Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

Xeno RAT Open-Source Trojan Sparks Alarm

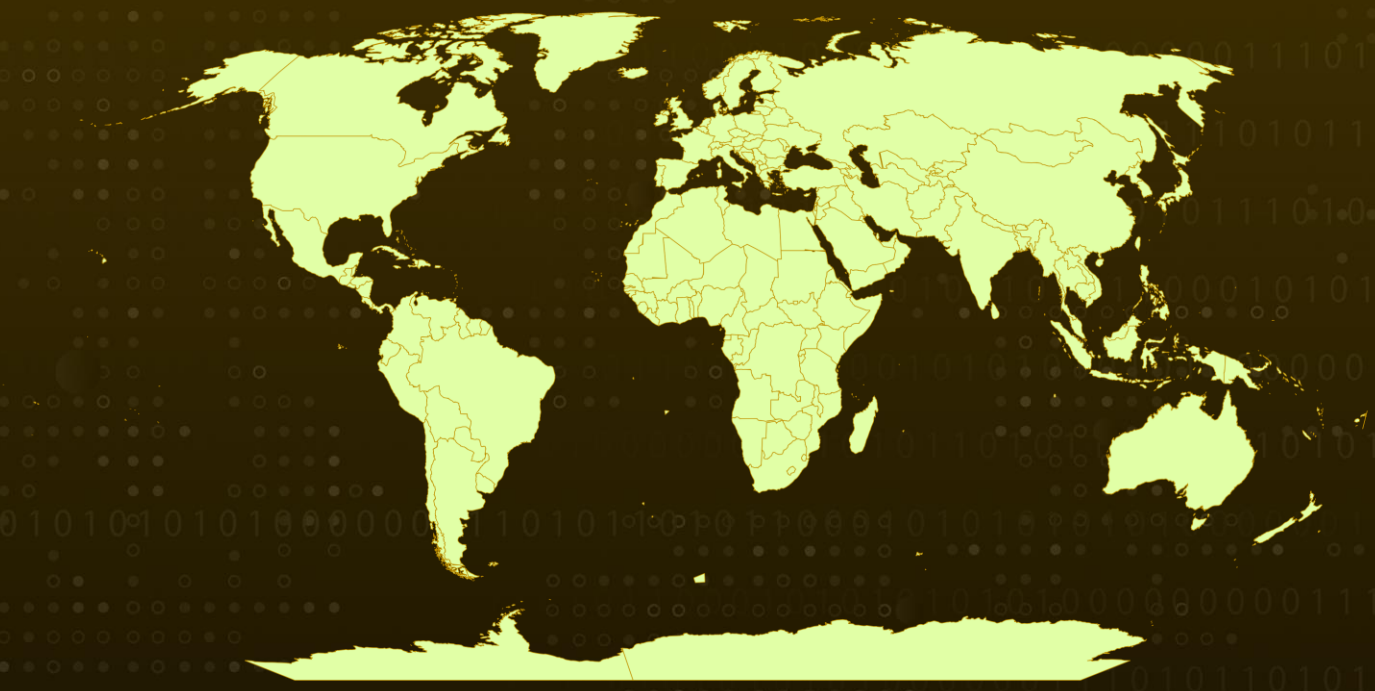
Date of Publication	Admiralty Code	TA Number
February 28, 2024	A1	TA2024079

Summary

Malware: Xeno RAT
Affected Platform: Windows
Attack Region: Worldwide

Attack: The Xeno RAT, a remote access trojan (RAT) available on GitHub, has gained attention in the threat landscape due to its open-source nature. This C#-based malware is compatible with both Windows 10 and 11, specifically targeting consumers by presenting itself as disguised binaries that masquerade as video game installers.

Attack Regions



Attack Details

#1 A remote access trojan, known as Xeno RAT, has been candidly shared on GitHub by its developer, identified as moom825. Xeno-RAT has been actively circulating in the threat landscape for the past few months, gaining popularity due to its open-source nature and availability on development and version control hosting services, as well as hack forums.

#2 Various groups and individuals have embraced this malware for drive-by-download campaigns. It is noteworthy that moom825 is not only the creator of Xeno RAT but also the mind behind another C#-based remote access trojan named DiscordRAT 2.0. Xeno RAT, developed in C#, is compatible with Windows 10 and Windows 11 operating systems.

#3 While the primary targets of this threat are currently consumers, who fall prey to Xeno-RAT binaries masquerading as popular video game installers, enterprise customers are not immune to its menace. The primary delivery method involves a disguised shortcut file posing as a WhatsApp screenshot, acting as a downloader distributed through the Discord content delivery network (CDN).

#4 The Xeno RAT Server boasts a builder module that facilitates the creation of customized malware versions. This malware exhibits advanced functionalities, featuring a SOCKS5 reverse proxy, real-time audio recording capabilities, and integration of a hidden virtual network computing (hVNC).

#5 It allows attackers to access the webcam, engage in live microphone surveillance, perform keylogging, control the screen, and execute other intrusive actions on an infected computer. Xeno RAT follows a multi-stage sequence, leveraging DLL side-loading. The developer also pledges to continuously provide updates over time, underscoring the growing trend of easily accessible and cost-free malware contributing to the rise in RAT-based campaigns.

Recommendations

Continuous Monitoring and Analysis: Establish continuous monitoring and analysis protocols to promptly detect any unusual network behavior, potentially indicating a long-term cyber espionage operation.

Network Segmentation: Employ network segmentation to isolate critical systems and sensitive data, limiting the lateral movement of an attacker within the network in case of a successful infiltration.

Disable Unnecessary Services: Review and disable unnecessary services and features on systems to minimize potential attack vectors. Restrict user privileges to limit the impact of potential breaches.

Heighten Awareness: Familiarize yourself with common social engineering tactics and deceptive strategies employed by threat actors. Knowing the signs of malicious activity can help you avoid falling victim to scams.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0007 Discovery	TA0009 Collection	TA0011 Command and Control	TA0010 Exfiltration
T1204.001 Malicious Link	T1204.002 Malicious File	T1622 Debugger Evasion	T1497 Virtualization/Sandbox Evasion
T1055 Process Injection	T1071.001 Web Protocols	T1574.002 DLL Side-Loading	T1059.003 Windows Command Shell
T1056.001 Keylogging	T1113 Screen Capture	T1125 Video Capture	T1053.005 Scheduled Task
T1041 Exfiltration Over C2 Channel	T1036 Masquerading	T1001 Data Obfuscation	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	13b1d354ac2649b309b0d9229def8091, 6f9e84087cabbb9aaa7d8aba43a84dcf, 7704241dd8770b11b50b1448647197a5, 0aa5930aa736636fd95907328d47ea45
SHA256	848020d2e8bacd35c71b78e1a81c669c9dc63c78dd3db5a97200fc87aeb44c3c, 4d0d8c2696588ff74fe7d9f8c2097fddd665308fccf16ffea23b9741a261b1c0, 1762536a663879d5fb8a94c1d145331e1d001fb27f787d79691f9f8208fc68f2, 96b091ce5d06afd11ee5ad911566645dbe32bfe1da2269a3d3ef8d3fa0014689
IPv4	45[.]61[.]139[.]51
Domain	internal-liveapps[.]online

References

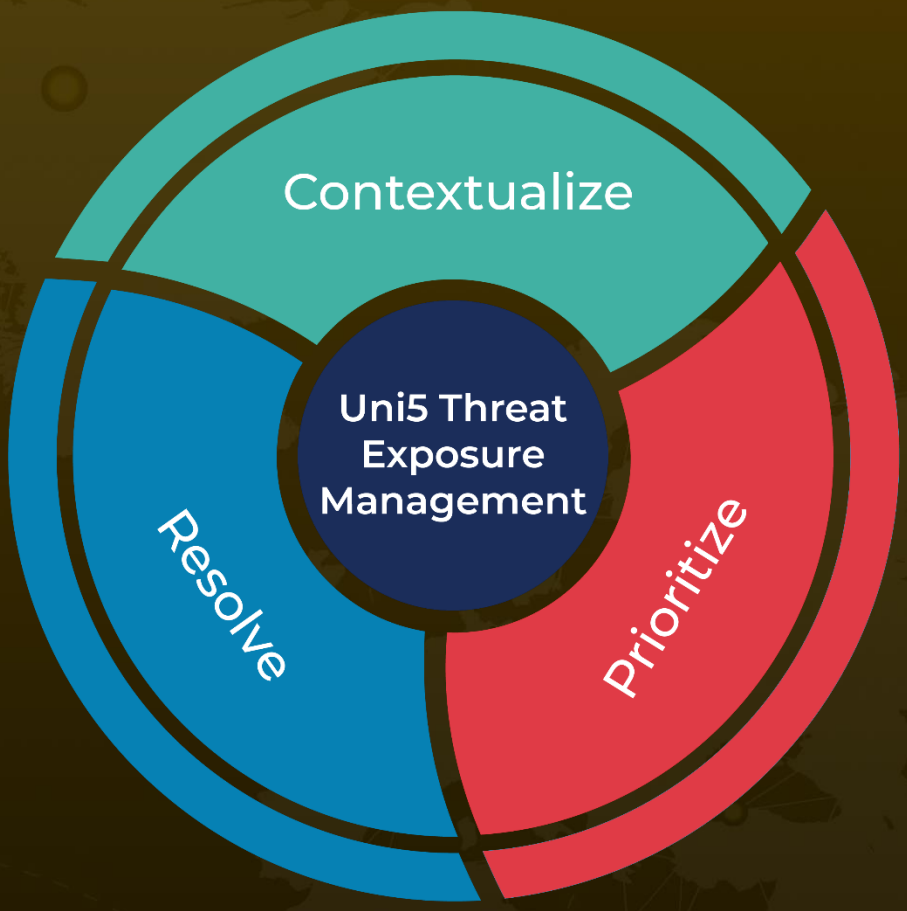
https://www.cyfirma.com/outofband/xeno-rat-a-new-remote-access-trojan-with-advance-capabilities/

https://github.com/moom825/xeno-rat

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

February 28, 2024 • 3:00 AM

More at www.hivepro.com