Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

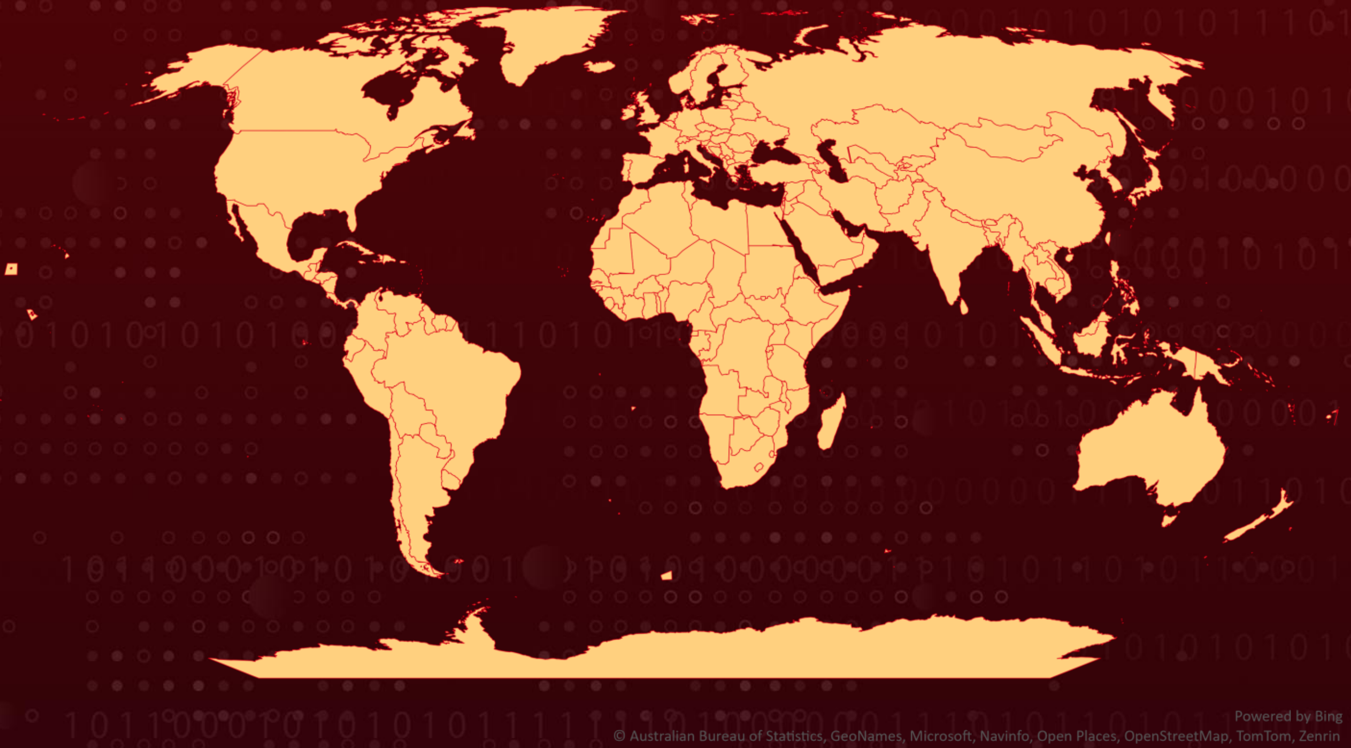
Rhadamanthys Stealer Version 0.5.0 Upgrade Overview

Date of Publication	Admiralty Code	TA Number
December 15, 2023	A1	TA2023507

Summary

Attack Began: December 2023
Attack Region: Worldwide
Malware: Rhadamanthys stealer
Attack: Rhadamanthys, the information-stealing malware, has taken a significant leap with its v0.5.0 upgrade, introducing expanded stealing features, raw syscalls, and an enhanced loader design, showcasing advanced evasion techniques. Its modular architecture allows for continuous updates, showcasing improved loader design and enhanced spying functionalities.

Attack Regions


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

Attack Details

#1 The Rhadamanthys stealer is a sophisticated, multi-layered malware available on the black market, regularly updated by its author. The recent release of version 0.5.0 introduces expanded stealing capabilities, general-purpose spying functions, and a plugin system for customization. The malware employs custom executable formats (XS1 and XS2) for its modules.

#2 In version 0.5.0, the initial loader undergoes changes, with an added check for executable names to evade sandbox analysis. The loader contains configuration data and unpacks additional modules. The second-stage loader (XS1) remains consistent in format but shows enhancements. Notably, the use of Thread Local Storage (TLS) for temporary buffers is introduced for string deobfuscation.

#3 The malware employs raw syscalls, a technique to evade monitoring and function hooking, with a specific implementation using Heaven's Gate for 32-bit processes on 64-bit Windows. The execution flow involves preparing and obfuscating the downloading of stealers from a command-and-control server (C2). The malware uses various modules to check the environment and hinder analysis.

#4 Depending on settings, the malware can load the next modules into the current process or inject itself into a new process. The restart flag causes the main loader module to run twice with different execution paths. The first path involves injecting the malware into a new process, while the second path, executed inside the new process, deletes the original file and loads additional modules from the package. The netclient module is then used to connect to the C2 and download the next package with the stealer modules.

#5 The malware's modular architecture allows it to evolve, introducing a newer version 0.5.1 with additional features, such as a Clipper plugin. The sophistication of its design involves string encryption, communication through pipes, and the ability to disable security features. Overall, Rhadamanthys 0.5.0 demonstrates advanced evasion techniques, improved loader design, and enhanced capabilities for stealing information and spying.

Recommendations

Update Security Software: Ensure that all security software, including antivirus and anti-malware tools, is up-to-date. Regularly check for updates and patches to enhance protection against evolving threats like Rhadamanthys.

Network Monitoring: Implement robust network monitoring solutions to detect and block malicious activities. Pay special attention to unusual network traffic patterns or connections, as these may indicate a Rhadamanthys infection attempting to communicate with a command-and-control server.

Regular Backups: Regularly back up critical data and ensure that backup systems are secure. In the event of a Rhadamanthys infection or any other malware attack, having up-to-date backups can facilitate quick data recovery and reduce the impact of data loss.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0009 Collection	TA0006 Credential Access
TA0043 Reconnaissance	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0011 Command and Control	T1566.001 Spearphishing Attachment	T1204.002 Malicious File	T1204 User Execution
T1497 Virtualization/Sandbox Evasion	T1055 Process Injection	T1027 Obfuscated Files or Information	T1573.001 Symmetric Cryptography
T1140 Deobfuscate/Decode Files or Information	T1059.001 PowerShell	T1059 Command and Scripting Interpreter	T1606 Forge Web Credentials
T1056.001 Keylogging	T1056 Input Capture	T1592 Gather Victim Host Information	T1566 Phishing

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	a87032195e38892b351641e08c81b92a1ea888c3c74a0c7464160e86613c4476, 50b1f29ccdf727805a793a9dac61371981334c4a99f8fae85613b3ee57b186d2, 4fd469d08c051d6997f0471d91ccf96c173d27c8cff5bd70c3f2c5008faa786f, bb8bbcc948e8dca2e5a0270c41c062a29994a2d9b51e820ed74d9b6e2a01ddcf, 6ed3ac428961b350d4c8094a10d7685578ce02c6cd41cc7f98d8eeb361f0ee38, 01609701a3ea751dc2323bec8018e11742714dc1b1c2dcb39282f3c4a4537c7d, f82ec2246dde81ca9edb69fb9c7ce3f7101f5ffcdc3bdb86fea2a5373fb026fb, fcb00beaa88f7827999856ba12302086cadbc1252261d64379172f2927a6760e, 3d010e3fce1b2c9ab5b8cc125be812e63b661ddcbde40509a49118c2330ef9d0, 5890b47df83b992e2bd8617d0ae4d492663ca870ed63ce47bb82f00fa3b82cf9, a905226a2486ccc158d44cf4c1728e103472825fb189e05c17d998b9f5534d63, ed713454c20844522304c49cfe25fe1490418c300e5ab0c9fca431ede1e91d7b, 2b6faa98a7617db2bd9e70c0ce050588c8b856484d97d46b50ed3bb94bdd62f7, 22a67f510dfb7ca822b5720b89cd81abfa5e63fefa1cdc7e266fbcbb0698db33, f1f33618bbb8551b183304ddb18e0a8b8200642ec52d5b72d3c75a00cdb99fd4, ee4a487e78f23f5dffc35e73aeb9602514ebd885eb97460dd26635f67847bd16, ecab35dfa6b03fed96bb69ffcecd11a29113278f53c6a84adced1167b66abe62, 633b0fe4f3d2bfb18d4ad648ff223fe6763397daa033e9c5d79f2cae89a6c3b2

References

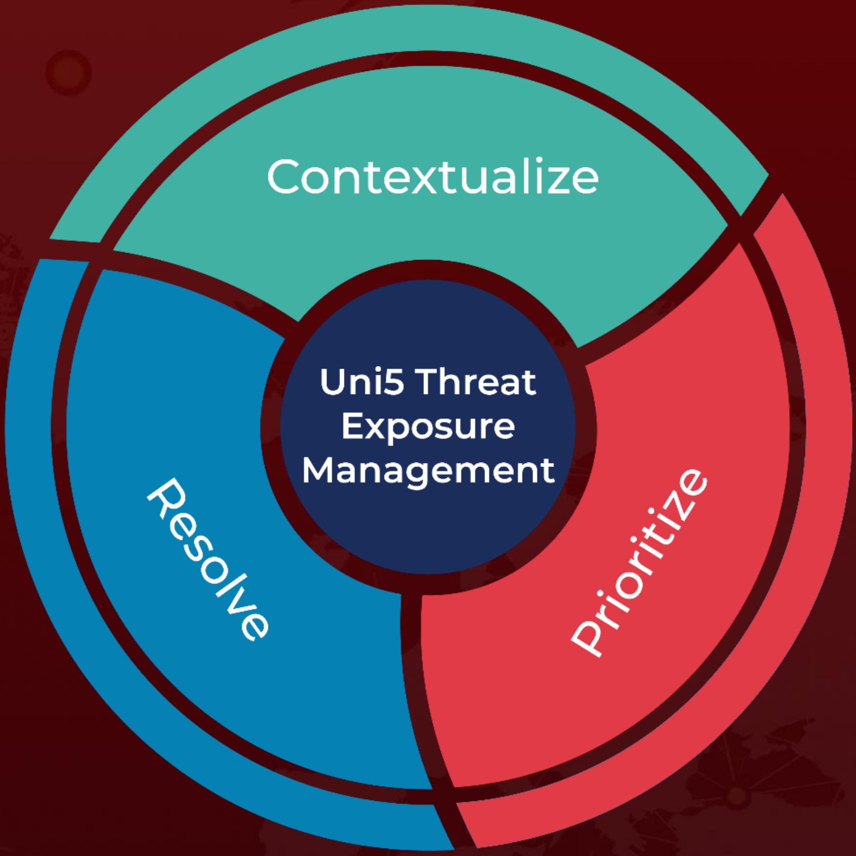
https://research.checkpoint.com/2023/rhadamanthys-v0-5-0-a-deep-dive-into-the-stealers-components/

https://www.hivepro.com/threat-advisory/rhadamanthys-a-new-evasive-information-stealer/

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

December 15, 2023 • 5:30 AM

More at www.hivepro.com