UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00244

BRATA TROJAN FOR ANDROID INCLUDES DEVICE WIPING

DATE ISSUED: 14th February 2022

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	MEDIUM	[✓ EASY]

OVERVIEW

Three new versions of the Android banking Remote Access Trojan (RAT) BRATA have been discovered with numerous new features including GPS tracking, new obfuscation techniques and the ability to wipe all data from devices after its exfiltration.

BREAKDOWN

Traditionally targeting banks and other financial institutions the RAT is now being distributed through a downloader to avoid detection by anti-virus solutions. Discovered by Kaspersky in January 2019 on the Google Play Store, this banking Trojan conveys information back to the operator in real time and since then has been adopted by various malicious who have added capabilities to the malware. Tailored versions are being delivered to various countries globally. One of these new capabilities includes a “killswitch” that is able to perform a factory reset of the device in two scenarios. The first is after bank fraud has been completed and the second is when the app is installed in a virtual environment to prevent dynamic analysis. Some versions include tailored overlay pages used to steal the PIN for the targeted application.

REMEDIATION STEPS

- Always install applications from trusted app stores and never from third party app stores
- Use NGAV (Next Generation Anti-Virus) software to detect anomalous behaviour on your device
- Back up your device regularly to prevent data loss.
- If you suspect your bank account has unusual activity or has been breached, contact your bank immediately to remediate.

REFERENCES & RESOURCES

ThreatPost	https://threatpost.com/brata-android-trojan-kill-switch-wipes/177921/