

RSAConference2018

San Francisco | April 16 – 20 | Moscone Center

SESSION ID: SPO2-W12

A MULTILAYERED SECURITY APPROACH TO KEEPING HEALTHCARE DATA SECURE

Frank Bunton

VP, CISO
MedImpact Healthcare Systems, Security
@frankbunton

Larry Biggs

Security Engineer III - Threat Analytics
MedImpact Healthcare Systems, Security
@larrybiggs



#RSAC

HIPAA Compliance Framework



- Healthcare data is governed by HIPAA, the Health Insurance Portability and Accountability Act
**Not a female "HIPPA" as it turns out*
- The HIPAA Privacy Rule is deeply concerned about Personal Health Information (PHI)





- 18 key elements to focus on
- HIPAA Privacy rule protects individually identifiable health information of deceased individuals for 50 years
- HIPAA/HITECH have a punitive side as well – something to watch for
- Don't get us started on GDPR!

1. Names
2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code or equivalents except for the initial 3 digits of a zip code if the corresponding zone contains more than 20,000 people.
3. All elements of dates (except year) for dates directly related to the individual (birth date, admission date, discharge date, date of death). Also all ages over 89 or elements of dates indicating such an age.
4. Telephone numbers
5. Fax numbers
6. E-mail addresses
7. Social security numbers
8. Medical record numbers
9. Health plan numbers
10. Account numbers
11. Certificate or license numbers
12. Vehicle identification or serial numbers including license plate numbers
13. Device identification or serial numbers
14. Universal resource locators (URL's)
15. Internet Protocol addresses (IP addresses)
16. Biometric identifiers
17. Full face photographs and comparable images
18. Any other unique identifying number, characteristic, or code

MedImpact approach to securing information



- A balanced approach (work vs fun) with HIPAA in mind:
 - No end user administrator access on laptops/desktops
 - Security Awareness training for users
 - Patching of endpoints, servers, and devices
 - Web content filtering both on and off premises
 - Mobile device management to protect data
 - Interconnected security solutions to increase herd immunity
 - Trend Micro OfficeScan, Control Manager, Smart Protection Server
 - Trend Micro TippingPoint IP Reputation, filter-based blocking
 - Trend Micro Deep Discovery on internal networks for anomaly detection
 - Network Access Control to prevent random machines from popping up on the network
 - All tools feed into the ATT TMLA SIEM, props to Kevin Wessel and team for supporting us



A Layered Approach – Risks vs. Controls



#RSAC

	Internet	Social Engineering (Employees)	Phishing (Email)	Social Media (Malware, Personal & Corp Data)	Mobile (Personal & Corp Data)
Hardware (Appliances)	<ul style="list-style-type: none"> • IPS • Advanced Persistent Threat • VPN Firewall • Next Gen Firewall • Firewall • Security Manager • Web Content Filter • Hybrid Web Services Firewall • Network Access Control 		<ul style="list-style-type: none"> • Web Content Filtering • SPAM Filtering • Secure email • IPS • Advanced Persistent Threat 	<ul style="list-style-type: none"> • Web Content Filtering • IPS • Advanced Persistent Threat 	<ul style="list-style-type: none"> • Wireless Controller • Web Content Filtering • IPS
Tools	<ul style="list-style-type: none"> • Smart Protection Services • Anti-Virus & Endpoint Mgmt • Identity & Access Mgmt • Virtual Private Database • Secure File Transfer • Vulnerability Assessment 	<ul style="list-style-type: none"> • Security and Compliance • Policies & Procedures • Internal & External Audit Reporting 	<ul style="list-style-type: none"> • Anti-Virus • Endpoint Management 	<ul style="list-style-type: none"> • Anti-Virus • Smart Protection Services • Endpoint Management • Administrative Management • File Integrity Mgmt 	<ul style="list-style-type: none"> • Wireless Access Management • Mobile Device Management • 2 Factor Authentication

A Layered Approach – Risks vs. Controls



#RSAC

	Internet	Social Engineering (Employees)	Phishing (Email)	Social Media (Malware, Personal & Corp Data)	Mobile (Personal & Corp Data)
Training & Education	<ul style="list-style-type: none"> • Security & Compliance Training • Vulnerability Assessment Reports • Educational Articles – Intranet • Secure Coding Techniques 	<ul style="list-style-type: none"> • Security & Compliance Training • Phishing Awareness • Social Engineering Training 	<ul style="list-style-type: none"> • Security & Compliance Training • Educational Articles for Intranet • Phishing Awareness • Social Engineering Training 	<ul style="list-style-type: none"> • Security & Compliance Training • Phishing Awareness and Social Engineering Training 	<ul style="list-style-type: none"> • Security & Compliance Training
Third Party Services	<ul style="list-style-type: none"> • 7x24 SOC and Security Event & Threat Analysis • Managed Security Services • Threat Management Services • URL/IP Reputation Services 	<ul style="list-style-type: none"> • Background Checks 	<ul style="list-style-type: none"> • 7x24 SOC and Security Event & Threat Analysis • Threat Management Services 	<ul style="list-style-type: none"> • 7x24 SOC and Security Event & Threat Analysis • Threat Management Services 	<ul style="list-style-type: none"> • Security Event & Threat Analysis • Threat Management Services • URL/IP Reputation Services

