

LockFile Ransomware Bypasses Protection Using Intermittent File Encryption

thehackernews.com/2021/08/lockfile-ransomware-bypasses-protection.html

August 28, 2021

LOCKBIT2.0

ALL YOUR IMPORTANT FILES ARE STOLEN AND ENCRYPTED!

Any attempts to restore your files with the third-party software will be **fatal** for your files!
To recovery your data and not to allow data leakage, it is possible only through purchase of a private key [from us](#)

There is only one way to get your files back:

Through a standard browser

- Brave (supports Tor links)
- FireFox
- Chrome
- Edge
- Opera

♦ Open link - <https://decoding.at/>

Through a Tor Browser - recommended

ATTENTION!

- ♦ <https://decoding.at> may be blocked. We recommend using a Tor browser (or Brave) to access the TOR site
- ♦ Do not rename encrypted files.
- ♦ Do not try to decrypt using third party software, it may cause permanent data loss.
- ♦ Decryption of your files with the help of third parties may cause increased price (they add their fee to our).
- ♦ Tor Browser may be blocked in your country or corporate network. Use <https://bridges.torproject.org> or use Tor Browser over VPN.
- ♦ Tor Browser user manual <https://7b-manual.torproject.org/abc>

A new ransomware family that emerged last month comes with its own bag of tricks to bypass ransomware protection by leveraging a novel technique called "intermittent encryption."

Called LockFile, the operators of the ransomware have been found exploiting recently disclosed flaws such as ProxyShell and PetitPotam to compromise Windows servers and deploy file-encrypting malware that scrambles only every alternate 16 bytes of a file, thereby giving it the ability to evade ransomware defences.

 CyberSecurity

"Partial encryption is generally used by ransomware operators to speed up the encryption process and we've seen it implemented by BlackMatter, DarkSide and LockBit 2.0 ransomware," Mark Loman, Sophos director of engineering, said in a statement. "What sets LockFile apart is that, unlike the others, it doesn't encrypt the first few blocks. Instead, LockFile encrypts every other 16 bytes of a document."

"This means that a file such as a text document remains partially readable and looks statistically like the original. This trick can be successful against ransomware protection software that relies on inspecting content using statistical analysis to detect encryption," Loman added.

Sophos' analysis of LockFile comes from an artifact that was uploaded to VirusTotal on August 22, 2021.

Once deposited, the malware also takes steps to terminate critical processes associated with virtualization software and databases via the Windows Management Interface (WMI), before proceeding to encrypt critical files and objects, and display a ransomware note that bears stylistic similarities with that of LockBit 2.0.

```
267 |      uVar8 = uVar18;
268 |      lVar15 = lVar17;
269 |      do {
270 |          local_13e8 = ZEXT816(0);
271 |          EncryptBuffer_0002cbf4(local_13c0,lVar15,local_13e8,lVar15);
272 |          lVar15 = lVar15 + 0x20;
273 |          uVar8 = uVar8 + 1;
274 |          *(ulonglong *) (lVar16 + 0x208 + lVar17) = uVar8;
275 |          if (0x4e1fffff < uVar8) break;
276 |          uVar14 = uVar14 - 1;
277 |      } while (uVar14 != 0);
278 |      FUN_00002a30(&local_13c8);
279 |      (*_UnmapViewOfFileStub_00062040) (lVar17);
280 |      (*_CloseHandle_00062058) (local_res20);
281 |      (*_CloseHandle_00062058) (lVar12);
```

The ransom note also urges the victim to contact a specific email address "contact@contipauper.com," which Sophos suspects could be a derogatory reference to a competing ransomware group called Conti.

What's more, the ransomware deletes itself from the system post successful encryption of all the documents on the machine, meaning that "there is no ransomware binary for incident responders or antivirus software to find or clean up."

"The message here for defenders is that the cyberthreat landscape never stands still, and adversaries will quickly seize every possible opportunity or tool to launch a successful attack," Loman said.

The disclosure comes as the U.S. Federal Bureau of Investigation (FBI) released a [Flash report](#) detailing the tactics of a new Ransomware-as-a-Service (RaaS) outfit known as Hive, consisting of a number of actors who are using multiple mechanisms to compromise business networks, exfiltrate data and encrypt data on the networks, and attempt to collect a ransom in exchange for access to the decryption software.

SHARE     

SHARE 