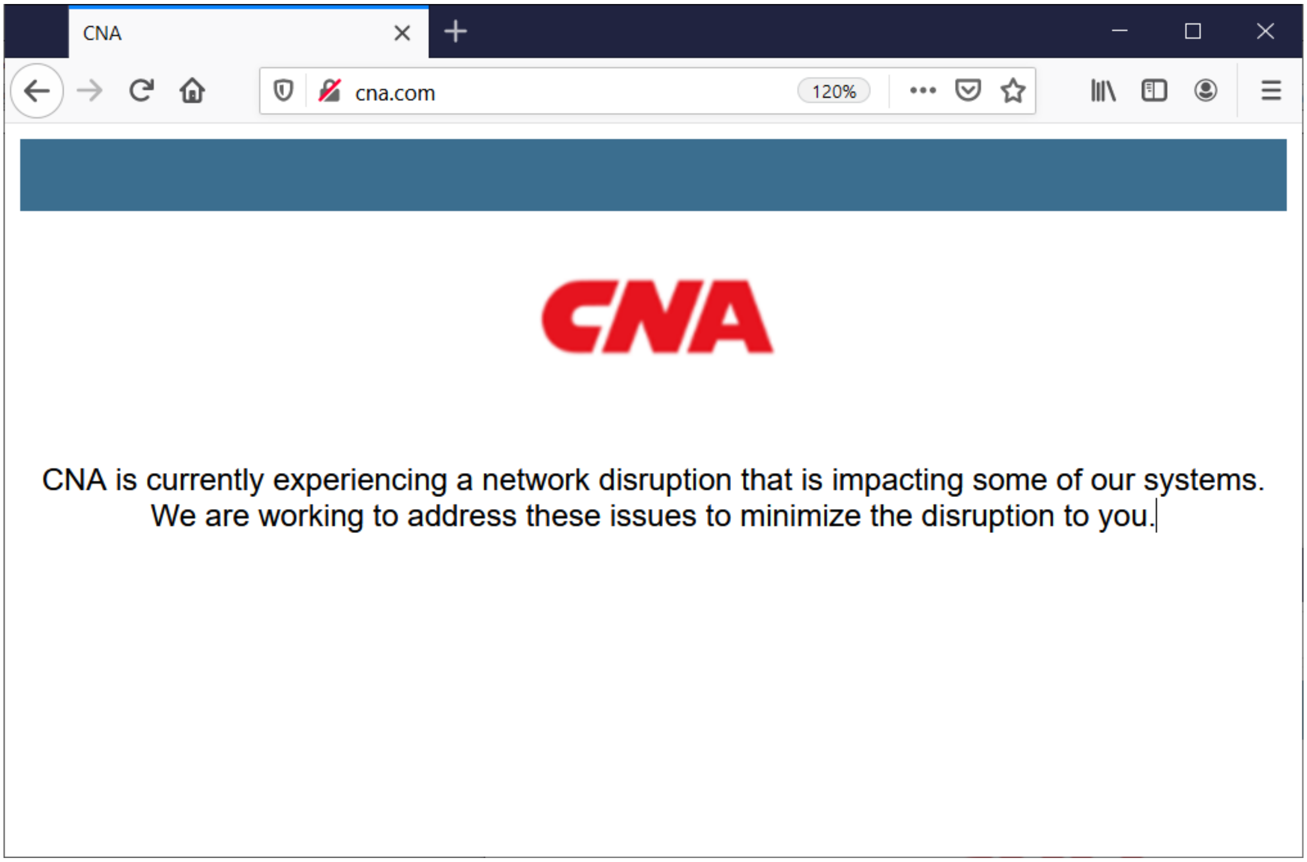
Lawrence Abrams

By
Lawrence Abrams

- March 25, 2021
- 02:26 PM
- 0

Insurance giant CNA has suffered a ransomware attack using a new variant called Phoenix CryptoLocker that is possibly linked to the Evil Corp hacking group.

This week, BleepingComputer reported that CNA had suffered a cyberattack impacting their online services and business operations.



CNA is currently experiencing a network disruption that is impacting some of our systems. We are working to address these issues to minimize the disruption to you.

CNA website outage caused by the ransomware attack

Soon after we reported on the attack, CNA issued a statement confirming that they had suffered a cyber attack last weekend.

"On March 21, 2021, CNA determined that it sustained a sophisticated cybersecurity attack. The attack caused a network disruption and impacted certain CNA systems, including corporate email," CNA disclosed in a statement.

If you have first-hand information about this or other unreported cyberattacks, you can confidentially contact us on Signal at +16469613731 or on Wire at @lawrenceabrams-bc.

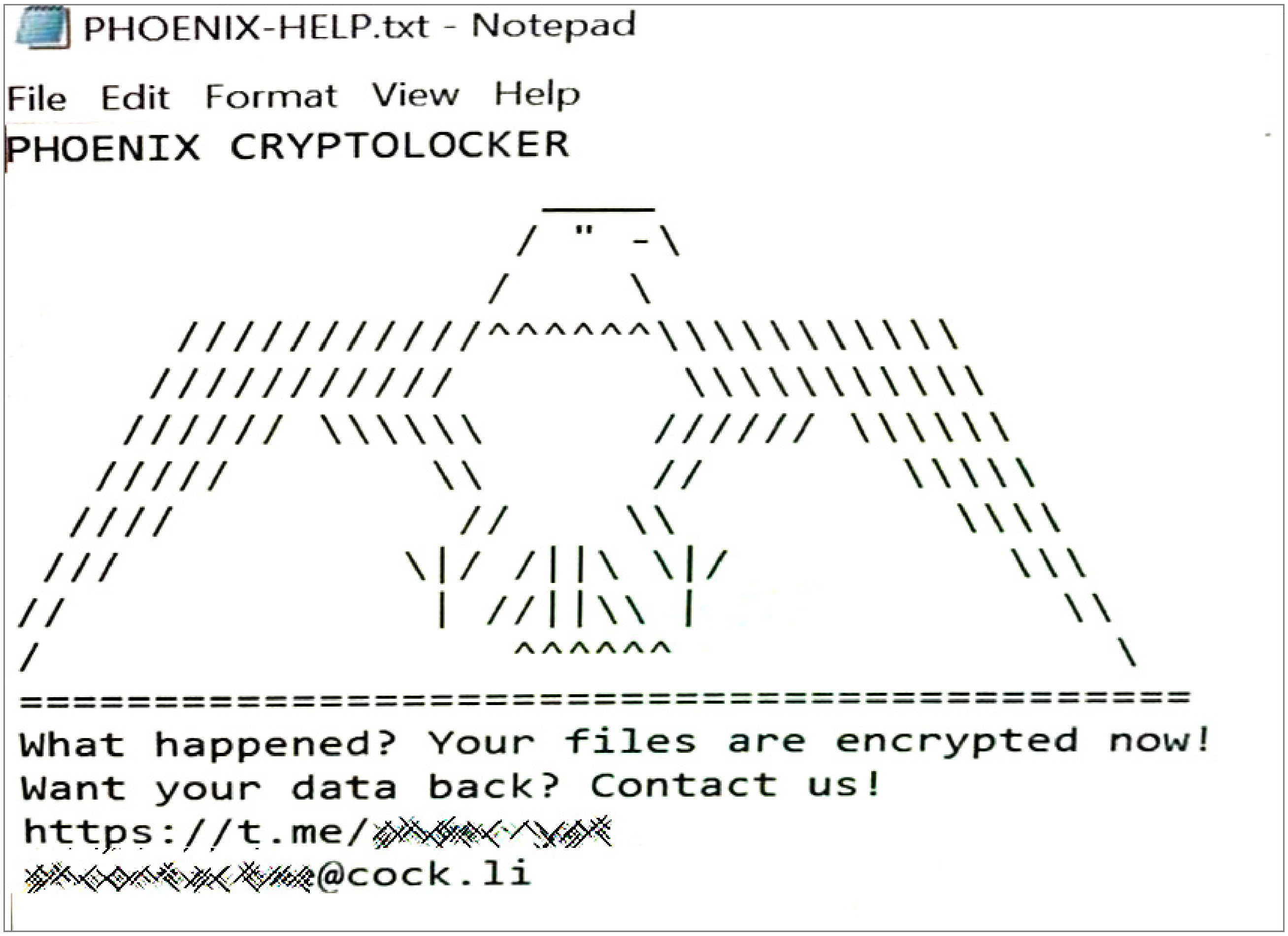
CNA hit by a ransomware attack

Since our first reporting, BleepingComputer has confirmed that CNA suffered an attack by a new ransomware known as 'Phoenix CryptoLocker.'

