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

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

Ionut Ilascu

By
Ionut Ilascu

- February 22, 2019
- 06:18 AM
- 2

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.

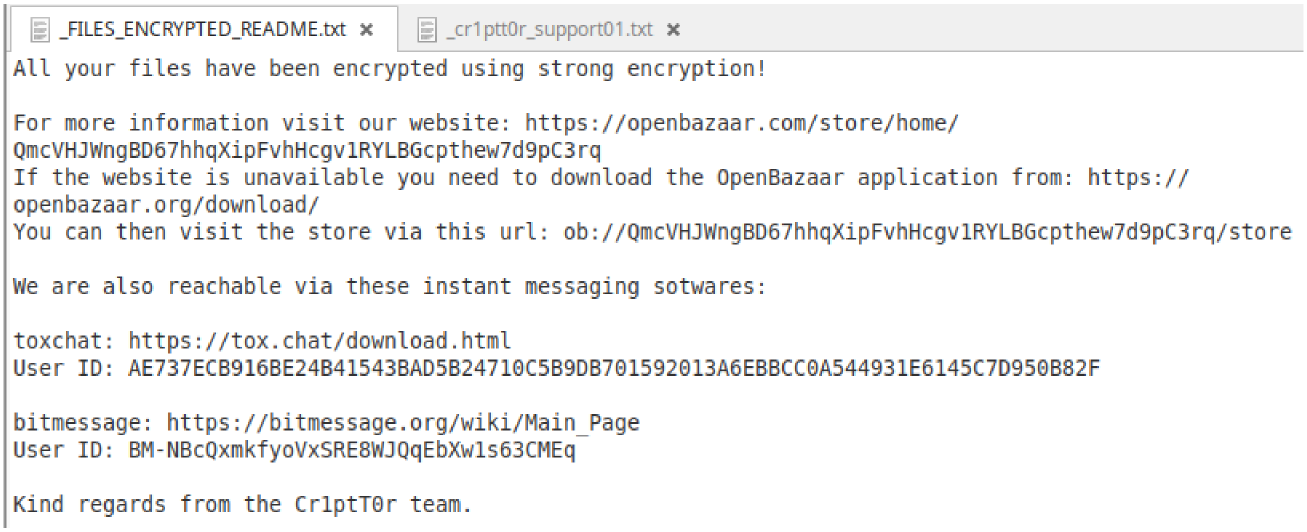
Old firmware is a sitting duck

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Some users affected by Cr1ptT0r admitted to having an outdated firmware version installed and that their device was exposed to the internet at the time of the attack.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



```
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.
```

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.

