ProLock Ransomware teams up with QakBot trojan for network access

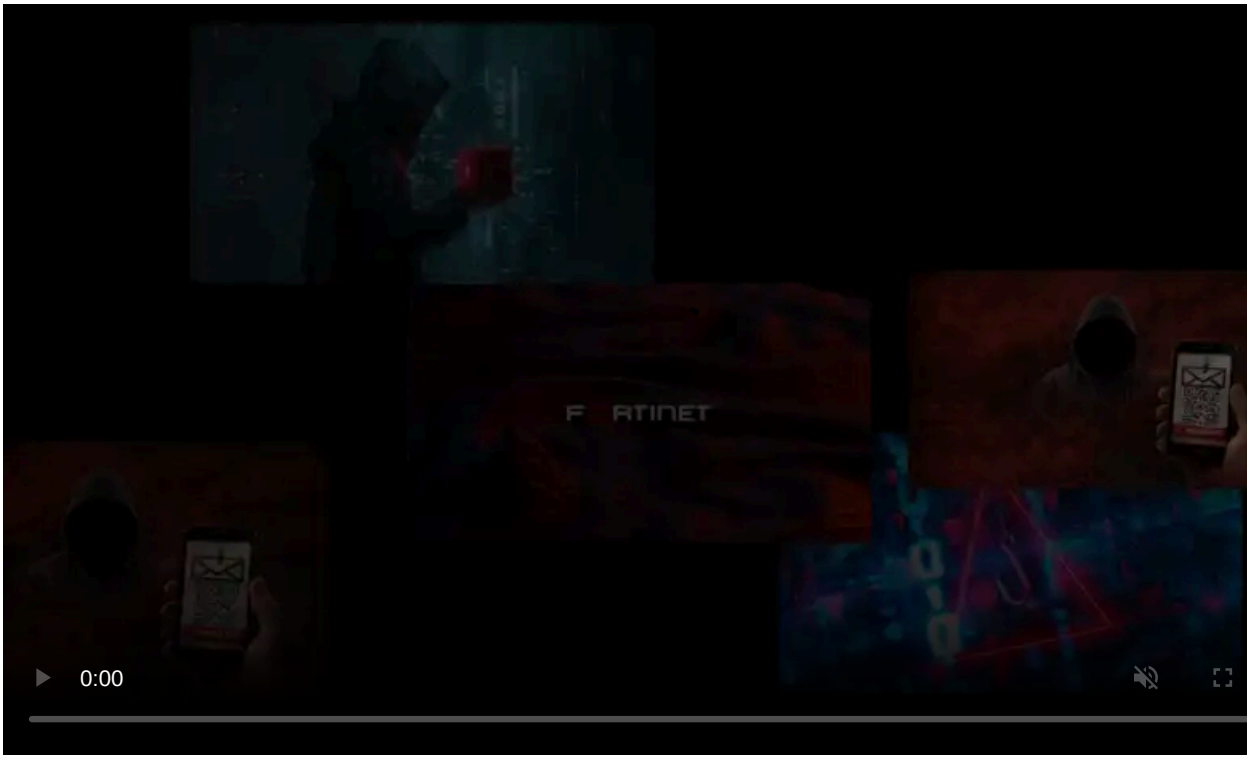
By Ionut Ilascu

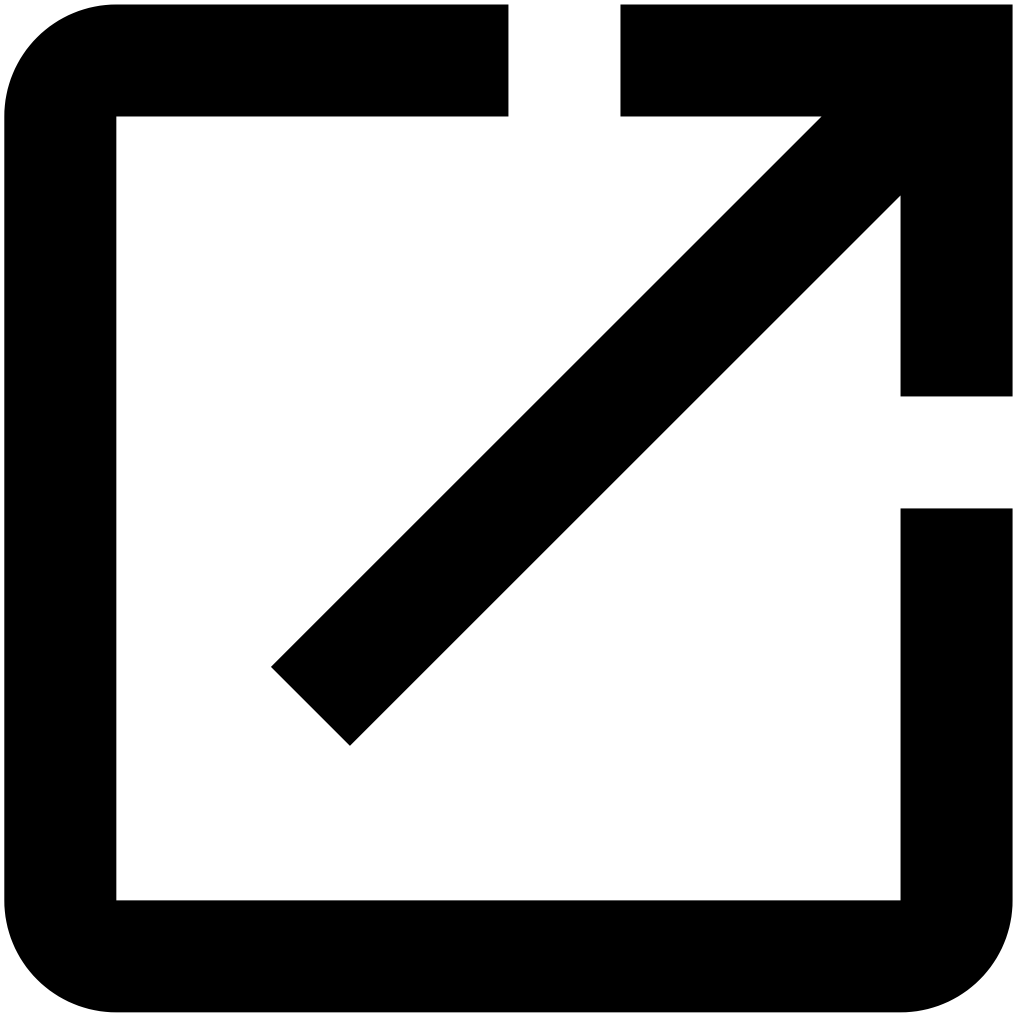
Published: 2020-05-14 · Archived: 2026-04-06 02:10:19 UTC

ProLock is a relatively new malware on the ransomware scene but has quickly attracted attention by targeting businesses and local governments and demanding huge ransoms for file decryption.

Its most recent victim is Diebold Nixdorf, mostly known for providing automated teller machines (ATMs).

This attack was caught before the encryption stage and did not impact these systems; it did cause some disruptions as it affected the corporate network.


F RTINET
0:00



Average prices

This ransomware family started as PwndLocker but it was rebranded to ProLocker in March after the developers fixed a bug that allowed free decryption of the files.

According to research conducted by BleepingComputer, ProLock demands ransoms ranging between $175,000 to over $660,000 depending on the size of the network.

However, the skills and techniques seen with ProLock operators are similar to those of high-profile ransomware groups such as Sodinokibi and Maze, BleepingComputer learned from Oleg Skulkin, Senior Digital Forensics Analyst at Group-IB. a Singapore-based cybersecurity company.

Victims breached via QakBot and RDP

The researcher says that these groups may intersect through third-party individuals providing operational support (distribution, initial breach, lateral movement).

Skulkin presented in a report today ProLock's tactics, techniques, and procedures (TTP), in the hope of better understanding and defending against this threat actor.

To breach victims, ProLock relies on two main vectors: distribution via QakBot (QBot) - previously affiliated with MegaCortex ransomware, and access via public-facing remote desktop (RDP) servers.

"Access via public-facing RDP-server is a very common technique used by many ransomware operators. Commonly this kind of access is bought from the third party, but may be obtained by some of group members as well" - Oleg Skulkin

Similar to how Ryuk works with TrickBot and DoppelPaymer/BitPaymer work with Dridex for access to networks, ProLock is working with QakBot to gain access.

