Cyber Incident Response Exercise for Leadership

Moderated by John Riggi, Senior Advisor, Cybersecurity and Risk

2/28/2020

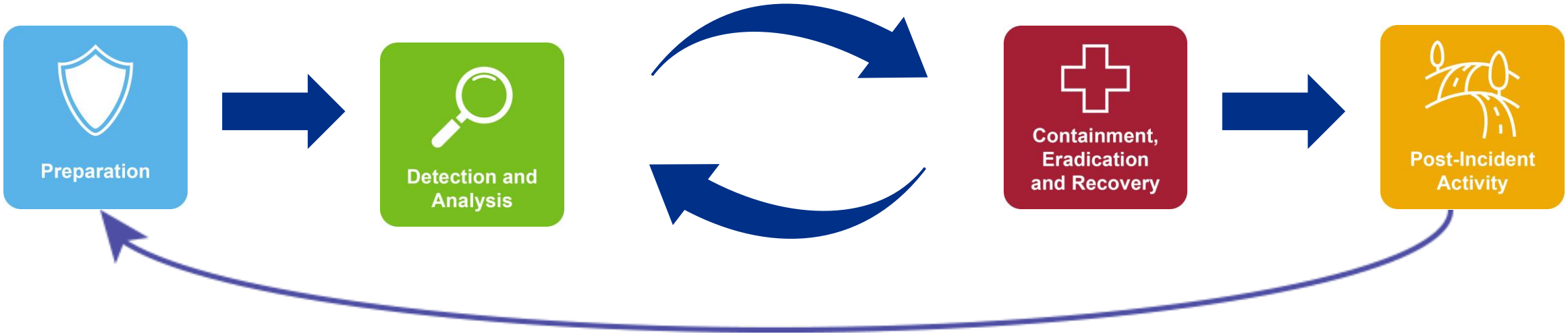
American Hospital Association™
Advancing Health in America

AHA CENTER FOR HEALTH INNOVATION

Cyber Exercise

Overviews and Objectives

- The goal of the tabletop exercise is to employ knowledge provided in the previous sessions and to increase situational awareness for hospital leadership in dealing with a major cyber incident. The target time range for the exercise is 90 minutes followed by discussion.
- *The exercise has multiple, complex elements, based upon real world events which will be covered in a compressed timeline.* There are **no absolute correct or incorrect responses**, we hope to learn as a group based upon our collective knowledge and experience. The intent is to test incident response plans, provoke discussion and thought on how the multiple facets of incident response are employed in combination with clinical and non-technical priority issues which arise as a result of the incident.



Exercise Scenario: Day 1 - Saturday

You hear unconfirmed reports that a sophisticated malware which **has both ransomware and destructive capability** has been found on certain hospital networks in Europe.

6:00 PM

Further news reports indicate no destruction or encryption of data has occurred. The malware my be exploiting the **DEJABLUE** family of vulnerabilities, **similarities to the WannaCry ransomware outbreak**.

6:30 PM

Reports from national media AHA, H-ISAC and HITRUST indicate the appearances of the **same malware** found in Europe, in a rural hospital in the Northwest US.

8:00 PM

The FBI and DHS release an urgent **TLP AMBER FLASH bulletin** confirming that a sophisticated malware, with destructive and ransomware properties, originating from a foreign based criminal organization with possible ties to a state sponsor of terrorism is **targeting the healthcare, financial services and energy sectors.**

11:00 PM

Included in the FBI/DHS FLASH bulletin is a lengthy list of **technical indicators of compromise** (IOCs) which may be exploiting a zero day in addition to the **DEJABLUE** vulnerability – analysis is ongoing. **NO patch is available yet for the zero-day.**

Exercise Scenario: Day 2 - Sunday

The information security team has found certain FBI-DHS published IOCs related to both the ransomware and destructive variant of the malware **have been found on parts of the administrative network and the backups of two servers.**

Logs indicate unusual activity and access to the backups by a vendor contracted to maintain them.