Sources familiar with the attack have told BleepingComputer that the threat actors deployed the ransomware on CNA's network on March 21, where it proceeded to encrypt over 15,000 devices on their network.

BleepingComputer has learned that it also encrypted the computers of employees working remotely who were logged into the company's VPN at the time of the attack.

When encrypting devices, the ransomware appended the **.phoenix** extension to encrypted files and created a ransom note named **PHOENIX-HELP.txt**, as shown below.



```
PHOENIX CRYPTOLOCKER

                   ____
                  / " -\
                 /    \
      ///////////^^^^^^\\\\\\\\\\\
     ///////////        \\\\\\\\\\\
    ////// \\\\\\      ////// \\\\\\
   /////       \\      //       \\\\\
  ////          //    \\          \\\\
 ///          \|/ /||\ \|/          \\\
//             | //||\\ |             \\
/                 ^^^^^^                \
==========================================
What happened? Your files are encrypted now!
Want your data back? Contact us!
https://t.me/[redacted]
[redacted]@cock.li
```

Ransom note created during CNA ransomware attack

BleepingComputer was further told that CNA would be restoring from backups but has not confirmed that with the company.

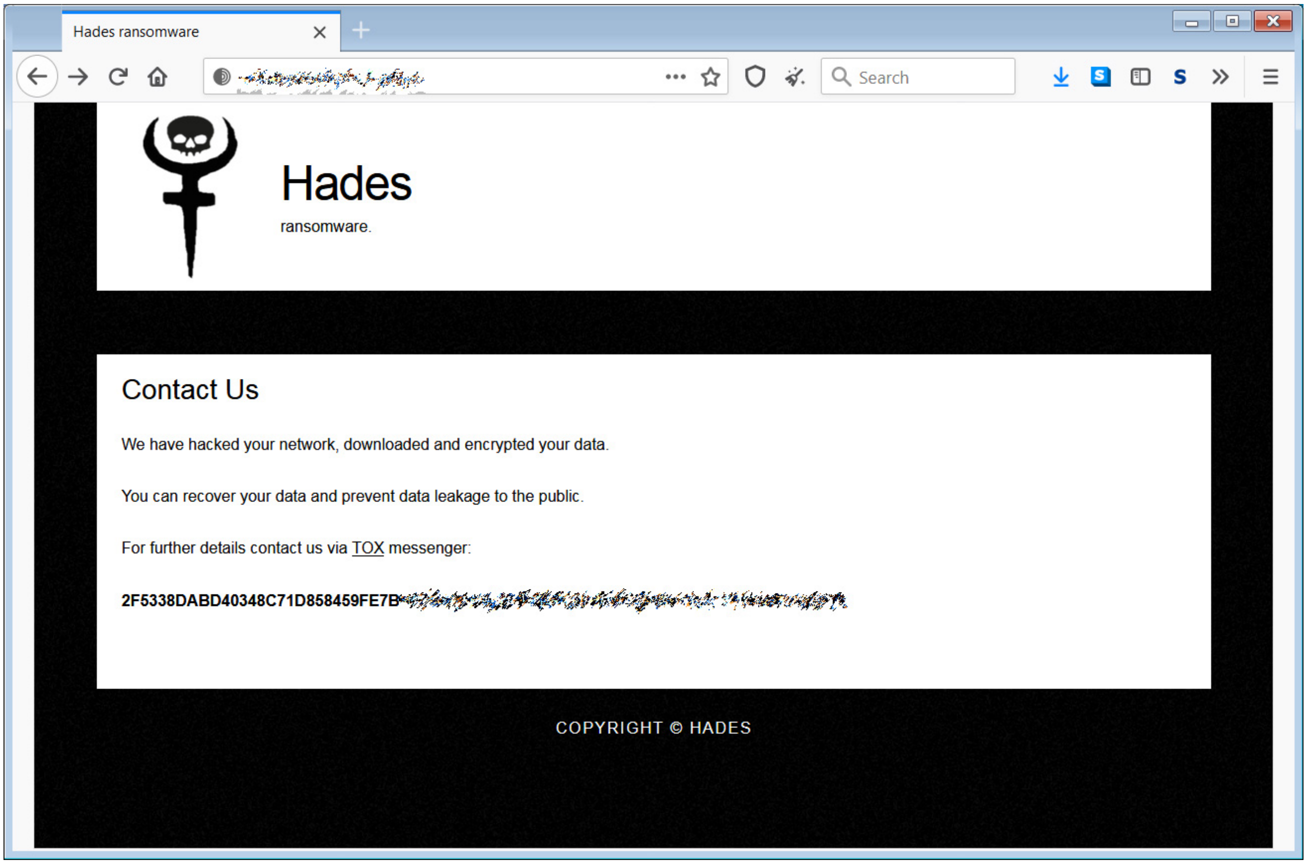
Possible links to Evil Corp

A source has told BleepingComputer that Phoenix Locker is believed to be a new ransomware family released by Evil Corp based on similarities in the code.

Evil Corp historically used the WastedLocker ransomware when conducting attacks against compromised organizations.

Since the US government sanctioned the hacking group in 2019, most ransomware negotiation firms would no longer facilitate WastedLocker ransom payments to avoid facing fines or legal action.

According to a recent CrowdStrike report, the Evil Corp hacking group switched to a new ransomware family called Hades to bypass the US sanctions.



Hades

ransomware.

Contact Us

We have hacked your network, downloaded and encrypted your data.

You can recover your data and prevent data leakage to the public.

For further details contact us via TOX messenger:

2F5338DABD40348C71D858459FE7B[redacted]

COPYRIGHT © HADES

Hades Tor site

The new Hades ransomware family has been seen in multiple attacks since then, including a ransomware attack on trucking giant Forward Air.

