Severity

High

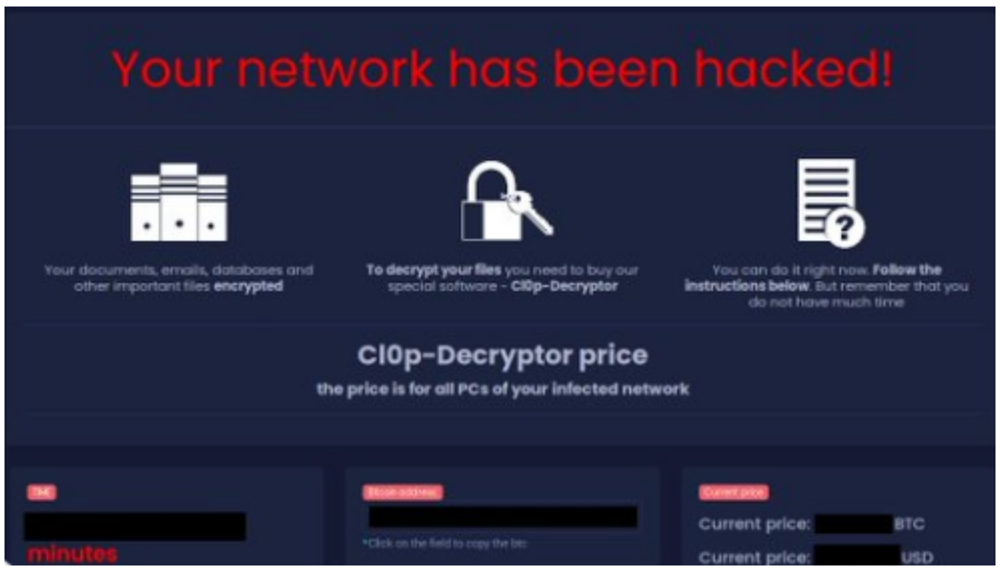
Analysis Summary

The crypter being used reuses the code from the ransomware itself. According to the security Researchers, the crypter is a modified form of RC4 encryption and written in Delphi.

Ransom Note:

——=== Welcome. Again. ===—— [-] Whats HapPen? [-] Your files are encrypted, and currently unavailable. You can check it: all files on your system has extension csruj. By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER). [+] What guarantees? [+] Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities — nobody will not cooperate with us. Its not in our interests. To check the ability of returning files, You should go to our website. There you can decrypt one file for free. That is our guarantee. If you will not cooperate with our service — for us, its does not matter. But you will lose your time and data, cause just we have the private key. In practice — time is much more valuable than money. [+] How to get access on website? [+] You have two ways: 1) [Recommended] Using a TOR browser! a) Download and install TOR browser from this site: b) Open our website: 2) If TOR blocked in your country, try to use VPN! But you can use our secondary website. For this: a) Open your any browser (Chrome, Firefox, Opera, IE, Edge) b) Open our secondary website: Warning: secondary website can be blocked, thats why first variant much better and more available. When you open our website, put the following data in the input form: Key: ——— !!! DANGER !!! DON'T try to change files by yourself, DON'T use any third party software for restoring your data or antivirus solutions — its may entail damage of the private key and, as result, The Loss all data. !!! !!! !!! ONE MORE TIME: Its in your interests to get your files back. From our side, we (the best specialists) make everything for restoring, but please should not interfere. !!! !!! !!!

Researchers believe that the ransomware is linked to REvil Ransomware group.



Your network has been hacked!

Your documents, emails, databases and other important files **encrypted**

To decrypt your files you need to buy our special software - **Cl0p-Decryptor**

You can do it right now. **Follow the instructions below**. But remember that you do not have much time

Cl0p-Decryptor price

the price is for all PCs of your infected network

Time

[redacted]

minutes

Bitcoin address

[redacted]

*Click on the field to copy the btc

Current price

Current price: [redacted] BTC

Current price: [redacted] USD

The interface is similar to the Cl0p ransomware.

Impact

- Data Theft
- File Encryption
- Financial Loss
- Security Bypass

Indicators of Compromise

MD5

- 72a63d3fa404d68096a0327c34f677c8
- d0b24313df94b7dab1091ebe5914d04f

- 32ae1e5f5b231e464280633f7744d09e
- 50e7dde91425de6797b582bc8843de2b
- 25114401f045effa032c10a9cf607c90
- 08b52ad57604262d819a246d940d7121
- 16658c0126f282d1c3a837e57465a473
- 937906b46fcc3a62105721924518061b
- 7c06d521509198da3d8bc3b5f3571af7
- 937413106f3970bbc4a5c05e2777c14e
- 691e46fb5ebd82510c5f6a28867d3d5b
- d0928784dc12aea56e358fac7f1dd9fa
- 4d50eb39ff8ff771b71ff3d1179e2391

SHA-256

- 0125d8e744bb40ee8bf74beb9c43eb4ffc4e5217cf80a1843f8d19dfb888ad68
- 0329a7ec26e9a76e729a45e73dffd80e1e91f9bc6449d8557913cb52fe83e0f6
- 036d5608101b352f119180d2dabb8261fd43d134aca84137c4f6ad1ae289b10a
- 06812b8d48f1bb00b49bd2366031a471598e093ff117e7403b5bdc87dbc189fa
- 06cce1044e58ebfa48fe2399857e82519d47773f112a81c053455d0dd6955de4
- 07fab613fd41f52673bf67e84cecba39c719d724769cfe8f37afbd0d6ff45860
- 089cc9981931e492dfea30fdbdb9381db2f3467208192179983c7520d53b690b
- 094997ed8543b42a78aa0ce9aaef8e2caca2a882c5b21832d50844f38a7d2973
- 0a38130da830fc1b164e963894fb869b5aa8b225fb4ffab730c7e08dabe5bb10
- 0abc7d41f326b4a5915d2656a142daf809391f2275f148b31f96b4e3be641f89
- 0bdb3a563c28d818d5b6cc3057d60878283ac28bffff9954449b2384b68e60b6
- 0f05b893b67c4fc8680f2040b4069eba81e144253a7f6e20507eaa4d2576461d
- 0f61649fca3c5a8570421d5a241fee3fafabcef70f1ea6a81ff2dd26c7d07874

SHA-1

- d81173de0becd320040ca950e153f4860719e599
- 269bfa65fc234d897d1d055ff73c34a6e199e46b
- a4d2a8a905726286ffbb84344c7a730e6071a92d
- f3977680482f9bc36bbc0d37f7e0dbda52ce3eec
- b7418b1738f18e67ca28e3eeac93e9a5590f91f6
- 37c8ab26e6576c3dbc2004ffc99d2e765432465e
- e60347839ea8c9925e72d524c10cd3b2c7c907f0
- e7646a66a5a47a05a5b2b8aa83ce090835277c97
- 60d640eabc0fe7cac54cef1c61c2245ace9dcd0e
- d4c6e553df8bea09a65aa8d849396c23e43d0d68
- 5980a6e5f32bbf1d3b25e3082740f897ec2fd0c3
- 78f0f09d6ef900cf31bf44edfed6d7bf22997b0e
- 332632dcdfc273aa5adf66b3c5d24301f22771ab

Remediation

- Never open attachments or links received by unknown senders.
- Emails from unknown senders should always be treated with caution.
- Look for IOCs in your surroundings.
- At your respective controls, disable all threat indicators.