Master decryption keys for Maze, Egregor, and Sekhmet ransomware leaked online

securityaffairs.co/wordpress/127826/malware/egregor-sekhmet-decryption-keys.html

February 9, 2022

February 9, 2022 By Pierluigi Paganini

The master decryption keys for the Maze, Egregor, and Sekhmet ransomware operations were released last night on the BleepingComputer forums.

The master decryption keys for the Maze, Egregor, and Sekhmet ransomware families were released on the BleepingComputer forums by the alleged malware developer.

The Maze group was considered one of the most prominent ransomware operations since it began operating in May 2019. The gang was the first to introduce a double-extortion model in the cybercrime landscape at the end of 2019. At the end of 2019, the Maze ransomware implemented data harvesting capabilities and started threatening the victims to release the stolen data for all those victims who refuse to pay the ransom.

In November 2020, the Maze ransomware operators announced that they have officially shut down their operations and denied the creation of a cartel.

Maze operation then rebranded in September as Egregor, but on February 2021 several members of the Egregor group were arrested in Ukraine.

The Sekhmet operation was launched in March 2020 and it has some similarities with the above ransomware operations.

While TTP's of Egregor operators are almost identical to that of ProLock, the analysis of Egregor ransomware sample obtained during an incident response conducted by Group-IB revealed that the executable code of Egregor is very similar to Sekhmet. The two strains share some core features, use similar obfuscation technique. Egregor source code bears similarities with Maze ransomware as well.

Now the decryption keys for these operations have now been leaked in the BleepingComputer forums. The keys were shared by a user named 'Topleak' who claims to be the developer for all three operations.

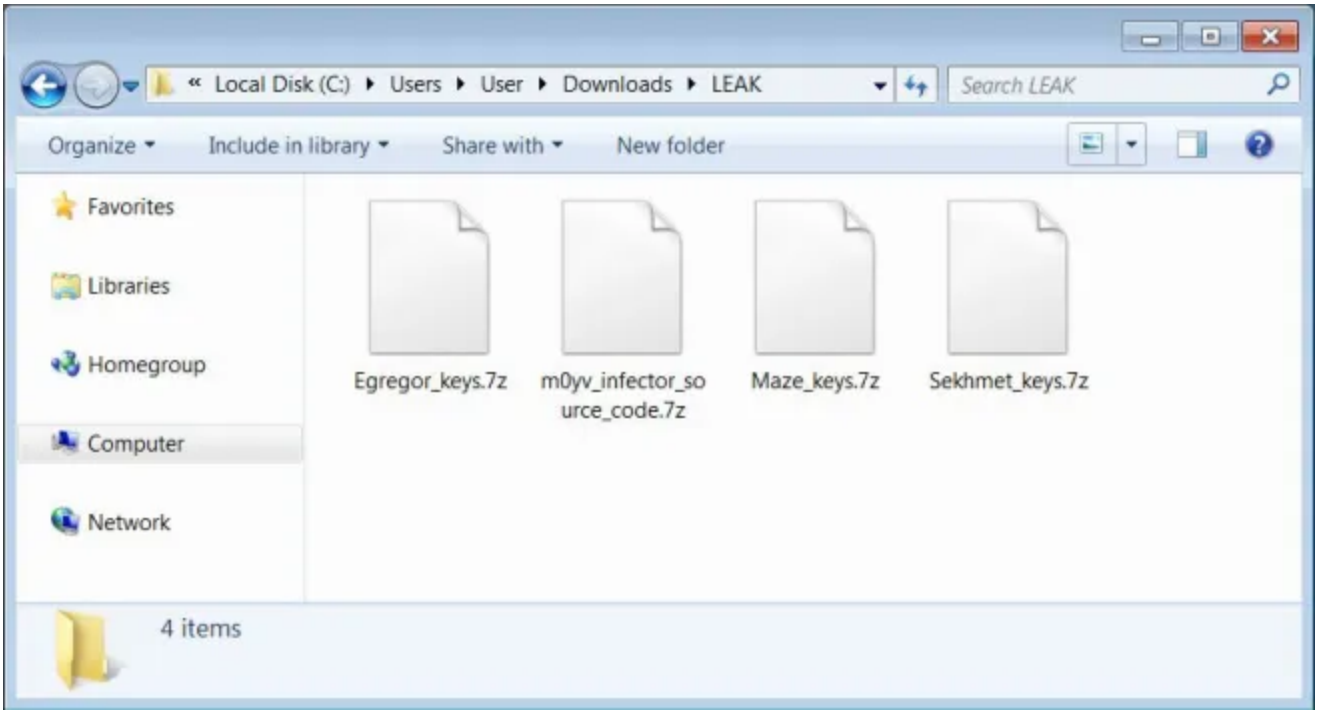
"Hello, It's developer. It was decided to release keys to the public for Egregor, Maze, Sekhmet ransomware families. also there is a little bit harmless source code of polymorphic x86/x64 modular EPO file infector m0yv detected in the wild as Win64/Expiro virus, but it is

not expiro actually, but AV engines detect it like this, so no single thing in common with gazavat." *the user wrote on the forum*.

"Each archive with keys have corresponding keys inside the numeric folders which equal to advert id in the config. In the "OLD" folder of maze leak is keys for it's old version with e-mail based. Consider to make decryptor first for this one, because there were too many regular PC users for this version. Enjoy!"

TopLeak user pointed out that it is a planned leak, and is not linked to recent arrests and takedowns conducted by law enforcement. The alleged ransomware developer added that none of the ransomware gang will ever return in ransomware operation and that the source code of tools ever made is wiped out.

In one of the archives leaked by the user there is the source code for a malware dubbed 'M0yv' that was part of the gang's arsenal.



Source Bleeping Computer

The popular malware researchers Michael Gillespie and Fabian Wosar confirmed to BleepingComputer that they are decryption keys are legitimate and allow to decrypt files encrypted by the three ransomware families for free.

Emsisoft has released a decryptor a free decryption tool for the Maze, Egregor, and Sekhmet ransomware.

Pierluigi Paganini

(SecurityAffairs – hacking, Maze ransomware)

You might also like

Experts believe that Russian Gamaredon APT could fuel a new round of DDoS attacks

May 28, 2022 By Pierluigi Paganini

There you can buy or download for free private and compromising data of your competitors. We public schemes, drawings, technologies, political and military secrets, accounting reports and clients databases. All this things were gathered from the largest worldwide companies, conglomerates and concerns with every activity. We gather data using vunlerability in their IT infrastructure. in their IT infrastructure.

Industrial spy team processes huge massives every day to devide you results. You can fid it in their portal:

http://[redacted]

(Tor browser required)

We can save your time gaining your own goals or goals of your company.With our information you could refuse partnership with unscrupulous partner, reveal dirty secrets of your competitors and enemies and earn millions dollars using insider information.

"He who owns the information, owns the world"

Nathan Mayer Rothschild

The strange link between Industrial Spy and the Cuba ransomware operation

May 28, 2022 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