Defending Against Phishing

Effective Phishing Incident Response Using Employees, Incident Responders, and Intelligence

Mike Saurbaugh, Director, Technical Alliances
October 19, 2016
• Founded in 2011
• Technology first deployed in 2008
• HQ – Washington, Offices - New York, San Francisco, Birmingham (AL), London, Dubai, Singapore, Melbourne
• 1,000+ active customers
  • 50+% of the Fortune 100
• Licenses span over 20 Million seats globally
• 6 Patents granted, several pending
• 275+ Employees
• External Investors: Paladin Capital, Aldrich Capital and Bessemer Ventures
But experts say a fully automated vehicle that is **100 percent safe 100 percent** of the time and can operate on any street in any weather condition in the U.S. is not right around the corner. It's a decade or more down the road.

"We as humans have common sense and reasoning powers that we apply, and most of the time, if not always, we do the right thing," said Rajkumar. "Computers, though very powerful, are unfortunately lacking in common sense.

"Self-driving cars can only do what programmers tell them to do. They can't anticipate everything that can happen on the road."

Thinking Fast, Thinking Slow

<table>
<thead>
<tr>
<th>System 1</th>
<th>System 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fast</td>
<td>Slow</td>
</tr>
<tr>
<td>Unconscious</td>
<td>Conscious</td>
</tr>
<tr>
<td>Automatic</td>
<td>Effortful</td>
</tr>
<tr>
<td>Everyday Decisions</td>
<td>Complex Decisions</td>
</tr>
<tr>
<td>Error prone</td>
<td>Reliable</td>
</tr>
</tbody>
</table>

https://www.amazon.com/Thinking-Fast-Slow-Daniel-Kahneman/dp/0374275637/ref=tmm_hrd_swatch_0?_encoding=UTF8&qid=1471289790&sr=1-1

© Copyright 2016. Confidential. PhishMe, Inc. All rights reserved.
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)

Cyber Threat Kill Chain

© Copyright 2016. Confidential. PhishMe, Inc. All rights reserved.
Simulation – Conditioning Employees

• Employee behavior can be modified via repeated exposure to a variety of phishing simulations.

• Increased repetitive exposure causes early recognition of themes and tactics.

• Increased exposure to various themes also helps condition employees to be wary and suspicious of previously unseen emails.

4 simulations yields a 97% decrease
Enable Human Sensors

Attacker Surveillance
Target Analysis
Access Probe
Attack Set-up
System Intrusion
Attack Begins
Discovery/Persistence
Cover-up Starts
Leap Frog Attacks Complete
Cover-up Complete
Maintain foothold
TIME

ATTACKER FREE TIME
Need to shrink free time

Detect earlier

Response
Recovery
System Reaction
Damage Identification
Incident Reporting
Containment & Eradication
Impact Analysis
Response & Controls
Monitoring & Controls
Attack Forecast
Attack Identified
Containment & Eradication
System Reaction
Recovery
Response

© Copyright 2016. Confidential. PhishMe, Inc. All rights reserved.
Zero-Day Exploits – Reported

THREE “LAWFUL INTERCEPT” PRODUCTS USED AGAINST MANSOOR

From: Marcuzz & Scott-Railton
The Million Dollar Dissident: NSO Group’s iPhone Zero Days used against a UAE Human Rights Defender

CITIZEN LAB 2016
Defending Business Email Compromise (BEC)
Managing Reported Email
## Triage – Organize, Analyze, Respond

### Syslog

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Off</td>
</tr>
<tr>
<td>Format</td>
<td>CEF</td>
</tr>
<tr>
<td>Host</td>
<td>172.20.1.1</td>
</tr>
<tr>
<td>Port</td>
<td>1514</td>
</tr>
</tbody>
</table>

**Categorized Reports**

- **Priority: 4**
  - Size: 2 reports
  - Reputation Score: 197

**Sent Syslog Events For**

- **Active Clusters**
  - Active in the last 3 months

**Pie Chart**

- Non-Malicious: 36.8%
- Advanced Threats: 31.6%
- Crimeware: 29.8%
- Spam: 9.8%
Output to SIEM

start=JUL 26 2016 20:55:21
rt=JUL 27 2016 08:20:35
deviceCustomDate1=JUL 27 2016 08:17:08
duser=support@phishme.com
suser=accountspayable@example.com
cat=Crimeware
cs1=Crimeware_workflow  cs1Label=Recipe Name
cn1=4  cn1Label=Highest Priority Rule Matched – Priority Level
cs2=PM_Locky_Delivery cs2Label=Highest Priority Rule Matched - Rule Name
cs3=https://hostnamevm/reports/14 cs3Label=Report URL
cs4=urgent invoice cs4Label=Subject
Data $\neq$ Intelligence

Information without context is data

Intelligence is information with context

Human-Verified $==$ Operationalized
3, 2, 1 – Context!

