CALIFORNIA HOSPITAL ASSOCIATION
Leadership in Health Policy and Advocacy

From Digital to Physical Disaster: The Impact of Ransomware Attacks on Hospitals and Health Systems

John Riggi AHA Senior Advisor
Cybersecurity and Risk
09/14/2021

American Hospital Association™ Advancing Health in America | AHA CENTER FOR HEALTH INNOVATION

1

Hacking Incidents Reported to OCR

2020 Total:
425 Breaches Impacting 26.7 Million Individuals

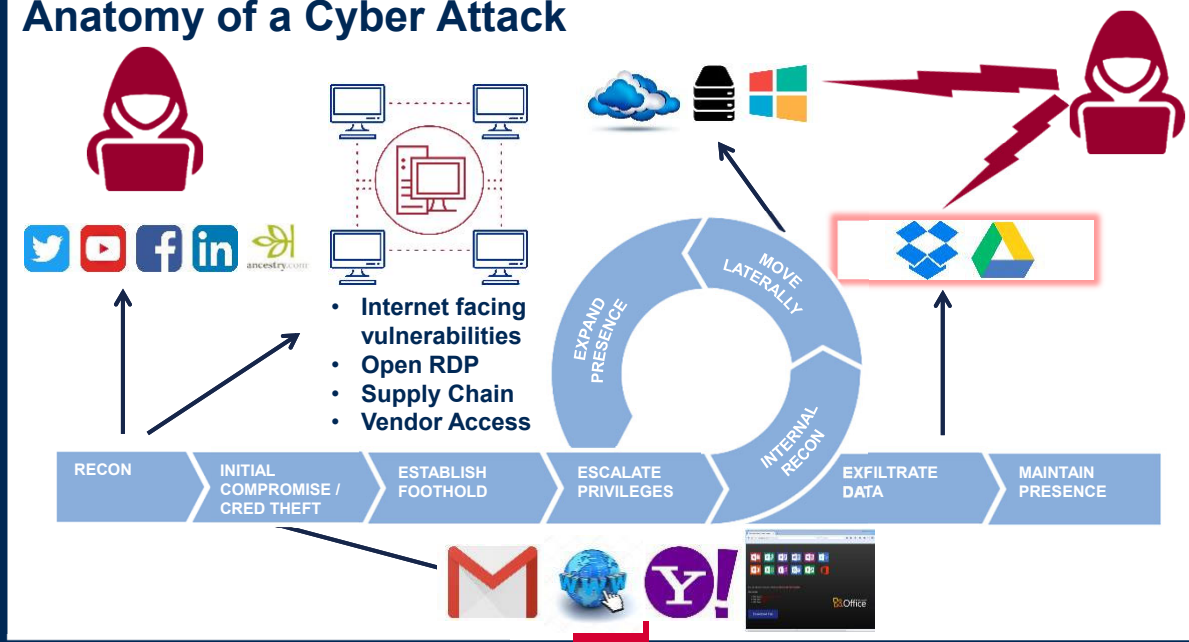
1/1/2021 - 8/30/2021
331 Breaches Impacting 32.4 Million Individuals

California: 31 Breaches Impacting 2.4 Million Individuals

Source: HHS, OCR website data accessed 01/11/2021 and 09/09/2021 https://ocrportal.hhs.gov

2

Anatomy of a Cyber Attack



3

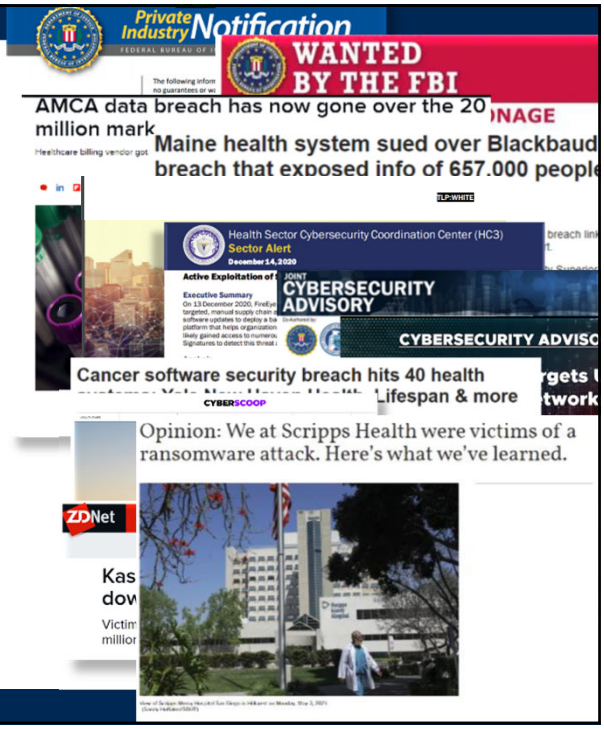
Attack Patterns – Priority Risks

#1 Priority - High impact ransomware attacks especially those that result in a regional or statewide disruption of care delivery

2) Cyber risk exposure and impact through business associates:

- **Theft of large quantities of covered entity data in possession of business associates**
- **Business associate as digital pathway into covered entity**
- **Mission critical business associate becomes victim of ransomware attack**

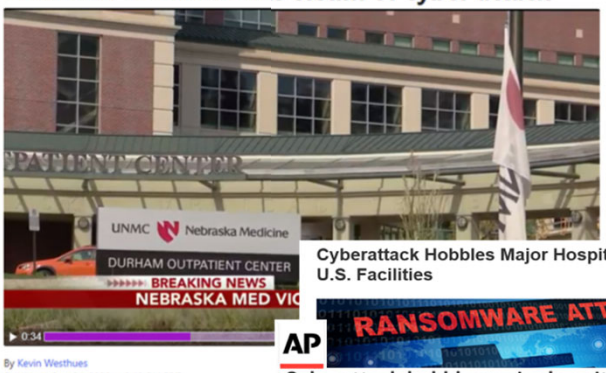
3) Theft of PHI and medical research related to COVID-19 treatment protocols and COVID-19 vaccine development from hospitals/health systems directly.



4

4

Nebraska Medicine was victim of cyber attack



By Kevin Westhues
Published: Sep. 24, 2020 at 9:19 PM EDT

UHS says all U.S. facilities affected by apparent ransomware attack

Computer systems at Pennsylvania-based Universal Health Services began to fail over the weekend, leading to a network shutdown at hospitals around the country.

By Kat Jercich | October 02, 2020 | 11:53 AM

Cyberattack Hobbles Major Hospital Chain's U.S. Facilities

AP

Cyberattack hobbles major hospital chain's

"We are most concerned with ransomware attacks which have disrupt patient care operations and risk patient safety," said Ri cybersecurity adviser to hospitals. "We believe any cyberattack hospital or health system is a threat-to-life crime and should b and pursued as such by the government."

Frank Bajak | Sep 30

Claims Journal - John Riggi, senior cybersecurity adviser to the American Hospital Association, called it a "suspected ransomware attack," affirming reporting on the social media site Reddit by people

5

5

NEWS

'We got taken down': UVM Medical Center says cyberattackers were likely after money

Dan D'Ambrosio Burlington Free Press
Published 3:53 p.m. ET Dec. 22, 2020 | **Updated 4:34 p.m. ET Dec. 22, 2020**

View Comments

IT staff at the University of Vermont Medical Center in Burlington continue work to scan thousands of the hospital's computer systems for malware on Friday, Nov. 20, 2020, after a cyberattack forced a shutdown of the hospital's electronic medical records system and other key systems. *COURTESY RYAN MERCER/UNIVERSITY OF VERMONT HEALTH NETWORK*

Cyberattack on UVM Health Network Impedes Chemotherapy Appointments

The cyberattack has halted chemotherapy, mammogram and screening appointments, and led to 300 staff being furloughed or reassigned.

6

6

Irish Hospitals Are Latest to Be Hit by Ransomware Attacks

Hospitals in Ireland, New Zealand and Scripps Health in San Diego are reeling from digital extortion attacks.

Naas General Hospital in County Kildare, Ireland. The country's health system has been hobbled for a week by a ransomware attack. Niall Carson/Press Association, via Associated Press

National Disruption of Healthcare

The Irish Government Refuses to Pay the Ransom

7

7

American Hospital Association™
Advancing Health in America

AHA TODAY
Your source of news and insight.

December 2, 2020

Coronavirus News: Bipartisan Bill Seeks to End Medicare Sequester; CDC Adjusts Quarantine Options

AHA testifies at Senate hearing on cyber threats amid pandemic. The Senate Homeland Security and Governmental Affairs Committee today held a hearing on defending communities from cyber threats during the COVID-19 pandemic.

Testifying at the hearing, John Riggi, AHA senior advisor for cybersecurity and risk, said the pandemic has led to a cyber "triple threat" for hospitals and health systems: an expanded attack surface due to rapidly expanded network- and internet-connected technologies and services; increased cyberattacks of all types; and fewer available resources to bolster cybersecurity defenses.

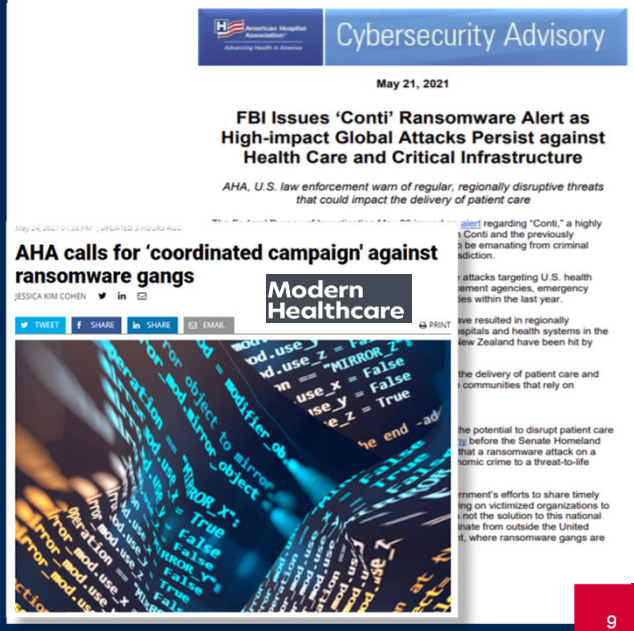
"A ransomware attack on a hospital crosses the line from an economic crime to a threat-to-life crime; such attacks should therefore be aggressively pursued and prosecuted as such by the federal government," Riggi said. "…We recommend that, given the increased cyber threat environment and attacks specifically targeting hospitals and health systems, along with resource constraints imposed upon hospitals and health systems in response to COVID-19, additional safe harbor protections from civil and regulatory liability be provided to hospital and health system victims of cyberattacks."

"A ransomware attack on a hospital crosses the line from an economic crime to a **threat-to-life crime;** these attacks should therefore be aggressively pursued and prosecuted as such"

"…***additional safe harbor protections from civil and regulatory liability be provided to hospital and health system victims of cyberattacks."***

8

8


Cybersecurity Advisory

May 21, 2021

FBI Issues 'Conti' Ransomware Alert as High-impact Global Attacks Persist against Health Care and Critical Infrastructure

AHA, U.S. law enforcement warn of regular, regionally disruptive threats that could impact the delivery of patient care

AHA calls for 'coordinated campaign' against ransomware gangs

JESSICA KIM COHEN

Modern Healthcare

- *A ransomware attack on a hospital or health system crosses the line from an economic crime to a threat-to-life crime.*
- *This is a national security threat.*
- *The vast majority of these attacks originate from outside the United States.*
- *The AHA has urged the government to embark upon a coordinated whole of government and a whole of nation campaign.*

9

9


THE UNITED STATES DEPARTMENT of JUSTICE

ABOUT OUR AGENCY TOPICS NEWS RESOURCES CAREERS

Home » Office of Public Affairs » News

JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE Monday, June 7, 2021

Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside

WASHINGTON – The Department of Justice today announced that it has seized 63.7 bitcoins currently valued at approximately $2.3 million. These funds allegedly represent the proceeds of a May 8, ransom payment to individuals in a group known as DarkSide, which had targeted Colonial Pipeline, resulting in critical infrastructure being taken out of operation. The seizure warrant was authorized earlier today by the Honorable Laurel Beeler, U.S. Magistrate Judge for the Northern District of California.

"Following the money remains one of the most basic, yet powerful tools we have," said Deputy Attorney General Lisa O. Monaco for the U.S. Department of Justice. "Ransom payments are the fuel that propels the digital extortion engine, and today's announcement demonstrates that the United States will use all available tools to make these attacks more costly and less profitable for criminal enterprises. We will continue to target the entire ransomware ecosystem to disrupt and deter these attacks. Today's announcements also demonstrate the value of early notification to law enforcement; we thank Colonial Pipeline for quickly notifying the FBI when they learned that they were targeted by DarkSide."

"There is no place beyond the reach of the FBI to conceal illicit funds that will prevent us from imposing risk and consequences upon malicious cyber actors," said FBI Deputy Director Paul Abbate. "We will continue to use all of our available resources and leverage our domestic and international partnerships to disrupt ransomware attacks and protect our private sector partners and the American public."

"We've got to recognize these ransomware attacks for what they are. It's a serious national security threat," said Sen. Rob Portman, a Republican from Ohio. "Attacks against critical infrastructure are not just attacks on companies. They are attacks on our country itself."

FBI official explains how they recovered millions from hackers 02:53

10

10

American Hospital Association™ AHA TODAY
Advancing Health in America — Your source of news and insight.

June 11, 2021

Technology

Exclusive: U.S. to give ransomware hacks similar priority as terrorism

Christopher Bing

Reuters last week reported that the U.S. Justice Department is elevating the priority of ransomware investigations similar to those of terrorism attacks following a May 7 attack on the Colonial Pipeline and damage to other sectors. The department this week announced it had seized $2.3 million in bitcoin proceeds allegedly from the attack.

"The AHA has been leading a call to the government to pursue a coordinated campaign to disrupt these criminal organizations and seize their illegal proceeds, as was done so effectively during the global fight against terrorism," said John Riggi, AHA senior advisor for cybersecurity and risk. "*We have good reason to believe that our persistent advocacy and expert point of view on this issue helped influence this policy change.*"

11

11

- ***We need to do our part to defend against these threats with all available technical, human and financial resources.***

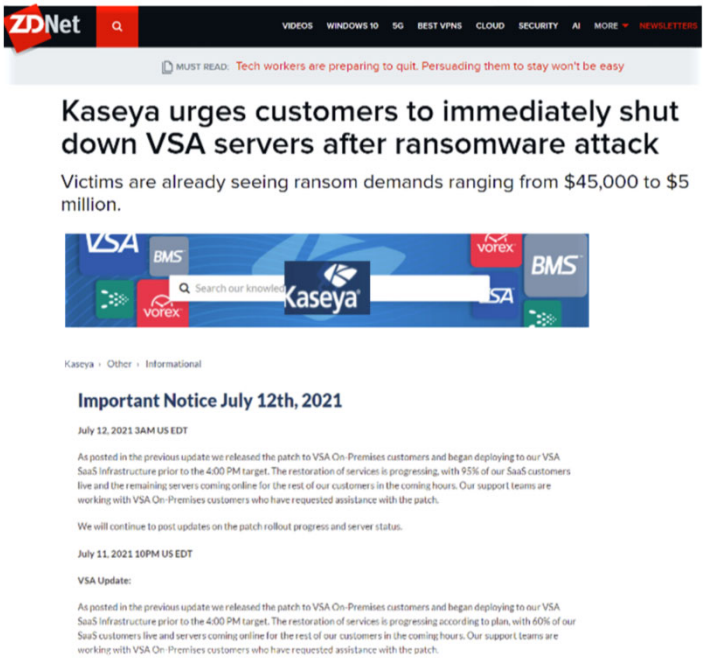
- We continue to call on the government to embark on a coordinated campaign utilizing all diplomatic, financial, law enforcement, intelligence and cyber military capabilities to disrupt these criminal organizations***, seize their illegal proceeds and increase consequences for those nations which harbor them - as we effectively did in the global fight against terrorism.***

Encouraging to see the Federal Bureau of Investigation (FBI) and the U.S. Department of Justice recently raise the investigative priority level of ransomware attacks to the same level as terrorist attacks. We are moving in the right direction."

