THE STATE OF THE PHISH AND RESPONSE

Mike Saurbaugh
Director, Technical Alliances
PhishMe
• Founded in 2011 and technology first deployed in 2008

• HQ – Washington, Offices - New York, San Francisco, Birmingham (AL), London, Dubai, Singapore, Melbourne

• 1,600+ active customers – 50+% of the Fortune 100

• Licenses span over 25 Million seats globally

• 425+ Employees

• External Investors: Paladin Capital, Aldrich Capital and Bessemer Ventures
• Prairie dogs have a complex ability to provide warning of approaching predators… or threats to their organization.

• Data is provided through a series of ‘chee’ like calls.

• Members of the community respond to the warning.

• Communication is nearly as complex as that of dolphins.

• Convey specific threat types – hawk, coyote, domesticated dog, human.

• Can differentiate details.
AWARENESS IS NOT THE PROBLEM

QUESTION - Phishing is a term used to describe a deceptive email designed to infect your computer or steal your passwords. Were you already aware of that before reading this definition?

- 94.4% are aware of phishing
- 5.6% are not aware
Number of reported security incidents rose 48 percent last year*
  • Spear-phishing attacks rose 55%
  • Ransomware attacks grew 4X

Big losses were more common last year as organizations reporting financial loss in excess of $20 million rose 92 percent.*
  • Business Email Compromise (BEC) losses skyrocketed 1300%.

* The Global State of Information Security® Survey 2015, a worldwide survey by CIO, CSO and PwC
INTELLIGENCE

Dropbox, Google Drive, and Generic Email Phish Clusters for March 1, 2017 to April 10, 2017

554 of 2534 phish
ThreatID 25496992

214 phish
ThreatID 25497222

205 phish
#25494659

91 phish
#25496988

81 phish
#25495460

75 phish
#25496093
• Each dot on the cluster maps represents a phishing site that is composed of the same files that make the site at the center of each core.

• This illustrates the Domain, IP address, drop email addresses, and other relevant information.
Demonstrated the intersection of phishing and cloud services

Malicious code was not executed on the endpoint

Nor was it designed to create a fake login page

2017 revisits 2010
INTELLIGENCE

LOCKY BORROWS FROM DRIDEX
INTELLIGENCE CAN YOU SEE ME NOW?

- Steganography
- Word doc with macro script to download image
- Hide malware (exe) in benign content (JPEG)
INTELLIGENCE

LOCKY OR TRICKBOT?

```javascript
choice = detectCountry()
need = Array("GB",
If UBound(Filter(name))
mual = Array("auto",
Else
mual = Array("astil"
End If
```
mymonero.com ≠ mymonero.com

https://mymonero.com
default

The Simplest Way to Use Monero
Send and receive Monero safely and securely, anywhere and any time

Create an Account

https://twitter.com/lukasstefanko/status/920541599339368449  @LukasStefanko
Find Bad Faster

- Earlier Detection
- Minimize incident scope
- Reduce incident response costs
- Limit the ability for attackers to move freely on your network (attacker slack time)
EMPLOYEE CONDITIONING

Self Enumeration
- Technical Baseline
- Process Baseline

Simulation Design
- Phishing Intelligence
- IR Models
- SIM Results Data

Simulation Delivery
- Entire User Base
- Spear Phishing
- Repetition
- Analyze Results

Reporting
- Focus for ALL Awareness Activities
- Track Simulation Reports
- Track Suspicious Email Reports

Triage and Mitigation
- Analyze Reported Emails
- Categorize Types
- Neutralize Threats

Left of Breach
EMPLOYEE CONDITIONING

- Overt versus covert is very
- Leadership support and show
- Positive vs. negative tone
- Keep it simple
- Empower and encourage results
- May take 6-months to 1-year results

After baseline and employees are reporting and less susceptible

What is happening in the wild today?

Assess higher risk employees (executives, DBAs, HR, IT)

Based on previous improvements, selective spear phish

Business context
Curiosity
Entertaining
Avoid the “how bad is it” penetration test approach
Move away from susceptibility rate only
Avoid punishment
Don’t ‘game’ the system to make stats look good

Reporting enhances incident response
Otherwise, hacker dwell time persists if host(s) are compromised or creds stolen
IR teams can disrupt the attacker’s mission when employees report
Drive down time to report (minutes vs. days)
HUMAN PHISHING DEFENSE

Decrease in Repeat Offenses

Number of Times Responded

Population That Responded

- 35% for 1 Response
- 13% for 2 Responses
- 4% for 3 Responses
- 1% for 4 Responses
- 0% for 4+ Responses
PHISHME INCIDENT RESPONSE

• Automation and orchestration
Prioritize based on:
→ High Volume
→ Strong Reputation
→ Didn’t match an existing rule!
→ Recently Reported

Create Playbooks (Recipes for Automation):
→ To process future reports similarly
→ Respond to employees
→ Simplify creation of YARA rules
→ Export bad URLs, MD5 hashes to other systems
PREP & INCIDENT RESPONSE

✓ Reported by employees
✓ Analyze reported email
✓ Assess and remediate (integrations are key)
✓ Employee feedback
✓ Postmortem

✓ Get IR and helpdesk on board
✓ Supportive of the mission
✓ Not silos
✓ Opportunity to address weaknesses
✓ Working with IR and Intelligence teams and sources of intelligence
✓ What is happening *right now?*
✓ This is what the attackers *will* do!
Mike Saurbaugh
Director, Technical Alliances
mike.saurbaugh@phishme.com

phishme.com/blog
phishme.com/resources/videos
phishme.com