RTM Locker ransomware targets VMware ESXi servers

Target Industry

Indiscriminate, opportunistic targeting.

Overview

The threat actor group, tracked as Read The Manual (RTM) Locker, has been detected targeting virtual machines on VMware ESXi servers via the deployment of a Linux encryptor. Analysis of the associated malware indicates that the encryptor has been crafted specifically for targeting VMware ESXi systems due to the linked commands used to manage virtual machines.

Impact

Successful exploitation by RTM Locker ransomware will result in the encryption and exfiltration of significant amounts of data held on the compromised device or system before a ransom of a predetermined amount is issued. The ransom fee demanded will almost certainly depend on the estimated value of the compromised organisation. Encrypted data may include private customer data, corporate finance data and system credentials. The double extortion strategy employed by the group will almost certainly result in all stolen data being published to dark web forums, where there is a realistic possibility that stolen data will be used for initial compromise in future attacks.

Incident Detection

The encryptor appends the ".RTM" file extension to the encrypted file names. Ransom notes are then created with the name, "!!! Warning !!!" on the target system.

Affected Products

VMware ESXi servers

Containment, Mitigations & Remediations

To mitigate against ransomware attacks, technical controls should be explored. These controls could encompass the enforcement of multi-factor authentication (MFA) for all users, conditional access policies and web proxies filtering on low- or non-reputation domains.

A primary method of reducing the threat posed by RTM ransomware is to detect it in the early stages using an effective and monitored endpoint detection and response (EDR) solution. An effective EDR tool, such as the Microsoft Defender suite, will block ransomware attempts once detected.

Organisations can also perform routine back-ups of sensitive data that is required for business operations and to keep a copy offline in case back-ups are impacted by the attack. Therefore, if a breach occurs and the business can no longer function, a back-up is ready to use, and the business can continue to operate with minimal disruption. However, this does not nullify the fact that customer and employee data may have also been lost, and potentially released because the Clop ransomware group operates via double or triple extortion.

Indicators of Compromise

RTM associated file hashes (SHA1):
– f4c746696b0f5bb565d445ec49dd912993de6361
– 025c718ba31e43db1b87dc13f94a61a9338c11ce
– 03de8622be6b2f75a364a275995c3411626c4d9f
– 094ac3c414a9e6028afa5cdc0d4b4f3aa98b92ca
– 1e4b84be1e4287c9787cd56009e1e2adb3348db8
– 42a4b04446a20993ddae98b2be6d5a797376d4b6
– 6cf45111b2d71862803cf91f2a79780149c46a27
– 6f036c802384826b630aec70d9833b5b0ed735eb
– 8966319882494077c21f66a8354e2cbca0370464
– 9ac461ef9848367f46bf64649d46de955c4afc66
– af862050a01972db36589653dc8b155e2b3e2f8c
– b1ee562e1f69efc6fba58b88753be7d0b3e4cfab
– c6e3aa123a52762bf2690b97cc79148eedd0e1e0
– daa0673cb1d3eb7dbe8aa435997ecd9e1da228fd
– df1a4c99791570a2d203075581a6aeef59ece02b
– f89e56dd9ca78cec02d0a2b95803843c59234082
– fca3d02a53e66d8975997ff2b03c8008a254a508
– 00fe6cf9c85821a2a2479083acb538ee49c8c141
– 2f6fd3b5a7611d72f9f9eb60b04471f9bebc738f
– 471a8fd0aa32ce61cf5e4ebece95527d1b234de6

RTM associated domains:
– micro4n[.]top
– vpntap[.]top
– vpnkeep[.]bit
– vpnomnet[.]bit
– webstatisticaonline[.]tech
– cainmoon[.]net
– cash-money-analitica[.]bit
– d47ea26b7faa[.]bit
– fde05d0573da[.]bit
– feb96eb2aa59[.]bit

– money-cash-analitica[.]bit
– rtm[.]dev
– ssdcool[.]top

RTM associated IP addresses:
– 185[.]141[.]27[.]249
– 185[.]82[.]216[.]14
– 188[.]138[.]71[.]117
– 158[.]255[.]208[.]197
– 185[.]169[.]229[.]42
– 185[.]61[.]149[.]78
– 5[.]154[.]191[.]57
– 91[.]207[.]7[.]69
– 95[.]183[.]52[.]182
– 109[.]236[.]82[.]150
– 109[.]248[.]32[.]152
– 131[.]72[.]138[.]169
– 154[.]70[.]153[.]125
– 158[.]255[.]6[.]150
– 185[.]128[.]42[.]237
– 185[.]61[.]149[.]70
– 185[.]82[.]201[.]45
– 200[.]74[.]240[.]134
– 212[.]48[.]90[.]155
– 213[.]184[.]127[.]137

