CISA Central Weekly Health Sector News Summary

Date: 11/19/2020

DISCLAIMER: This report is provided "as is" for informational purposes only. The Cybersecurity and Infrastructure Security Agency (CISA) does not provide any warranties of any kind regarding any information within. CISA does not endorse any commercial product or service referenced in this advisory or otherwise.

Date	Geographic Location	Item	Notes	Source(s)

11/13/2020	**International**	**Cyberattacks targeting health care must stop**	• Microsoft reports observing three state-sponsored APT groups targeting COVID-19 vaccine research
			• APT groups: Strontium (aka APT28, Russia), Zinc (aka APT38 and Lazarus Group, DPRK), and Cerium (DPRK)
			• CISA products on similar activity:
			  ○ AA20-302A: Ransomware Activity Targeting the Healthcare and Public Health Sector (TLP:WHITE)
			  ○ AA20-099A: COVID-19 Exploited by Malicious Cyber Actors (TLP:WHITE)
				• https://blogs.microsoft.com/on-the-issues/2020/11/13/health-care-cyberattacks-covid-19-paris-peace-forum/?2020-11-12
				• https://www.cyberscoop.com/russian-north-korean-hackers-targeted-covid-19-vaccine-researchers-attacks-got-microsoft-says/

11/13/2020	**International**	**Australian government warns of possible ransomware attacks on health sector**	• The Australian Cyber Security Centre (ACSC) reported an increase in attacks against the Health Sector using SDBBot, a precursor to Clop ransomware • TA505 (also known as Dudear, Evil Corp, Hive0065, TEMP.Warlock) has been observed using SDBBot	• https://www.zdnet.com/article/australian-government-warns-of-possible-ransomware-attacks-on-health-sector/ • https://www.cyber.gov.au/acsc/view-all-content/publications/ransomware-australia
11/14/2020	**International**	**Biotech research firm Miltenyi Biotec hit by ransomware, data leaked**	• Miltenyi Biotec, a Germany-based global biomedical research company. Its products are used by COVID-19 vaccine researchers. • October 2020 attack affected the company's global infrastructure, MountLocker ransomware actors have claimed responsibility	• https://www.bleepingcomputer.com/news/security/biotech-research-firm-miltenyi-biotec-hit-by-ransomware-data-leaked/ • https://www.terabitweb.com/2020/11/14/miltenyi-biotec-ransomware-attack-html/

Date	Geographic Location	Item	Notes	Source(s)
				• https://healthitsecurity.com/news/hackers-hit-covid-19-biotech-firm-cold-storage-giant-with-cyberattacks
11/16/2020	**National**	**Cold storage giant Americold hit by cyberattack, services impacted**	• Atlanta, Georgia-based cold storage giant Americold hit by cyberattack, services impacted • Ransomware attack is suspected, but unconfirmed • Cold storage facilities are increasingly important as they will be needed for long term storage of COVID vaccines • Chicago Rockford Airport is seeking to partner with Americold for storing vaccines ready for distribution	• https://www.bleepingcomputer.com/news/security/cold-storage-giant-americold-hit-by-cyberattack-services-impacted/ • https://www.infosecurity-magazine.com/news/americold-operations-downed-by/ • https://seekingalpha.com/filing/5236787 • https://healthitsecurity.com/news/hackers-hit-covid-19-biotech-firm-cold-storage-giant-with-cyberattacks
11/17/2020	**CT**	**Ransomware Attack Impacts First Impressions Orthodontics, Kids First Dentistry & Orthodontics**	• First Impressions Orthodontics, (subsidiary of Professional Dental Alliance of Connecticut PLLC) hit with a ransomware attack on Sept 28, 2020 • It's possible that the threat actors accessed patient data (and data for patient of Kids First Orthodontics and Dentistry who had x-rays at First Impressions), but "no evidence of data access, theft, or misuse were found." • First Impressions restored their system from backups, did not pay ransom	• https://www.hipaajournal.com/ransomware-attacks-impact-first-impressions-orthodontics-kids-first-dentistry-orthodontics-and-hendrick-health-patients/

11/18/2020	**MN
	FL**
		PHI Potentially Compromised in Security Incidents at People Incorporated and My Choice HouseCalls	• Cyberattack exposed People Incorporated Mental Health Services patient data
			  ○ Threat actor access was between April 28 and May 4, 2020.
			  ○ "No evidence was found to indicate any information was stolen or has been misused."
				• https://www.hipaajournal.com/phi-potentially-compromised-in-security-incidents-at-people-incorporated-and-my-choice-housecalls/

Date	Geographic Location	Item	Notes	Source(s)
			• Several computers were stolen from in-home healthcare provider My Choice HouseCalls (Jacksonville, Florida) around Sept 3, 2020 ○ The stolen computers had patient PII and PHI; the computers have not yet been recovered	
11/18/2020	**IA**	**Mercy Iowa City email hack exposed info of 60,000 patients**	• A breach at Mercy Iowa City hospital exposed the data of 60,473 patients • "[T]he hospital said it is unaware of any fraud or identity theft related to the incident."	• https://www.iowaattorneygeneral.gov/media/cms/11132020_Mercy_Iowa_City_1D095956B076E.pdf • https://www.beckershospitalreview.com/cybersecurity/mercy-iowa-city-email-hack-exposed-info-of-60-000-patients-4-details.html
11/19/2020	**CT**	**Derby's Griffin Hospital website taken offline due to major ransomware incident with webservice provider Managed.com**	• Managed.com hit with REvil ransomware attack on Nov 16, 2020, the ransom demand is $500,000 in Monero bitcoin • All Managed.com client sites, including Griffin Hospital (Derby, Connecticut) are currently offline • Griffin Health has setup an alternative website (griffinhealthct[.]org), including a secure patient portal	• https://www.fairfieldcitizenonline.com/business/article/Derby-s-Griffin-Hospital-website-taken-down-in-15739406.php • https://www.bleepingcomputer.com/news/security/revil-ransomware-hits-managedcom-hosting-provider-500k-ransom/ • https://www.zdnet.com/article/web-hosting-provider-managed-shuts-down-after-ransomware-attack/ • https://status.managed.com/
11/19/2020	**International**	**APT10 (China) Targets Japan-Linked Organizations in Long-Running and Sophisticated Attack Campaign**	• Campaign active (approximately) Oct 2019-Oct 2020 • Targets include automotive, engineering, and pharmaceutical organizations ○ No organizations have been named in open-source reports • Used variety of attacks, including Zerologon (CVE-2020-1472)	• https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/cicada-apt10-japan-espionage • https://www.zdnet.com/article/cicada-hacking-group-exploits-zerologon-launches-new-backdoor-in-automotive-industry-attack-wave/

Date	Geographic Location	Item	Notes	Source(s)
			• Malware used includes QuasarRAT (see CISA AR18-352A: Quasar Open-Source Remote Administration Tool) ○ Additional CISA products on Chinese-sponsored threat actor activity are available here: https://us-cert.cisa.gov/china	• https://www.bleepingcomputer.com/news/security/chinese-apt10-hackers-use-zerologon-exploits-against-japanese-orgs/

Recent Publications

- 11/12/2020 **ACSC Alert: SDBBot Targeting Health Sector** https://www.cyber.gov.au/acsc/view-all-content/alerts/sdbbot-targeting-health-sector
- 11/19/2020 **CISA Insider Threat Mitigation Guide (TLP:WHITE)** https://www.cisa.gov/publication/insider-threat-mitigation-resources

Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community. For more information about TLP, see: https://www.us-cert.gov/tlp.