INFORMATION SECURITY UPDATE

STEVE READY
SYSTEM VP, CHIEF INFORMATION OFFICER, NORTON HEALTHCARE

RON PELLETIER
PARTNER, PONDURANCE
CURRENT STATISTICS

2015
Total Monthly Email
1.2 million
Total Monthly Blocked Email
1.6 million

2016
Total Monthly Email
1.4 million
Total Monthly Blocked Email
2.8 million

2017/18
Total Monthly Email
2.61 million
Total Monthly Blocked Email
1.41 million

50% reduction with high risk email
Cyber Threats Evolving

< - 2014

• Information Extraction
• Scripting Malware and Hobbyists
• Steal Credentials Extract PHI
• Stay Under the Radar
• Rise of Dark Web

2015 - 2016

• Ransomware
• Rise of For Profit Hacking
• Encrypt Files and Extract a Ransom
• Political Hacks Make National Headlines
• Looking for Pay Day
• Enabled by Crypto Currency

2017 - 2018 >

• Operations Interruption
• Nation States and Hacktivists are a larger player
• Goal Becomes Taking Over Operational Control and Extract Ransoms
• Large Profits
• Global Agendas
# Additional High Profile Threats

<table>
<thead>
<tr>
<th>Discovered</th>
<th>June</th>
<th>July</th>
<th>July</th>
<th>August</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impact</td>
<td>• Ransomware Attack</td>
<td>• Brute Force Attack Against Cloud Customers</td>
<td>• Service Interruption</td>
<td>• Potential Risk to Siemens Medical Equipment</td>
</tr>
<tr>
<td></td>
<td>• WannaCry Variant</td>
<td>• Detected 100,000 failed-login attempts across 7 months</td>
<td>• Related to a Malware Attack</td>
<td>• Recommended taking systems offline</td>
</tr>
<tr>
<td></td>
<td>• Targeted Unpatched Windows Machines</td>
<td>• Considered a “slow and low” strategy designed to avoid detection</td>
<td>• Impacted ability to support NHC through normal channels</td>
<td>• Deferred patients at NHC</td>
</tr>
<tr>
<td></td>
<td>• Service and Operations Interruptions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Nationwide Impact</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Norton Response</td>
<td>• Froze Email Attachments</td>
<td>• Monitoring</td>
<td>• Site Blocked</td>
<td>• Tactical Segmentation</td>
</tr>
<tr>
<td></td>
<td>• Monthly Patching</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Norton Response**

- Froze Email Attachments
- Monthly Patching
- Monitoring
- Site Blocked
- Tactical Segmentation
SHADOW BROKERS - UPDATE

Initial Subscription

• “Wine of the month Club”
• $21k per month in cryptocurrency
• Each month the group releases security exploits and user-ids

Current model

• They have seen incredible success with the subscriptions
• They have increased the fees to $64k per month
• Created a VIP section for members to pay a one-time fee of $128k for additional cyber weapons
Executive Incident Response

- Executive Incident Response Table Top conducted on August 16, 2017
- Representatives from the executive team attended the table top exercise
- Presented a real world scenario and discussed best practices for responding to a cyber incident
- Discussed opportunities to include steps for executive response in the event of a cyber incident
- Annual Event, will include real data (both attack and defend) from Pondurance
Pondurance is a Full Services Cyber Security Firm

CHICAGO OFFICE
111 W Jackson St
Suite 1700
Chicago, IL 60604

INDIANAPOLIS OFFICE
PRIMARY SOC
500 N Meridian St
Suite 500
Indianapolis, IN 46204

TAMPA OFFICE
ALTERNATE SOC
360 Central Ave
Suite 668
St. Petersburg, FL 33701

HEALTHCARE BY THE NUMBERS
41% OF OUR CUSTOMER PORTFOLIO IS HEALTHCARE

60 HEALTHCARE ENGAGEMENTS OVER THE LAST YEAR

12 HEALTHCARE THREAT CLIENTS

24 HEALTHCARE SPECIFIC INCIDENT RESPONSE ENGAGEMENTS

3 SEPARATE INTERACTIONS WITH THE OCR ON BEHALF OF CLIENTS
Quick Note on “Breach Season”

• Sharp increase in reported breach events for healthcare companies between February – April
• Criminal groups are well organized and well funded, usually planning their endeavors in the Q3 timeframe, executing reconnaissance and initial attacks in Q4, breach finally detected in Q1-Q2 timeframe
• Also influenced by tax season and the “hurried” nature of financial transactions, which malicious actors take advantage of (i.e., tax fraud, wire fraud, etc.)
Profile of Incidents

Hancock Health – Highly publicized ransomware event, Pondurance provided IR services to provide crisis management and restoration

• Large Health System Southeast—Pondurance provided forensics investigation to determine extent of an Office365 email breach and compromise

• Health System in Florida – Pondurance is providing Corrective Action Plan monitoring related to an action taken by the OCR, related to a breach investigation

Key Takeaways

• Multi-factor Authentication, Vulnerability Management, Threat Hunting Services

• Check with your Cyber Insurance Broker, know your options for incident response

• Ensure you have the right amount of logging and auditing enabled

• Take the time to do your post-incident analysis to determine your reporting obligations

• Security is not cheap, but ensure you right-size your program