Qlocker ransomware shuts down after extorting hundreds of QNAP users

bleepingcomputer.com/news/security/qlocker-ransomware-shuts-down-after-extorting-hundreds-of-qnap-users/

Lawrence Abrams

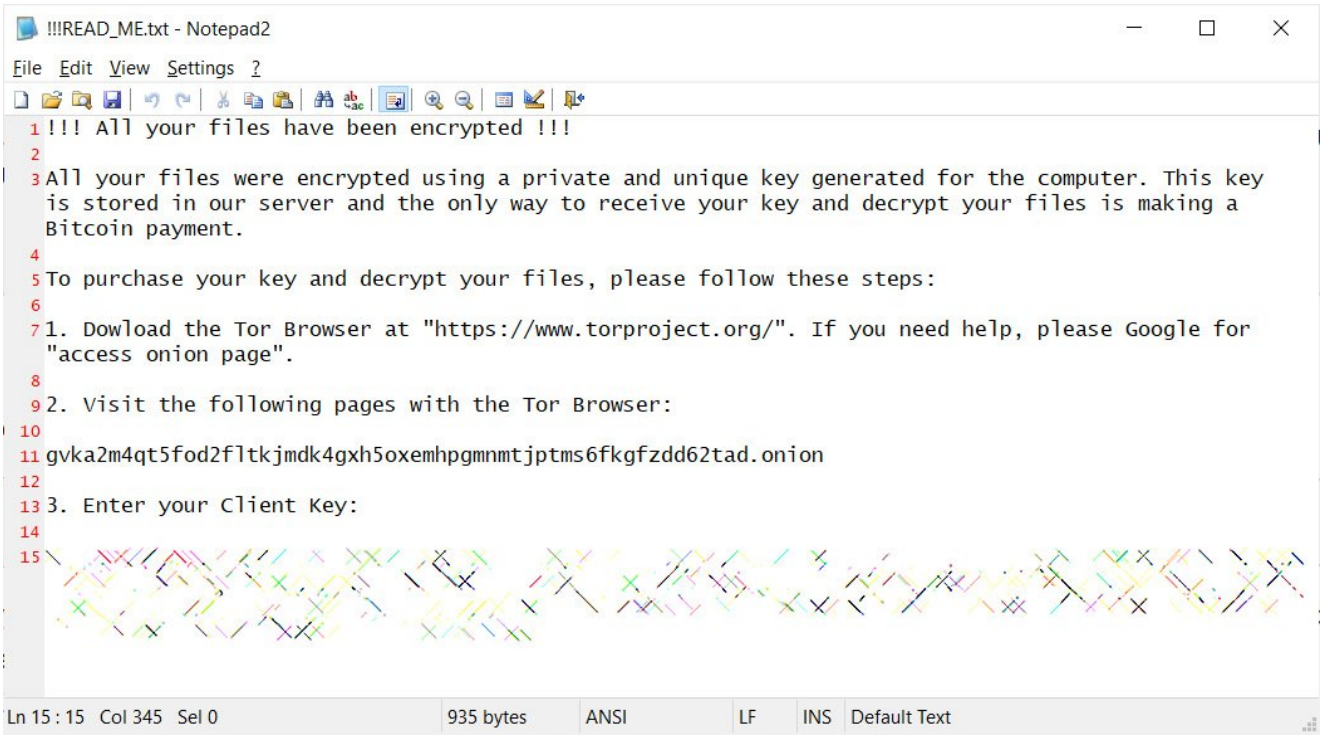
By
Lawrence Abrams

- May 19, 2021
- 01:59 PM
- 1

The Qlocker ransomware gang has shut down their operation after earning $350,000 in a month by exploiting vulnerabilities in QNAP NAS devices.

Starting on April 19th, QNAP NAS device owners worldwide suddenly discovered that their device's files were replaced by password-protected 7-zip archives.

In addition to the encrypted files, QNAP owners found a !!!READ_ME.txt ransom note explaining that their files were encrypted and needed to visit a Tor site to pay a ransom to get their files back.