Microsoft Office documents with malware delivery scripting

This category of hostile files represents an infection vector that has been in use for many years but still

<table>
<thead>
<tr>
<th>Locky PaySites</th>
</tr>
</thead>
<tbody>
<tr>
<td>hxxp://zjfq4lnfbs7pncr5.tor2web.org</td>
</tr>
<tr>
<td>hxxp://zjfq4lnfbs7pncr5.onion.to</td>
</tr>
</tbody>
</table>

View Threat Detail: https://www.threathq.com/p42/search/default?malware=6631

<table>
<thead>
<tr>
<th>New Doc 520-58.docm</th>
<th>6e6b500abe229b41dad085319c328a6</th>
<th>35,922</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Doc 8-51.docm</td>
<td>38e51b4970e3acdb09b5a1dbef76c0</td>
<td>5,102</td>
</tr>
</tbody>
</table>

Bitcoin required for payment.
Ransomware – Just Getting Started?
Ransomware Trends

Percentage of Ransomware Analyses

- Other Ransomware
- PowerWare
- Bart
- Troldesh
- Cerber
- Locky
- CTB
- TeslaCrypt
- CryptoWall

Month
- January 2016
- February 2016
- March 2016
- April 2016
- May 2016
- June 2016
- July 2016
- August 2016
Ransomware Trends

![Graph showing ransomware trends]

Number of Campaigns Analyzed

- **Locky**: 336
- **Cerber**: 90
- **TeslaCrypt**: 61
- **CryptoWall**: 26
- **CTB**: 12
- **Troldesh**: 3

Ransomware Variety
Hiding in Plain Sight

000042c0: 5b6a 5986 26cc 0d88 d86f 198d 0b79 2e29
000042d0: 74a7 5105 248b 13e2 371e ce00 fa08 c663
000042e0: 3198 f2cd 4bff d93e 29e3 7370 7373 7377
000042f0: 7373 738c 8c73 73cb 7373 7373 7373 7373
00004300: 7373 7373 7373 7373 7373 7373 7373 7373
00004310: 7373 7373 7373 7373 7373 7373 7373 7373
00004320: 7373 73ab 7373 737d 6cc9 7d73 c77a be52
00004330: cb72 3fbe 5227 1b1a 0053 0301 1c14 0112
00004340: 1e53 1012 1d1d 1c07 5311 1653 0106 1d53
00004350: 1a1d 5337 3c20 531e 1c17 165d 7e7e 7957
00004360: 7373 7373 7373 73e2 7d30 a3a6 1c5e f0a6
00004370: 1c5e f0a6 1c5e f081 da25 f0af 1c5e f0a6
00004380: 1c5f f0be 1c5e f0b8 4edd f0a7 1c5e f0a6
00004390: 1c5f f0be 1c5e f0b8 4edd f0a7 1c5e f0b8
000043a0: 4ecf f0a7 1c5e f021 1a10 1ba6 1c5e f073
000043b0: 7373 7373 7373 7373 7373 7373 7373 7323
000043c0: 3673 733f 7277 7326 1750 2473 7373 7373

PhishMe Confidential. All rights reserved.
Threat Intelligence Case Study – Background

- Global retailer
- Needed insight into criminal infrastructure worldwide
- Many providers didn’t have depth into phishing infrastructure
- Gateways missing too much
- Context was a must-have
- Analyze campaigns and changes to infrastructure
- Over 40 feeds (many of which they have to de-duplicate)
Threat Intelligence Case Study – Production Workflow

1. Ingest Intelligence into SIEM
2. Enriched and applied to blocking rules
3. Alerts trigger IR team to engage
4. Analysts use Active Threat Reports for context around IOC
5. Host(s) are contained and threat(s) remediated
6. Retailer’s advice: correlate IoCs to network traffic, block, remediate
Conditioning, IR, Intelligence

**Condition Employees** to
Recognize and Report
Phishing Threats

**Speed Incident**
Detection and Response
Leveraging
Internal Attack Reports and
Phishing Threat Intelligence
For More Information

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