tracesecurity

A Sample of SMS Phishing Test Results in Enterprise Organizations

One year after the launch of our SMS phishing technology, we provide insights into the results of pilot testing campaigns with enterprise organizations on a global scale.

October 2020

Introduction

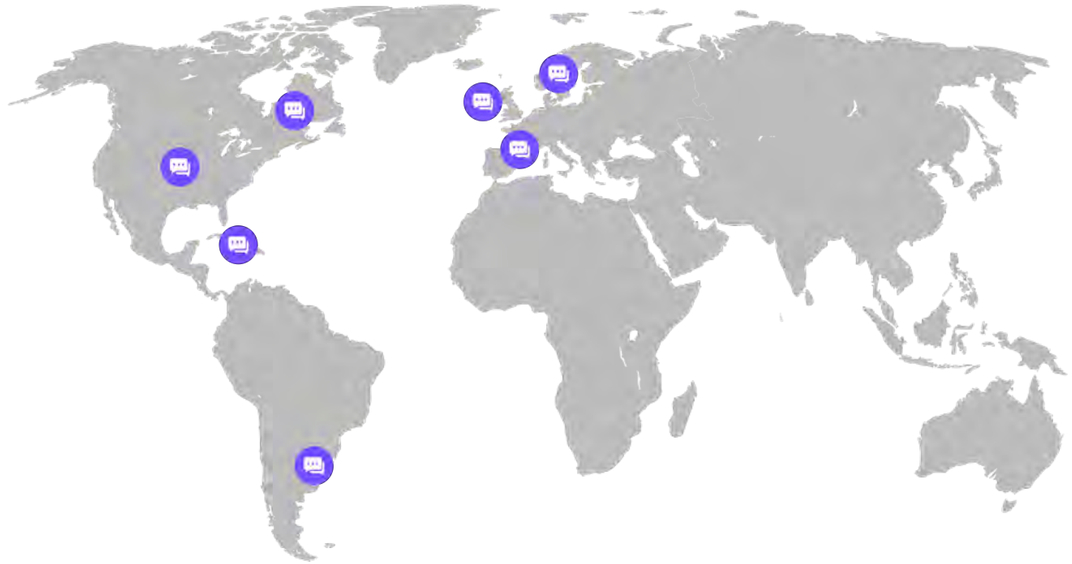
TraceSecurity introduced the first SMS phishing, or *smishing*, solution in 2019.

The pilot program was made available to a limited number of organizations to ensure scalability and compliance with international regulations for wireless communications.

The following briefing provides insight into the findings and observed state of awareness regarding SMS phishing and *SIM Jacking* among enterprises in the early campaigns.

The organizations are anonymous, the industries are unrelated, and the data is presented in aggregate.

Financial institutions by region



By the numbers

Sample size of early pilot engagements

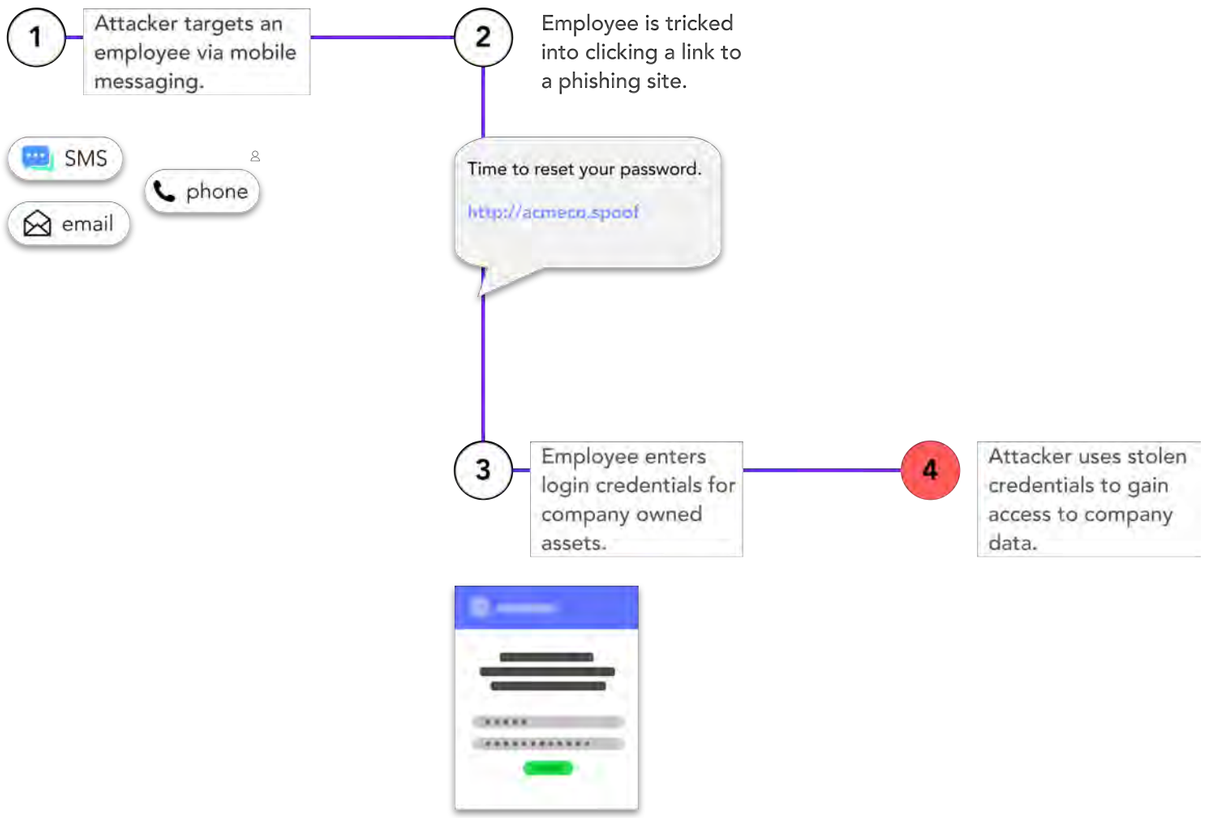
100,000+
SMS messages sent

13
countries

5
languages

SIM Jacking

A social engineerg attack that exploits a mobile phone service provider's ability redirect a telephone number to a device containing a different Subscriber Identity Module (SIM) that is normally used when a customer has lost or had their phone stolen, or upgrading devices.



Jack Dorsey's Twitter account was hacked through SIM Jacking in 2019.

Sample Test + Results

Overview

Posing as the client's IT organization, our analysts sent messages to employees requesting they verify their current PIN for their company owned SIM card.

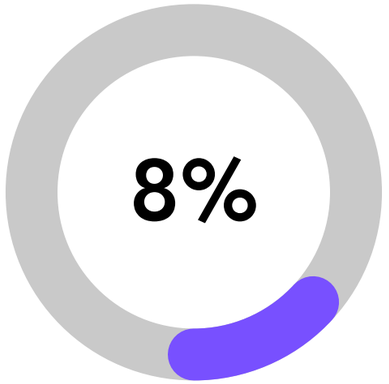
The SMS messages contained a link to a landing page that closely mimicked the design of a local wireless carrier and contained data input fields to collect the PINs. Even though the input fields were completely interactive, no actual data was recorded upon submittal.

TraceSecurity recorded message opens, link clicks, and attempted data submissions.

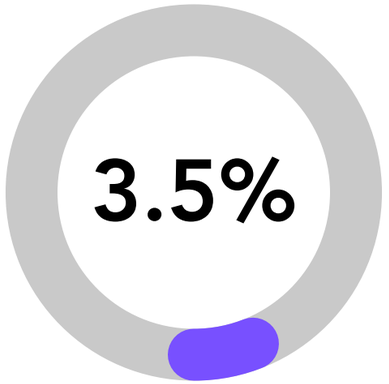
Results

Across all companies tested, on average; 8% of employees opened the link, 3.5% submitted their PIN for the company owned device, and 40% of the employees who failed by submitting their data, r***efreshed the landing page and resubmitted the data a second time***.

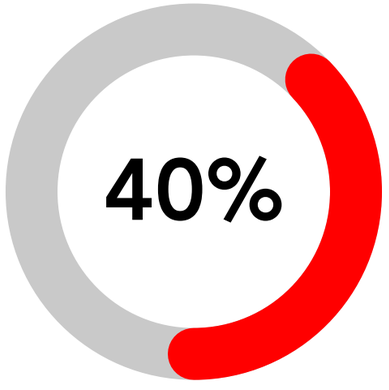
While 3.5% may seem nominal at first glance, it is significant when measuring the risk exposure of an ogranization with 10,000+ employees.



of employees opened the link



Submitted their PIN



of employees who submitted data, refreshed the page and resubmitted data after the first error message

tracesecurity | Insights