Malware Analysis Spotlight: Rhino Ransomware

vmray.com/cyber-security-blog/rhino-ransomware-malware-analysis-spotlight/

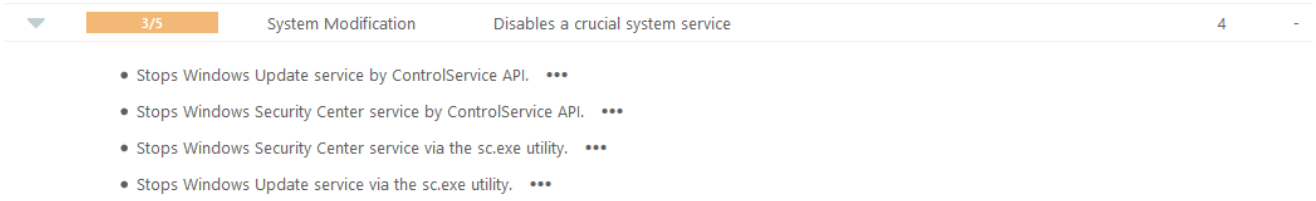
In this Malware Analysis Spotlight, the VMRay Labs Team examines the behavior of Rhino Ransomware (first identified in April 2020). This sample was found by Twitter user @GrujaRS on May 4th.

View the VMRay Analyzer Report

The first step before the ransomware encrypts user files, it disables various services:

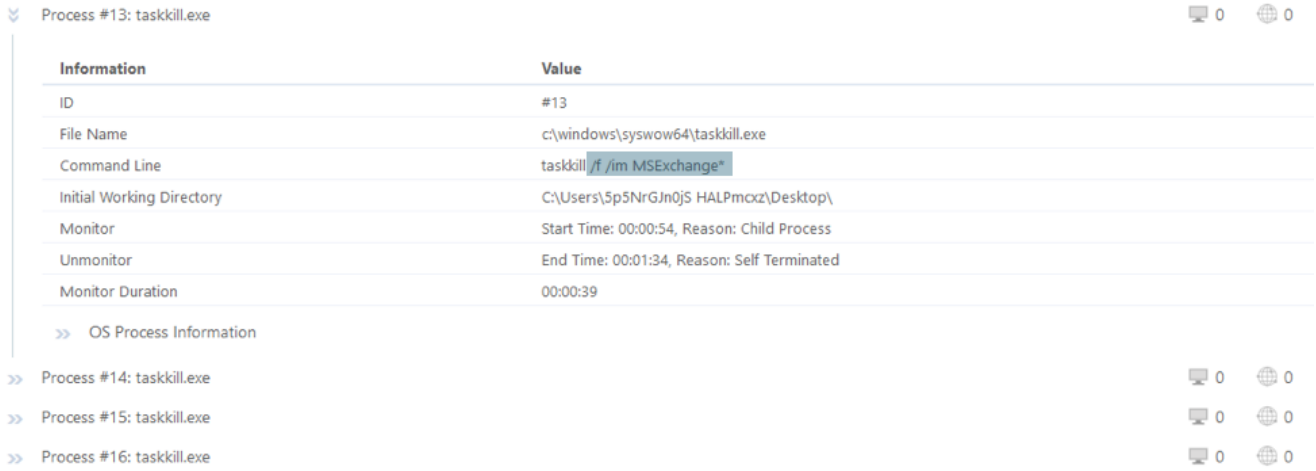
- wscsvc (Windows Security Center Service)
- WinDefend (Windows Defender Service)
- wuauserv (Windows Update Service)
- BITS
- ERSvc (Error Reporting Service)
- and WerSvc (Windows Error Reporting Service)

The malware author is disabling these services that would lead to an interruption (like restarting after a Windows Update) or an error in encryption (notifying an end-user of malicious activity using Windows Defender).

