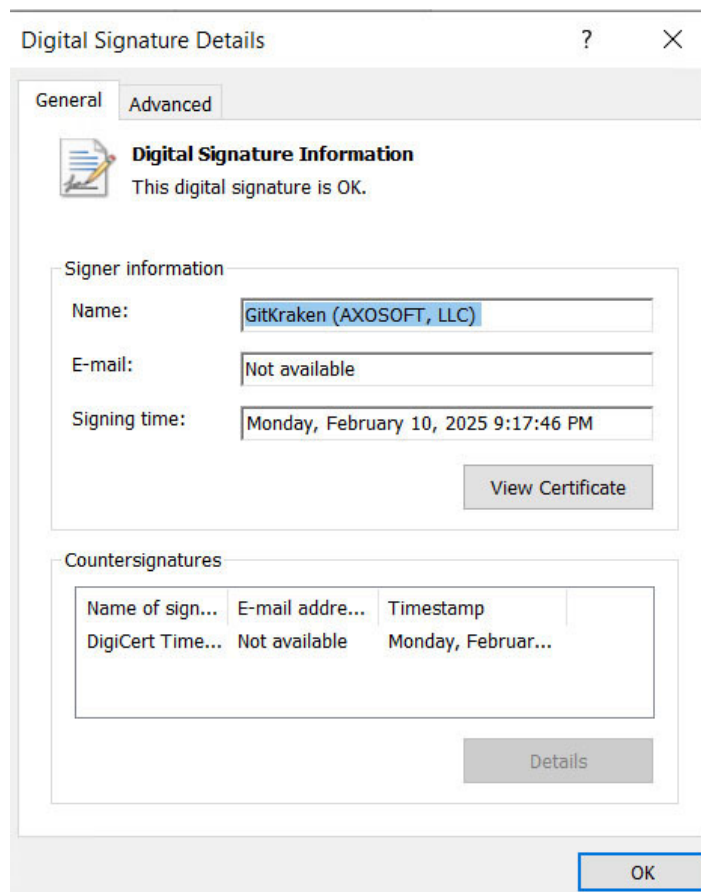


Hiding in Plain Sight: Multi-Actor ahost.exe Attacks

trellix.com/en-au/blogs/research/hiding-in-plain-sight-multi-actor-ahost-exe-attacks



Blogs

The latest cybersecurity trends, best practices, security vulnerabilities, and more

Hiding in Plain Sight: Deconstructing the Multi-Actor DLL Sideload Campaign abusing ahost.exe

By [Mallikarjun Wali](#) and [Mohideen Abdul Khader](#) · January 14, 2026

Executive summary

The Trellix Advanced Research Center has uncovered an active malware campaign that exploits a DLL sideloading vulnerability within the legitimate **ahost.exe** utility. This utility is a component of the open-source [c-ares](#) library (used for asynchronous DNS lookups) and is commonly bundled within Git for Windows installations, including those embedded in developer tools like GitKraken or GitHub Desktop. Attackers achieve evasion by pairing a malicious libcares-2.dll with any signed version of the legitimate ahost.exe (which they often rename) to execute their code. This DLL sideloading technique allows the malware to bypass traditional signature-based security defenses.

The campaign primarily delivers commodity malware, including infostealers (AgentTesla, FormBook, Lumma Stealer, Vidar, CryptBot) and Remote Access Trojans, aka RATs (Remcos, QuasarRAT, DCRat, XWorm), disguised as business documents. Targets are typically employees in finance, procurement, supply chain, and administration roles within commercial and industrial sectors such as oil and gas and import/export. The attackers use localized filenames in multiple languages like Arabic, Spanish, Portuguese, Farsi, and English, indicating a global and tailored approach.

DLL sideloading enables the malware to evade legacy security solutions that rely solely on signature-based detection and static indicators of compromise. The exploitation of trusted applications poses significant risk to target organizations that lack advanced [endpoint detection and response](#) (EDR) or [extended detection and response](#) (XDR) solutions. This campaign highlights the critical need for organizations to implement advanced EDR solutions, robust application control policies, and endpoint hardening. They should also maintain up-to-date [threat intelligence](#) to detect and respond to these attacks effectively.

Exploitation of legitimate ahost.exe utility

The core of this campaign lies in the abuse of a legitimate utility and for additional advantage attackers are inclined to use the signed version of this utility, for instance this file (MD5 Hash: fd3c8166e7fbbb64d12c1170b8f4bacf) is signed by GitKraken and distributed with the Gitkraken Desktop application. This utility, designed to retrieve DNS records, relies on libcares-2.dll, a Windows DLL from the c-ares DNS resolver library. The key vulnerability is that the design of ahost.exe is vulnerable to DLL side-loading or search order hijacking. An attacker can exploit this vulnerability by placing a malicious DLL, named libcares-2.dll, in the same directory as ahost.exe, thereby gaining unauthorized access.

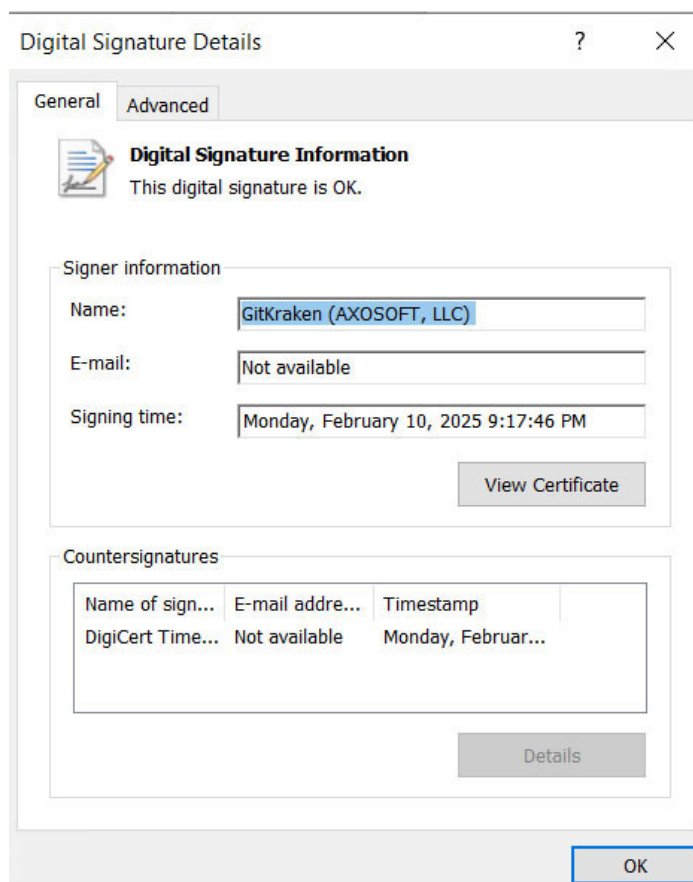


Figure 1: A valid digital signature for the “ahost.exe” utility lures the victim to run this executable, which sideloads a maliciously crafted “libcares-2.dll” library

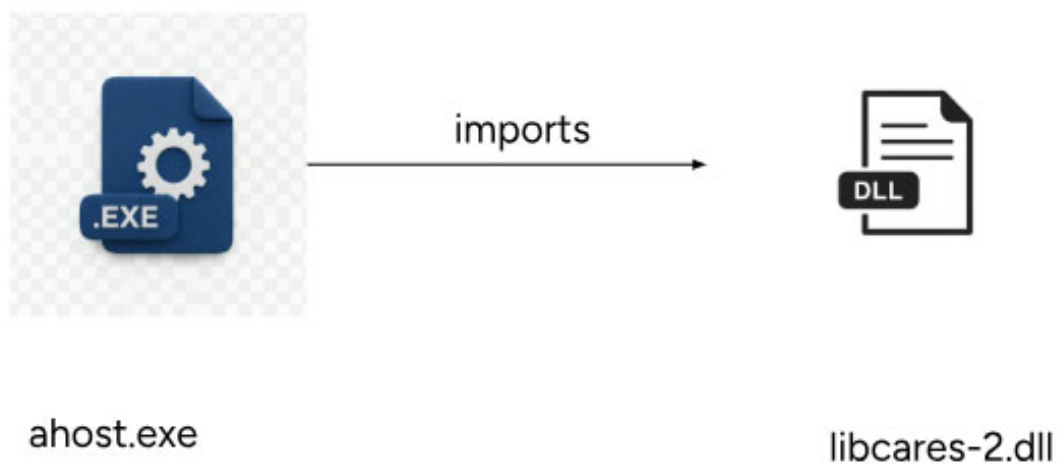


Figure 2: ahost.exe imports libcares-2.dll

This tactic is effective because it leverages the inherent trust users place in signed and legitimate applications, making detection more challenging.

What is DLL sideloading?

DLL sideloading is a technique used by attackers especially by advanced persistent threat (APT) groups where an attacker exploits the way Windows applications load DLLs. This can allow malicious DLLs to be loaded instead of legitimate ones, often to execute code in a trusted application's context, effectively evading detection mechanisms.

Sideloading Flow Chart:

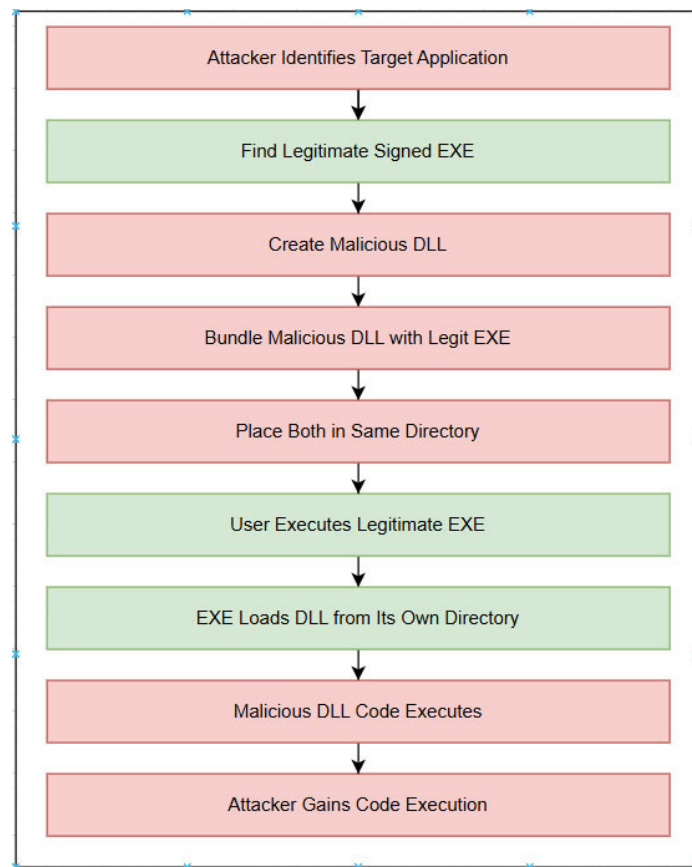


Figure 3: Attack flow

1. Attacker finds a vulnerable executable (preferably a signed and known executable that loads DLLs from its directory)
2. Creates a malicious DLL with the same name as a DLL the application tries to load
3. Places both the trusted executable and the malicious DLL in the same directory
4. When the .exe runs, it loads the malicious DLL, executing attacker code

