Decrypting a Ransomware Strategy

Rebecca Warren
Hussein Syed
Erica Woebse

Discussion Points
• Health IT
• Security in Healthcare
• Ransomware
• Breach Risk Maturity
• Discussion

Delivery of Care Has Transformed

MORE TECHNOLOGY ENHANCED ACCESS HIGHER AVAILABILITY

...YET HEALTHCARE IS STILL NOT SECURE
Provider / Patient Infrastructure

- Family physicians / PCP / GP
- Specialist clinics
- Blood lab
- X-Ray / Cat. Scan provider
- Local hospital
- Rehab facility after hospital discharge
- Other patient records
- Insurance company (payer)
- Health Information Exchanges
- EMR-to-EMR Integration
- Data Sharing
- Data push to patients & other providers
- Data push to the State, research consortiums
- Data push of lab results to providers
- Data pull from EMRs for visiting patients (Patient Portal)
- IoT
- Medical Devices

Transformed Care is a Hotbed for CyberSecurity

- Digitalizing patient record
- Sharing patient across H/LS ecosystem
- Data-based collaborative care
- Analytics to enhance care
- Electronic registries for population health
- Personalized medicine

DATA EXPLOSION
Unprecedented Security Risk

“WHAT THREAT VECTOR IS MOST CONCERNING TO YOU AND WHY.”
The Next Battleground

CHANGING HEALTHCARE LANDSCAPE

HAVE WE BEEN HACKED?
SECURITY INCIDENTS AND BREACHES

<table>
<thead>
<tr>
<th>BREACH TYPE</th>
<th>AFFECTED ENTITIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>329 2016 &amp; 51 2017 REPORTED BREACHES OF 500 OR MORE AFFECTED</td>
<td>713 14</td>
</tr>
<tr>
<td>16.6MM INDIVIDUALS AFFECTED</td>
<td>425K</td>
</tr>
<tr>
<td>425K INDIVIDUALS AFFECTED</td>
<td>2016 &amp; 51 2017 REPORTED BREACHES</td>
</tr>
<tr>
<td>OVER $20MM IN FINES IN 2016</td>
<td>329 2016</td>
</tr>
<tr>
<td>OVER $11MM IN FINES IN 2017</td>
<td>51 2017</td>
</tr>
</tbody>
</table>

Source: U.S. Department of Health and Human Services
Office for Civil Rights Breach Portal
https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

OVER $11MM IN FINES IN 2017
OVER $20MM IN FINES IN 2016

Notable Breaches in 2016

<table>
<thead>
<tr>
<th>AFFECTED ENTITIES</th>
<th>NO.</th>
<th>BREACH TYPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCESS/DISCLOSURE</td>
<td>256</td>
<td>329</td>
</tr>
<tr>
<td>329</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TYPE NOT DISCLOSED</td>
<td>51</td>
<td></td>
</tr>
<tr>
<td>TOTAL</td>
<td>329</td>
<td></td>
</tr>
</tbody>
</table>

| NOT SPECIFIED | 9 |
| HEALTH PLAN | 2 |
| HEALTHCARE PROVIDER | 20 |
| NOT SPECIFIED | 3 |
| TOTAL | 329 |

| ACCESS/DISCLOSURE | 40 |
| 40 |
| IMPROPER DISPOSAL | 51 |
| TOTAL | 20 |

| ACCESS/DISCLOSURE | 51 |
| 51 |
| THEFT | 1 |
| TOTAL | 51 |

| ACCESS/DISCLOSURE | 62 |
| 62 |
| UNAUTHORIZED ACCESS/DISCLOSURE | 21 |
| TYPED NOT DISCLOSED | 5 |
| TOTAL | 91 |

| ACCESS/DISCLOSURE | 113 |
| 113 |
| LOST | 51 |
| TOTAL | 164 |

| ACCESS/DISCLOSURE | 51 |
| 51 |
| IMPROPER DISPOSAL | 51 |
| TOTAL | 102 |

14 Ransomware Incidents
Hospitals are hit with 88% of all ransomware attacks

MedStar Health
THEFT VS HACKING TREND

Source: U.S. Department of Health and Human Services
Office for Civil Rights Breach Portal
https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Healthcare Industry: Challenges – Cyber Threats