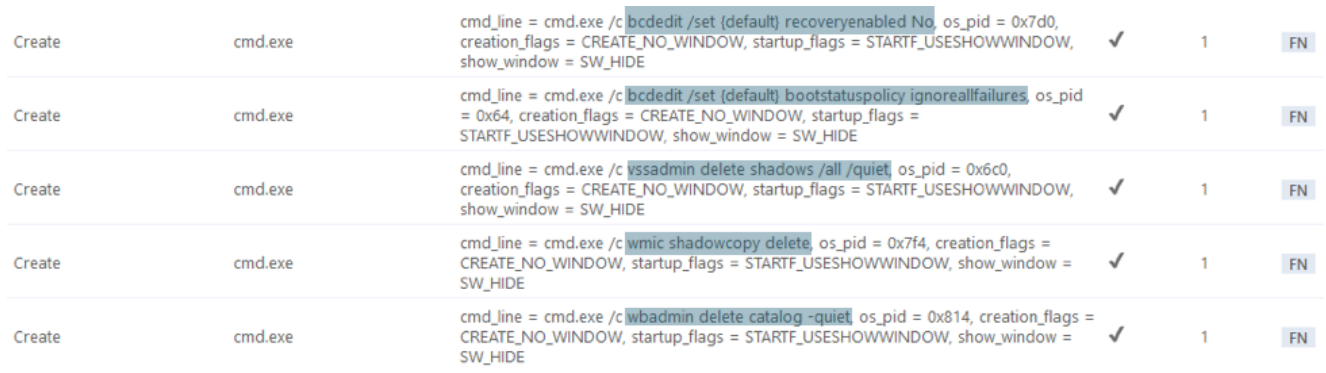


In addition to stopping the system services, the ransomware tries to stop running tasks of Microsoft Exchange, sqlserver, and sqlwriter. Stopping these tasks is also a way to ensure it's able to encrypt all files which might still be used by Microsoft Exchange during the encryption.

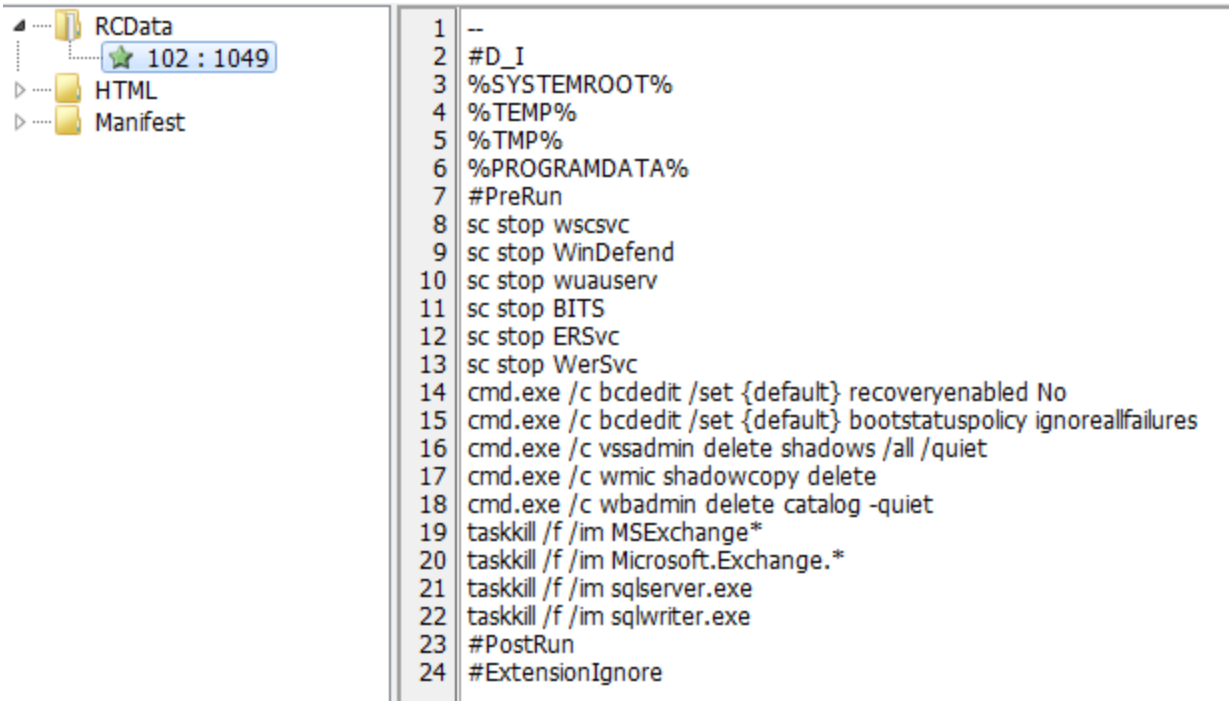
By focusing on Microsoft Exchange this could mean that Rhino Ransomware could be targeting businesses.



It hinders the recovery from backups by deleting relevant data like shadow copies and the backup catalog as well as disabling the Windows Recovery Mode with bcdedit.