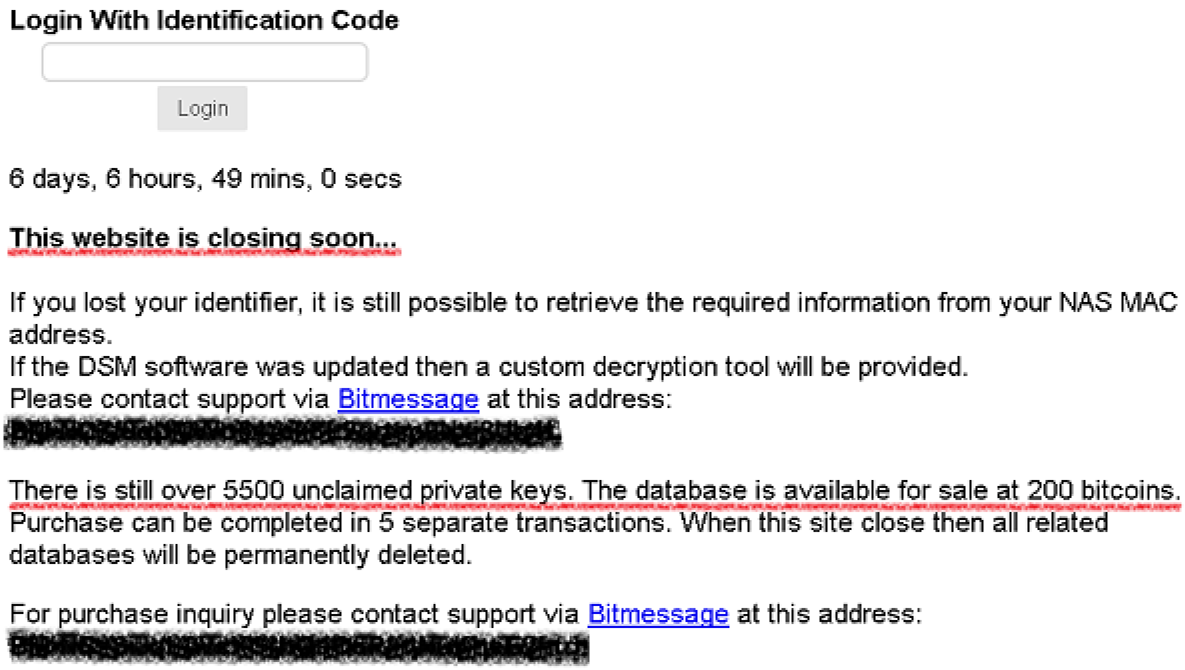
Although the Cr1ptT0r member says they are just interested in getting paid and that spying is not on their agenda, they cannot guarantee privacy.

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.



Login With Identification Code

6 days, 6 hours, 49 mins, 0 secs

This website is closing soon...

If you lost your identifier, it is still possible to retrieve the required information from your NAS MAC address.
