Mphasis
The Next Applied

# TargetCompany Ransomware Group

Date: June 9th 2024 | Severity: Medium

## Summary

The TargetCompany ransomware group is now employing a new Linux variant that uses a custom shell script as a means of payload delivery and execution, a technique not seen in previous variants.

## Attack Vectors

- In a report today, cybersecurity company Trend Micro says that the new Linux variant for TargetCompany ransomware makes sure that it has administrative privileges before continuing the malicious routine.
- To download and execute the ransomware payload, the threat actor uses a custom script that can also exfiltrate data to two separate servers, likely for redundancy in case of technical issues with the machine or if it gets compromised.
- Once on the target system, the payload checks if it runs in a VMware ESXi environment by executing the ‘uname’ command and looking for ‘vmkernel.’
- Next, a “TargetInfo.txt” file is created and sent to the command and control (C2) server. It contains victim information such as hostname, IP address, OS details, logged-in users and privileges, unique identifiers, and details about the encrypted files and directories.
- The ransomware will encrypt files that have VM-related extensions (vmdk, vmem, vswp, vmx, vmsn, nvram), appending the.locked extension to the resulting files.
- Finally, a ransom note named “HOW TO DECRYPT.txt” is dropped, containing instructions for the victim on how to pay the ransom and retrieve a valid decryption key.
- After all tasks have been completed, the shell script deletes the payload using the ‘rm -f x’ command so all traces that can be used in post-incident investigations are wiped from impacted machines.
- Trend Micro analysts are attributing the attacks deploying the new Linux variant of TargetCompany ransomware to an affiliate named vampire, who is likely the same one in a Sekoia report last month.
- The IP addresses used for delivering the payload and accepting the text file with the victim information were traced to an ISP provider in China. However, this is not enough for accurately determining the origin of the attacker.
- Typically, TargetCompany ransomware focused on Windows machines but the release of the Linux variant and the shift to encrypting VMWare ESXi machines shows the evolution of the operation.

- Trend Micro’s report includes a set of recommendations such as enabling multifactor authentication (MFA), creating backups, and keeping systems updated.
- The researchers provide a list of indicators of compromise with hashes for the Linux ransomware version, the custom shell script, and samples related to the affiliate vampire.

## Indicator of compromise

| INDICATOR TYPE | INDICATORS |
|---|---|
| File Hash | • dffa99b9fe6e7d3e19afba38c9f7ec739581f656<br>• 2b82b463dab61cd3d7765492d7b4a529b4618e57<br>• 9779aa8eb4c6f9eb809ebf4646867b0ed38c97e1<br>• 3642996044cd85381b19f28a9ab6763e2bab653c<br>• 4cdee339e038f5fc32dde8432dc3630afd4df8a2<br>• 0f6bea3ff11bb56c2daf4c5f5c5b2f1afd3d5098 |
| URLS | • hxxp://111.10.231[.]151:8168/general/vmeet/upload/temp/x.sh<br>• hxxp://111.10.231[.]151:8168/general/vmeet/upload/temp/x<br>• hxxp://111.10.231[.]151:8168/general/vmeet/upload/temp/post.php |

## Recommendation

- Submit the File Hash to the Antivirus team to update their database with the file hashes.
- 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://www.bleepingcomputer.com/news/security/linux-version-of-targetcompany-ransomware-focuses-on-vmware-esxi/
- https://www.trendmicro.com/en_us/research/24/f/targetcompany-s-linux-variant-targets-esxi-environments.html#:~:text=The%20Linuxbased%20variant%20can%20determine%20whether%20the%20victim%27s,and%20increase%20their%20chances%20of%20a%20ransom%20payout.