REvil ransomware has a new ‘Windows Safe Mode’ encryption mode

bleepingcomputer.com/news/security/revil-ransomware-has-a-new-windows-safe-mode-encryption-mode/

Lawrence Abrams

By
Lawrence Abrams

- March 19, 2021
- 07:15 AM
- 0

The REvil ransomware operation has added a new ability to encrypt files in Windows Safe Mode, likely to evade detection by security software and for greater success when encrypting files.

Windows Safe Mode is a special startup mode that allows users to run administrative and diagnostic tasks on the operating system. This mode only loads the bare minimum of software and drivers required for the operating system to work.

Furthermore, any programs installed in Windows that are configured to start automatically will not start in Safe Mode unless their autorun is configured a certain way.

One of the ways to create an autorun in Windows is to create entries under the following Registry keys:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

The 'Run' keys will launch a program every time you log in, while the 'RunOnce' key will launch a program only once and then remove the entry from the Registry.

For example, the following Registry key will automatically start the C:\Users\test\test.exe program when you log in to Windows.

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
"Startup"="C:\Users\test\test.exe"

However, the above autorun will not launch in Safe Mode unless you add an asterisk (*) to the beginning of the value name like the following:

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
"*Startup"="C:\Users\test\test.exe"

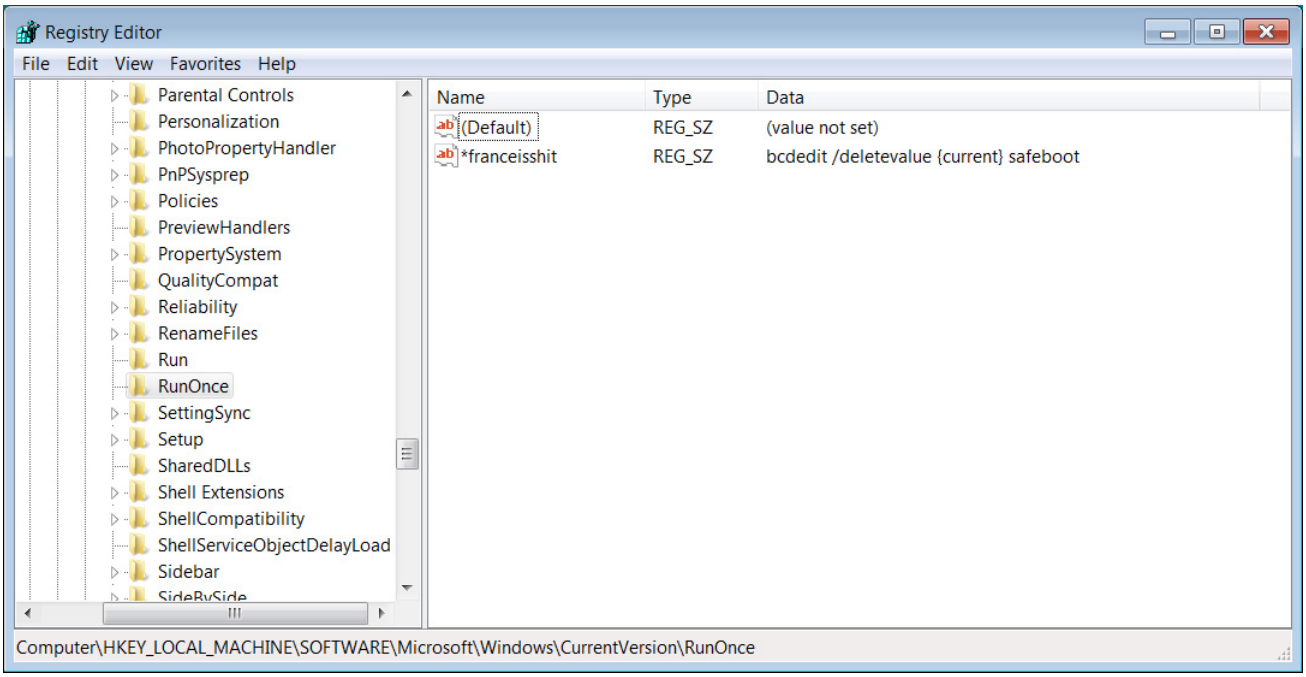
REvil now includes a 'Safe Mode' mode

In a new sample of the REvil ransomware discovered by MalwareHunterTeam, a new -smode command-line argument was added that forces the computer to reboot into Safe Mode before encrypting a device.

To do this, REvil will execute the following commands to force the computer to boot into Safe Mode with Networking when Windows next restarts.

```
bootcfg /raw /a /safeboot:network /id 1
bcdedit /set {current} safeboot network
```

It then creates a 'RunOnce' autorun called '*franceisshit' that executes ' `bcdedit /deletevalue {current} safeboot` ' after the users logs into Safe Mode.

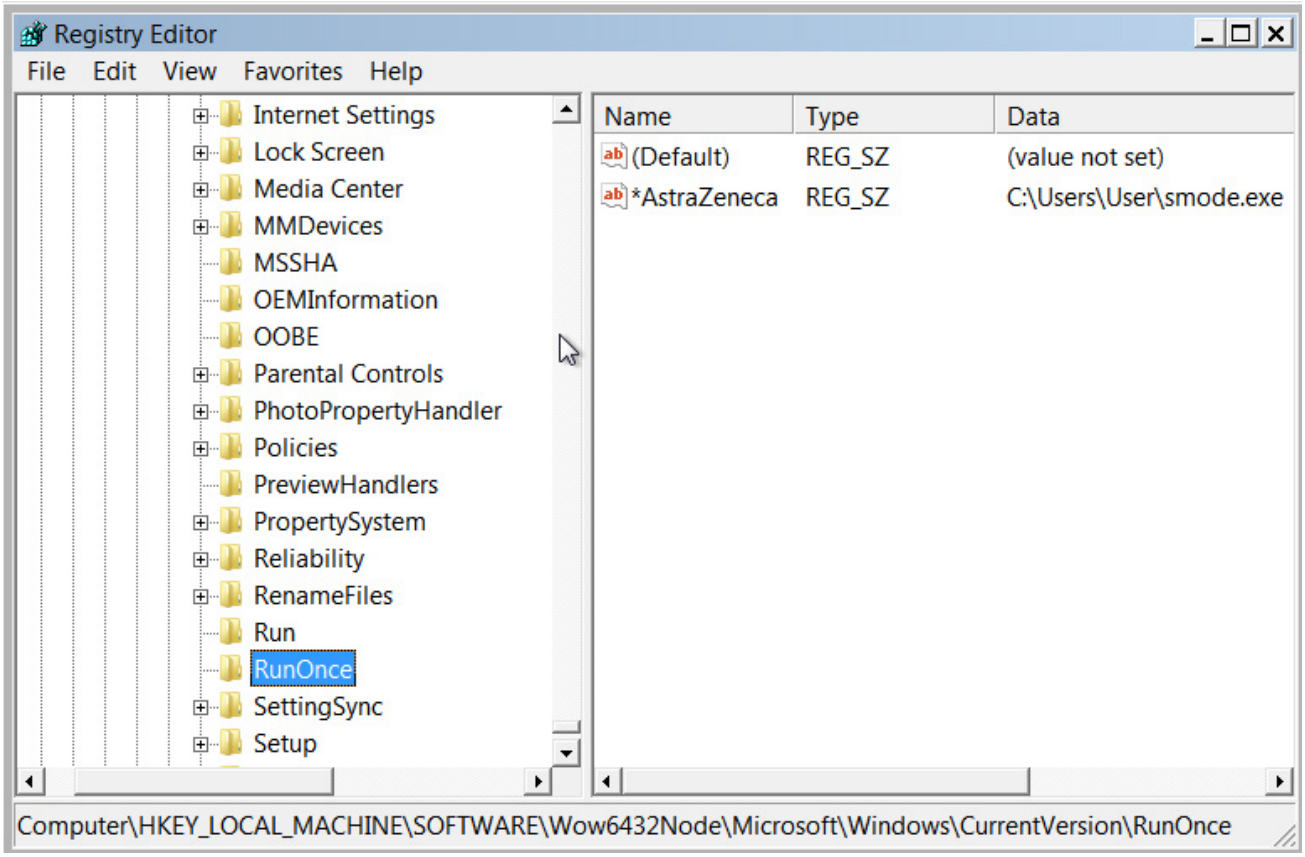


RunOnce entry to delete the

Finally, the ransomware performs a forced restart of Windows that cannot be interrupted by the user.

Right before the process exits, it will create an additional RunOnce autorun named 'AstraZeneca,' possibly about France's recent deliberations about using the vaccine.

This autorun will relaunch the REvil ransomware without the -smode argument when the next user logs in after the device is rebooted.



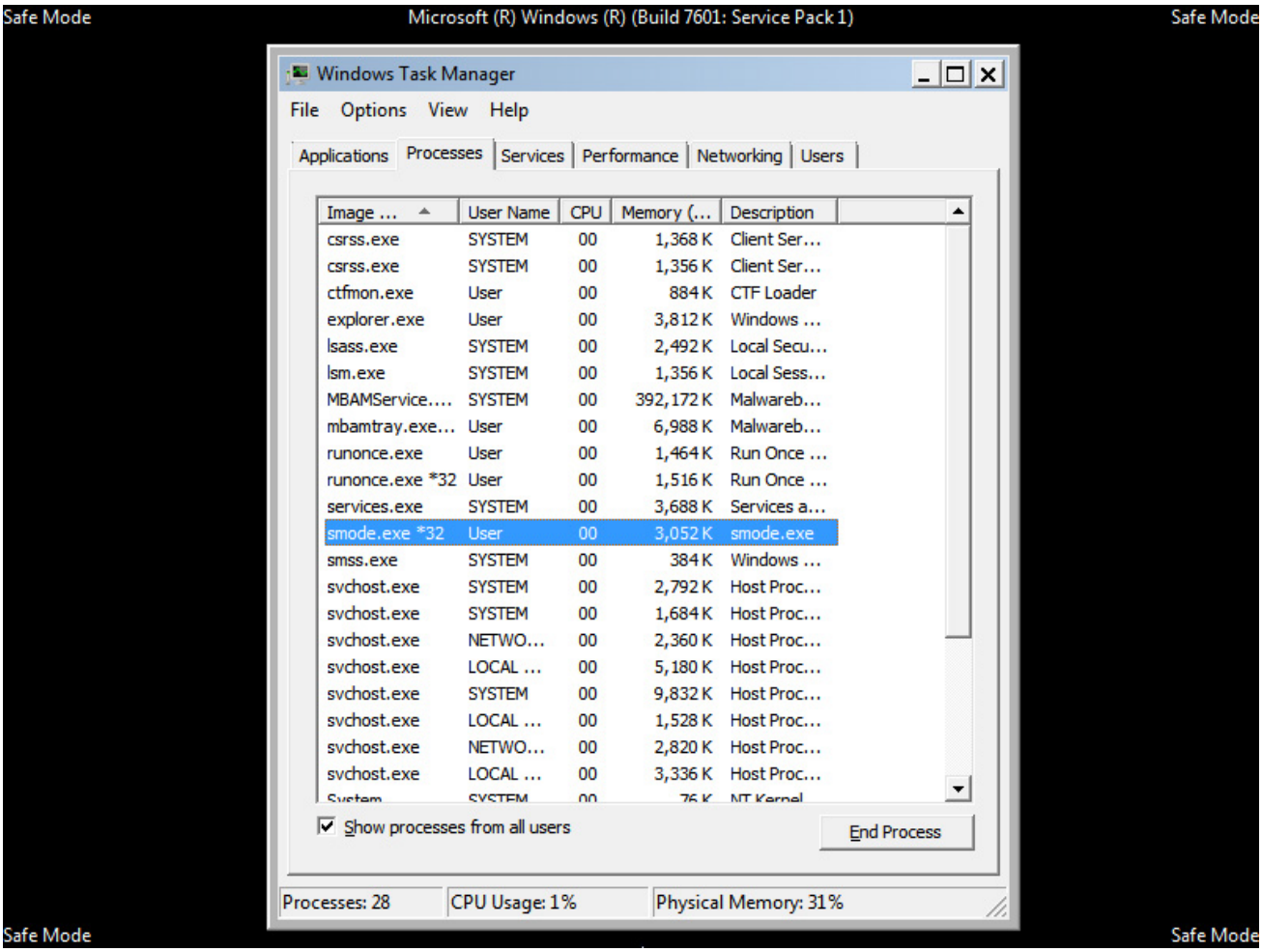
AstraZeneca autorun entry

It is important to remember that both of these 'RunOnce' entries will be executed after logging into Safe Mode and will automatically be deleted by Windows.

On reboot, the device will start up in Safe Mode With Networking, and the user will be prompted to log into Windows. Once they login, the REvil ransomware will be executed without the -smode argument so that it begins to encrypt the files on the device.

Windows will also run the '`bcdedit /deletevalue {current} safeboot`' command configured by the '*AstraZeneca' Registry key so that the machine can reboot into normal mode when the ransomware is finished.

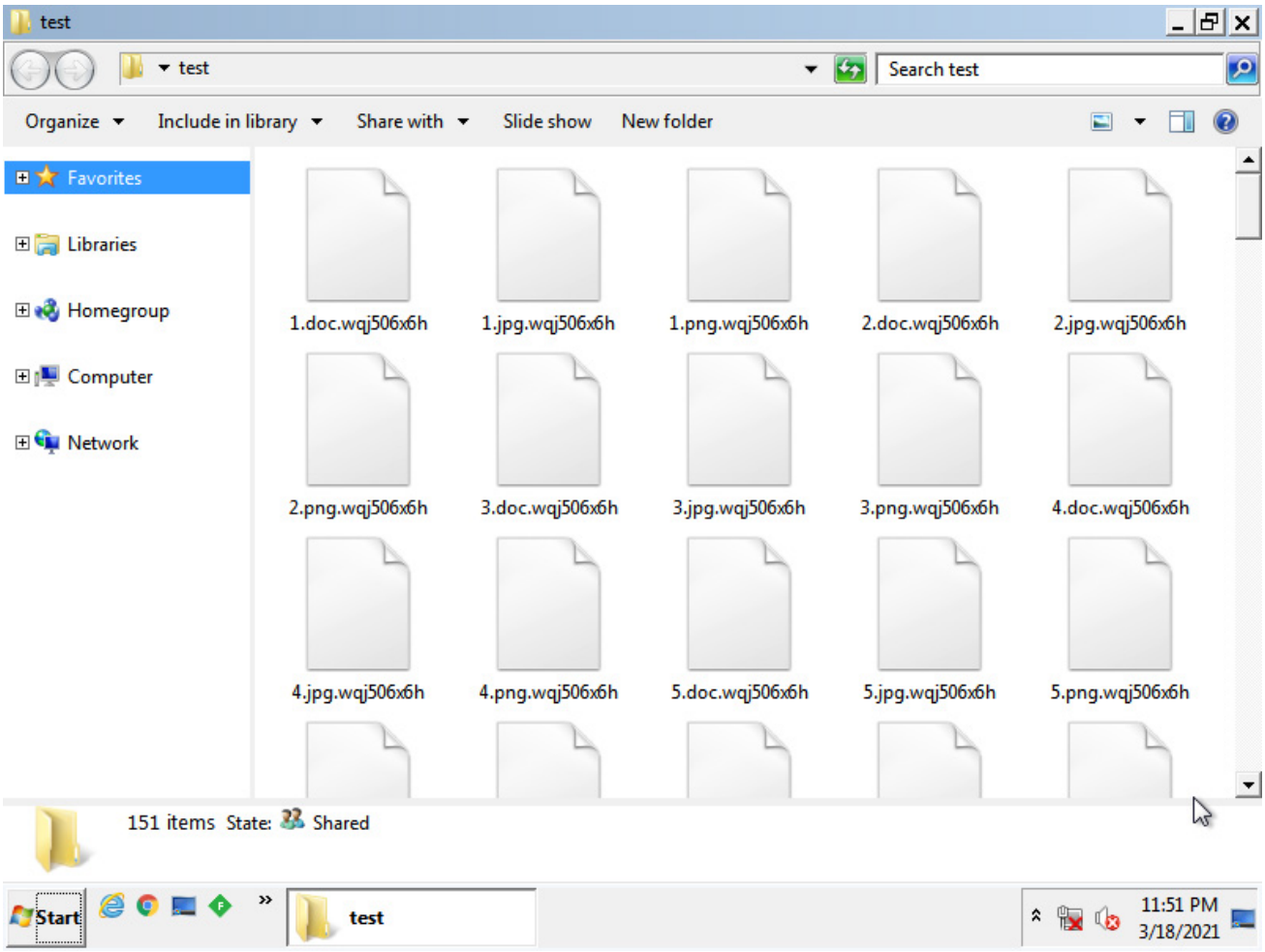
While REvil is encrypting files, the Safe Mode screen will be blank, but it is still possible to use Ctrl+Alt+Delete to launch the Windows Task Manager. From there, you can see the executable running, which in our test is named 'smode.exe,' as shown below.



REvil ransomware running in Safe Mode

While running, the ransomware will prevent users from launching any programs through Task Manager until it finishes encrypting the device.

Once the device is encrypted, it will allow the rest of the bootup sequence to proceed, and the desktop will be shown with a ransom note and encrypted files.



Device encrypted in Safe Mode

Unusual approach

REvil's new Safe Mode operation is a bit strange as it requires users to log in to the device after they restart into Safe Mode.

Furthermore, once they log into Safe Mode, they will be presented with a blank screen, and heavy thrashing of drives as the ransomware encrypts the device.

This behavior could cause users to become instantly suspicious and hibernate or shut down their computers to be safe.

For this reason, it is possible that the attackers are manually running the new Safe Mode command against specific computers, such as virtual machines or servers, that they want to encrypt without issues.

Regardless of the reasons, this is another new attack method that security professionals and Windows admins need to watch out for as ransomware gangs constantly evolve their tactics.

REvil is not the only operation to utilize Safe Mode for encrypting devices.

In 2019, another ransomware known as 'Snatch' also added the ability to encrypt a device in Safe Mode using a Windows service.

Related Articles:

Conti, REvil, LockBit ransomware bugs exploited to block encryption

The Week in Ransomware - May 6th 2022 - An evolving landscape

REvil ransomware returns: New malware sample confirms gang is back

New Black Basta ransomware springs into action with a dozen breaches

REvil's TOR sites come alive to redirect to new ransomware operation

- Encryption
- Ransomware
- REvil
- Safe Mode
- Sodinokibi
- Windows

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

You may also like: