PhishMe: Disrupting Cyber Attack Detection & Response

The PhishMe Ecosystem
January 2015
Spear Phishing: The Attack Vector of Choice

91% of cyberattacks that begin with spear phishing
We Have a Detection Problem!

Median number of days that attackers were present on a victim network before detection\(^1\)

Percentage of breaches that went undetected for “months or more”\(^2\)

1 \[\text{www.mandiant.com/resources/mandiant-reports/}\]
2 \[\text{http://www.verizonenterprise.com/DBIR/2013/}\]
We Need to Cultivate Human Attack Sensors

2010 Times Square car bombing attempt

From Wikipedia, the free encyclopedia

The attempted car bombing of Times Square on May 1, 2010, was a planned terrorist attack which was foiled when two street vendors discovered a car bomb and alerted a New York Police Department (NYPD) patrolman to the threat after they spotted smoke coming from a vehicle. The bomb had been ignited, but failed to explode, and was disarmed before it caused any casualties.[1][3][4]

Two days later federal agents arrested Faisal Shahzad, a 30-year-old Pakistan-born resident of Bridgeport, Connecticut, who had become a U.S. citizen in April 2009.[5] He was arrested after he had boarded Emirates Flight 202 to Dubai at John F. Kennedy International Airport.[5][6][7][8][9] He admitted attempting the car bombing and said that he had trained at a Pakistani terrorist training camp, according to U.S. officials.[10]

United States Attorney General Eric Holder said that Shahzad's intent had been "to kill Americans."[5] Shahzad was charged in federal court in Manhattan on May 4 with attempted use of a weapon of mass destruction and other federal crimes related to explosives.[5] More than a dozen people were arrested by Pakistani officials in connection with the plot. Holder said the Pakistani Taliban directed the attack and may have financed it.[11]

U.S. Secretary of State Hillary Clinton warned of "severe consequences" if an attack like this were to be successful and traced back to Pakistan.[12] The Obama administration saw a need for retaliatory options, including unilateral military strike in Pakistan, if a future successful attack was to be traced to Pakistan-based militants.[13]

On October 5, 2010, Shahzad was sentenced to life in prison after pleading guilty to a 10-count indictment in June, including charges of conspiracy to use a weapon of mass destruction and attempting an act of terrorism.[14]
Mitigation is necessary

..but not sufficient
Can Employees Act as Attack Sensors?

- People respond to emails quickly
- Empowered and encouraged users report
- IR & SOC teams get relevant and timely threat intelligence
- New source of “big data”
PhishMe Reporter: User-sourced Detection

- Simplified single-click reporting for users
- Standardized submission format for IR/help desk
- Taps into human intelligence
- Generate a new source of threat data
Shrink Detection Time to Seconds

At 8:07 PM, the first of several diligent users reported the attack – 11 minutes before the first compromised user clicked on the fraudulent link (8:18 PM).

Next set of users correctly identified the attack

Customer deployed Reporter to 80,000 endpoints
Recent deployment
Established reporter install base

Response Breakdown

75.16%
17.52%
7.32%

Clicked Link
Opened Email, only
Unread/No Response

Responses by Day

Dec 5:
3 Recipients Clicked Link
3 Recipients Reported Phish

Reports by Day

0k
5k
10k
7.5k
5k
0
0
7.5k

New Reporter
Repeat Reporter
First Reporter Nov 17, 14 7:07PM
First Click/Open: Nov 17, 14 7:18PM

07:30 PM 08:00 PM 08:30 PM 09:00 PM

© Copyright 2014 PhishMe, Inc. All rights reserved.
The new face of incident detection

VP, Finance and avid reporter of suspicious emails

Discovered Dyre malware

*How many Sams do you have in your organization?*