Sep 20 2023

NETMANAGEIT

Intelligence Report

CapraTube | Transparent Tribe's CapraRAT Mimics YouTube to Hijack Android Phones

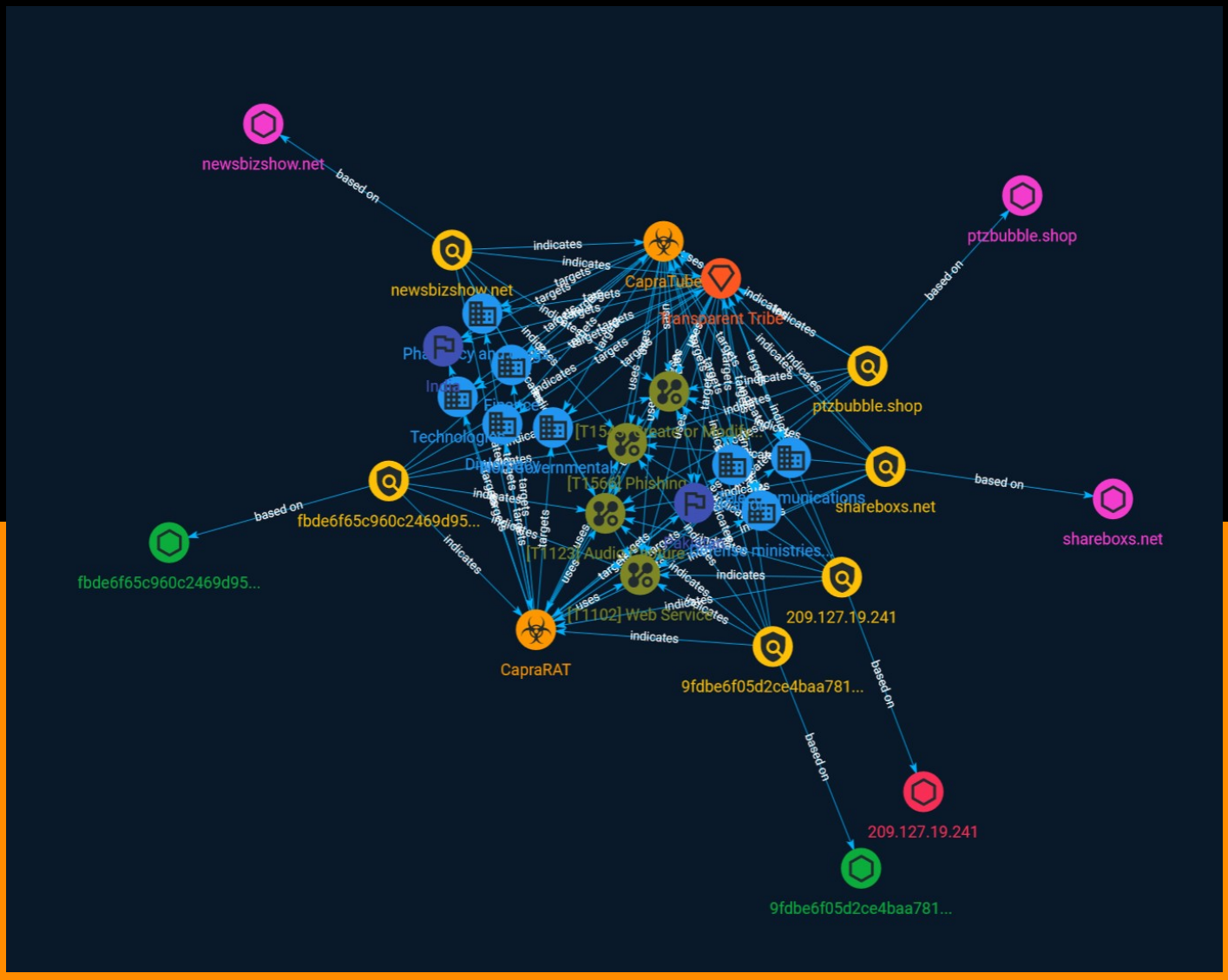

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Transparent Tribe is a suspected Pakistani actor known for targeting military and diplomatic personnel in both India and Pakistan, with a more recent expansion to the Indian Education sector. Since 2018, reports have detailed the group's use of what is now called CapraRAT, an Android framework that hides RAT features inside of another application. The toolset has been used for surveillance against spear-phishing targets privy to affairs involving the disputed region of Kashmir, as well as human rights activists working on matters related to Pakistan.

Confidence

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

15 / 100

Attack-Pattern

Name
Audio Capture
ID
T1123
Description
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
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

Create or Modify System Process

ID

T1543

Description

Adversaries may create or modify system-level processes to repeatedly execute malicious payloads as part of persistence. When operating systems boot up, they can start processes that perform background system functions. On Windows and Linux, these system processes are referred to as services.(Citation: TechNet Services) On macOS, launchd processes known as [Launch Daemon](https://attack.mitre.org/techniques/T1543/004) and [Launch Agent](https://attack.mitre.org/techniques/T1543/001) are run to finish system initialization and load user specific parameters.(Citation: AppleDocs Launch Agent Daemons) Adversaries may install new services, daemons, or agents that can be configured to execute at startup or a repeatable interval in order to establish persistence. Similarly, adversaries may modify existing services, daemons, or agents to achieve the same effect. Services, daemons, or agents may be created with administrator privileges but executed under root/SYSTEM privileges. Adversaries may leverage this functionality to

create or modify system processes in order to escalate privileges.(Citation: OSX Malware Detection)

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).

Sector

Name
Diplomacy
Description
Public or private entities which are actors of or involved in international relations activities.
Name
Defense ministries (including the military)
Description
Includes the military and all defense related-space activities.
Name
Finance
Description
Public and private entities involved in the allocation of assets and liabilities over space and time.
Name

Education

Description

Public or private entities operating to facilitate learning and acquiring knowledge and skills, composed of infrastructures and services to host teachers, students, and administrative services related to this activity. This does not include research activities.

Name

Non-Governmental Organizations (NGOs)

Description

A legally constituted non-commercial organization created by natural or legal persons with no participation or representation of any government.

Name

Pharmacy and drugs manufacturing

Description

Public and private entities involved in producing and selling medicinal products and drugs.

Name

Telecommunications

Description

Private and public entities involved in the production, transport and dissemination of information and communication signals.

Name
Technologies
Description
Private entities related to the research, development, manufacturing and distribution of electronics, softwares, computers and products related to information technologies.

Indicator

Name
9fdbe6f05d2ce4baa7819a0789caa3b49a835093193370ba49bdc4dfd4d9c7c7
Description
SHA256 of 14110facecceb016c694f04814b5e504dc6cde61
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '9fdbe6f05d2ce4baa7819a0789caa3b49a835093193370ba49bdc4dfd4d9c7c7']
Name
newsbizshow.net
Pattern Type
stix
Pattern

[domain-name:value = 'newsbizshow.net']

Name

shareboxs.net

Pattern Type

stix

Pattern

[domain-name:value = 'shareboxs.net']

Name

fbde6f65c960c2469d957f1fdb6d7240bd6eec5e4f34b68e01dda85cb9bf6841

Description

SHA256 of 8beab9e454b5283e892aeca6bca9afb608fa8718

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fbde6f65c960c2469d957f1fdb6d7240bd6eec5e4f34b68e01dda85cb9bf6841']

Name

ptzbubble.shop

Pattern Type
stix
Pattern
[domain-name:value = 'ptzbubble.shop']
Name
209.127.19.241
Description
CC=CA ASN=AS55286 SERVER-MANIA
Pattern Type
stix
Pattern
[ipv4-addr:value = '209.127.19.241']

Intrusion-Set

Name
Transparent Tribe

Description
[Transparent Tribe](https://attack.mitre.org/groups/G0134) is a suspected Pakistan-based threat group that has been active since at least 2013, primarily targeting diplomatic, defense, and research organizations in India and Afghanistan.(Citation: Proofpoint Operation Transparent Tribe March 2016)(Citation: Kaspersky Transparent Tribe August 2020)(Citation: Talos Transparent Tribe May 2021)

Country

Name
India
Name
Pakistan

Malware

Name
CapraRAT

Name
CapraTube

Domain-Name

Value
newsbizshow.net
shareboxs.net
ptzbubble.shop

StixFile

Value
fbde6f65c960c2469d957f1fdb6d7240bd6eec5e4f34b68e01dda85cb9bf6841
9fdbe6f05d2ce4baa7819a0789caa3b49a835093193370ba49bdc4dfd4d9c7c7

IPv4-Addr

Value
209.127.19.241

External References

- https://otx.alienvault.com/pulse/6509cea53f9f3994e928d8a6
- https://www.sentinelone.com/labs/capratube-transparent-tribes-caprarat-mimics-youtube-to-hijack-android-phones/