Time	Process	Operation	Path	Result
1:41:34	a52e245dd7937...	CreateFile	C:\Users\... \Desktop\22586098741\libcares-2.dll	NAME NOT FOUND Desired Access: R...
1:41:34	a52e245dd7937...	CreateFile	C:\Windows\System32\libcares-2.dll	NAME NOT FOUND Desired Access: R...
1:41:35	a52e245dd7937...	CreateFile	C:\Windows\System\libcares-2.dll	NAME NOT FOUND Desired Access: R...
1:41:35	a52e245dd7937...	CreateFile	C:\Users\... \Desktop\22586098741\libcares-2.dll	NAME NOT FOUND Desired Access: R...
1:41:35	a52e245dd7937...	CreateFile	C:\Python39\Scripts\libcares-2.dll	NAME NOT FOUND Desired Access: R...
1:41:35	a52e245dd7937...	CreateFile	C:\Python39\libcares-2.dll	NAME NOT FOUND Desired Access: R...
1:41:35	a52e245dd7937...	CreateFile	C:\Program Files\Eclipse Adoptium\jdk-11.0.19-hotspot\bin\libcares-2.dll	NAME NOT FOUND Desired Access: R...
1:41:35	a52e245dd7937...	CreateFile	C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_3976093\libcares-2.dll	REPARSE Desired Access: R...
1:41:35	a52e245dd7937...	CreateFile	C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_3976093\libcares-2.dll	NAME NOT FOUND Desired Access: R...
1:41:35	a52e245dd7937...	CreateFile	C:\ProgramData\Boxstarter\libcares-2.dll	NAME NOT FOUND Desired Access: R...
1:41:35	a52e245dd7937...	CreateFile	C:\Windows\System32\libcares-2.dll	NAME NOT FOUND Desired Access: R...
1:41:35	a52e245dd7937...	CreateFile	C:\Windows\libcares-2.dll	NAME NOT FOUND Desired Access: R...
1:41:35	a52e245dd7937...	CreateFile	C:\Windows\System32\wbem\libcares-2.dll	NAME NOT FOUND Desired Access: R...
1:41:35	a52e245dd7937...	CreateFile	C:\Windows\System32\WindowsPowerShell\v1.0\libcares-2.dll	NAME NOT FOUND Desired Access: R...
1:41:35	a52e245dd7937...	CreateFile	C:\Windows\System32\OpenSSH\libcares-2.dll	NAME NOT FOUND Desired Access: R...
1:41:35	a52e245dd7937...	CreateFile	C:\ProgramData\chocolatey\bin\libcares-2.dll	NAME NOT FOUND Desired Access: R...
1:41:35	a52e245dd7937...	CreateFile	C:\Program Files\010 Editor\libcares-2.dll	NAME NOT FOUND Desired Access: R...
1:41:35	a52e245dd7937...	CreateFile	C:\Program Files\Omni-IDK\jdk-20.0.1\bin\libcares-2.dll	NAME NOT FOUND Desired Access: R...
1:41:35	a52e245dd7937...	CreateFile	C:\Users\... \AppData\Local\Microsoft\WindowsApps\libcares-2.dll	NAME NOT FOUND Desired Access: R...
1:41:35	a52e245dd7937...	CreateFile	C:\Tools\Cmder\libcares-2.dll	NAME NOT FOUND Desired Access: R...
1:42:04	a52e245dd7937...	Thread Exit		SUCCESS Thread ID: 3592. U...
1:42:04	a52e245dd7937...	Thread Exit		SUCCESS Thread ID: 6632. U...
1:42:22	a52e245dd7937...	Thread Exit		SUCCESS Thread ID: 9294. U...

Figure 4: Depicts the DLL search order for libcares-2.dll by the ahost.exe utility

Campaign reach and disguise tactics

Trellix has identified that ahost.exe, signed and distributed by Gitkraken, has attracted multiple threat actors as the telemetry suggests association of this particular executable (MD5 Hash: fd3c8166e7fbbb64d12c1170b8f4bacf) with multiple malware campaigns, including XWorm and DCRat. This file has been submitted to VirusTotal numerous times under various names, with 190 submissions from 115 unique submitters, first seen in the United States and last seen in Egypt. This suggests a widespread distribution effort.

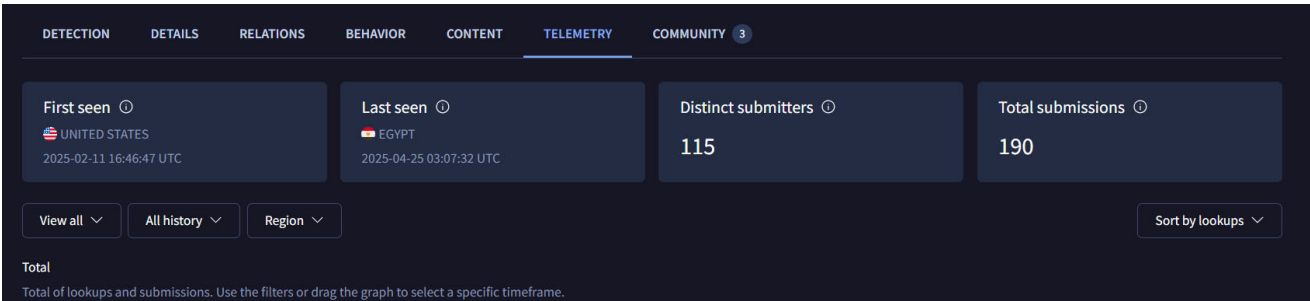


Figure 5 : VirusTotal user submissions highlighting total submissions and Distinct submitters

Attackers employ various deceptive filenames to lure victims into execution, mimicking legitimate documents or orders. Examples include:

- order.exe
- protect.exe
- ESTADO DE CUENTA 24 de abril del 2025.ex_ RFQ 536120 -R43500 V5560001/RFQ 536120 -R43500 V5560001.exe
- FXCREX.exe
- 1DOC-PDF.exe
- Your file name without extension goes here.exe
- PO-069709-MQ02959-Order-S103509.exe
- Faktura od DHL.exe

These filenames indicate a likely phishing component, where users are tricked into opening seemingly innocuous files.

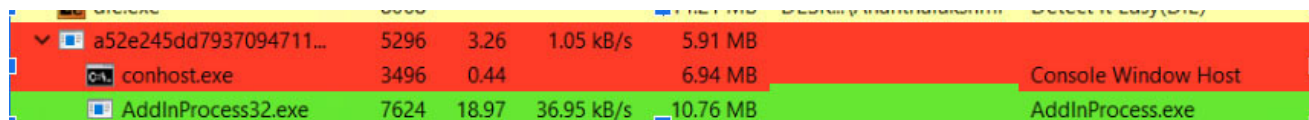
DCRat malware and persistence mechanism

One prominent campaign identified uses the DCRat (DarkCrystal RAT) malware. In this specific instance, threat actors renamed the ahost.exe executable to 1DOC-PDF.exe. This sample included a malicious libcares-2.dll, identified as DCRat malware. Executing the renamed file triggers the invocation of the malicious DLL.

Name	Date modified	Type	Size
 1DOC-PDF.exe	3/1/2025 5:55 AM	Application	63 KB
 libcares-2.dll	3/1/2025 5:55 AM	Application extens...	5,486 KB

Figure 6 : A Zip archive containing renamed ahost.exe(1DOC-PDF.exe) along with malicious libcares-2.dll

The DCRat DLL executes and launches Addinprocess32.exe. It then injects itself into this process before terminating. Analysis of the infected Addinprocess32.exe reveals an injected executable file. Examination of the strings within this file shows associations with DCRat. Even after the initial parent process is terminated, DCRat persists in running under the guise of AddInProcess32.

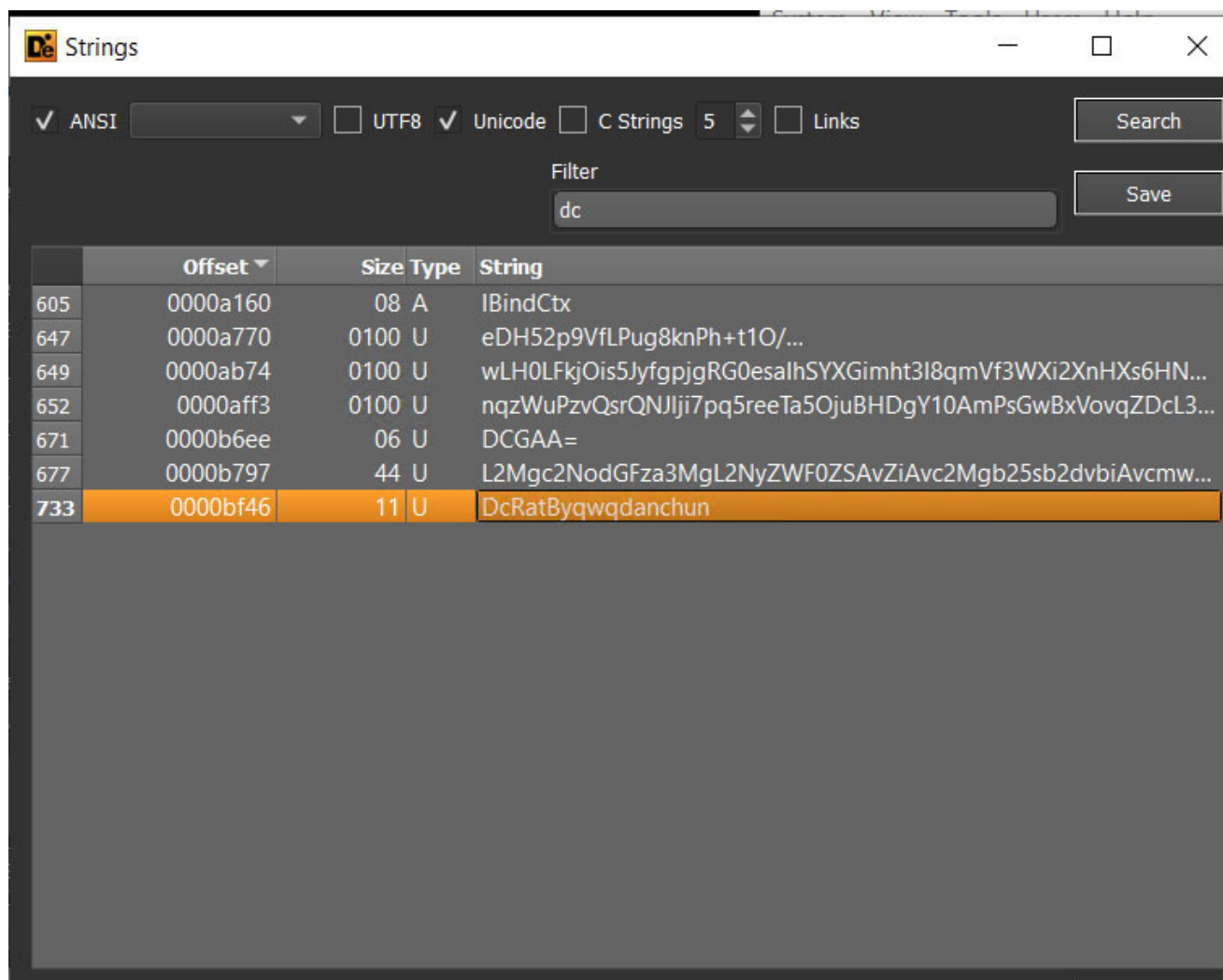


Process Name	Private Bytes	Working Set	Private Bytes/s	Private Bytes	Parent Process
a52e245dd7937094711...	5296	3.26	1.05 kB/s	5.91 MB	
conhost.exe	3496	0.44		6.94 MB	Console Window Host
AddInProcess32.exe	7624	18.97	36.95 kB/s	10.76 MB	AddInProcess.exe

Figure 7 : Depicts the ahost.exe(or a52e245dd7937094711, as seen on the picture) spawning AddInProcess32.exe

Figure 8 : Depicts the DCRat stealthily running under the guise of AddInProcess32 as a standalone process

DCRat reference in Strings



	Offset	Size	Type	String
605	0000a160	08	A	IBindCtx
647	0000a770	0100	U	eDH52p9VfLPug8knPh+t1O/...
649	0000ab74	0100	U	wLH0LFkjOis5JyfgpjgRG0esalhSYXGimht3I8qmVf3WXi2XnHXs6HN...
652	0000aff3	0100	U	nqzWuPzvQsrQNJlji7pq5reeTa5OjuBHDgY10AmPsGwBxVovqZDcl3...
671	0000b6ee	06	U	DCGAA=
677	0000b797	44	U	L2Mgc2NodGFza3MgL2NyZWFOZSAvZiAvc2Mgb25sb2dvbiAvcmw...
733	0000bf46	11	U	DcRatByqwqdanchun

Figure 9: Strings of the process AddinProcess32.exe reveals the malware is DCRat payload

