Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

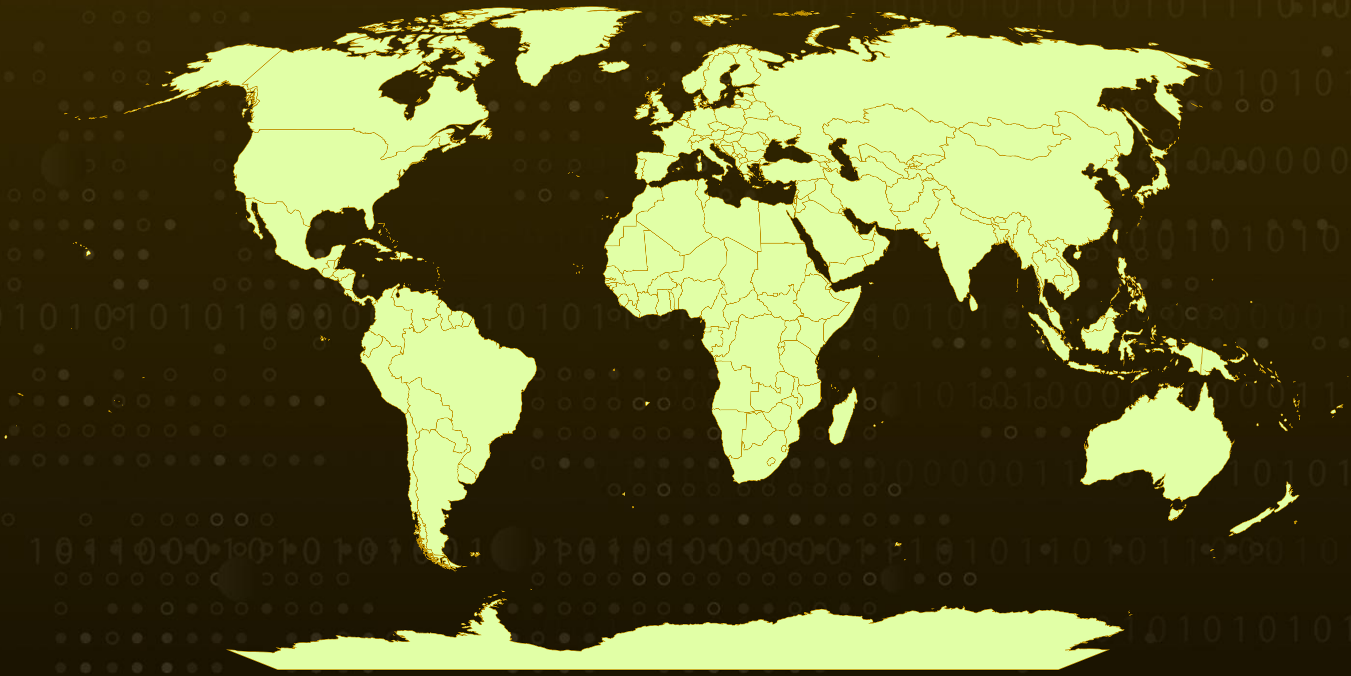
When Trust Turns Toxic: Exploiting Avast Drivers in BYOVD Attacks

Date of Publication	Admiralty Code	TA Number
November 26, 2024	A1	TA2024443

Summary

Attack Discovered: 2024
Targeted Countries: Worldwide
Attack: A new malicious campaign has been uncovered where attackers use a cunning evasion technique, deploying the legitimate Avast Anti-Rootkit driver (aswArPot.sys) to bypass detection mechanisms. This strategy exploits the driver's kernel-mode privileges, corrupting its trusted status to execute malicious actions. Once deployed, the driver becomes a tool for disabling protective processes, effectively neutralizing system defenses and compromising infected machines.

Attack Regions



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

Attack Details

#1 A recently uncovered malicious campaign reveals a sophisticated evasion tactic where attackers misuse the legitimate Avast Anti-Rootkit driver (aswArPot.sys) to compromise systems. By leveraging the driver's deep kernel-level privileges, the malware terminates security processes, disables protective software, and establishes dominance over the infected machine. This manipulation of a trusted driver underscores the risks associated with kernel-mode components, which, while designed to safeguard systems, can become potent tools in the hands of attackers.

#2 The malware, identified as kill-floor.exe, begins by planting the Avast Anti-Rootkit driver in the `C:\Users\Default\AppData\Local\Microsoft\Windows` directory. Exploiting the driver's legitimate status, the malware avoids raising red flags while registering the driver as a service (`aswArPot.sys`). Once installed, the driver grants kernel-level access, enabling the malware to bypass tamper protection, terminate critical security processes, and gain complete control over the system.

#3 This attack operates by taking snapshots of running processes, cross-referencing them with a list of 142 hardcoded security process names. When a match is found, the malware utilizes the driver's capabilities to terminate these processes using the DeviceIoControl API and the IOCTL code. Through this approach, the Avast driver, originally designed to protect systems, becomes a weapon for overriding user-mode processes and neutralizing antivirus and endpoint detection and response (EDR) solutions.

#4 The driver's behavior reveals its reliance on Windows kernel functions to execute these attacks. This technique exemplifies a Bring Your Own Vulnerable Driver (BYOVD) attack, where legitimate but flawed drivers are exploited to gain kernel-level access. Such attacks bypass traditional defenses, making them a significant threat to modern systems.

Recommendations

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Deploy BYOVD-Specific Detection Rules: Implement expert rules or policies in Endpoint Detection and Response (EDR) and antivirus solutions to identify and block vulnerable drivers based on unique attributes like file hash, signature, or known behaviors.

Monitor Driver Activities: Enable logging and monitoring of kernel driver installations and activities. Configure alerts for unusual driver behaviors, such as the unexpected termination of security processes.

Leverage Application Whitelisting: Restrict the execution of unauthorized programs or binaries, ensuring only approved applications and drivers can run on critical systems.

Implement Behavioral Analysis: Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0007 Discovery	T1543 Create or Modify System Process	T1543.003 Windows Service	T1106 Native API
T1014 Rootkit	T1036 Masquerading	T1036.005 Match Legitimate Name or Location	T1547 Boot or Logon Autostart Execution
T1547.006 Kernel Modules and Extensions	T1068 Exploitation for Privilege Escalation	T1505 Server Software Component	T1059 Command and Scripting Interpreter
T1057 Process Discovery	T1548 Abuse Elevation Control Mechanism		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	40439f39f0195c9c7a3b519554afd17a, a179c4093d05a3e1ee73f6ff07f994aa
SHA256	e882af8b945c92e5a7dd337378e6a8bffc2b93f1e2719e853d756123cc8ab947, 4b5229b3250c8c08b98cb710d6c056144271de099a57ae09f5d2097fc41bd4f1

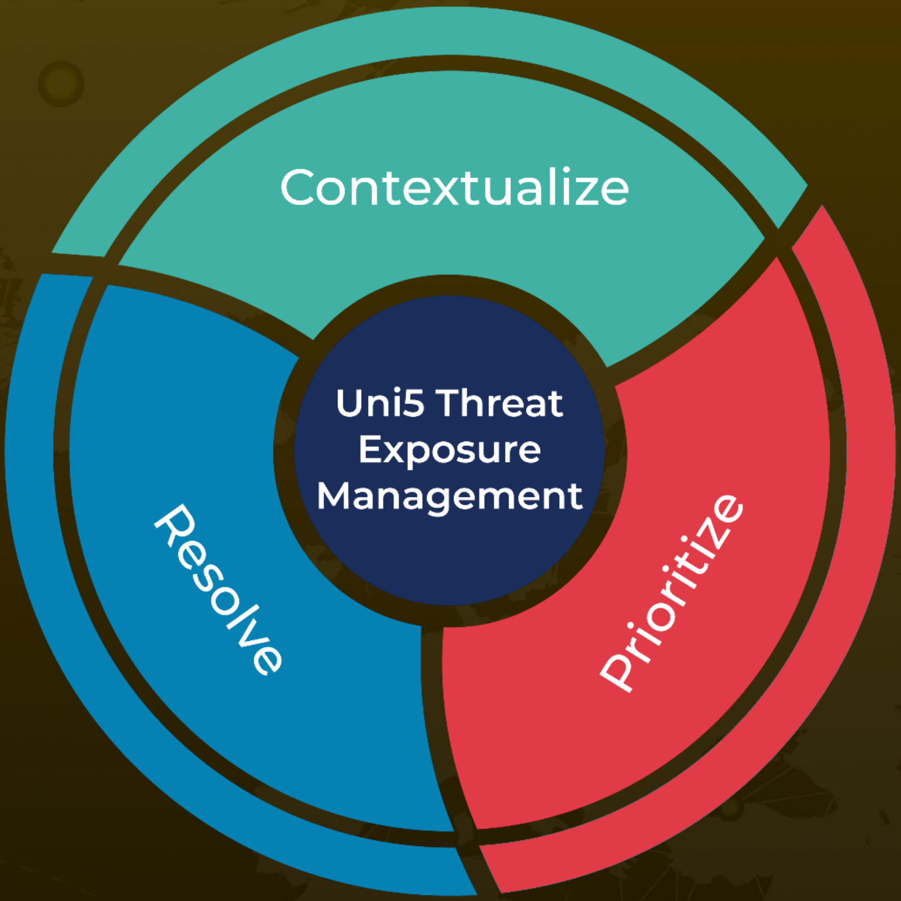
References

https://www.trellix.com/blogs/research/when-guardians-become-predators-how-malware-corrupts-the-protectors/

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

November 26, 2024 • 5:00 AM

More at www.hivepro.com