Threat Landscape

It was recently reported by Trellix that RTM Locker had launched a new Ransomware-as-a-Service (RaaS) operation and had started recruiting affiliates, including those from the former Conti cybercrime syndicate. At the time of the initial reporting, only a Windows ransomware encryptor had been discovered. However, RTM has now expanded its mode of operation to target VMware ESXi servers.

VMware has a significant proportion of the virtualisation market. Given that threat actors generally utilise a combination of probability and asset value to determine which attack surfaces to focus on, VMware products have become a prime target for threat actors. Due to the fact that virtual machines have become an integral aspect of both personal and business affairs, threat actors will continue to exploit vulnerabilities contained within the associated devices in an attempt to extract the sensitive information contained therein.

Threat Group

The RTM cybercrime group has been observed to target remote banking systems, primarily in Russia. The group uses drive-by downloads and spam with attachments of fake contracts, invoices or tax forms to deliver a custom malware (RTM Banking Trojan) that targets accounting software and is used for the purposes of financial gain.

Further, the group operates within the confines of a RaaS model, whereby other threat actors are recruited to become affiliates. This indicates that the group is associated with a high level of sophistication and organisation and, as such, should be considered as a significant threat.

Mitre Methodologies

Execution Technique:
T1106 – Native API

Privilege Escalation Technique:
T1134.002 – Access Token Manipulation: Create Process with Token

Defense Evasion Techniques:
T1070.001– Indicator Removal: Clear Windows Event Logs
T1070.004 – Indicator Removal: File Deletion
T1134.002 – Access Token Manipulation: Create Process with Token

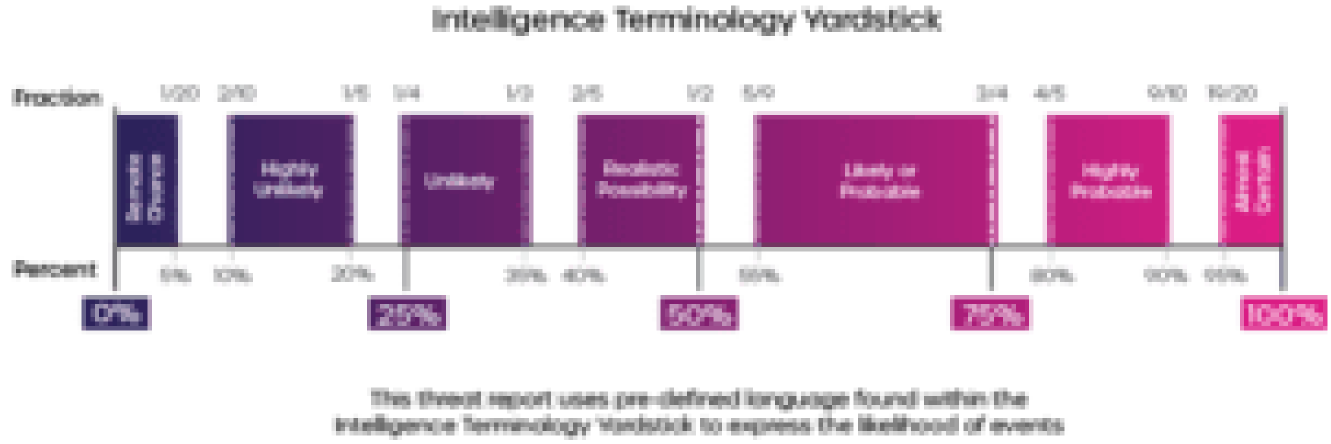
Discovery Technique:
T1057 – Process Discovery

Collection Technique:
T1005 – Data from Local System

Impact Techniques:
T1486 – Data Encrypted for Impact
T1489 – Service Stop

Further Information

Trellix Report



-
-
-

Powered by GDPR Cookie Compliance

Privacy Overview

This website uses cookies so that we can provide you with the best user experience possible. Cookie information is stored in your browser and performs functions such as recognising you when you return to our website and helping our team to understand which sections of the website you find most interesting and useful.