Supply Chain Risks to the Vaccine Rollout

Perspective

MARCH 18, 2021

Key takeaways

Ransomware attacks against healthcare organizations, suppliers and distributors are likely to intensify and wreak havoc.

Healthcare organizations can increase security by evaluating identity and access practices around the millions of devices they deploy.

Leaders should update service level agreements with supply chain partners, even outside lawyers and

on uncertain times to undermine national security.

In March 2020, worried that notoriously underprotected healthcare institutions would soon face significant cyberattacks as the world braced for a global pandemic, Zaidenberg co-founded the CTI League, for cyberthreat intelligence. Think of it as a global defense force, a nonprofit using volunteer cybersecurity experts to thwart attacks on healthcare facilities.

"I created the CTI League to take part in this global war against the pandemic and to make sure that nobody would die because of a cyberattack during this sensitive time," says Zaidenberg. The league's co-founders also include security leaders Marc Rogers of Okta and Christopher Mills and Nate Warfield at Microsoft.

When COVID-19 first emerged, the idea that anyone would take advantage of such a dire situation to disrupt healthcare might have seemed unfathomable. Yet around the same time, cybercriminal gangs began extorting vaccine test facilities. A significant ransomware attack disrupted operations and delayed surgeries at Brno University Hospital in the Czech Republic, another major COVID-19 testing facility.

Since the pandemic began, the CTI League has helped numerous hospitals, pharmaceutical companies and suppliers cope with a spiraling security threat from malicious actors targeting the world's population when it is at its weakest. The league's message: Healthcare needs to batten down the hatches.

Ransomware rises

dangerously exposed. Separately, VMware Carbon Black researchers found 239.4 million attempted attacks targeting healthcare organizations in 2020, with an average of 816 attempts per endpoint, or a 9,851% jump from 2019.

Many attacks involved what's known as "island hopping," where bad guys build on an attack against one organization to launch secondary infections among other organizations, partners and patients.

The practice is similar to the way in which Russian spies are believed to have pulled off a massive supply chain hack of U.S. government systems in late 2019. Last year, operatives planted code in servers owned by SolarWinds, a major software contractor. That route is similar to a series of cyberattacks thought to have been the work of the North Korean government, which infiltrated companies and governments distributing Pfizer's coronavirus vaccine. Researchers from the Department of Homeland Security and IBM believe criminals were attempting to steal network log-in credentials from executives and officials connected to the "cold chain" refrigeration storage process for the Pfizer vaccine, which must be kept at a minimum of minus 76 degrees Fahrenheit until shortly before inoculation.

9,851%

Increase in attempted attacks per endpoint targeting healthcare from 2019 to 2020

Attacks go crazy

endpoint devices by tens of thousands of users. All those digital instances represent potential targets — opportunities to disrupt the administration of vaccines and other much-needed treatments."

Moring says attacks against healthcare organizations, suppliers and distributors are likely to intensify and wreak havoc. For example, hackers could potentially reduce the number of vaccine doses that a healthcare provider receives from a pharmaceutical company, say from 1 million to 100, forcing facilities to turn away patients. Hackers could also alter appointment counts to show nobody arriving when, in fact, hundreds are expecting to see doctors or nurses. Or hackers could instruct delivery drivers to transport goods to out-of-the-way locations in hopes that the temperature-sensitive vaccines will spoil.

[Read also: Supply chain security: What should good look like?]

Experts say gangs of cyberthieves looking to seize and sell confidential patient data on the dark web are behind many attacks. As providers rush to get vaccines into as many arms as possible, hackers are luring unsuspecting medical employees and patients into clicking on links and attachments in seemingly innocent phishing emails that launch TrickBot and ransomware like Ryuk to infect organizations.

The threat became so pervasive late last year that the Cybersecurity and Infrastructure Security Agency (CISA), the Department of Health and Human Services (HHS), and the FBI delivered a strongly worded warning about "an increased and

whenever there's a rush, as with getting vaccines out during the pandemic, they know human beings will make mistakes."

Securing endpoints

Dr. Russell Handorf, a former FBI computer scientist and principal threat intelligence hacker at White Ops, says the logical way for healthcare organizations to increase security would be to evaluate identity and access practices around the millions of endpoint devices they currently deploy.

"It all starts with the endpoint, because that is the storefront to network access," he says. "You can have firewalls and other security systems spread evenly around your network to build castle walls. But your endpoints are still portals that everyone goes through to get into the castle."

Endpoints are still the portals that everyone goes through to get into the castle.

Dr. Russell Handorf, former FBI computer scientist and principal threat intelligence hacker at White Ops

unauthorized requests.

"If I were to be scared of anything right now in healthcare, it would be the risk around the delivery of vaccines and other medications using these endpoints," Handorf says. "I am confident pharmaceutical companies are taking the right measures to create, ship and track their products. But all it takes is one person to accidentally plug in an insecure laptop for that last mile of delivery to go sideways."

Practicing security hygiene

Endpoint devices are the soft underbelly of healthcare security. Experts say organizations must have visibility across an integrated IT infrastructure. Good IT security hygiene practices include running behavioral anomaly detection and prevention programs, conducting regular cyberthreat hunting exercises to find compromised systems, and enforcing multifactor authentication that can head off most, if not all, phishing attempts.

Leaders should also update service level agreements (SLAs) with partner organizations, setting levels of information security, notification, and response processes when incidents occur, and then defining the consequences of noncompliance. These SLAs should not only apply to the traditional supply chain but also to the often forgotten information supply chain, including outside lawyers, marketing firms and other vendors that hackers often target.

also doing the right things.

"It's not enough to push out the highest possible security requirements you can think of if you're not following them yourself," he says. "If you're not, you are the weak link in the chain. You first have to secure your own house. And then you can start looking at suppliers in order to bring them up to your level."

David Rand

David Rand is a business and technology reporter whose work has appeared in major publications around the world. He specializes in spotting and digging into what's coming next – and helping executives in organizations of all sizes know what to do about it.

Focal Point

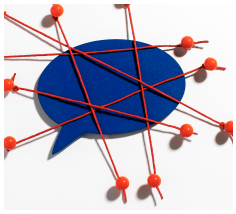
Dedicated to helping business executives and IT leaders effectively use technology to connect with customers, empower employees and achieve better results.

Tanium Subscription Center

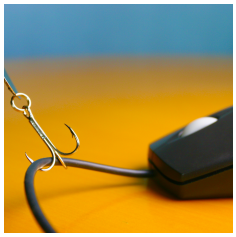
Get Tanium digests straight to your inbox, including the latest thought leadership, industry news and best practices for IT security and operations.

SUBSCRIBE NOW

Related



Misinformation / Disinformation, Part 1 – The Coming Crisis and Enterprises Most at Risk



What Is Phishing?

Leading the paradigm shift in legacy approaches to managing complex security and IT environments

CONTACT US

About Tanium

Careers

Leadership

Newsroom

Events

Converged Endpoint Management

Platform

XEM Core

Endpoint Management

TANIUM

IT OPERATIONS RISK & SECURITY THREAT INTELLIGENCE BUSINESS TRANSFORMATION

Focal Point Magazine

Tanium Blog

Let's Converge Podcast

Community

Resource Center

Training

Certifications

Partner Learning Hub

Customers

Success Stories

Partners

Partner Finder

Become a Partner

Legal

Privacy Policy

Terms of Use

CCPA Notice of Collection

Do Not Sell or Share My Personal Information

English