Warning campaign of large-scale ransomware attack, misuse of 7zip to encrypt QNAP devices

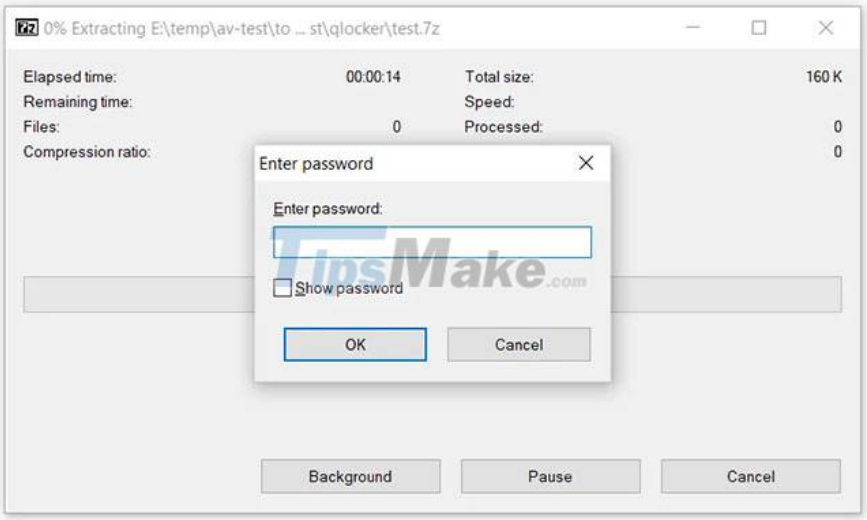
International cybersecurity researchers have warned of a massive ransomware attack against QNAP devices around the world.

It is worth mentioning that this offensive campaign is still actively deployed, and especially many victims discovered that their encrypted files were stored in password protected 7zip archives. .

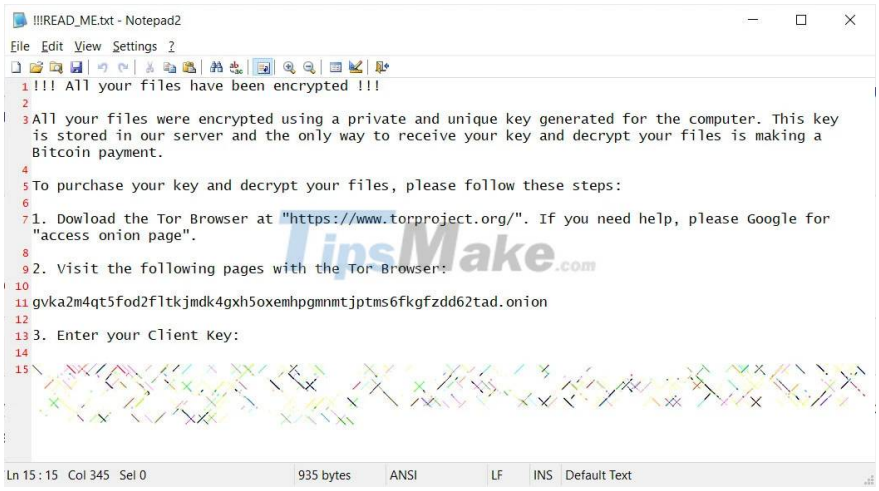
The ransomware used in this attack campaign is Qlocker - a name no stranger to the global security community. According to preliminary investigation results, malicious intentional activities began targeting QNAP devices globally on April 19, 2021. Since that time, there have been numerous reports, Urgent message from QNAP users regarding their file system being encrypted for a ransom.

In the majority of reports, most victims reported that the attackers misused 7-zip to move the file system on the QNAP device into password-protected archives. While the files are locked, the QNAP Resource Monitor will display the '7z' processes as the 7zip command line execution.

