TechTips Newsletter

tech hero

Insider Tips To Make Your Business Run Faster, Easier And More Profitably

Solarwinds Orion Breach Prompts Emergency Directive From CISA

The SolarWinds code compromise cybersecurity incident has become one of the biggest stories as the year comes to an end. In short, SolarWinds Orion products were actively exploited by malicious actors. The breach occurred as a result of a supply-chain attack that tampered with software updates via rootkits and other means.

As many United States government agencies use SolarWinds Orion products, the Cybersecurity and Infrastructure Security Agency (a division of the Department of Homeland Security) has issued an emergency directive on the SolarWinds Orion breach.

Continued on next page...

January 2021

This monthly publication provided courtesy of Richard Lynn, VP of Sales and Marketing Tech Hero

Our Mission

To build a community of successful minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.

Emergency Directive 21-01 was released on Dec. 13, 2020, to reduce the compromise of government agencies. The emergency directive is a result of Section 3553(h) of title 44, U.S. Code, which gives the DHS direct power to take drastic actions "*in response to a known or reasonably suspected information security threat.*" CISA's Emergency Directive 21-01 enforces a number of immediately effective restrictions, including the following:

"*Forensically image system memory and/or host operating systems hosting all instances of SolarWinds Orion versions 2019.4 through 2020.2.1 HF1]. Analyze for new user or service accounts, privileged or otherwise... Analyze stored network traffic for indications of compromise, including new external DNS domains to which a small number of agency hosts (e.g., SolarWinds systems) have had connections... Affected agencies shall immediately disconnect or power down SolarWinds Orion products, versions 2019.4 through 2020.2.1 HF1, from their network. Until such time as CISA directs affected entities to rebuild the Windows operating system and reinstall the SolarWinds software package, agencies are prohibited from (re) joining the Windows host OS to the enterprise domain.*"

The directive also requires agencies to assume any host handling SolarWinds Orion products as compromised. Even further, it requires a total credential reset so that malicious actors do not have access. CISA plans on enforcing Emergency Directive 21-01 until one of two circumstances come to pass. The first is that all affected software is patched and determined to be secure. In the second scenario, CISA can cancel the emergency directive through a rather vague "other appropriate action."

Not surprisingly, the SolarWinds Orion breach incident is a rapidly developing story. We will be keeping an eye on any major developments. —*Derek Kortepeter for Techgenix*

tech hero

Cloud Portal

Did you know about our new Cloud Portal? This new tool will allow you to open tickets directly with us here at Tech Hero at the click of a button!

To try it out, just go down to your system tray and look for the small blue IT icon. After you've double clicked on it you will need to sign in (You will only need to do this once!)

Once you are in you can click around explore the software.

If you have any questions, feel free to reach out to us at the number below!

(800) 900-TECH x2

vmware PARTNER

PROFESSIONAL SOLUTION PROVIDER

Free Consultation to review your VMware Licensing!

Contact your Tech Hero sales representative to schedule a FREE review of your VMware licensing.

Find out ways to save money, ways to receive free upgrades, and a better understanding on the VMware license models.

tech hero

1-(800) 900-TECH (option 2)

Sales@TechHero.com

Healthcare.gov breach results in prison time for hacker

The hacker who breached healthcare.gov is now in prison. According to an official press release from the Department of Justice (Eastern District of Louisiana), Colbi Trent Defiore, a 27-year-old resident of Carriere, Miss., has been given the sentence of "42 months imprisonment, 3 years of supervised release and payment of a $100 special assessment fee." The sentence was handed down by United States District Judge Jay A. Zainey and follows a previous guilty plea from Defiore for violating computer access laws as they are stated in 18 U.S.C. ' 1030(a)(2)(C).

In 2018, Colbi Trent Defiore illegally accessed private data on the healthcare.gov website, a site primarily used for U.S. citizens who receive medical coverage under the Affordable Care Act (aka Obamacare). Defiore was able to gain access by leveraging his position as a seasonal employee at Centers for Medicare & Medicaid Services (CMS), namely in the Louisiana city of Bogalusa, to illegally access and steal personal data from the healthcare.gov database. In total, Defiore was able to access personal data of over 8,000 individuals in the database.

Continued on next page...

The following excerpt from the DOJ press release details Defiore's exact attack methodology of the healthcare.gov breach, usage of data, and damage caused:

"*DEFIORE conducted "bulk searches" of the database... DEFIORE then copied the results of his searches onto a virtual clipboard and sent them to himself via email. After work hours, DEFIORE accessed Company A's network remotely without authorization to retrieve his work email. DEFIORE used the personal information of at least five consumers to apply fraudulently for at least six credit cards, loans, and lines of credit for his personal benefit. In total, DEFIORE'S conduct caused reasonably foreseeable loss to the companies that operated the call center, including costs associated with responding to the offense, conducting a damage assessment, responding to and remediating damage, contacting consumers who were potential victims, and providing theft protection services for consumer-victims, in the amount of $587,000.*"

According to the DOJ of Lousiana's Eastern District, the FBI was largely responsible for the investigation that led to Defiore's apprehension. Assistant United States Attorney Jordan Ginsberg was the leading prosecutor on the case.

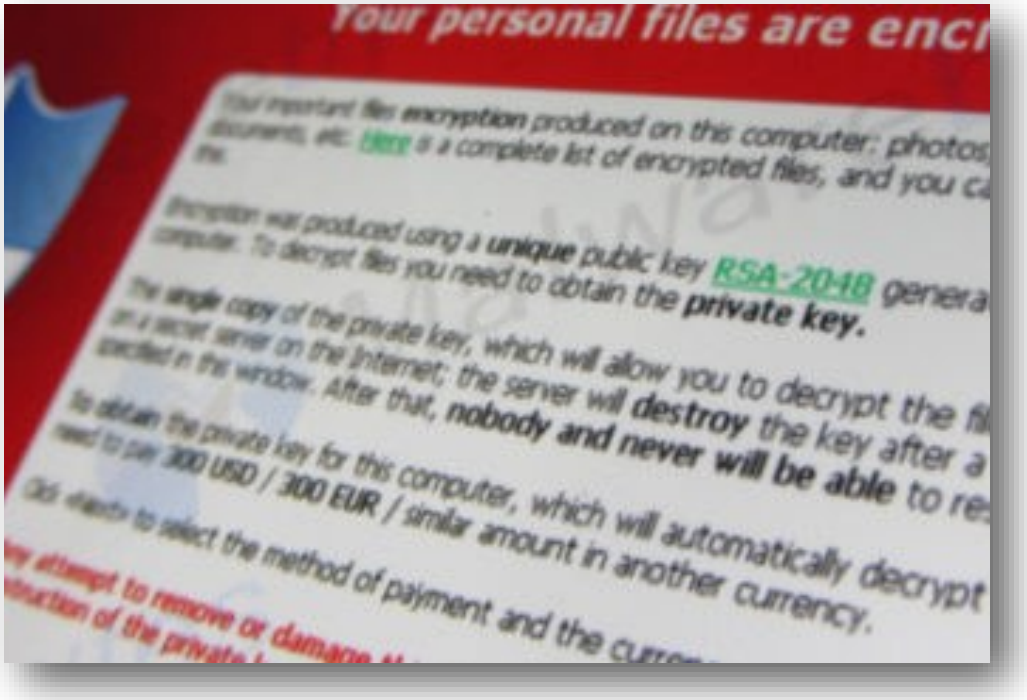
With government agencies and municipalities being targeted more and more by cybercriminals, this sentence will, hopefully, send a message to any would-be hackers.

—*Derek Kortepeter for Techgenix*

Client Spotlight

Since establishing in 1985, South Australian owned Antelco has leapt ahead with its continuing focus on providing high quality, low volume, micro irrigation products to meet the global need for efficient water distribution.

To keep up with growing demand, Antelco Corporation was established in 1989 in Florida USA and serves the North American, Canadian and Mexican markets.



Microsoft, Citrix, other heavyweights form massive ransomware task force

Ransomware is a persistent threat that eclipses all other cybercrime attacks. It can cripple businesses, hospitals, and entire city infrastructures. The lucrative nature of ransomware, with payouts totaling in the billions, means that cybercriminals will likely use the attack for as long as they can get a payday. Considering the vast number of ransomware attacks in just 2020 alone, it is clear that this is an issue that will plague cybersecurity for years to come.

The Institute for Security and Technology (IST) has recognized this threat, and as of Dec. 21, created a task force to mount a massive effort against ransomware.

Continued on next page...

According to a press release from the IST, the following organizations have formed a large task force with the explicit goal of fighting ransomware:

Aspen Digital

Citrix

The Cyber Threat Alliance

Cybereason

The CyberPeace Institute

The Cybersecurity Coalition

The Global Cyber Alliance

McAfee

Microsoft

Rapid7

Resilience

SecurityScorecard

Shadowserver Foundation

Stratigos Security

Team Cymru

Third Way

UT Austin Stauss Center

This coalition of companies includes heavyweights in software development, cybersecurity research, and malware defense. The stated goal of the IST ransomware task force is to create concrete defensive solutions over the course of two to three months. The official start of the IST task force's work will commence this month, at least according to the press release. The actual work that the task force will engage in is lined out in the following press release excerpt:

The RTF will assess existing solutions at varying levels of the ransomware kill chain, identify gaps in solution application, and create a roadmap of concrete objectives and actionable milestones for high-level decision-makers. To contribute to the final roadmap, the RTF will commission expert papers and engage stakeholders across industries to coalesce around vetted solutions.

The IST ransomware task force is an exciting development in the fight against ransomware. Their progress will be followed and reported on should any breakthroughs occur.

—*Derek Kortepeter for Techgenix*