T2022_17 What you should know about RedAlert Ransomware (9th September 2022)

What is RedAlert (N13V)?

RedAlert (N13V) is a piece of malicious software that is classified as ransomware, a type of malware that encrypts data and demands payment to decrypt it. This ransomware is multi-platform; the Windows variant is known as RedAlert, while the Linux VMware ESXi server-targeting version is known as N13V.

When a RedAlert (N13V) is executed, it encrypts files and appends a ".crypt[number]" extension to their filenames. For example, a file named "1.jpg" became "1.jpg.crypt416," and so on. Following this, the RedAlert (N13V) ransomware generated a ransom note called "HOW TO RESTORE.txt." The message contained within this file indicated that this ransomware is aimed at businesses rather than individuals.

Technical Details

This ransomware is mostly distributed through phishing and social engineering techniques. Malicious software is typically disguised as or bundled with legitimate software/media. Viruses can be delivered in a variety of formats, including archives, executables, Microsoft Office and PDF documents, JavaScript, etc. The infection process begins when a malicious file is executed, run, or otherwise opened. Online scams, drive-by downloads, dubious download channels (e.g., unofficial and free file-hosting sites, Peer-to-Peer sharing networks, etc.), malicious attachments/links in spam emails and messages, illegal program activation tools ("cracks"), and fake updates are among the most common distribution methods.

This ransomware has been discovered to target VMware ESXi servers running on both Windows and Linux systems. The Linux encryptor is intended to target VMware ESXi servers and includes command line parameters that enable threat actors to shut down running virtual machines before encrypting the file. The malware only targets files associated with VMware ESXi servers, such as log files (.log), swap files (.vswp), virtual disks (.vmdk), and memory files, and has been observed to use the NTRUEncrypt algorithm for encryption operations (.vmem).

The ransomware also has been observed to add a description of the data compromised to each folder, as well as a Tor link that directs victims to the ransom

payment site. The payment page on the Tor network is similar to other Ransomware operation pages in that a ransom demand is displayed and options for negotiating with threat actors are provided. For ransom payment, RedAlert/N13V threat actors only accept Monero cryptocurrency.

Mitigation

To avoid becoming a victim of similar ransomware attacks that may occur, the following steps should be taken.

- Be wary of untrustworthy e-mail content.
- Suspicious email attachments and links should be avoided.
- Using dependable anti-malware software should be avoided.
- It is best to avoid using licensed and current technologies.
- Used a security solution since it blocks shared IOC (Indicator of Compromise) findings regarding the malware campaign.

Remediation

It is never a good idea to pay the attackers to decrypt your files because they will take the ransom and then disappear. If you believe you have been infected with RedAlert (N13V) ransomware, take the following steps to isolate and remediate the infection:

- Isolate the infected device(s)
- Reimage the infected device(s).
- Restore a clean copy of files from backups.

The Guyana National CIRT recommends that users and administrators review these recommendations and implement them where necessary.

References

- Meskauskas, T. (2022, September 2). *RedAlert (N13V) Ransomware*. Decryption, Removal, and Lost Files Recovery. Retrieved from PcRisk https://www.pcrisk.com/removal-guides/24501-redalert-n13v-ransomware#:%7E:text=RedAlert%20(N13V)%20is%20a%20piece,targeting%20version%20is%20called%20N13V.
- Toulas, B. (2022, September 1). *New ransomware hits Windows, Linux servers of Chile govt agency*. BleepingComputer. Retrieved from beeping

computer https://www.bleepingcomputer.com/news/security/new-ransomware-hits-windows-linux-servers-of-chile-govt-agency/