Use of articles

adapted by D.Potter - 20180127

practice based on an internet press release
Complete the text with either a zero article (-), a definite or an indefinite article

INSIGHT-Tech firms let Russia probe software widely used by U.S. government

https://ru.reuters.com/article/americasRegulatoryNes/idUKL2N1PK290?symbol=SAP

By Dustin Volz, Joel Schectman and Jack Stubbs

WASHINGTON/MOSCOW, Jan 25 (Reuters) - Major global technology providers SAP, Symantec and McAfee have allowed Russian authorities to hunt for vulnerabilities in software deeply embedded across [ ] U.S. government, [ ] Reuters investigation has found.

[ ] practice potentially jeopardizes [ ] security of computer networks in at least [ ] dozen federal agencies, U.S. lawmakers and security experts said. It involves more companies and [ ] broader swath of [ ] government than previously reported. In order to sell in [ ] Russian market, [ ] tech companies let [ ] Russian defense agency scour [ ] inner workings, or source code, of some of their products. Russian authorities say [ ] reviews are necessary to detect flaws that could be exploited by hackers. (Graphic: tmsnrt.rs/2sZudWT)

But those same products protect some of [ ] most sensitive areas of [ ] U.S government, including [ ] Pentagon, NASA, [ ] State Department, [ ] FBI and [ ] intelligence community, against hacking by sophisticated cyber adversaries like Russia.

Reuters revealed in October that Hewlett Packard Enterprise software known as ArcSight, used to help secure [ ] Pentagon’s computers, had been reviewed by [ ] Russian military contractor with close ties to Russia’s security services.

Now, [ ] Reuters review of hundreds of U.S. federal procurement documents and Russian regulatory records shows that [ ] potential risks to [ ] U.S. government from Russian source code reviews are more widespread.

Beyond [ ] Pentagon, ArcSight is used in at least seven other agencies, including [ ] Office of [ ] