BlackSuit Ransomware Strikes Windows and Linux Users

Date: 22nd April 2024 | Severity: High

Summary

The BlackSuit ransomware group was first reported by Palo Alto’s Unit 42 in May 2023. The group targets users of both Windows and Linux operating systems.

Attack Vectors

- Once executed, BlackSuit’s ransomware strain uses several command-line arguments (slightly different for each of its OS-specific variants) as part of its operation.
- Using these arguments and appropriate functions, the ransomware assigns a unique identifier for each victim, enumerates available network shares on the local system, retrieves a list of logical drives, and terminates processes (for example, virtual machines).
- BlackSuit 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.
- The BlackSuit ransomware strain shares many similarities with the one used by the Royal ransomware group.
- This may indicate that BlackSuit is either a new variant developed by the same threat actors, a copycat, or an affiliate of Royal.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• 1c849adcccad4643303297fb66bfe81c5536be39a87601d67664af1d14e02b9e • 9656cd12e3a85b869ad90a0528ca026e • 748de52961d2f182d47e88d736f6c835 • 90ae0c693f6ffd6dc5bb2d5a5ef078629c3d77f874b2d2ebd9e109d8ca049f2c • 861793c4e0d4a92844994b640cc6bc3e20944a73 • 30cc7724be4a09d5bcd9254197af05e9fab76455 • b57e5f0c857e807a03770feb4d3aa254d2c4c8c8d9e08687796be30e2093286c • 69feda9188dbebc2d2efec5926eb2af23ab78c5d • 6ac8e7384767d1cb6792e62e09efc31a07398ca2043652ab11c090e6a585b310 • 4d7f6c6a051ecb1f8410243cd6941b339570165ebcfd3cc7db48d2a924874e99 • 7e7f666a6839abe1b2cc76176516f54e46a2d453
URL	• http://weg7sdx54bevnvulapqu6bpzwztryeflq3s23tegbmnhkbpqz637f2yd[.]onion/

Recommendation

- Monitor darkweb activities for early indicators and threat mitigation.
- Conduct cybersecurity awareness programs for employees, third parties, and vendors.
- Implement a risk-based vulnerability management process for IT infrastructure to ensure that critical vulnerabilities and security misconfigurations are identified and prioritized for remediation.
- Instruct users to refrain from opening untrusted links and email attachments without verifying their authenticity.
- Deploy reputed anti-virus and internet security software packages on your company-managed devices, including PCs, laptops, and mobile devices.
- Turn on the automatic software update features on computers, mobiles, and other connected devices.

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 Link

- https://cyble.com/blog/blacksuit-ransomware-strikes-windows-and-linux-users/

Copyright © Mphasis Corporation. All rights reserved