

Cr1ptT0r Ransomware spreads on D-Link NAS devices, targeting embedded systems

A new ransomware software called Cr1ptT0r is built for embedded systems that target network attached storage devices (NAS) that have been spread over the internet, and have the task of encrypting data available on infected devices. .

A new ransomware software called Cr1ptT0r is built for embedded systems that target network attached storage devices (NAS) that have been spread over the internet, and have the task of encrypting data available on infected devices. .

Cr1ptT0r was first discovered on the BleepingComputer forum, in which many users reported that their D-Link DNS-320 devices were infected with this ransomware. D-Link no longer sells the DNS-320 model, but this product is still supported by the manufacturer. But the problem is that the latest firmware for the device has also appeared since 2016, and since then, there have been many security holes used to penetrate the device because there is no Additional patches from D-Link.

The malicious ELF binary scanning processes performed last Thursday showed the minimum malware detection rate on VirusTotal, only one antivirus tool identified Cr1ptT0r is a threat.



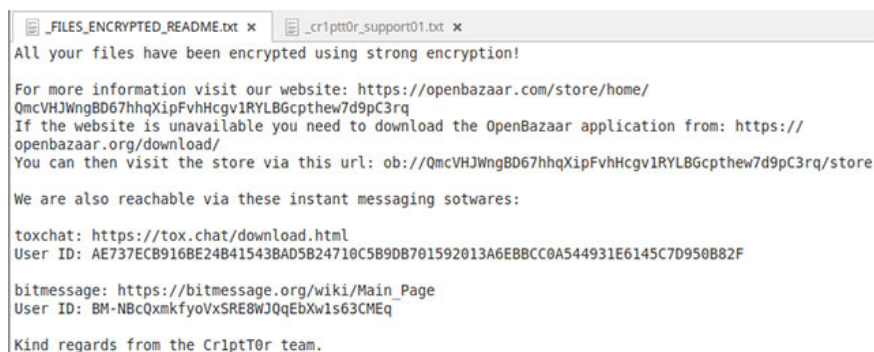
Cr1ptT0r RANSOMWARE

Too old firmware can result in serious security consequences

Members on the BleepingComputer forum have also provided a lot of information to show that the attack method is likely to originate from a vulnerability that appears in the old firmware version. A member of the Cr1ptT0r group confirmed this and said there were many holes in the D-Link NAS-320 NAS models that should have been patched earlier.

Some users affected by Cr1ptT0r acknowledge that they have installed the outdated software version, and their device has been 'exposed' on the internet at the time of the attack.

Malware only assigns two simple text files on infected devices. One is the ransom note named "_FILES_ENCRYPTED_README.txt", instructing the victim on how to get more detailed information about the situation that is happening on their system, and how to contact malicious scammers to pay ransom in exchange for decoding keys for encrypted files.

A screenshot of a text editor window showing a ransom note. The window title is "_FILES_ENCRYPTED_README.txt". The text inside reads: "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." data-bbox="229 279 763 445"/>

```
_FILES_ENCRYPTED_README.txt x  _cr1ptt0r_support01.txt x
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.
```

The ransom note takes the victim to the Cr1ptT0r decoding service, which stores the same contact details, as well as steps to get the encryption key open. And to prove to the victim that they are holding real decryption keys, malicious code dispersers will decrypt a "free" file on the system.

Besides, the remaining text is named "_cr1ptt0r_support.txt" and contains the address of a web page in the Tor network. This is a support URL that the victim can use in case they do not know what to do, it allows to create a remote cover on the infected device if the device is in the state online. The Cr1ptT0r team member also added that the URLs and IP addresses will not be recorded, so there will not be any correlation between the data and the victim.

Although saying that it is only about getting paid and collecting personal information is not something the attackers aim for, there is nothing to ensure that your data is not collected and why Unauthorized storage!

Synolocker decoding key is also available for use

The keys to unlock encrypted files have been sold through OpenBazaar for 0.30672022 BTC (about \$ 1,200 at the current Bitcoin exchange rate). There is also a less expensive option for decrypting individual files. The cost for this is \$ 19.99 and you will have to manually send the encrypted files.

A recent update to the OpenBazaar site shows that publishers have also provided decryption keys for Synolocker malware at the same price. This ransomware category caused serious damage in 2014 when it infected NAS servers from Synology, running outdated versions of DiskStation Manager containing up to two major security holes, although the provider delivered it. Release the patch at least 8 months earlier.

The team behind Synolocker closed their website in mid-2014, and offered to sell all the bulk decoding keys for 200 BTC (about \$ 100,000 at the time). The group also announced that all databases will be permanently deleted when the official website is closed.

Login With Identification Code

Login

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]

Going back to the present, combining private keys to unlock data without a victim ID can be accomplished via brute-forcing quickly, in particular, only a few minutes in case this.

No extensions are added to the locked file

This Ransomware is essentially an ARM ELF binary, ie it will not append any specific extension to the encrypted data. However, security researcher Michael Gillespie also briefly analyzed this malware as well as the files it encrypted and found that the mark "_Cr1ptT0r_" was added at the end of the file.

