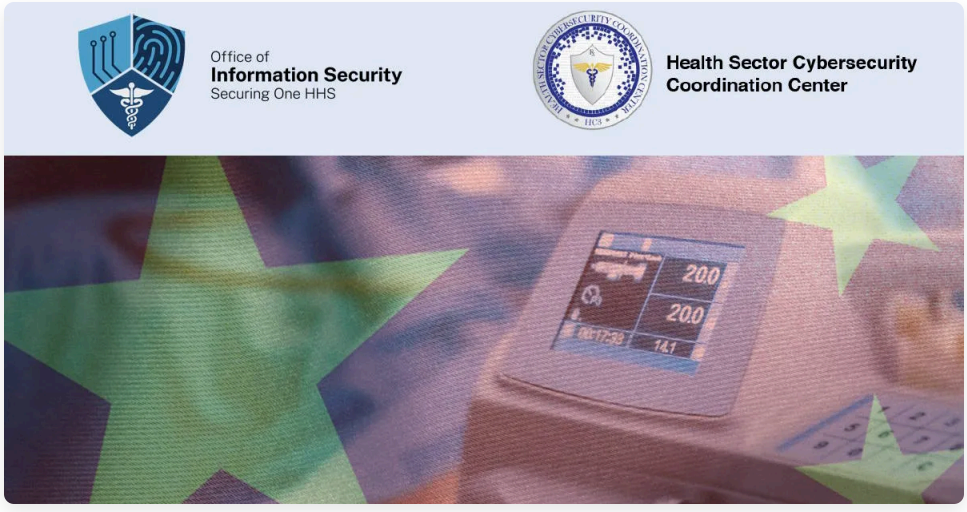
Attacks And Vulnerabilities Critical Infrastructure

Malware, Phishing & Ransomware Medical News Threat Landscape

Vulnerabilities

HC3 white paper cautions about Chinese-based hackers targeting US public, private health sector

AUGUST 18, 2023



The Health Sector Cybersecurity Coordination Center (HC3) in the U.S. Department of Health & Human Services (HHS) published a white paper that outlines Chinese cyber hackers who are known to

healthcare sector and should be treated with priority when designing and maintaining an appropriate risk posture for a health sector entity.

"Cybercriminals have proven to be formidable adversaries to the health sector in recent years, with digital extortion often in the form of ransomware, as well as data breaches being some of the most common criminal tactics being leveraged by these gangs," the HC3 white paper defined. "State-sponsored threat actors also pose a significant threat, with data exfiltration attacks for the purposes of intellectual property theft and espionage being the primary motivations behind foreign governments targeting the U.S. health sector in cyberspace."

The agency added that the hackers in this document consist of groups that have previously and are highly likely to continue to target U.S. healthcare organizations aggressively. "This very often involves stealing intellectual property related to medical technology and medicine, in order to operationalize it and bring it to market. It also involves national security and public health-related cyberattacks, such as the attempts to steal COVID-19 vaccine research in recent years. In the case of at least one threat actor, it can involve attacks for financial gain."

The first group listed in the HC3 white paper was APT41 which has a history of targeting the health sector. They are known to conduct state-sponsored espionage activities as well as digital extortion through their cyber operations. "APT41 is a hacking group believed to be based out of Chengdu, China and has an alleged association with China's Ministry of State Security. APT41 is also known as BARIUM, Winnti, LEAD, WICKED SPIDER, WICKED PANDA, Blackfly, Suckfly, Winnti Umbrella, and Double Dragon, among other labels," the document added.

"APT41 has directly targeted organizations in over a dozen countries, dating back to its earliest known operations in 2007. This includes both government and private organizations based in the U.S., the UK, China, Taiwan, Hong Kong, India, Thailand,

telecommunications, software, and the high-tech sector, media/news, retail, travel, hospitality, sports, education, logistics, finance, entertainment (especially video games), and digital currencies. They are also known to target state governments, which can include healthcare organizations."

The document added that much of their targeting has historically included theft of intellectual property, and generally has been observed to align with China's most recent five-year plan. "There are also indications that the group tracks individuals and conducts surveillance, although HC3 is unaware of these types of activities specifically being leveraged against the U.S. health sector to date."

The HC3 added that APT41 is "a group whose goals include cyber espionage and financial gain. They distinguish themselves by primarily engaging in financially-motivated cybercriminal activities, possibly without the knowledge of the state and ostensibly for the benefit of the individual members of the group. This combination of operational goals is the reason they are referred to by some as Double Dragon."

APT41 will exploit known vulnerabilities, HC3 added. "They demonstrated this when they targeted ProxyLogon vulnerabilities, as an example. They are known to be very aggressive when targeting such vulnerabilities. They reportedly began exploiting the Log4J vulnerabilities in December of 2021 within hours after they were disclosed to the public."

The document further identified that one of the subgroups that are believed to operate as part of APT41 is called Earth Longzhi. "They were first identified as being active in 2020, and were observed as using both public as well as custom malware."

The HC3 also highlighted the APT10 group, which is known to conduct cyberespionage and cyberwarfare activities, and has leveraged zero-day vulnerabilities as well as an array of public and custom tools. Much of their activities are believed to involve the collection of military and intelligence data in support of China's

Cloud Hopper. According to the U.S. Department of Justice, APT10 is a capability of the Tianjin State Security Bureau of China's Ministry of State Security.

"APT10's geographic targeting has been reported to cover six continents (particularly the United States, Japan, and various European countries) and includes industries such as healthcare, construction, telecommunications, government, engineering, and aerospace," according to the HC3 white paper.

APT10 relies heavily on traditional spearphishing and access to victims' networks through managed service providers (MSPs). They are known to be able and willing to establish and maintain a long dwell time. They also frequently leverage 'living-off-the-land' techniques, exploiting and utilizing capabilities already existing in a victim's environment, as well as DLL-side-loading and custom DLL loaders. Legitimate tools and malware known to be used by APT10 include certutil, adfind, csvde, ntdsutil, WMIExec, PowerShell, HAYMAKER AKA ChChes AKA Scorpion, SNUGRIDE, BUGJUICE AKA RedLeaves (overlap with PlugX), and QUASARRAT, also known asxRAT.

The HC3 white paper disclosed that very little is known about APT18 group, as they are believed to be affiliated with China's military and, despite limited public knowledge, appear to be as capable as any of China's other cyberwarfare capabilities. "They target a number of industries, including healthcare, and are capable of leveraging complex vulnerabilities and utilizing a wide array of malware," it added.

"APT18, also known as Wekby, TA-428, TG-0416, Scandium, and Dynamite Panda, is believed to be affiliated with the Chinese People's Liberation Navy," the document identified. "APT18 is known to target human rights groups, governments, and various sectors, including medical (especially pharmaceutical and biotechnology), aerospace, defense, construction, engineering, education, industrial, transportation, and information technology."

sophisticated malware, including Ghost RAT, HTTPBrowser, pis loader, and PoisonIvy. They frequently develop and adapt zero-day exploits for operations, and are believed to have exploited the OpenSSL heartbleed vulnerability in the previously-mentioned 2014 compromise of a healthcare provider."

Lastly, the HC3 white paper covers APT22 which has likely been operational since at least 2014, and often targets political entities (especially dissidents against the Chinese government) and the health sector. APT22 is also known as Barista, Group 46, and Suckfly, though it is unknown which area of the Chinese government they are affiliated with.

"APT22 is known to target information technology companies, healthcare companies (especially biomedical and pharmaceutical), and political, military, and economic targets in the United States, in Europe, and across East Asia," the white paper identified. "APT22 is known to leverage complex malware such as PISCES, SOGU (AKA PlugX), FLATNOTE, ANGRYBELL, BASELESS, SEAWOLF, and LOGJAM. They are known to use strategic webcom promises in order to passively exploit targets of interest, and identify vulnerable public-facing web servers on victim networks and uploaded web shells in order to gain access to the victim network."

Due to the nature of advanced persistent threats, including their high level of sophistication as well as their constant evolution of capabilities, it is challenging to attempt to compile a list of specific technical steps to defend against a single threat, much less a list of them such as is in this white paper.

Earlier this month, the HC3 alerted the healthcare sector of the presence of Rhysida, a new ransomware-as-a-service (RaaS) group that has emerged since May this year. The group drops eponymous ransomware via phishing attacks and Cobalt Strike to breach targets' networks and deploy their payloads while threatening to publicly distribute the exfiltrated data if the ransom is not paid. Also, the group then threatens victims in a ransom note

Anna Ribeiro

Industrial Cyber News Editor. Anna Ribeiro is a freelance journalist with over 14 years of experience in the areas of security, data storage, virtualization and IoT.

Features

Need to build robust industrial supply chain security while considering emerging technologies

As the industrial sector advances into 2025, industrial supply chain security is increasingly...

News

US lawmakers sound alarm on COSCO SHIPPING's national security risks, seek USCG briefing

JANUARY 27, 2025

Kristi Noem takes over as Secretary of Homeland Security, confirmed in sweeping bipartisan vote

JANUARY 27, 2025

SANS Institute launches SECWA to empower underrepresented communities with cybersecurity careers

JANUARY 24, 2025

Decision Point Summary: OT Network Perimeter Security and Compensating Controls (Takepoint Research)

Download

Application of Cyber-Informed Engineering for Protecting BESS (INL)

Download

Related

US lawmakers sound alarm on COSCO SHIPPING's national security risks, seek USCG briefing

Join the Industrial Cyber Community

Get the latest breaking OT/ICS news, access the resources and participate in our ICS Forum.

Register

Follow Us