Jun 26 2023

NETMANAGEIT

Intelligence Report

"Operation Triangulation" campaign exploit 0-day vulnerabilities on Apple mobile devices

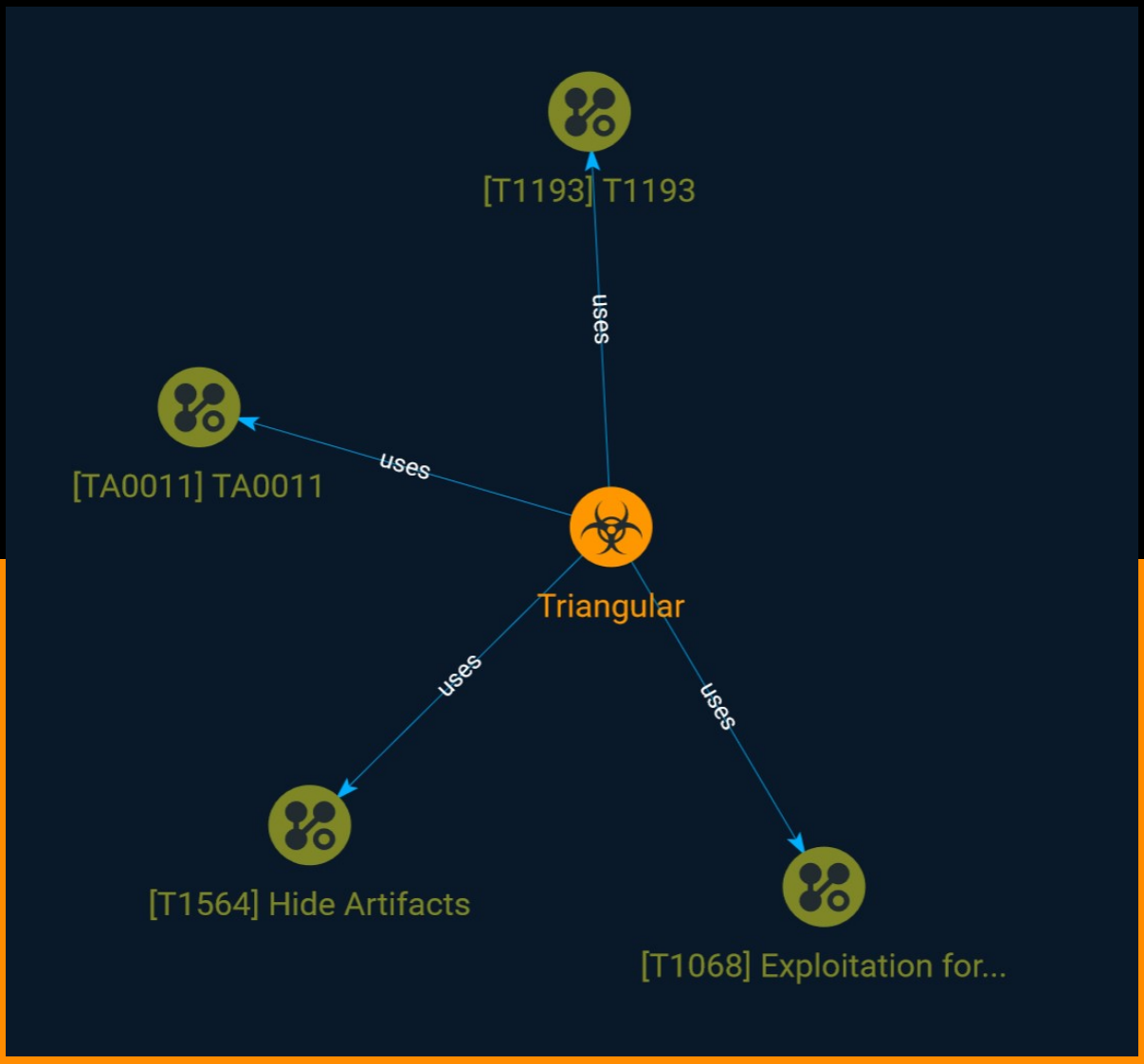

Table of contents

Overview

Entities

External References

Overview

Description

CERT Yoroi announces that since the beginning of June the news of a zero-click exploitation by a malware campaign called "Triangular" has emerged from two vulnerabilities on various Apple technoligies.

Confidence

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

15 / 100

Attack-Pattern

Name

Hide Artifacts

ID

T1564

Description

Adversaries may attempt to hide artifacts associated with their behaviors to evade detection. Operating systems may have features to hide various artifacts, such as important system files and administrative task execution, to avoid disrupting user work environments and prevent users from changing files or features on the system. Adversaries may abuse these features to hide artifacts such as files, directories, user accounts, or other system activity to evade detection.(Citation: Sofacy Komplex Trojan) (Citation: Cybereason OSX Pirrit)(Citation: MalwareBytes ADS July 2015) Adversaries may also attempt to hide artifacts associated with malicious behavior by creating computing regions that are isolated from common security instrumentation, such as through the use of virtualization technology.(Citation: Sophos Ragnar May 2020)

Name

T1193

ID

T1193

Name

Exploitation for Privilege Escalation

ID

T1068

Description

Adversaries may exploit software vulnerabilities in an attempt to elevate privileges. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Security constructs such as permission levels will often hinder access to information and use of certain techniques, so adversaries will likely need to perform privilege escalation to include use of software exploitation to circumvent those restrictions. When initially gaining access to a system, an adversary may be operating within a lower privileged process which will prevent them from accessing certain resources on the system. Vulnerabilities may exist, usually in operating system components and software commonly running at higher permissions, that can be exploited to gain higher levels of access on the system. This could enable someone to move from unprivileged or user level permissions to SYSTEM or root permissions depending on the component that is vulnerable. This could also enable an adversary to move from a virtualized environment, such as within a virtual machine or container, onto the underlying host. This may be a necessary step for an adversary compromising an endpoint system that has been properly configured and limits other privilege escalation methods. Adversaries may bring a signed vulnerable driver onto a compromised machine so that they can exploit the vulnerability to execute code in kernel mode. This process is sometimes referred to as Bring Your Own Vulnerable Driver (BYOVD).(Citation: ESET InvisiMole June 2020)(Citation: Unit42 AcidBox June 2020) Adversaries may include the vulnerable driver with files delivered during Initial Access or download it to a compromised system via [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105) or [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570).

Name

TA0011

ID

TA0011

Malware

Name
Triangular

External References

- https://otx.alienvault.com/pulse/6499bc66157b409c963775f8
- https://yoroi-company.translate.goog/warning/campagna-operation-triangulation-che-sfruttano-vulnerabilita-0-day-di-tipo-0-click-su-dispositivi-mobili-apple/?_x_tr_sl=auto&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=wapp