COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 24, Number 6. June 27, 2024 Security Checklist: DDoS, Spear Phishing and Baxter Devices

By Jane Anderson

The HHS Health Sector Cybersecurity Coordination Center (HC3) is warning health care organizations that bad actors currently are targeting them specifically in three ways: distributed-denial-of-service (DDoS) attacks, business email compromise through spear phishing and via two Baxter International Inc. tools commonly used in facilities.

The spate of warnings came on the heels of another HC3 bulletin in April warning that hackers were employing advanced social engineering tactics to target IT help desks in the health sector and gain initial access to target organizations.[1] Together, the warnings indicate a threat atmosphere for the health care sector that shows no signs of abating.

BEC Growing Threat

Spear phishing involves targeting a specific individual in an organization to steal their login credentials. According to HC3's warning on business email compromise (BEC), spear phishing is a "next level" technique in which the attacker often gathers information about the person, such as their name, position and contact details, before starting the attack.[2]

BEC is a spear phishing attack that utilizes social engineering, HC3 said. "It is one of the most damaging and expensive types of phishing attacks in existence, costing businesses billions of dollars each year," the agency said.

"At a basic level, BEC is a type of cybercrime where the scammer uses email to trick someone into sending money or divulging confidential company info. The cybercriminal spoofs a person or organization the target knows, like a supplier, and asks for a fake invoice to be paid, sensitive company information, or other data they can profit from," HC3 said.

Instead of relying solely on technical vulnerabilities, the attacks "exploit the human tendency to trust authority, act impulsively, and respond emotionally to urgent requests," the agency said in its BEC briefing document.

Between October 2013 and December 2022, the FBI reported 277,918 BEC incidents domestically and internationally, with a total loss to businesses of more than $50 billion. In the U.S. during the same time period, the FBI reported 137,601 total victims and a total U.S.-based dollar loss of more than $17 billion.

Types of BEC scams include attorney impersonation, CEO fraud, data theft, account compromise and false invoice, and attackers often use more than one method as part of their attacks, HC3 said. For example, an attacker might pose as a lawyer or legal team member and pressure or manipulate the employee into sending data or requesting a wire transfer, the agency said.

"Since the request is typically framed as urgent, confidential or both, it typically takes advantage of the fact that low-level employees within an organization are likely to comply with requests from a lawyer or legal representative, because they do not know how to validate the request and simply comply to avoid negative

consequences," HC3 said.

Similarly, attackers often pose as someone with executive authority and target a member of the finance team, claiming to need urgent support on a time-sensitive or confidential matter that may not be verifiable with anyone else, potentially goading an employee into transferring funds or exposing data to the attacker, HC3 said.