No User Level Admin Access



- No end user admin access, regular users cannot install software
- You need a compensating mechanism to install software (whitelist)
- You can use rights elevation software that allows the users to install software that has already been vetted
- This can be a political battle in the beginning, once you can show results, things will calm down



Security Awareness Training



- Raise awareness of social engineering patterns and schemes
- Phishing training helps users recognize phishing attempts
- Password hygiene and multifactor authentication training
- Personal accounts and sites need to be protected just like work accounts



Web Content Filtering



- We deploy web content filtering on, and off premises to support remote users
- Web content filtering: Blocks access to sites based on categorization and reputation
- Blocks access to recently registered domain names
- If the user is remote, web traffic is sent to a cloud proxy
- If at work, traffic is sent through a local proxy
- The same filter profile is applied both on, and off premises



Mobile Device Management



- Mobile device management to protect corporate assets and data
- We use company issued iDevices to reduce attack surface and management overhead
- MDM can be used to isolate and protect company data and whitelist/blacklist applications
- MDM also supports the usual functions: find my device, wipe company data, stolen phone wipe everything, etc



Patching is critical to your survival



- Endpoints – BIOS, operating system, drivers
- Appliances – routers, switches, security gear
- Application servers – BIOS, operating system, drivers, database, application server software
- ICS – Building management systems, security systems, access control systems
- IOT – coffee machines talking to toasters becoming DDOS bots
- Software and Mobile – they're everywhere!

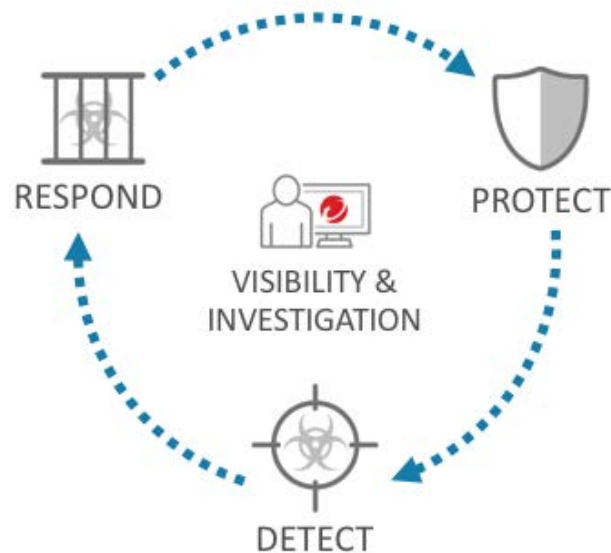


Have an inventory of your assets

AntiVirus and Endpoint Detection Response



- Trend Micro OfficeScan, Smart Protection Server, Control Manager
- Herd immunity, one device detects something, it is communicated to the rest
- Suspected files from endpoints or the security gear are sandboxed, malicious files are flagged and updates sent to the herd
- OfficeScan on the endpoint has web reputation based blocking, USB port blocking
- Leverages Trend's robust cloud Smart Protection Network



RSAConference2018



#RSAC

REAL WORLD USE CASE EXAMPLES

User Security Awareness



- In addition to our various security systems and so forth
- We have people paying attention!

From: Document via DocuSign [mailto:jason@emeraldcitycabinetcompany.com]
Sent: Tuesday, March 06, 2018 7:01 AM
To: [REDACTED]
Subject: Po-8877883-Scanned



A Document has been sent to your email below:



[Download Pdf-8877883](#)



Web filtering and Trend Micro OfficeScan reveal CoinHive



- Web filtering blocks CoinHive

- Trend Micro OfficeScan detects CoinHive

Date: Mon 25 Sep 2017 09:25:16 AM PDT
Type: Information
Source: Websense Usage Monitor

Suspicious activity has exceeded the alerting threshold for this severity level.

Severity: Medium
Category: Malicious Web Sites
Filtering action: Blocked
Threshold (in hits): 10

Log on to the TRITON Manager and access the Threats dashboard for more details about these incidents.

---Most recent incident---

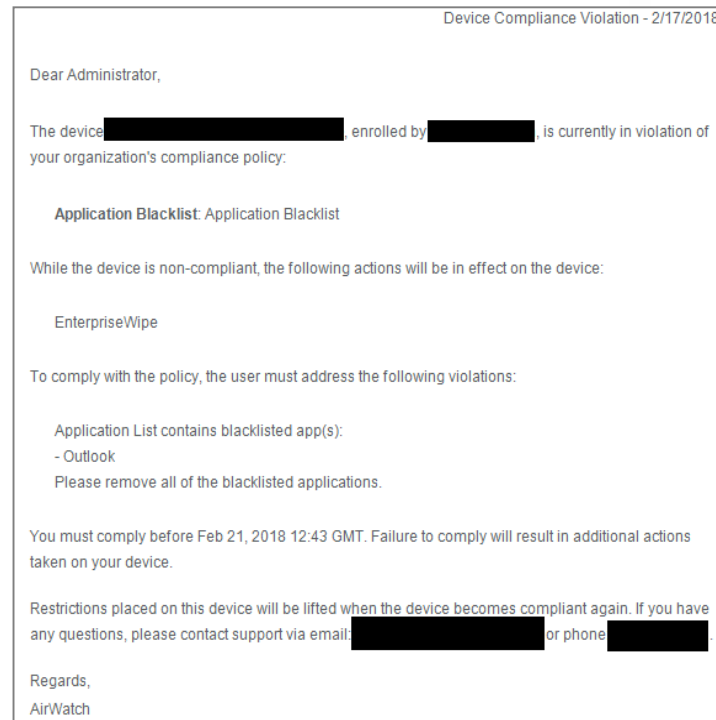
User: [REDACTED]
IP address: [REDACTED]
Hostname: [REDACTED]
URL: <https://coin-hive.com/lib/coinhive.min.js>
Destination IP address: 94.130.128.243 Port: 443

Virus/Malware: JS_COINHIVE.GA
Endpoint: [REDACTED]
Domain: [REDACTED]
File: [REDACTED]\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\F44KIN1B\coinhive.min[1].js
Date/Time: 1/10/2018 10:41:49
Result: Encrypted

Mobile Device Management Enforcing Policy



- User installs a blacklisted application
- MDM detects and schedules remediation



A Good Patching Program For The Win!



- Wannacry hits the streets May 2017
- Microsoft had already patched for the exploit in March
- MalwareTech begins working on WC, finds and registers the sinkhole domain, stopping spread
- Environments with good patching hygiene slept well!
- Automated patching allows rapid deployment when needed

May 2017



WannaCry

Trend Micro Deep Discovery detects bad rep repository



- Machines check repo for updates
- Trend alerts based on bad reputation
- Security reaches out to Systems
- Systems removes bad repo from approved list





2017-05-30

Export

Customize Columns

Mark Displayed as Resolved

Refresh

Status	Timestamp	Source Host	Destination Host	Interested Host	Threat Description	Detect...	Protocol	Detection Severity
	2017-05-30 15:47:25				Dangerous URL in Web Reputation Services database - HTTP (Request)		HTTP	 Medium
	2017-05-30 15:45:44				Dangerous URL in Web Reputation Services database - HTTP (Request)		HTTP	 Medium

Threat Description

Dangerous URL in Web Reputation Services database - HTTP (Request)

Detection Severity


Medium

Type

Malicious URLs

Export Connection Details

Connection Details



Host

IP Address:

Port:

55970

MAC Address:

Network Group:

Default

Network Zone:

Trusted

Destination

IP Address:

Port:

80

MAC Address:

Network Group:

No group

Network Zone:

No network zone

HTTP

User Agent:

Additional Details

Detected By:

Protocol:

URL:

Outbreak Containment Services:

URL Category:

Attack Phase:

Tarnished Attack Related:

URL filter engine

HTTP

http://micro-

Disease Vector

Point of Entry

No

Trend Micro TippingPoint constrains Sudoku



- TippingPoint 3/7/17 2:29:01 PM PST Low RepDV-Cleanup: (matched 69.172.201.217) Reputation Block
- ATT TMLA case, multiple machines with possible proxyback infection
- Investigation begins, nothing detectable on machines reaching out
- Additional machines reaching out
- Interview users of machines, they all play Sudoku at lunch
- www.uclick.com/client/sut/fcx/ contains malware loaded print button
- Block URL in web filtering, flatten machines for good measure

Closing Thoughts...



- Things you can apply when you get back to the office
 - ❑ No end user admin access on workstations – start the discussion
 - ❑ Security Awareness Training – raise awareness of both personal accounts and corporate accounts, multifactor auth, password hygiene, social eng
 - ❑ Web content filtering on and off premises
 - ❑ Mobile device management to protect data
 - ❑ Inventory assets, Develop good patching hygiene





QUESTIONS?

REFERENCE TO WANNACRY - [HTTPS://WWW.MALWARETECH.COM/2017/05/HOW-TO-ACCIDENTALLY-STOP-A-GLOBAL-CYBER-ATTACKS.HTML](https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html)

RSA®Conference2018

San Francisco | April 16 – 20 | Moscone Center

SESSION ID: SPO2-W12

A MULTILAYERED SECURITY APPROACH TO KEEPING HEALTHCARE DATA SECURE

Frank Bunton

VP, CISO
MedImpact Healthcare Systems, Security
@frankbunton

Larry Biggs

Security Engineer III - Threat Analytics
MedImpact Healthcare Systems, Security
@larrybiggs



#RSAC