Nemty ransomware operation shuts down public RaaS

By Catalin Cimpanu

Published: 2020-04-15 · Archived: 2026-04-05 23:10:16 UTC

The operators of the Nemty ransomware have announced this week they were shutting down their public Ransomware-as-a-Service operation and opting to go private in order to focus and put more rersources on targeted attacks.

For those unfamiliar with this malware operation, Nemty is a classic RaaS (Ransomware-as-a-Service). It launched in the summer of 2019 and has been heavily advertised on underground Russian-speaking hacking forums.

Users who signed up with the Nemty RaaS were granted access to a web portal where they could create custom versions of the Nemty ransomware.

The customers were then free to distribute these custom versions via their own methods. Over the past few months, the Nemty ransomware has been spotted being distributed via email spam (malspam) campaigns, exploit kits, boobytrapped apps, and by brute-forcing RDP endpoints.

Distribution methods varied based on the Nemty RaaS customer who was spreading that particular Nemty strain.

If any of the victims who had computers infected with Nemty paid the ransom demand, the Nemty operator kept 30% of the payment, while the distributors got %70 for their efforts.

Nemty goes private after 10 months

But in an update posted on a dedicated topic on the Exploit hacking forum, the Nemty operator announced yesterday they were shutting down their RaaS operation and "going private." Going private in the cybercriminal underground means working with a few selected partners to distribute your malware.

The Nemty operator gave victims a week to pay any ransom demands they have before they'd would shut down all servers, and users would be unable to decrypt their files, even if they wanted to pay.

Announcement of the Nemty ransomware shutdown. Text translated from Russian with Google Translate.

Image supplied by Under the Breach

A day after the announcement, the Nemty crew also shut down its "leak site," a portal where the Nemty gang publish files from companies that refused to pay ransom demands.

"Leak site" for the Nemty ransomware

Image: ZDNet

In October 2019, Tesorion security researchers released free decrypters, for three versions of the Nemty ransomware. However, recent versions are not decryptable.

The author of the Nemty ransomware also appears to have shared Nemty's source code with others, as last month a new ransomware strain named Nefilim was spotted online. SentinelLabs' Vitali Kremez and ID Ransomware's Michael Gillespie said the new Nefilim ransomware appears to be based on Nemty's code.

The Nefilim ransomware has been deployed only in a small number of attacks against large companies. It is this modus operandi that the Nemty gang is now hoping to transition to.

Editorial standards