Cr1ptT0r Ransomware Infects D-Link NAS Devices, Targets Embedded Systems

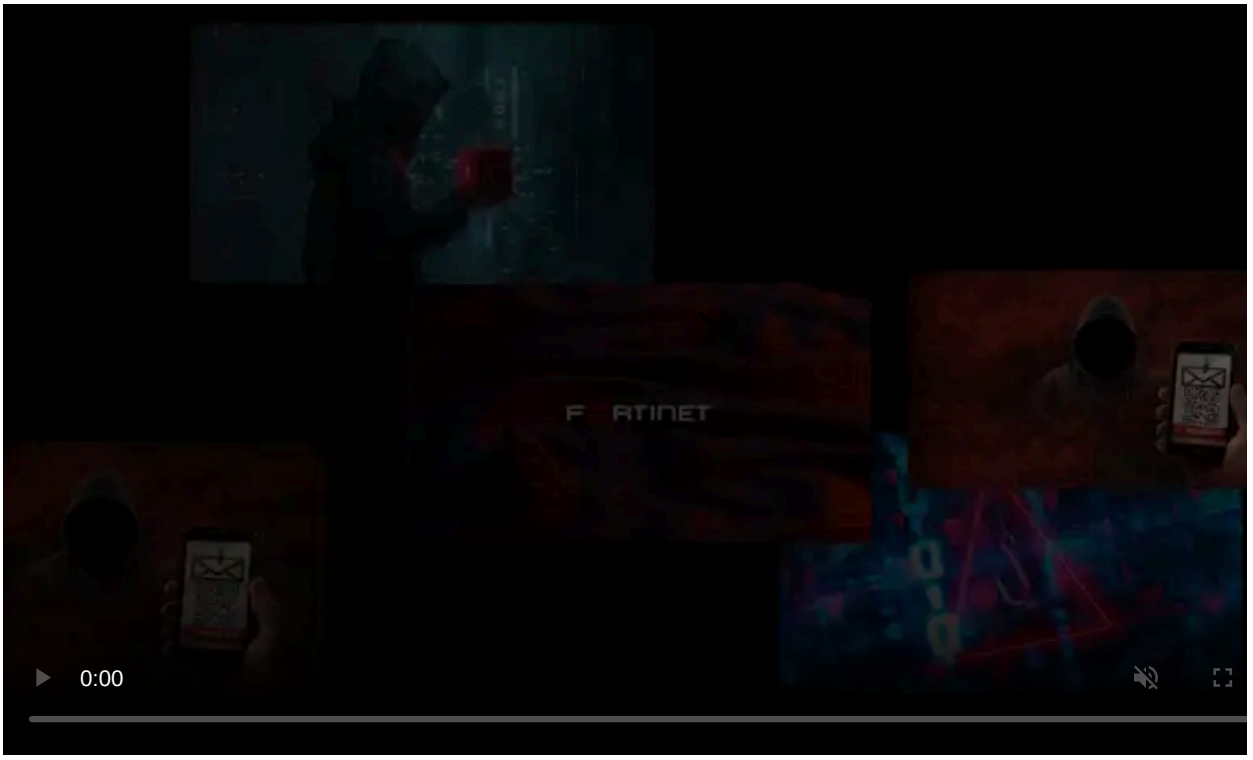
By Ionut Ilascu

Published: 2019-02-22 · Archived: 2026-04-05 21:55:27 UTC

A new ransomware called Cr1ptT0r built for embedded systems targets network attached storage (NAS) equipment exposed to the internet to encrypt data available on it.

Cr1ptT0r was first discovered in the BleepingComputer forums where users stated that their D-Link DNS-320 devices were infected by the ransomware. D-Link no longer sells the DNS-320 enclosure but the product page indicates that it is still supported. However, the newest firmware revision came out in 2016 and there are plenty of known bugs that can be leveraged to compromise the equipment.

Scanning the malicious ELF binary on Thursday showed a minimum detection rate on VirusTotal, with only one antivirus engine identifying Cr1ptT0r as a threat. At the time of publishing, the malware is picked up by at least six antivirus engines.


F RTINET
0:00

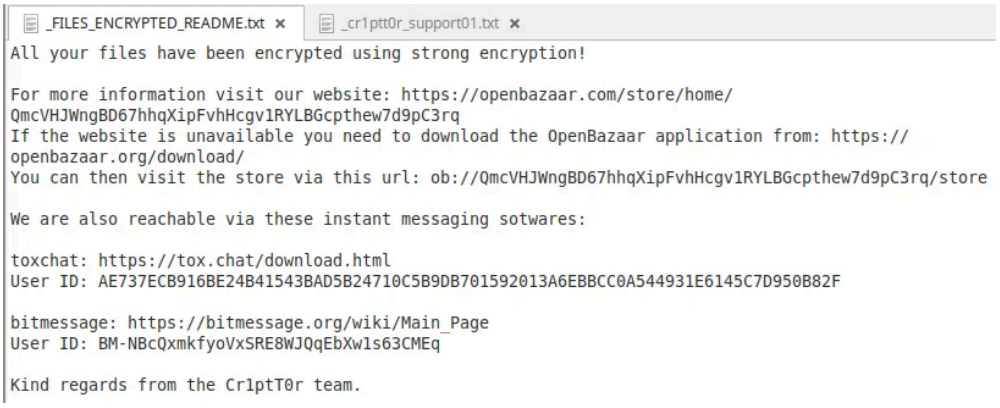
Old firmware is a sitting duck

Details are scarce at the moment, but BleepingComputer forum members offer information suggesting that the attack vector is most likely vulnerabilities in old firmware. A member of the Cr1ptT0r team confirmed this to us, saying that there are so many vulnerabilities in D-Link DNS-320 NAS models that they should be built from scratch to make things better.

Although old versions of the firmware for DNS-320 are known to be vulnerable to at least one bug leading to remote code execution, a hard-coded backdoor was published in 2018 for ShareCenter DNS-320L.

Some users affected by Cr1ptT0r admitted to having an outdated firmware version installed and that their device was exposed to the internet at the time of the attack.

The malware drops two plain text files on the infected devices. One is the ransom note called "_FILES_ENCRYPTED_README.txt," which gives information to the victim on how to get more details about what happened and how to reach the ransomware operators to pay the ransom in exchange for the file decryption key.



h/t Desdra

The ransom note points the victim to the Cr1ptT0r decryption service, which holds the same contact details and the steps for getting the unlock key.

To verify that they can decrypt the data, the operators offer to unlock the first file for free.

The other text file has the name "_cr1ptt0r_support.txt" and stores the address of a website in the Tor network. This is a support URL that victims can provide if they are at a loss about what to do; it enables a remote shell on an infected device if it is online. The Cr1ptT0r group member added that the URLs and IP addresses are not logged, so there is no correlation between data and the victim.

Although the Cr1ptT0r member says they are just interested in getting paid and that spying is not on their agenda, they cannot guarantee privacy.

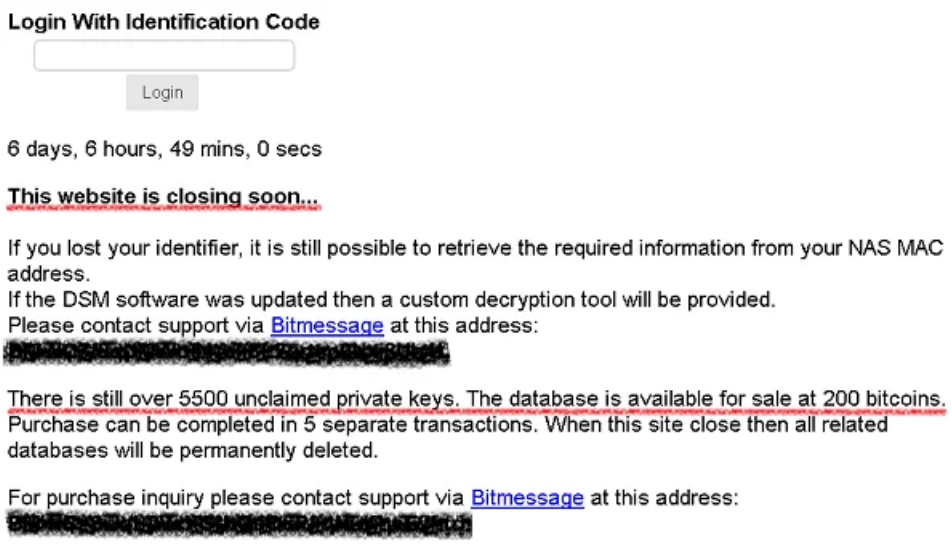
Synolocker decryption keys also available

Keys for unlocking files are sold via OpenBazaar marketplace, for BTC 0.30672022 (about $1,200 at the current Bitcoin price). There is also an option to pay less for individual file decryption. The cost for this is $19.99 and you have to send the encrypted file to receive it decrypted.

A recent update to the OpenBazaar store page shows that the operator of the ransomware also offers decryption keys for Synolocker for the same price. This ransomware strain did serious damage back in 2014 when it infected NAS servers from Synology that ran outdated versions of the DiskStation Manager containing two vulnerabilities. This was possible despite the vendor releasing the patches at least eight months before.

The crew behind Synolocker shut down their website in mid-2014 and offered to sell in bulk all the unclaimed decryption key they had for 200 BTC (about $100,000 at the time), over 5,500 of them. The crew announced that when all the databases

would be permanently deleted when closing the website.



Today, matching the private key that unlocks the data in lack of a victim ID is possible via by brute-forcing, a process that is fairly quick in this case, with a few minutes to complete, the ransomware handler told us.

No extension added to locked files

The ransomware, which is an ELF ARM binary, does not append a specific extension to the encrypted data, but security researcher Michael Gillespie did a brief analysis of the malware and the files it encrypts and found it added the end-of-file marker "_Cr1ptT0r_"

He also says that the strings he noticed suggest that this ransomware strain uses the Sodium crypto library and that it uses the "curve25519xsalsa20poly1305" algorithm for asymmetric encryption. We received confirmation about these details from the Cr1ptT0r group member we talked to.

The public key (256-bit) used for encrypting the data is available in a separate file named "cr1ptt0r_logs.txt," which stores a list of the encrypted files as well, and it is also appended at the end of the encrypted files, just before the marker. Gillespie says that it matches the encryption algorithm he noted above.

At the moment, the ransomware handler seems interested in targeting NAS devices, which are popular with small businesses to store and share data internally. This is likely the reason for the steep ransom demand.

Cr1ptT0r is new on the market, but it looks like it's planning a long stay. It is built for Linux systems, with a focus on embedded devices, but it can be adapted to Windows, too, according to its maker. The end game is making money, and, as someone familiar with this sort of business told us, it can have an almost infinite return on investment. The malware does not have a significant presence at the moment but it could turn into a nasty threat.

Update 2/27/19: D-Link issued a security advisory for this ransomware.

IOCs

Hash:

```
9a1de00dbc07271a27cb4806937802007ae5a59433ca858d52678930253f42c1
```

File names:

```
cr1ptt0r
```

Ransom note text:

```
 All your files have been encrypted using strong encryption!

For more information visit our website: https://openbazaar.com/store/home/QmcVHJWngBD67hhqXipFvhHcgv1RYLBGcpthew7d9pC3rq
If the website is unavailable you need to download the OpenBazaar application from: https://openbazaar.org/download/
You can then visit the store via this url: ob://QmcVHJWngBD67hhqXipFvhHcgv1RYLBGcpthew7d9pC3rq/store

We are also reachable via these instant messaging sotwares:

toxchat: https://tox.chat/download.html
User ID: AE737ECB916BE24B41543BAD5B24710C5B9DB701592013A6EBBCC0A544931E6145C7D950B82F

bitmessage: https://bitmessage.org/wiki/Main_Page
User ID: BM-NBcQxmkfyoVxSRE8WJQqEbXw1s63CMEq

Kind regards from the Cr1ptT0r team.
```

Source: https://www.bleepingcomputer.com/news/security/cr1ptt0r-ransomware-infects-d-link-nas-devices-targets-embedded-systems/