

HiveForce Labs

THREAT ADVISORY



ATTACK REPORT

ToddyCat Hackers Exploit ESET Flaw to Deploy Hidden Malware

Date of Publication

April 8, 2025

Admiralty Code

A1

TA Number

TA2025105

Summary

Attack Commenced: 2024

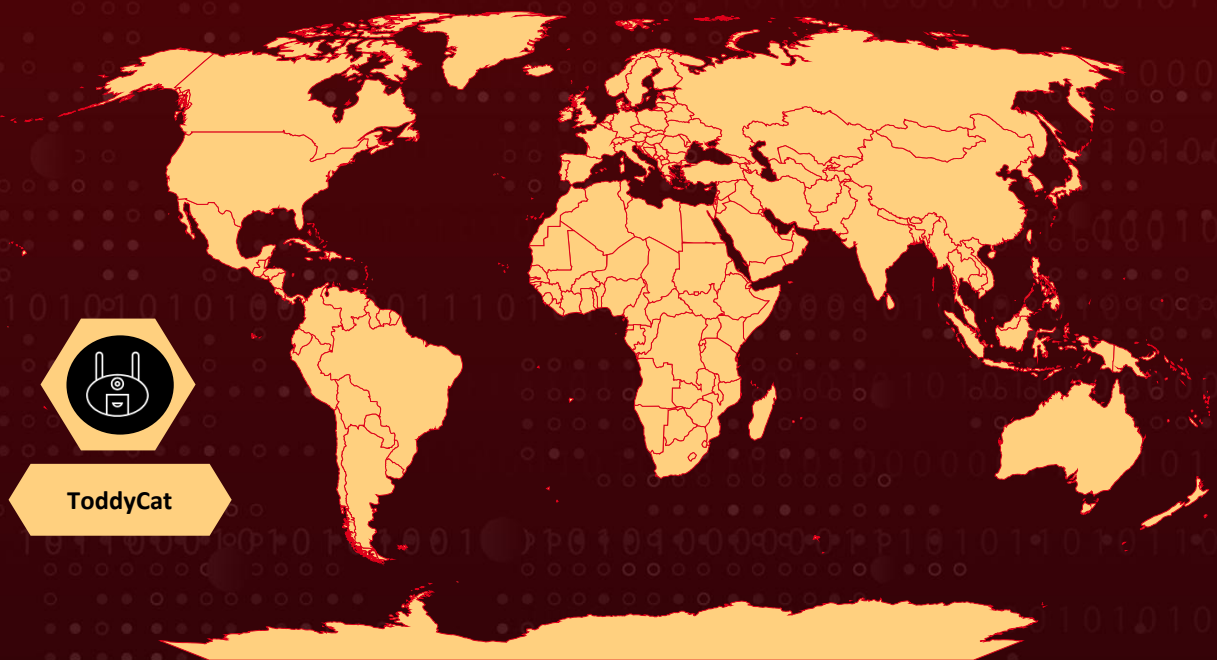
Targeted Countries: Worldwide

Targeted Platform: Windows







Threat Actor: ToddyCat

Attack: ToddyCat, an advanced persistent threat (APT) group, exploited a vulnerability (CVE-2024-11859) in ESET's command-line scanner using DLL proxying. This technique allowed them to load malicious code stealthily by mimicking legitimate libraries. The attackers used a modified tool named TCESB to bypass security measures and manipulate kernel structures. This incident highlights the need for timely patching and vigilance, even with trusted security software.

🔪 Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-11859	ESET Multiple Products DLL Search Order Hijacking Vulnerability	ESET Multiple Products			
CVE-2021-36276	Dell DBUtilDrv2.sys Driver Insufficient Access Control Vulnerability	Dell DBUtilDrv2.sys Driver			

Attack Details

#1

ToddyCat is an advanced persistent threat (APT) group known for targeting high-profile entities across Europe and Asia since late 2020. It has previously exploited vulnerabilities such as ProxyLogon in Microsoft Exchange servers and deployed custom malware like the Samurai backdoor and Ninja Trojan for remote control and data exfiltration.

#2

The group is exploiting CVE-2024-11859, a vulnerability in ESET's command-line scanner, which allows stealthy execution of malicious payloads. This is a DLL search order hijacking vulnerability that enables attackers to trick Windows into executing malicious DLLs. Specifically, it involves improper loading of the version.dll library, allowing attackers to substitute it with a malicious version.

#3

The malicious DLL, part of a tool named TCESB, mimics the legitimate library's exported functions, loading the real DLL in the background to preserve normal functionality while injecting malicious behavior, a technique known as DLL proxying. This allows the malware to operate undetected within the context of a trusted application.

