Dec 06 2023

NETMANAGEIT

Intelligence Report

Analysis of a new macOS Trojan-Proxy

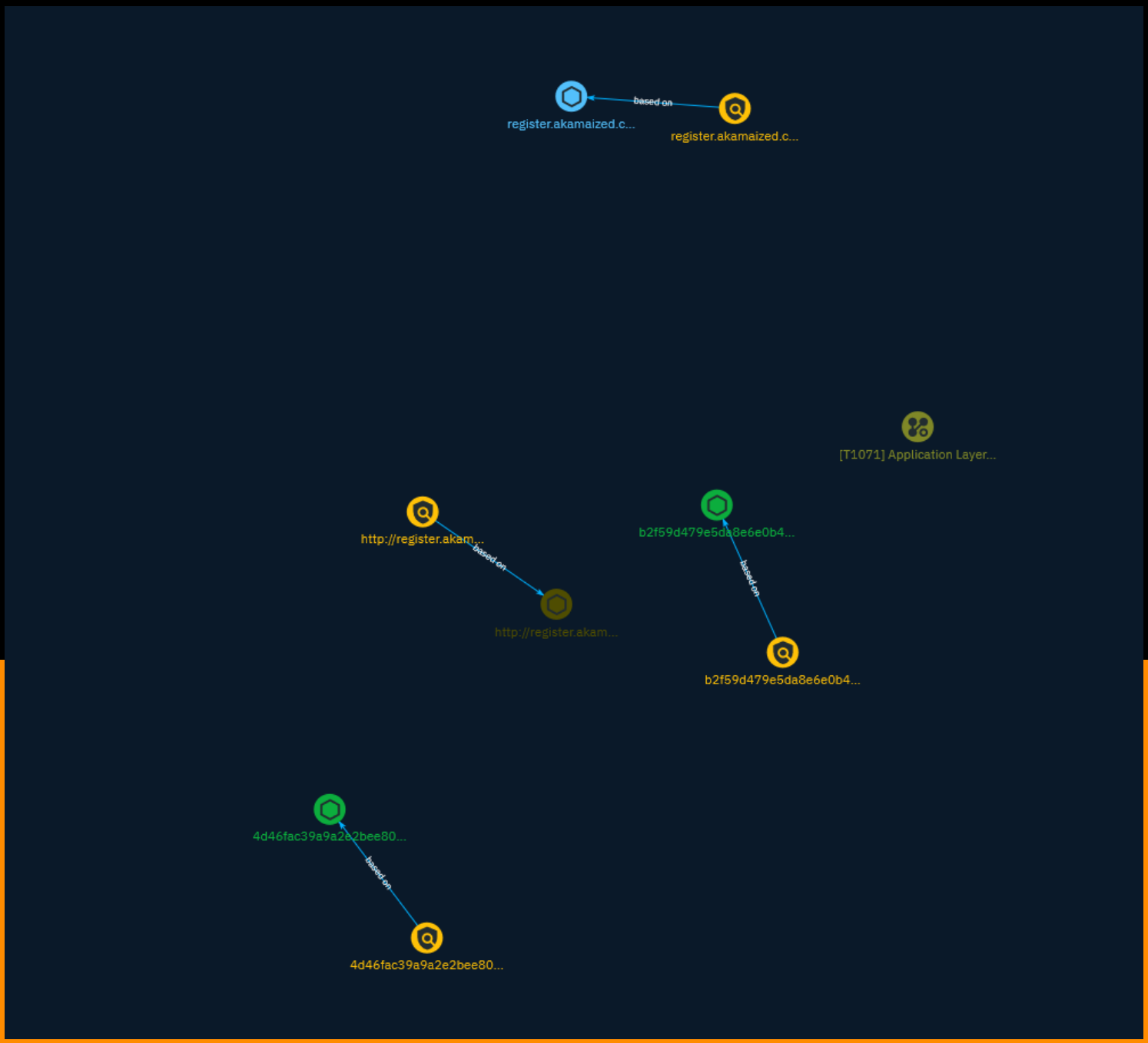

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Researchers recently discovered several cracked applications distributed by unauthorized websites and loaded with a Trojan-Proxy. Attackers can use this type of malware to gain money by building a proxy server network or to perform criminal acts on behalf of the victim: to launch attacks on websites, companies and individuals, buy guns, drugs, and other illicit goods.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name
Application Layer Protocol
ID
T1071
Description
Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.

Indicator

Name
b2f59d479e5da8e6e0b4ad67d34c781ef72d7b8253d4a543cc36a885f7809f07
Description
SHA256 of fb3c42ca1ff0ba96ac146c1672357994
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'b2f59d479e5da8e6e0b4ad67d34c781ef72d7b8253d4a543cc36a885f7809f07']
Name
http://register.akamaized.ca:6101/strvn
Pattern Type
stix
Pattern

[url:value = 'http://register.akamaized.ca:6101/strvn']

Name

register.akamaized.ca

Pattern Type

stix

Pattern

[hostname:value = 'register.akamaized.ca']

Name

4d46fac39a9a2e2bee806685b24245944e3dabae8e14a6389a6d9339e47a7154

Description

SHA256 of d605b5673ca89a767662a4a83662eaa0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4d46fac39a9a2e2bee806685b24245944e3dabae8e14a6389a6d9339e47a7154']

StixFile

Value
4d46fac39a9a2e2bee806685b24245944e3dabae8e14a6389a6d9339e47a7154
b2f59d479e5da8e6e0b4ad67d34c781ef72d7b8253d4a543cc36a885f7809f07

Hostname

Value
register.akamaized.ca

Url

Value
http://register.akamaized.ca:6101/strvn

External References

- https://otx.alienvault.com/pulse/65707986b5636647af655f97
- https://securelist.com/trojan-proxy-for-macos/111325/