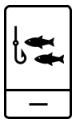
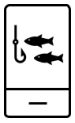


Twitter Phone Spear Phishing Attack



Overview

On July 15th, 2020, Twitter experienced a security incident where a malicious actor gained access to the back-end account management console through a phone spear phishing campaign. The incident affected the accounts of 130 highly influential individuals, including Barack Obama, Bill Gates, Elon Musk and Kanye West. The attacker then tweeted a link to a Bitcoin wallet address promising to send $2,000 back to anyone that sent them $1,000.

Phone spear phishing is a form of phishing that targets individuals on smartphones using social engineering to lure them to tap on a phishing link. Successful phone spear phishing attacks typically use social engineering through mobile apps like Twitter, Facebook, WhatsApp rather than email. These campaigns exploit human vulnerabilities and smaller screens on smartphones to bypass legacy security tools.

How Does it Work?

What's important to understand is that the Twitter employees that were originally targeted weren't necessarily the ones with administrative access. This means the attacker moved laterally and gained access to privileged credentials.

Twitter's report states the "[attackers] used their [employees'] credentials to access our internal systems and gain information about our processes. This knowledge then enabled them to target additional employees who did have access to our account support tools." Seeing that this was a two-step process shows that this was a sophisticated attack with a very specific plan of action.

This attack adds to the increasing trend of phishing campaigns targeting mobile. Malicious actors leverage mobile because it's more difficult to spot a phishing attempt on a mobile phone due to the smaller screen, the inability to see the full URL in the mobile browser, and lack of awareness on how to safely preview where a link is sending you before you tap it.

Lookout Recommendation for Admins

Lookout Phishing and Content Protection inspects any URL requests, including corporate and personal email, SMS, messaging apps, and Apps containing URLs that download malicious plug-ins. Lookout dynamically blocks URL requests for websites identified by Lookout as malicious and phishing.

Lookout admins can force activation of Phishing & Content Protection by not allowing employees to access corporate apps and data without having it turned on.

Lookout Mobile Phishing Protection

Lookout provides comprehensive mobile phishing protection on both Android and iOS devices, gives admins powerful tools for monitoring, managing and protecting mobile devices, and enables organizations to confidently embrace the use of smartphones within their organization.

Click here to learn more about Lookout mobile phishing protection