Phobos Ransomware

Date: 06th March 2024 | Severity: High

Summary

Phobos is a ransomware that locks or encrypts files to demand a ransom. It uses AES encryption with different extensions, which leaves no chance to recover the infected files.

Phobos attackers gain initial access through vulnerabilities in Remote Desktop Protocol (RDP) ports, utilizing phishing techniques and brute-force attacks to compromise networks.

Subsequent to gaining access, they deploy tools like Smokeloader, enhancing their ability to execute the ransomware, escalate their privileges, and navigate through the compromised networks all while evading detection by manipulating system settings.

The malicious program uses encrypt data using AES and adds extensions to infected files such as .Phobos, .phoenix, .actin, .help, .mamba and others. These files can be fully or partially encrypted

Attack Vectors

- The ransomware targets organizations all over the world. Phobos compromises RDP servers that are open or have weak security.
- Then cyber criminals send ransom notes, where the victim is asked to contact one of the emails to get the decryption key.
- The executable file makes its way into an infected system and runs, then the main malicious activity begins. After the start of execution, the Ransomware deletes shadow copies. Interestingly though, as soon as it encrypts all targeted files, Phobos pops up a ransom note on the desktop, which is the ransomware executable file itself.

Phobos Ransomware distribution several ways to end up on your machine:

- phishing emails with attachments
- poorly secured RDP ports
- fake updates

- exploits
- deceptive downloads
- web injectors
- repacked and infected installers
- These distribution methods help attackers to steal victims' information and encrypt the data by running Trojan or other malware.

Indicator of Compromise

INDICATOR TYPE	INDICATORS
File Hash	58626a9bfb48cd30acd0d95debcaefd188ae794e1e0072c5bde8adae9bccafa6[.] f3be35f8b8301e39dd3dffc9325553516a085c12dc15494a5e2fce73c77069ed[.] 518544e56e8ccee401ffa1b0a01a10ce23e49ec21ec441c6c7c3951b01c1b19c[.] 32a674b59c3f9a45efde48368b4de7e0e76c19e06b2f18afb6638d1a080b2eb3[.] FC6865253D4C6BC89CE344A15778AD374C4BCB128FAD7CD7CDCB2A3DA178FB4E[.] 25E3689F86ED1836778F07977F0D4B491B8D6976218A4D9C3F4C45257D8A7004[.] ED42BB9E3F5959E3D58872874381D92E50C601CD1BE46EFFEB3724FF19EEEF71[.] 7FB694FDC0C631F0C7DE4CAC710103449AF7190297FB414E6FA2EFAB0AED9C1D[.] 9859774E60063ABD001E036C3A86D6C48D4A25F48A3CE00E70FDA34FFBB76807[.] 9969E4C5B2496651BE60078E79551A2F8A4440C3D150FAC77A7E29621A766924[.] C8D9A9758516D5A8936BD3BC01A9997FB677ED1DC54081CAA985883935FF092B[.] 0385DD2419ADF0FE1A1E5D5ED28AAECBCEB1411010FB06A1B0798D84ECA4732E[.] 84A1D361FD86517F8329952B8D6E492B2FAC2A7B99672DF9849C42656AFF36F5[.] F25A3E2BBAA9BED0210ADF5BFF0BC5D76FBF44E09AE4BC22E40473814A6EBAD1[.] 4AE6519E0D6A7AAF9B684497763257E3A752EF0B31B4BA31AFB9AECD1AF59D9A[.] 883162246C3D0A2C10E5C35A2A43FF444A24DBCF9E64DC5CC09009B9CD0AB48E[.] 80F8B5688126DB9F1B410E922DA7307DF0668988BCF477D9D99EAB04960BAC13[.] 1F2C57FEB6FCB80FE02D53778FA7C6B3BCBA0319229FE9B9FF725A24D939C2B6[.] F08472DCE8F14D5EAC38C530B6D467E01150CC68DEDDC5EB238F672578F88C98[.] 30999D295AA681D2B6B7CA9F05C0D15B22E76D9772BC6DDF734E83C5B3F5EF2B[.] 00AD311A7EF556AF6C73A9D21C1E5D1ED7A48FE132F4849B6963F3381E02FDC4[.] 305433E3B14F864EF9CB91AC082726C5D4B98D0DA4A75C880E501516DC54FF68[.] 43E33028A0A27A61BA859B06B3DC3B4415A484B143E8C3989CBC299774E4D3B2[.] 4D30670F6311DC373DCBFB5BD93CF1621B1D6C425C8C9A95DC0A1317D0BDF648[.]
Domian	adstat477d[.].xyz demstat577d[.].xyz serverxlogs21.[.]xyz

Recommendation

Submit the File Hash to the Antivirus team to update their database with the file hashes.

Submit the Domains to the Network team to update their database with the Domains.

Secure RDP ports to prevent threat actors from abusing and leveraging RDP tools.

Prioritize remediating known exploited vulnerabilities.

Implement EDR solutions to disrupt threat actor memory allocation techniques.

Make regular backups of important and critical files.

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://thehackernews.com/2024/03/phobos-ransomware-aggressively.html

https://any.run/malware-trends/phobos

Copyright © Mphasis Corporation. All rights reserved.