May 02 2024

NETMANAGEIT

Intelligence Report

macOS Adload Pivots Just Days After Apple's XProtect Clampdown

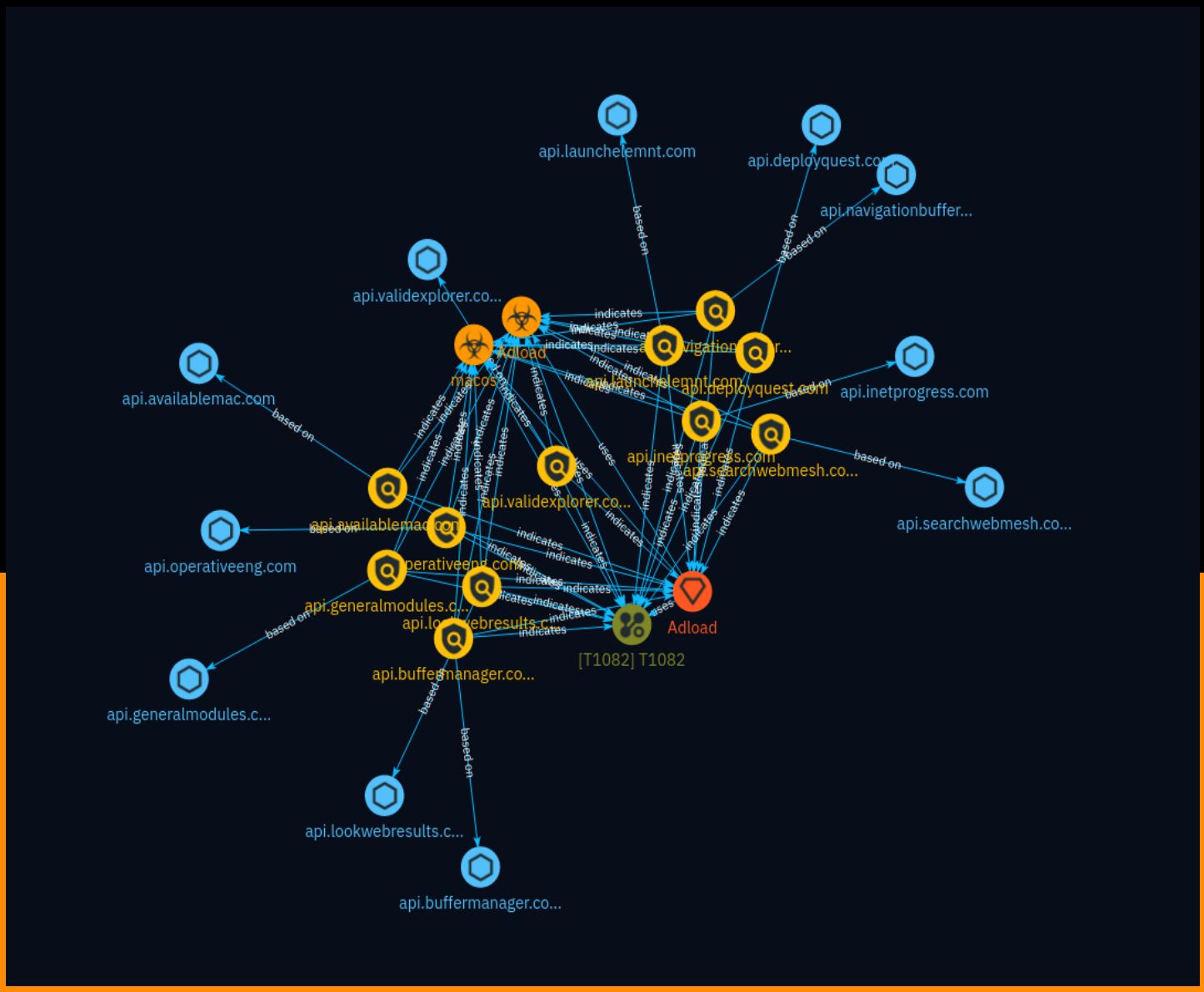

Table of contents

Overview

Entities

Observables

External References

Overview

Description

The report analyzes a new variant of the Adload adware that evades Apple's recent XProtect malware signature updates. Despite Apple adding 74 new rules targeting Adload in XProtect version 2192, the adware authors have rapidly modified their code to bypass these detections. The report examines a specific 4.55MB Intel x86_64 dropper sample that employs Go language components and connects to hardcoded domains for retrieving next-stage payloads. While undetected by most antivirus engines on VirusTotal, SentinelOne's multi-engine platform effectively identifies and blocks this Adload variant.

Confidence

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

100 / 100

Content

N/A

Indicator

Name
api.validexplorer.com
Pattern Type
stix
Pattern
[hostname:value = 'api.validexplorer.com']
Name
api.searchwebmesh.com
Pattern Type
stix
Pattern
[hostname:value = 'api.searchwebmesh.com']
Name
api.operativeeng.com

Pattern Type
stix
Pattern
[hostname:value = 'api.operativeeng.com']
Name
api.navigationbuffer.com
Pattern Type
stix
Pattern
[hostname:value = 'api.navigationbuffer.com']
Name
api.lookwebresults.com
Pattern Type
stix
Pattern
[hostname:value = 'api.lookwebresults.com']
Name
api.launchelemnt.com

Pattern Type
stix
Pattern
[hostname:value = 'api.launchelemnt.com']
Name
api.inetprogress.com
Pattern Type
stix
Pattern
[hostname:value = 'api.inetprogress.com']
Name
api.generalmodules.com
Pattern Type
stix
Pattern
[hostname:value = 'api.generalmodules.com']
Name
api.deployquest.com

Pattern Type
stix
Pattern
[hostname:value = 'api.deployquest.com']
Name
api.buffermanager.com
Pattern Type
stix
Pattern
[hostname:value = 'api.buffermanager.com']
Name
api.availablemac.com
Pattern Type
stix
Pattern
[hostname:value = 'api.availablemac.com']

