ProLock ransomware - everything you need to know

By Written by Catalin Cimpanu, ContributorContributor Sept. 10, 2020 at 1:00 a.m. PT

Archived: 2026-04-05 18:12:02 UTC

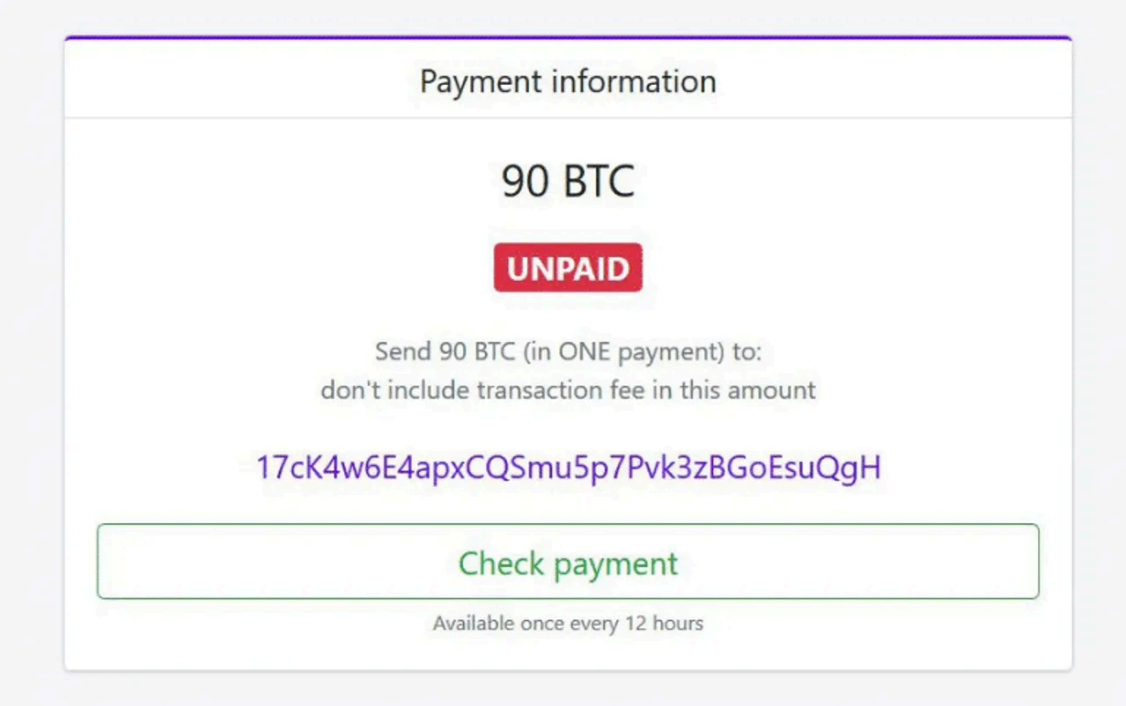

Image: Group-IB

Executive guide

Since the start of the year, a new ransomware gang named **ProLock** has made a name for itself by hacking into large companies and government networks, encrypting files, and demanding huge ransom payments.

ProLock is the latest ransomware gang that has adopted the "big-game hunting" approach to its operations. Big-game hunting refers to going after larger targets in order to extract big payments from victims who can afford it.

System administrators who manage these larger networks are most likely to see attacks from this particular group.

Below is a short summary of all ProLock activities that system administrators need to be aware of, based on reports published by Group-IB, Sophos, and two FBI alerts [1, 2].

ProLock's start

The ProLock gang began its activity (attacks) in late 2019. They initially operated under the name of PwndLocker but rolled out a major code upgrade and changed their name to ProLock in March 2020, after security researchers identified a bug in the original PwndLocker strain and released a free decrypter.

Distribution

In most of the incidents analyzed by security researchers, the ProLock ransomware was deployed on networks that have been previously infected with the Qakbot trojan.

The Qakbot trojan is distributed via email spam campaigns or is dropped as a second-stage payload on computers previously infected with the Emotet trojan. System administrators who find computers infected with either of these two malware strains should isolate systems and audit their networks, as the ProLock gang could be already wandering around their systems.

Lateral movement

But since the ProLock gang usually buys access to one Qakbot-infected computer and not entire networks, they also have to expand their access from this initial entry point to other nearby computers, for maximum damage.

This operation is called "lateral movement," and there are various ways the ProLock gang does this.

Group-IB says ProLock uses the CVE-2019-0859 Windows vulnerability to gain administrator-level access on infected hosts and then deploys the MimiKats tool to dump credentials from the infected system.

Depending on what they find, the ProLock gang can use these credentials to move laterally across a network via RDP, SMB, or via the local domain controller.

WMIC is used at the last moment to push the actual ransomware to all compromised hosts, where it encrypts files, and according to Sophos, plays the OS alert tone at the end to signal the end of the encryption routine.

Impact

All the operations needed to move laterally across a network are executed by a human operator in front of a terminal — and are not automated.

As a result, ProLock incidents usually manage to infect a large number of computers, as the ProLock human operator bides their time in order to maximize damage.

Group-IB says this tactic allows the group to demand very high decryption fees from victims, most of which face prolonged downtimes, in case they decide to rebuild internal networks.

"The fact that their average ransom demands range anywhere from 35 to 90 Bitcoin (approx. $400,000 to $1,000,000) only confirms their 'think big' strategy," Group-IB said in a private report shared with ZDNet today.

These sums are below the average ($1.8 million) of some other big-game hunting ransomware gangs, but ProLock extortions have been gradually increasing in recent months. For example, Group-IB told ZDNet that the recent ProLock case they traced involved a ransom of 225 Bitcoin, which is around $2.3 million.

Some of the group's past victims include big names like ATM maker Diebold Nixdorf, the city of Novi Sad in Serbia, and Lasalle County in Illinois.

Paying the ransom

But despite the damage this ransomware group can do, in one of its two alerts, the FBI warned organizations against paying the ransom, as the ProLock decrypter that victims receive doesn't always work as intended, and usually fails when decrypting larger files.

Victim shaming

Furthermore, ProLock has also been seen in some incidents leaking data from the networks of victims they infected, and which refused to pay.

While some other ransomware groups have created special sites where they leak this data, ProLock prefers to dump it on hacking forums or pass it to journalists via email.

All in all, ProLock appears to be the first ransomware gang that uses Qakbot as an initial entry point, but most of its other tactics are shared with most other big-game hunting and human-operated ransomware gangs — so, defending networks against ProLock should be straightforward for companies that have already taken precautions against the other ransomware groups.

Cybersecurity reads for every hacker's bookshelf

Security
