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

Date: 19 Dec 2019

Advisory No: Adv/2019/Dec/006

Cyber Security Advisory: GINP ANDROID BANKING TROJAN

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

Our trusted partner reported a malware initially masquerading as a “Google Play Verificator” app, has implemented some banking-specific features and started spreading the malicious code as fake “Adobe Flash Player” apps. Upon execution in a victim device, malware Ginp removes its icon from the app drawer before asking the user for Accessibility Service privilege. Once it receives the Accessibility Service privilege, it grants itself additional permissions for sending messages and making calls without user interaction. At this point, the malware waits for commands from the Command and Control (C2) Server.

Analyst's Note:

Ginp is implementing the following features such as Dynamic (local overlays obtained from the Command and Control (C2)),SMS listing, SMS forwarding, collection Application listing, SMS sending, Call forwarding, Hiding the App icon, Preventing removal & Emulation-detection.

IoCs: The list of IoC's is attached (IOC_ Adv2019Dec006.txt)**.**

Recommendations:

- Ginp’s use of deceptive overlay screens to steal login credentials and credit card details should prompt users to be more vigilant when installing apps on their devices. They should only download apps from official sources to minimize the chances of downloading a malicious app.
- Monitor Connection attempts towards the listed hashes.
- Users and enterprises should use mobile security software or antivirus to prevent unauthorized access to apps, detection and blocking of malware and fraudulent websites.

Reference: CERT-In

Links:
https://www.trendmicro.com/vinfo/in/security/news/cybercrime-and-digital-threats/ginp-trojan-targets-android-banking-app-users-steals-login-credentials-and-credit-card-details
https://securityaffairs.co/wordpress/94533/cyber-crime/ginp-android-trojan-anubis.html

This document is distributed as TLP:WHITE. Recipients may only share TLP:WHITE 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.

Advisory No: Adv/2019/Dec/007

Cyber Security Advisory: NukeSped-The APT RAT

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

Our trusted partner reported a malware NukeSped RAT. The NukeSped samples have the language ID for Korean, compiled for 32-bit systems and were using encrypted strings to make analysis harder. NukeSped has sole intention of gaining remote access on the compromised computer. It also opens a backdoor by modifying registry and firewall settings. NukeSped RAT inserts itself into a Run registry key, though in some cases it installs itself as a service.

Analyst’s Notes:

NukeSped RAT malware is preforming various activities on compromised system e.g.iterate files in a folder, create a process as another user, iterate processes and modules, terminate a process, Read/Write a file, connect to a remote host, Move a file, Retrieve and launch additional payloads from the internet.

IoCs: The list of IoC's is attached (IOC_ Adv2019Dec007.txt).

Recommendations:

- Monitor Connection attempts of both ingress and egress traffic of the listed URLs / Domains / IPs. All hash values should be kept under an active watch-list in the respective/supported endpoints and security solutions. The list may include compromised domains /IP resources as well.
- Deploy web and email filters on the network. Scan all emails, attachments, and downloads both on the host and at the mail gateway with a reputable antivirus solution.
  - Enforce application whitelisting on all endpoint workstations. This will prevent droppers or unauthorized software from gaining execution on endpoints.

Reference: CERT-In

This document is distributed as TLP:GREEN. Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.

Advisory No: Adv/2019/Dec/008

Cyber Security Advisory: Weekly Mirai Activity Report

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

Our trusted partner reported following IoC's from statically analyzed Mirai samples identified over a week. There are a couple things to be aware of while looking at this data:

* Network IoCs may be associated with binary distribution or one of the "cnc" or "report" functions.
* Network IoCs are identified from newly identified samples but may themselves not necessarily be new.
* Because of the nature of the static analysis there is MODERATE confidence in the accuracy of the network IoCs.

IoCs: The list of IoC's is attached(IOC_ Adv2019Dec008.txt).

Reference: CISCO Talos Intelligence

This document is distributed as TLP:GREEN. Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.

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.

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