Qlocker ransom note

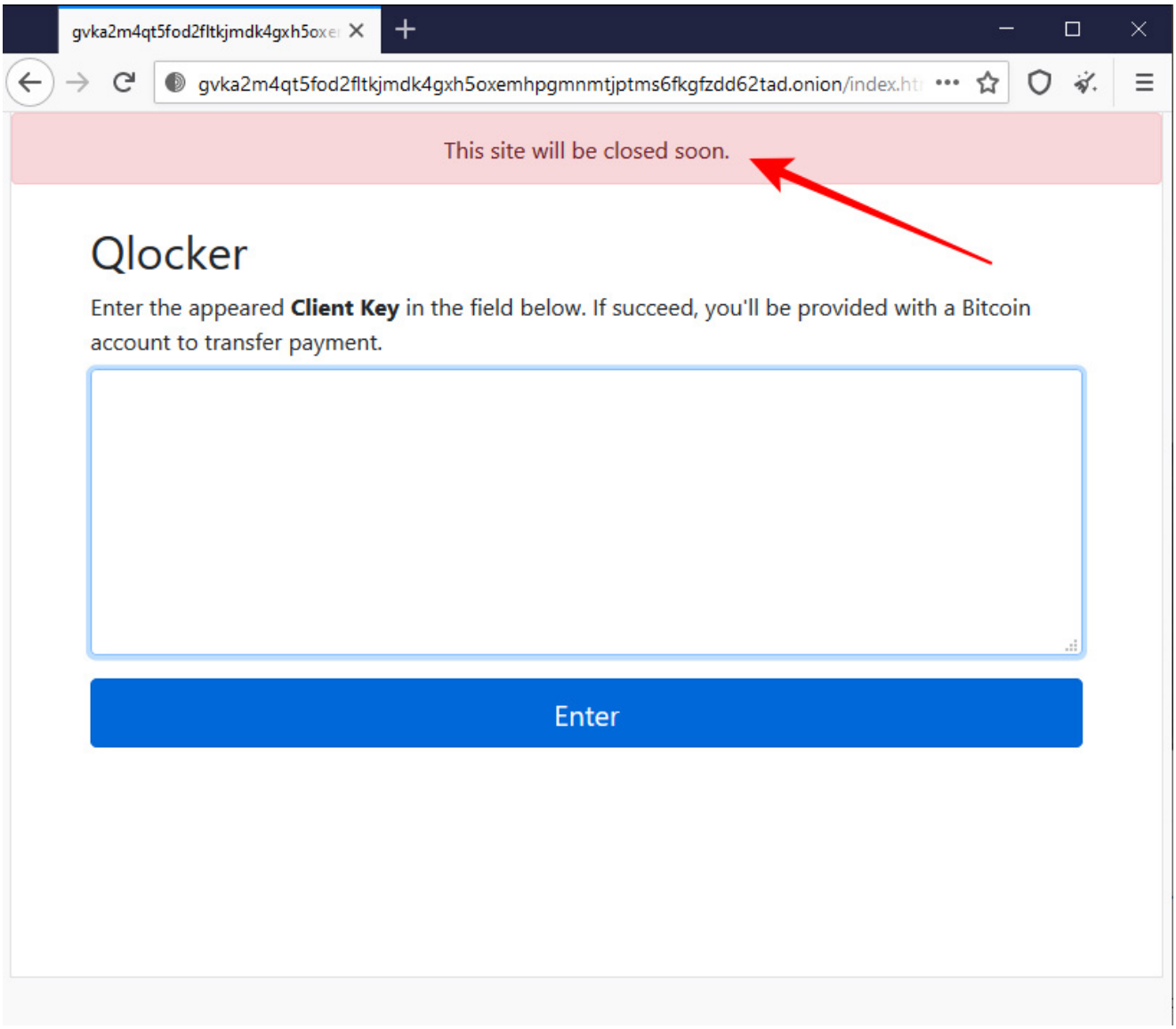
The Tor site identified the attackers as Qlocker and demanded .01 bitcoins, or approximately $550, to receive the password for their files.

Later, it was determined that threat actors conducted the attacks through recently disclosed QNAP vulnerabilities that allowed threat actors to encrypt victims' files using the built-in 7-zip application remotely.

Using such a simple approach allowed them to encrypt over a thousand, if not thousands, of devices in just a month.

Qlocker operation shuts down

As a possible sign of their impending shutdown, the Qlocker Tor sites began displaying a message stating that "This site will be closed soon."



Qlocker Tor site indicating it will shut down soon

More recently, the Qlocker gang began a bait-and-switch tactic when it came to ransom payments.

