Additional Ransomware Government Updates

May 15, 2017 –

From: OCR HIPAA Privacy Rule information distribution [mailto:OCR-PRIVACY-LIST@LIST.NIH.GOV] **On Behalf Of** OS OCR PrivacyList, OCR (HHS/OS)
Sent: Monday, May 15, 2017 8:49 AM
To: OCR-PRIVACY-LIST@LIST.NIH.GOV
Subject: HHS Update #2: International Cyber Threat to Healthcare Organizations --UPDATED LINKS

Please note that the links for "If you are the victim of ransomware or have cyber threat indicators to share" have been updated below.

HHS Update #2: International Cyber Threat to Healthcare Organizations

May 15, 2017

- Executive Summary from Sector call
- Where can I find the most up-to-date information from the U.S. government?
- Where can I find the latest Microsoft Security Information?
- ASPR TRACIE: Healthcare Cybersecurity Best Practices

- How to request an unauthenticated scan of your public IP addresses from DHS
- If you are the victim of ransomware or have cyber threat indicators to share

We would like to flag for the community that a partner noted an exploitative social engineering activity whereby an individual called a hospital claiming to be from Microsoft and offering support if given access to their servers. It is likely that malicious actors will try and take advantage of the current situation in similar ways.

Additionally, we received anecdotal notices of medical device ransomware infection. Please note the directions below for reporting ransomware attacks to FBI.

Where can I find the most up-to-date information from the U.S. government?

- For overall Cyber Situational Awareness visit the US-CERT National Cyber Awareness System webpage at: https://www.us-cert.gov/ncas
- NCCIC portal for those who have access: hsin.dhs.gov
- FBI FLASH: Indicators Associated With WannaCry Ransomware

Where can I find the latest Microsoft Security Information?

Visit the Microsoft Update Catalog for the latest security updates.

ASPR TRACIE: Healthcare Cybersecurity Best Practices

Our message from May 12, 2017 including information on how to protect from email-based and open RDP ransomware attacks can be found on the TRACIE portal here.

ASPR TRACIE also has the best and promising healthcare cybersecurity practices available in our Technical Resources domain. Issue 2 of The Exchange (released in 2016) highlights lessons learned from a recent attack on a U.S. healthcare system and features articles that demonstrate how collaboration at all levels is helping healthcare facilities implement practical, tangible steps to prevent, respond to, and recover from cyberattacks. The video Cybersecurity and Healthcare Facilities features subject matter experts describing last year's attack on MedStar, steps we can take to prevent and mitigate attacks, and what the federal government is doing to address cybersecurity. The Cybersecurity and Information Sharing Topic Collections include annotated resources reviewed

and approved by a variety of subject matter experts.

How to request an unauthenticated scan of your public IP addresses from DHS

The US-CERT's National Cybersecurity Assessment & Technical Services (NCATS) provides integrated threat intelligence and provides an objective third-party perspective on the current cybersecurity posture of the stakeholder's unclassified operational/business networks.

- NCATS focuses on increasing the general health and wellness of the cyber perimeter by broadly assessing for all known external vulnerabilities and configuration errors on a persistent basis, enabling proactive mitigation prior to exploitation by malicious third parties to reduce risk.
- Attributable data is not shared or disseminated outside of DHS or beyond the stakeholder; non-attributable data is used to enhance situational awareness.
- NCATS security services are available at no-cost to stakeholders. For more information please contact NCATS_INFO@hq.dhs.gov

If you are the victim of ransomware or have cyber threat indicators to share

If your organization is the victim of a ransomware attack, please contact law enforcement immediately.

1. Contact your FBI Field Office Cyber Task Force immediately to report a ransomware event and request assistance. These professionals work with state and local law enforcement and other federal and international partners to pursue cyber criminals globally and to assist victims of cyber-crime.
2. Report cyber incidents to the US-CERT and FBI's Internet Crime Complaint Center.
3. For further analysis and healthcare-specific indicator sharing, please also share these indicators with HHS' Healthcare Cybersecurity and Communications Integration Center (HCCIC) at HCCIC_RM@hhs.gov

---

From: OCR HIPAA Privacy Rule information distribution [mailto:OCR-PRIVACY-LIST@LIST.NIH.GOV] **On Behalf Of** OS OCR PrivacyList, OCR (HHS/OS)
Sent: Monday, May 15, 2017 7:49 AM
To: OCR-PRIVACY-LIST@LIST.NIH.GOV
Subject: HHS Update #2: International Cyber Threat to Healthcare Organizations

HHS Update #2: International Cyber Threat to Healthcare Organizations

May 13, 2017

We would like to flag for the community that a partner noted an exploitative social engineering activity whereby an individual called a hospital claiming to be from Microsoft and offering support if given access to their servers. It is likely that malicious actors will try and take advantage of the current situation in similar ways.

