Indicators of Compromise (IOC)

CapraRAT malware is fully detected by SentinelOne’s applications with spyware and distributing them to targets through social media.

Conclusion

Decoy Dog Pupy RAT DNS tunneling

The group’s Android apps that leveraged other C2 domains.

The C2 port is in hexadecimal Big Endian format; the human readable port can be

C2 & Infrastructure

statements that map the string command to a related method.

10,000 lines of Smali code. By comparison, the March versions’ equivalents have only about 8,000 lines.

The RAT’s core functionality is in an activity similar to the

once per minute.

saw in CrimsonRAT.

often named and arranged differently depending on the app. The CapraRAT APKs we analyzed contain the following

Because CapraRAT is a framework inserted into a variety of Android applications, the files housing malicious activity are

Key Components

Notable features include:

CapraRAT is a comprehensive RAT that provides the actors with the ability to harvest data on demand and exfiltrate it.

and that Piya Sharma is a related persona.

clips of a woman in various locales. This APK also borrows the individual’s name and likeness. This theme suggests that

engineering to entice users to install a weaponized application. Earlier in 2023, the group

toolset has been used for surveillance against spear-phishing targets privy to affairs involving the disputed region of

Transparent Tribe is a suspected Pakistani actor known for targeting military and diplomatic personnel in both India and

Executive Summary

ADVANCED PERSISTENT THREAT

Do not install a third-party version of an application already on your device.

with. Do these permissions expose you to more risk than the potential benefit of the app?

Evaluate the permissions requested by an application, particularly an application you are not particularly familiar

with.

Source code.

Applications icons on an Android device, including

YouTube_052647.apk

14110facecceb016c694f04814b5e504dc6cde61

YouTube_052647.apk displays the YouTube website when launched

Main

MainActivity

Configuration

Name

Main

Configuration

Malicious Activity

Main

Configuration

Extra_Class

Variable declarations:

SERVERIP

domain was registered the same week of ESET’s report outlining the

is_phical

method which uses

method, which creates an alarm at the interval specified in the settings file’s

0xea60

resolution history for IP hosting

smsMoniter

Any connection between these campaigns is unclear; it is plausible that a

smsmons

state-sponsored activity. She relentlessly questions why actors pivot to a new technique or attack

claudfront[.]net

209[.]127.19.241

ptzbubble[.]shop

©2023 SentinelOne, All Rights Reserved.

working on matters related to Pakistan.

against a computer worm. Over the past decade, Alex has worked with blue, purple, and red teams

in her spare time, she can be found DJing or servicing her music arcade games.