Ransomware uses WinRAR to lock victim's data

Because the encryption method is constantly being exposed by security software, ransomware called Memento used WinRAR to lock the victim's data.

Memento started operating last month. It exploits the VMware vCenter Server web client vulnerability to infiltrate the victim's system. This vulnerability is codenamed CVE-2021-21971 and has a score of 9.8 so the severity is extremely high.

CVE-2021-21971 allows anyone with remote access to TCP/IP port 443 on the exposed vCenter server to execute commands on elementary OS with administrative privileges.

The patch for CVE-2021-21971 was released in February 2021. However, based on Memento's activities, it can be seen that many organizations and businesses have not updated the patch.

Memento started exploiting CVE-2021-21971 from April. In May, another dangerous actor appeared to exploit this vulnerability to install XMR virtual currency mining tool via PowerShell command.

After infiltrating the victim's computer, Memento used WinRAR to create an archive of the stolen files and extract it. Next, they used Jetico's BCWipe data deletion utility to erase all remaining traces. After use, they use a ransomware strain programmed in Python to encrypt AES.

However, Memento's attempts to encrypt files failed because the system was protected by an anti-ransomware engine. The encryption process has been prevented so it has not caused any damage.

In the difficult, the wisdom emerges, Memento skips the file encryption step. Instead, they transfer all stolen files to a password-protected archive.

To do this, the hacker group would move the files to the WinRAR archive, set a strong password, encrypt the password, and then delete the original files.

Memento often requires victims to pay huge amounts of Bitcoin to ransom data. However, according to statistics so far, Memento victims often do not pay the ransom but use the backup to restore the files.

However, Memento is a new group, so it is likely that in the future they will upgrade their attack methods or change the target of attacks to be more effective.