New LockBit Green ransomware variant borrows code from Conti ransomware

securityaffairs.com/141666/cyber-crime/lockbit-green-ransomware-variant.html

February 1, 2023

February 1, 2023 By Pierluigi Paganini

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:

> Lockbit ransomware group has informed us they have acquired a 3rd ransomware variant.
>
> – Lockbit Red
> – Lockbit Black
> – Lockbit Green
>
> They also have modified their ESXI ransomware variant.
>
> Yes, they actually wrote "TLP:RED" in the image. pic.twitter.com/Oacbl2ZJk7
>
> — vx-underground (@vxunderground) January 27, 2023

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.

> ⚠️On January 27, 2023, the LockBit ransomware team made a so-called "LockBit Green" version of their ransomware available. The hashes and YARA rule can be found here: 👉https://t.co/0A9waHAwZj#lockbit #ransomware
>
> — PRODAFT (@PRODAFT) January 30, 2023

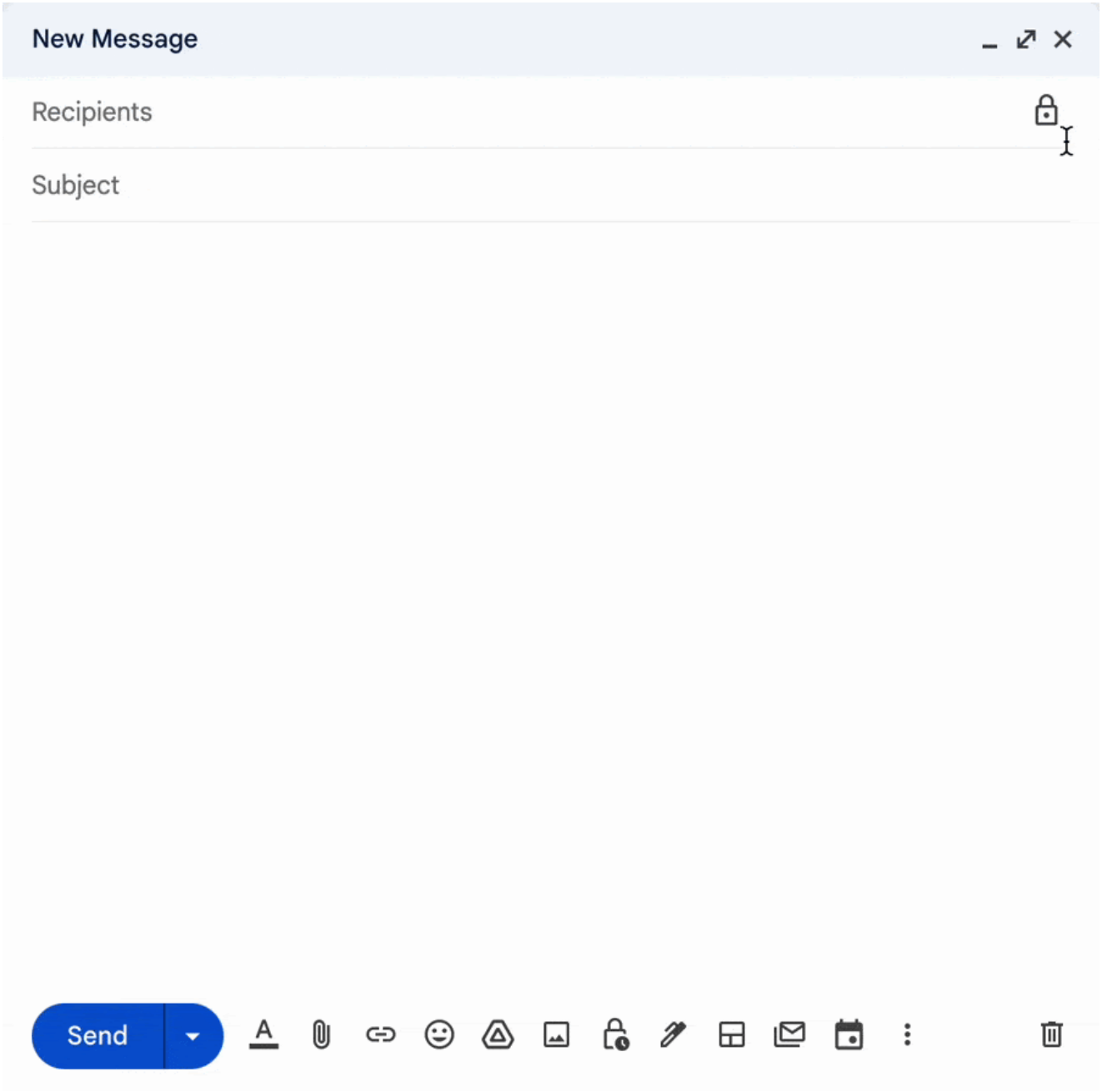
Pierluigi Paganini

(SecurityAffairs – hacking, LockBit green)

