Decryptor released for Prometheus ransomware victims

By Catalin Cimpanu

Published: 2023-01-04 · Archived: 2026-04-05 17:25:10 UTC

Taiwanese security firm CyCraft has released a free application that can help victims of the Prometheus ransomware recover and decrypt some of their files.

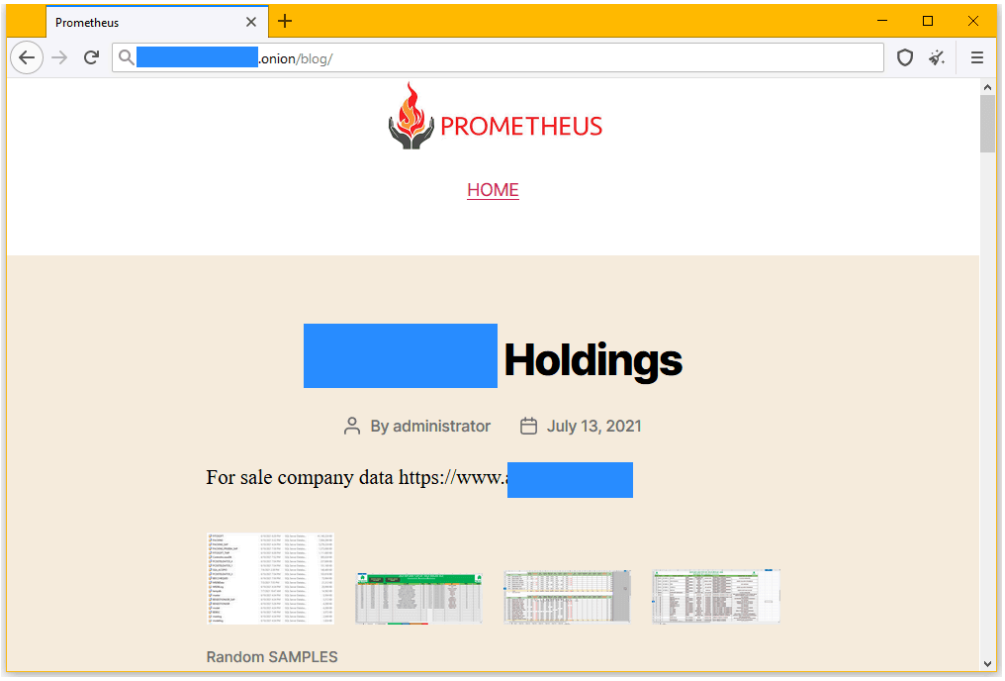
Available on GitHub, the decryptor effectively works by brute-forcing the encryption key used to lock the victim's data.

"[The] Prometheus ransomware use Salsa20 with a tickcount-based random password to encrypt [files]. The size of the random password is 32 bytes, and every character is a visible character. Since the password use [the] tickcount as the key, we can guess it brutally," the company's experts wrote in a blog post at the start of the month.

The only downside of CyCraft's decryptor is that it can only handle brute-forcing the decryption key from small files only, Emsisoft, a company known for breaking several ransomware strains, has told *The Record*.

However, the decryptor's release appears to have had an impact on the activity of the Prometheus gang.

Released on July 13, this also marked the last date when the Prometheus gang published any content on its dark web leak site. Two and a half weeks later, the Prometheus gang appears to have ceased operations.



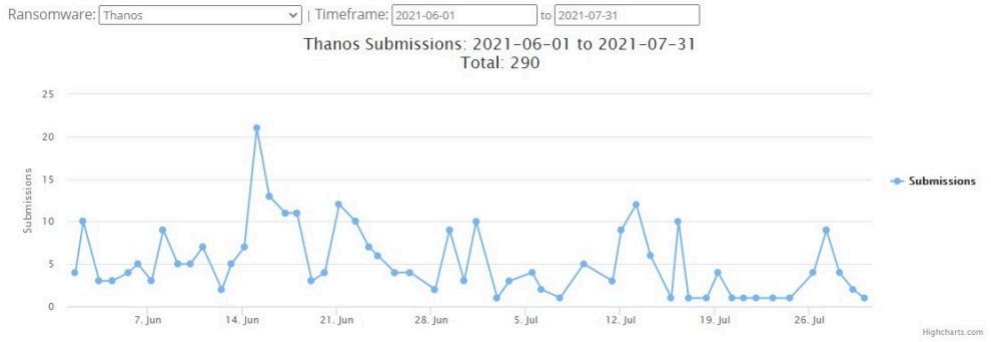
First spotted in February this year, the gang had previously listed more than 40 victims on its leak site. It drew some attention to itself by claiming an association with the more infamous REvil gang, which they removed after the REvil gang's attack on Kaseya.

In fact, codewise, the two ransomware strains couldn't have been more different. REvil was an advanced piece of C++ malware, while Prometheus was based on the leaked code of the Thanos ransomware, coded in C#.

Shortly after Prometheus went silent, a new group called Haron, also operating on top of the Thanos codebase, started attacks, leading some experts to believe that Prometheus operators rebranded as Haron.

An Emsisoft spokesperson did not rule out that the company would eventually create a decryptor for Prometheus and the other Thanos strains that could also recover large files. If they do, the app would be made available on the company's website and the NoMoreRansom portal.

With Thanos-based ransomware strains making new victims on a weekly basis, this might be sooner than later.



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.
