Government of India
National Critical Information Infrastructure
Protection Centre
(A Unit of NTRO)

Date: 05 Dec 2019

Cyber Security Advisory: Gutstuff Android Banking Trojan

This data is to be considered as **TLP:AMBER**

Our trusted partner reported about an advanced Android banking Trojan named Gustuff. The initial version of Gustuff recorded several similarities with another banking trojan, Marcher. Once installed on a device, Gustuff trojan uses android accessibility services to interact with screens from other apps. It also disables Google Play Protect, anti-virus and anti-malware software to prevent detection. It can spread to other mobile devices by reading the contact list of compromised device and sending out messages with a link to its APK installation file.

Analyst's Notes:

This malware is reportedly capable of sending information about the infected device to the Command and Control (C2) server, reading/sending SMS messages, sending USSD requests, launching SOCKS5 Proxy, resetting the device to factory settings and showing fake push notifications with icons from legitimate apps to steal account credentials by displaying a false login page.

IOCs:

Domain/IPs:

88[.]99[.]174[.]142
88[.]99[.]175[.]152
88[.]99[.]170[.]43
88[.]99[.]170[.]141
78[.]46[.]201[.]36
88[.]99[.]174[.]140
instagram-shared[.]pw
instagram-shared[.]store
instagram-shared[.]info
instagram-share[.]com
intagram-share[.]com
instagram-shared[.]net
instagram-shared[.]com
video-hd33[.]site
video-hd30[.]site
video-hd29[.]site
video-hd24[.]site
video-hd20[.]site
video-hd18[.]site
video-hd17[.]site
hd-video5[.]site
hd-video4[.]site
video-hosting[.]site
video-hd1[.]site
video-hd[.]site
hd-video1[.]site
homevideo641a[.]cf
homevideo651a[.]cf
homevideo5-23b[.]ml
homevideo631a[.]cf
homevideo611a[.]cf
homevideo4-23b[.]ml
homevideo641a[.]ga
homevideo3-23b[.]ml
homevideo54-1a[.]ml
videohosting32-e[.]cf

videohosting23c[.]cf
videohosting62-b[.]tk

Hashes(SHA-256):
5981f8ec5b35f3891022f1f1cdbf092c56a9b0ac8acbcd20810cc22e7efb5e0b
03d1a55ce6879d79239db32c2c8e83c4a3e10cb9123d513ce7fd04defb971886
3027fbd59b8dd25dcabd21800d8e8ab3222a1ae3e2d268857def4311bb01ea2e
b13e6d70b07d6127d803d2374ebfb1e66a3b4cfd865cc2eb0e45455401be527e
65a7d4f9b3549198b008a089d0c8feb30c5409efc52e8a496f503fa262a6e922
edb838be33fde5878010ca84fc7765c8ff964af9e8387393f3fa7860c95fc70b
9eaad594dd8038fc8d608e0c4826244069a7a016ffd8881d8f42f643c972630f
4efcc22da094e876346cff9500e7894718c8b6402ff3735ea81a9e057d488849

Recommendations:

- Users if found any above mentioned package, android app in their phone should immediately uninstall it from their device.
- Even though the malware is being spread through the Google Play Store itself, it is advisable to stick to verified application stores as they are much safer than untrusted sources.
- Install applications downloaded from reputed application market only. Install and maintain updated antivirus solution on Android devices.
- Install Android updates and patches as and when available from Android device vendors.
- Users are advised to use device encryption or encrypting external SD card feature available with most of the Android OS.
- Avoid using unsecured, unknown Wi-Fi networks.

Reference: CERT-In

Disclaimer:

The information provided by NCIIPC above is on "as is" basis only. System owners are advised to independently evaluate the contents for its applicability in their specific environment, and take appropriate action as per their own assessment of the implications of the alert/ advisory on their systems. NCIIPC will not be liable for any issues or problems that may arise from application or non-application of the alert/ advisory. System owners are wholly responsible for cyber security updates to their information technology systems.

This document is distributed as TLP:AMBER. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.

With Best Regards,
Knowledge Management System
National Critical Information Infrastructure Protection Centre
Block-III, Old JNU Campus, New Delhi - 110067
Website: www.nciipc.gov.in
Toll Free: 1800-11-4430