Malware

Name
Adload

Name
macos

Intrusion-Set

Name
Adload

Attack-Pattern

Name
T1082
ID
T1082
Description
An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from [System Information Discovery](https://attack.mitre.org/techniques/T1082) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Tools such as [Systeminfo](https://attack.mitre.org/software/S0096) can be used to gather detailed system information. If running with privileged access, a breakdown of system data can be gathered through the `systemsetup` configuration tool on macOS. As an example, adversaries with user-level access can execute the `df -aH` command to obtain currently mounted disks and associated freely available space. Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather detailed system information (e.g. `show version`).(Citation: US-CERT-TA18-106A) [System Information Discovery](https://attack.mitre.org/techniques/T1082) combined with information gathered from other forms of discovery and reconnaissance can drive payload development and concealment.(Citation: OSX.FairyTale)(Citation: 20 macOS Common Tools and Techniques) Infrastructure as a Service (IaaS) cloud providers such as AWS, GCP, and Azure allow access to instance and virtual machine information via APIs. Successful authenticated API calls can return data such as the operating system platform and status of a particular instance or the model view of a virtual machine.(Citation: Amazon Describe Instance)(Citation: Google Instances Resource)(Citation: Microsoft Virutal Machine API)

Hostname

Value
api.validexplorer.com
api.searchwebmesh.com
api.operativeeng.com
api.navigationbuffer.com
api.lookwebresults.com
api.launchelemnt.com
api.inetprogress.com
api.generalmodules.com
api.deployquest.com
api.buffermanager.com
api.availablemac.com

External References

- https://www.sentinelone.com/blog/macos-adload-prolific-adware-pivots-just-days-after-apples-xprotect-clampdown/
- https://otx.alienvault.com/pulse/66329f6a4a00630aea010628