Lookout Phishing AI Discovers Campaign Targeting Verizon Employees

Advanced phishing attack imitates internal login page for employees

Overview

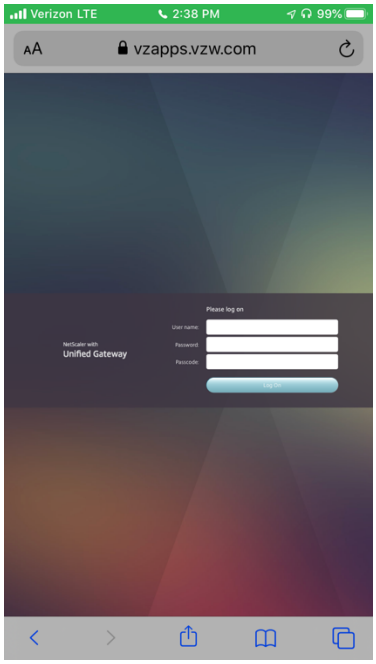
On September 20th, 2019, Lookout Phishing AI discovered a new phishing campaign targeting Verizon employees. The attack targets employees when they attempt to login to the internal apps portal for Verizon with the intention of stealing login credentials and multi-factor authentication passcodes. Lookout Phishing AI was first to pick up on this campaign after the attack was launched.

Lookout identified the malicious URL based on this and other phishing activity originating from the source IP address. By quickly identifying, scoring, and convicting the URL as phishing, Lookout notified Verizon of the page, and Phishing AI was able to prevent a major security incident tied to the theft of corporate credentials.

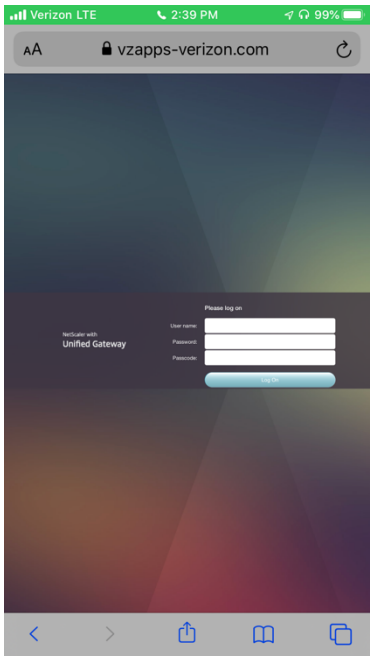
Potential impact

Verizon employees would have risked having their corporate identities taken over, which would compromise personal and corporate data. This would expose employees to fraud and identity theft and put the entire company at risk if the attacker is able to leverage their credentials to steal internal corporate data.

Real



Fake



Key Facts

- Very minor differences between the two login screens make it difficult to spot.
- After enough times going through these screens, employees fly through the login process and don't look closely at the page or URL.
- With shortened URLs on mobile, there is little that would tip off a user unless they checked the full URL, and remembered the exact URL for the legitimate page.

Lookout Phishing AI

With our advanced Phishing and Content Protection technology, 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 here.

Learn more about Phishing and Content Protection