Client Advisory:  
FBI, HHS, and CISA Warn of Imminent and Widespread Ransomware and Healthcare Attacks  

The Issue  
The Advisory issued October 28, 2020 from the Cybersecurity and Infrastructure Security Agency (“CISA”), the Federal Bureau of Investigation (“FBI”), and the Department of Health and Human Services (“HHS”) stated:

CISA, FBI, and HHS have credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers. CISA, FBI, and HHS are sharing this information to provide warning to healthcare providers to ensure that they take timely and reasonable precautions to protect their networks from these threats.

Key Findings  
CISA, FBI, and HHS assess malicious cyber actors are targeting the HPH Sector with Trickbot malware, often leading to ransomware attacks, data theft, and the disruption of healthcare services.

These issues will be particularly challenging for organizations within the COVID-19 pandemic; therefore, administrators will need to balance this risk when determining their cyber security investments.

Our Experience  
The Stroz Friedberg/Aon’s Cyber Solutions team has been responding to multiple ransomware incidents in the Healthcare industry related to the evolving Ryuk threat.

While Trickbot is one threat to be aware of, one very common entry point for Ryuk and other ransomware threat actors is a carefully crafted phishing campaign designed to create a sense of urgency to the recipient and to bypass email security systems.

Please be sure to monitor and educate your users for these phishing attacks, as they are a critical line of defense. You can expect to see emails referencing a sense of urgency such as “An employee has made a complaint against you” or “Bonus plan” that invites the user to click a link to a cloud storage provider (usually Google Docs). If users follow the link, it will typically initiate a malicious series of events including a Bazar Loader/Bazar Backdoor and Cobalt Strike, a post-exploitation toolkit, lateral movement to domain controllers and privilege escalation, and finally spreading Ryuk ransomware to the entire network.

What you can do now  
- Read the Advisory, including downloading the IOCs and implementing recommended mitigations. https://us-cert.cisa.gov/ncas/alerts/aa20-302a
- Ensure backups of medical records, including electronic records and have a 321-backup strategy – have hard copy or remote backup or both
- Protect your back-ups of critical systems – ensure that you have offline backups that cannot be impacted by an active threat on the network
- Establish and practice out of band, non-VoIP, communications
- Rehearse IT lockdown protocol and process, including practicing backups
- Contact any potentially relevant third-party vendors and have them on stand-by, including outside breach counsel, public relations and communications firms, external IT resources, and incident response partners
- Place internal IT resources on high alert
- Increase security monitoring of the IT environment with heightened emphasis on potential ingress points such as email, cloud hosted services, and remote access points

Find out how our cyber security solutions can help you.

Visit aon.com/cyber-solutions or call +1 212.981.6540
• Draft a notice to employees of the threat and reinforce their role in security. Highlight diligence with respect to phishing emails and other social engineering tactics (LinkedIn messaging, phone calls posing as IT, etc.) as this is still one of the most prevalent attack vectors for ransomware and other cyber attacks
• Have a plan in place for responding in the event of compromise. If not already in place as part of an Incident Response Plan, identify relevant stakeholders across the company who should be part of the core decision-making team
• Understand your Cyber insurance coverage and specifically the claim reporting provisions

HIPAA Concerns
When threat actors move throughout a healthcare system during a ransomware attack, it is imperative to have an experienced forensic investigation team that can quickly ascertain whether ePHI was accessed, downloaded and/or exfiltrated. Quick forensic response along with advice from cyber security breach legal counsel helps to ensure that all legal notification requirements are met for both state data breach notification laws as well as HIPAA breach notification rules.

How Aon’s Cyber Solutions Can Help
• Digital Forensics Incident Response: Our forensic leaders have extensive experience responding to ransomware attacks and can assist in investigating the attack, containment, remediation and recovery
• Threat Hunt: Our experienced cyber security teams conduct a proactive search for attackers within your networks based on identifiers we have collected while working a large number of similar ransomware events to potentially identify in-process attacks before encryption occurs
• Deep Dark Web Scan: Our Investigations team will assess online and externally facing risk exposure of exposed accounts, corporate assets, breached data, compromised credentials and online security vulnerabilities
• Incident Response Planning & Playbooks: Our tailored, comprehensive plans consider your organization’s industry threat landscape, governance model, and security framework
• Incident/Breach Tabletop Exercises: We perform a customized cyber threat simulation on your security program and IT infrastructure that mimics a real breach scenario specific to your industry
• $0 Incident Response Retainer: We set up a master services agreement with pre-negotiated terms and conditions, including preferred rates which allows you to be ready to react and call upon our specialists in times of crisis
• Cyber Insurance: Aon’s experienced brokerage team considers your security posture, your appetite for risk, and your existing portfolio of traditional property and casualty policies

Contacts
Tom Hibarger
Senior Managing Director
202.754.2815
thomas.hibarger@strozfriedberg.com

Cheri D. Carr
Managing Director, DFIR and Cyber Solutions CISO
469.866.2478
cheri.carr@strozfriedberg.com

Heather Hughes, CHPC, HCISPP
Vice President, Engagement Management
832.459.6790
heather.hughes@strozfriedberg.com

Jonathan Rajewski
Vice President, Digital Forensics and Incident Response
802.238.8530
jonathan.rajewski@strozfriedberg.com

About Cyber Solutions: Aon’s Cyber Solutions offers holistic cyber risk management, unsurpassed investigative skills, and proprietary technologies to help clients uncover and quantify cyber risks, protect critical assets, and recover from cyber incidents.

About Aon: Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

The information contained herein and the statements expressed are of a general nature and are not intended to address the circumstances of any particular individual or entity. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.


©2020 Aon plc. All rights reserved.