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	9E	46	13	60	17	B6	F1	äáyff. 'ñ, žF. ' .qñ
00037A40	27	76	42	0F	0B	C8	DB	CC	30	92	B2	3B	4B	62	62	90	'vB..ÈÛI0'";Kbb.
00037A50	5B	05	6E	72	6B	CB	5B	6C	6F	10	9C	52	69	8A	E9	D0	[.nrkĚ[1o.eRiŠēD
00037A60	7D	86	FE	2A	15	8B	0F	5B	C5	F1	D6	EE	9E	80	5C	D9	}tp*.<.[Āñ0izē\Ů
00037A70	0A	34	88	2B	E7	8E	7E	8F	E0	FA	BD	7E	92	C5	1F	C0	.4'+qž~.äú~-'Ā.Ā
00037A80	BE	F5	16	E9	8E	B6	EB	FC	5A	E4	97	3D	6E	EC	A8	A5	%ō.éžžēūZā~ni"Ÿ
00037A90	2E	26	89	E9	96	7B	96	76	28	41	16	5E	A2	FD	A5	4E	.šwē-{-v(A.^ōyŸN
00037AA0	93	45	A9	D2	09	0C	C9	7B	B7	4B	06	0A	BE	43	6E	F0	"E@Ō..Ě(-K..%Cn8
00037AB0	AB	12	CF	0C	D2	00	2A	80	5F	1C	19	54	67	5C	B0	B8	«.Ī.Ō.*Ě...Tg'°»
00037AC0	7C	BA	D9	A5	41	48	3F	01	5B	7A	ED	FB	31	D6	5C	D5	!°ŮWAH?.[ziĪLŌŌ
00037AD0	40	8D	98	23	1D	4D	68	73	92	54	AB	E0	28	52	D2	41	@."#.Mns'Twā (RŌA
00037AE0	DE	8C	F9	CB	59	C4	3B	95	34	A7	19	91	48	32	FF	40	ŤGŪĚYĀ; *4\$. 'H2y8
00037AF0	5B	D3	3D	F5	D6	24	A2	2C	35	87	11	48	09	3A	17	81	[Ō=šŌšc,5+.H...
00037B00	22	F9	65	BB	D0	61	5E	67	A8	87	2E	56	5C	6C	FC	45	"ŭe»Đa^g"+.V\lŭE
00037B10	A1	99	24	FF	FD	F4	9F	3B	20	86	47	EC	EE	CD	57	34	!ŸŸyŏŸ; +GliĪW4
00037B20	02	65	9E	F7	42	C1	DB	DD	1A	6D	4E	16	15	1E	8E		.ež~BĀ~ŮŸ.mN...ž
00037B30	80	E9	40	0C	4A	45	65	02	16	4A	ED	00	57	A9	32	E8	ēē@.JEe..Ji.WŌžē
00037B40	54	5D	08	6C	19	07	9F	E2	30	9A	41	1B	A8	C0	54	BA	T].1..YāŌŌA.'ĀT°
00037B50	4A	B4	9F	E6	DF	77	43	EB	F8	91	C7	CC	EB	B9	2E	9E	J'ŸBwCēo'Çiē'.ž
00037B60	34	45	73	E9	04	44	4E	C6	65	A3	61	45	80	BF	C2	61	4Ešē.DNĚēfaEēĀa
00037B70	47	10	73	EB	50	91	39	A3	51	92	6D	C5	97	E4	46	41	G.sēP'9ēŌ' mĀ~āFA
00037B80	5F	DB	7B	23	AB	16	60	28	2F	A9	84	66	30	0A	11	36	Ů{#x.'(/@.,ŤŌ..6
00037B90	35	DB	9E	16	47	C2	D7	AE	7C	F5	E4	BF	EF	EB	5A	41	ŮŮž.GĀ*Ÿ šž;ŸēZĀ
00037BA0	E7	73	21	7A	7B	46	28	46	0F	7A	A6	36	25	EB	AD	42	çš!z{F(F.z; çšē.B
00037BB0	69	4A	16	A8	EB	AC	DB	D7	B8	D8	5C	5F	43	72	31	70	iJ."ē~Ůx,Ō\ Cr1p
00037BC0	74	54	30	72	5E												tT0r

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

In addition, the researcher said that the strings he observed suggested that this ransomware strain used a sodium cryptographic library and it used the algorithm "curc25519xsalsa20poly1305" to perform asymmetric encryption.

Besides, the public key (256-bit) used to encrypt the data available in a separate file named "cr1ptt0r_logs.txt" also stores the list of encrypted files and is also added. The end of the files is encrypted, and according to Gillespie, this is entirely consistent with the encryption algorithm he noted above.

Currently, ransomware dispersers seem to be paying more attention to targeting NAS devices, which are commonly used by small businesses in storing and sharing internal data.

Cr1ptT0r is a new name that appears, but it doesn't seem to be easy to deal with at all. According to malicious developers, this ransomware is built for Linux systems, focusing on embedded devices, but it can also be adjusted to target Windows, and of course the ultimate goal is only Ransom from the victim. Cr1ptT0r is currently only distributed on a small scale, its presence is not too significant at this time, but it can become a major threat if preventive measures are not implemented in time. .

You finished reading the article "**Cr1ptT0r Ransomware spreads on D-Link NAS devices, targeting embedded systems**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.