Lookout Phishing AI Discovery

Lookout Phishing AI is constantly discovering and auto-convicting malicious URLs to protect its customers

Background and Discovery Timeline

Lookout Phishing AI detected a phishing campaign impersonating local government websites, including the City of San Mateo, City of Tampa, and Dallas County. While the actor behind this phishing campaign has been active for four years, they have recently evolved to target small and medium businesses (SMBs) with uncommon techniques, such as impersonating local governments.

SMBs have become an easy target for attackers since a growing business may feel they do not have the time or resources to devote to cybersecurity. In fact, according to the 2019 Verizon DBIR, almost half of cybersecurity breaches involve small businesses. A breach of any kind can be devastating for an organization, but for many small business owners, it can put them out of business.

Key Facts

1. Targets smaller businesses by impersonating local government websites
2. The same actor has registered over 200 domains with the same email address since 2015
3. Tricks victim into entering PII on sites such as false vendor registration pages

Capabilities and Affected Parties

The threat actor has registered more than 200 domains with the same email address since 2015 and is now averaging about seven to ten per week. And recently, the actor has created a series of fake local government websites, impersonating the likes of Dallas County, Polk County, the City of San Mateo, the City of Tampa, and the City of North Las Vegas. These phishing sites were a near-perfect mirror of the legitimate sites, but the phishing sites included a "Vendor Registration Form" designed to steal PII and account credentials. The sites leveraged the authority of these local governments to entice their targets with bid solicitations, requiring its victims to provide their name, phone number, address, and SSN/EIN. After entering this information, the victim is directed to a credential phishing kit. This is typically done with a pretext to access a document.

How Lookout Detects and Protects Against Phishing Threats

When phishing domains get reported, they get taken down—however, no other phishing detection tools are correlating repeated characteristics of a malicious actor. However, Lookout Phishing AI is able to correlate data with thousands of automated investigations that are performed every day to build profiles of phishing campaigns. In the case of this campaign, we know that the domains have been used as command and control (CC) servers for Windows malware, phishing web sites and contain multiple confirmed Microsoft credential phishing kits.

Lookout Threat Advisory Service

In the fast-changing world of mobile security, keeping your finger on the pulse can be challenging. Lookout Threat Advisory taps into the massive dataset from Lookout's global sensor network of millions of devices, pairing it with insight from its top security researchers to give you actionable intelligence on the latest mobile threats and risks.

Click here to learn more about Threat Advisory