Reynolds: Defense Evasion Capability Embedded in Ransomware Payload

By About the Author

Archived: 2026-04-05 18:58:01 UTC

Update, February 9 2026: An earlier version of this blog stated that the ransomware payload used was Black Basta. This attribution was based on similarities in TTPs. After further analysis, we've concluded the payload used was Reynolds, an emergent ransomware family.

A recent Reynolds ransomware campaign was notable because the ransomware contained a bring-your-own-vulnerable-driver (BYOVD) defense evasion component embedded within the ransomware payload itself.

Normally the BYOVD defense evasion component of an attack would involve a distinct tool that would be deployed on the system prior to the ransomware payload in order to disable security software. However, in this attack, the vulnerable driver (an NsecSoft NSecKrnl driver) was bundled with the ransomware itself.

BYOVD is by far the most frequently used technique for defense impairment these days. Generally, attackers will deploy a signed vulnerable driver to the target network, which they then exploit to elevate privileges and disable security software. Since the vulnerable drivers operate with kernel-mode access, they can be used to terminate processes, making them an effective tool for disrupting security measures. In most cases, the vulnerable driver is deployed along with a malicious executable, which will use the driver to issue commands.

While bundling a defense evasion component within the ransomware itself isn’t entirely novel, it is quite unusual and not what we typically see ransomware actors doing today. It was previously seen in a Ryuk ransomware attack in 2020, as well as an attack in which a little-known ransomware called Obscura was deployed in 2025.

Recent activity

The ransomware payload drops a vulnerable NsecSoft NSecKrnl driver and tries to create an NSecKrnl service. This driver is then exploited to attempt to kill processes. It targets the following processes:

"Sophos UI.exe"

"SEDService.exe"

"SophosHealth.exe"

"SophosFS.exe"

"SSPService.exe"

"SophosFileScanner.exe"

"McsAgent.exe"

"McsClient.exe"

"SophosLiveQueryService.exe"

"SophosNetFilter.exe"

"SophosNtpService.exe"

"hmpalert.exe"

"Sophos.Encryption.BitLockerService.exe"

"SophosOsquery.exe"

"ccSvcHst.exe"

"SymCorpUI.exe"

"SISIPSService.exe"

"SISIDSService.exe"

"SmcGui.exe"

"sisipsutil.exe"

"sepWscSvc64.exe"

"MsMpEng.exe"

"CSFalconService.exe"

"cydump.exe"

"cyreport.exe"

"cyrestart.exe"

"cyrprtui.exe"

"cyserver.exe"

"cytool.exe"

"cytray.exe"

"cyuserserver.exe"

"CyveraConsole.exe"

"tlaworker.exe"

"ekrn.exe"

"eguiProxy.exe\t"

"egui.exe"

"aswEngSrv.exe"

"aswidsagent.exe"

"AvastUI.exe"

"ccSvcHst.exe"

The ransomware payload appends the ".locked" extension to files it encrypts.

The NSecKrnl driver is a Windows kernel-mode driver with a known critical security vulnerability (CVE-2025-68947), which means that it fails to verify if a user has sufficient permissions before executing commands. This allows a local, authenticated attacker to terminate processes owned by other users, including SYSTEM and Protected Processes, by issuing crafted Input/Output Control (IOCTL) requests to the driver.

Also of note in this attack campaign was the presence of a suspicious side-loaded loader on the target's network several weeks prior to the ransomware being deployed. It is not certain if this was linked to the subsequent ransomware activity, but if it was it points to a long dwell time for the attackers.

The GotoHTTP remote access tool was also found on some machines on the target network the day after the ransomware was deployed. It is relatively unusual to see attacker activity on the victim network post ransomware deployment. This could be unrelated to the ransomware activity, but it could also point to an attempt by the attackers to maintain persistent access to the network, even after the ransomware was deployed.

Defense evasion: A key step in ransomware attacks

The impairment of defenses, usually by attempting to disable antivirus (AV) or endpoint detection and response (EDR) products, is a key part of ransomware attacks in 2026. Ransomware actors have added this step to their playbooks in a bid to evade detection prior to the deployment of a file-encrypting payload.

The use of impairment techniques and tools has risen markedly among ransomware actors over the past two years, most likely in response to vendors improving their ability to identify patterns of malicious activity that occur prior to ransomware deployment.

By far the most frequently used technique for defense impairment is the BYOVD technique. Attackers will generally deploy a signed vulnerable driver to the target network, which they then exploit to elevate privileges and disable security software. These drivers are considered "vulnerable" as it should not be possible to leverage them in this way. A correctly written driver will contain safeguards to ensure they only respond to legitimate requests

from authorized software. However, when these drivers fall into the wrong hands, they effectively become tools for privilege escalation.

BYOVD is popular with attackers due to its effectiveness and reliance on legitimate, signed files, which are less likely to raise red flags. A wide range of drivers have been used in such attacks, with anti-rootkit drivers developed by security vendors being among the most commonly exploited. Popular BYOVD tools frequently used by attackers include:

- **TrueSightKiller:** A publicly available tool that leverages a vulnerable driver named truesight.sys.
- **Gmer:** A rootkit scanner that can be used to kill processes.
- **Warp AVKiller:** A variant of a Go-based information-stealing threat called Warp Stealer, which appears to be just used to bypass security products. It uses a vulnerable Avira anti-rootkit driver to disable security products.
- **GhostDriver:** A publicly available tool that leverages vulnerable drivers to kill processes.
- **Poortry (aka BurntCigar):** A malicious driver documented by Sophos that is frequently employed alongside a loader known as Stonestop. Unlike many drivers, Poortry may have been developed by attackers who then succeeded in getting it signed.
- **AuKill:** A tool documented by Sophos that uses an outdated version of the driver used by the Microsoft utility Process Explorer to disable EDR processes

Attackers do also leverage living-off-the-land techniques, using common Windows utilities, to disable security software, particularly Windows Defender. However, there is no doubt that BYOVD is the most common defense evasion tool we see used by ransomware actors today.

Will this tactic be adopted by more ransomware actors?

The question raised by this recent activity is whether we are likely to see this tactic be adopted by more ransomware actors and what advantages it might bring for them.

The advantages of wrapping the defense evasion capability in with the ransomware payload, and the reason ransomware actors might do this, may include the fact that packaging the defense evasion binary and the ransomware payload together is “quieter”, with no separate external file dropped on the victim network. It also may speed up the attack - if there is no gap between the defense evasion tool being deployed and the ransomware being dropped, there is no opportunity for defenders to stop the attack. In other scenarios, if defenders saw a suspicious driver being dropped on a system, they may have time to stop the attack before the ransomware is deployed.

Embedding more capabilities into the ransomware payload itself may also help act as a unique selling point for ransomware developers who are attempting to attract affiliates. Having additional capabilities bundled with the ransomware payload may make ransomware attacks easier to carry out, as they would require less steps, potentially making such a payload more attractive to affiliates.

It will be interesting to see if more ransomware families begin embedding additional capabilities, such as defense evasion and others, in their ransomware payloads in the future.

Protection/Mitigation

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise

If an IOC is malicious and the file available to us, Symantec Endpoint products will detect and block that file.

5213706ae67a7bf9fa2c0ea5800a4c358b0eaf3fe8481be13422d57a0f192379 – Suspicious file

e09686fde44ae5a804d9546105ebf5d2832917df25d6888aefa36a1769fe4eb4 – Webshell – xxxxx.aspx

bf6686858109d695ccdabce78c873d07fa740f025c45241b0122cecbdd76b54e – Loader – vspmsg.dll

6bd8a0291b268d32422139387864f15924e1db05dbef8cc75a6677f8263fa11d – Reynolds ransomware – wxt4e.exe, wxt4e.txt

206f27ae820783b7755bca89f83a0fe096dbb510018dd65b63fc80bd20c03261 – Vulnerable NsecSoft NSecKrnl Driver – 402.sys

230b84398e873938bbcc7e4a1a358bde4345385d58eb45c1726cee22028026e9 - GotoHTTP - gotohttp.exe

---