#4

TCESB is a modified version of the open-source tool EDRSandBlast, engineered to exploit weak points in system-level protections, including kernel structure modifications to disable security notifications. To further evade detection and gain higher privileges, ToddyCat also uses the Bring Your Own Vulnerable Driver (BYOVD) technique, leveraging a known vulnerable driver from Dell (CVE-2021-36276) to perform unauthorized operations at the kernel level.

#5

ESET has addressed this issue by releasing a patch in January 2025. Users are strongly advised to update their ESET software to the latest version to mitigate this vulnerability. This case highlights the critical need for timely patching and proactive defense measures, even for trusted security tools, as sophisticated actors like ToddyCat can weaponize overlooked weaknesses.

Recommendations



Update ESET Products: Ensure all ESET products are updated to the latest versions that address CVE-2024-11859. ESET released patches in January 2025 to fix this vulnerability. Regularly check for and apply security updates to maintain protection.



Remove or Update Dell's DBUtilDrv2.sys Driver: Identify and remove versions 2.5 and 2.6 of the DBUtilDrv2.sys driver, which contain the CVE-2021-36276 vulnerability. Dell has provided guidance on how to remove the vulnerable driver and obtain an updated, secure version.



Restrict Administrative Privileges: Limit administrative access to essential personnel only. Since exploiting this vulnerability requires administrative privileges, minimizing the number of users with such access reduces potential attack vectors.



Monitor for Suspicious Activity: Implement continuous monitoring to detect unusual behaviors, such as unauthorized driver installations or unexpected DLL loads. Pay particular attention to the use of known vulnerable drivers, like Dell's DBUtilDrv2.sys, which attackers have exploited for kernel-level operations.



Implement Application Whitelisting: Use application control policies to allow only approved software to run on your systems. This can prevent unauthorized executables, including malicious DLLs, from being executed.



Potential MITRE ATT&CK TTPs

<u>TA0042</u> Resource Development	<u>TA0007</u> Discovery	<u>TA0002</u> Execution	<u>TA0004</u> Privilege Escalation
<u>TA0005</u> Defense Evasion	<u>TA0003</u> Persistence	<u>TA0011</u> Command and Control	<u>T1068</u> Exploitation for Privilege Escalation
<u>T1588</u> Obtain Capabilities	<u>T1036</u> Masquerading	<u>T1588.005</u> Exploits	<u>T1588.006</u> Vulnerabilities
<u>T1574</u> Hijack Execution Flow	<u>T1059</u> Command and Scripting Interpreter	<u>T1027</u> Obfuscated Files or Information	<u>T1082</u> System Information Discovery
<u>T1574.001</u> DLL Search Order Hijacking	<u>T1562.001</u> Disable or Modify Tools	<u>T1562</u> Impair Defenses	<u>T1083</u> File and Directory Discovery
<u>T1211</u> Exploitation for Defense Evasion			

✂ Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	008f506013456ea5151df779d3e3ff0f, 8795271f02b30980ebd9950fcc141304, b87944dcc444e4c6ce9bb9fb8a9c0def, d38e3830c8ba3a00794ef3077942ad96, dacb62578b3ea191ea37486d15f4f83c, de39ee41d03c97e37849af90e408abbe
SHA256	697061b0c1032f0f8e134438ed793506208c328c3039bea5aeb9d5f c432d9444, 56ed7ff7299c83b307282ce8d1def51d72a3663249e72a32c09f626 4348b1da2, 2e6b339597a89e875f175023ed952aaac64e9d20d457bbc07acf15 86e7fe2df8, c77c24e945acc73d6b723f60bcd0330ff501eea34b7da95061101d d1120392a



Patch Links

<https://support.eset.com/en/ca8810-dll-search-order-hijacking-vulnerability-in-eset-products-for-windows-fixed>

<https://www.dell.com/support/kbdoc/en-us/000190105/dsa-2021-152-dell-client-platform-security-update-for-an-insufficient-access-control-vulnerability-in-the-dell-dbutildrv2-sys-driver>

References

<https://securelist.com/toddy-cat-exploits-vulnerability-in-eset-software-for-dll-proxying/116086/>

<https://hivepro.com/threat-advisory/toddy-cats-toolkit-and-tactics-fueling-data-theft/>

<https://hivepro.com/threat-advisory/unraveling-the-intricate-arsenal-of-stayin-alive-campaign/>

<https://hivepro.com/threat-advisory/toddy-cat-exploits-unknown-vulnerability-in-microsoft-exchange-servers-to-targets-entities-in-europe-and-asia/>

What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON
April 8, 2025 • 6:30 AM

