Chubb Cyber Insurer Allegedly Hit By Maze Ransomware Attack

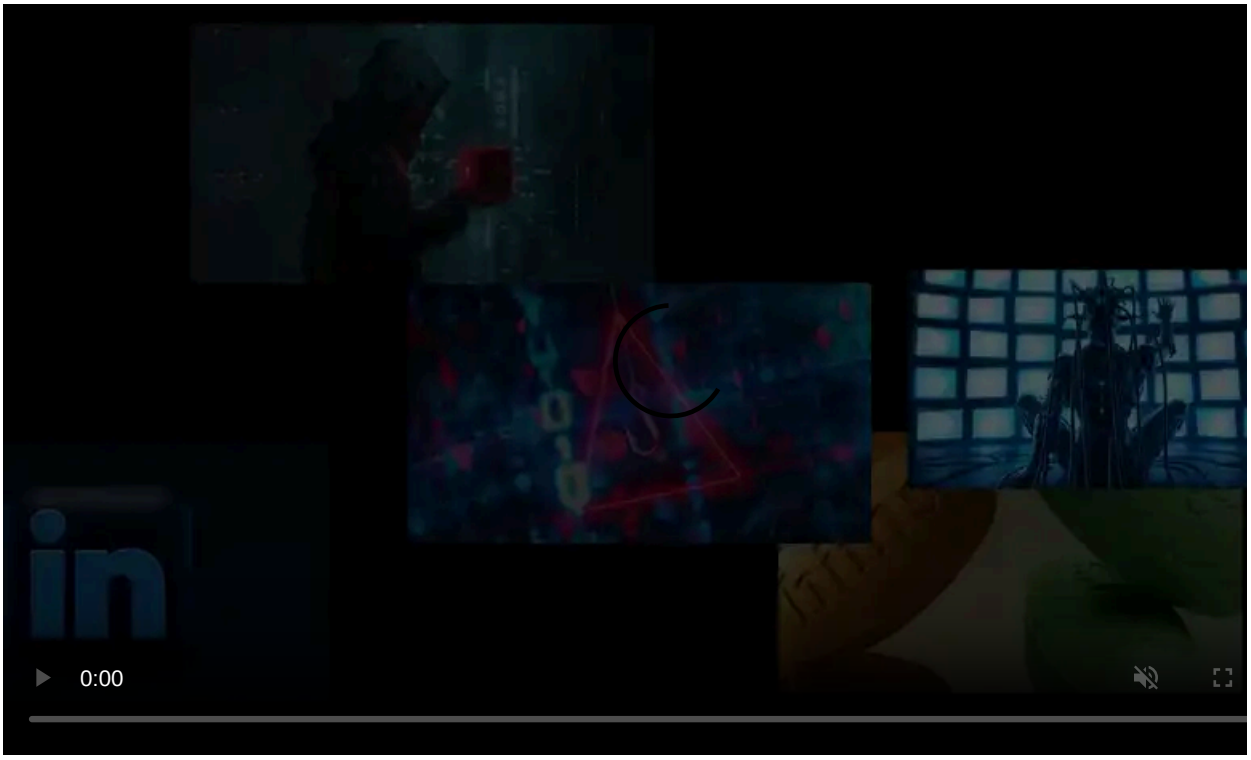
By Lawrence Abrams

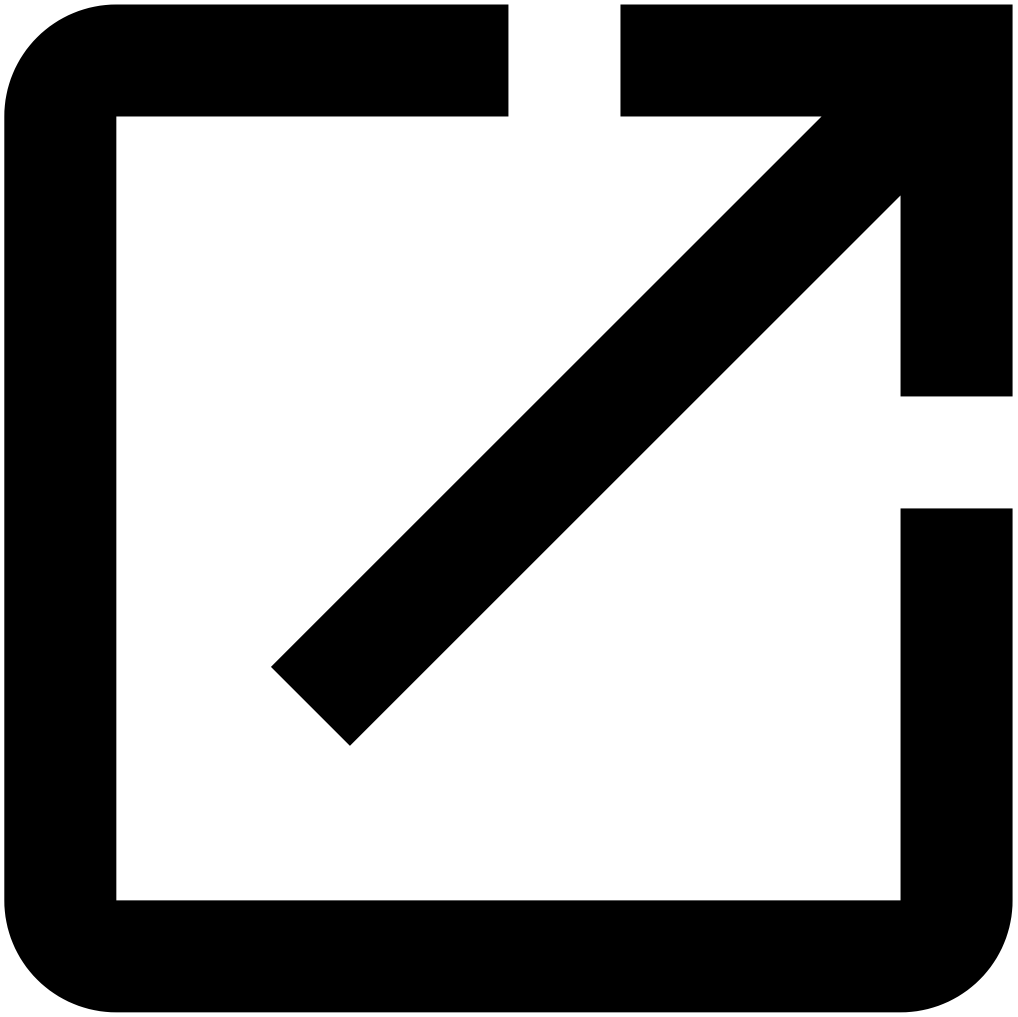
Published: 2020-03-26 · Archived: 2026-04-05 17:35:21 UTC

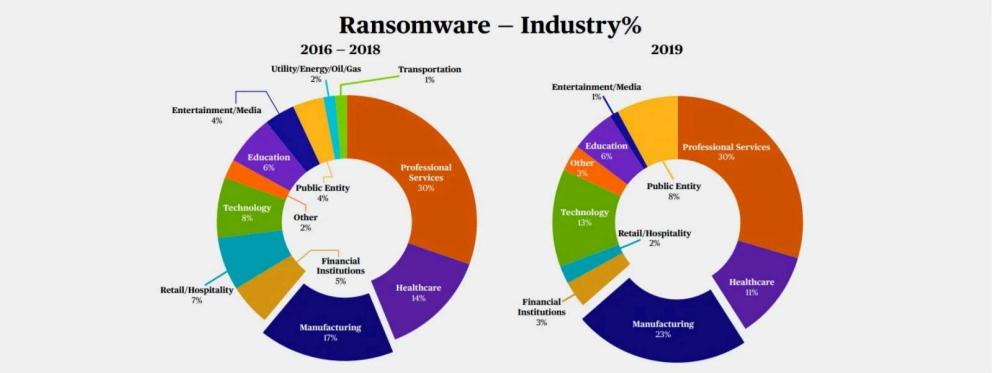
Cyber insurer giant Chubb is allegedly the latest ransomware victim according to the operators of the Maze Ransomware who claim to have encrypted the company in March 2020.

Chubb is one of the leading insurance carriers in the world with an extensive line of cyber insurance products that include incident response, forensics, legal teams, and even public relations.

Ransomware is not unknown to Chubb, as in their 2019 Cyber InFocus Report Chubb explains that malware-related claims have risen by 18% in 2019, with ransomware being responsible for 40% of manufacturer's cyber claims and 23% of cyber claims for smaller businesses.


