Jul 25 2023

NETMANAGEIT

Intelligence Report

New Reptile Rootkit Malware Attacking Linux Systems Using Port Knocking

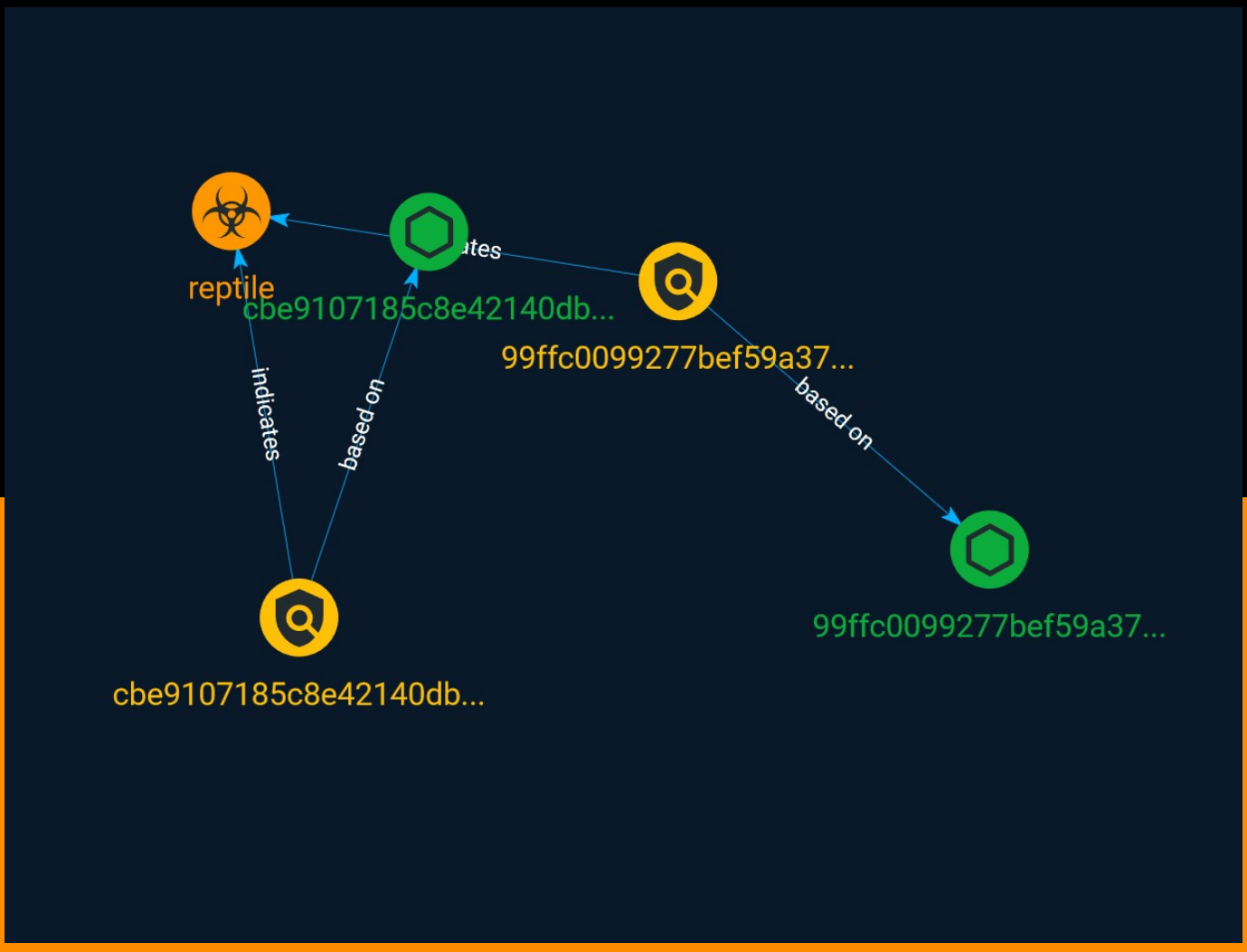

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Reptile is a kernel module rootkit for Linux systems released as open source on GitHub. A rootkit is a malicious code that has the ability to hide itself or other malicious codes, and its targets are mainly files, processes, and network communication. The hiding functions supported by Reptile include files and directories, contents of files, processes, and network traffic in addition to the kernel module itself.

Confidence

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

15 / 100

Indicator

Name

99ffc0099277bef59a37a4cfcf4cdd71df13ad33d1c7bf943dc87f803e75dd2c

Description

is__elf SHA256 of 246c5bec21c0a87657786d5d9b53fe38

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '99ffc0099277bef59a37a4cfcf4cdd71df13ad33d1c7bf943dc87f803e75dd2c']

Name

cbe9107185c8e42140dbd1294d8c20849134dd122cc64348f1bfcc90401379ec

Description

is__elf SHA256 of 5b788feef374bbac8a572adaf1da3d38

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cbe9107185c8e42140dbd1294d8c20849134dd122cc64348f1bfcc90401379ec']

Malware

Name
reptile

StixFile

Value
cbe9107185c8e42140dbd1294d8c20849134dd122cc64348f1bfcc90401379ec
99ffc0099277bef59a37a4cfcf4cdd71df13ad33d1c7bf943dc87f803e75dd2c

External References

- https://otx.alienvault.com/pulse/64bfcca7dbe2f3ba4226f3a4
- https://asec.ahnlab.com/ko/55379/