
GETTY IMAGES

Malware Ties Up SUPPLY CHAINS

By **Victoria G. Myers, @myersPF**

Cyberattacks on U.S. businesses have risen markedly during the last year, but it's their potential to damage the world's supply chains that Federal Bureau of Investigation (FBI) agent Henry Heim says keeps him awake nights.

Heim spoke to attendees at the recent USDA Cybersecurity Expo. It addressed cybersecurity issues specific to the food and agriculture sectors. Presenters pointed to supply chains as being especially vulnerable.

"It's crucial [the supply chain] to the industry, but it's not necessarily controlled by the industry," Heim explains. "A threat actor can take a lot of time to go after a piece of software used throughout an industry and know it will pay big dividends, as they won't have a single victim but hundreds, even thousands of victims."

The food and ag sector continue to be vulnerable to ransomware attacks.

He notes that globally, the costs of cybercrime are projected to hit the $6-trillion mark this year, up from $3 trillion in 2015.

Secretary of Agriculture Tom Vilsack opened the Expo saying the USDA recognizes ransomware attacks are directly impacting lives and businesses on a daily basis. Ransomware is a type of malware that encrypts files on a device, making those files and the systems that rely on them unusable. A ransom is demanded in exchange for decryption.

"They [ransomware attacks] also compromise our economy and the security of our nation," Vilsack continues. In ransoms alone, he notes $350 million had been paid out in 2020 to cybercriminals, a 300% increase over 2019.

"Between June and September [2021], multiple ransomware attacks have been directly connected to the food and agriculture sectors," he points out. "We know these attacks disrupted our food supply chain, eroded some confidence folks may have had in the safety and security of our food sector, and resulted in significant resources being paid."

In response to these attacks and growing concerns, Vilsack announced the U.S. government has launched the website **stopransomware.gov**. This is a one-stop shop of best practices to protect against ransomware, with clear guidance on how to report attacks and a source of alerts from participating agencies.

WAYS TO SELF-PROTECT

Presenters at the Expo stressed the first line of protection against cyberattacks is the individual.

Matt Allen, with the Cybersecurity and Infrastructure Security Agency (CISA), says his group is the nation's risk adviser working to defend against threats and build a more resilient infrastructure. He explains common ways malware gets into systems include phishing, compromised websites, malvertising, downloads and messaging applications. Third-party vendors, managed service providers and infrastructure providers are common sources, as well.

The five most targeted critical infrastructure sectors today, Allen says, are government facilities, health care/public health, education facilities, information technology and critical manufacturing. Frequency of attacks rose dramatically between 2019 and 2020.

FBI's Heim points out there is no silver-bullet approach to solving the problem.

"It's the basics. You're just stopping malware. Two-factor authentication, passwords, backups, make sure your patch is up to date and most important is cybersecurity training," he says. "Your people are your greatest asset, but the weak link is the one they are going after. Over 90% of cyberattacks are the result of a phishing email."

Heim also encourages businesses to share information with each other when it comes to cybersecurity.

"Being a competitor is fine in the open marketplace. But, competitors, when it comes to cybersecurity, need to share with each other. It's either share with competitors or face the cybercriminals, that's what ➤

you're looking at."

Lastly, the agent says it's important to know, before a cyberattack takes place, your point of contact at the FBI.

"If you suffered a cyberattack, what's going to happen with the response? If the first time you're talking to the FBI point of contact is after a cyberattack or during it, you're already behind. Time is of the essence in every cyberattack to halt the attack, to prevent further loss, to recover. It's not a time for introductions," he stresses, noting that when the FBI does arrive on the scene, it will treat victims as victims.

"You're the victim. We're not going to take all your computers and walk out the door. We're not going to rope off the area. We will work with you to limit disruption to your business, and we will take whatever you allow us to take. We are just looking for that intrusion detail so we can identify who, in fact, was at the bottom of this and try to hold them accountable."

GETTY IMAGES

VICTIM SHARES LESSONS

CGB Enterprises works in the agricultural and transportation sectors. Greg Beck, senior vice president of the organization, shared his real-life story during the Expo about the effects of a cybercrime on CGB in 2020.

A mid-sized company, with about 2,500 employees, CGB was hit with a ransomware attack about 2 a.m. on June 2020. By 5 a.m., most of the business' truck scales were inoperable. By 7 a.m., a systemwide shutdown was implemented by CGB's Information Technology (IT). There was no way to dump trucks, print checks, etc.

"What we did not know was if we disconnected our PLCs [programmable logic controller], could we operate the basic functions of the grain elevator? Would our dust systems operate? Could we load barges? Could we load railcars? That was an unknown," Beck explains.

After shutting down all the computers, Beck says IT could still "see" someone looking at them. Turns out the criminals got in through an unused PC still connected underneath someone's desk.

Recovery was expensive and time-consuming. Beck says they ordered 344 new computers, and IT had to rebuild the operation's system scale by scale. Systems were restored using backups. There were no paper lists of customers, so there was no way to get in touch with anyone immediately. There also were no paper checks, no paper scale tickets.

CGB alerted state and federal licensing agencies in the event any payments were delayed. They hired legal counsel to see what data had been lost and, if so, whether it was of a sensitive nature. The company resorted to manual operations totally.

After nine weeks, Beck says they had an all-new protocol and were getting back to somewhat normal operations.

In hindsight, he wishes they had insisted employees who failed phishing tests had consequences tied to those failures. He cautioned that businesses today must be diligent on all IT phishing, spyware tests and training, and follow-up. He says they now perform continuous risk assessments, and they will never use old computers to operate scales, cameras, etc. They have also instituted training on how to perform all the company's processes manually.

Beck points out the company did have a plan before the cyberattack.

"We had an IT plan. We thought about this, we did phishing tests, and we thought we were OK," he says, adding that IT had wanted to add multifactor authentication, but company management balked.

"We felt it [multifactor authentication] takes too long. We thought IT was just being overzealous. They talked about the risk, and we were not as concerned as they were. I'm here today to say that executive management of other companies must take this extremely, extremely seriously." ///