2:00 AM

Although no damage or encryption of data has occurred, as a precaution, the team is beginning to shut down and isolate the affected parts of the network and the affected servers, **causing operational and administrative disruptions. The incident response plan is not accessible.**

7:00 AM

FBI-DHS reports that the vulnerability being exploited allows the malware to **replicate and spread laterally very quickly**. The malware appears to successfully execute only **50% of the time** for unknown technical reasons. However, when it does execute, it has caused **massive disruptions to networks, successfully encrypting data and potentially poised to destroy data**.

11:30 AM

The security team reports that IOCs related to both the destructive variant and the ransomware variant have been found on **several drug infusion pumps and ventilators**.

Employees are beginning to notice **network and operational disruptions** related to the ongoing isolation efforts. However the malware has not executed.

Exercise Scenario: Day 2 - Sunday

1:00 PM

A screen appears on certain computers bearing the logo of a named foreign based militant/criminal organization indicating that your hospital has been **intentionally infected** by the organization and they are demanding:

$1 million in bitcoin be paid to a provided bitcoin wallet. You have **24 hours** to pay or the ransom will double. If **$2 million** not paid within **48 hours** your **data and networks will be destroyed.** In exchange, they promise not to detonate the destructive malware and provide a decryption key for the ransomware variant.

2:30 PM

The FBI recommends **not paying** the ransom, if at all possible. The FBI advises **several hospitals in the area may be impacted as well.**

IT team advises that if entire network is encrypted, It will take five days to restore critical systems and ten days to complete full system restore. Uncertain if medical devices can be restored from backup.

4:00 PM

Employees and patients are asking questions about the network and operational disruptions. But no media inquiries or press coverage of your organization.

Patients and staff are on social media **discussing disruption and speculating** they have impacted by the malware.

American Hospital Association™
Advancing Health in America

Exercise Scenario: Day 3 - Monday

6:30 AM

Media inquiries being received as they are hearing **on social media from patients and staff** that your hospital has been infected with malware and are requesting a statement.

11:30 AM

The Audit Department informs you that a vendor has complained that an expected **$1 million** payment was never received. After research from Audit, it appears that the hospital **misdirected payment** to an unknown account based on internal email from the hospital CFO **yesterday**. **The CFO is also part of the incident command team.**

1:00 PM

The Facilities Department reports there is an **unscheduled elevator and HVAC outage** on parts of the hospital.

Information security reports these systems, the **infant protection system and other physical security systems** are running a susceptible operating system and have previously unmapped network connections.

4:00 PM

HHS-OCR and State regulators are making inquiries and would like to come on site.

Your Board is demanding a briefing.

American Hospital Association™

Advancing Health in America

DISCUSSION

General Thoughts?

What functions were required in this scenario?

What functions were missing?

Best Practices?

Challenges?

Lessons Learned?

Documentation?

What changes will you make if any?

TLP: GREEN

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

17 October 2017

PIN Number

171017-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:
www.fbi.gov/contact-us/field

E-mail:
cywatch@ic.fbi.gov

Phone:
1-855-292-3937

The following guarantees o recipients in provided to h administrator criminals.

This PIN has b product is use within their s publicly acces

Medical D US Health

Summary

This year's W marked the fi device operat especially vul outdated, uns remain vulne

Threat

The increased networks inva vectors. Cybe widespread disruptions to US healthcare operations, especially because of the interconnectivity of devices throughout healthcare

TLP: GREEN

WANTED BY THE FBI

PARK JIN HYOK

Conspiracy to Commit Wire Fraud; Conspiracy to Commit Computer-Related Fraud (Computer Intrusion)

DESCRIPTION

Aliases: Pak Jin Hek, Jin Hyok Park	
Place of Birth: Democratic People's Republic of Korea (North Korea)	**Hair:** Black
Eyes: Brown	**Sex:** Male
Race: Asian	**Languages:** English, Korean

REMARKS

Park attended the Kim Chaek University of Technology in Pyongyang, North Korea. He is a North Korean citizen last known to be in North Korea. Park has traveled to China in the past and conducted legitimate IT work under the front company "Chosun Expo" or the Korean Expo Joint Venture in addition to activities conducted on behalf of North Korea's Reconnaissance General Bureau.

