Hive Pro®

Threat Level

Red

HiveForce Labs

# THREAT ADVISORY

## ATTACK REPORT

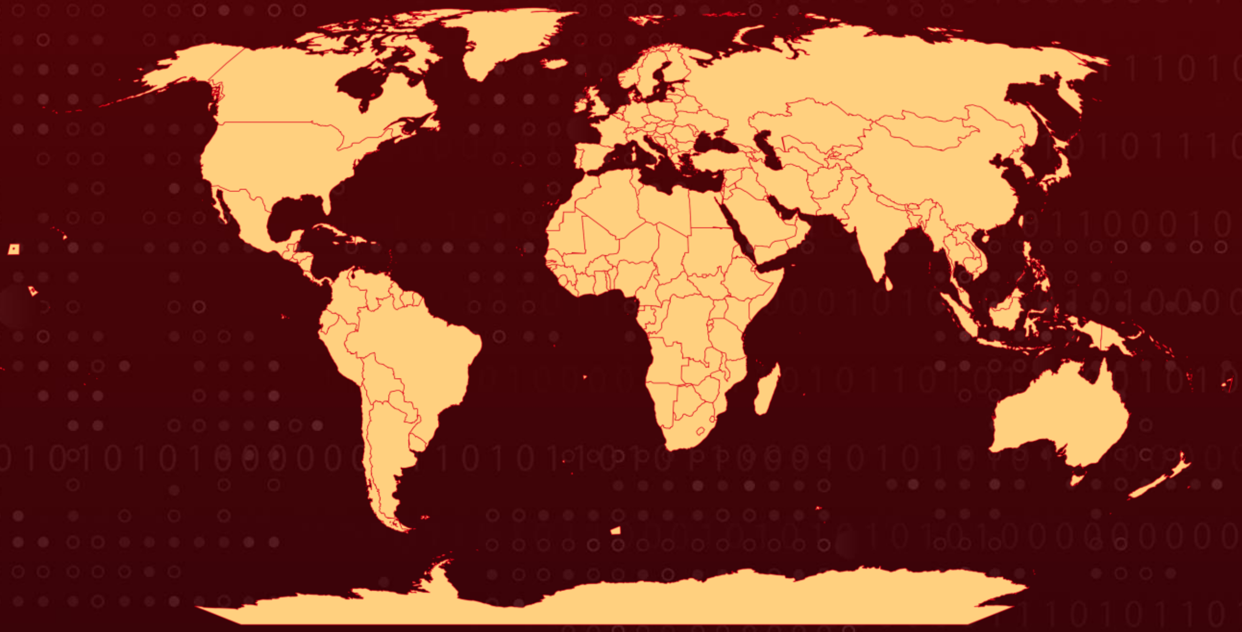
# SeroXen RAT Leverages NuGet Packages

| Date of Publication | Admiralty Code | TA Number |
|---|---|---|
| October 13, 2023 | A1 | TA2023416 |

# Summary

**Attack Began:** October 6, 2023
**Attack Region:** Worldwide
**Malware:** SeroXen RAT
**Attack:** Several malicious packages have been detected in NuGet, a widely used package manager for the .NET Framework. These packages utilized typosquatting methods to masquerade as legitimate ones and were discovered distributing the SeroXen RAT malware.

## Attack Regions



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

# Attack Details

#1

A malicious package was discovered on the NuGet package manager for the .NET Framework. The package was designed as a typosquatting attempt to impersonate a legitimate package as Pathoschild.Stardew.ModBuildConfig. However, the malicious package distributed a remote access trojan (RAT) known as SeroXen RAT. While the genuine package, "Pathoschild.Stardew.ModBuildConfig," has received nearly 79,000 downloads to date, the malicious version of the package, published on October 6, 2023, artificially inflated its download count to surpass 100,000 downloads.

#2

SeroXen RAT, marketed as a user-friendly Remote Access Trojan (RAT), is available for purchase on a dedicated website. Its distinctive feature lies in its fileless nature, making it highly effective at evading detection. SeroXen RAT harnesses the power of various open-source projects, integrating components from Quasar RAT, r77-rootkit, and the NirCmd command-line utility. Such RATs pose serious security threats, enabling unauthorized remote access and control, potentially resulting in data theft, system compromise, and other malicious activities.

#3

The attack chain begins during the installation of the package, facilitated by a script named "init.ps1". This script is specifically designed to execute code without raising any warning alerts and enables them to trigger malicious activities on the system during the package installation process.

#4

The PowerShell script retrieves another heavily obfuscated file named "x.bin" from a remote server. This Batch script is responsible for creating and running another PowerShell script, which downloads and deploy final payload, SeroXen RAT. This multi-layered approach is used to obfuscate the attack and increase the chances of successful deployment of the remote access trojan.

#5

In addition, six other deceptive packages on NuGet platform were found to be deploying SeroXen. Four of these packages masquerade as libraries related to various cryptocurrency services, including well-known names like Kraken, KuCoin, Solana, and Monero. These deceptive packages mimic popular cryptocurrency projects, exchanges, and platforms, even featuring official logos in an attempt to deceive users. However, their true purpose is to distribute the SeroXen RAT. This discovery underscores the fact that threat actors are actively exploiting open-source ecosystems and specifically targeting the developers who rely on them.

# Recommendations

**Download Packages from Official Websites:** Always download software packages from the official website of the vendor or developer. Verify the website's URL to make sure it's the correct and official domain.

**Remain vigilant:** It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

**Educate Your Users:** Make your users aware of the possibility of typosquatting and advise them to check the URL before entering sensitive information and emphasize the importance of verifying the legitimacy of websites by checking URLs carefully.

**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.

**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<br>Execution | TA0003<br>Persistence | TA0004<br>Privilege Escalation | TA0009<br>Collection |
| TA0011<br>Command and Control | TA0005<br>Defense Evasion | TA0006<br>Credential Access | TA0007<br>Discovery |
| TA0008<br>Lateral Movement | T1059<br>Command and Scripting Interpreter | T1059.003<br>Windows Command Shell | T1547<br>Boot or Logon Autostart Execution |
| T1547.001<br>Registry Run Keys / Startup Folder | T1548<br>Abuse Elevation Control Mechanism | T1548.002<br>Bypass User Account Control | T1140<br>Deobfuscate/Decode Files or Information |

| | | | |
|---|---|---|---|
| **T1005**<br>Data from Local System | **T1105**<br>Ingress Tool Transfer | **T1053**<br>Scheduled Task/Job | **T1053.005**<br>Scheduled Task |
| **T1112**<br>Modify Registry | **T1553**<br>Subvert Trust Controls | **T1553.002**<br>Code Signing | **T1564**<br>Hide Artifacts |
| **T1564.001**<br>Hidden Files and Directories | **T1564.003**<br>Hidden Window | **T1552**<br>Unsecured Credentials | **T1552.001**<br>Credentials In Files |
| **T1555**<br>Credentials from Password Stores | **T1555.003**<br>Credentials from Web Browsers | **T1016**<br>System Network Configuration Discovery | **T1033**<br>System Owner/User Discovery |
| **T1082**<br>System Information Discovery | **T1614**<br>System Location Discovery | **T1021**<br>Remote Services | **T1021.001**<br>Remote Desktop Protocol |
| **T1056**<br>Input Capture | **T1056.001**<br>Keylogging | **T1125**<br>Video Capture | **T1090**<br>Proxy |
| **T1095**<br>Non-Application Layer Protocol | **T1571**<br>Non-Standard Port | **T1573**<br>Encrypted Channel | **T1573.001**<br>Symmetric Cryptography |

## Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| SHA256 | e7dc6a2f0c65a2c6f3d7cc2a11c3fd2acb4e23af1e55a8769366766ee22278c3,<br>8bf56c92865fade8d06d4a57e1d049bccd3041842b2a1c71503a29729a71073d,<br>075acd923103e731e91140e663756699e7379a7f63ea31487434ce04cca02b02,<br>4c6e90e178396d000b5dd5c5bb2b9ae5bbbca5986f26ffad2a6bd0845b6b2c83,<br>050efb70d521f74a42dcd63c703900433b03cf138fcfa1812705c8cb37deb1ea,<br>a840fb6ea2354c5bdd1b531aa548620ed7c962a4241e4a384b03939eca8345b8,<br>5bcebf01c55b24ba2097f86c5074898ff8f04aca40064903d3afc2ca0593dde2,<br>0f0e9dfbe8a36d5a2447c1a0ae3af05779088329e7a796d17aba97fd233c3592,<br>9936d687086d0adfd38efa1304ad52f1007fb57027ebcfa2ca243cab7ff77ee8 |

| TYPE | VALUE |
|---|---|
| SHA1 | 618bd8c29d1698b69970684d55bc29406ccfa2c8 |
| MD5 | d9def0536fac4b4ad965c17eab2f6ff3 |
| Packages | Kraken.Exchange,<br>KucoinExchange.Net,<br>SolanaWallet,<br>Modern.Winform.UI,<br>Monero,<br>DiscordsRpc |

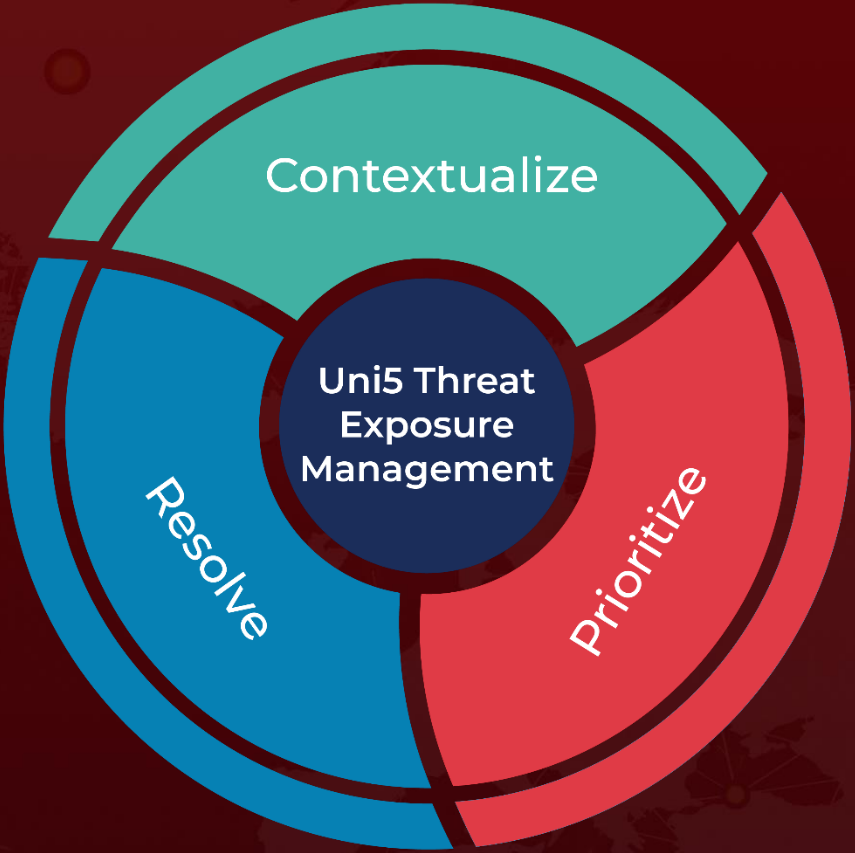
## References

https://blog.phylum.io/phylum-discovers-seroxen-rat-in-typosquatted-nuget-package/

# 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 13, 2023 • 6:00 AM**

More at www.hivepro.com