

Ransomware gang says it has hacked 49ers football team

February 14 2022, by Alan Suderman



San Francisco 49ers' Jimmie Ward, left, is called for a penalty as he hits Los Angeles Rams' Odell Beckham Jr. during the second half of the NFC Championship NFL football game Sunday, Jan. 30, 2022, in Inglewood, Calif. Credit: AP Photo/Mark J. Terrill

The San Francisco 49ers have been hit by a ransomware attack, with

cyber criminals claiming they stole some of the football team's financial data.

The [ransomware](#) gang BlackByte recently posted some of the purportedly stolen team documents on a dark web site in a file marked "2020 Invoices." The gang did not make any of its ransom demands public or specify how much data it had stolen or encrypted.

The team, which is among the most valuable and storied franchises in the NFL and lost a close playoff game two week ago, said in a statement Sunday that it recently became aware of a "network security incident" that had disrupted some of its corporate IT network systems. The 49ers said they'd notified [law enforcement](#) and hired cybersecurity firms to assist.

"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," the team said in a statement, referencing its home stadium.

News of the attack comes two days after the FBI and U.S. Secret Service [issued an alert](#) on BlackByte ransomware, saying it had "compromised multiple US and foreign businesses, including entities in at least three US critical infrastructure sectors" since November.

Ransomware gangs, which hack targets and hold their data hostage through encryption, have caused widespread havoc in the last year with high-profile attacks on the world's largest meat-packing company, the biggest U.S. fuel pipeline and other targets. Western governments have pledged to crack down on the cyber criminals, who operate largely in and around Russia, but have little to show for their efforts.

In the past month, ransomware victims have included operators of

maritime fuel depots in Belgium and Germany and media outlets in Portugal. A cyberattack on the wireless provider Vodafone in Portugal this past week had all the hallmarks of ransomware, though the company's CEO for Portugal said it received no ransomware demand.

BlackByte is a ransomware-as-a-service group. That means it's decentralized, with independent operators developing the malware, hacking into organizations or filling other roles. It's part of a trend of ransomware groups becoming increasingly professionalized. A recent report by the FBI, NSA and others said that ransomware operators are even setting up [an arbitration system](#) to resolve payment disputes among themselves.

Brett Callow, a threat analyst at the cybersecurity firm Emisoft, said BlackByte's malware, like many ransomware variants, is hardcoded to not encrypt systems that use Russian or languages used by certain Russian allies.

But Callow said that doesn't mean whoever is behind the 49ers attack is in Russia or one of its neighbors.

"Anyone can use the malware to launch attacks," he said.

© 2022 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed without permission.

Citation: Ransomware gang says it has hacked 49ers football team (2022, February 14) retrieved 6 August 2024 from

<https://techxplore.com/news/2022-02-ransomware-gang-hacked-49ers-football.html>

| |
|--|
| <p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p> |
|--|