PTA Cyber Security Advisory No: 133 **20-04-2021**

Name: Android malware presents itself as a fake 'System Update'

Threat Classification: Malware

Affected Device: Android OS

Summary:

It has been reported that a powerful new android malware disguises itself as a **system update application**. This malware can record calls, take photos, and perform a variety of invasive actions including full control of Android phones. Once in control, hacker can also review browser history, access WhatsApp messages and even search for specific file types present in the phone. Upon installation (from a third party store, **not Google Play Store**), the device gets registered with the Firebase Command and Control (C&C) with details such as the presence or absence of WhatsApp, battery percentage, storage stats, the token received from the Firebase messaging service, and the type of internet connection.

For further details, please visit following link:
https://blog.zimperium.com/new-advanced-android-malware-posing-as-system-update/

Indictors of Compromise (IoCs):

1. **Spyware applications**:
   - 96de80ed5ff6ac9faa1b3a2b0d67cee8259fda9f6ad79841c341b1c3087e4c92
   - 6301e2673e7495ebdfd34fe51792e97c0ac01221a53219424973d851e7a2ac93
2. **C&C Servers**:
   - hxxps://mypro-b3435.firebaseio.com
   - hxxps://licences.website/backendNew/public/api/

Recommendations:

For Network/ System Admins:

- All the operators must block the aforementioned C&C Servers (URLs) at their organization’s perimeter level or Gateway.
- IOC Sweeping must be performed as per aforementioned IoCs across the infrastructure.

For Users:

- It is recommended that when accepting updates or before installing new apps on your Android device, always confirm the software vendor you're using.
- Never install anything sent via text message unless it's from a trusted source.
- Android updates never come in the form of a new, self-contained app.
- Use licensed antivirus and regularly obtain its latest updates with its real-time scanning capabilities enabled.
- Only use licensed software and avoid download/use of cracked and pirated software.
- In case of any incident, please report to this office.