CybercrimeHackinghacking newsinformation security newsIT Information SecurityLockbit GreenLockBit RansomwaremalwarePierluigi PaganiniSecurity AffairsSecurity News

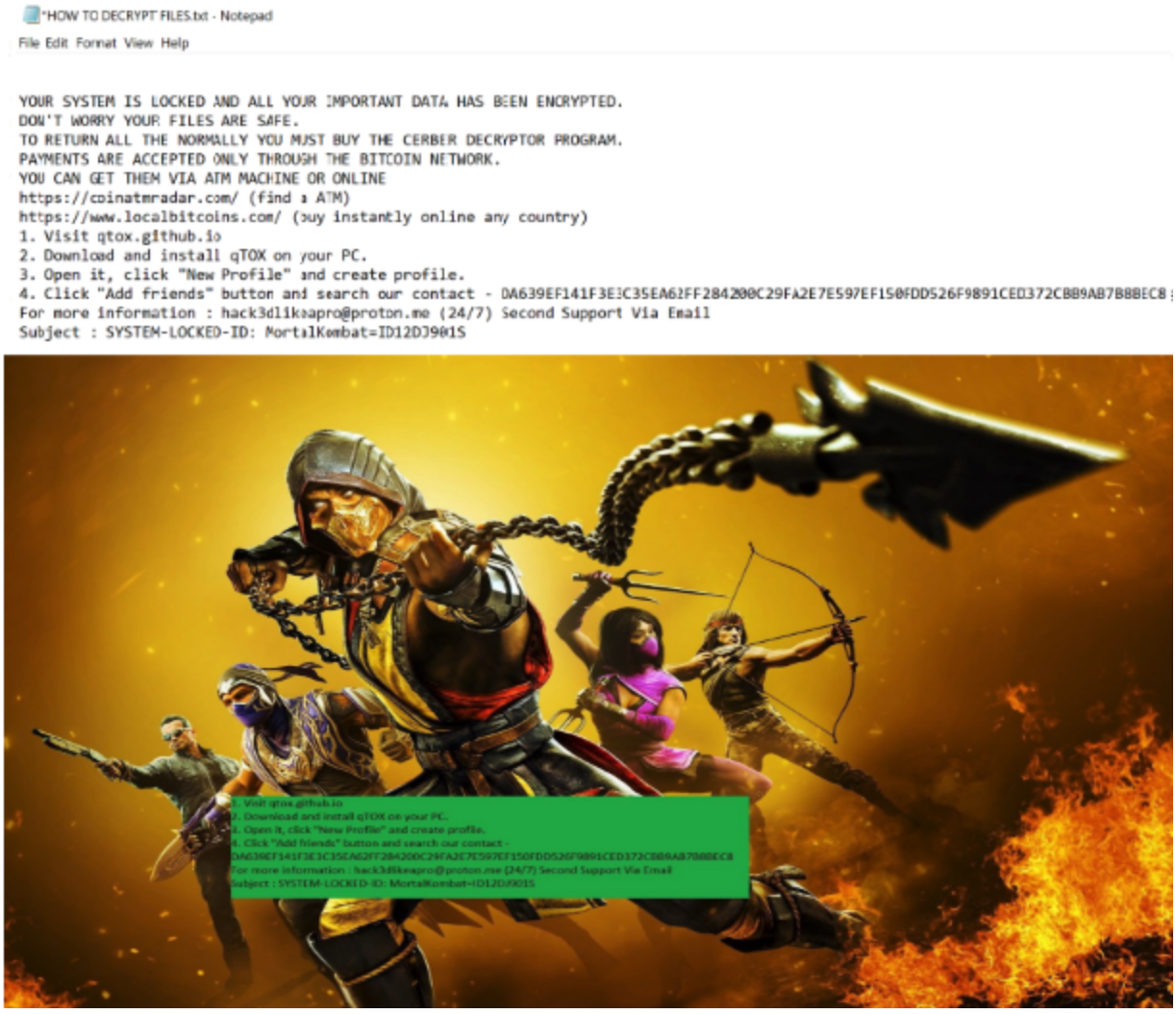
Share On

You might also like



Google Gmail client-side encryption is available globally

March 1, 2023 By Pierluigi Paganini



Bitdefender released a free decryptor for the MortalKombat Ransomware family

February 28, 2023 By Pierluigi Paganini

Back to top

- Home
- Cyber Crime
- Cyber warfare
- APT
- Data Breach
- Deep Web
- Digital ID
- Hacking
- Hacktivism
- Intelligence
- Internet of Things
- Laws and regulations

- Malware
- Mobile
- Reports
- Security
- Social Networks
- Terrorism
- ICS-SCADA
- EXTENDED COOKIE POLICY
- Contact me