Frequency & Velocity
E.g. Ransomware
Zero Day
Malware

Business Impact
$400B Market
Cyber Crime
L赔付s

Typical Ransomware Infection
Ransomware is malware for data kidnapping, an exploit in which the attacker encrypts the victim's data and demands payment for the decryption key. Ransomware spreads through e-mail attachments, infected programs and compromised websites.
DISCUSS SOME OF THE WAYS YOU CAN BREAK THE KILL CHAIN AND DEFEND AGAINST MULTI-VECTOR ATTACKS.

Decrypting a Ransomware Strategy
SECURE NETWORK THREAT DETECTION & ANALYSIS

Sample Secure Network Topology
**Segmentation: Not all assets are equal**

**LIFE CRITICAL:**
No Internet -> Connection to Internal; APPS and DC only
Highly Segmented from the rest of the network
SEGMENTED NETWORK

**HIGH PHI/PII/PCI:**

**Low/Medium:**
DNS Firewalling, Endpoint Protection, Server side Protection, Proxyed Internet Access, Content Filtering/Inspection.

**Security Operations Center**

**SOC: Data Aggregation for Improved Incident Handling**

Visibility.
By centralizing these various sources of data into a security monitoring system, the SOC gains actionable insight into threats and anomalies indicative of threat activity.

Analysis.
Security operations analysts can analyze data from various sources and further interrogate and triage devices of interest to scope an incident.

Action.
Based on findings, automated and manual interventions can be made to include patching, threat remediation, system quarantine, and credential revocation.
Tiered Security Operations

- SOC Alert Analyst
- Tier 2 Incident Responder
- SME/Hunter

Threat Management

- Consolidate functions of incident monitoring, detection, response, coordination, and computer network defense tool engineering, operation, and maintenance under one organization: the Cyber Security Operations Center (CSOC.)
- Achieve balance between size and visibility/agility, so that the CSOC can execute its mission effectively.
- Give the CSOC the authority to do its job through effective organizational placement and appropriate policies and procedures.
- Focus on a few activities that the CSOC practices well and avoid the ones it cannot or should not do.
- Favor staff quality over quantity, employing professionals who are passionate about their jobs, provide a balance of soft and hard skills, and pursue opportunities for growth.
- Realize the full potential of each technology through careful investment and keen awareness of—and compensation for—each tool's limitations.

Common Vocabulary

- Attack method: The manner or technique and means an adversary may use in an assault on information or an information system.
- Exfiltration: The unauthorized transfer of information from an information system.
- Attack Vector
- Indicator of Compromise
- C2—command and control
- DPP (Deep Packet Processing): Deep Packet Processing delivers the ability to inspect, forward, drop, clone, or even modify network traffic, at line rates. With Deep Packet Processing and combinations of policies and/or programming, the lag time from inspection to action drops from minutes or hours or worse, days, to milliseconds.
- EPP (endpoint protection): Including host-based features like firewall, anti-malware, whitelisting and disk encryption
- EVC—Endpoint Visibility and Control
- ETDR—endpoint threat detection and response
- Tactical Threat Intelligence—often referred to as tactics, techniques and procedures (TTPs) and is information about how threat actors are conducting attacks
- TTPs—Tools, Techniques and Processes
Threat Intelligence

- Cyber Intel Collection and Analysis: Collection, consumption, and analysis of cyber intelligence reports, cyber intrusion reports, and new related information security covering new trends, vulnerabilities, products, and research.

