

GodDamn Ransomware: Latest Beast Rebrand Uses Malicious Driver to Disable Defenses

By About the Author

Archived: 2026-07-28 02:00:51 UTC

Analysis of a recent GodDamn ransomware attack indicates that this seemingly new ransomware is in fact the latest rebrand of the Beast ransomware, which in itself was a rebrand of the Monster ransomware, which was [first seen in 2022](#). The Symantec Threat Hunter Team tracks the developer behind these ransomware families as Hyadina.

The GodDamn ransomware, which our analysts found has significant code overlap with Beast, was documented as being first seen on May 21, 2026, with the attack we investigated taking place around two weeks later, in early June. During this attack, the threat actors leveraged AnyDesk for remote access, used a NirSoft-based credential harvesting toolkit comprising multiple different hacking tools and credential stealers, and used a user-mode defense evasion tool disguised as a Symantec product and the PoisonX kernel driver to disable endpoint defenses before deploying the ransomware.

The PoisonX kernel driver was [first documented](#) as being used to disable security software in early 2026, when it was used by an attacker to kill the CrowdStrike Falcon service by sending a crafted IOCTL to the driver's undocumented interface. The driver is signed by Microsoft and so to the system it appears to be a legitimate driver. This means it can be used to stop or disable security software at the kernel level. We commonly call this type of defense evasion a bring-your-own-vulnerable-driver (BYOVD) attack, where a vulnerability in a legitimate driver is exploited to shut down defenses. However, the PoisonX driver seems to be slightly more unusual, in that it appears to be a malicious driver that its developers succeeded in getting signed by Microsoft, and it is now being used by ransomware attackers.

In some GodDamn ransomware attacks, the encrypted files are renamed with the .God8Damn file extension. However, in the incident investigated by Symantec, encrypted files were renamed with the name of the victim organization as the file extension, which is somewhat unusual.

Attack chain

The initial infection vector used by the attackers in this incident is unknown. The earliest observed malicious activity occurred on May 29, 2026, when AnyDesk appeared on Computer 1 in a location inconsistent with a standard installation.

```
csidl_profile\music\anydesk.exe
```

Placing AnyDesk under the user Music folder rather than a standard installation directory is consistent with manual delivery by an attacker who had already obtained access to the host by an earlier means. Shortly after

execution, the process began making outbound connections to AnyDesk relay infrastructure, reaching addresses including 15.235.230[.]188, 185.229.191[.]39, 141.95.145[.]210, and 162.19.171[.]150.

On May 30, 2026, the attackers deployed two defensive-evasion capabilities on a second host within the same enterprise network. The first was a defense evasion tool with the filename `symantec.exe`, staged in the user Music folder and designed to impersonate a Symantec product.

```
csidl_profile\music\symantec.exe
```

The file (SHA-256: b29f91a440527fb621d106a2048f6379fff3263c60aeda9c82ff8c1d5ae880a8) dropped a signed kernel driver (PoisonX) into the system driver store.

```
csidl_system\drivers\g11.sys
```

PoisonX (SHA-256: 2d91a78e739891c9854c254f5b2a6b84c0e167dfa253466cbccd2cdd1c20145d) carries a signature attributed to “Microsoft Windows Hardware Compatibility Publisher”. It can terminate security-product processes and remove user-mode API hooks, effectively disabling endpoint visibility on the host.

On the same host, the attackers staged a comprehensive credential-harvesting toolkit in a subdirectory of the user profile.

```
csidl_profile\music\mimik\pass\
```

The toolkit comprised 14 tools covering the full breadth of credential storage on a Windows host: Mimikatz (`mimik.exe`), `WebBrowserPassView`, `ChromePass`, `PasswordFox`, `MessengerPass`, `VNCPassView`, `MailPassView`, `SniffPass`, `OperaPassView`, `CredentialsFileView`, `WirelessKeyView`, `ExtPassword`, `PSTPassword`, and `NetPass`. Together they can recover credentials from the most common browsers, Windows Credential Manager, cached domain credentials, VNC sessions, email clients, Wi-Fi profiles, and live network traffic. `Netscan.exe`, which can map the network, was also placed in the staging directory, likely to assist in mapping reachable hosts.

There was then a gap in activity by the attackers of approximately two days. On June 1, 2026, lateral movement began across the enterprise network. All malicious commands during this phase shared a process lineage running through `psexesvc.exe`, `services.exe`, and `wininit.exe`, confirming that PsExec was being used to push commands to remote targets. The session opened with basic network and process reconnaissance on Computer 2.

```
ipconfig
```

```
tasklist
```

The attackers then launched the previously mentioned defense evasion tool and disabled Windows Defender real-time monitoring.

```
cmd /c "start /b D:\symantec.exe"
```

```
powershell -Command "Set-MpPreference -DisableRealtimeMonitoring $true"
```

To reach an adjacent host, the attackers mounted an administrative share using stolen credentials.

```
net use \\192.168.0[.]25\c$ /user:[REMOVED] [REMOVED]
```

The attackers then established AnyDesk on each PsExec-reached host in a configuration suited to unattended access. A dedicated configuration directory was created on the D: drive, and a configuration file was written to set `ad.security.interactive_access=2`, which suppresses AnyDesk's standard interactive consent prompt and allows incoming connections without requiring the local user to approve them. A remote-access password was piped directly to AnyDesk's standard input to set the client credential.

```
powershell -Command "New-Item -ItemType Directory -Force -Path 'CSIDL_DRIVE_FIXED\ad_data'; Set-Content -Path 'CSIDL_DRIVE_FIXED\ad_data\system.conf' -Value 'ad.security.interactive_access=2'; Start-Sleep -Seconds 1; echo '[REMOVED]' | & 'CSIDL_DRIVE_FIXED\anydesk.exe' [REMOVED]; & 'CSIDL_DRIVE_FIXED\anydesk.exe' --get-id"
```

In subsequent runs across additional hosts, the access password was updated, suggesting the operators were refining their deployment script as they propagated the installation.

```
powershell -Command "Add-Content -Path 'CSIDL_DRIVE_FIXED\ad_data\system.conf' -Value 'ad.security.interactive_access=2'; echo '[REMOVED]' | & 'CSIDL_DRIVE_FIXED\anydesk.exe' [REMOVED]"
```

The `--get-id` flag that followed each AnyDesk launch retrieved the AnyDesk client identifier for the newly configured instance, which the attackers would need to initiate sessions back to each host.

To ensure AnyDesk survived a reboot, the attackers registered it as two separate auto-start Windows services, both pointing to the same binary and configuration directory on the D: drive.

```
sc create AnyDeskService binPath= "CSIDL_DRIVE_FIXED\anydesk.exe --service --conf-dir=d:\ad_data --data-dir=d:\ad_data" start= auto DisplayName= "AnyDesk Service"
```

```
sc create AnyDesk_D binPath= "CSIDL_DRIVE_FIXED\anydesk.exe --service --conf-dir=d:\ad_data --data-dir=d:\ad_data" start= auto DisplayName= "AnyDesk D-Drive Service"
```

```
net start AnyDeskService
```

On some targets, the entire AnyDesk setup was handled by a PowerShell script pre-staged on the system drive, suggesting the attackers had prepared a reusable installer for the rollout.

```
"powershell.exe" -ExecutionPolicy Bypass -File CSIDL_SYSTEM_DRIVE\apps\install_ad.ps1
```

AnyDesk was also installed to the standard 32-bit Program Files location with start-with-Windows persistence enabled, providing a fallback access point alongside the custom D:-drive installation.

```
CSIDL_DRIVE_FIXED\anydesk.exe --install "CSIDL_PROGRAM_FILESX86\anydesk" --start-with-win --silent --accept-3rd-party-licenses
```

After completing the AnyDesk setup on each host, the attackers terminated the running AnyDesk process, waited briefly, then rebooted the machine.

```
taskkill /f /im anydesk.exe
```

```
timeout /t 3
```

```
shutdown -r -t 0
```

By the end of June 2, this deployment sequence had been repeated across at least 10 hosts within the targeted organization.

On June 3, 2026, the GodDamn ransomware was first detected on a separate network segment associated with a distinct organizational unit. The binary, named `encrypter-windows-gui-x86.exe`, appeared in user profile directories, typically under Downloads or Music folders.

```
csidl_profile\downloads\encrypter-windows-gui-x86.exe
```

```
csidl_profile\music\encrypter-windows-gui-x86.exe
```

The four-day gap between the first observed pre-ransomware activity on May 29 and the first ransomware detections on June 3 is consistent with a dwell period during which the attackers may have staged payloads, exfiltrated data, or conducted additional reconnaissance before triggering the encryption phase.

Hyadina

Hyadina first emerged in March 2022, when it was seen deploying its Monster ransomware variant. Monster was primarily written in Delphi and targeted 32-bit Windows operating systems. It avoided targeting machines that appeared to be located in the Commonwealth of Independent States (CIS). Hyadina appeared to operate Monster as a typical ransomware-as-a-service operation, working with affiliates to carry out attacks.

One of the hallmarks of a November 2022 Monster attack documented by Symantec was the use by the attackers of a password protected self-extracting archive containing the Mimikatz credential-dumping tool and a large number of password-harvesting tools developed by NirSoft, much like the tools we saw used in this recent GodDamn attack, with many of the same tools used, including AnyDesk and NetScan also.

Hyadina then rebranded its ransomware as Beast in June 2024. The attackers leveraged a similar toolset as used in earlier Monster attacks, however, the update also made a number of fixes and changes that allowed for greater customization and control by the attacker, as well as enhancing the performance of the encryption process. Another notable change to the capabilities of Beast was the addition of support for targeting Linux and VMware ESXi operating systems instead of just Windows-based computers. Like before, the ransomware made extensive use of NirSoft tools and avoided targets in multiple countries of the CIS. However, support for various languages, including Chinese, showed that the threat actor was casting its net wide open.

In activity investigated by Symantec in June 2025, we observed Beast ransomware attackers using a custom tool for finding valid admin credentials, as well as some other tools that were not used previously alongside the ransomware. These included the Gmer rootkit scanner, which was used to kill processes, Defender Control to disable Windows Defender, and the IObit Unlocker to help with unlocking locked files and folders.

GodDamn appears to be the latest ransomware iteration from this group, which continues to develop its stealth and defense evasion capabilities. GodDamn's use of the [relatively newly discovered](#) PoisonX malicious driver

component represents an escalation in defensive evasion capability by this group, indicating that Hyadina is continuing to actively develop its ransomware and its capabilities.

Protection/Mitigation

For the latest protection updates, please visit the [Symantec Protection Bulletin](#).

Indicators of Compromise (IOCs)

File indicators

141b2190f51397dbd0dfde0e3904b264c91b6f81febc823ff0c33da980b69944 – PsExec – psxessvc.exe
17fb52476016677db5a93505c4a1c356984bc1f6a4456870f920ac90a7846180 – Netpass – netpass64.exe
19bab15a34d5ad838ccf4d187eb40379c335fa56446d0f9621865b2767d4ac7d – WirelessKeyView – wirelesskeyview64.exe
2d91a78e739891c9854c254f5b2a6b84c0e167dfa253466cbccd2cdd1c20145d – PoisonX Driver – g11.sys
31eb1de7e840a342fd468e558e5ab627bcb4c542a8fe01aec4d5ba01d539a0fc – Mimikatz – mimik.exe
35296e7a34688ca3e3159bcd9f2b4d60ba4173a2369aca531bb7bc959f68ed9c – CredentialsFileView – credentialsfileview64.exe
45126297c07c6ef56b51440cd0dc30acf7b3b938e2e9e656334886fe2f81f220 – AnyDesk – anydesk.exe
5be325905df8aab7089ab2348d89343f55a2f88dadd75de8f382e8fa026451bd – Mailpassview – mailpv.exe
5c4c98d774eb100f9a89ae4e984c27a4f532e58c7cf8c87046dc87db5a065404 – ChromePass – chromepass.exe
5e85446910e732111ca9ac90f9ed8b1dee13c3314d2c5117dcf672994ce73bd6 – PstPassword – pstpassword.exe
7a313840d25adf94c7bf1d17393f5b991ba8baf50b8cacb7ce0420189c177e26 – MessengerPass – mspass.exe
816d7616238958dfe0bb811a063eb3102efd82eff14408f5cab4cb5258bfd019 – VNCPassView – vncpassview.exe
8e4b218bdbd8e098fff749fe5e5bbf00275d21f398b34216a573224e192094b8 – OperaPassview – operapassview.exe
8ff1c1967841a595d996a649c8134b7a5970dcf94624b237d1b089e7c6266167 – Webbrowserpassview – webbrowserpassview.exe
9fae3f15900e13ec3860a109555ecd33ca43d38907c63438c50a2d6d91bfee1d – Netscan – netscan.exe
b29f91a440527fb621d106a2048f6379fff3263c60aeda9c82ff8c1d5ae880a8 - Defense evasion tool – Symantec.exe
c92580318be4effdb37aa67145748826f6a9e285bc2426410dc280e61e3c7620 – SniffPass – sniffpass64.exe
e097f3b445b63b07afacde8d6a67f0be654dd51e228a3610fb0710a1f7e29a69 - GodDamn ransomware – encrypter-windows-gui-x86.exe
ece33e4b7e2d26eeca8ad9db4439f9801a7a77e33261116156738b1b0316046 – Extpassword – extpassword.exe
faca9e856c369b63d6698c74b1d59b062a9a8d9fe84b8f753c299c9961026395 – PasswordFox – passwordfox64.exe

Source: <https://www.security.com/threat-intelligence/goddamn-ransomware-beast-rebrand>