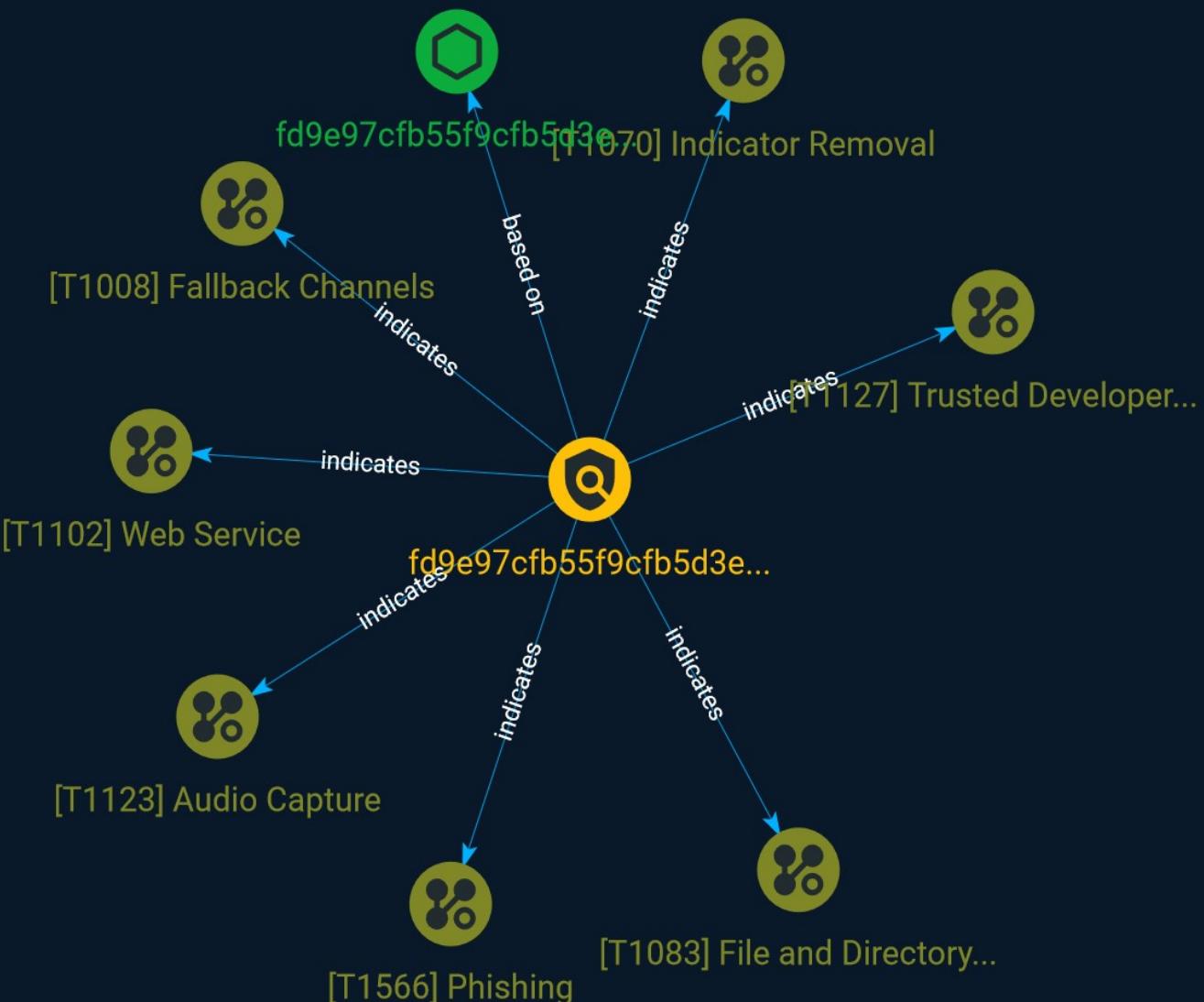




# Intelligence Report

## Dissecting TriangleDB, a Triangulation spyware implant



# Table of contents

---

## Overview

---

- Description 3
- Confidence 3

---

## Entities

---

- Attack-Pattern 4
- Indicator 8

---

## Observables

---

- StixFile 9

---

## External References

---

- External References 10

# Overview

## Description

An in-depth analysis of a spyware implant developed by attackers using an exploit known as Operation Triangulation to infect iOS devices in the next 20th Century, and how it is deployed.

## Confidence

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

15 / 100

# Attack-Pattern

<b>Name</b>
Fallback Channels
<b>ID</b>
T1008
<b>Description</b>
Adversaries may use fallback or alternate communication channels if the primary channel is compromised or inaccessible in order to maintain reliable command and control and to avoid data transfer thresholds.
<b>Name</b>
Audio Capture
<b>ID</b>
T1123
<b>Description</b>
An adversary can leverage a computer's peripheral devices (e.g., microphones and webcams) or applications (e.g., voice and video call services) to capture audio recordings for the purpose of listening into sensitive conversations to gather information. Malware or scripts may be used to interact with the devices through an available API provided by the

operating system or an application to capture audio. Audio files may be written to disk and exfiltrated later.

**Name**

Indicator Removal

**ID**

T1070

**Description**

Adversaries may delete or modify artifacts generated within systems to remove evidence of their presence or hinder defenses. Various artifacts may be created by an adversary or something that can be attributed to an adversary's actions. Typically these artifacts are used as defensive indicators related to monitored events, such as strings from downloaded files, logs that are generated from user actions, and other data analyzed by defenders. Location, format, and type of artifact (such as command or login history) are often specific to each platform. Removal of these indicators may interfere with event collection, reporting, or other processes used to detect intrusion activity. This may compromise the integrity of security solutions by causing notable events to go unreported. This activity may also impede forensic analysis and incident response, due to lack of sufficient data to determine what occurred.

**Name**

Phishing

**ID**

T1566

**Description**

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be

targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](<https://attack.mitre.org/techniques/T1564/008>)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](<https://attack.mitre.org/techniques/T1204>)).(Citation: Unit42 Luna Moth)

**Name**

Web Service

**ID**

T1102

**Description**

Adversaries may use an existing, legitimate external Web service as a means for relaying data to/from a compromised system. Popular websites and social media acting as a mechanism for C2 may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection. Use of Web services may also protect back-end C2 infrastructure from discovery through malware binary analysis while also enabling operational resiliency (since this infrastructure may be dynamically changed).

**Name**

## Trusted Developer Utilities Proxy Execution

**ID**

T1127

**Description**

Adversaries may take advantage of trusted developer utilities to proxy execution of malicious payloads. There are many utilities used for software development related tasks that can be used to execute code in various forms to assist in development, debugging, and reverse engineering.(Citation: engima0x3 DNX Bypass)(Citation: engima0x3 RCSI Bypass)(Citation: Exploit Monday WinDbg)(Citation: LOLBAS Tracker) These utilities may often be signed with legitimate certificates that allow them to execute on a system and proxy execution of malicious code through a trusted process that effectively bypasses application control solutions.

**Name**

File and Directory Discovery

**ID**

T1083

**Description**

Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Adversaries may use the information from [File and Directory Discovery](<https://attack.mitre.org/techniques/T1083>) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Many command shell utilities can be used to obtain this information. Examples include `dir`, `tree`, `ls`, `find`, and `locate`. (Citation: Windows Commands JPCERT) Custom tools may also be used to gather file and directory information and interact with the [Native API](<https://attack.mitre.org/techniques/T1106>). Adversaries may also leverage a [Network Device CLI] (<https://attack.mitre.org/techniques/T1059/008>) on network devices to gather file and directory information (e.g. `dir`, `show flash`, and/or `nvram`). (Citation: US-CERT-TA18-106A)

# Indicator

Name
fd9e97cfb55f9cfb5d3e1388f712edd952d902f23a583826ebe55e9e322f730f
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'fd9e97cfb55f9cfb5d3e1388f712edd952d902f23a583826ebe55e9e322f730f']

# StixFile

Value
fd9e97cfb55f9cfb5d3e1388f712edd952d902f23a583826ebe55e9e322f730f

# External References

---

- <https://otx.alienvault.com/pulse/6492f346dc563381f721adb7>
- <https://securelist.com/triangledb-triangulation-implant/110050/>

---