Additionally, we received anecdotal notices of medical device ransomware infection. Please note the directions below for reporting ransomware attacks to FBI.

Where can I find the most up-to-date information from

the U.S. government?

- For overall Cyber Situational Awareness visit the US-CERT National Cyber Awareness System webpage at: https://www.us-cert.gov/ncas
- NCCIC portal for those who have access: hsin.dhs.gov
- FBI FLASH: Indicators Associated With WannaCry Ransomware

Where can I find the latest Microsoft Security Information?

Visit the Microsoft Update Catalog for the latest security updates.

ASPR TRACIE: Healthcare Cybersecurity Best Practices

Our message from May 12, 2017 including information on how to protect from email-based and open RDP ransomware attacks can be found on the TRACIE portal here.

ASPR TRACIE also has the best and promising healthcare cybersecurity practices available in our Technical Resources domain. Issue 2 of The Exchange (released in 2016) highlights lessons learned from a recent attack on a U.S. healthcare system and features articles that demonstrate how collaboration at all levels is helping healthcare facilities implement practical, tangible steps to prevent, respond to, and recover from cyberattacks. The video Cybersecurity and Healthcare Facilities features subject matter experts describing last year's attack on MedStar, steps we can take to prevent and mitigate attacks, and what the federal government is doing to address cybersecurity. The Cybersecurity and Information Sharing Topic Collections include annotated resources reviewed and approved by a variety of subject matter experts.

How to request an unauthenticated scan of your public IP addresses from DHS

The US-CERT's National Cybersecurity Assessment & Technical Services (NCATS) provides integrated threat intelligence and provides an objective third-party perspective on the current cybersecurity posture of the stakeholder's unclassified operational/business networks.

- NCATS focuses on increasing the general health and wellness of the cyber perimeter by broadly assessing for all known external vulnerabilities and configuration errors on a persistent basis, enabling proactive mitigation prior to exploitation by malicious third parties

to reduce risk.

- Attributable data is not shared or disseminated outside of DHS or beyond the stakeholder; non-attributable data is used to enhance situational awareness.
- NCATS security services are available at no-cost to stakeholders. For more information please contact NCATS_INFO@hq.dhs.gov

If you are the victim of ransomware or have cyber threat indicators to share

If your organization is the victim of a ransomware attack, please contact law enforcement immediately.

1. Contact your FBI Field Office Cyber Task Force immediately to report a ransomware event and request assistance. These professionals work with state and local law enforcement and other federal and international partners to pursue cyber criminals globally and to assist victims of cyber-crime.
2. Report cyber incidents to the US-CERT and FBI's Internet Crime Complaint Center.
3. For further analysis and healthcare-specific indicator sharing, please also share these indicators with HHS' Healthcare Cybersecurity and Communications Integration Center (HCCIC) at HCCIC_RM@hhs.gov

OCR's web page on filing complaints at http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html. To subscribe to or unsubscribe from the list serv, go to https://list.nih.gov/cgi-bin/wa.exe?SUBED1=OCR-PRIVACY-LIST&A=1.

From: OCR HIPAA Privacy Rule information distribution [mailto:OCR-PRIVACY-LIST@LIST.NIH.GOV] **On Behalf Of** OS OCR PrivacyList, OCR (HHS/OS)
Sent: Tuesday, May 16, 2017 6:53 AM
To: OCR-PRIVACY-LIST@LIST.NIH.GOV
Subject: HHS Update #3: International Cyber Threat to Healthcare Organizations (Resend)

HHS Update #3: International Cyber Threat to Healthcare Organizations (Resend)

May 16, 2017

- NOTE: We are resending this notice as we have updated our distribution list.
- If you are the victim of ransomware or have cyber threat indicators to share
- HHS HCCIC Slack Channel
- Where can I find the most up-to-date information from the U.S. government?
- Receive Healthcare Intelligence through InfraGard participation
- DHS support for private sector cyber incident table top exercises
- How to request an unauthenticated scan of your public IP addresses from DHS
- EMS Partner activities

NOTE: We are resending this notice as we have updated our distribution list.

If you are the victim of ransomware or have cyber threat indicators to share

If your organization is the victim of a ransomware attack, HHS recommends the following steps:

1. Please contact your FBI Field Office Cyber Task Force immediately to report a ransomware event and request assistance. These professionals work with state and local law enforcement and other federal and international partners to pursue cyber criminals globally and to assist victims of cyber-crime.
2. Please report cyber incidents to the US-CERT and FBI's Internet Crime Complaint Center.
3. For further analysis and healthcare-specific indicator sharing, please also share these indicators with HHS' Healthcare Cybersecurity and Communications Integration Center (HCCIC) at HCCIC_RM@hhs.gov

HHS HCCIC Slack Channel

- HCCIC Slack Channel: Please provide the email addresses of personnel that would like to part of the HHS HCCIC Channel. Send the information to HHSHCCIC@hhs.gov

Where can I find the most up-to-date information from the U.S. government?

- For overall Cyber Situational Awareness visit the US-CERT National Cyber Awareness System webpage at: https://www.us-cert.gov/ncas
- NCCIC portal for those who have access: hsin.dhs.gov
- FBI FLASH: Indicators Associated With WannaCry Ransomware
- SMB Vulnerability: SMB version1 is affected as per US-CERT guidance:
- http://www.malwaretech.com
- https://www.endgame.com/blog/wcrywanacry-ransomware-technical-analysis
- http://www.ransomwarehotline.com
- Second Sink Hole Domain: ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com
- Open Source Links for Information and Indicators:
- https://www.us-cert.gov/ncas/current-activity/2017/03/16/Microsoft-SMBv1-Vulnerability
- https://www.us-cert.gov/security-publications/Ransomware

Healthcare and Public Health-directed Resources:

- ASPR TRACIE: Healthcare Cybersecurity Best Practices: https://asprtracie.hhs.gov/documents/newsfiles/NEWS_05_13_2017_08_17_11.pdf
- Fact Sheet on the FDA's Role in Medical Device Security: https://www.fda.gov/downloads/medicaldevices/digitalhealth/ucm544684.pdf

Receive Healthcare Intelligence through InfraGard participation

Cyber Health Working Group is a component of Healthcare Intelligence, a national special interest group of InfraGard, the only public-private, non-profit organization affiliated with the FBI. The CHWG is a force multiplier, leveraging its distinct model to connect and collaborate with other organizations and the USG. Partnerships with HITRUST, NHISAC, HHS, and others only make us stronger in the fight to protect the healthcare sector. The three benefits to the group are:

- Peer-To-Peer
- Trusted Forum
- Threat Exchange

The requirements to join:

- Current InfraGard membership or a pending application;
- IT position in a healthcare-related company or organization;
- Access, and ability to share, tactical cyber threat information.

For more information and to register, go to www.intelligence.healthcare.

DHS support for private sector cyber incident table top exercises

Contact the National Cyber Exercise and Planning Program for information about planning your own Cyber Table Top Exercise @ 703-235-5641 or email: cep@hq.dhs.gov.

How to request an unauthenticated scan of your public IP addresses from DHS

The US-CERT's National Cybersecurity Assessment & Technical Services (NCATS) provides integrated threat intelligence and provides an objective third-party perspective on the current cybersecurity

posture of the stakeholder's unclassified operational/business networks.

- NCATS focuses on increasing the general health and wellness of the cyber perimeter by broadly assessing for all known external vulnerabilities and configuration errors on a persistent basis, enabling proactive mitigation prior to exploitation by malicious third parties to reduce risk.
- Attributable data is not shared or disseminated outside of DHS or beyond the stakeholder; non-attributable data is used to enhance situational awareness.
- NCATS security services are available at no-cost to stakeholders. For more information please contact NCATS_INFO@hq.dhs.gov

EMS Partner activities

EMS partners reported that the NEMSIS TAC has taken precautions to protect against network and computer infection from the latest variants of ransomware. They also recommended their software partners take appropriate actions and report safeguards to clients.

http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html. To subscribe to or unsubscribe from the list serv, go to https://list.nih.gov/cgi-bin/wa.exe?SUBED1=OCR-PRIVACY-LIST&A=1.