Learn How Zimperium MTD Protects Against This New Threat

zimperium.com/blog/zimperium-mtd-against-oilalpha-a-comprehensive-defense-strategy/

Zimperium's MTD Against OilAlpha: A Comprehensive Defense Strategy

May 18, 2023 Nicolás Chiaraviglio

At Zimperium, we're always on the lookout for emerging threats that could potentially harm our customers. One such threat, recently identified by Recorded Future, is the OilAlpha group. This group has been linked to pro-Houthi threat actors and has been actively targeting entities across the Arabian Peninsula since May 2022.

The OilAlpha group primarily targets entities in the non-governmental, media, international humanitarian, and development sectors. Their modus operandi includes launching social engineering attacks via encrypted chat messengers like WhatsApp, using URL link shorteners, and deploying malicious Android applications. They have been seen targeting individuals who share an interest in Yemen's political and security developments, particularly those involved in humanitarian aid and reconstruction efforts.

The group uses a variety of malware to carry out their attacks, including SpyNote, SpyMax, and njRAT. These Spyware tools have a wide range of capabilities:

SpyNote and SpyMax are feature-rich spyware capable of installing arbitrary apps, gathering SMS messages, calls, videos and audio recordings, tracking GPS locations, and hindering efforts to uninstall the malicious app.

njRAT, on the other hand, is capable of performing surveillance or even taking control of the infected system. Its capabilities include logging keystrokes, capturing screenshots, password stealing, exfiltrating data, accessing web cameras and microphones, and downloading additional files.

While these threats are significant, we want to reassure our customers that Zimperium is prepared and vigilant. Our on-device dynamic detection engine can detect all samples reported in Recorded Future's blog with zero day coverage, without requiring any update and relying 100% in the machine learning component of the engine. Moreover, our web content filtering can correctly identify 94% of all reported URLs (that belong to a cluster of dynamic DNS servers used as C2 servers) used for the attack, rendering it completely ineffective.

We believe in proactively protecting our customers from all kinds of threats. Our continuous monitoring and threat intelligence capabilities allow us to respond promptly to new threats, while our robust security infrastructure provides a strong defense against established ones.

The safety of our customers is our top priority, and we are committed to keeping you safe from the OilAlpha group and other similar threats.

For more information on how Zimperium's customers are protected, visit https://www.zimperium.com/mtd/ or contact us today.

Author: Nicolás Chiaraviglio

Security Research. View the author's experience and accomplishments on LinkedIn.