Victims reported that after paying the demanded .01 bitcoins and submitting the transaction ID on the Qlocker Tor site, the site would state that they needed to pay an additional .02 bitcoins to get their files back.

"Bitcoin is getting harder to find, time waits for nothing. The new price is 0.03," the Qlocker Tor site would display during their bait-and-switch.

Eventually, the above site shut down, but another Qlocker Tor site appeared a day or so later.

Today, in BleepingComputer tests and victim's reports in our Qlocker support topic, all of the Qlocker Tor sites are no longer accessible, and victims no longer have a way to pay the ransom.

Since the DarkSide ransomware attack on Colonial Pipeline and the subsequent intensifying of pressure by US law enforcement, the DarkSide ransomware shut down, and REvil has begun to restrict their targets.

Since then, other ransomware operations' Tor sites have gone offline, including those for Ako/Ranzy and Everest.

It is not clear if the shutdown of the Qlocker sites is related to fear of increased law enforcement activity.

Following the money

Instead of demanding millions of dollars to recover files, the threat actors priced their ransom demands at only $500, which led to many businesses paying the ransom to recover their files.

As the Qlocker ransomware operation used a fixed set of Bitcoin addresses that victims were rotated through, it has been possible to track how many bitcoins they received in ransom payments.

Out of the twenty-two Qlocker Bitcoin addresses known by BleepingComputer, victims paid a total of 8.93258497 bitcoins in ransomware. Today that is worth $353,708, but before this week's Bitcoin crash, those same bitcoins would be worth almost $450,000.

Bitcoin Address	Total Bitcoin payments
34vbPQLgGZwKG2FikitGU6QR7K25aB6Shh	0.73258748
37m57HiP5rPceopgEWF9sM58CkzaDFYtaU	0.29021317
3Ekwztte7oWR1odC1eKeL2Va4cpBuGXPgU	0.28990667
3EPBKN3bcax81U3MdKYUhMC1fzFEFGPC6E	0.27850668
3EvCKQ38y8ePUwM4w49XWVtAK7KhYbmeMH	0.45781656
3FvLioiqF2TrQgZ9zRMdd7QUfc2hTjKZfL	0.19945862
3FXVLv8TmcHNmnfwLfc5g7f2a32xp3XugW	0.59099550
3G6fbWX6At9uRzKf6kwS6R6pn5EQ8UsxKY	0.32033215
3GfAJxhUen3oqb4sDDnPmXyhs5mDboHbyG	0.57134513
3JRdPjB8U3nfDqQHzTqw9yYra49Gsd8Rar	0.57093368
3KmK5z4CAvn3aL4Q8F2gWbhuPRy9ZmEurN	0.48956001

3Kywg92E877KUWmyaeeLNSXFc5bqBvFbAm	0.62479830
3LLzycFNFh7mDsqRhfknfGBa6TKq6HcfwS	0.42901320
3Lp1NkJHYsmFRBfM3ggoWsS1PF5hXxrwrD	0.50386846
3PDfzkTnD1E7gB7peZ2prRyDxjQ1BhqcV1	0.32164647
3PunvFGpVWLX7PNAoT3bMDbPQU2QQW4kxN	0.26000332
3Q8WmjQyFs1EKCdu415t2P9cxY7AbqorPd	0.58281373
3EWRngsRDhCxMHtKxeK6k9kX3pyWZSA2YB	0.29090963
3Gwz3yVmrGr5AqmUrAS8H2QQaPz2v9Rhpx	0.27875489
3JtUAz4aKUrjcBK47ocdv52tTJkriat1nx	0.25999912
3NtgDQCu7xck4UEpyTf8HNSSvrMCnKZRjt	0.28975298
3DhE1iZ5Ui6HALVKuuYXW52ArZPVJjUgJA	0.29936922

If we divide the number of Bitcoins earned by the ransom payment of .01 bitcoins, we come out to approximately 893 victims who have paid the ransom.

This amount of ransoms and victims might be larger if Qlocker used other bitcoin addresses.

Related Articles:

QNAP alerts NAS customers of new DeadBolt ransomware attacks

QNAP warns of ransomware targeting Internet-exposed NAS devices

Ransom payment is roughly 15% of the total cost of ransomware attacks

BlackCat/ALPHV ransomware asks $5 million to unlock Austrian state

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.