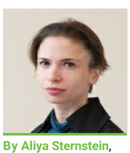
Third-Party Software Was Entry Point for Background-Check System Hack

WK1003MIKE/SHUTTERSTOCK.COM

MAY 10, 2015



By Aliya Sternstein, Senior Correspondent

Intruders piggybacked on a vulnerability in an enterprise resource planning application.

Hackers broke into third-party software in 2013 to open personal records on federal employees and contractors with access to classified intelligence, according to the government's largest private employee investigation provider.

That software apparently was an SAP enterprise resource planning application. It's unclear if there was a fix available for the program flaw at the time of the attack. It's also not clear whether SAP—which was responsible for maintaining the application—or USIS would have been responsible for patching the flaw.

But in the end, sensitive details on tens of thousands of national security personnel were exposed in March 2014.

Assailants infiltrated USIS by piggybacking on an "exploit," a glitch that can be abused by hackers, that was "present in a widely used and highly-regarded enterprise resource planning ('ERP') software package," an internal investigation obtained by *Nextgov* found.

USIS officials declined to explicitly name the software application, saying they would let the report, compiled by Stroz Friedberg, a digital forensics firm retained by USIS, speak for itself.

The report, written in December 2014, noted: "Forensic evidence shows the cyberattacker gained access to USIS systems through an exploit in a system managed by a third party, and from there migrated to company managed systems. . . . Our findings were largely informed by a variety of logs, including, firewall logs, security event logs, VPN logs, and SAP application trace logs."

A September 2014 letter from Stroz reported, "The initial attack vector was a vulnerability in an application server, housed in a connected, but separate network, managed by a third party not affiliated with USIS." The reference to "SAP application trace logs" in the report indicates the third party was SAP.

During the period of the hacking operation, which began in 2013 and was exposed in June 2014, 20 to 30 new critical vulnerabilities were identified in SAP's enterprise resource planning software.

The number of SAP vulnerabilities "would have given attackers many options to target SAP directly," based on how USIS deployed the ERP tool, said Richard Barger, chief intelligence officer at ThreatConnect, a firm that tracks cyber threats. Barger is a former Army intelligence analyst.

It is unclear which vulnerability the intruders exploited. Defects in programs used by the government and contractors sometimes aren't fixed for years after software developers announce a weakness.

Referencing the Stroz report, USIS spokeswoman Ellen Davis said, "the third-party contractor was hacked and the hacker was then able to navigate into the USIS network via the third party's network."

Stroz officials deferred comment to USIS.

SAP, a major IT contractor with 50,000 customer organizations worldwide, would neither confirm nor deny allegations that assailants reached USIS through one of its systems. SAP spokesman Mat Small said in an email, "Since we don't comment on the specifics of any customer engagement without their explicit consent, SAP is unable to make a statement on the situation."

Addressing SAP's response to security vulnerabilities, he added, "No company is more committed to data privacy and security than SAP, and we respond rapidly, vigorously and thoroughly when potential security risks are identified."

The targeting of middlemen and downstream suppliers has become common in sophisticated hacking campaigns, according to researchers.

The top three sectors victimized by cyber espionage last year were professional services firms, which typically support large organizations; manufacturing; and government, according to an annual Verizon data breach investigations study released last month.

Computer snoops have learned it is easier to compromise "the partner and the third party dealing with that intellectual property than the source of the intellectual property itself," Jay Jacobs, a Verizon senior analyst and study co-author, said at the time of the study's publication.

And PWC's most recent State of Cybercrime Survey found that only 22 percent of U.S. organizations plan incident response strategies with outside suppliers.

"Not all companies recognize that supply chain vendors and business partners . . . can have lower—even nonexistent—cybersecurity policies and practices, a situation that can increase cybercrime risks across any entity that partner or supplier touches," according to the survey, which came out a year ago.

(*Image via* wk1003mike/ *Shutterstock.com*)

Share This:

NEXT STORY: Healthy Living Natural Foods Store Probing Possible Payment System Hack

Healthy Living Natural Foods Store Probing Possible Payment System Hack

MAY 8, 2015

Food and Beverage // United States

THREATWATCH

The Vermont-based grocery market on May 8 notified customers of a potential security breach after some customers found unauthorized charges to their credit cards late last year.

Healthy Living Vice President Eli Lesser-Goldsmith said the business learned of the incident on March 25.

"At this point," Healthy Living doesn't believe its IT systems were the source of the breach, he said.

"Because we have not yet been able to confirm that there was a data security breach, we have not yet determined what remedial steps will need to be taken, if any, to prevent future breaches," Lesser-Goldsmith said. "We recommend that customers closely monitor their account statements for unauthorized charges."

Original Report:
www.burlingtonfreepress.com/story/money/2015/05/08/healthy-living-possibly-ta...

Share This:

NEXT STORY: Hackers Rig Ratings of Pro-Putin Videos and Spy on Iranian Expat Living in the US

Researchers At Oak Ridge National Lab Tap Into Supercomputing To Help Combat Coronavirus

EXCLUSIVE: Pentagon To Take Corrective Action On JEDI

NIH Uses Urgent Award Vehicle For The First Time To Address Coronavirus Outbreak

Former DHS Acting Inspector General Indicted For Stealing Database With Personnel Information

You Might Be Buying A Hand Sanitizer That Won't Work For Coronavirus

SECURING THE GOVERNMENT CLOUD Download The Special Report

Nextgov Special Report: Securing The Government Cloud

Hackers Rig Ratings of Pro-Putin Videos and Spy on Iranian Expat Living in the US

Russian President Vladimir Putin attends a forum of independent regional and local mass media in St. Petersburg, Russia. ALEXEI DRUZHININ/AP FILE PHOTO

MAY 8, 2015

By Aliya Sternstein, Senior Correspondent

Just another week in ThreatWatch, our regularly updated index of noteworthy data breaches.

In case you missed our coverage this week in ThreatWatch, *Nextgov's* regularly updated index of cyber breaches:

Canadian Woman Allegedly Harassed Kids through Hacked Webcams, Showed Victims 'Extreme Porn'

Valérie Gignac, of Quebec, apparently took control of people's computers remotely, to peer at and bully them. The 27-year-old is believed to have created a botnet -- or infected a series of computers with malware that turns them into zombie machines, commanding them to perform tasks without the owner's knowledge.

Hackers Launch Campaign of Intimidation against Iranian Expat Writer

The opinionated Iranian author Roya Hakakian, who has spent 30 years living in the United States, was subjected to cyber espionage starting last February. "The common bond among all Hakakian's outspoken work for the past decade is that she wrote it in English," the Daily Beast reports. Once Hakakian's work was published in Farsi, "she seems to have tripped a wire that alerted the Iranian cyber hounds."

Web Scrape of Buried Twitter Financials Technically Amounts to a Hack

Financial-intelligence firm Selerity took credit for publishing Twitter's earnings announcement before NASDAQ's closing bell. Web-crawling bots run by Selerity uncovered the financial report -- an abysmal $162 million first-quarter loss -- buried deep in Twitter's public investor relations page.

Hackers Manipulated Ratings of Pro-Russian Videos

Hacktivists and/or cybercrooks compromised the computers of victims to invisibly load propaganda videos and ads, upping click-views, and thus the popularity, of party line promos and commercial products.

Share This:

NEXT STORY: Canadian Woman Allegedly Harassed Kids through Hacked Webcams, Showed Victims 'Extreme Porn'

Most Popular

1 Why Singapore's Coronavirus Response Worked—and What We Can All Learn

2 Senators Call on Agencies to Post Contingency Plans for Public

3 Government's Maximum Telework Policy Overlooks Contractors

Get the latest federal technology news delivered to your inbox.

Featured eBooks

SECURING THE GOVERNMENT CLOUD

THE SUITE LIFE

Emerging Technology Trends

Recommended For You

CBP Intercepts First Package of Counterfeit COVID-19 Test Kits

Senators Call on Agencies to Post Contingency Plans for Public

Regulators Say Maritime Industry's Pandemic Plans Can Skip Cybersecurity Details

Researchers At Oak Ridge National Lab Tap Into Supercomputing To Help Combat Coronavirus

EXCLUSIVE: Pentagon To Take Corrective Action On JEDI

NIH Uses Urgent Award Vehicle For The First Time To Address Coronavirus Outbreak

Former DHS Acting Inspector General Indicted For Stealing Database With Personnel Information

You Might Be Buying A Hand Sanitizer That Won't Work For Coronavirus

SECURING THE GOVERNMENT CLOUD Download The Special Report

Nextgov Special Report: Securing The Government Cloud