A ransomware gang made $260,000 in 5 days using the 7zip utility

bleepingcomputer.com/news/security/a-ransomware-gang-made-260-000-in-5-days-using-the-7zip-utility/

Lawrence Abrams

By
Lawrence Abrams

- April 24, 2021
- 12:06 PM
- 9

A ransomware gang has made $260,000 in just five days simply by remotely encrypting files on QNAP devices using the 7zip archive program.

Starting on Monday, QNAP NAS users from all over the world suddenly found their files encrypted after a ransomware operation called Qlocker exploited vulnerabilities on their devices.

While most ransomware groups put considerable development time in their malware to make it efficient, feature-rich, and have strong encryption, the Qlocker gang didn't even have to create their own malware program.

Instead, they scanned for QNAP devices connected to the Internet and exploited them using the recently disclosed vulnerabilities. These exploits allowed the threat actors to remotely execute the 7zip archival utility to password protect all the files on victims' NAS

storage devices.

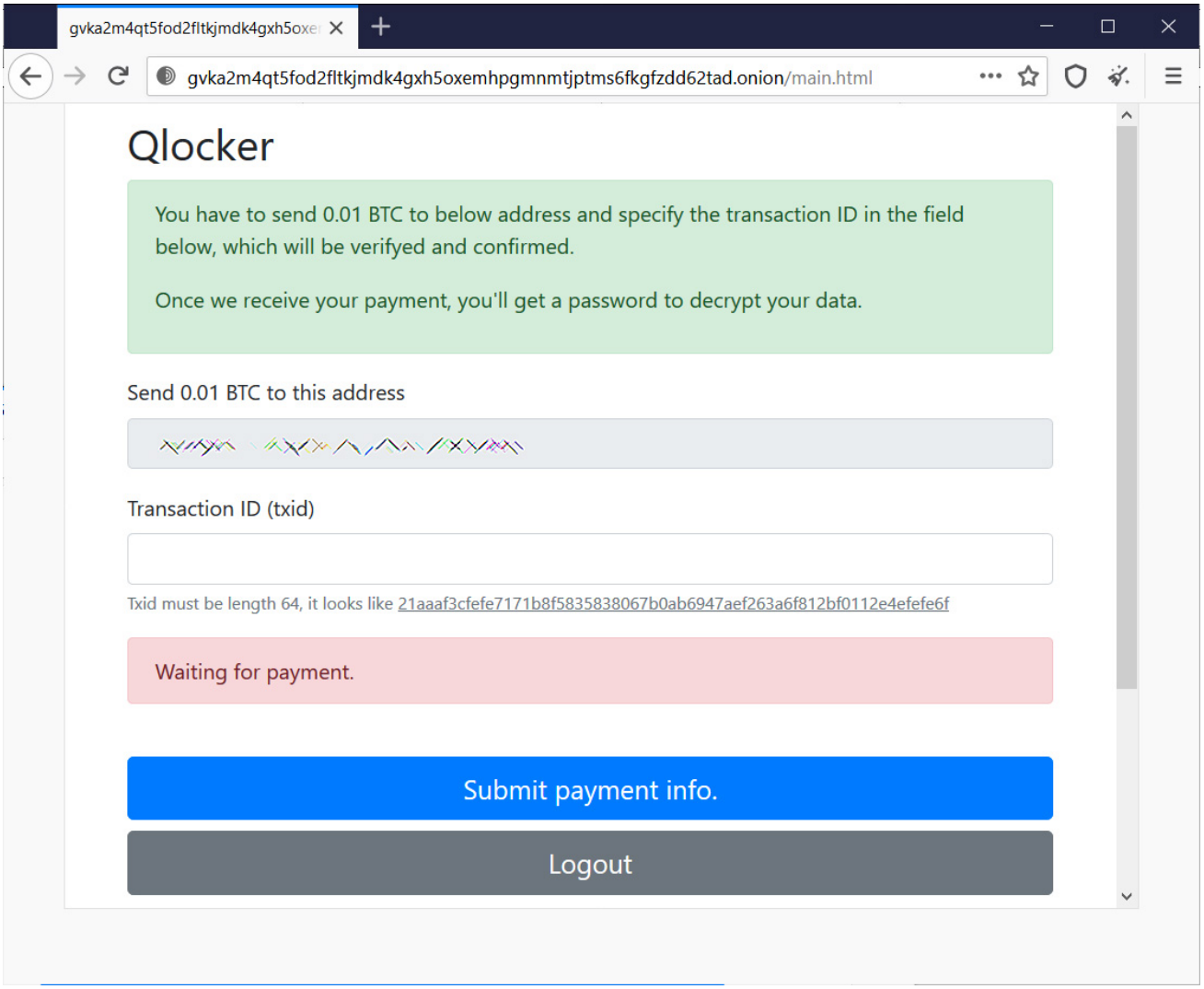
Using such a simple approach allowed them to encrypt over a thousand, if not thousands, of devices in just five days using a time-tested encryption algorithm built into the 7zip archive utility.

Ransom demands were priced correctly

Enterprise-targeting ransomware usually demands ransom payments ranging from $100,000 to $50 million to decrypt all of a victim's devices and not leak their stolen data.

However, Qlocker chose a different target - consumers and small-to-medium business owners utilizing QNAP NAS devices for network storage.

It seems that the threat actors knew their targets well as they priced their ransom demands at only 0.01 Bitcoins, or at today's Bitcoin prices, approximately $500.



Qlocker ransom demand

Deciding to pay millions of dollars requires a company to think hard about whether the lost data is worth millions of dollars.

However, paying $500 can be seen as a small price to pay to recover important files, no matter how violated a victim may feel.

Qlocker's decision appears to have paid off as the payments have started to rush in earning the threat actors a sizeable return for a few days of activity.

Qlocker made almost $260,000 so far

As the Qlocker ransomware uses a fixed set of Bitcoin addresses that victims are rotated through, it has been possible for BleepingComputer to collect the addresses and monitor their payments.

Tuesday night, security researcher Jack Cable discovered a short-lived bug that allowed him to recover the passwords for 55 victims passwords for free. While utilizing this bug, he collected ten different Bitcoin addresses that the threat actors were rotating with victims and shared them with BleepingComputer.

Since then, BleepingComputer has collected an additional 10 addresses, for a total of 20 bitcoin addresses used by the Qlocker threat actors.

At this time, the 20 bitcoin addresses, shown below, have received ransom payments totaling 5.25735623 Bitcoins. This amount is equivalent to approximately $258,494.

Bitcoin Address	Total Bitcoin payments
34vbPQLgGZwKG2FikitGU6QR7K25aB6Shh	0.55216220
37m57HiP5rPceopgEWF9sM58CkzaDFYtaU	0.14021317
3Ekwztte7oWR1odC1eKeL2Va4cpBuGXPgU	0.09962125
3EPBKN3bcax81U3MdKYUhMC1fzFEFGPC6E	0.10915462
3EvCKQ38y8ePUwM4w49XWVtAK7KhYbmeMH	0.34801656
3FvLioiqF2TrQgZ9zRMdd7QUfc2hTjKZfL	0.08951304
3FXVLv8TmcHNmnfwLfc5g7f2a32xp3XugW	0.38088464
3G6fbWX6At9uRzKf6kwS6R6pn5EQ8UsxKY	0.16983215
3GfAJxhUen3oqb4sDDnPmXyhs5mDboHbyG	0.46134513
3JRdPjB8U3nfDqQHzTqw9yYra49Gsd8Rar	0.40133268

3KmK5z4CAvn3aL4Q8F2gWbhuPRy9ZmEurN	0.29910901
3Kywg92E877KUWmyaeeLNSXFc5bqBvFbAm	0.48277236
3LLzycFNFh7mDsqRhfknfGBa6TKq6HcfwS	0.31901320
3Lp1NkJHYsmFRBfM3ggoWsS1PF5hXxrwrD	0.32386846
3PDfzkTnD1E7gB7peZ2prRyDxjQ1BhqcV1	0.14020000
3PunvFGpVWLX7PNAoT3bMDbPQU2QQW4kxN	0.15954000
3Q8WmjQyFs1EKCdu415t2P9cxY7AbqorPd	0.40031185
3EWRngsRDhCxMHtKxeK6k9kX3pyWZSA2YB	0.13081244
3Gwz3yVmrGr5AqmUrAS8H2QQaPz2v9Rhpx	0.15965435
3JtUAz4aKUrjcBK47ocdv52tTJkriat1nx	0.08999912

If we divide the amount of Bitcoins earned, we come out to approximately 525 victims having paid the ransom so far.