DCRat Mutex

Figure 10: Mutex created by DCRat

DNS connections initiated by DCRat:

```
05/12/25 01:48:19 PM [      Diverter] svchost.exe (1948) requested UDP 192.168.31.128:53
05/12/25 02:01:19 PM [      DNS Server] Received A request for domain 'checkappexec.microsoft.com'.
05/12/25 02:01:19 PM [      DNS Server] Received A request for domain 'dgflex.duckdns.org'.
05/12/25 02:01:19 PM [      Diverter] ICMP type 3 code 3 192.168.31.128->192.168.31.128
05/12/25 02:01:22 PM [      DNS Server] Received A request for domain 'dgflex.duckdns.org'.
05/12/25 02:01:23 PM [      Diverter] AddInProcess32.exe (7624) requested TCP 192.0.2.123:35440
05/12/25 02:01:29 PM [      Diverter] svchost.exe (1948) requested UDP 192.168.31.128:53
05/12/25 02:01:29 PM [      DNS Server] Received A request for domain 'dgflex.duckdns.org'.
05/12/25 02:01:29 PM [      Diverter] AddInProcess32.exe (7624) requested TCP 192.0.2.123:35440
```

Figure 11: DNS connections made by DCRat

Conclusion

This DLL sideloading campaign poses a significant threat, utilizing trusted open source software and advanced attack techniques to distribute malware such as DCRat. The campaign's active and adaptable nature is evident from the widespread VirusTotal submissions and the variety of deceptive filenames.

Given the pervasive nature of this threat, it is important for organizations to adopt strict measures to eliminate the risks posed by the threat actors. This malware campaign highlights the growing threat of DLL sideloading attacks that exploit trusted, signed utilities like GitKraken's `ahost.exe` to bypass security defenses. By leveraging legitimate software and abusing its DLL loading process, threat actors can stealthily deploy powerful malware such as XWorm and DCRat, enabling persistent remote access and data theft.

[Trellix Endpoint Security \(ENS\)](#) offers a powerful, multilayered approach to defending against advanced threats like the DLL sideloading campaign. Trellix ENS combines several security controls to create a proactive defense posture, thereby moving beyond a reliance on signature-based detection.

Key to this strategy is the ability to configure and manage Exploit Prevention settings. This includes customizing exclusions to prevent legitimate applications from being flagged, and fine-tuning Trellix-defined signatures to block known exploit techniques. Furthermore, organizations can manage Trellix-defined application protection rules, enabling them to control which applications are monitored and how they behave. For even greater control, you can create and duplicate custom rules to address specific threats or tailor protection to your environment, with any changes persisting through content updates.

By integrating strong endpoint hardening with advanced behavioral detection and automated response capabilities, Trellix ENS allows organizations to move from a reactive to a proactive security model. This comprehensive defense strategy effectively mitigates the risks posed by DLL sideloading and other evasive techniques, ensuring the security of systems against an ever-evolving landscape of cyber threats.

We appreciate GitKraken's collaboration, their establishment of a bug bounty program, and their prompt attention to resolving this issue.

<https://www.gitkraken.com/bug-bounty-program>
<https://gitkraken.atlassian.net/servicedesk/customer/portal/7/create/10687>

Remediations from Trellix:

Behavioral detection: Advanced EDR tools employ behavioral detection to identify malicious activity. They monitor for suspicious patterns such as unusual DLL loads, abnormal process creation, and network traffic that may indicate a threat.

Application control: Through application control, strict allowlisting policies can be enforced to allow only trusted executables and their verified DLLs to run, thereby preventing unauthorized DLL sideloading.

Threat intelligence: Updated threat intelligence needs to be continuously integrated. This ensures timely awareness of emerging indicators linked to the malware campaigns.

Automated response: When suspicious activity is detected, automated workflows can swiftly contain the threat by quarantining compromised devices and shutting down malicious processes.

Endpoint hardening: Strengthening endpoint configurations by disabling obsolete DLL search paths, applying current software patches, and limiting user privileges reduces the overall attack surface.

Reference:

[Configure Exploit Prevention settings to block threats](#)
[Endpoint Security \(ENS\) | Trellix](#)

Indicator of Compromise(IOCs):

7c41ac7b5bf15e34d50d6abbe28254e94e6c21e0ccab9fa68aca05049a515758	Cesvaine.dll
e7be7413c4cff8595de4cbc9c8621163565afe3e57412e59be3389aef1a18cc5	Ջերմուկ.dll
0b7660173e0bfe2ff7015014d5c7cc1f27e9e80c330f5553316f5c031b387d15	Gdansk.dll
a7d7965baed40cfd0edbc9d7ef3052dcf20148769b2dfe32d0117dbd762b8a9d	F**kLuciferJesusIsTheLORD.dll
791a7d2710409cf72cf34bd4c29a3ebfe17ad3217d138215c0e03aa3513c8d0e	Emifimozicozopinu
e533da586b912241cc8c5d4762d78607b50b75cb7070ad839d72f8ee76cb5636	Avasirexexoyaxuzo

Trellix detection signatures

Trellix Endpoint Security (ENS)	Generic trojan.prf Trojan-FXMD Trojan-FXOW
---------------------------------	--

Trellix Endpoint Security (HX)	Gen:Variant.Tedy.765584 Gen:Variant.Lazy.655556 Trojan.GenericKD.76272268 Gen:Variant.Mikey.177808
Trellix EDR	Wrote PE header into remote process (PE file DOS header)(T1106 T1055.002 T1620) Potential injection into dotnet process(T1055) Remote process section unmap, possible Process Injection(T1106 T1055.011 T1055.012) Process hollowed for execution (T1106 T1055.012) Executed Microsoft .NET InstallUtil.exe without parameters (T1218.004) Suspicious DNS Query (Commonly Abused Web Services) by AddInProcess32.exe (T1071.004 T1568) Suspicious launch of Microsoft .NET framework binary (T1059.003) Suspicious binary communicates via Web Protocol (potential C2 activity) (T1071.001)

Contacted Domains (C2 Communication)

hxxp[:]//dgflex[.]duckdns[.]org The site is Categorization as “Malicious Sites” , High Risk by Trellix security in <https://trustedsource.org>

Discover the latest cybersecurity research from the Trellix Advanced Research Center:

<https://www.trellix.com/advanced-research-center/>

This document and the information contained herein describes computer security research for educational purposes only and the convenience of Trellix customers.

RECENT NEWS

- Dec 16, 2025

[Trellix NDR Strengthens OT-IT Security Convergence](#)

- Dec 11, 2025

[Trellix Finds 97% of CISOs Agree Hybrid Infrastructure Provides Greater Resilience](#)

- Oct 29, 2025

[Trellix Announces No-Code Security Workflows for Faster Investigation and Response](#)

- Oct 28, 2025

[Trellix AntiMalware Engine secures I-O Data network attached storage devices](#)

- Oct 23, 2025

[Trellix CyberThreat Report Reveals Blurring Lines Between Nation-State Espionage and Financially Motivated AI Attacks](#)

RECENT STORIES

- Jan 21, 2026

[Trellix and Nozomi Networks: Charting the Future of IT/OT Security](#)

- Jan 20, 2026

[From the Shadows to the Headlines: A Decade of State-Sponsored Cyber Leaks](#)

- Jan 15, 2026

[Dark Web Roast December 2025 Edition](#)

- Jan 14, 2026

[Hiding in Plain Sight: Multi-Actor ahost.exe Attacks](#)

- Jan 13, 2026

[8 Reasons NDR Is Essential in Hybrid Environments](#)

Latest from our newsroom

Blogs | Platform

[Trellix Launches Database Security 10.3](#)

By [Gourav Mehta](#) · December 10, 2025

Trellix Database Security 10.3 launches with Analytics Hub for deep insights, expanded IPv6 and Azure IaaS support, and coverage for the latest databases.

[Read the Blog](#)

Blogs | Platform

[5 Ways Trellix NDR 4.1 Advances the SOC](#)

By [Ravi Adireddi](#) and [Haroon Malik](#) · December 16, 2025

New Trellix NDR 4.1 delivers speed and unified security with no-code hyperautomation, IT/OT convergence, and AI-based detections that work on-prem/air-gapped.

[Read the Blog](#)

Blogs | Research

[Fake Domain Controllers: Detecting DCShadow via Trellix NDR](#)

By [Maulik Maheta](#) and [Chao Sun](#) · December 17, 2025

Understanding how DCShadow works and how to detect it is critical for protecting your identity infrastructure, whether you're a SOC analyst, Active Directory administrator, or member of a red team or incident response function.

[Read the Blog](#)

Get the latest

Stay up to date with the latest cybersecurity trends, best practices, security vulnerabilities, and so much more.

Zero spam. Unsubscribe at any time.