Ryuk Ransomware Stops Encrypting Linux Folders

bleepingcomputer.com/news/security/ryuk-ransomware-stops-encrypting-linux-folders/

Lawrence Abrams

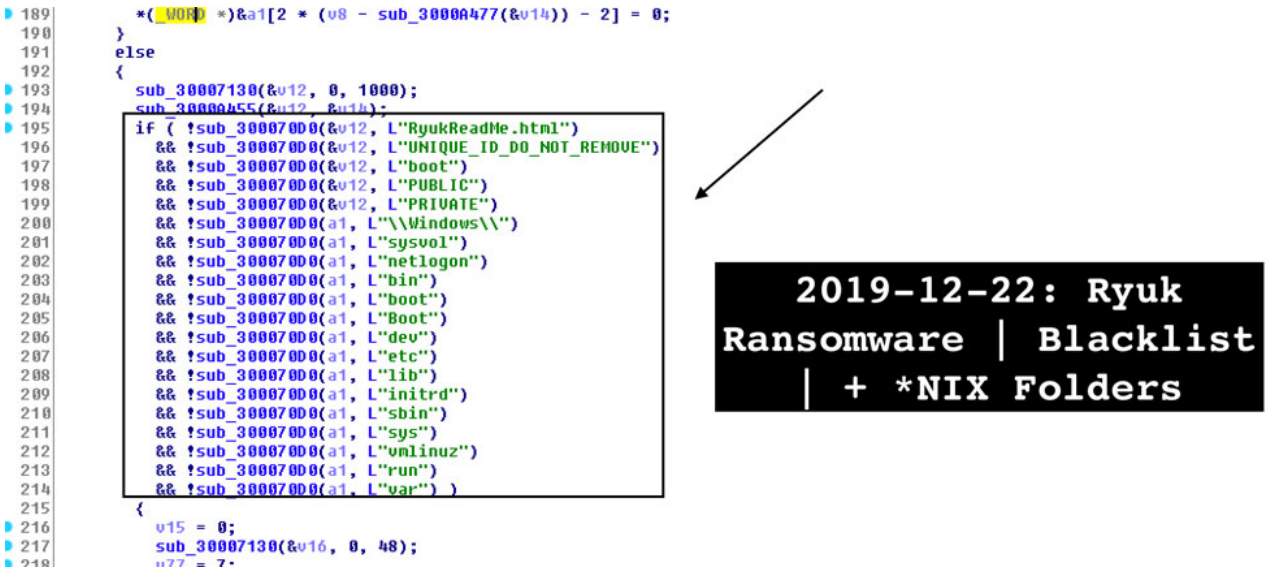
By
Lawrence Abrams

- December 26, 2019
- 12:15 PM
- 0

A new version of the Ryuk Ransomware was released that will purposely avoid encrypting folders commonly seen in *NIX operating systems.

After the City of New Orleans was infected by ransomware, BleepingComputer confirmed that the city was infected by the Ryuk Ransomware using an executable named v2.exe.

After analyzing the v2.exe sample, security researcher Vitali Kremez shared with BleepingComputer an interesting change in the ransomware; it would no longer encrypt folders that are associated with *NIX operating systems.



Blacklist *NIX Folders

The list of Ryuk blacklisted *NIX folders are:

```
bin
boot
Boot
dev
etc
lib
initrd
sbin
sys
vmlinuz
run
var
```

At first glance, it seems strange that a Windows malware would blacklist *NIX folders when encrypting files.

Even stranger, Kremez told us that he has been asked numerous times whether there was a Unix variant of Ryuk as data stored in these operating systems have been encrypted in Ryuk attacks.

A Linux/Unix variant of Ryuk does not exist, but Windows 10 does contain a feature called the Windows Subsystem for Linux (WSL) that allows you to install various Linux distributions directly in Windows. These installations utilize folders with the same blacklisted names as listed above.

With the rising popularity of WSL, the Ryuk actors likely encrypted a Windows machine at some point that also affected the *NIX system folders used by WSL. This would have caused these WSL installations to no longer work.

"They definitely have cases affecting WSL environments, which likely led them to blacklist NIX folders as they similarly do with the Windows ones. It is new to me and might explain why Ryuk and how Ryuk affects NIX machines via WSL," Kremez told BleepingComputer.

As the goal of most successful ransomware is to encrypt a victim's data, but not affect the functionality of the operating system, this change makes sense

With these folders being blacklisted, Ryuk eliminates an additional headache that they would need to deal with for a paying customer whose WSL installations are ruined.

Related Articles:

Microsoft adds support for WSL2 distros on Windows Server 2022

Fake Windows 10 updates infect you with Magniber ransomware

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

- Blacklist
- Ransomware
- Ryuk
- Unix
- Windows 10
- Windows Subsystem for Linux
- WSL

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: