Lookout Discovers Phishing Attack Targeting AT&T Employees

Sophisticated phishing site mirrors employee portal login screen

Overview

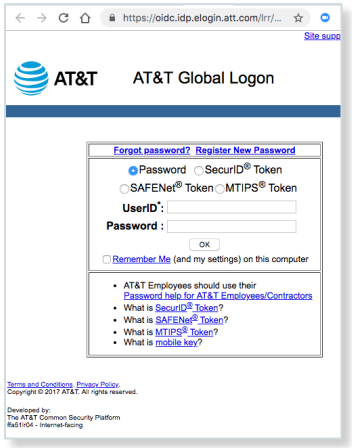
On April 16, 2019, Lookout discovered a new phishing attack targeting AT&T employees. The attacker developed a copy of the AT&T Global portal login screen in an effort to steal user credentials including multi-factor identification values. The moment the attacker began building the phishing site, Lookout flagged it as suspicious and monitored its development.

First, the attacker registered a spoofed version of the AT&T domain. Next, Phishing AI applied computer vision to analyze the use of logos and graphics, resulting in a final conviction. Lookout quickly notified AT&T and continued to monitor changes until the malicious site was taken down.

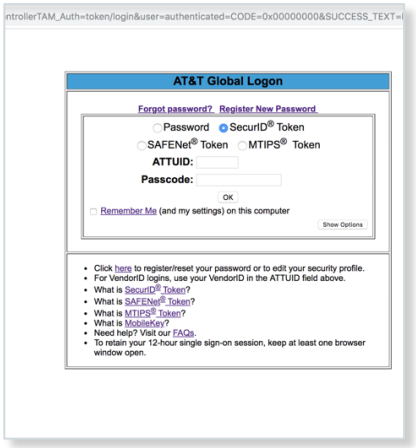
Potential impact

AT&T employees would have risked having their accounts taken over, compromising their privacy and exposing themselves to fraud and identity theft. This login provides access to proprietary corporate applications and could have exposed AT&T to significant business risk as well as a longer term advanced persistent threat.

Real



Fake



Real vs Fake

- Fake screen is a very close replica of a previous version of login screen
- Login screen becomes 'white noise' to employees after frequent logins throughout the workday
- On mobile this phishing attack could also be highly successful

Early detection by Lookout Phishing AI

With its advanced Phishing & Content Protection technology, Lookout is able to identify early signals of a phishing attack and build protection for Lookout users, as well as provide early warning to Lookout partners before their customers are impacted.