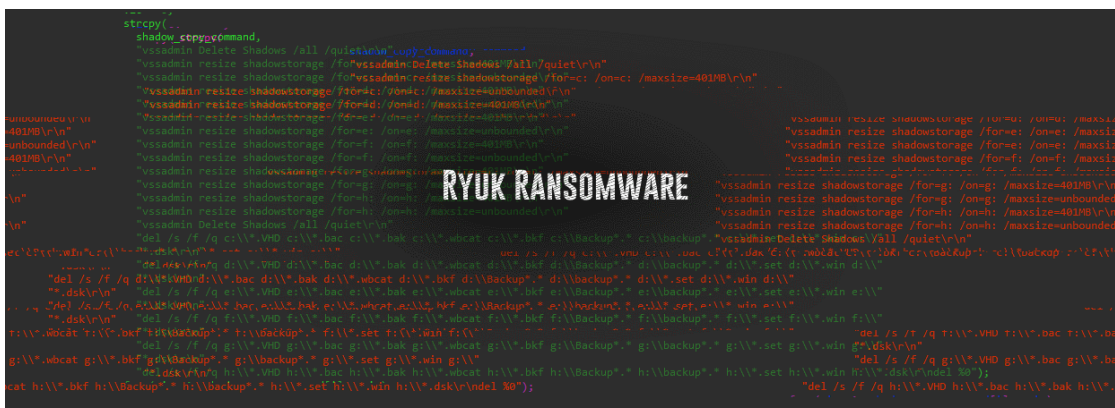


# Ryuk Ransomware Stops Encrypting Linux Folders

By Lawrence Abrams

Published: 2019-12-26 · Archived: 2026-04-05 12:52:00 UTC



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.



Visit Advertiser website [GO TO PAGE](#)

```

189 *(&v010) &{2 * (v0 - sub_30000477(&v14)) - 2} = 0;
190 }
191 else
192 {
193   sub_30007130(&v12, 0, 1000);
194   sub_30000455(&v12, &v14);
195   if ( !sub_30007000(&v12, L"RyukReadMe.html")
196       && !sub_30007000(&v12, L"UNIQUE_ID_DO_NOT_REMOVE")
197       && !sub_30007000(&v12, L"boot")
198       && !sub_30007000(&v12, L"PUBLIC")
199       && !sub_30007000(&v12, L"PRIVATE")
200       && !sub_30007000(a1, L"\\Windows\\")
201       && !sub_30007000(a1, L"sysvol")
202       && !sub_30007000(a1, L"netlogon")
203       && !sub_30007000(a1, L"bin")
204       && !sub_30007000(a1, L"boot")
205       && !sub_30007000(a1, L"boot")
206       && !sub_30007000(a1, L"dev")
207       && !sub_30007000(a1, L"etc")
208       && !sub_30007000(a1, L"lib")
209       && !sub_30007000(a1, L"initrd")
210       && !sub_30007000(a1, L"sbin")
211       && !sub_30007000(a1, L"sys")
212       && !sub_30007000(a1, L"vmlinuz")
213       && !sub_30007000(a1, L"run")
214       && !sub_30007000(a1, L"var") )
215   {
216     v15 = 0;
217     sub_30007130(&v16, 0, 48);
218     v17 = 7;

```

**2019-12-22: Ryuk Ransomware | Blacklist + \*NIX Folders**

**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.



### [Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

---

Source: <https://www.bleepingcomputer.com/news/security/ryuk-ransomware-stops-encrypting-linux-folders/>