Aug 24 2023

NETMANAGEIT

Intelligence Report

XLoader's Latest Trick | New macOS Variant Disguised as Signed OfficeNote App

Table of contents

Overview

Entities

Observables

External References

Overview

Description

XLoader has returned in a new form and without the dependencies. Written natively in the C and Objective C programming languages and signed with an Apple developer signature, XLoader is now masquerading as an office productivity app called ‘OfficeNote’.

Confidence

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

15 / 100

Indicator

Name
www.corkagenexus.com
Pattern Type
stix
Pattern
[hostname:value = 'www.corkagenexus.com']
Name
www.spv88.online
Pattern Type
stix
Pattern
[hostname:value = 'www.spv88.online']
Name
www.raveready.shop

Pattern Type
stix
Pattern
[hostname:value = 'www.raveready.shop']
Name
www.switchmerge.com
Pattern Type
stix
Pattern
[hostname:value = 'www.switchmerge.com']
Name
www.activ-ketodietakjsy620.cloud
Pattern Type
stix
Pattern
[hostname:value = 'www.activ-ketodietakjsy620.cloud']
Name
www.akrsnamchi.com

Pattern Type
stix
Pattern
[hostname:value = 'www.akrsnamchi.com']
Name
www.mommachic.com
Pattern Type
stix
Pattern
[hostname:value = 'www.mommachic.com']
Name
www.pinksugarpopmontana.com
Pattern Type
stix
Pattern
[hostname:value = 'www.pinksugarpopmontana.com']
Name
www.hatch.computer

Pattern Type
stix
Pattern
[hostname:value = 'www.hatch.computer']
Name
www.qq9122.com
Pattern Type
stix
Pattern
[hostname:value = 'www.qq9122.com']
Name
www.lushespets.com
Pattern Type
stix
Pattern
[hostname:value = 'www.lushespets.com']
Name
www.kiavisa.com

Pattern Type
stix
Pattern
[hostname:value = 'www.kiavisa.com']
Name
www.brioche-amsterdam.com
Pattern Type
stix
Pattern
[hostname:value = 'www.brioche-amsterdam.com']
Name
www.growind.info
Pattern Type
stix
Pattern
[hostname:value = 'www.growind.info']
Name
www.qhsbobfv.top

Pattern Type
stix
Pattern
[hostname:value = 'www.qhsbobfv.top']
Name
www.nationalrecoveryllc.com
Pattern Type
stix
Pattern
[hostname:value = 'www.nationalrecoveryllc.com']

Malware

Name
XLoader

Attack-Pattern

Name
T1503
ID
T1503
Name
Clipboard Data
ID
T1115
Description
Adversaries may collect data stored in the clipboard from users copying information within or between applications. For example, on Windows adversaries can access clipboard data by using `clip.exe` or `Get-Clipboard`.(Citation: MSDN Clipboard)(Citation: clip_win_server)(Citation: CISA_AA21_200B) Additionally, adversaries may monitor then replace users' clipboard with their data (e.g., [Transmitted Data Manipulation](https://attack.mitre.org/techniques/T1565/002)).(Citation: mining_ruby_reversinglabs) macOS and Linux also have commands, such as `pbpaste`, to grab clipboard contents.(Citation: Operating with EmPyre)
Name

Masquerading

ID

T1036

Description

Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site)

Hostname

Value
www.akrsnamchi.com
www.pinksugarpopmontana.com
www.lushespets.com
www.kiavisa.com
www.qq9122.com
www.raveready.shop
www.corkagenexus.com
www.growind.info
www.activ-ketodietakjsy620.cloud
www.spv88.online
www.hatch.computer
www.nationalrecoveryllc.com
www.qhsbobfv.top

www.brioche-amsterdam.com

www.mommachic.com

www.switchmerge.com

External References

- https://otx.alienvault.com/pulse/64e6226b9b630a2479f8fb89
- https://www.sentinelone.com/blog/xloaders-latest-trick-new-macos-variant-disguised-as-signed-officenote-app/