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.

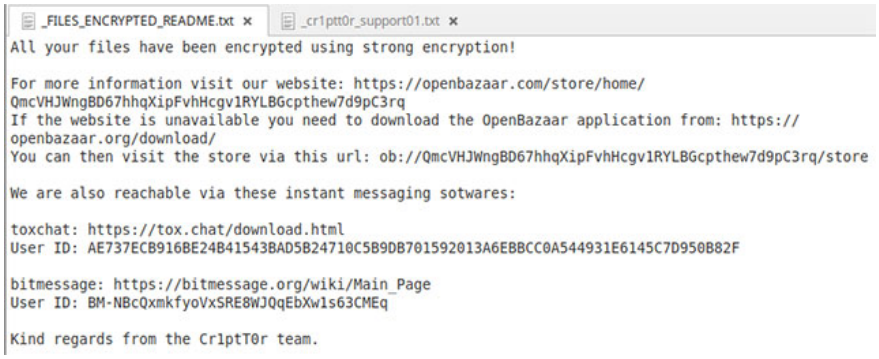
The malicious ELF binary scanning processes performed last Thursday showed the minimum malware detection rate on VirusTotal, only one antivirus tool identified Cr1ptT0r is a threat.

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Some users affected by Cr1ptT0r acknowledge that they have installed the outdated software version, and their device has been 'exposed' on the internet at the time of the attack.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



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.

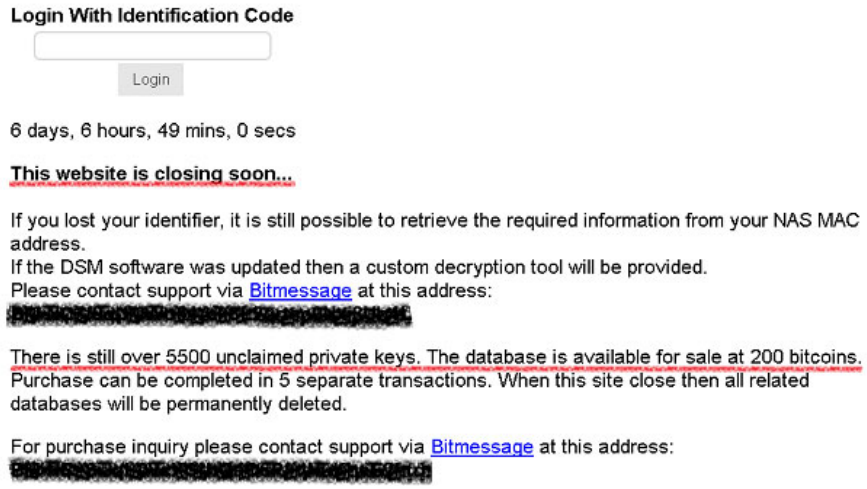
Although saying that it is only about getting paid and collecting personal information is not something the attackers aim for, there is nothing to ensure that your data is not collected and why Unauthorized storage!

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.

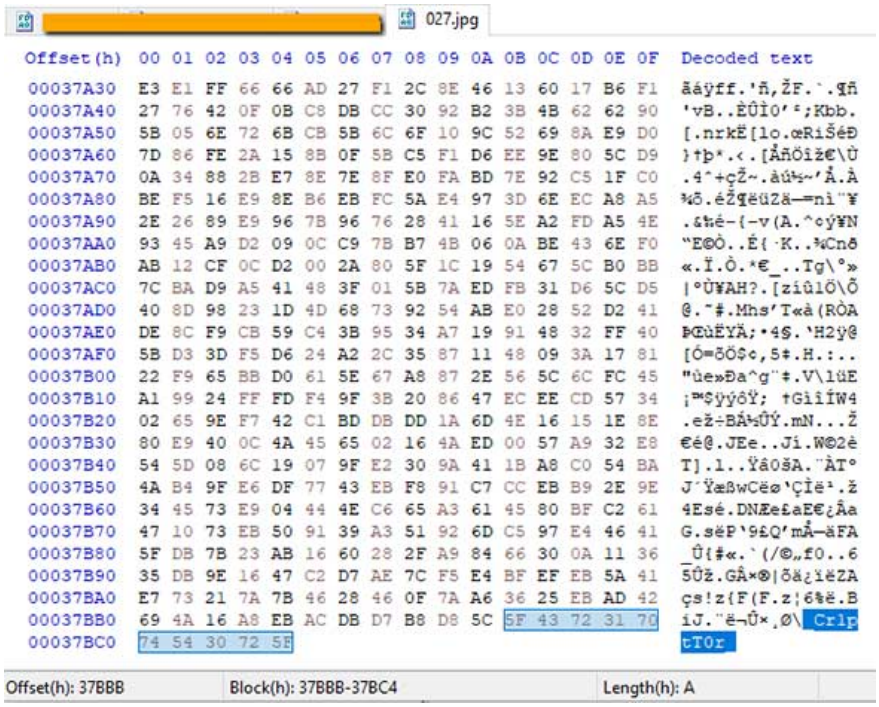
The team behind Synolocker closed their website in mid-2014, and offered to sell all the bulk decoding keys for 200 BTC (about $ 100,000 at the time). The group also announced that all databases will be permanently deleted when the official website is closed.



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.



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.

© 2019 TipsMake.com