Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

⚔ ATTACK REPORT

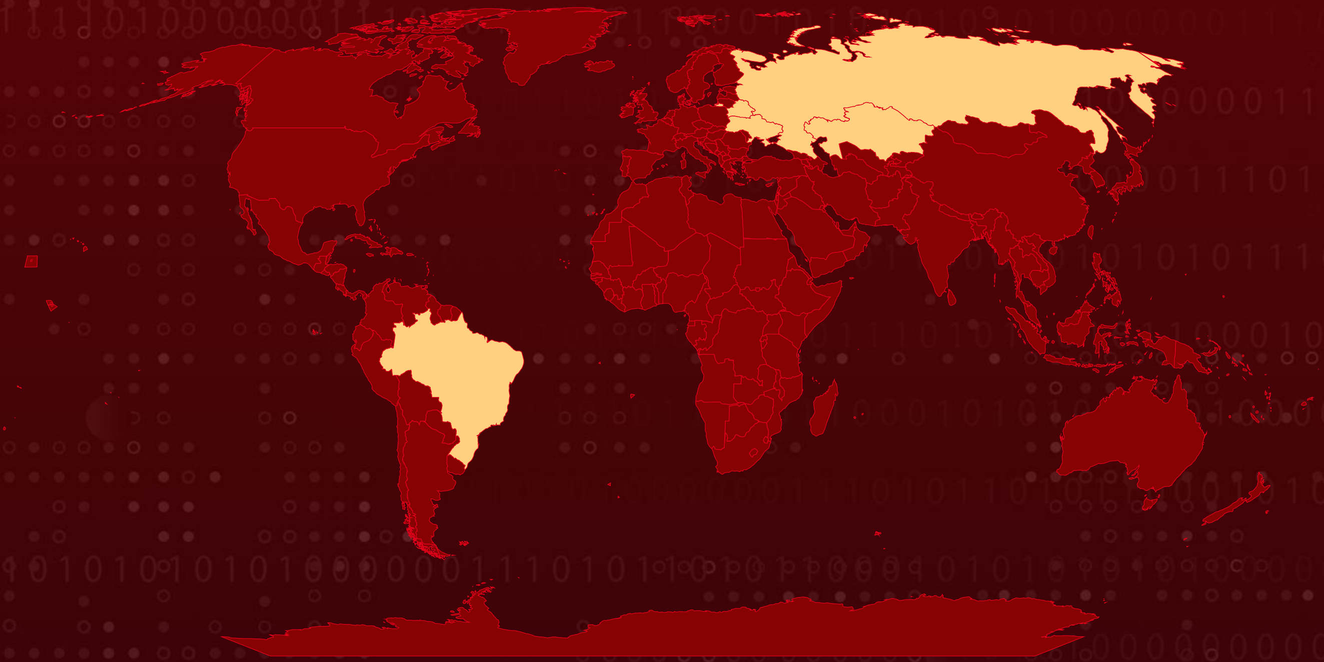
MedusaLocker Uses ThrottleStop.sys Flaw to Kill AV on Windows

Date of Publication	Admiralty Code	TA Number
August 8, 2025	A1	TA2025244

Summary

First Seen: October 2024
Targeted Countries: Russia, Belarus, Kazakhstan, Ukraine, Brazil
Targeted Platforms: Windows
Malware: MedusaLocker ransomware
Attack: A new BYOVD attack abuses a vulnerability in the legitimate ThrottleStop.sys driver (CVE-2025-7771) to disable antivirus and EDR protections by enabling kernel-level memory manipulation from user mode. In one incident in Brazil, attackers used stolen RDP credentials, deployed a renamed version of the driver (ThrottleBlood.sys) with a malicious tool to terminate AV processes, and then launched MedusaLocker ransomware. Defenders are urged to monitor for or block the driver until a fix becomes available.

Attack Regions



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

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-7771	TechPowerUp ThrottleStop Privilege Escalation Vulnerability	TechPowerUp ThrottleStop	✓	✗	✗

Attack Details

#1

A new cyberattack uncovered where criminals exploit a legitimate Windows driver, ThrottleStop.sys, to disable antivirus (AV) and endpoint detection and response (EDR) protections. ThrottleStop is a legitimate tool created by TechPowerUp for controlling CPU performance, but its driver contains a vulnerability, now tracked as CVE-2025-7771, that allows kernel-level read and write access to physical memory via unsafe IOCTL functions. By abusing this flaw, attackers can terminate protected AV processes directly from user mode, bypassing normal Windows security restrictions.

#2

This technique falls under the “Bring Your Own Vulnerable Driver” (BYOVD) category, where legitimate signed drivers are weaponized for malicious purposes.In a real-world attack observed in Brazil, the threat actor first gained network access through valid RDP credentials and expanded their reach via lateral movement using tools like Mimikatz and pass-the-hash.

#3

Once inside, they deployed a renamed version of the vulnerable driver (ThrottleBlood.sys) alongside a malicious executable (All.exe). This toolset effectively neutralized the victim’s AV defenses, paving the way for the deployment of MedusaLocker ransomware, which encrypted network systems and demanded payment.

#4

The attack highlights the dangers of BYOVD techniques, which have become increasingly common as cybercriminals target weak points in trusted software. Because these drivers are digitally signed, they can bypass driver signature enforcement, making them harder to block without specific detection rules.

#5

Until a vendor patch is available, defenders are urged to monitor for or block the presence of ThrottleStop’s driver in enterprise environments. Proactive measures, such as hardening systems against unsigned driver loading and monitoring for unusual driver installations, can significantly reduce the risk.

Recommendations

Block or Monitor the Driver: Identify and prevent loading of ThrottleStop.sys or its renamed variants (e.g., ThrottleBlood.sys) through driver blocklists or endpoint policies. Proactive monitoring can catch driver deployment before it's used to disable security tools.

Patch and Update: Apply the vendor's patch for CVE-2025-7771 as soon as it becomes available, and keep all drivers and software up to date to reduce BYOVD attack surfaces.

Harden Driver Loading Policies: Implement Windows Defender Application Control (WDAC) or similar allowlisting to restrict which drivers can load, even if digitally signed. This prevents attackers from abusing legitimate but vulnerable drivers.

Restrict and Secure Remote Access: Limit RDP exposure, enforce multi-factor authentication, and monitor for unusual remote login attempts. Many ransomware campaigns start with stolen or brute-forced remote credentials.

Monitor for BYOVD Attack Indicators: Set up detection rules for unexpected driver installations, kernel module changes, and unusual IOCTL requests. Early detection can stop AV-killer tools before they disable defenses.

Use Endpoint Tools with Self-Defense: Deploy security solutions that protect their own processes, files, and registry keys at the kernel level. This prevents attackers from terminating or bypassing AV and EDR agents.

Potential MITRE ATT&CK TTPs

TA0007 Discovery	TA0008 Lateral Movement	TA0001 Initial Access	TA0002 Execution
TA0040 Impact	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access

T1057 Process Discovery	**T1562.001** Disable or Modify Tools	**T1562** Impair Defenses	**T1562.006** Indicator Blocking
T1543.003 Windows Service	**T1543** Create or Modify System Process	**T1078** Valid Accounts	**T1489** Service Stop
T1059.001 PowerShell	**T1059** Command and Scripting Interpreter	**T1550.002** Pass the Hash	**T1550** Use Alternate Authentication Material
T1021.001 Remote Desktop Protocol	**T1021** Remote Services	**T1486** Data Encrypted for Impact	**T1068** Exploitation for Privilege Escalation

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	a88daa62751c212b7579a57f1f4ae8f8, eb927d21f6b072ae81618aa784cfff36
SHA1	0a15be464a603b1eebc61744dc60510ce169e135, 86a2a93a31e0151888c52dbbc8e33a7a3f4357db, 987834891cea821bcd3ce1f6d3e549282d38b8d3, c0979ec20b87084317d1bfa50405f7149c3b5c5f, d5a050c73346f01fc9ad767d345ed36c221baac2, dcaed7526cda644a23da542d01017d48d97c9533, eff7919d5de737d9a64f7528e86e3666051a49aa, 18484384c0b486b5a1de14f7eeada44f37de390b, f02daf614109f39babdcb6f8841dd6981e929d70
SHA256	53ec23e45303511066b478bc58e02df108417d748bdbecc3bb55a881a26f90a4, 7a311b584497e8133cd85950fec6132904dd5b02388a9feed3f5e057fb891d09

Patch Details

The patch has not been released yet. As a temporary measure, block ThrottleStop.sys until the vendor provides a secure version.

References

https://securelist.com/av-killer-exploiting-throttlestop-sys/117026/

https://github.com/klsecservices/Advisories/blob/master/K-TechPowerUp-2025-001.md

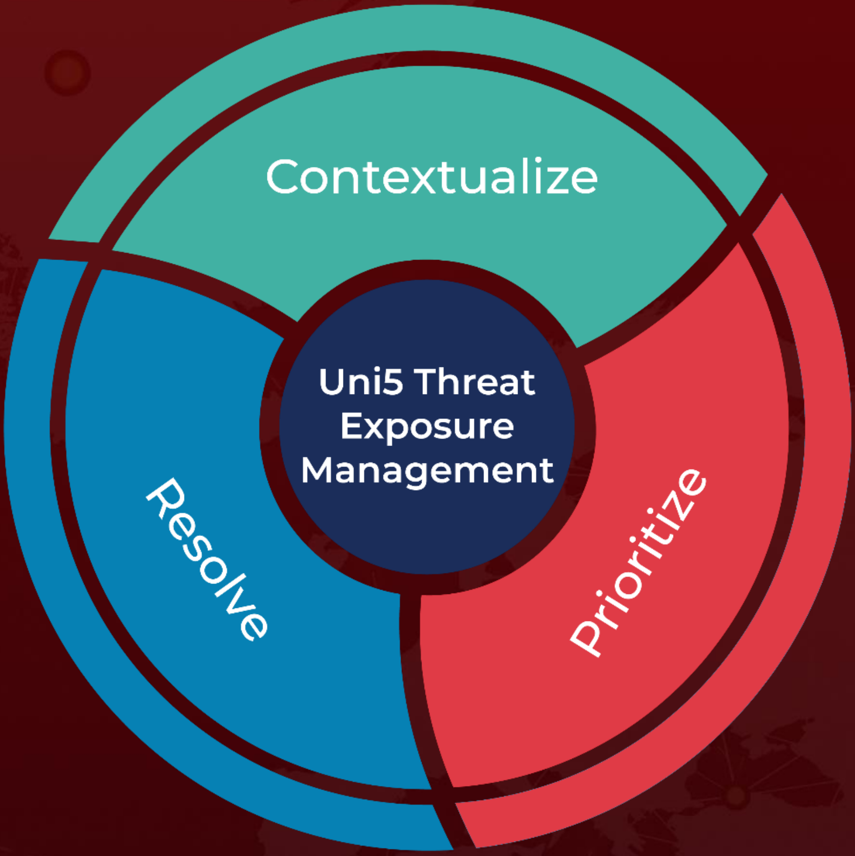
https://www.techpowerup.com/forums/threads/throttlestop-sys-driver-vulnerability.339687/

https://hivepro.com/threat-advisory/medusalocker-ransomware-is-back-targeting-organizations-in-us/

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

August 8, 2025 • 6:30 AM

More at www.hivepro.com