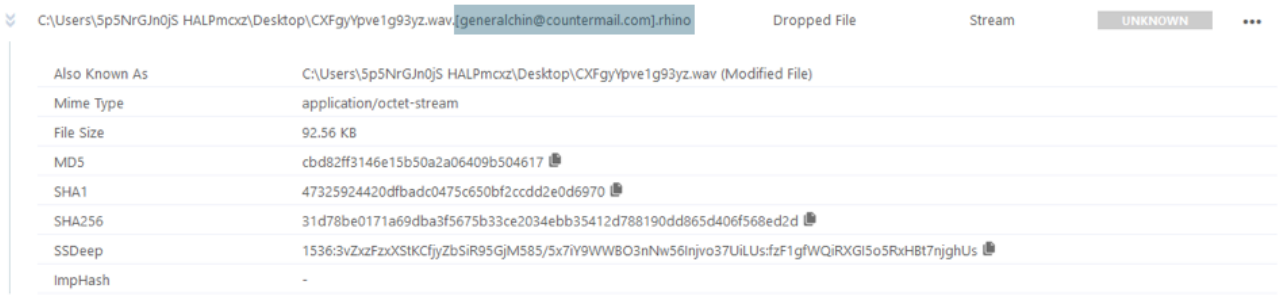
Typically, these commands are hardcoded in the program/malware itself but in this sample, the commands are embedded as a resource file. This design allows the malware author to change/update the commands without changing the logic inside.



To achieve persistence, the sample copies itself to the %AppData% directory as “mshtop32bit.exe” and creates a new entry in HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run for the value “MarvelHost”.

After the files have been encrypted, it adds the file marker “Marvel01” at offset filesize-32 to the content and appends the string “.[generalchin@countermail.com].rhino” to the filenames. The email in the appended string is also displayed in the ransom note.

The ransomware excludes files with the extension exe, sys, lnk, dll, msi and its ransom notes.

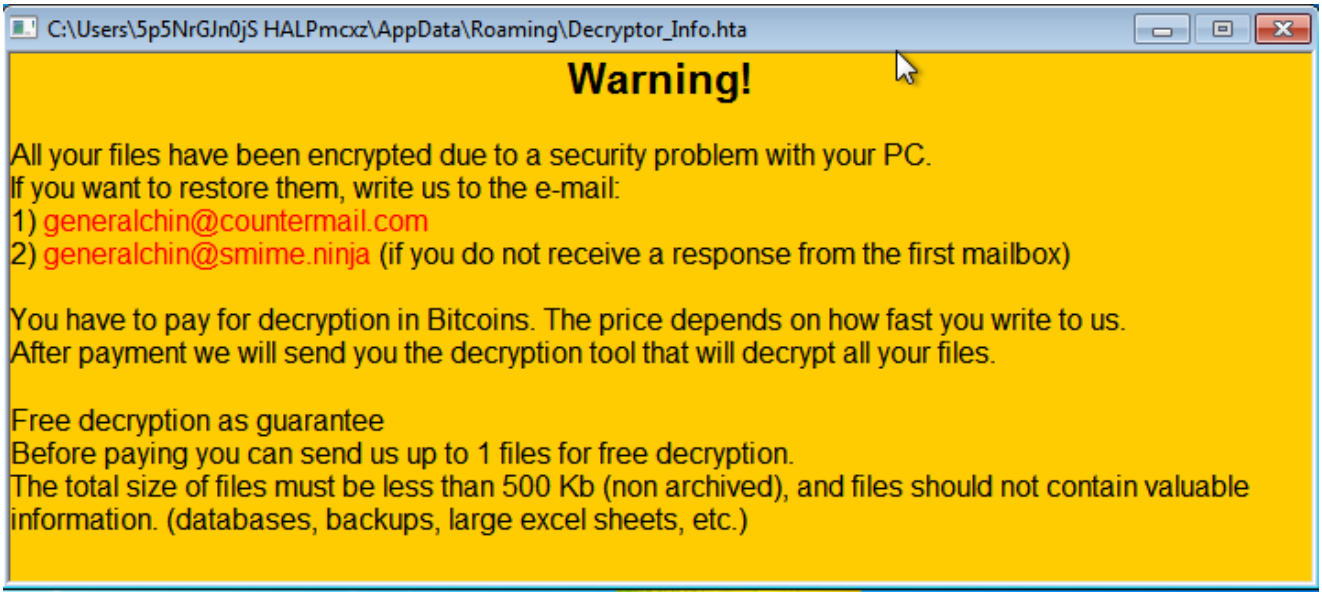


To inform the user about the infection, the text file “ReadMe_Decryptor.txt” is dropped in various directories. Furthermore, another ransom note (“Decryptor_Info.hta”) is dropped in %AppData% and shown to the user.

```
All your files have been encrypted due to a security problem with your PC. If you want
to restore them, write us to the e-mail:
1)generalchin@countermail.com
2)generalchin@smime.ninja (if you do not receive a response from the first mailbox)

You have to pay for decryption in Bitcoins. The price depends on how fast you write to us.
After payment we will send you the decryption tool that will decrypt all your files.

Free decryption as guarantee
Before paying you can send us up to 1 files for free decryption.
The total size of files must be less than 500 Kb (non archived), and files should not
contain valuable information. (databases,backups, large excel sheets, etc.)
```



SHA256: 8af0d99cef6fb1d040083ff8934f9a7ce01f358ca796b3c60087a2ebf6335c83