- Cyber Intel Distribution: Synthesis, summarization, and redistribution of cyber intelligence reports, cyber intrusion reports, and news related to information security to members of the constituency on either a routine basis (such as a weekly or monthly cyber newsletter) or a non-routine basis (such as an emergency patch notice or phishing campaign alert).

- Cyber Intel Creation: Primary authorship of new cyber intelligence reporting, such as threat notices or highlights, based on primary research performed by the SOC. For example, analysis of a new threat or vulnerability not previously seen elsewhere. This is usually driven by the SOC’s own incidents, forensic analysis, malware analysis, and adversary engagements.

- Cyber Intel Fusion: Extracting data from cyber intel and synthesizing it into new signatures, context, and understanding of adversary TTPs, thereby existing monitoring operations (e.g., new signatures or SIEM content).

- Trending: Long-term analysis of event feeds, collected malware, and incident data for evidence of malicious or anomalous activity or to better understand the constituency or adversary’s TTPs (Tools, Techniques and Processes). This may include unstructured, open-ended, deep dives into various data feeds, trending and correlation over weeks or months of log data, “low and slow” data analysis, and explicit anomaly detection methods.

- Threat Assessment: Holistic estimation of threats posed by various actors against the constituency, its enclaves, or lines of business, within the cyber realm. This will include leveraging existing resources such as cyber intel feeds and trending, along with the enterprise’s architecture and vulnerability status. Often performed in coordination with other cybersecurity stakeholders.

Security Outreach

- Product Assessment: Testing the security features of applications being acquired by constituency members. Analogous to vulnerability assessments of one or a few hosts, this testing allows in-depth analysis of an application’s strengths and weaknesses.

- Security Consulting: Providing cybersecurity advice to constituencies outside the scope of CND; supporting new system design, business continuity, and disaster recovery plans; and performing threat modeling, risk assessments, and other efforts.

- Security Outreach: Direct communication with the news media. The SOC is responsible for all aspects of information technology impacting the reputation of the constituency or ongoing response.

Decrying a Ransomware Strategy

BREACH SECURITY ASSESSMENT
Healthcare Breach Security Assessment Program

- Created by Intel and VMware
- The assessment is free of Cost
- Confidential
- Contact:
  Chris Logan
  Sr. Healthcare Strategist
  VMware Healthcare
  clogan@vmware.com

Breach Security Assessment
How it Works

- One (1) hour assessment
- By conference call or in person
- Priority across 8 breach types
- Presence of 42 breach security capabilities from the maturity model
- Org type, country, size for future comparison with similar peers
- Post assessment and quarterly reports
- Maturity score, priorities and capabilities benchmarked against industry
- Spreadsheet used to gather assessment input
- No personally identifiable information or patient information collected

Breach Types Assessed

1. Cybercrime Hacking
2. Ransomware
3. Loss or Theft of Mobile Device or Media
4. Insider Accidents or Workarounds
5. Business Associates
6. Malicious Insiders or Fraud
7. Insider Snooping
8. Improper Disposal
Breach Security Capabilities Maturity Model

Baseline
- Policy
- Risk assessments
- Audit and compliance
- User training
- Endpoint device encryption
- Business associates agreements
- Virtualization

Enhanced
- Server solid state drive (encrypted)
- Network data loss prevention (prevention)
- Database activity monitoring
- Digital forensics
- Server application whitelisting
- De-identification / anonymization
- Tokenization

Advanced
- Server solid state drive (encrypted)
- Network data loss prevention (monitoring, capture)
- Database activity monitoring
- Threat intelligence
- Server application whitelisting
- De-identification / anonymization
- Tokenization

Improved Breach Security, Usability, Cost, IT Operations

Breach Security as well as Compliance

Traceability from this breach solution to breach types, regulations, laws, standards, and other broader security frameworks

Strategic Approach

ADOPT A FRAMEWORK

PERFORM FOCUSED RISK ASSESSMENTS

DEVELOP A STRATEGIC PLAN: 3 YEARS OR MORE

FOCUS ON INCIDENT RESPONSE