Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

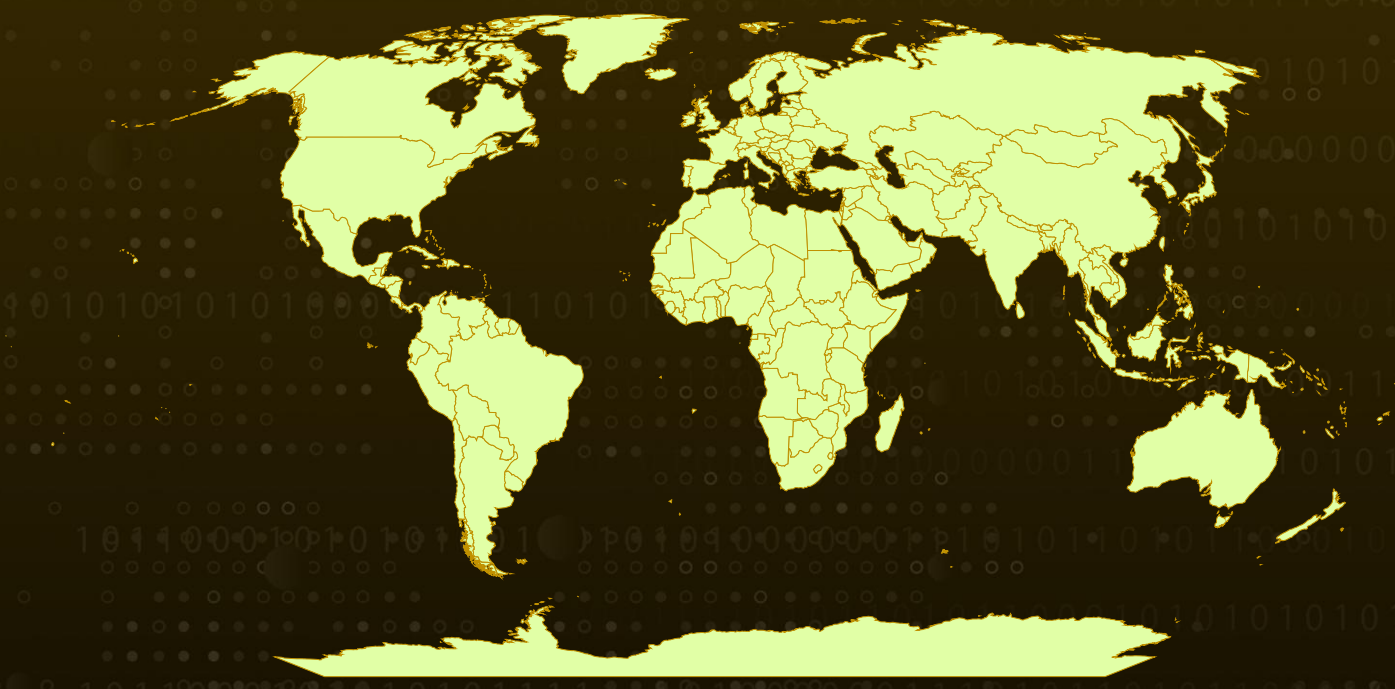
Silent Sabotage: EDRSilencer Disables Detection and Enables Stealth Attacks

Date of Publication	Admiralty Code	TA Number
October 16, 2024	A1	TA2024396

Summary

Attack Discovered: October 2024
Targeted Countries: Worldwide
Attack: EDRSilencer, a red team tool originally designed to test security defenses, has now been weaponized by hackers in live attacks. Rather than helping organizations improve their security posture, it's being used to silence endpoint detection and response (EDR) solutions by blocking alerts to management consoles. This allows attackers to operate stealthily, evading detection and making it harder for security teams to uncover malicious activities. The abuse of tools like EDRSilencer serves as a stark reminder that security solutions can be turned against us, highlighting the need for continuous vigilance and adaptive defenses.

Attack Regions



Attack Details

#1 Red team tools are vital for assessing and strengthening an organization's security infrastructure. However, cybercriminals have increasingly found ways to weaponize these tools for malicious purposes. One such case is EDRSilencer an open-source tool, which manipulates the Windows Filtering Platform (WFP) to disable endpoint detection and response (EDR) solutions. This tool interferes with EDRs by blocking their network communication, preventing them from reporting suspicious activities or malware to their management consoles. By doing so, attackers can evade detection and maintain persistence within compromised environments.

#2 The WFP is a robust framework within Windows that enables the creation of security applications that filter, monitor, and control network traffic. While it plays a critical role in firewalls and antivirus software, EDRSilencer exploits this framework to selectively block EDR traffic by applying filters to outbound network communication on both IPv4 and IPv6 protocols. This tactic ensures that even if malware is operating on the system, it remains hidden from the EDR's surveillance. The filters EDRSilencer applies are persistent, meaning they remain effective even after the system reboots.

#3 The attack chain involving EDRSilencer starts with a process discovery phase, where the tool scans the system for running processes tied to popular EDR solutions. Using the "blockedr" argument, attackers can either block all detected EDR processes or target specific ones by specifying their full paths. Once identified, Windows Filtering Platform (WFP) filters are applied to block outbound network traffic for both IPv4 and IPv6 protocols, ensuring that these blocks remain in effect even after system reboots.

#4 As a result, EDR tools are effectively disabled, unable to send critical data like telemetry and alerts to their management consoles. This significantly weakens an organization's ability to detect and respond to malicious activities. In some cases, certain EDR processes may continue to communicate if they are not part of the tool's predefined hardcoded list, but overall, the EDR system is rendered ineffective. This allows malware or other malicious actions to go undetected, increasing the likelihood of successful and prolonged attacks without swift intervention from security teams.

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.

Least Privilege: Adhere to the idea of "least privilege" by giving users only the essential permissions they need for their tasks, restrict the access to the trusted parties only.

Network Segmentation: To enhance protection against evolving threats, organizations should implement multi-layered security controls. One critical strategy is network segmentation, which isolates sensitive systems and data, reducing the risk of lateral movement in case of a breach.

Multi-layered Security Control: Layering multiple protection mechanisms such as firewalls, intrusion detection systems (IDS), antivirus, and endpoint detection and response (EDR) solutions. This ensures that even if one layer is compromised, others remain to detect, prevent, or block the threat. By employing a diverse set of defenses, this strategy reduces vulnerabilities and improves an organization's ability to withstand and mitigate different types of cyberattacks, bolstering the overall security posture.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0007 Discovery
TA0040 Impact	T1057 Process Discovery	T1059 Command and Scripting Interpreter	T1543 Create or Modify System Process
T1543.005 Container Service	T1562 Impair Defenses	T1562.001 Disable or Modify Tools	T1569 System Services
T1569.002 Service Execution	T1498 Network Denial of Service	T1499 Endpoint Denial of Service	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	721af117726af1385c08cc6f49a801f3cf3f057d9fd26fcec2749455567888e7

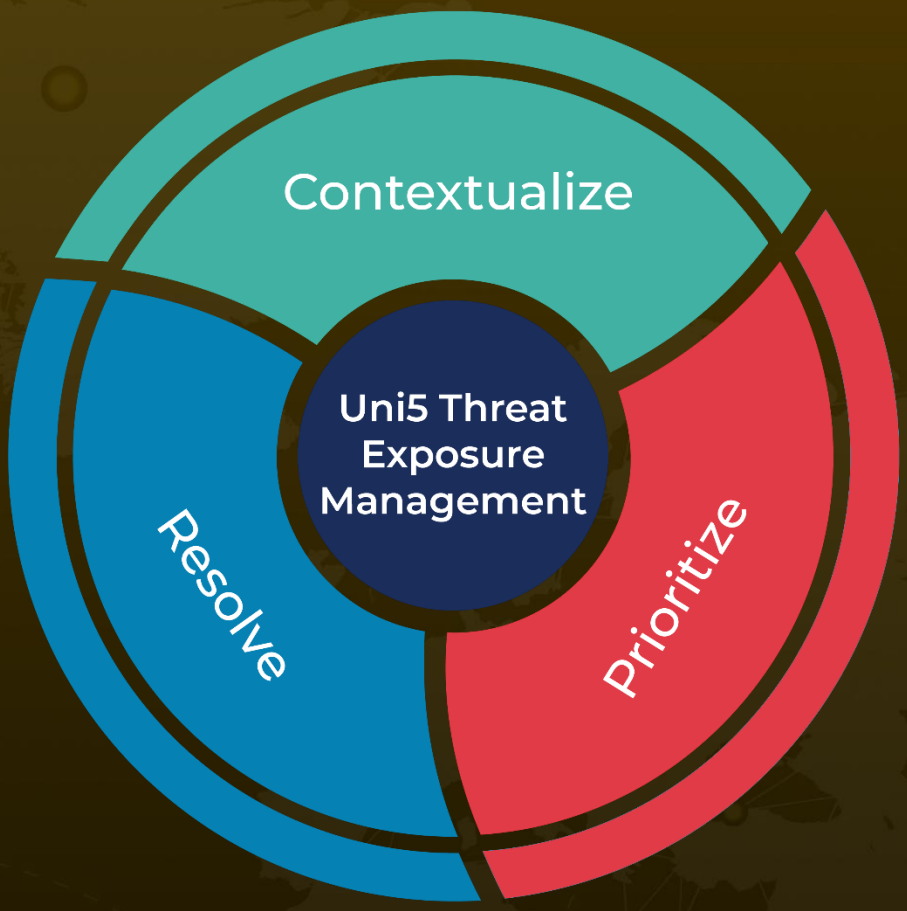
References

https://www.trendmicro.com/en_us/research/24/j/edrsilencer-disrupting-endpoint-security-solutions.html

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

October 16, 2024 • 6:15 AM

More at www.hivepro.com