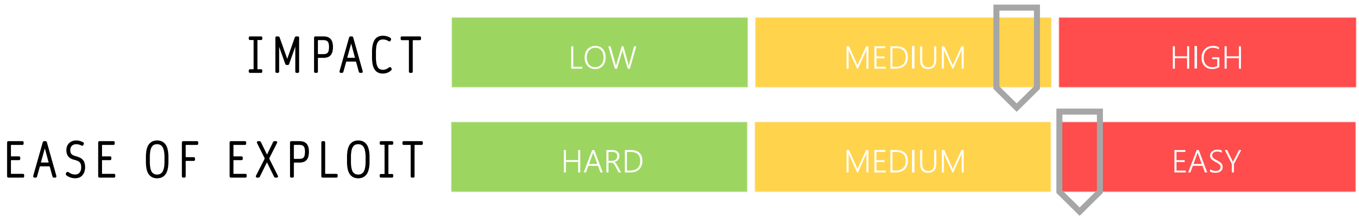
UNISPHERE SOLUTIONS

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

CYBER GUIDANCE ISSUE 00104

LODARAT MOVES FROM WINDOWS TO ANDROID

DATE ISSUED: 15th February 2021



OVERVIEW

Previously known to focus on Microsoft Windows devices, a new variant of the LodaRAT malware has been discovered which targets Android devices to spy on victims in a new espionage campaign signalling success and a strategy shift for attackers.

BREAKDOWN

LodaRAT is known for stealing victim's credentials in order to drain their bank accounts in previous versions, but this new evolution features information gathering commands set to steal and exfiltrate other information. The Remote Access Trojan or RAT was first discovered in 2016 and has undergone many advancements and was originally distributed through emails containing links to malicious applications or documents and is now being seen to use false, typo-squatted domains or file directly targeting individuals with relations to their products or services offered. Attackers are exploiting a remote code execution vulnerability in Microsoft Office (CVE-2017-11882) to download LodaRAT and connect to a Command-and-Control centre (C2) and begin collection of location data, recording audio and phone calls, take photos and screenshots and exfiltrate contacts as well as call and SMS logs (but is not capable of intercepting either of these types of communications.) Attackers are able to gain access to Remote Desktop Protocol (RDP) in the latest version and leverage the BASS audio library to connect to the infected machine's microphone and is able to record for any duration of time specified.

REMEDIATION STEPS

- Educate users on the dangers of social engineering, phishing attacks, how to spot them and how to report them and deal with them.
- Ensure only allowed applications are able to be downloaded and installed on any company owned devices.
- Always download applications from verified suppliers
- Monitor networks and mobile devices for any anomalous activities.
- Implement incident response procedures if abnormal activities are detected to isolate and remediate.

REFERENCES & RESOURCES

Threatpost:	https://threatpost.com/android-devices-lodarat-windows/163769/
Bank Info Security	https://www.bankinfosecurity.com/lodarat-malware-now-target-android-devices-a-15957
The Hacker News	https://thehackernews.com/2021/02/lodarat-windows-malware-now-also.html