ProLock ransomware increases payment demand and victim count

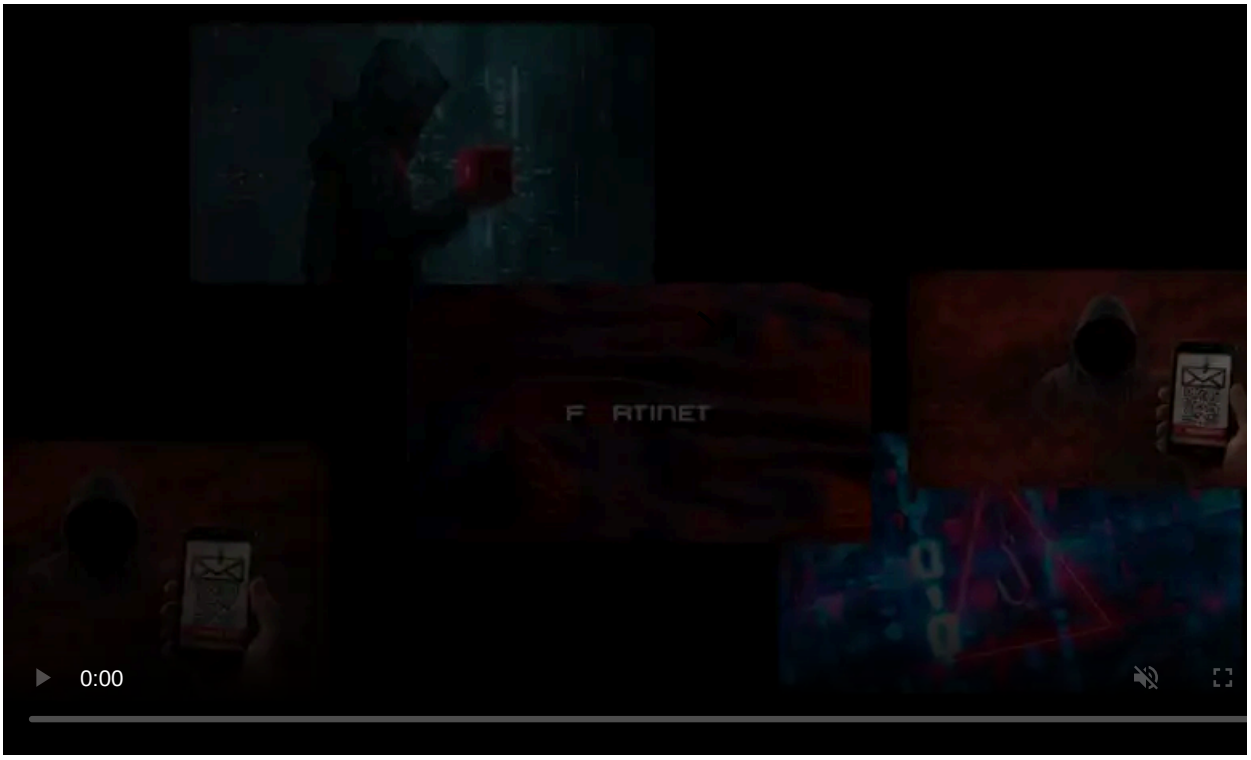
By Ionut Ilascu

Published: 2020-09-10 · Archived: 2026-04-05 21:22:15 UTC

Using standard tactics, the operators of ProLock ransomware were able to deploy a large number of attacks over the past six months, averaging close to one target every day.

Following a failed start in late 2019, under the name PwndLocker, due to a crypto bug that allowed unlocking the files for free, the operators rebooted the operation with fixing the flaw and renaming the malware to ProLock.

From the beginning, the threat actor aimed high, targeting enterprise networks and demanding ransoms between $175,000 to more than $660,000.

