


Black Suit Ransomware

Date: 06th June 2024 | Severity:  High

Summary

- Black Suit uses intermittent encryption techniques to speed up the encryption process and then appends each encrypted file with the <.blacksuit> extension.
- The ransomware also drops a ransom note (README.BlackSuit.txt) in every encrypted directory. Finally, the ransomware disables the system's safe boot mode, restarts the system, and deletes its traces.
- Black Suit operates an active leak site, in which it uploads the data of victims who refuse to pay the ransom.
- The Black Suit ransomware strain shares many similarities with the one used by the Royal ransomware group. This may indicate that Black Suit is either a new variant developed by the same threat actors, a copycat, or an affiliate of Royal.

Attack Vectors

- An analysis of the Linux variant of a new ransomware strain called Black Suit has covered significant similarities with another ransomware family called Royal.
- It runs a double extortion scheme that steals and encrypts sensitive data in a compromised network in return for monetary compensation. Data associated with a single victim has been listed on its dark web leak site.
- The latest findings from Trend Micro show that, both Black Suit and Royal use OpenSSL's AES for encryption and utilize similar intermittent encryption techniques to speed up the encryption process.
- The emergence of Black Suit ransomware (with its similarities to Royal) indicates that it is either a new variant developed by the same authors, a copycat using similar code, or an affiliate of the Royal ransomware gang that has implemented modifications to the original family," Trend Micro said.
- Triple extortion refers to a three-pronged approach wherein data exfiltration and encryption is coupled with distributed denial-of-service (DDoS) attacks against the targets in an attempt to disrupt their business and coerce them into paying the ransom.
- The DDoS service, per Cyble, is available for an added \$500,000 fee, with the operators imposing conditions that forbid affiliates from striking entities located in the Commonwealth of Independent States (CIS) countries.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	<ul style="list-style-type: none">• 1c849adcccad4643303297fb66bfe81c5536be39a87601d67664af1d14e02b9e• 9656cd12e3a85b869ad90a0528ca026e• 30cc7724be4a09d5bcd9254197af05e9fab76455• 90ae0c693f6ffd6dc5bb2d5a5ef078629c3d77f874b2d2ebd9e109d8ca049f2c• 861793c4e0d4a92844994b640cc6bc3e20944a73• 748de52961d2f182d47e88d736f6c835• b57e5f0c857e807a03770feb4d3aa254d2c4c8c8d9e08687796be30e2093286c• 69feda9188dbebc2d2efec5926eb2af23ab78c5d• 6ac8e7384767d1cb6792e62e09efc31a07398ca2043652ab11c090e6a585b310• 4d7f6c6a051ecb1f8410243cd6941b339570165ebcfd3cc7db48d2a924874e99• 7e7f666a6839abe1b2cc76176516f54e46a2d453
URL	<ul style="list-style-type: none">• http://weg7sdx54bevnvulapqu6bpz wztryeflq3s23tegbmnhkbpqz637f2yd[.]onion/

Recommendation

- Submit the File Hash to the Antivirus team to update their database with the file hashes.
- Avoid browsing the unsafe websites, clicking on suspicious links, or opening unknown email attachments.
- Update and Patch operating system, applications, and security software's up to date with latest patches.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- [https://dashboard\[.\]ti\[.\]insight\[.\]rapid7\[.\]com/#/tip/cyber-term/647c6ca9a91394258676e462](https://dashboard[.]ti[.]insight[.]rapid7[.]com/#/tip/cyber-term/647c6ca9a91394258676e462)
- [thehackernews\[.\]com/2023/06/new-linux-ransomware-strain-blacksuit\[.\]html](thehackernews[.]com/2023/06/new-linux-ransomware-strain-blacksuit[.]html)