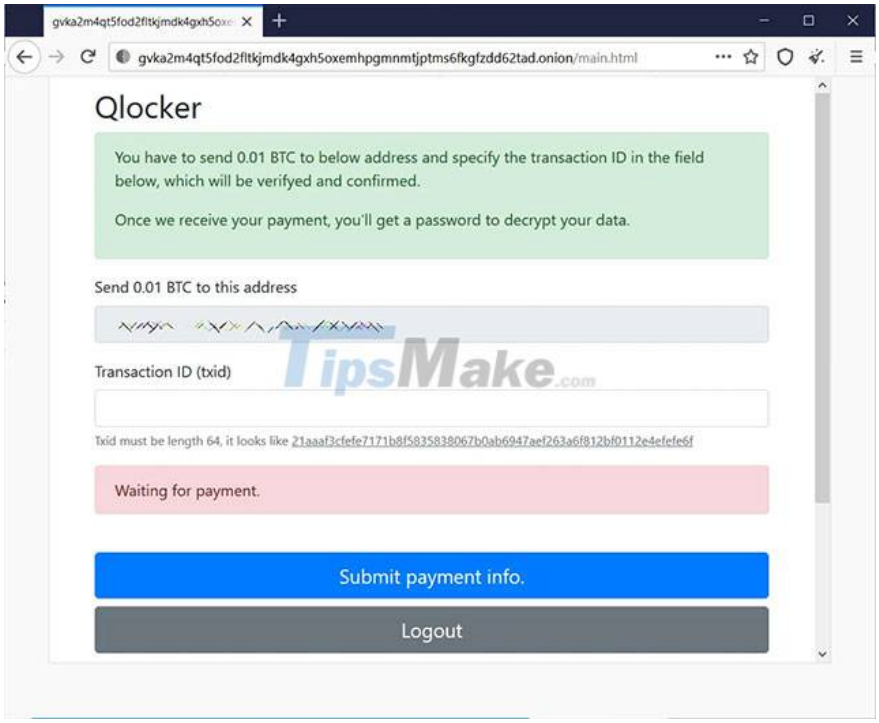
Once the ransomware completes the encryption process, the files of the QNAP device will be stored in password-protected 7-zip archives (zipped files), ending with the extension .7z. In order to unzip these archives, the victim will need to enter a password known only to the attacker.



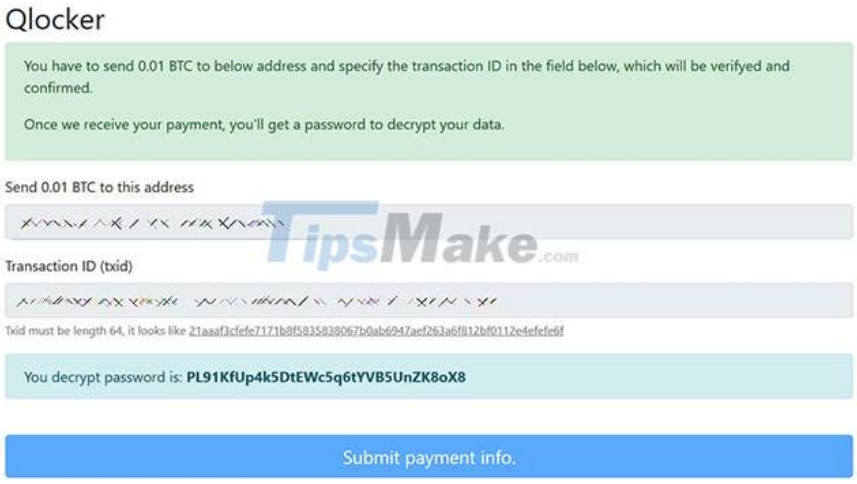
After the QNAP device is encrypted, the victim will receive a ransom warning titled !!! READ_ME.txt. This includes a unique client key that the victim needs to enter to log into the ransomware's Tor payments page.



As can be seen in the content of the announcement, all victims were asked to pay 0.01 Bitcoin, or about $ 557.74, in exchange for a password for their encrypted 7zip archives.



After paying the ransom and entering a valid Bitcoin transaction ID, the Tor payment page will display the password for the victim's 7Zip archive, as shown below.



This password is unique to each victim, and cannot be used on other victim devices.

Where is the hole?

The QNAP side believes that the attackers are exploiting a series of different vulnerabilities to deploy this malicious campaign.

Previously, (April 16) QNAP claimed to have addressed a series of critical security vulnerabilities that could allow a remote agent to have full access to the device and execute ransomware, including :

1. CVE-2020-2509: Command Injection vulnerability in QTS and QuTS hero

2. CVE-2020-36195: SQL Injection vulnerability in Multimedia Console and Media Streaming Add-On

However, QNAP experts claim that this Qlocker campaign exploited the CVE-2020-36195 vulnerability to execute ransomware on vulnerable devices, in other words, devices that have not been updated. latest patch.

Therefore, QNAP device users should immediately update their QTS, Multimedia Console and Media Streaming Add-on to the latest version.

> "QNAP specifically urges all users to immediately install the latest version of Malware Remover and scan for malware on the QNAP NAS. Multimedia Console, Media Streaming Add-on and Hybrid Backup Sync applications also need to be updated. update to the latest available version to further secure QNAP NAS systems from ongoing ransomware attacks. .

At the same time, the QNAP side also warned that victims should not restart the device, but instead run the malware scanner.

> "If your data has been encrypted or is being encrypted, you should not turn off or restart the NAS device. Instead, scan for malware with the latest Malware Remover immediately, later. Then contact QNAP Technical Support (QNAP Technical Support) at: service.qnap.com '.