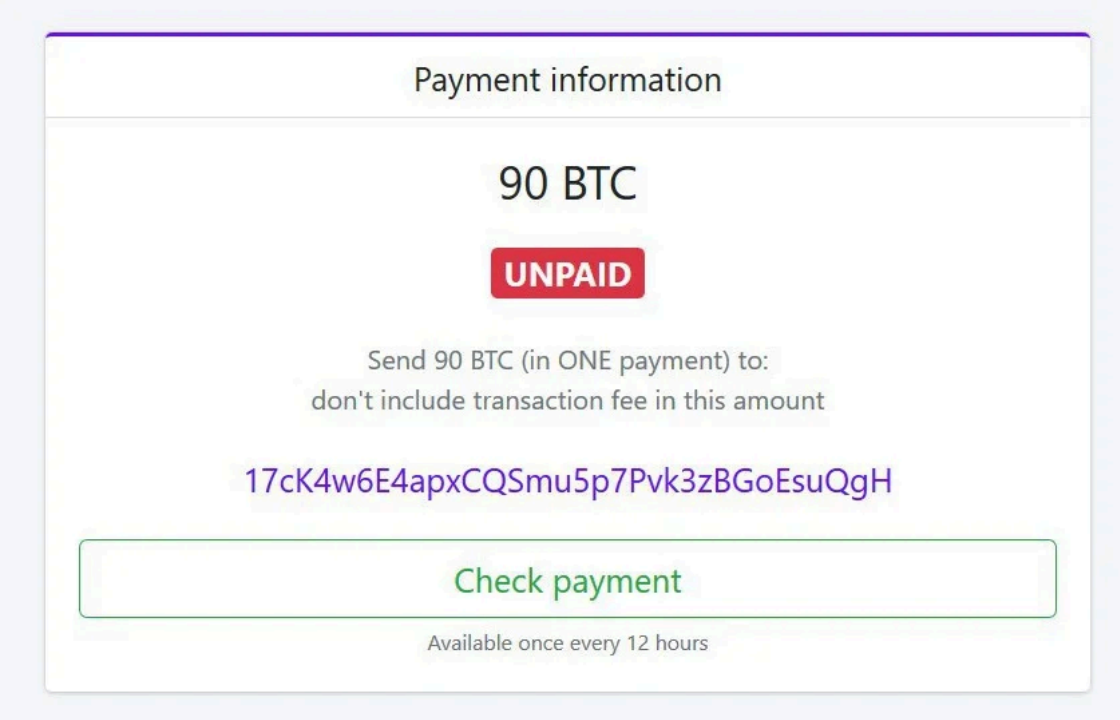

F RTINET
0:00

A fresh start in March under the ProLock label also meant increased activity and larger ransoms. Since then, the average figure swelled to $1.8 million, indicates incident response data from cybersecurity company Group-IB.

Simple, efficient tactics

The threat actor has no preference for its targets or the sector of their activity as long as they are companies with big networks, able to pay a higher ransom. So far, the focus seems to be on businesses in Europe and North America.

For the past half-year, Group-IB detected more than 150 ProLock operations, the most recent victim being asked 225 Bitcoins (more than $2,3 million at current value).



The group's tactics, techniques, and procedures are simple and effective, the partnership with QakBot (QBot) banking trojan allowing them to map the network, move laterally, ultimately deploy the ransomware.

Between the initial compromise and running the file-encryption routine, the actor spends about a month on the network, gathering information for better targeting and exfiltrating data (via Rclone).

Running ProLock on the target network is the last step of the attack, which typically starts with a spear-phishing email containing weaponized VBScripts and Office documents that deliver QakBot, oftentimes via replies in hijacked email threads.

Group-IB found that many times the VBScripts for downloading QakBot are very large, weighing even 40MB, to bypass security solutions that skip scanning large files.

Once on the target host, QakBot establishes persistence and makes sure that active defenses don't spot it by modifying Windows Registry to add its binaries on the list of Windows Defender exclusions.

"QakBot also collects a lot of information about the infected host, including the IP address, hostname, domain, and list of installed programs. Thanks to this information, the threat actor acquires a basic understanding of the network and can plan post-exploitation activities" - Group-IB

With tools like Bloodhound and ADFind, the threat actor profiles the environment to distribute the banking trojan to other hosts on the network. In some cases, this was done manually using PsExec, suggesting a strong connection between ProLock and QakBot operators.

Moving laterally also involved the use of remote desktop (RDP), and when this was not available on a machine, the actor ran the following batch script via PsExec to enable the remote connection:

```
reg add "HKLM\System\CurrentControlSet\Control\Terminal Server" /v "fDenyTSConnections" /t REG_DWORD /d 0 /f
netsh advfirewall firewall set rule group="Remote Desktop" new enable=yes
reg add "HKLM\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v "UserAuthentication" /t REG_DWORD /d 0 /f
```

ProLock's toolkit includes Mimikatz post-exploitation tool for penetration testers, which is deployed through Cobalt strike software for red team engagements.

Group-IB found that the ransomware actor sometimes relies on a vulnerability in Windows (CVE-2019-0859) that enables them to escalate privileges on compromised systems.

According to the report today, the file-encrypting malware lands on the host either via QakBot, downloaded with the Background Intelligent Transfer Service (BITS) from the attacker's server or by executing a script using Windows Management Instrumentation (WMIC) on a remote host.

Despite using standard tools, ProLock attacks remain largely undetected on the network, giving them time to prepare the file encryption stage and steal data.

Attacks from this threat actor have intensified lately, causing the FBI to release two FLASH Alerts about this actor this year [1, 2]. In the first one, the agency warns that the ProLock decryption tool may cause data loss because it does not work properly all the time.

Group-IB said that they could not verify this statement because they're none of their customers had to pay the ransom.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
