RTM Locker Ransomware Variant Targeting ESXi Servers



A newly identified variant of the RTM Locker ransomware appears specifically designed to target ESXi servers, CNAPP and XDR platform provider Uptycs reports.

RTM Locker – RTM stands for 'Read The Manual' – is offered under the ransomware-as-a-service (RaaS) business model, with affiliates required to be continuously active, otherwise they would be removed from the operation.

The threat does not target countries in the Commonwealth of Independent States (CIS) region and, unlike other ransomware gangs out there, its operators appear rather focused on staying under the radar instead of making headlines.

Following the analysis of a Windows version of RTM Locker earlier this month, Uptycs took a deep dive into the Linux variant of the threat, which has been observed targeting ESXi/Linux devices, and network-attached storage (NAS) systems.

The malware appears to have been inspired by Babuk ransomware's leaked code, based on the use of similar random number generation and on employing ECDH in Curve25519 for asymmetric encryption.

"The ransomware binary seems to be geared towards ESXi, because of the two ESXi commands that were noticed at the start of the program. It is statically compiled and stripped, making reverse engineering more difficult and allowing the binary to run on more systems," Uptycs notes.

RTM Locker's encryption process relies on asymmetric encryption as an initial step, and then moves to ChaCha20 symmetric encryption.

The ransomware creates an ephemeral key (it reads /dev/urandom for that) that is used as a private key during encryption. The private key is also used to generate a public key that is appended at the end of encrypted files. A shared key is also generated, to be used in symmetric ChaCha20 encryption.

The public key and the attacker's private key are used to obtain the shared secret and restore files.

"Use of both asymmetric and symmetric encryption makes it impossible to decrypt the encrypted files without the attacker's private key," Uptycs explains.

Related: Microsoft: Cl0p Ransomware Exploited PaperCut Vulnerabilities Since April 13

Related: Capita Confirms Data Breach After Ransomware Group Offers to Sell Stolen Information

Related: Ransomware Attack Hits Health Insurer Point32Health

https://www.securityweek.com/rtm-locker-ransomware-variant-targeting-esxi-servers/