0:00

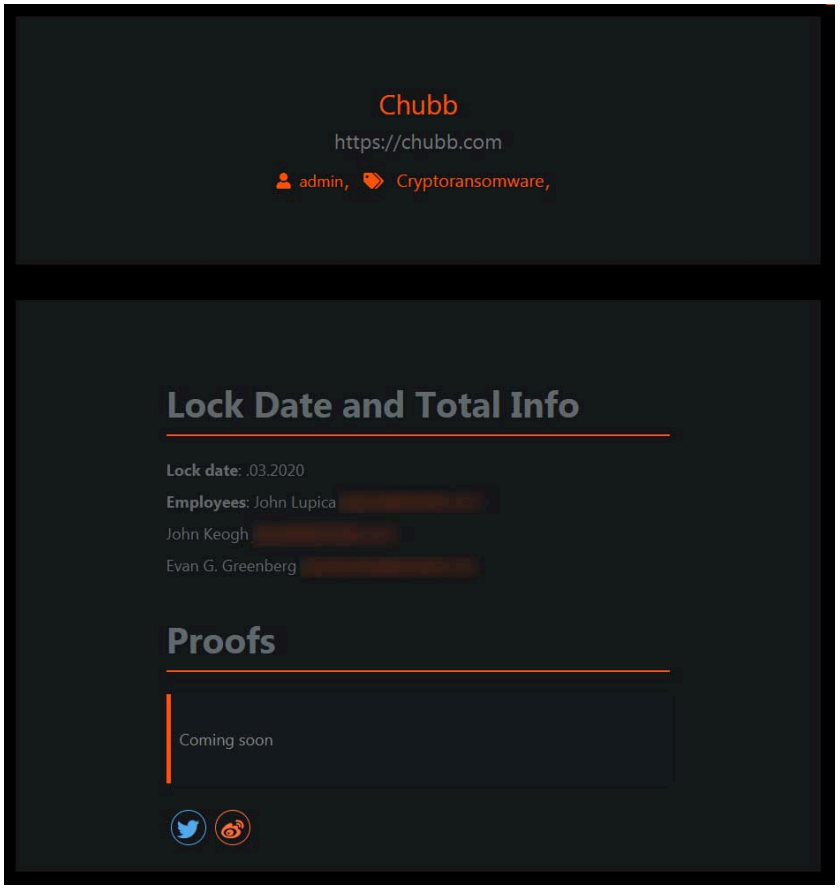




Ransomware targets per industry
Source: Chubb Cyber InFocus Report

Maze claims they encrypted Chubb's network

In a new entry on their Maze 'News' site, the ransomware operators claim to have encrypted devices on Chubb's network in March, 2020.



Chubb Entry on Maze's News Site

As part of these attacks, the Maze operators will steal a company's files before encrypting their network. These stolen files will then be used as leverage by threatening to publicly release it if a ransom is not paid.

Since then, other ransomware operators such as REvil, DoppelPaymer, and CLOP have also begun to adopt this extortion tactic.

After encrypting victims, Maze will create an entry on their news site as a warning to the victim that if they do not pay, their data will be published. If a victim does not pay, the operators publish an increasingly larger amount of stolen data until it is all released.

Maze has not published any of the allegedly stolen data, but have included the email addresses of executives such as CEO Evan Greenberg, COO John Keogh, and Vice Chairman John Lupica. This information, though, should not be considered proof of encryption as the emails are readily available on public websites.

Furthermore, as published stolen data usually contains the personal information of employees and sensitive client information, it causes ransomware attacks to become a data breach. This brings along all of the legal and notification requirements, PR nightmares, and the potential of lawsuits.

In a statement to BleepingComputer, Chubb stated that they are investigating whether this is unauthorized access to their data held at a third-party service provider as there is no evidence that their network was breached.

"We are currently investigating a computer security incident that may involve unauthorized access to data held by a third-party service provider. We are working with law enforcement and a leading cybersecurity firm as part of our investigation. We have no evidence that the incident affected Chubb's network. Our network remains fully operational and we continue to service all policyholder needs, including claims. Securing the data entrusted to Chubb is a top priority for us. We will provide further information as appropriate", Chubb told BleepingComputer.

The Maze operators have told BleepingComputer that they are not providing any further details of the attack at this time.

Vulnerable Citrix gateways on Chubb network

While Chubb states that their network has not been compromised, cybersecurity intelligence firm Bad Packets has stated that the company has numerous Citrix ADC (Netscaler) servers that are vulnerable to the CVE-2019-19871 vulnerability.

This vulnerability has been exploited in the past to hack into networks and install ransomware.

Phobos Group's Dan Tentler also tweeted that Chubb has a Remote Desktop server publicly accessible from the Internet, which is a huge security risk.

According to the FBI, "RDP is still 70-80% of the initial foothold that ransomware actors use."

It is not known if any of these devices were used as part of the attack, but should be secured to enhance perimeter security.

Update 3/26/20: Added information about vulnerable Citrix gateways, RDP servers, and Chubb's statement.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