CAUTION

Park Jin Hyok is allegedly a North Korean computer programmer who is part of a state-sponsored hacking organization responsible for some of the costliest computer intrusions in history, including the cyber attack on Sony Pictures Entertainment, a series of attacks targeting banks across the world that collectively attempted to steal more than one billion dollars, and the WannaCry ransomware attack that affected tens of thousands of computer systems across the globe

TLP: GREEN

Notification

U OF INVESTIGATION, CYBER DIVISION

ation is provided by the FBI, with no ities, for potential use at the sole discretion ct against cyber threats. This data is er security professionals and system against the persistent malicious actions of

LP: GREEN: The information in this product eness of all participating organizations community, but should not be shared via annels.

Cry Attribution to North Korea Persistent Cyber Targeting of

JS Government publicly attributed the 2017 tbreak to North Korea cyber actors. The scores the continued intent and increasing g to conduct cyber attacks against US and The North Korean government has devoted developing its cyber operations, which have histicated. The FBI encourages the US private t, evaluate network security, and report suspicious network activities to their local FBI offices or FBI CyWatch.

URGENT/11 Cybersecurity Vulnerabilities in a Widely-Used Third-Party Software Component May Introduce Risks During Use of Certain Medical Devices: FDA Safety Communication

Date Issued: October 1, 2019

The U.S. Food and Drug Administration (FDA) is informing patients, health care providers and facility staff, and manufacturers about cybersecurity vulnerabilities that may introduce risks for certain medical devices and hospital networks. The FDA is not aware of any confirmed adverse events related to these vulnerabilities. However, software to exploit these vulnerabilities is already publicly available.

A security firm has identified 11 vulnerabilities, named "URGENT/11." These vulnerabilities may allow anyone to remotely take control of the medical device and change its function, cause denial of service, or cause information leaks or logical flaws, which may prevent device function.

These vulnerabilities exist in IPnet, a third-party software component that supports network communications between computers. Though the IPnet software may no longer be supported by the original software vendor, some manufacturers have a license that allows them to continue to use it without support. Therefore, the software may be incorporated into other software applications, equipment, and systems which may be used in a variety of medical and industrial devices that are still in use today.

Windows 7 – Out of Support 1/14/2020

Support for Windows 7 is ending

After January 14, 2020, Microsoft will no longer provide security updates or support for PCs running Windows 7. Now is the time to upgrade to Windows 10.

Get Windows 10 >

Why Windows 10? | Upgrade Options | Deployment Resources | Frequently asked questions

What does end of support mean?

If you continue to use Windows 7 after support has ended, your PC will still work, but it may become more vulnerable to security risks and viruses. Your PC will continue to start and run, but Microsoft will no longer provide the following support for your business.

No technical support | No software updates | No security updates

FierceHealthcare

HOSPITALS & HEALTH SYSTEMS | TECH | PAYER | FINANCE | PRACTICES | REGULATORY | SPECIAL

Tech

70% of medical devices will be running unsupported Windows operating systems by January: report

by Heather Landi | May 15, 2019 1:55pm

The number of connected medical devices being used in hospitals and healthcare organizations continues to grow at a rapid pace, representing a vulnerable attack surface for cyberattacks. (Gettyicfotart)

The number of connected medical devices being used in hospitals and healthcare organizations continues to grow at a rapid pace, representing a vulnerable surface for cyberattacks.

Raising the cyberrisks even further, 70% of devices in healthcare organizations will be running unsupported Windows operating systems by January 2020, according to a new cybersecurity report

Windows 10 Has a Security Flaw So Severe the NSA Disclosed It

n a shift toward transparency, the National Security Agency announced a bug that could have left over 900 million PCs vulnerable to attack.

SA Cybersecurity Directorate head Anne Neuberger briefed reporters Tuesday about a critical Windows 10 bug that the agency chose to disclose rath
HOTOGRAPH: PHILLIP FARAONE/GETTY IMAGES

Microsoft released a patch for Windows 10 and Server 2016 today after the National Se Agency found and disclosed a serious vulnerability. It's a rare but not unprecedented ti one that underscores the flaw's severity—and maybe hints at new priorities for the NS/

The bug is in Windows' mechanism for confirming the legitimacy of software or establ secure web connections. If the verification check itself isn't trustworthy, attackers can exploit that fact to remotely distribute malware or intercept sensitive data.

"[We are] recommending that network owners expedite implementation of the patch immediately as we will also be doing," Anne Neuberger, head of the NSA's Cybersecurity Directorate, said on a call with reporters on Tuesday. "When we identified a broad cryptographic vulnerability like this we quickly turned to work with the company to ensure that they could mitigate it."

CISA
CYBER+INFRASTRUCTURE

Search

About Us | Alerts and Tips | Resources | Industrial Control Systems

National Cyber Awareness System > Alerts > Critical Vulnerabilities in Microsoft Windows Operating Systems

Alert (AA20-014A)

More Alert

Critical Vulnerabilities in Microsoft Windows Operating Systems

Original release date: January 14, 2020

Print | Tweet | Send | Share

Summary

On January 14, 2020, Microsoft released software fixes to address 49 vulnerabilities as part of their monthly Patch Tuesday announcement. Among the vulnerabilities patched were critical weaknesses in Windows CryptoAPI, Windows Remote Desktop

- Crypt
  10 op
  Crypt
  masq
  malw
  hostn
  an att
- Windo
  Serve
  —allo
  explo

The Cybe
released.

2. HHS urges health care entities to patch new Windows vulnerabilities

The Department of Health and Human Services' Office of the Assistant Secretary for Preparedness and Response strongly recommends that all health care and public health entities consider patching as soon as possible several new critical vulnerabilities affecting Microsoft Windows operating systems. "This recommendation is based on the likelihood of the vulnerabilities being weaponized, combined with the widespread use of the affected software across the sector and high potential for a compromise of integrity and confidentiality of information," ASPR's Division of Critical Infrastructure Protection said yesterday in a bulletin to the sector. For more on the vulnerabilities and recommended actions, see the alert from the Cybersecurity and Infrastructure Security Agency. For more information on this or other cybersecurity issues, contact John Riggi, AHA senior advisor for cybersecurity and risk, at jriggi@aha.org.

Cybersecurity Vulnerabilities in Certain GE Healthcare Clinical Information Central Stations and Telemetry Servers: Safety Communication

Share | Tweet | Linkedin | Email | Print

Date Issued: January 23, 2020

The U.S. Food and Drug Administration (FDA) is raising awareness among health care providers and facility staff that cybersecurity vulnerabilities in certain GE Healthcare Clinical Information Central Stations and Telemetry Servers may introduce risks to patients while being monitored.

These devices are used mostly in health care facilities for displaying information, such as the physiologic parameters of a patient (such as temperature, heartbeat, blood pressure), and monitoring patient status from a central location in a facility, such as a nurse's workstation. To date, the FDA is not aware of any adverse events related to these vulnerabilities. Learn more about these vulnerabilities

On November 12, 2019, GE Healthcare issued an "Urgent Medical Device Correction" letter informing consumers of security vulnerabilities for certain GE Healthcare Clinical Information Central Stations and Telemetry Servers, instructions for risk mitigation, and where to find the software updates or patches when they become available. The following table provides information on the specific versions of the devices that have these security vulnerabilities.

2. FDA alerts providers to cyber vulnerabilities in certain GE medical devices

The Food and Drug Administration today alerted health care providers to cybersecurity vulnerabilities in certain GE Healthcare clinical information central stations and telemetry servers that may allow an attacker to remotely take control of these medical devices and silence, generate and interfere with alarms for connected patient monitors. The devices are used mostly in health care facilities to display a patient's physiologic information (such as temperature, heartbeat and blood pressure) and monitor patient status from a central location, such as a nurse's workstation. FDA currently is not aware of any related adverse events. GE Healthcare plans to issue a software patch to address the vulnerabilities and notify affected customers when the patches are ready. For more information, see the FDA notice. For more on this or other cybersecurity issues, contact John Riggi, AHA senior advisor for cybersecurity and risk, at jriggi@aha.org.

Zeppelin Overview

TLP:WHITE

- **Zeppelin** – new ransomware observed targeting U.S and European Healthcare and IT companies
  - Derived from the VegaLocker Ransomware family
  - Distributed through remote desktop servers publicly exposed to the internet
  - Many elements of Zeppelin are similar to ransomware campaigns like sodinokibi
    - Known to steal victim data before the encryption process
    - Targeted Managed Service Providers (MSP) in order to further infect customers via management software
  - Considered a Ransomware-as-a-Service or Attack-as-a-Service package.
    - Allows users to selectively craft ransomware payloads for customized campaigns.
    - Offers high degree of evasion against anti-malware tools and services.
  - Checks to see if the user is in a Commonwealth of Independent States (CIS) country, namely (specifically Russia, Ukraine, Belorussia, and Kazakhstan).
    - Will stop processes if the user is found to be in a CIS country.

Source: Zdnet, Beckers Hospital Review

John Riggi, Strategic Advisor for Cybersecurity and Risk

Advisory services uniquely informed by:

- Extensive and varied FBI and CIA experience
- Trusted and confidential access to the nation's hospital leaders
- Ongoing exchange with federal law enforcement, intelligence and regulatory agencies

jriggi@aha.org (O) 202-626-2272; (M) 24/7 202-640-9159

John Riggi, having spent nearly 30 years as a highly decorated veteran of the FBI, serves as the first Senior Advisor for Cybersecurity and Risk for the American Hospital Association (AHA) and their 5000+ member hospitals. In this role, John serves as a national resource to assist members defend against cyber attacks and other threats to their organizations. While at the FBI, John served as a representative to the White House Cyber Response Group. He also led the FBI Cyber national outreach program to develop mission critical, investigative and information sharing partnerships with the healthcare and other critical infrastructure sectors. John held a national strategic role in the FBI investigation of the largest cyber-attacks targeting healthcare and other critical infrastructure.

In coordination with the FBI and other government agencies, John is currently leading an AHA national campaign to advise members on threats to intellectual property, including nation state sponsored theft of medical research and innovation. He currently co-leads a national HHS/healthcare sector task group to develop resources to assist the field in translating cyber risk into enterprise risk. John serves as an official private sector validator for the White House's Presidential Policy Directive (PPD)-41 on U.S. Cyber Incident Coordination, to improve coordination among government agencies and cooperation with the private sector.

Previously in his career, John served in leadership positions in the FBI's Washington Office Intelligence Division, New York Office Joint Terrorist Task Force, and High Intensity Financial Crimes Area Task Force. He also served as the National Operations Manager for the FBI's Terrorist Financing Operations Section, a senior FBI representative to the CIA's Counterterrorism Center and served on the New York FBI SWAT Team for eight years. John is the recipient of the FBI Director's Award for Special Achievement in Counterterrorism and the recipient of the CIA George H.W. Bush Award for Excellence in Counterterrorism, the CIA's highest counterterrorism award. John presents extensively on cybersecurity and risk topics and is frequently interviewed by the media on cybersecurity issues.

AHA Membership Includes: