Tampa Bay Times hit by Ryuk, new variant of stealer aimed at gov't, finance

By Teri Robinson

Published: 2020-01-28 · Archived: 2026-04-06 02:06:33 UTC

Content

January 27, 2020

On the heels of a Ryuk ransomware attack on the Tampa Bay Times, researchers reported a new variant of the Ryuk stealer being aimed at government, financial and law enforcement targets.

The Times attack didn't result in a breach, noted David Ruiz, 0f Malwarebytes Labs, who cited the Times Publishing Company Chief Digital Officer Conan Gallaty as saying not only did the paper not respond to the attackers, it wouldn't have paid a ransom. Ryuk has been on the rise taking down systems in Lake City, Fla., and at DCH Health System in Alabama.

"From January 1–23, 2020, Malwarebytes recorded a cumulative 724 Ryuk detections. The daily detections fluctuated, with the lowest detection count at 18 on January 6, and the highest detection count at 47 on January 14," Ruiz wrote in a blog post. "The ransomware frequently works in conjunction with Emotet and TrickBot in multi-stage attacks. Those separate malware families have also been active in the new year, with small spikes into the thousands of detections" and Emotet,in particular, kicking "into high gear" again on Jan. 13.

"Ryuk malware has been evolved to make it especially dangerous as it targets government offices, the military and the financial sector with a swiss army knife of malicious software that can penetrate desktops and into the network at a rapid speed," said David Jemmett, CEO and founder of Cerberus Cybersecurity. "It is delivered in the form of a phishing email with attachments designed to dump Trickbot onto the first machine and then deploy other pieces of malware like Emotet armed with mimicats to search out passcodes and credentials."

Malwarebytes researchers also found a new variant of Ryuk Stealer aiming at stealing large volumes of sensitive data from government, financial and law enforcement entities.

"This is an example of how malware is becoming more focused on specific sectors and information in order to efficiently steal the data with the most value, while minimizing the risk of being caught. While this specific malware is a data exfiltrator, the same techniques are being applied to different strains of ransomware in order to encrypt the most valuable files with the least probability of detection," said Erich Kron, security awareness advocate at KnowBe4. "It's the difference between stealing the whole ATM machine versus just stealing the money that is in it."

Kron explained that using an "FTP to exfiltrate the data reinforces the need to not only filter incoming internet traffic at the firewalls, but also to limit and monitor outbound traffic to required services," adding that the FTP

protocol “is not needed by a majority of people, yet allows data exfiltration and even command and control channels for malware.”

Considering the harm it could cause “compared to the typical usage within organizations, careful consideration should be given to allowing FTP connections from corporate networks," he said.

Teri Robinson

Related

DevSecOps Scanning Challenges & Tips

Bill BrennerOctober 26, 2021

There are many ways to do DevSecOps, and each organization — each security team, even — uses a different approach. Questions such as how many environments you have and the frequency of deployment of those environments are important in understanding how to integrate a security scanner into your DevSecOps machinery. The ultimate goal is speed […]

It Should Be 'Cybersecurity Culture Month'

Bill BrennerOctober 19, 2021

It's Cybersecurity Awareness Month, but security awareness is about much more than just dedicating a month to a few activities. Security awareness is a journey, requiring motivation along the way. And culture. Especially culture.That's the point Proofpoint Cybersecurity Evangelist Brian Reed drove home in a recent appearance on Business Security Weekly."If your security awareness program […]

Get daily email updates

SC Media's daily must-read of the most current and pressing daily news

---

Source: https://www.scmagazine.com/home/security-news/tampa-bay-times-hit-by-ryuk-new-variant-of-stealer-aimed-at-govt-finance/