San Francisco 49ers confirm ransomware attack

By Catalin Cimpanu

Published: 2023-01-17 · Archived: 2026-04-05 20:11:01 UTC

The San Francisco 49ers NFL team has fallen victim to a ransomware attack that encrypted files on its corporate IT network, a spokesperson for the team has told *The Record*.

The team confirmed the attack earlier today after the operators of the BlackByte ransomware listed the team as one of their victims on Saturday on a dark web "leak site" the group typically uses to shame victims and force them into paying their extortion demands.

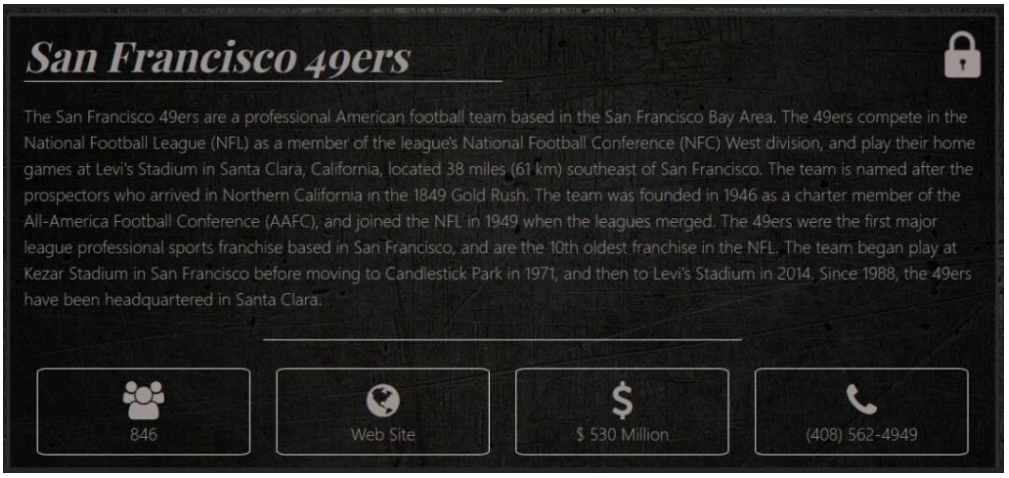

Image: Screenshot of the BlackByte 49ers extortion page (via @CyberKnow20)

"Upon learning of the incident, we immediately initiated an investigation and took steps to contain the incident," the team told us earlier today.

"While the investigation is ongoing, we believe the incident is limited to our corporate IT network; to date, we have no indication that this incident involves systems outside of our corporate network, such as those connected to Levi's Stadium operations or ticket holders," it added.

The team said it notified law enforcement and is working with third-party cybersecurity firms to investigate the attack.

"[W]e are working diligently to restore involved systems as quickly and as safely as possible," the team said.

Attack could have been catastrophic in "what if?" scenario

The attack could have been catastrophic if the team had qualified for Super Bowl LVI, which will take place later today.

The 49ers dramatically lost 17 to 20 after the Los Angeles Rams mounted a 4th quarter comeback in the NFC Championship game two weeks ago.

If they had made it to the Super Bowl, this ransomware attack could have seriously disrupted the team's game preparations, bringing ransomware to the forefront of the US media cycle once again after several high-profile incidents last year, including one that took place over the 4th of July weekend.

Nonetheless, it is unclear how the current attack will impact the team's plan for the next NFL season/year, which will start later this month with the free agency signing period, NFL Combine event, and subsequent NFL Draft.

FBI warns about BlackByte attacks

As for the attackers, the BlackByte ransomware gang is one of the smaller ransomware operations active today, operating on a RaaS (Ransomware-as-a-Service) model where they rent out their ransomware to "affiliates" who then carry out intrusions into organizations and deploy it to encrypt files.

These "affiliates" also steal files from the hacked networks, which the BlackByte gang uses as leverage in negotiations, threatening victims that they will release the stolen files on a dark web "leak site" if they don't pay their extortion demands.

> Leak site for new BlackByte ransomware pic.twitter.com/JGJRBJkpPC
>
> — Catalin Cimpanu (@campuscodi) September 28, 2021

The first BlackByte attacks were seen in September 2021, and this first version of the ransomware was not very well coded, allowing cybersecurity firm Trustwave to find a weakness and use it to create a free decrypter.

In the following weeks, the BlackByte group released a second version, without the encryption bug, which they have been using in attacks since then.

According to an FBI security alert, since November 2021, the agency said the "BlackByte ransomware had compromised multiple US and foreign businesses, including entities in at least three US critical infrastructure sectors (government facilities, financial, and food & agriculture)."

The FBI released its security alert [PDF] on Friday, a day before the attack on the 49ers organization became public, which has led some security experts to believe the document might contain tactics and indicators of compromise from the current 49ers attack.

No previous article

No new articles

Catalin Cimpanu

is a cybersecurity reporter who previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.
