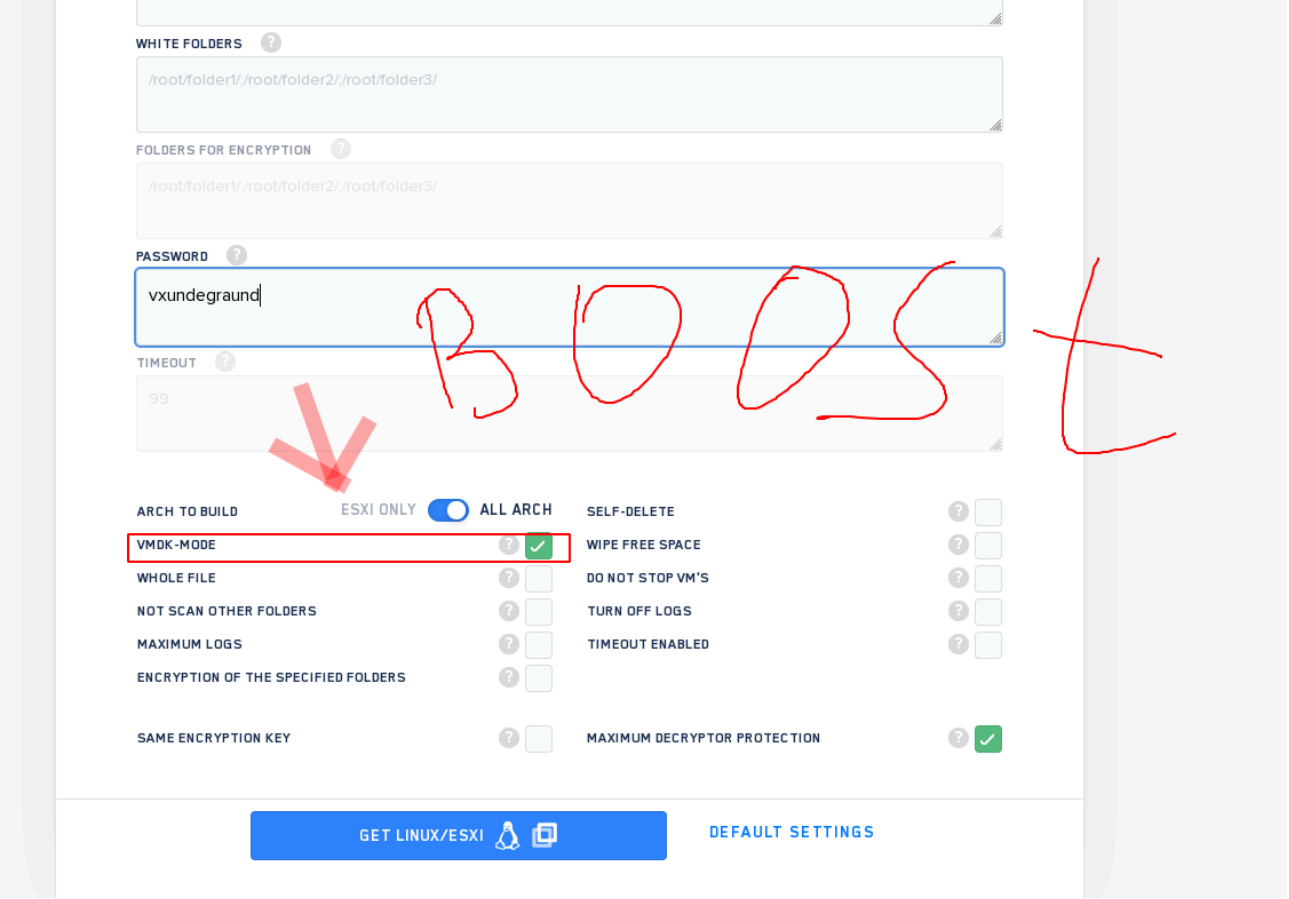
LockBit Green ransomware variant borrows code from Conti one

By Pierluigi Paganini

Published: 2023-02-01 · Archived: 2026-04-05 12:57:49 UTC

Pierluigi Paganini February 01, 2023



Lockbit ransomware operators have released a new version of their malware, LockBit Green, that also targets cloud-based services.

Lockbit ransomware operators have implemented a new version of their malware, dubbed LockBit Green, which was designed to include cloud-based services among its targets.

This is the third version of the ransomware developed by the notorious gang, after the Lockbit Red and Lockbit Black ones. Affiliates to the Lockbit RaaS can obtain LockBit Green using the builder feature on the LockBit portal.

The release of the new version was confirmed by the vx-underground researchers:

According to the researchers who analyzed the new version, the operators have modified their ESXI ransomware variant.

Antonio Cocomazzi, a senior threat intelligence researcher from SentinelOne, reported that the new variant has a significant overlap with the Conti ransomware, whose source code was leaked months ago.

"I conducted an analysis of the sample and found that it has significant overlap (89% similarity) with the #Conti Ransomware, specifically its v3 version, which the source code has been leaked several months ago. The commandline flags for LockBit Green are identical to those of Conti v3, making it a derivative of the original source code." ***explained Cocomazzi****.*

The experts pointed out that only a small part of the source code has been modified by LockBit, including the ransom note which is identical to the one used by the LockBit Black variant.
The ransom note filename has been changed to "!!!-Restore-My-Files-!!!.txt".

The availability of the source code of other malware allows operators to create their own version, improving it, and speeding up the development lifecycle.

"The approach of reusing and adapting the source code of reputable competitors, such as the now-defunct Conti, helps to lower the cost and time of development allowing the #RaaS maintainers to maximize their speed of release to attract new affiliates." concludes Cocomazzi.

Prodaft researchers shared Indicators of Compromise for the Lockbit Green variant along with the Yara rule for its pattern detection.

Follow me on Twitter: **@securityaffairs** and **Facebook** and **Mastodon**

Pierluigi Paganini

(SecurityAffairs – hacking, LockBit green)