However, CrowdStrike's analysis has shown that Hades is simply a rebranded version of their previously used WastedLocker ransomware.

The new Phoenix Locker ransomware used in the CNA attack is believed to be another Evil Corp spinoff.

When BleepingComputer asked CNA about a connection between the sanctioned Evil Corp and the Phoenix group, they replied that there was no confirmed nexus.

> "The threat actor group, Phoenix, responsible for this attack, is not a sanctioned entity and no U.S. government agency has confirmed a relationship between the group that attacked CNA and any sanctioned entity. We have notified the FBI of this incident and are actively cooperating with them as they conduct their investigation of the incident."

Cyberinsurance companies are a valuable target

The attack on CNA could have tremendous impact on other companies, especially those that have cyberinsurance policies through the company.

Conducting attacks on companies with cyberinsurance policies are often lucrative for ransomware gangs as the insurance companies may be more likely to pay the ransom.

There could be no better way to create a list of insured companies to target than to hack an insurer's network and steal policy information about their customers.

Using this information, a ransomware operation can create a list of insured companies and their policy limits. The ransomware operators could then create ransom demands tailored around a particular victim's policy coverage.

At this time, it is not known if the threat actors stole unencrypted files before encrypting CNA's devices.

However, stealing unencrypted data has become a common tactic used by ransomware operations, so it is likely that some data was stolen during the attack.

Related Articles:

Costa Rica declares national emergency after Conti ransomware attacks

New Black Basta ransomware springs into action with a dozen breaches

American Dental Association hit by new Black Basta ransomware

Wind turbine firm Nordex hit by Conti ransomware attack

Hackers use Conti's leaked ransomware to attack Russian companies

- CNA
- Cyberattack
- Evil Corp
- Phoenix Cryptolocker
- Ransomware

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- 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: