Dec 14 2023

NETMANAGEIT

Intelligence Report

Rhadamanthys v0.5.0 - a deep dive into the stealer's components

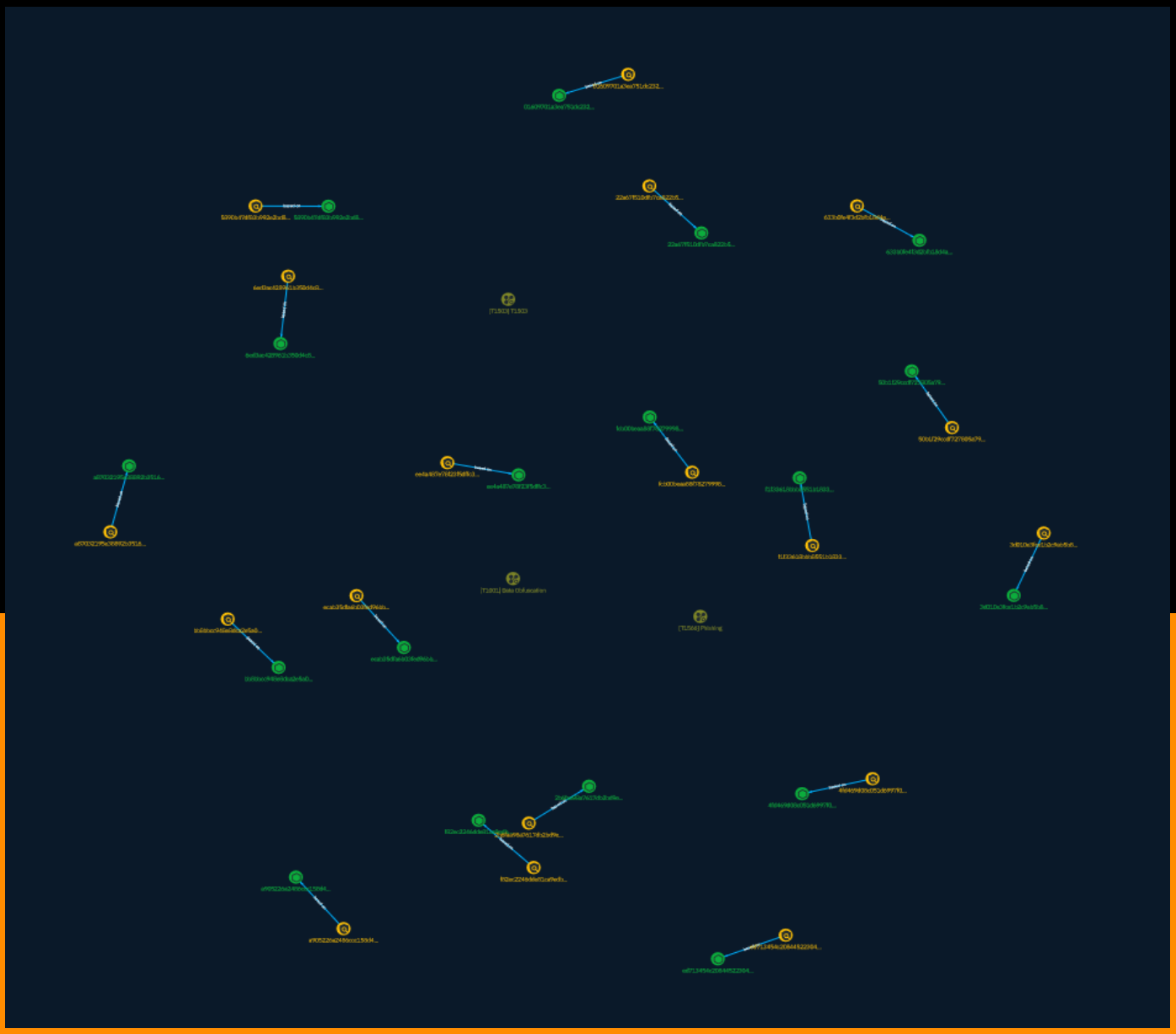

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Rhadamanthys is a well-designed, modular stealer. In this article, Check Point Research presented some details of its implementation, showing the incorporated techniques and execution flow. Although the core component comes with a lot of interesting built-in features, the power of this malware lies in its extensibility. The currently analyzed version 0.5.0 supports multiple scripting languages, from LUA (whose interpreter is built-in to the main module) to PowerShell and other scripting languages, that are supported via an additional module.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Content

N/A

Attack-Pattern

Name
Phishing
ID
T1566
Description
Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name
Data Obfuscation
ID
T1001
Description
Adversaries may obfuscate command and control traffic to make it more difficult to detect. Command and control (C2) communications are hidden (but not necessarily encrypted) in an attempt to make the content more difficult to discover or decipher and to make the communication less conspicuous and hide commands from being seen. This encompasses many methods, such as adding junk data to protocol traffic, using steganography, or impersonating legitimate protocols.
Name
T1503
ID
T1503

Indicator

Name
50b1f29ccdf727805a793a9dac61371981334c4a99f8fae85613b3ee57b186d2
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '50b1f29ccdf727805a793a9dac61371981334c4a99f8fae85613b3ee57b186d2']
Name
ee4a487e78f23f5dffc35e73aeb9602514ebd885eb97460dd26635f67847bd16
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'ee4a487e78f23f5dffc35e73aeb9602514ebd885eb97460dd26635f67847bd16']
Name

633b0fe4f3d2bfb18d4ad648ff223fe6763397daa033e9c5d79f2cae89a6c3b2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '633b0fe4f3d2bfb18d4ad648ff223fe6763397daa033e9c5d79f2cae89a6c3b2']

Name

f1f33618bbb8551b183304ddb18e0a8b8200642ec52d5b72d3c75a00cdb99fd4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f1f33618bbb8551b183304ddb18e0a8b8200642ec52d5b72d3c75a00cdb99fd4']

Name

ecab35dfa6b03fed96bb69ffcecd11a29113278f53c6a84adced1167b66abe62

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ecab35dfa6b03fed96bb69ffcecd11a29113278f53c6a84adced1167b66abe62']

Name

3d010e3fce1b2c9ab5b8cc125be812e63b661ddcbde40509a49118c2330ef9d0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3d010e3fce1b2c9ab5b8cc125be812e63b661ddcbde40509a49118c2330ef9d0']

Name

a905226a2486ccc158d44cf4c1728e103472825fb189e05c17d998b9f5534d63

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a905226a2486ccc158d44cf4c1728e103472825fb189e05c17d998b9f5534d63']

Name

6ed3ac428961b350d4c8094a10d7685578ce02c6cd41cc7f98d8eeb361f0ee38

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6ed3ac428961b350d4c8094a10d7685578ce02c6cd41cc7f98d8eeb361f0ee38']

Name

4fd469d08c051d6997f0471d91ccf96c173d27c8cff5bd70c3f2c5008faa786f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4fd469d08c051d6997f0471d91ccf96c173d27c8cff5bd70c3f2c5008faa786f']

Name

a87032195e38892b351641e08c81b92a1ea888c3c74a0c7464160e86613c4476

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a87032195e38892b351641e08c81b92a1ea888c3c74a0c7464160e86613c4476']

Name

01609701a3ea751dc2323bec8018e11742714dc1b1c2dcb39282f3c4a4537c7d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '01609701a3ea751dc2323bec8018e11742714dc1b1c2dcb39282f3c4a4537c7d']

Name

f82ec2246dde81ca9edb69fb9c7ce3f7101f5ffcdc3bdb86fea2a5373fb026fb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f82ec2246dde81ca9edb69fb9c7ce3f7101f5ffcdc3bdb86fea2a5373fb026fb']

Name

5890b47df83b992e2bd8617d0ae4d492663ca870ed63ce47bb82f00fa3b82cf9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5890b47df83b992e2bd8617d0ae4d492663ca870ed63ce47bb82f00fa3b82cf9']

Name

fcb00beaa88f7827999856ba12302086cadbc1252261d64379172f2927a6760e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fcb00beaa88f7827999856ba12302086cadbc1252261d64379172f2927a6760e']

Name

2b6faa98a7617db2bd9e70c0ce050588c8b856484d97d46b50ed3bb94bdd62f7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2b6faa98a7617db2bd9e70c0ce050588c8b856484d97d46b50ed3bb94bdd62f7']

Name

22a67f510dfb7ca822b5720b89cd81abfa5e63fefa1cdc7e266fbcbb0698db33

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '22a67f510dfb7ca822b5720b89cd81abfa5e63fefa1cdc7e266fbcbb0698db33']

Name

ed713454c20844522304c49cfe25fe1490418c300e5ab0c9fca431ede1e91d7b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ed713454c20844522304c49cfe25fe1490418c300e5ab0c9fca431ede1e91d7b']

Name

bb8bbcc948e8dca2e5a0270c41c062a29994a2d9b51e820ed74d9b6e2a01ddcf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bb8bbcc948e8dca2e5a0270c41c062a29994a2d9b51e820ed74d9b6e2a01ddcf']

StixFile

Value
bb8bbcc948e8dca2e5a0270c41c062a29994a2d9b51e820ed74d9b6e2a01ddcf
f82ec2246dde81ca9edb69fb9c7ce3f7101f5ffcdc3bdb86fea2a5373fb026fb
22a67f510dfb7ca822b5720b89cd81abfa5e63fefa1cdc7e266fbcbb0698db33
4fd469d08c051d6997f0471d91ccf96c173d27c8cff5bd70c3f2c5008faa786f
5890b47df83b992e2bd8617d0ae4d492663ca870ed63ce47bb82f00fa3b82cf9
2b6faa98a7617db2bd9e70c0ce050588c8b856484d97d46b50ed3bb94bdd62f7
6ed3ac428961b350d4c8094a10d7685578ce02c6cd41cc7f98d8eeb361f0ee38
50b1f29ccdf727805a793a9dac61371981334c4a99f8fae85613b3ee57b186d2
ecab35dfa6b03fed96bb69ffcecd11a29113278f53c6a84adced1167b66abe62
a87032195e38892b351641e08c81b92a1ea888c3c74a0c7464160e86613c4476
633b0fe4f3d2bfb18d4ad648ff223fe6763397daa033e9c5d79f2cae89a6c3b2
a905226a2486ccc158d44cf4c1728e103472825fb189e05c17d998b9f5534d63
f1f33618bbb8551b183304ddb18e0a8b8200642ec52d5b72d3c75a00cdb99fd4

3d010e3fce1b2c9ab5b8cc125be812e63b661ddcbde40509a49118c2330ef9d0

fcb00beaa88f7827999856ba12302086cadbc1252261d64379172f2927a6760e

ee4a487e78f23f5dffc35e73aeb9602514ebd885eb97460dd26635f67847bd16

ed713454c20844522304c49cfe25fe1490418c300e5ab0c9fca431ede1e91d7b

01609701a3ea751dc2323bec8018e11742714dc1b1c2dcb39282f3c4a4537c7d

External References

- https://otx.alienvault.com/pulse/657b35750b6b5bb04a2dc2b7
- https://research.checkpoint.com/2023/rhadamanthys-v0-5-0-a-deep-dive-into-the-stealers-components/