QakBot is a banking trojan that spreads via phishing campaigns that deliver malicious Microsoft Word documents, usually to businesses. Emotet botnet was seen distributing this malware.

The researcher points out that both QakBot and ProLock rely on PowerShell to get the payload running. For the banking malware, malicious macros are employed for the task, while for the ransomware the code is extracted from a JPG or BMP image file.

image with ProLock binary

If ProLock operators use RDP access to reach their victim, persistence is established using valid accounts. With QakBot, multiple methods are used but popular ones rely on Run keys and scheduled tasks.

According to data from Group-IB, it takes about a week before QakBot makes room for ProLock. Skulkin told us that the trojan does not install the ransomware but downloads batch scripts from cloud storage repositories and executes them.

Lateral movement and file exfiltration

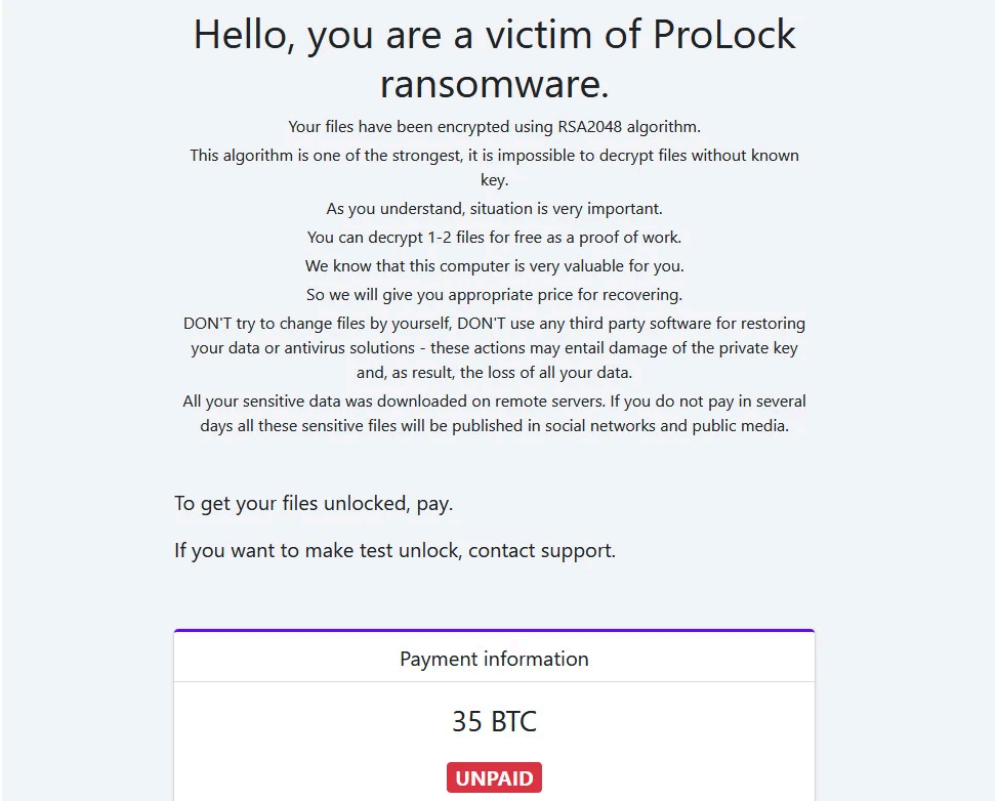
Lateral movement activity begins after the operators obtain credentials to some servers. Usually, RDP access for reconnaissance is enabled through the scripts, which are executed with PsExec.

The ransomware is later deployed using the command line interface for Windows Management Instrumentation (WMI).

Aligning to the current trend, ProLock operators steal data from a compromised network. The files are archived with 7-zip and uploaded to various cloud storage spaces (OneDrive, Google Drive, Mega) using Rclone, a command line program that syncs data with an impressive number of cloud storage services.

After exfiltration, the operators execute a PowerShell script to extract the ProLock binary embedded in an image file and unleash it across the enterprise network to encrypt data on reachable systems.

Each encrypted file has the ransomware mark (extensions .proLock, .pr0Lock, .proL0ck, .key, or .pwnd) and recovery instructions are provided in a text file dropped in every folder.



Skulkin says that ProLock does not have a “leak site” at the moment, although this may change in the near future.

Group-IB's report is available here and includes MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) knowledge.
