# OFFICIAL GOVERNMENT ALERT EMAILS RECEIVED THE WEEKEND OF MAY 12 THROUGH 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:** Friday, May 12, 2017 1:38 PM
**To:** OCR-PRIVACY-LIST@LIST.NIH.GOV
**Subject:** HHS notification: international cyber threat to healthcare organizations


# HHS notification: international cyber threat to healthcare organizations

**May 12, 2017**

Dear HPH Sector Colleagues,

HHS is aware of a significant cyber security issue in the UK and other international locations affecting hospitals and healthcare information systems. We are also aware that there is evidence of this attack occurring inside the United States. We are working with our partners across government and in the private sector to develop a better understanding of the threat and to provide additional information on measures to protect your systems. We advise that you continue to exercise cyber security best practices – particularly with respect to email.

Laura Wolf,

Critical Infrastructure Protection Lead

HHS-ASPR-OEM

Additional information on ransomware provided by HHS Office for Civil Rights can be found at:

Cyber Newsletters:

https://www.hhs.gov/sites/default/files/hippa-cyber-awareness-monthly-issue1.pdf

https://www.hhs.gov/sites/default/files/hipaa-cyber-awareness-monthly-issue3.pdf
https://www.hhs.gov/sites/default/files/february-2017-ocr-cyber-awareness-newsletter.pdf

Ransomware Guidance:
https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

---

**From:** ONC Health IT [mailto:onchealthit@service.govdelivery.com]
**Sent:** Friday, May 12, 2017 9:00 PM
**To:** dmcociu@advancedbenefitconsulting.com
**Subject:** Multiple Ransomware Infections Reported


# Multiple Ransomware Infections Reported

United States Computer Emergency Readiness Team (US-CERT) has received multiple reports of WannaCry ransomware infections in several countries around the world. Ransomware is a type of malicious software that infects a computer and restricts users' access to it until a ransom is paid to unlock it. Individuals and organizations are discouraged from paying the ransom, as this does not guarantee access will be restored.

Ransomware spreads easily when it encounters unpatched or outdated software. The WannaCry ransomware may be exploiting a vulnerability in Server Message Block 1.0 (SMBv1). For information on how to mitigate this vulnerability, review the US-CERT article on Microsoft SMBv1 Vulnerability and the Microsoft Security Bulletin MS17-010. Users and administrators are encouraged to review the US-CERT Alert TA16-091A to learn how to best protect against ransomware. Please report any ransomware incidents to the Internet Crime Complaint Center (IC3).

Homeland Security

US-CERT United States Computer Emergency Readiness Team

Questions? Contact Us | Visit HealthIT.gov
Share Your Health IT Issues and Challenges

The Office of the National Coordinator for Health Information Technology

STAY CONNECTED:

SUBSCRIBER SERVICES:
Manage Preferences | Unsubscribe | Help

This service is provided to you by
The Office of the National Coordinator for Health Information Technology.

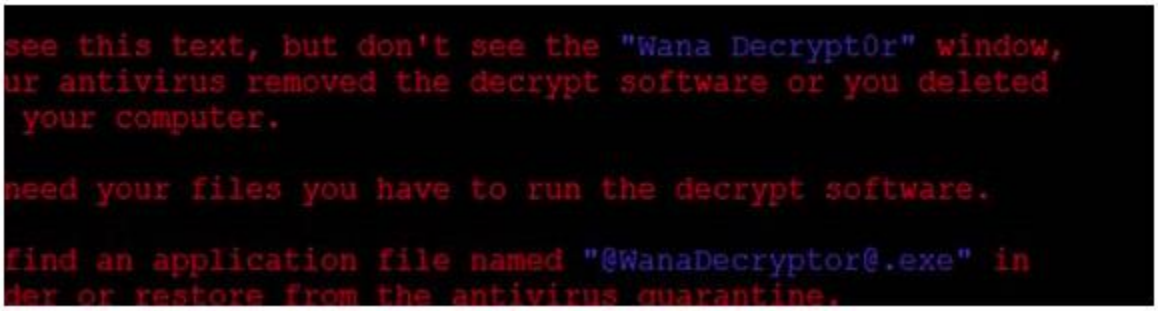
**From:** ONC Health IT [mailto:onchealthit@service.govdelivery.com]
**Sent:** Saturday, May 13, 2017 6:43 AM
**To:** dmcociu@advancedbenefitconsulting.com
**Subject:** HHS Update: International Cyber Threat to Healthcare Organizations


# HHS Update: International Cyber Threat to Healthcare Organizations

## Executive Summary

Ransomware can infect computers multiple ways and may or may not require user interaction. This message outlines several vectors of attack and what users can do to help protect themselves.

## Example of Ransomware




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

www.us-cert.gov/

hsin.dhs.gov (NCCIC portal for those who have access. We are not posting anything to the HPH portal at this time.)

## How can I help protect myself from email-based ransomware attacks?

Ransomware can be delivered via email by attachments or links within the email. Attachments in emails can include documents, zip files, and executable applications. Malicious links in emails can link directly to a malicious website the attacker uses to place malware on a system. To help protect yourself, be aware of the following:

- Only open up emails from people you know and that you are expecting. The attacker can impersonate the sender, or the computer belonging to someone you know may be infected without his or her knowledge.
- Don't click on links in emails if you weren't expecting them – the attacker could camouflage a malicious link to make it look like it is for your bank, for example.
- Keep your computer and antivirus up to date – this adds another layer of defense that could stop the malware.

## How can I help protect myself from open RDP ransomware attacks?

Recently, attackers have been scanning the Internet for Remote Desktop Protocol (RDP) servers open to the Internet. Once connected, an attacker can try to guess passwords for users on the system, or look for

backdoors giving them access. Once in, it is just like they are logged onto the system from a monitor and keyboard. To help protect yourself, be aware of the following:

- If you do not need RDP, disable the service on the computer. There are several ways of doing this based on which version of Microsoft Windows you are using.
- If RDP is needed, only allow network access where needed. Block other network connections using Access Control Lists or firewalls, and especially from any address on the Internet.
- To find which version of Microsoft you are using: https://support.microsoft.com/en-us/help/13443/windows-which-operating-system

## What is HHS doing to secure our systems?

- HHS Office of the Chief Information Officer implemented enterprise block across all OpDivs and StaffDivs and is ensuring all patching is up to date.
- HHS is working with Department of Homeland Security to scan HHS' CIDR IP addresses through the DHS NCATS program to identify RDP and SMB
- HHS notified VA and DHA and shared cyber threat information.
- HHS is coordinating with National Health Service (England) and UK-CERT.
- HHS through its law enforcement and intelligence resources with the Office of Inspector General and Office of Security and Strategic Information, have ongoing communications and are sharing and exchanging information with other key partners including the US Department of Homeland Security and the Federal Bureau of Investigation

## Requests for Information, impacts, and indicators

**Please notify us at cip@hhs.gov if:**

- you identify a new attack vector identified for this Ransomware other than Email, or the following Ports: SMB share and RDP; or
- if there are any impacts to patient care or supply chain distribution because of ransomware.

**Please share any indicators or cyber threat information with the HHS Healthcare Cybersecurity and Communications Integration Center at HCCIC-mgmt@hhs.gov.**

## If you are the victim of ransomware

If your organization is the victim of a ransomware attack, please contact law enforcement immediately. We recommend organizations contact their 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. Victims are also encouraged to report cyber incidents to the US-CERT and FBI's Internet Crime Complaint Center.

**From:** OCR HIPAA Privacy Rule information distribution [mailto:OCR-PRIVACY-LIST@LIST.NIH.GOV] **On Behalf Of** OS OCR PrivacyList, OCR (HHS/OS)
**Sent:** Saturday, May 13, 2017 8:47 AM
**To:** OCR-PRIVACY-LIST@LIST.NIH.GOV
**Subject:** Multiple Ransomware Infections Reported

Homeland Security

US-CERT United States Computer Emergency Readiness Team

National Cyber Awareness System:

## Multiple Ransomware Infections Reported

*05/12/2017 03:05 PM EDT*

Original release date: May 12, 2017

US-CERT has received multiple reports of WannaCry ransomware infections in several countries around the world. Ransomware is a type of malicious software that infects a computer and restricts users' access to it until a ransom is paid to unlock it. Individuals and organizations are discouraged from paying the ransom, as this does not guarantee access will be restored. Ransomware spreads easily when it encounters unpatched or outdated software. The WannaCry ransomware may be exploiting a vulnerability in Server Message Block 1.0 (SMBv1). For information on how to mitigate this vulnerability, review the US-CERT article on Microsoft SMBv1 Vulnerability and the Microsoft Security Bulletin MS17-010. Users and administrators are encouraged to review the US-CERT Alert TA16-091A to learn how to best protect against ransomware. Please report any ransomware incidents to the Internet Crime Complaint Center (IC3).

---



Additional information on ransomware provided by HHS Office for Civil Rights can be found at:

Cyber Newsletters:

https://www.hhs.gov/sites/default/files/hippa-cyber-awareness-monthly-issue1.pdf
https://www.hhs.gov/sites/default/files/hipaa-cyber-awareness-monthly-issue3.pdf
https://www.hhs.gov/sites/default/files/february-2017-ocr-cyber-awareness-newsletter.pdf

Ransomware Guidance:

https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

---



**From:** OCR HIPAA Privacy Rule information distribution [mailto:OCR-PRIVACY-LIST@LIST.NIH.GOV] **On Behalf Of** OS OCR PrivacyList, OCR (HHS/OS)
**Sent:** Saturday, May 13, 2017 9:02 AM
**To:** OCR-PRIVACY-LIST@LIST.NIH.GOV
**Subject:** Update: international cyber threat to healthcare organizations

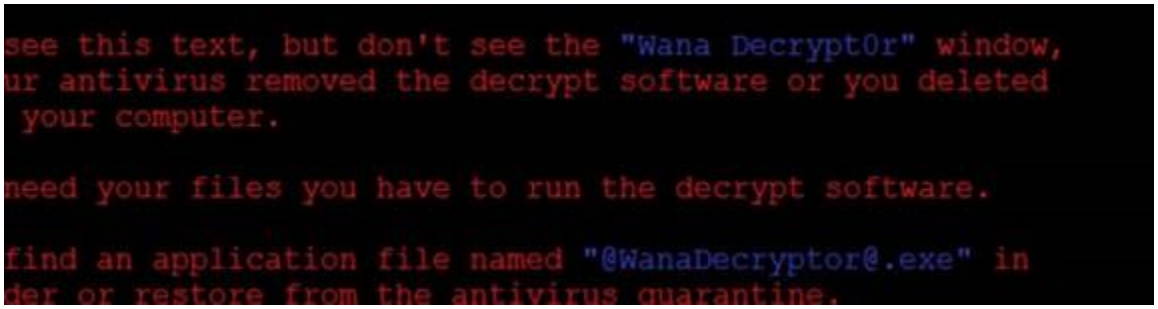

# HHS Update: international cyber threat to healthcare organizations

**May 13, 2017**

## Executive Summary

Ransomware can infect computers multiple ways and may or may not require user interaction. This message outlines several vectors of attack and what users can do to help protect themselves. Dial in information for a Sector-wide call for 1100 ET, May 13, 2017 is included.

## Example of Ransomware




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

www.us-cert.gov/

hsin.dhs.gov (NCCIC portal for those who have access. We are not posting anything to the HPH portal at this time.)

## How can I help protect myself from email-based ransomware attacks?

Ransomware can be delivered via email by attachments or links within the email. Attachments in emails can include documents, zip files, and executable applications. Malicious links in emails can link directly to a malicious website the attacker uses to place malware on a system. To help protect yourself, be aware of the following:

- Only open up emails from people you know and that you are expecting. The attacker can impersonate the sender, or the computer belonging to someone you know may be infected

without his or her knowledge.

- Don't click on links in emails if you weren't expecting them – the attacker could camouflage a malicious link to make it look like it is for your bank, for example.
- Keep your computer and antivirus up to date – this adds another layer of defense that could stop the malware.

## How can I help protect myself from open RDP ransomware attacks?

Recently, attackers have been scanning the Internet for Remote Desktop Protocol (RDP) servers open to the Internet. Once connected, an attacker can try to guess passwords for users on the system, or look for backdoors giving them access. Once in, it is just like they are logged onto the system from a monitor and keyboard. To help protect yourself, be aware of the following:

- If you do not need RDP, disable the service on the computer. There are several ways of doing this based on which version of Microsoft Windows you are using.
- If RDP is needed, only allow network access where needed. Block other network connections using Access Control Lists or firewalls, and especially from any address on the Internet.
- To find which version of Microsoft you are using: https://support.microsoft.com/en-us/help/13443/windows-which-operating-system

## What is HHS doing to secure our systems?

- HHS Office of the Chief Information Officer implemented enterprise block across all OpDivs and StaffDivs and is ensuring all patching is up to date.
- HHS is working with Department of Homeland Security to scan HHS' CIDR IP addresses through the DHS NCATS program to identify RDP and SMB
- HHS notified VA and DHA and shared cyber threat information.
- HHS is coordinating with National Health Service (England) and UK-CERT.
- HHS through its law enforcement and intelligence resources with the Office of Inspector General and Office of Security and Strategic Information, have ongoing communications and are sharing and exchanging information with other key partners including the US Department of Homeland Security and the Federal Bureau of Investigation

## Requests for Information, impacts, and indicators

**Please notify us at cip@hhs.gov if:**

- you identify a new attack vector identified for this Ransomware other than Email, or the following Ports: SMB share and RDP; or
- if there are any impacts to patient care or supply chain distribution because of ransomware.

**Please share any indicators or cyber threat information with the HHS Healthcare Cybersecurity and Communications Integration Center at HCCIC-mgmt@hhs.gov.**

## If you are the victim of ransomware

If your organization is the victim of a ransomware attack, please contact law enforcement immediately. We recommend organizations contact their 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. Victims are also encouraged to report cyber incidents to the US-CERT and FBI's Internet Crime Complaint Center.

**From:** ONC Health IT [mailto:onchealthit@service.govdelivery.com]
**Sent:** Monday, May 15, 2017 11:44 AM
**To:** dmcociu@advancedbenefitconsulting.com
**Subject:** HHS Update #2: International Cyber Threat to Healthcare Organizations


# HHS Update #2: International Cyber Threat to Healthcare Organizations

**IN THIS ISSUE**



## 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