Mphasis
The Next Applied

AridSpy Malware

Date: 13th June 2024 | Severity: Medium

Summary

- The threat actor known as Arid Viper has been attributed to a mobile espionage campaign that leverages trojanized Android apps to deliver a spyware strain dubbed AridSpy.
- The activity is said to have spanned as many as five campaigns since 2022, with prior variants of AridSpy documented by Zimperium and 360 Beacon Labs. Three out of the five campaigns are still active.
- The malware is distributed through dedicated websites impersonating various messaging apps, a job opportunity app, and a Palestinian Civil Registry app," ESET researcher Lukáš Štefanko said in a report published today. "Often these are existing applications that had been trojanized by the addition of AridSpy's malicious code."
- The infection chain begins with convincing victims to download and install a fake yet functional app. Once installed, the trojanised app executes a JavaScript file named myScript.js, which facilitates the download of the malicious payload. This script generates the correct download path for the AridSpy payload and initiates the process.

Attack Vectors

- The attack chains mainly involve targeting users in Palestine and Egypt via bogus sites that function as distribution points for the booby-trapped apps.
- Some of the fake-but-functional apps claim to be secure messaging services such as LapizaChat, NortirChat, and ReblyChat, each of which is based on legitimate apps like StealthChat, Session, and Voxer Walkie Talkie Messenger, while another app purports to be from the Palestinian Civil Registry
- The malicious app available on palcivilreg[.]com is not a trojanized version of the app on Google Play; however, it uses that app's legitimate server to retrieve information," Štefanko said. "This means that Arid Viper was inspired by that app's functionality but created its own client layer that communicates with the legitimate server.
- The main responsibility of the first stage is to download the next-stage component, which harbors the malicious functionality and makes use of a Firebase domain for C2 purposes.
- The first-stage payload, designed to appear as an update to Google Play services, is responsible for downloading the second-stage payload. If the device has security software installed, AridSpy refrains from downloading further payloads, thereby reducing the risk of detection.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• 797073511A15EB85C1E9D8584B26BAA3A0B14C9E • 5F0213BA62B84221C9628F7D0A0CF87F27A45A28 • A934FB482F61D85DDA5E52A7015F1699BF55B5A9 • F49B00896C99EA030DCCA0808B87E414BBDE1549 • 3485A0A51C6DAE251CDAD20B2F659B3815212162 • 568E62ABC0948691D67236D9290D68DE34BD6C75 • DB6B6326B772257FDDCB4BE7CF1A0CC0322387D8 • 2158D88BCE6368FAC3FCB7F3A508FE6B96B0CF8A • B806B89B8C44F46748888C1F8C3F05DF2387DF19 • E71F1484B1E3ACB4C8E8525BA1F5F8822AB7238B • 16C8725362D1EBC8443C97C5AB79A1B6428FF87D • A64D73C43B41F9A5B938AE8558759ADC474005C1 • C999ACE5325B7735255D9EE2DD782179AE21A673 • 78F6669E75352F08A8B0CA155377EEE06E228F58 • 8FF57DC85A7732E4A9D144F20B68E5BC9E581300
URLS	• gameservicesplay[.]com • crashstoreplayer[.]website • reblychat[.]com • proj3-1e67a.firebaseio[.]com • proj-95dae.firebaseio[.]com • proj-2bedf.firebaseio[.]com • proj-54ca0.firebaseio[.]com • project44-5ebbd.firebaseio[.]com • www.palcivilreg[.]com • analyticsandroid[.]com • almoshell[.]website • orientflags[.]com • elsilvercloud[.]com • www.lapizachat[.]com • lapizachat[.]com • alwaysgoodidea[.]com • nortirchats[.]com • ultraversion[.]com

Recommendation

- Block all threat indicators at your respective controls.
- Search for indicators of compromise (IOCs) in your environment utilizing your respective security controls.
- Never trust or open links and attachments received from unknown sources/senders.
- Regularly monitor network activity for any unusual behavior, as this may indicate that a cyberattack is underway.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https://thehackernews[.]com/2024/06/arid-viper-launches-mobile-espionage[.]html
- https://github[.]com/eset/malware-ioc/blob/master/aridspy/README[.]adoc
- https://candid[.]technology/arid-viper-campaigns-target-palestine-egypt-via-malicious-apps/