June 23, 2021
https://video.foxbusiness.com/v/6260730434001#sp=show-clips

12

12



ZDNet

VIDEOS WINDOWS 10 5G BEST VPNS CLOUD SECURITY AI MORE NEWSLETTERS

MUST READ: Tech workers are preparing to quit. Persuading them to stay won't be easy

Kaseya urges customers to immediately shut down VSA servers after ransomware attack

Victims are already seeing ransom demands ranging from $45,000 to $5 million.

Kaseya › Other › Informational

Important Notice July 12th, 2021

July 12, 2021 3AM US EDT

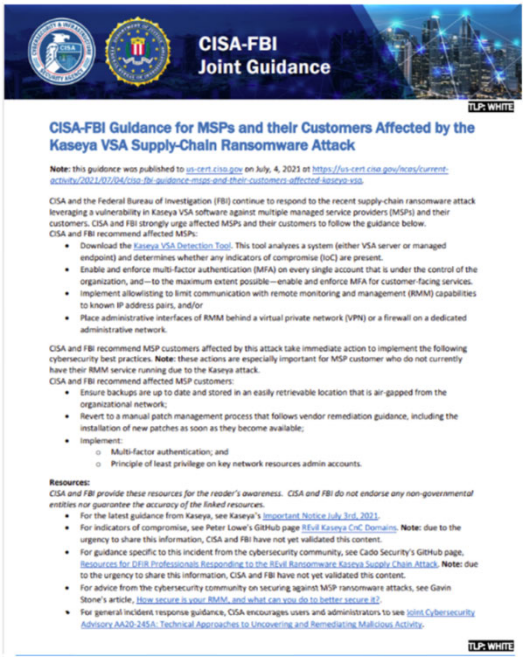
As posted in the previous update we released the patch to VSA On-Premises customers and began deploying to our VSA SaaS infrastructure prior to the 4:00 PM target. The restoration of services is progressing, with 95% of our SaaS customers live and the remaining servers coming online for the rest of our customers in the coming hours. Our support teams are working with VSA On-Premises customers who have requested assistance with the patch.

We will continue to post updates on the patch rollout progress and server status.

July 11, 2021 10PM US EDT

VSA Update:

As posted in the previous update we released the patch to VSA On-Premises customers and began deploying to our VSA SaaS infrastructure prior to the 4:00 PM target. The restoration of services is progressing according to plan, with 60% of our SaaS customers live and servers coming online for the rest of our customers in the coming hours. Our support teams are working with VSA On-Premises customers who have requested assistance with the patch.



CISA-FBI Joint Guidance

TLP: WHITE

CISA-FBI Guidance for MSPs and their Customers Affected by the Kaseya VSA Supply-Chain Ransomware Attack

Note: this guidance was published to us-cert.cisa.gov on July, 4, 2021 at https://us-cert.cisa.gov/ncas/current-activity/2021/07/04/cisa-fbi-guidance-msps-and-their-customers-affected-kaseya-vsa.

CISA and the Federal Bureau of Investigation (FBI) continue to respond to the recent supply-chain ransomware attack leveraging a vulnerability in Kaseya VSA software against multiple managed service providers (MSPs) and their customers. CISA and FBI strongly urge affected MSPs and their customers to follow the guidance below.
CISA and FBI recommend affected MSPs:

- Download the Kaseya VSA Detection Tool. This tool analyzes a system (either VSA server or managed endpoint) and determines whether any indicators of compromise (IoC) are present.
- Enable and enforce multi-factor authentication (MFA) on every single account that is under the control of the organization, and—to the maximum extent possible—enable and enforce MFA for customer-facing services.
- Implement allowlisting to limit communication with remote monitoring and management (RMM) capabilities to known IP address pairs, and/or
- Place administrative interfaces of RMM behind a virtual private network (VPN) or a firewall on a dedicated administrative network.

CISA and FBI recommend MSP customers affected by this attack take immediate action to implement the following cybersecurity best practices. **Note:** these actions are especially important for MSP customer who do not currently have their RMM service running due to the Kaseya attack.
CISA and FBI recommend affected MSP customers:

- Ensure backups are up to date and stored in an easily retrievable location that is air-gapped from the organizational network;
- Revert to a manual patch management process that follows vendor remediation guidance, including the installation of new patches as soon as they become available;
- Implement:
  - Multi-factor authentication; and
  - Principle of least privilege on key network resources admin accounts.

Resources:
CISA and FBI provide these resources for the reader's awareness. CISA and FBI do not endorse any non-governmental entities nor guarantee the accuracy of the linked resources.

- For the latest guidance from Kaseya, see Kaseya's Important Notice July 3rd, 2021.
- For indicators of compromise, see Peter Lowe's GitHub page REvil Kaseya CnC Domains. **Note:** due to the urgency to share this information, CISA and FBI have not yet validated this content.
- For guidance specific to this incident from the cybersecurity community, see Cado Security's GitHub page, Resources for DFIR Professionals Responding to the REvil Ransomware Kaseya Supply Chain Attack. **Note:** due to the urgency to share this information, CISA and FBI have not yet validated this content.
- For advice from the cybersecurity community on securing against MSP ransomware attacks, see Gavin Stone's article, How secure is your RMM, and what can you do to better secure it?
- For general incident response guidance, CISA encourages users and administrators to see Joint Cybersecurity Advisory AA20-245A: Technical Approaches to Uncovering and Remediating Malicious Activity.

TLP: WHITE

13

Top FBI official advises Congress against banning ransomware payments

© Greg Nash

"..regardless of whether or not a victim chooses to pay, ***our goal is to identify, pursue, and impose consequences on criminal actors, not their victims."***
The FBI strongly encourages victims to report ransomware incidents to the FBI.

14

14

Photographer: A

Cybersecurity

Ransomware Gang REvil Vanishes From Web After Biden Warning

By William Turton

July 13, 2021, 10:01 AM EDT *Updated on July 13, 2021, 11:11 AM EDT*

- Unclear if sites taken down voluntarily or by law enforcement
- Hacking group hit meat supplier JBS, Kaseya in recent weeks

LISTEN TO ARTICLE

▶ 2:28

The Russia-linked ransomware gang REvil has seemingly vanished from the dark web, where it maintains several pages documenting its activities including one called the "happy blog."

Most Read

15

15

Wednesday, 8/4/2021

Sanford Health target of attempted cyber attack

Sanford Health issued a statement disclosing that it has sustained an attempted 'cyber security incident' but said it believes no personal or financial information has been compromised. An investigation continues.

Written By: Patrick Springer | 4:46 pm, Aug. 4, 2021

Sanford Medical Center Fargo is seen Monday, Aug. 2, 2021, at 5225 23rd Ave. S. Michael Vosburg / Forum Photo Editor

Thursday, 8/5/2021

Eskenazi Health diverting ambulances as cyber-attack investigation continues

16

16

Sunday, 8/15/2021 – Tuesday, 8/17/201

Memorial Health System experiences cyber attack

LOCAL NEWS

AUG 16, 2021

AMY PHELPS
Staff Reporter
aphelps@newsandsentinel.com

In the early ho

"IT noticed
Cantley at
system."

Surgeries canceled, ambulances diverted, IT system down at Ohio health system after ransomware attack

Hannah Mitchell - yesterday Print | Email

Share Tweet Share 22 Listen

Marietta, Ohio-based Memorial Health System is diverting some patients after a ransomware attack that forced it to shut down its IT systems, according to an Aug. 16 *Marietta Times* report.

17

17

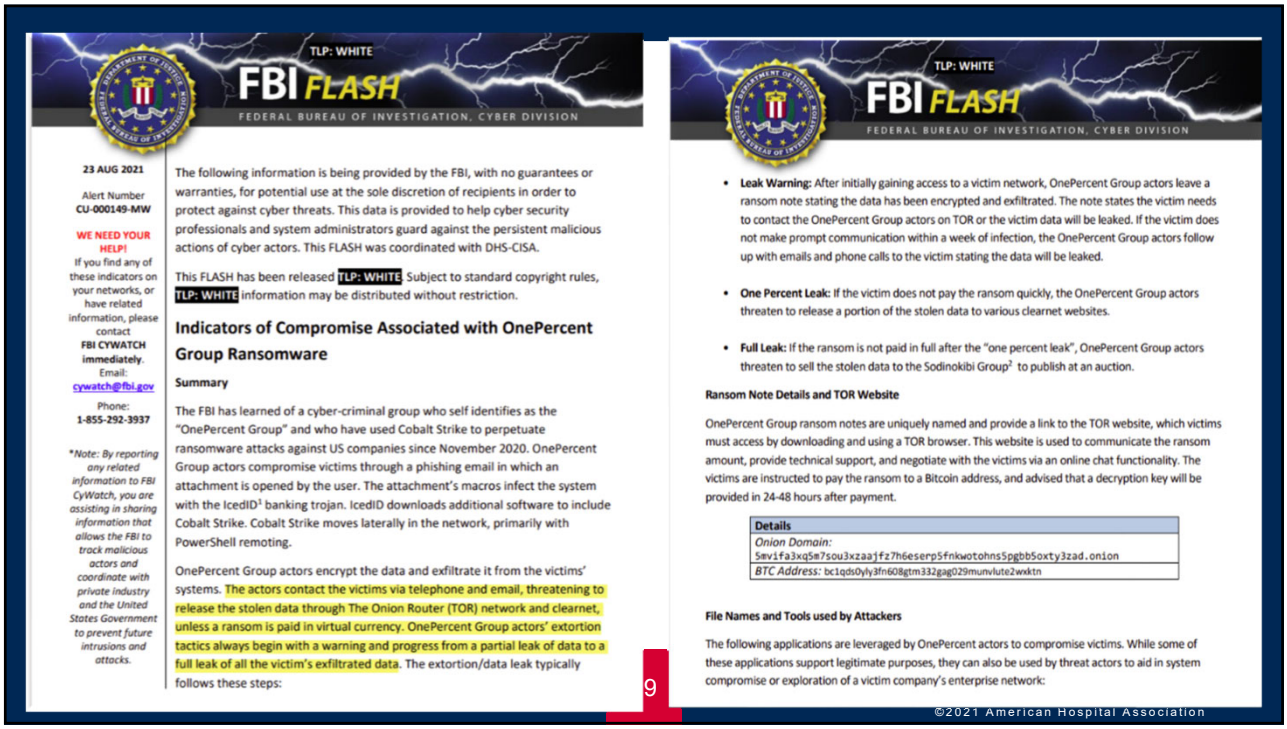
Russian Ransomware Group REvil Back Online After 2-Month Hiatus

September 09, 2021 Ravie Lakshmanan

The operators behind the REvil ransomware-as-a-service (RaaS) staged a surprise return after a two-month hiatus following the widely publicized attack on technology services provider Kaseya on July 4.

18

18



TLP: WHITE

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

23 AUG 2021

Alert Number
CU-000149-MW

WE NEED YOUR HELP!
If you find any of these indicators on your networks, or have related information, please contact **FBI CYWATCH immediately**.
Email: cywatch@fbi.gov
Phone: **1-855-292-3937**

**Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This FLASH was coordinated with DHS-CISA.

This FLASH has been released **TLP: WHITE**. Subject to standard copyright rules, **TLP: WHITE** information may be distributed without restriction.

Indicators of Compromise Associated with OnePercent Group Ransomware

Summary

The FBI has learned of a cyber-criminal group who self identifies as the "OnePercent Group" and who have used Cobalt Strike to perpetuate ransomware attacks against US companies since November 2020. OnePercent Group actors compromise victims through a phishing email in which an attachment is opened by the user. The attachment's macros infect the system with the IcedID[1] banking trojan. IcedID downloads additional software to include Cobalt Strike. Cobalt Strike moves laterally in the network, primarily with PowerShell remoting.

OnePercent Group actors encrypt the data and exfiltrate it from the victims' systems. The actors contact the victims via telephone and email, threatening to release the stolen data through The Onion Router (TOR) network and clearnet, unless a ransom is paid in virtual currency. OnePercent Group actors' extortion tactics always begin with a warning and progress from a partial leak of data to a full leak of all the victim's exfiltrated data. The extortion/data leak typically follows these steps:

9

TLP: WHITE

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

- **Leak Warning:** After initially gaining access to a victim network, OnePercent Group actors leave a ransom note stating the data has been encrypted and exfiltrated. The note states the victim needs to contact the OnePercent Group actors on TOR or the victim data will be leaked. If the victim does not make prompt communication within a week of infection, the OnePercent Group actors follow up with emails and phone calls to the victim stating the data will be leaked.
- **One Percent Leak:** If the victim does not pay the ransom quickly, the OnePercent Group actors threaten to release a portion of the stolen data to various clearnet websites.
- **Full Leak:** If the ransom is not paid in full after the "one percent leak", OnePercent Group actors threaten to sell the stolen data to the Sodinokibi Group[2] to publish at an auction.

Ransom Note Details and TOR Website

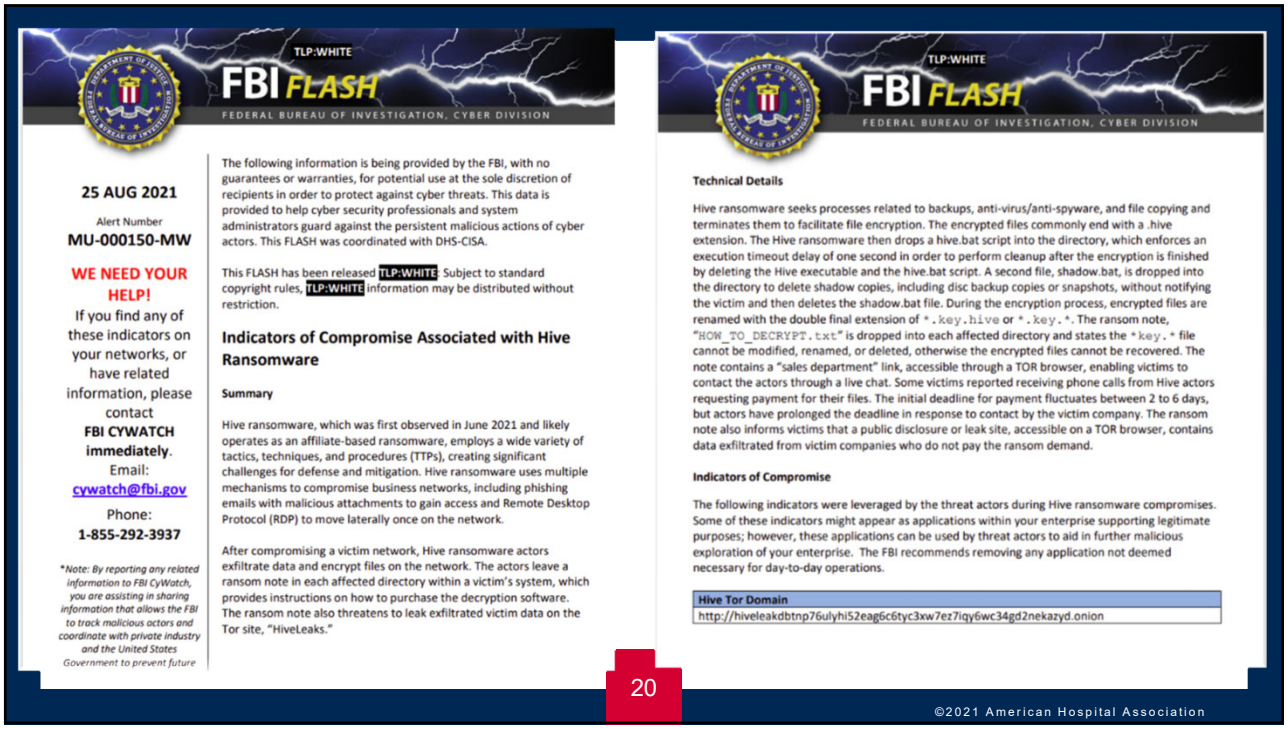
OnePercent Group ransom notes are uniquely named and provide a link to the TOR website, which victims must access by downloading and using a TOR browser. This website is used to communicate the ransom amount, provide technical support, and negotiate with the victims via an online chat functionality. The victims are instructed to pay the ransom to a Bitcoin address, and advised that a decryption key will be provided in 24-48 hours after payment.

Details
Onion Domain: 5mv1fa3xq5m7sou3xzaajfz7h6eserp5fnkwotohns5pgbb5oxty3zad.onion
BTC Address: bc1qds0yly3fn608gtm332gag029munvlute2wxktn

File Names and Tools used by Attackers

The following applications are leveraged by OnePercent actors to compromise victims. While some of these applications support legitimate purposes, they can also be used by threat actors to aid in system compromise or exploration of a victim company's enterprise network:

19



TLP:WHITE

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

25 AUG 2021

Alert Number
MU-000150-MW

WE NEED YOUR HELP!
If you find any of these indicators on your networks, or have related information, please contact **FBI CYWATCH immediately**.
Email: cywatch@fbi.gov
Phone: **1-855-292-3937**

**Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future*

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This FLASH was coordinated with DHS-CISA.

This FLASH has been released **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

Indicators of Compromise Associated with Hive Ransomware

Summary

Hive ransomware, which was first observed in June 2021 and likely operates as an affiliate-based ransomware, employs a wide variety of tactics, techniques, and procedures (TTPs), creating significant challenges for defense and mitigation. Hive ransomware uses multiple mechanisms to compromise business networks, including phishing emails with malicious attachments to gain access and Remote Desktop Protocol (RDP) to move laterally once on the network.

After compromising a victim network, Hive ransomware actors exfiltrate data and encrypt files on the network. The actors leave a ransom note in each affected directory within a victim's system, which provides instructions on how to purchase the decryption software. The ransom note also threatens to leak exfiltrated victim data on the Tor site, "HiveLeaks."

20

TLP:WHITE

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Technical Details

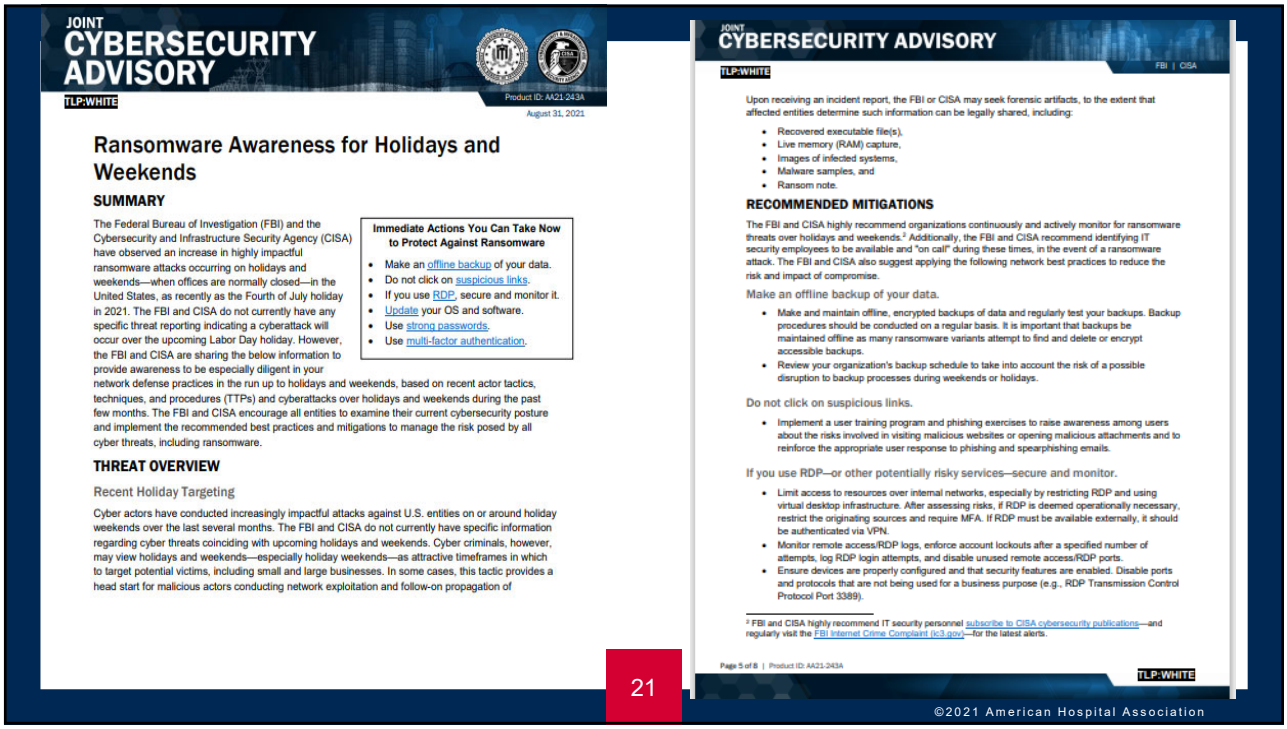
Hive ransomware seeks processes related to backups, anti-virus/anti-spyware, and file copying and terminates them to facilitate file encryption. The encrypted files commonly end with a .hive extension. The Hive ransomware then drops a hive.bat script into the directory, which enforces an execution timeout delay of one second in order to perform cleanup after the encryption is finished by deleting the Hive executable and the hive.bat script. A second file, shadow.bat, is dropped into the directory to delete shadow copies, including disc backup copies or snapshots, without notifying the victim and then deletes the shadow.bat file. During the encryption process, encrypted files are renamed with the double final extension of `*.key.hive` or `*.key.*`. The ransom note, "`HOW_TO_DECRYPT.txt`" is dropped into each affected directory and states the `*key.*` file cannot be modified, renamed, or deleted, otherwise the encrypted files cannot be recovered. The note contains a "sales department" link, accessible through a TOR browser, enabling victims to contact the actors through a live chat. Some victims reported receiving phone calls from Hive actors requesting payment for their files. The initial deadline for payment fluctuates between 2 to 6 days, but actors have prolonged the deadline in response to contact by the victim company. The ransom note also informs victims that a public disclosure or leak site, accessible on a TOR browser, contains data exfiltrated from victim companies who do not pay the ransom demand.

Indicators of Compromise

The following indicators were leveraged by the threat actors during Hive ransomware compromises. Some of these indicators might appear as applications within your enterprise supporting legitimate purposes; however, these applications can be used by threat actors to aid in further malicious exploration of your enterprise. The FBI recommends removing any application not deemed necessary for day-to-day operations.

Hive Tor Domain
http://hiveleakdbtnp76ulyhi52eag6c6tyc3xw7ez7iqy6wc34gd2nekazyd.onion

20



JOINT
CYBERSECURITY ADVISORY

TLP:WHITE

Product ID: AA21-243A

August 31, 2021

Ransomware Awareness for Holidays and Weekends

SUMMARY

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) have observed an increase in highly impactful ransomware attacks occurring on holidays and weekends—when offices are normally closed—in the United States, as recently as the Fourth of July holiday in 2021. The FBI and CISA do not currently have any specific threat reporting indicating a cyberattack will occur over the upcoming Labor Day holiday. However, the FBI and CISA are sharing the below information to provide awareness to be especially diligent in your network defense practices in the run up to holidays and weekends, based on recent actor tactics, techniques, and procedures (TTPs) and cyberattacks over holidays and weekends during the past few months. The FBI and CISA encourage all entities to examine their current cybersecurity posture and implement the recommended best practices and mitigations to manage the risk posed by all cyber threats, including ransomware.

Immediate Actions You Can Take Now to Protect Against Ransomware

- Make an offline backup of your data.
- Do not click on suspicious links.
- If you use RDP, secure and monitor it.
- Update your OS and software.
- Use strong passwords.
- Use multi-factor authentication.

THREAT OVERVIEW

Recent Holiday Targeting

Cyber actors have conducted increasingly impactful attacks against U.S. entities on or around holiday weekends over the last several months. The FBI and CISA do not currently have specific information regarding cyber threats coinciding with upcoming holidays and weekends. Cyber criminals, however, may view holidays and weekends—especially holiday weekends—as attractive timeframes in which to target potential victims, including small and large businesses. In some cases, this tactic provides a head start for malicious actors conducting network exploitation and follow-on propagation of

JOINT
CYBERSECURITY ADVISORY

TLP:WHITE

FBI | CISA

Upon receiving an incident report, the FBI or CISA may seek forensic artifacts, to the extent that affected entities determine such information can be legally shared, including:

- Recovered executable file(s),
- Live memory (RAM) capture,
- Images of infected systems,
- Malware samples, and
- Ransom note.

RECOMMENDED MITIGATIONS

The FBI and CISA highly recommend organizations continuously and actively monitor for ransomware threats over holidays and weekends.[2] Additionally, the FBI and CISA recommend identifying IT security employees to be available and "on call" during these times, in the event of a ransomware attack. The FBI and CISA also suggest applying the following network best practices to reduce the risk and impact of compromise.

Make an offline backup of your data.

- Make and maintain offline, encrypted backups of data and regularly test your backups. Backup procedures should be conducted on a regular basis. It is important that backups be maintained offline as many ransomware variants attempt to find and delete or encrypt accessible backups.
- Review your organization's backup schedule to take into account the risk of a possible disruption to backup processes during weekends or holidays.

Do not click on suspicious links.

- Implement a user training program and phishing exercises to raise awareness among users about the risks involved in visiting malicious websites or opening malicious attachments and to reinforce the appropriate user response to phishing and spearphishing emails.

If you use RDP—or other potentially risky services—secure and monitor.

- Limit access to resources over internal networks, especially by restricting RDP and using virtual desktop infrastructure. After assessing risks, if RDP is deemed operationally necessary, restrict the originating sources and require MFA. If RDP must be available externally, it should be authenticated via VPN.
- Monitor remote access/RDP logs, enforce account lockouts after a specified number of attempts, log RDP login attempts, and disable unused remote access/RDP ports.
- Ensure devices are properly configured and that security features are enabled. Disable ports and protocols that are not being used for a business purpose (e.g., RDP Transmission Control Protocol Port 3389).

[2] FBI and CISA highly recommend IT security personnel subscribe to CISA cybersecurity publications—and regularly visit the FBI Internet Crime Complaint (ic3.gov)—for the latest alerts.

Page 5 of 8 | Product ID: AA21-243A

TLP:WHITE

21

21

Ransomware Trends 2020 - 2021

- Attacks are highly targeted against specific healthcare entities
- Phishing emails is still the primary “attack vector” – because it’s simple and it work, followed by remote access, unpatched vulnerabilities and compromised credentials
- Increasing in sophistication and severity. Ryuk, Conti and DopplePaymer, Mamba, Nefilim, REvil
- Network and data backups may be targeted first
- Ransomware may now execute within hours or minutes upon initial compromise leaving very little reaction time to identify and contain
- Ransom demands are increasing and scaled based upon size of organization targeted, multi-million dollar requests common, reports of ransom demands exceeding $60,000,000 in 2020
- High volume/disruptive telephone calls to executives and staff demanding ransom payment
- Ransomware attack combined with other cyber crimes - data extortion. Criminals threaten to sell /publish stolen patient data

22

22

Ransomware Impact 2020 -2021

- Disruption to patient care and business operations – *Patient safety issue*
- Telemetry systems inoperable – nurse must be present for critical patients
- EMR rendered inaccessible – treatment and drug allergies / interactions unknown – delay in rendering care
- Lab results and imagery unavailable
- Surgeries and cancer treatments cancelled or delayed
- *ED's shutdown - Ambulances placed on full divert - delay of emergency treatment – Rural Impact – Regional Impact – Level 1 Trauma Center – Golden Hour, stroke patients, bad weather, could eliminate medivac option and increase diversion transport time*
- *Ransomware "blast radius" – dependent providers and third parties, also disru*Recovery time from ransomware attacks, even if able to restore from unaffected backups, minimum 3-4 weeks - residual impacts lasting up to 6 months
- Increased insurance premiums
- Increase in credit risk leading to increase in cost of financing
- Lost revenue implications, burn rate, and of course:
  - Reputational harm - loss of patient, community and investor confidence

©2021 American Hospital Association

23

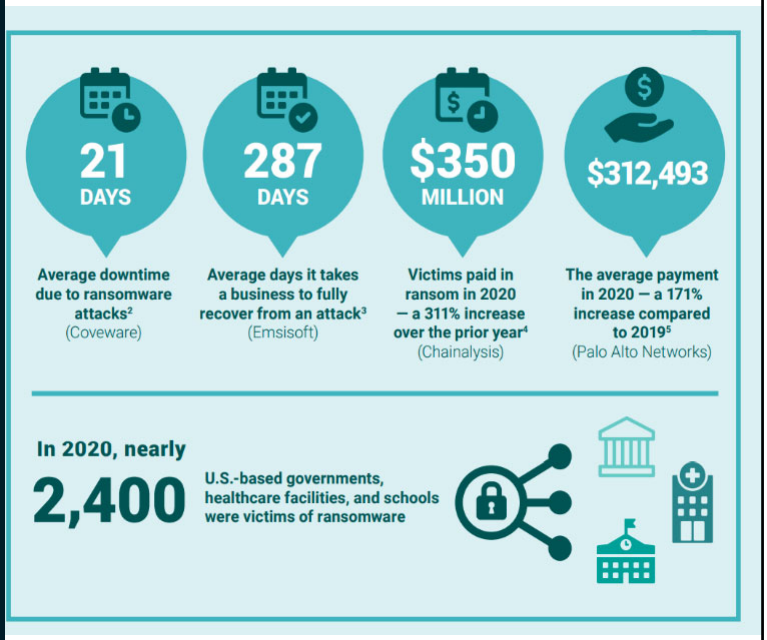
RANSOMWARE TASK FORCE

Combating Ransomware

A Comprehensive Framework for Action:
Key Recommendations from the Ransomware Task Force

Prepared by the Institute for Security and Technology

IST Institute for SECURITY + TECHNOLOGY



24

Contributing Factors 2020 -2021

- Email – Phishing Attack. Need for increased employee awareness and training
- Email – Insufficient email technical security controls. Need for increased email advanced threat protection, behavior and signature based, quarantine of attachments, safe links
- Lack of multifactor authorization (MFA) for remote access of networks, VPN, and email. Institute MFA for all categories of remote access – Then internally for all system administrative privileges
- "Flat" networks. Need for network segmentation
- Lack of real time 24/7 log, event, incident and alerts monitoring. Need full time internal or external Managed Detection and Response (MDR) service

25

25

Contributing Factors 2020 -2021 (cont.)

•Insufficient or delayed leadership notification, response and/or emergency containment actions. Need updated, organization wide, routinely tested cyber incident response plan, with clear lines of designated and delegated emergency action authorities.

•*Inability to restore from backups*. Need to ensure backups are offline, network segmented, multiple copies on prem and in cloud, highly secure, no remote access, MFA, 3-2-1 rule.

•*Unprepared for a multi-week or multi-month IT disruption. Need contingency plans for continuity of patient services, imaging, lab results, documentation on paper, revenue cycle disruption, 3rd party dependencies.*

•Insufficient cyber insurance coverage hindering response and recovery efforts. Conduct review of cyber insurance coverage for limitations, exclusions, ransomware coverage, forensics firms capabilities, bitcoin.

26

26

Good News, Helpful Strategies and Resources

27

27

THE WHITE HOUSE
WASHINGTON

TO: Corporate Executives and Business Leaders

FROM: Anne Neuberger, Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology

SUBJECT: What We Urge You To Do To Protect Against The Threat of Ransomware

DATE: June 2, 2021

The number and size of ransomware incidents have increased significantly, and strengthening our nation's resilience from cyberattacks – both private and public sector – is a top priority of the President's.

Under President Biden's leadership, the Federal Government is stepping up to do its' part, working with like-minded partners around the world to disrupt and deter ransomware actors. These efforts include disrupting ransomware networks, working with international partners to hold countries that harbor ransomware actors accountable, developing cohesive and consistent policies towards ransom payments and enabling rapid tracing and interdiction of virtual currency proceeds.

The private sector also has a critical responsibility to protect against these threats. All organizations must recognize that no company is safe from being targeted by ransomware, regardless of size or location. But there are immediate steps you can take to protect yourself, as well as your customers and the broader economy. Much as our homes have locks and alarm systems and our office buildings have guards and security to meet the threat of theft, we urge you to take ransomware crime seriously and ensure your corporate cyber defenses match the threat.

The most important takeaway from the recent spate of ransomware attacks on U.S., Irish, German and other organizations around the world is that companies that view ransomware as a threat to their core business operations rather than a simple risk of data theft will react and recover more effectively. To understand your risk, business executives should immediately convene their leadership teams to discuss the ransomware threat and review corporate security posture and business continuity plans to ensure you have the ability to continue or quickly restore operations.

Below you will find the U.S. Government's recommended best practices – we've selected a small number of highly impactful steps to help you focus and make rapid progress on driving down risk.

What We Urge You To Do Now

Implement the five best practices from the President's Executive Order: President Biden's *Improving the Nation's Cybersecurity* Executive Order is being implemented with speed and urgency across the Federal Government. We're leading by example because these five best practices are high impact: multifactor authentication (because passwords alone are routinely compromised), endpoint detection & response (to hunt for malicious activity on a network and block it), encryption (so if data is stolen, it is unusable) and a skilled, empowered security team (to patch rapidly, and share and incorporate threat information in your defenses). These practices will significantly reduce the risk of a successful cyber-attack.

Backup your data, system images, and configurations, regularly test them, and keep the backups offline: Ensure that backups are regularly tested and that they are not connected to the business network, as many ransomware variants try to find and encrypt or delete accessible backups. Maintaining current backups offline is critical because if your network data is encrypted with ransomware, your organization can restore systems.

Update and patch systems promptly: This includes maintaining the security of operating systems, applications, and firmware, in a timely manner. Consider using a centralized patch management system; use a risk-based assessment strategy to drive your patch management program.

Test your incident response plan: There's nothing that shows the gaps in plans more than testing them. Run through some core questions and use those to build an incident response plan: Are you able to sustain business operations without access to certain systems? For how long? Would you turn off your manufacturing operations if business systems such as billing were offline?

Check Your Security Team's Work: Use a 3rd party pen tester to test the security of your systems and your ability to defend against a sophisticated attack. Many ransomware criminals are aggressive and sophisticated and will find the equivalent of unlocked doors.

Segment your networks: There's been a recent shift in ransomware attacks – from stealing data to disrupting operations. It's critically important that your corporate business functions and manufacturing/production operations are separated and that you carefully filter and limit internet access to operational networks, identify links between these networks and develop workarounds or manual controls to ensure ICS networks can be isolated and continue operating if

28

28

TLP:WHITE

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Recommended Mitigations

- Back-up critical data offline.
- Ensure copies of critical data are in the cloud or on an external hard drive or storage device.
- Secure your back-ups and ensure data is not accessible for modification or deletion from the system where the data resides.
- Use two-factor authentication with strong passwords, including for remote access services.
- Monitor cyber threat reporting regarding the publication of compromise credentials and change passwords/settings if applicable.
- Keep computers, devices, and applications patched and up-to-date.
- Install and regularly update anti-virus or anti-malware software on all ho
- Review the following additional resources.
  - The joint advisory from Australia, Canada, New Zealand, the Unite United States on Technical Approaches to Uncovering and Remed Activity provides additional guidance when hunting or investigatir common mistakes to avoid in incident handling.
  - The Cybersecurity and Infrastructure Security Agency-Multi-State & Analysis Center Joint Ransomware Guide covers additional best to prevent, protect, and respond to a ransomware attack.
  - StopRansomware.gov is the U.S. Government's official one-stop lo to tackle ransomware more effectively.

If your organization is impacted by a ransomware incident, the FBI and CISA recommend the following actions.

- **Isolate the infected system.** Remove the infected system from all networks, and disable the computer's wireless, Bluetooth, and any other potential networking capabilities. Ensure all shared and networked drives are disconnected, whether wired or wireless.
- **Turn off other computers and devices.** Power-off and segregate (i.e., remove from the network) the infected computer(s). Power-off and segregate any other computers or devices that share a network with the infected computer(s) that have not been fully encrypted by ransomware. If possible, collect and secure all infected and potentially infected computers and devices in a central location, making sure to clearly label any computers that have been encrypted. Powering-off and segregating infected computers and computers that have not been fully encrypted may allow for the recovery of partially encrypted files by specialists.
- **Secure your backups.** Ensure that your backup data is offline and secure. If possible, scan your backup data with an antivirus program to check that it is free of malware.

29

29

TLP:WHITE

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Information Requested

The FBI does not encourage paying a ransom to criminal actors. Paying a ransom may embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. Paying the ransom also does not guarantee that a victim's files will be recovered. However, the FBI understands that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers. Regardless of whether you or your organization decide to pay the ransom, the FBI urges you to report ransomware incidents to your local field office. Doing so provides investigators with the critical information they need to track ransomware attackers, hold them accountable under US law, and prevent future attacks.

The FBI may seek the following information that you determine you can legally share, including:

- Recovered executable files
- Live memory (RAM) capture
- Images of infected systems
- Malware samples
- IP addresses identified as malicious or suspicious
- Email addresses of the attackers
- A copy of the ransom note
- Ransom amount
- Bitcoin wallets used by the attackers
- Bitcoin wallets used to pay the ransom
- Post-incident forensic reports

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. CyWatch can be contacted by phone at (855) 292-3937 or by e-mail at CyWatch@ic.fbi.gov. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's National Press Office at npo@ic.fbi.gov or (202) 324-3691.

30

30

American Hospital Association™ Advancing Health in America

AHA TODAY Your source of news and insight

Cybersecurity bill with AHA-supported provisions signed into law Jan. 05 2021

President Trump yesterday signed into law a bill (H.R. 7898) PL 116-321 containing provisions that require the Secretary of Health and Human Services to ***consider certain recognized cybersecurity best practices when making determinations against HIPAA-covered entities and business associates victimized by a cyberattack.*** For example, the bill recognizes cybersecurity practices established under the National Institute of Standards and Technology Act and approaches established under Section 405(d) of the Cybersecurity Act of 2015 by the Healthcare and Public Health Sector Coordinating Council (HSCC) Working Group, whose members include the AHA. The HSCC expressed strong support for the provisions. The legislation cleared the Senate by unanimous consent on Dec. 19.

- **Recognized Cybersecurity Practices in Place Previous 12 months**
- **Reduced Fines**
- **Early, Favorable Termination of Audits**
- **Mitigation of other penalties**
- **No Increased Penalties for Not Having Recognized Cybersecurity Practices in Place**

"This law will have long lasting positive impact for the entire health care sector in securing patient data and protecting patients from cyber risks," said John Riggi, AHA senior advisor for cybersecurity and risk. "*The law provides the right balance of incentivizing voluntary, enhanced cybersecurity protocols in exchange for regulatory relief and recognition that breached organizations are victims, not the perpetrators."*

31

Risk Tolerance and Cyber Insurance

- How much cyber risk are we willing to accept?
- How much risk are we willing to transfer?
- Do we have cyber insurance?
- What are the limitations and requirements?
- Vendor and subcontractor requirements?
- Scales with VRM risk prioritization
- Is our cyber insurance coverage adequate and current to cover all costs associated with a:
  - Multi-day network outage
  - Breach mitigation and recovery
  - Lost revenue
  - Reputational harm
  - Legal and regulatory exposure
  - Victim and patient services – credit monitoring
- Forensics firms panel – integration with IRP
- Interaction and integration with other insurance policies
- Ransomware coverage – bitcoin
- "Act of war" exemption for cyber?

32

32

HEALTH IT

E-Newsletters | Conferences | Virtual Conferences | Webinars

Artificial Intelligence Consumerism Cybersecurity Data

Cybersecurity insurance costs amid surges in ransomware att finds

Hannah Mitchell - 4 hours ago Print | Email

Hackers are increasingly carrying out cyberattacks on hospitals, highlighting the critical need for stable cybersecurity insurance. Yet, as the number of attacks on hospitals surges, so does the cost of insurance, according to a May 20 report by the Government Office of Accountability.

Moody's message to hospitals: Brace yourself for more ransomware attacks

Jackie Drees - 3 hours ago Print | Email

Hospitals and health systems will continue to be the targets of ransomware attacks because of the large amounts of sensitive data they harbor and the expanded use of less secure networks stemming from the pandemic-related shift to remote work, according to a Moody's Investor Services report released May 26.

Moody's estimates that the growing interconnectedness of healthcare delivery and technology will continue to leave the healthcare sector vulnerable to data breaches along with hospitals' extensive use of third-party software vendors for clinical and billing functions, among others.

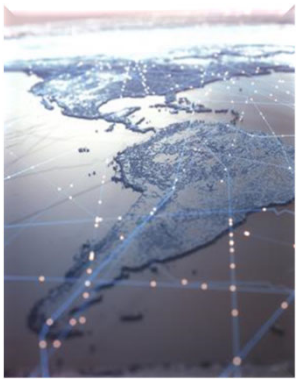
"VMware Carbon Black found there were 239.4 million attempted attacks on the firm's healthcare customers in 2020, a nearly 10,000 percent increase from 2019, according to Moody's."

33

33

Strategic Vendor Risk Management Program Considerations

- Does your organization have a vendor risk management program (VRM)? What is the governance structure and does that structure still make sense?
- Is there a formal process to incorporate cybersecurity in the VRM program?
- Is there process to conduct periodic in-depth technical, legal, policy and procedural review of the VRM program and the BAA?
- Does the BAA include cybersecurity and cyber insurance requirements for the vendor and any subs of the vendor? Are the coverages and limits sufficient?
- Annual cyber risk assessments for vendors?
- Compliance requirements with applicable regulatory standards - HIPAA, PCI, PII, taxpayer funded medical research and IP?



https://healthsectorcouncil.org/wp-content/uploads/2020/09/Health-Industry-Cybersecurity-Supply-Chain-Risk-Management-Guide-v2.pdf

American Hospital Association™

Advancing Health in America

34

34

Strategic Vendor Risk Management Program Considerations (cont.)

- Identify, risk classify and risk prioritize vendors *and their subcontractors* based upon:
- Aggregation of data – regulated data and unregulated data such as pop health genetic studies, clinical trials, COVID-19 research
- Access to sensitive data, networks, systems and physical locations
- Criticality/Impact to continuity of operations - Clinical, facilities, utilities, business (e.g. telecom, medical transcription, billing and coding, PPE supplies, etc)
- Foreign operations and foreign subcontractors
- Implement risk based controls and cyber insurance requirements
- Need to balance financial opportunities and greater supply-chain flexibility with potentially higher cyber risks associated with certain vendors

35

35

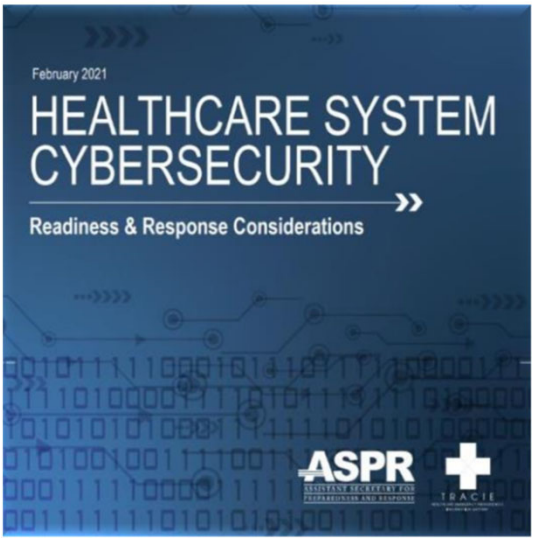
Cyber Incident Response Plan

- *Backup status and security, 3-2-1, restoration point and time, offline?*
- Do we have a **unified** cyber-incident response plan & is it up to date?
- Multi-day impact and multi-incident plan?
- Does it include specific individuals from all clinical, business, admin and facilities functions - with defined roles, responsibilities and ***off hours contact information and plan access?***
- Activation and decision escalation protocol and matrices?
- Leadership role – ***designation and delegation of critical authorities***?
- Is the plan regularly tested, gaps and best practices identified and updated to include current threat scenarios such as ransomware?
- Legal, regulatory, financial and reputational risks?
- Internal and external communications strategy?
- Out of band communications ?
- Paper copies and downtime procedures?
- Continuity of operations – emergency management?
- Cyber insurance requirements – forensics firm ?
- FBI, government and forensics firm integration?

36

36

INCIDENT RESPONSE PLANNING



https://files.asprtracie.hhs.gov/documents/aspr-tracie-healthcare-system-cybersercurity-readiness-response.pdf

37

37

Questions?

California Hospital Association

38

Thank You

John Riggi
Senior Advisor for Cybersecurity and Risk
American Hospital Association
jriggi@aha.org
(O) +1 202-626-2272

California Hospital Association

American Hospital Association

39