Unfortunately, the ransoms keep coming in as users make the hard decision of paying to recover their files, so this number will likely increase through the weekend and into next week.

This ransomware campaign is still ongoing, with new victims appearing every day. Therefore, all QNAP users must update the latest versions of the Multimedia Console, Media Streaming Add-on, and Hybrid Backup Sync apps to fix the vulnerabilities and protect against these ransomware attacks.

Users are also advised to secure their NAS devices so that other future attacks are harder to accomplish.

For more information, you can read our dedicated Qlocker article or visit our highly active Qlocker support topic, where users are helping each other recover files and secure their devices.

Related Articles:

QNAP alerts NAS customers of new DeadBolt ransomware attacks

QNAP warns of ransomware targeting Internet-exposed NAS devices

Magniber ransomware gang now exploits Internet Explorer flaws in attacks

QNAP urges customers to disable UPnP port forwarding on routers

QNAP warns severe OpenSSL bug affects most of its NAS devices

- 7zip
- Exploit
- NAS
- QLocker
- QNAP
- Ransomware

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.

- Previous Article
- Next Article

Comments

- 
  TsVk! - 1 year ago
  -
  -
  more than 7 bitcoin in payments now...
- 
  danynap - 1 year ago
  -
  -
  I am wishing to pay. This is the 2nd try, initially I've filled in the form with a wrong txid (just to try). They f*#ing system has stored this and now it does not accept other data in the fiels. The page shows "waiting for confirmations" eternally... Data lost forever! no chance neither to pay :-(

- 

danynap - 1 year ago

  -
  -

Solved. The website resumed working. Paid. Got the password. Works. Now, hard work to recover 4tb of files. I hope those criminals need all the money stolen this way to purchase medicines !

- 

Renzo85rm - 1 year ago

  -
  -

They are clearing the accounts in favor of this address:
3QP1rnycGirbRqDs6t6jCs8QBDED9zF4VZ
then turn to the following address:
1EFdmL5ZYYUQ32a63ENZtiU7F7VuDAJJKr
today only they moved the first 3BTC and the TOR site are 3 days with the wording at the top:
"This site will be closed soon."
they are closing "the shop", guys!

- 
  danynap - 1 year ago
    -
    -

  "They are clearing the accounts in favor of this address:
  3QP1rnycGirbRqDs6t6jCs8QBDED9zF4VZ
  then turn to the following address:
  1EFdmL5ZYYUQ32a63ENZtiU7F7VuDAJJKr
  today only they moved the first 3BTC and the TOR site are 3 days with the wording at the top:
  "This site will be closed soon."
  they are closing "the shop", guys! "

  Update (May 5th): the "website" is down. Shop closed.

- 
  Renzo85rm - 1 year ago
    -
    -

  no it's still open, a few minutes ago another victim paid the account I monitor, 1 in 20 listed above, to which my particular id was referring, the one where I paid too ...

- 
  danynap - 1 year ago
  -
  -
  it's strange. it was unreachable.. maybe a temporary down so,... or a joke just to panic more.
  or... BE CAREFUL the "campaign" may be alive, also for those already affected and recovered.. better to turn off the nas for some days...

- 
  Minipolice - 1 year ago
  -
  -
  Still open 8 of may but needed a few refreshments. Not all unarchivers works. The standard Mac unarchiver won't accept the key but download the unarchiver from App Store to try to see that you've got the right key before you make a script file.

- 
  danynap - 1 year ago
  -
  -
  Futher updates. I paid 0.01BTC and received the password, that works. Since few days, the price has increased to 0.03 !! Anyway with Widows and Linux (I have this) decrypters work fine. In case Mac has problems, try to access data through a different machine, maybe it's easier.

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: