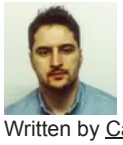
FBI: ProLock ransomware gains access to victim networks via Qakbot infections

zdnet.com/article/fbi-prolock-ransomware-gains-access-to-victim-networks-via-qakbot-infections/

Home Innovation Security

The FBI also warns that the ProLock decryptor doesn't always work correctly, even after victims pay the ransom.



Written by Catalin Cimpanu, Contributor on May 18, 2020

-
-
-
-
-

Image: FBI, ZDNet, Florian Krumm

See als

10 dangerous app vulnerabilities to watch out for (free PDF)

The FBI has issued a security alert earlier this month about a new ransomware strain named ProLock that has been deployed in intrusions at healthcare organizations, government entities, financial institutions, and retail organizations.

First spotted in March 2020, ProLock is part of the category of "human-operated ransomware."

These are ransomware strains that are installed manually on the networks of hacked companies. Hacker gangs breach or rent access to a hacked network, take manual control of the infected host, spread laterally through the network, and then deploy the ransomware after they've maximized their access.

In the case of ProLock, the FBI says this group gains access to hacked networks via the Qakbot (Qbot) trojan. Cyber-security firm Group-IB reported seeing the same thing last week.

This relationship between the operator of a malware dropper and a ransomware gang is not unique. It's been seen before with the Ryuk and Maze ransomware strains being installed on computers previously infected with TrickBot, and with DopplePaymer strains being dropped on computers infected with Dridex.

At the time of writing, it is unclear if the ProLock ransomware was created and managed by the Qakbot gang, or if the ProLock gang rents access to Qakbot-infected hosts part of a Crimeware-as-a-Service scheme.

Taking into account the FBI and Group-IB reports, this now also means that **computers inside an organization that have been found to be infected with Qakbot must be isolated from the rest of the network** as soon as possible, as they **can serve as entry points for a ransomware gang**.

ProLock decrypter not working properly

In addition to warning about the relationship between Qakbot and ProLock, the FBI also warned victims about bugs in the ProLock decrypter, the app the ProLock gang provides victims in order to decrypt their files after paying the ransom.

"The decryption key or 'decryptor' provided by the attackers upon paying the ransom has not routinely executed correctly," the FBI said.

"The decryptor can potentially corrupt files that are larger than 64MB and may result in file integrity loss of approximately 1 byte per 1KB over 100MB."

The FBI says that the decrypter may sometimes need to be modified to work correctly, incurring additional costs from lost business to organizations. This is reminiscent of the decryption bugs previously found in the Ryuk ransomware.

The ProLock ransomware was first spotted in March 2020. It initially went under the name of PwndLocker but rebranded into ProLock after Emsisoft found a way to decrypt files locked by the first version.

Sources told ZDNet that the FBI sent the flash alert to US organizations after ATM giant Diebold Nixdorf was infected with ProLock at the end of April.

A copy of the FBI flash security alert can be found here.

The FBI's most wanted cybercriminals