The Evolution of Ransomware: A Discussion of Policy, Compliance and Future Landscape

Monday, October 26th, 3:45-5:00 pm ET

Join Health Sector Coordinating Council (HSCC) leadership and officials from the U.S. Department of Health & Human Services (HHS) for a virtual fireside discussion on the evolution of ransomware. We will dive into how the sophistication level has evolved, the role of the Office for Civil Rights' (OCR) ransomware guidance plays in this changing threat-scape, mitigating a maturing ransomware environment, and collaborative approaches for attacking these threats. We will leave ample time for audience Q&A.

Greg Garcia
Executive Director, Healthcare and Public Health Sector Coordinating Council (HSCC)

Theresa Meadows
CIO, Cook Children's Hospital and Vice Chair of HSCC

Greg Singleton
Director, HHS' Health Sector Cybersecurity Coordination Center (HC3)

Erik Decker
Chief Security and Privacy Officer, The University of Chicago Medicine and HSCC Executive Committee

Nick Haesters
Health Information Privacy Security Specialist, HHS Office for Civil Rights (OCR)

Marl Savickis
VP, Public Policy, CHIME

CHIME PUBLIC POLICY

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP
Ransomware milestones and trends: up to 2013

1989
• First attempt at ransomware attack – AIDS researcher distributes infected floppy disks
  • Intended to distribute 20,000 disks to people in over 90 countries using fake “PC Cyborg Corporation” as cover
  • Attempted to extort by demanding payment by check – easy to trace and prosecute
  • His lawyers argued he was going to donate the proceeds; Some news reports disputed this

2008
• Satoshi releases Bitcoin whitepaper; anonymous digital currency begins to slowly gain acceptance

2012
• FBI
  • Internet Crime Complaint Center (IC3) received 1,969 ransomware complaints that cost victims over $135K
  • First time ransomware is mentioned in IC3 annual report; Reveton is called out by name
• Statista
  • Estimated total ransomware attacks worldwide in 2015: 3.8M

2013
• Between September and December 2013, Cryptolocker infected over 250,000 systems
  • Earned more than $3M in ransoms for attackers
  • Gameover ZeuS botnet was forced offline, Cryptolocker operations ceased
• FBI
  • Internet Crime Complaint Center (IC3) received 991 ransomware complaints that cost victims over $539K
  • Cryptolocker and Reveton ransomware called out by name
Ransomware milestones and trends: 2014 and 2015

2014

- Gameover ZeuS botnet re-emerged, cryptolocker attacks begin again
  - Targeting banking, healthcare and government
- CryptoWall ransomware goes into use
- FBI
  - Internet Crime Complaint Center (IC3) received 1,402 ransomware complaints that cost victims over $490K
- Statista
  - Estimated total ransomware attacks worldwide in 2015: 3.2M

2015

- CryptoWall has extorted over $18 million from victims to date
- FBI
  - Internet Crime Complaint Center (IC3) received 2,453 ransomware complaints that cost victims over $1.6 million; Releases advisory on CryptoWall
- Statista
  - Estimated total ransomware attacks worldwide in 2015: 3.8M
Ransomware milestones and trends: 2016 and 2017

2016

- Ransomware attack – Hollywood Presbyterian Medical Center (February); Some patients re-routed; Paid $17K ransom,
- Ottawa Hospital ransomware attack (March) - 9800 systems taken offline, Systems, rebuilt with backed up data
- Anonymous security expert reported that ransomware overall brought in over $1B – huge jump!
- First offering of ransomware-as-a-service (RaaS) – by Petya and Cerber (Cerber offers 40% cut to partners)
- UK National Cyber Security Center (NCSC) mentions RaaS and mobile ransomware in recognition of the increasing threat
- FBI
  - Internet Crime Complaint Center (IC3) received 2,673 ransomware complaints that cost victims over $2.4 million
- Statista
  - Estimated total ransomware attacks worldwide in 2016: 638M

2017

- WannaCry ransomware attack (May); Attributed to North Korea (impacts 200K systems globally including 70K British NHS system
- FBI
  - Internet Crime Complaint Center (IC3) received 1,783 ransomware complaints that cost victims over $2.3 million
- Statista
  - Total ransomware attacks worldwide in 2017: 184M
Ransomware milestones and trends: 2018 – 2019

2018
- FBI
  - Internet Crime Complaint Center (IC3) received 1,493 ransomware complaints that cost victims over $3.6 million
- Statista
  - Total ransomware attacks worldwide in 2018: 204M

2019
- Brookside Hearing and ENT in Michigan (April) and Wood Ranch Medical in California (September) close permanently after suffering ransomware attacks
- Ryuk ransomware targets DCH Health Systems of Alabama; stop admitting new non-critical patients (Oct.)
- Maze ransomware operators begin double extortion – charge ransom fee and fee to not leak data
- Virtual Care (managed service provider) of Wisconsin attacked with Ryuk ransomware; 110 customer nursing homes temporarily lose access to health records, possibly affecting administration of medication
- Cancer Center of Hawaii suffers ransomware attack; temporary suspension of cancer services (December)
- Ransomware attack - Hackensack Meridian Health of New Jersey; some surgeries canceled (December)
- Managed Service Provider (MSP) compromise - Allows for potential compromise of many more targets
  - Significant uptick in MSP compromises in 2019 – October Armor report states at least 13 MSPs compromised to date in 2019
- FBI
  - Internet Crime Complaint Center (IC3) received 2,047 ransomware complaints that cost victims over $8.9 million
- Statista
  - Total ransomware attacks worldwide in 2019: 187M
Ransomware trends in 2020

• By early 2020
  • Several ransomware operators (Clop, DoppelPaymer, Sodinokibi/REvil) adopted Maze’s double extortion tactics
  • Several ransomware operators also promised to cease attacks against healthcare organizations during the pandemic
    • Clop, DoppelPaymer, Netfilim, Netwalker, Maze all stated that they did not or will not target healthcare organizations
    • Most of those promises were eventually broken

• Blackbaud MSP attacked with ransomware, data exfiltrated (between February and May)
  • At least 36 healthcare organizations affected, over 3 million records compromised, in addition to the ransomware attack

• In June Maze operators begin sharing data on their leak site stolen by other ransomware operators (likely for a fee)
  • Labeled a cartel, Maze began sharing their site with many operators

• Pandemic-themed attacks
  • Infection vectors for ransomware attacks adopted COVID-9 themes
    • Malspam
    • Bogus websites

• Dusseldorf University Clinic in Germany was attacked with Doppelpaymer ransomware (September)
  • Patients had to be re-routed as operations ceased
  • One patient died as a result of the rerouting delay; first time in history a life was lost due to a cyberattack

• Universal Health Services ransomware attack (September)
  • 250 US-based facilities affected
Frequent ransomware/malware combination attack

- Ryuk - Initial activity, very aggressive!
  - August 2018 to Jan 2019: $4.7M USD in BTC acquired
  - Used in cyberattacks targeting various newspapers in December (slight delays in delivery but no significant operational impact):
    - San Diego Union-Tribune
    - Los Angeles Times and Tribune Publishing
      - Includes Chicago Tribune, New York Daily News, Baltimore Sun and Orlando Sentinel
  - Used to attack cloud hosting provider Data Resolution, Onslow Water and Sewer Authority in North Carolina and an unnamed Canadian company that owns several restaurant chains
- Combining Ryuk with Emotet and TrickBot

“Along with Emotet, TrickBot has become one of the most versatile and dangerous pieces of modular malware hitting enterprise environments.” – HelpNet Security

“Interactive deployment of ransomware” to conduct reconnaissance and ultimately “maximize their disruption of business operations” - FireEye
Emotet ➔ TrickBot ➔ Ryuk Delivery

Source: Kryptoslogic.com
Another workflow example: Emotet, TrickBot and Ryuk

The Lockheed Martin Kill Chain model

Image source: Sophos
Image source: Lockheed Martin
Questions

**Product Evaluations**

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to [HC3@HHS.GOV](mailto:HC3@HHS.GOV).

**Requests for Information**

Need information on a specific cybersecurity topic? Send your request for information (RFI) to [HC3@HHS.GOV](mailto:HC3@HHS.GOV) or call us Monday-Friday between 9am-5pm (EST) at **202-691-2110**.
Health Sector Cybersecurity Coordination Center (HC3) Background

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications
Directs communications to victims or potential victims of compromises, vulnerable equipment, or PII/PHI theft, and general notifications to the HPH about currently impacting threats via the HHS OIG.

White Papers
Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar
Briefing document and presentation that provides actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic, or want to join our listserv? Send your request for information (RFI) to HC3@HHS.GOV, or call us Monday-Friday between 9am-5pm (EST) at 202-691-2110.
Moderated Panel Discussion
Resources


HC3: www.hhs.gov/HC3

HSCC: https://healthsectorcouncil.org/

CHIME policy Team: policy@chimecentral.org
Thank you For Joining!