Dec 07 2023

NETMANAGEIT

Intelligence Report

Curse of the Krasue: New Linux Remote Access Trojan targets Thailand

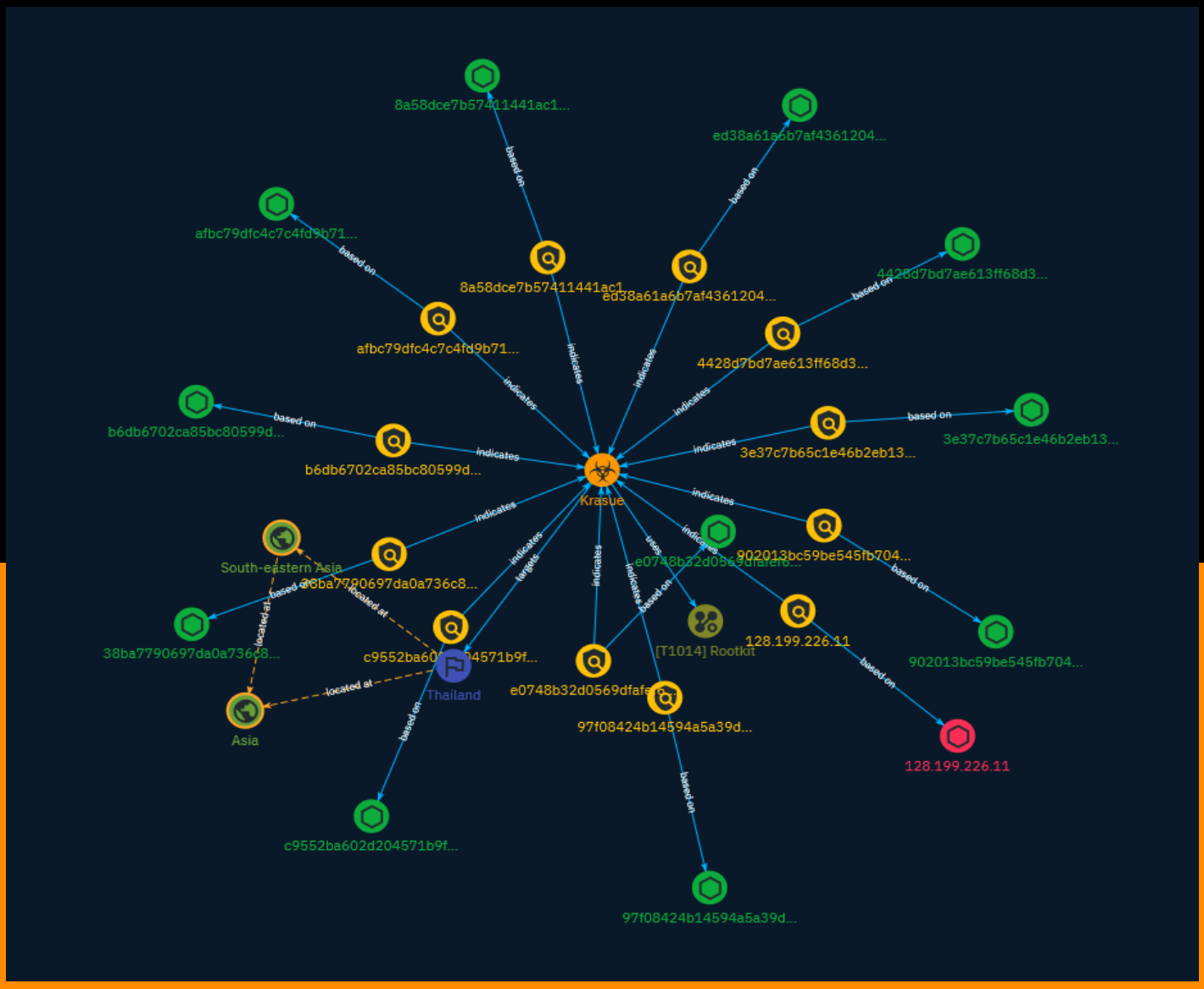

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Researchers offer their insights on the new RAT used in attacks against Thai companies.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name
Rootkit
ID
T1014
Description
Adversaries may use rootkits to hide the presence of programs, files, network connections, services, drivers, and other system components. Rootkits are programs that hide the existence of malware by intercepting/hooking and modifying operating system API calls that supply system information. (Citation: Symantec Windows Rootkits) Rootkits or rootkit enabling functionality may reside at the user or kernel level in the operating system or lower, to include a hypervisor, Master Boot Record, or [System Firmware](https://attack.mitre.org/techniques/T1542/001). (Citation: Wikipedia Rootkit) Rootkits have been seen for Windows, Linux, and Mac OS X systems. (Citation: CrowdStrike Linux Rootkit) (Citation: BlackHat Mac OSX Rootkit)

Indicator

Name
c9552ba602d204571b9f98bd16f60b6f4534b3ad32b4fc8b3b4ab79f2bf371e5
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'c9552ba602d204571b9f98bd16f60b6f4534b3ad32b4fc8b3b4ab79f2bf371e5']
Name
902013bc59be545fb70407e8883717453fb423a7a7209e119f112ff6771e44cc
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '902013bc59be545fb70407e8883717453fb423a7a7209e119f112ff6771e44cc']
Name

afbc79dfc4c7c4fd9b71b5fea23ef12adf0b84b1af22a993ecf91f3d829967a4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'afbc79dfc4c7c4fd9b71b5fea23ef12adf0b84b1af22a993ecf91f3d829967a4']

Name

3e37c7b65c1e46b2eb132f98f65c711b4169c6caeeaecc799abbda122c0c4a59

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3e37c7b65c1e46b2eb132f98f65c711b4169c6caeeaecc799abbda122c0c4a59']

Name

97f08424b14594a5a39d214bb97823690f1086c78fd877558761afe0a032b772

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '97f08424b14594a5a39d214bb97823690f1086c78fd877558761afe0a032b772']

Name

38ba7790697da0a736c80fd9a04731b8b0bac675cca065cfd42a56dde644e353

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '38ba7790697da0a736c80fd9a04731b8b0bac675cca065cfd42a56dde644e353']

Name

4428d7bd7ae613ff68d3b1b8e80d564e2f69208695f7ab6e5fdb6946cc46b5e1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4428d7bd7ae613ff68d3b1b8e80d564e2f69208695f7ab6e5fdb6946cc46b5e1']

Name

e0748b32d0569dfafef6a8ffd3259edc6785902e73434e4b914e68fea86e6632

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e0748b32d0569dfafef6a8ffd3259edc6785902e73434e4b914e68fea86e6632']

Name

8a58dce7b57411441ac1fbff3062f5eb43a432304b2ba34ead60e9dd4dc94831

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8a58dce7b57411441ac1fbff3062f5eb43a432304b2ba34ead60e9dd4dc94831']

Name

128.199.226.11

Description

ISP: DigitalOcean, LLC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **80:** ``` HTTP/1.1 200 OK Server: openresty/1.13.6.1 Date: Mon, 04 Dec 2023 19:09:48 GMT Content-Type: text/html Content-Length: 562 Last-Modified: Mon, 13 Nov 2017 08:05:52 GMT Connection: keep-alive ETag: "5a095260-232" Accept-Ranges: bytes ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '128.199.226.11']

Name

b6db6702ca85bc80599d7f1d8b1a9b6dd56a8e87c55fc831dc9c689e54b8205d

Description

is__elf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b6db6702ca85bc80599d7f1d8b1a9b6dd56a8e87c55fc831dc9c689e54b8205d']

Name

ed38a61a6b7af436120465d352baa4cdf4ed8f01a7db7245b6254353e52f818f

Description

SUSP_ELF_LNX_UPX_Compressed_File

Pattern Type

stix

Pattern

```
[file:hashes.'SHA-256' =
'ed38a61a6b7af436120465d352baa4cdf4ed8f01a7db7245b6254353e52f818f']
```

Region

Name
Asia
Name
South-eastern Asia

Country

Name
Thailand

Malware

Name
Krasue

StixFile

Value
4428d7bd7ae613ff68d3b1b8e80d564e2f69208695f7ab6e5fdb6946cc46b5e1
b6db6702ca85bc80599d7f1d8b1a9b6dd56a8e87c55fc831dc9c689e54b8205d
3e37c7b65c1e46b2eb132f98f65c711b4169c6caeeaecc799abbda122c0c4a59
902013bc59be545fb70407e8883717453fb423a7a7209e119f112ff6771e44cc
8a58dce7b57411441ac1fbff3062f5eb43a432304b2ba34ead60e9dd4dc94831
97f08424b14594a5a39d214bb97823690f1086c78fd877558761afe0a032b772
afbc79dfc4c7c4fd9b71b5fea23ef12adf0b84b1af22a993ecf91f3d829967a4
ed38a61a6b7af436120465d352baa4cdf4ed8f01a7db7245b6254353e52f818f
38ba7790697da0a736c80fd9a04731b8b0bac675cca065cfd42a56dde644e353
e0748b32d0569dfafef6a8ffd3259edc6785902e73434e4b914e68fea86e6632
c9552ba602d204571b9f98bd16f60b6f4534b3ad32b4fc8b3b4ab79f2bf371e5

IPv4-Addr

Value
128.199.226.11

External References

- https://otx.alienvault.com/pulse/6571e00a8d289f24a448f0a4