If the DSM software was updated then a custom decryption tool will be provided.
Please contact support via Bitmessage at this address:
[redacted]

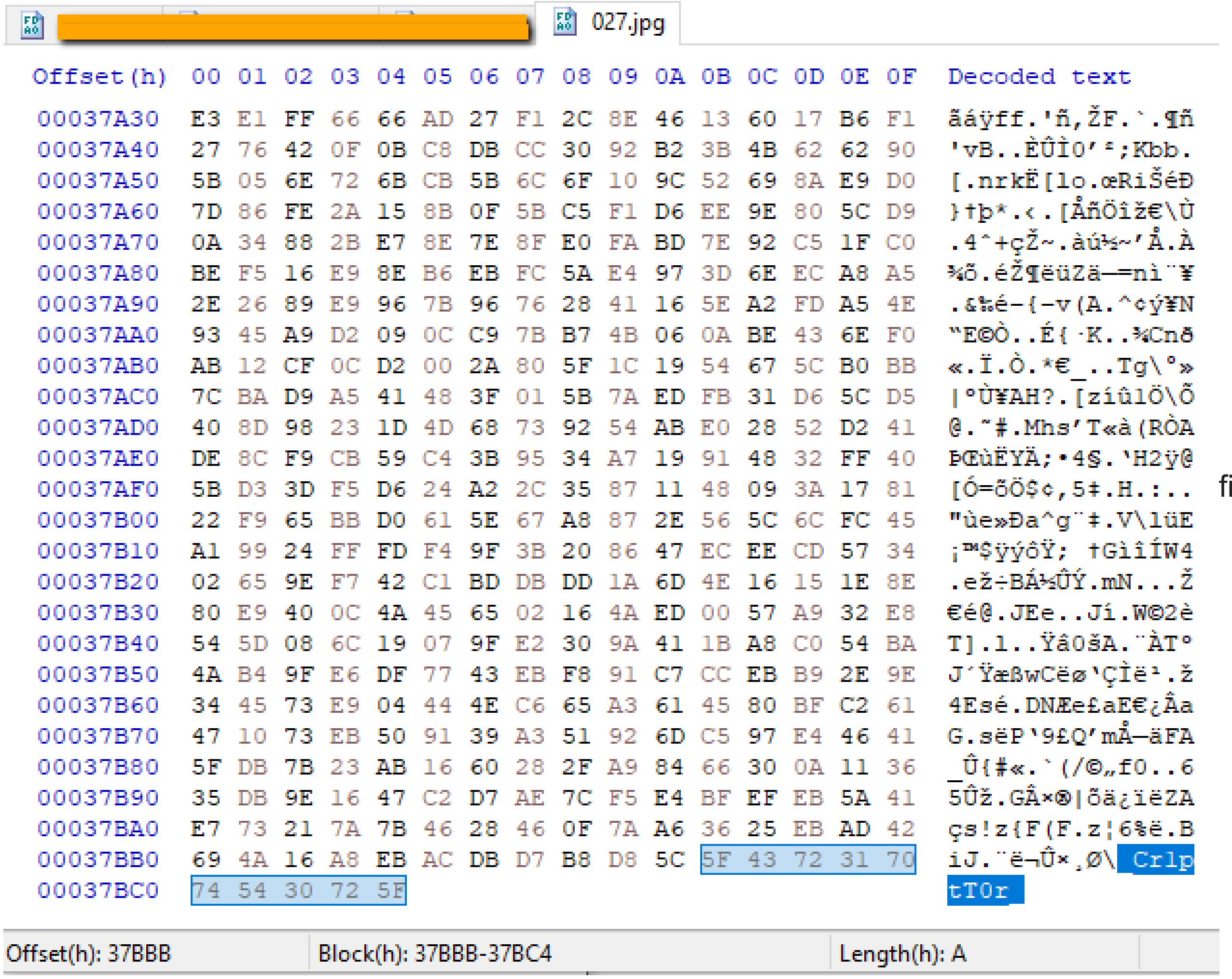
There is still over 5500 unclaimed private keys. The database is available for sale at 200 bitcoins.
Purchase can be completed in 5 separate transactions. When this site close then all related databases will be permanently deleted.

For purchase inquiry please contact support via Bitmessage at this address:
[redacted]

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_"



[redacted] 027.jpg

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00037A30   E3 E1 FF 66 66 AD 27 F1 2C 8E 46 13 60 17 B6 F1  ãáÿff.'ñ,ŽF.`.¶ñ
00037A40   27 76 42 0F 0B C8 DB CC 30 92 B2 3B 4B 62 62 90  'vB..ÈÛÌ0'²;Kbb.
00037A50   5B 05 6E 72 6B CB 5B 6C 6F 10 9C 52 69 8A E9 D0  [.nrkË[lo.œRiŠéÐ
00037A60   7D 86 FE 2A 15 8B 0F 5B C5 F1 D6 EE 9E 80 5C D9  }†þ*.‹.[ÅñÖîž€\Ù
00037A70   0A 34 88 2B E7 8E 7E 8F E0 FA BD 7E 92 C5 1F C0  .4ˆ+çŽ~.àú½~'Å.À
00037A80   BE F5 16 E9 8E B6 EB FC 5A E4 97 3D 6E EC A8 A5  ¾õ.éŽ¶ëüZä—=nì¨¥
00037A90   2E 26 89 E9 96 7B 96 76 28 41 16 5E A2 FD A5 4E  .&‰é–{–v(A.^¢ý¥N
00037AA0   93 45 A9 D2 09 0C C9 7B B7 4B 06 0A BE 43 6E F0  "E©Ò..É{·K..¾Cnð
00037AB0   AB 12 CF 0C D2 00 2A 80 5F 1C 19 54 67 5C B0 BB  «.Ï.Ò.*€_..Tg\°»
00037AC0   7C BA D9 A5 41 48 3F 01 5B 7A ED FB 31 D6 5C D5  |ºÙ¥AH?.[zíû1Ö\Õ
00037AD0   40 8D 98 23 1D 4D 68 73 92 54 AB E0 28 52 D2 41  @.˜#.Mhs'T«à(RÒA
00037AE0   DE 8C F9 CB 59 C4 3B 95 34 A7 19 91 48 32 FF 40  ÞŒùËYÄ;•4§.'H2ÿ@
00037AF0   5B D3 3D F5 D6 24 A2 2C 35 87 11 48 09 3A 17 81  [Ó=õÖ$¢,5‡.H.:..
00037B00   22 F9 65 BB D0 61 5E 67 A8 87 2E 56 5C 6C FC 45  "ùe»Ða^g¨‡.V\lüE
00037B10   A1 99 24 FF FD F4 9F 3B 20 86 47 EC EE CD 57 34  ¡™$ÿýôŸ; †GìîÍW4
00037B20   02 65 9E F7 42 C1 BD DB DD 1A 6D 4E 16 15 1E 8E  .ež÷BÁ½ÛÝ.mN...Ž
00037B30   80 E9 40 0C 4A 45 65 02 16 4A ED 00 57 A9 32 E8  €é@.JEe..Jí.W©2è
00037B40   54 5D 08 6C 19 07 9F E2 30 9A 41 1B A8 C0 54 BA  T].l..Ÿâ0šA.¨ÀTº
00037B50   4A B4 9F E6 DF 77 43 EB F8 91 C7 CC EB B9 2E 9E  J´ŸæßwCëø'ÇÌë¹.ž
00037B60   34 45 73 E9 04 44 4E C6 65 A3 61 45 80 BF C2 61  4Esé.DNÆe£aE€¿Âa
00037B70   47 10 73 EB 50 91 39 A3 51 92 6D C5 97 E4 46 41  G.sëP'9£Q'mÅ—äFA
00037B80   5F DB 7B 23 AB 16 60 28 2F A9 84 66 30 0A 11 36  _Û{#«.`(/©„f0..6
00037B90   35 DB 9E 16 47 C2 D7 AE 7C F5 E4 BF EF EB 5A 41  5Ûž.GÂ×®|õä¿ïëZA
00037BA0   E7 73 21 7A 7B 46 28 46 0F 7A A6 36 25 EB AD 42  çs!z{F(F.z¦6%ë.B
00037BB0   69 4A 16 A8 EB AC DB D7 B8 D8 5C 5F 43 72 31 70  iJ.¨ë¬Û×¸Ø\_Cr1p
00037BC0   74 54 30 72 5F                                   tT0r_
```

Offset(h): 37BBB   Block(h): 37BBB-37BC4   Length(h): A

file marker, h/t @demonslay335

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.

Related Articles:

QNAP alerts NAS customers of new DeadBolt ransomware attacks

QNAP warns of ransomware targeting Internet-exposed NAS devices

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

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

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.
```

- Cr1ptT0r
- DLink
- NAS

- Ransomware

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.

- Previous Article
- Next Article

Comments

-
  Bullwinkle-J-Moose - 3 years ago
  -
  -

  Remote code execution due to old firmware is irrelevant if I'm allowed to hardware write protect the drive

  Over 10 years ago, Western Digital's email response to my asking for hardware write protection was....
  You cannot make required changes or get updates if the drive is write protected!

  My response to their response is still the same.....
  The entire contents are scanned for malware and this is DATA I NEED TO KEEP!
  There is no need for changes or updates!

  Seagate's response was equally lame and not listed here

  Hello Manufacturers:

  We need to KEEP our data and stop relying on firmware updates that never work

  GET A CLUE!

  But what if we NEED to make changes to the data?
  You Don't!
  Keep the old data write protected
  Timestamp the new data being written and figure out a way to write protect it immediately or stop selling this garbage altogether

  If I wanted temporary data, I'd just write it to RAM!

-
  woody188 - 3 years ago
  -
  -

  Why would anyone put their NAS on the Internet to begin with?

  Maybe should have hired a professional instead of asking your nephew who plays Fortnite and claims to know computers to set up your SMB devices. Doh!

  I know I'm blaming the victim but get a clue. Stupid is as stupid does.

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: