Sep 09 2023

NETMANAGEIT

Intelligence Report

Spyware Telegram mod distributed via Google Play

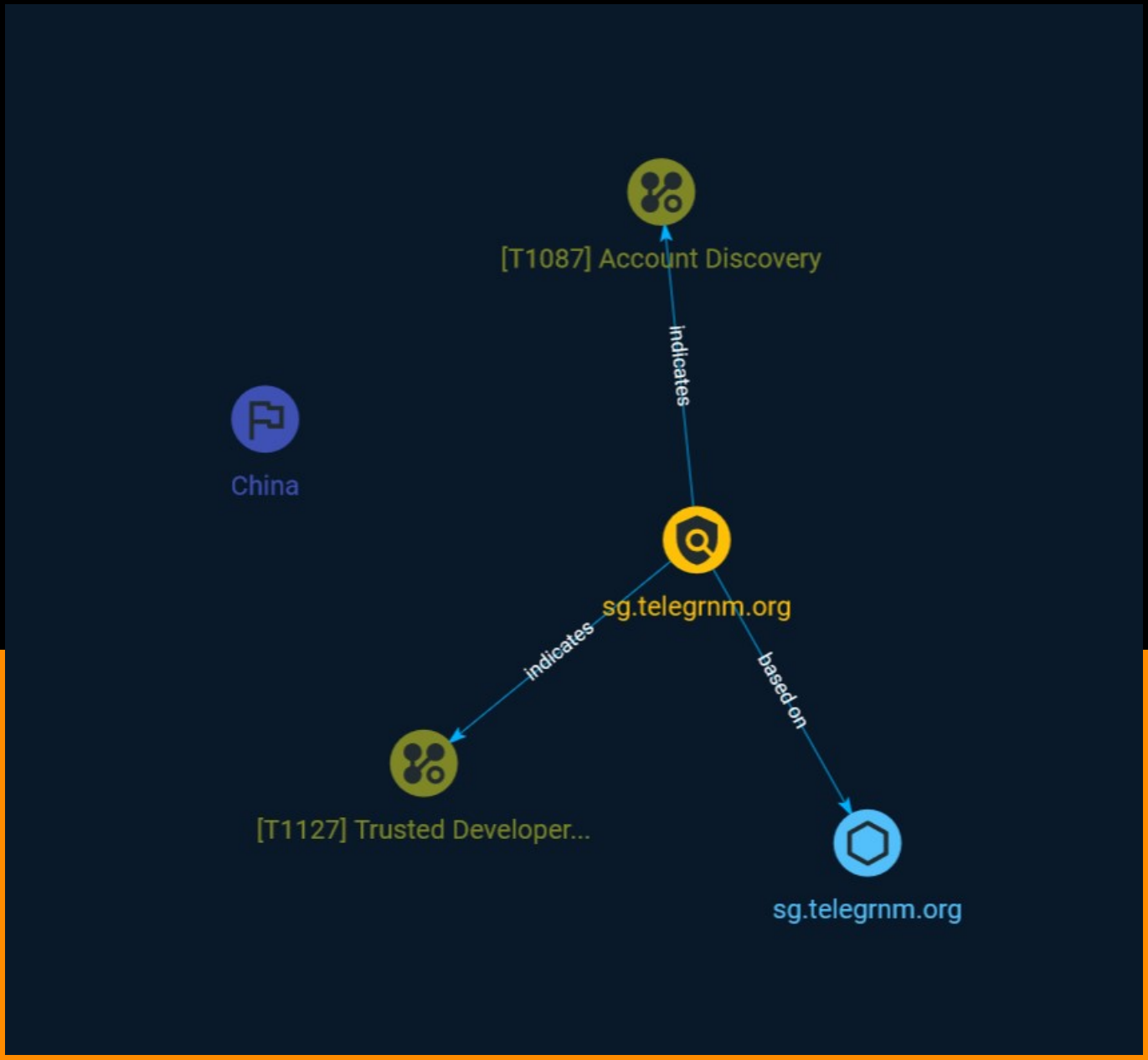

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A security firm Kaspersky has reviewed a Telegram mod app, which it says is the fastest app on Google Play and can be used to send malware to a server in China.

Confidence

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

15 / 100

Indicator

Name
sg.telegrnm.org
Pattern Type
stix
Pattern
[hostname:value = 'sg.telegrnm.org']

Country

Name
China

Attack-Pattern

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
Account Discovery
ID
T1087
Description

Adversaries may attempt to get a listing of valid accounts, usernames, or email addresses on a system or within a compromised environment. This information can help adversaries determine which accounts exist, which can aid in follow-on behavior such as brute-forcing, spear-phishing attacks, or account takeovers (e.g., [Valid Accounts](https://attack.mitre.org/techniques/T1078)). Adversaries may use several methods to enumerate accounts, including abuse of existing tools, built-in commands, and potential misconfigurations that leak account names and roles or permissions in the targeted environment. For examples, cloud environments typically provide easily accessible interfaces to obtain user lists. On hosts, adversaries can use default [PowerShell](https://attack.mitre.org/techniques/T1059/001) and other command line functionality to identify accounts. Information about email addresses and accounts may also be extracted by searching an infected system's files.

Hostname

Value
sg.telegrnm.org

External References

- https://otx.alienvault.com/pulse/64fb94c39d10b36e8315b4d0
- https://securelist.com/trojanized-telegram-mod-attacking-chinese-users/110482/