UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00016

NEW VARIANT LOKIBOT: BLACKROCK

DATE ISSUED: 22nd July 2020

	LOW	MEDIUM	HIGH
IMPACT		✓	
EASE OF EXPLOIT	✓		

OVERVIEW

Based on the source code of the Xerxes banking malware, which is a variant of Lokibot, the new BlackRock trojan is targeting financial apps and a raft of well-known android devices and applications including Amazon, eBay, Facebook, Grinder, Instagram, Netflix, PlayStation, Reddit, Skype, Snapchat, TikTok, Tinder, Tumblr, Twitter, Uber and VK.

BREAKDOWN

Whilst the original primary function of Lokibot and the many associated variants was to target banking applications in order to steal credentials, perform overlay attacks, lock devices, act as a keylogger and also steal or hide notifications from users, the BlackRock variant has added a string of further capabilities and targets. This modified version lifts data from a number of popular chatting, dating, gaming and social media applications including those in the aforementioned list and many more. A further unique capability of BlackRock is that it is able to evade detection by common anti-virus software and device cleaning applications including Avast, AVG, BitDefender, Esets, Symantec, TrendMicro, Kaspersky, McAfee and Avira as well as TotalCommander, SDMaid or Superb Cleaner. To achieve this, the user is redirected to their home screen upon trying to access their anti-virus program, avoiding removal by the clean-up software. It establishes itself by hiding itself from the app drawer, essentially becoming invisible and then poses as a fake Google update requesting permissions. Once permission is granted, it will grant itself further permissions without the need for user interaction, and once fully installed, receives its instructions from the Command and Control server

REMEDIATION STEPS

- Only use official distribution channels for downloading new applications
- Use an anti-malware software suite rather than solely anti-virus in android devices
- Be wary of third-party updates and verify before granting permissions

REFERENCES & RESOURCES

Threatpost: https://threatpost.com/lokibot-redux-common-android-apps/157458/
Hot for Security by Bitdefender https://hotforsecurity.bitdefender.com/blog/blackrock-malware-goes-after-banking-social-and-other-mobile-apps-23750.html
ZDNet https://www.zdnet.com/article/new-blackrock-android-malware-can-steal-passwords-and-card-data-from-337-applications/
Threat Fabric https://www.threatfabric.com/blogs/blackrock_the_trojan_that_wanted_to_get_them_all.html