



ReboundRAT



Overview

Israeli Defense Forces (IDF) announced that it was targeted by ReboundRAT - a very targeted and socially engineered Remote Access Trojan (RAT) malware campaign. Similar to [ViperRAT](#), which Lookout discovered in 2017, this campaign baits soldiers into downloading a fake dating app by messaging them on social media platforms under the ruse of being an attractive young woman.

Lookout Analysis

The campaign was discovered and taken down by the IDF in conjunction with the Israeli Security Agency (ISA). Even though this particular campaign targeted the IDF, it shows how malicious actors are going beyond email to take a personalized approach to targeting specific groups or individuals. Lookout continuously discovers and provides coverage for attacks like ReboundRAT including ViperRAT, BRATA, HeroRAT, TeleRAT, and AndroRAT, which were delivered in a variety of ways to the end user.

The nature of this attack highlights how mobile users are increasingly becoming a core focus of cybersecurity attacks. Targeting the military, specifically individuals whose location data and communication have significant value to adversaries, can be detrimental to the national security of any targeted nation. Leveraging social engineering is becoming a more popular way for bad actors to persuade end users to fall for phishing links and download malicious apps. Without tools in place to protect its end users, an organization or nation state's security is only as good as its least alert people.

How Lookout Detects and Protects

To ensure protection against Remote Access Trojan (RAT) attacks like ReboundRAT, Lookout Mobile Endpoint Security leverages security telemetry from over 100 million analyzed applications. With this visibility into malicious applications, Lookout extends the latest protections without any action needed from the end user. To protect against social engineering as one of the fastest-growing threat vectors, Lookout Phishing Protection can block the connection to malicious links and stop attacks before they start.

Lookout Threat Advisory Service

Threat Advisory combines data from Lookout's industry-leading dataset and global sensor network of tens of millions of devices to provide its customers with a direct line into the fast-changing world of mobile security. Take advantage of Threat Advisory to gain access to exclusive security intelligence research and immediately actionable insights that your team can use to stay ahead of the malicious actors and keep your organization safe.

[Click here to learn more about Lookout Threat Advisory](#)