Lookout Phishing AI Discovers Campaign Targeting UN and Humanitarian Orgs

Advanced attack imitates organizational email login pages

Overview

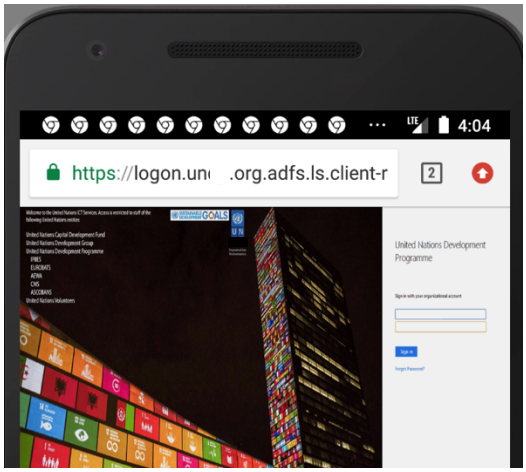
At the beginning of October 2019 Lookout researchers discovered a targeted phishing attack focusing on non-governmental organizations around the world, including but not limited to UN and humanitarian organizations. This attack is currently still ongoing and is aimed at employees of these organizations. The phishing pages captured by Lookout attempt to convince a target to enter their organizational Office 365 and Outlook account credentials.

The actor is targeting mobile devices. There is logic in existing JavaScript code of the site that checks if a device accessing the link is a mobile device. This is further confirmed by the fact that the initial part of the subdomain used in the phishing links closely mirror legitimate infrastructure. Only the initial part of the domain is visible in a mobile web browser, so many users won't recognize this as a phishing attempt.

Lastly, there is also evidence of key logging functionality embedded in the password field of the phishing login pages. Even if a target doesn't complete the login activity by pressing the login button or if they enter another, unintended password, this information is still sent back to the command and control infrastructure operated by this actor.

Potential impact

Workers at targeted organizations are at risk having their corporate identities taken over, which will compromise sensitive organizational data. This puts the entire organization at risk if the attacker is able to leverage stolen credentials to gain access to organizational infrastructure, and potentially opens the door for persistent threats.



Key Facts about this Phishing Attack

- That attack targets several United Nations programs, humanitarian institutions, and well-known non-governmental organizations.
- The attack mirrors the targeted organizations' login pages for Office 365 and Outlook to steal credentials which will provide access to sensitive information and opens the door for persistent threats.
- Mobile users are specifically targeted using initial subdomains mirroring legitimate sites that appear correct on smaller screens.
- With keylogging functionality, anything entered into a field is sent to the attacker, even if a target doesn't press the login button.

Lookout Phishing AI

With our advanced Phishing AI, Lookout is able to identify early signs of a phishing attack and build protection for Lookout users, as well as provide early warnings to Lookout partners before their customers are impacted. Follow @PhishingAI on Twitter.

Lookout Phishing and Content Protection alerts users to phishing attempts from any app on a mobile device.

Learn more about Phishing and Content Protection