

WannaCry Response: How Information Sharing and IOC Collection Made a Difference in Healthcare

HITRUST

Carl Anderson, Chief Legal Officer and
Senior VP of Government Affairs



Patient ID:
DOB:
Weight:

Procedure:

Accession:

Fluids:

Fluid A:

Fluid B:

Events:

Patient Worklist



Status



Oops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About Bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy Bitcoins>. And send the correct amount to the address specified in this window.



Send \$300 worth of bitcoin to this address:

13AS6VW2dHxYgXaQepoHkHSQuy8NgaE894

Copy

Check Payment

Decrypt

to the operations manual or the internet at:
<http://www.radiology.bayer.com>

Occurred

injection.

system to use.

and contact Services at

Contact Service

via VirtualCare, or refer

WannaCry Timeline



MS17-010

Microsoft Patch
March 14, 2017



Shadow Brokers
Leak Tools
April 14, 2017



WannaCry/WCRY 1.0
April 14, 2017



HITRUST CTX
Detects &
Automatically
shares IOC's
May 2, 2017

WannaCry/WCRY 2.0
May 12, 2017

March 14, 2017

 TechNet 

United States (English) [Sign in](#)

Security TechCenter

[Home](#) [Security Updates](#) [Tools](#) [Learn](#) [Library](#) [Support](#)

Security Advisories and Bulletins > Security Bulletins > 2017 *

...

MS17-013

MS17-012

MS17-011

MS17-010

MS17-009

MS17-008

MS17-007

MS17-006

MS17-005

MS17-004

Microsoft Security Bulletin MS17-010 – Critical

Security Update for Microsoft Windows SMB Server (4013389)

Published: March 14, 2017

Version: 1.0

Executive Summary

This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker sends specially crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server.

This security update is rated Critical for all supported releases of Microsoft Windows. For more information, see the **Affected Software and Vulnerability Severity Ratings** section.

The security update addresses the vulnerabilities by correcting how SMBv1 handles specially crafted requests.

For more information about the vulnerabilities, see the **Vulnerability Information** section.

For more information about this update, see [Microsoft Knowledge Base Article 4013389](#).

 Print

 Share

IN THIS ARTICLE

[Executive Summary](#)

[Affected Software and Vulnerability Severity Ratings](#)

[Vulnerability Information](#)

[Security Update Deployment](#)

[Acknowledgments](#)

[Disclaimer](#)

[Revisions](#)

On this page

[Executive Summary](#)

[Affected Software and Vulnerability Severity Ratings](#)

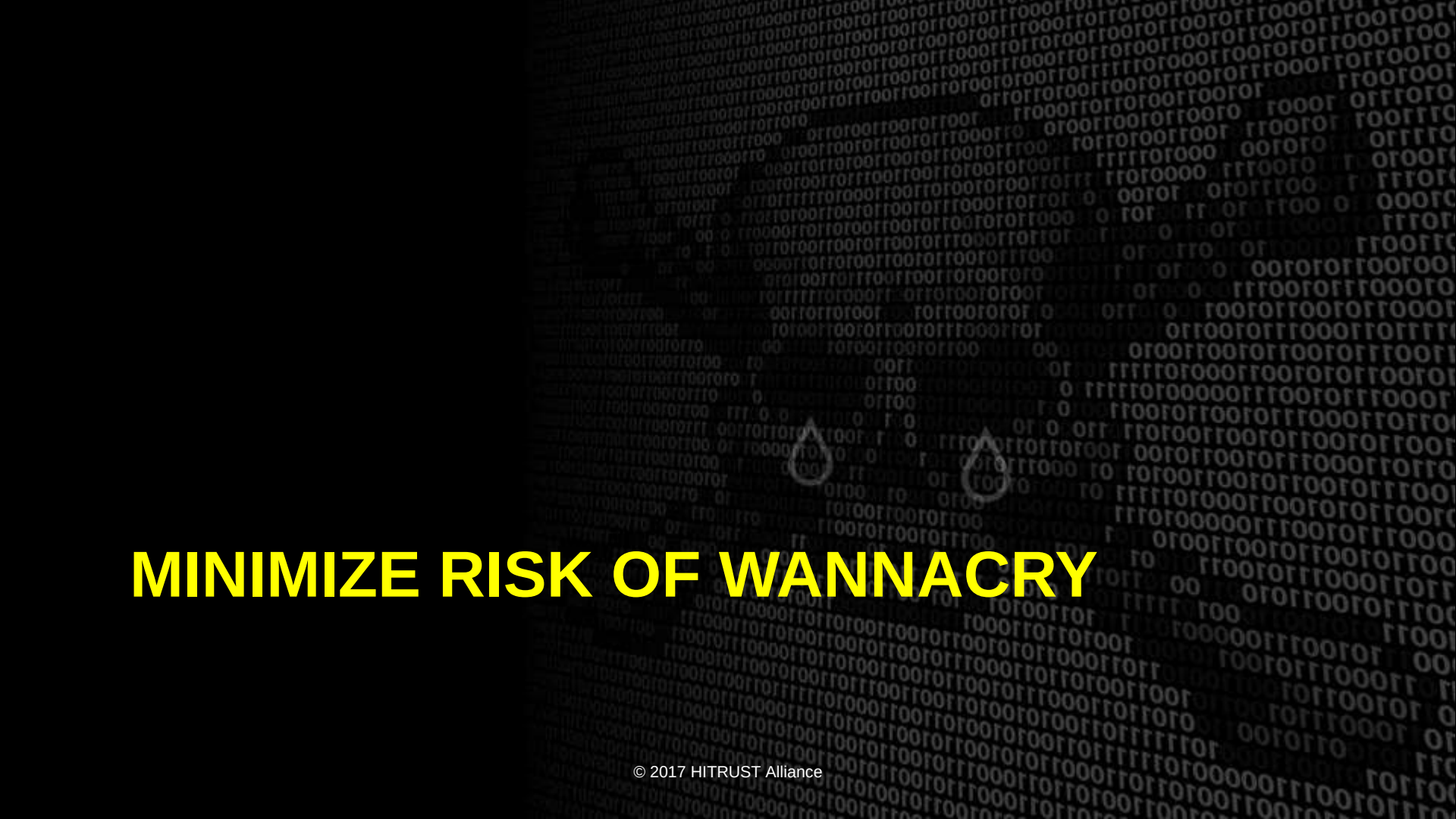
[Vulnerability Information](#)

[Security Update Deployment](#)

[Acknowledgments](#)

[Disclaimer](#)

[Revisions](#)

The background of the slide is a dark field filled with a dense, slightly blurred pattern of white binary code (0s and 1s). Two white water droplets are positioned above the main text, one to the left and one to the right of the center.

MINIMIZE RISK OF WANNACRY

HITRUST Cyber Threat XChange (CTX)

- **The HITRUST Cyber Threat XChange (CTX)** was created to significantly accelerate the detection and response to cyber threats targeted at the healthcare industry.
- WannaCry indicators were detected several weeks in advance of the outbreak.
- The CTX system detected indicators over SMB early in the attack lifecycle and automatically issued IOC's to all CTX participants for protection.
- Various indicators were collected and shared including WannaCry hashes, URL's and C&C IP's. CTX distributed actionable indicators automatically and seamlessly to the CTX organizations to protect their environments from attack.
- CTX greatly reduces the risk of cyber attack or breach of both known and unknown threats including ransomware by detecting threats across all stages of the attack lifecycle including lateral movement and sharing those threat indicators in near real-time.

HITRUST™

Visit www.HITRUSTAlliance.net for more information.

To view our latest documents, visit the [Content Spotlight](#).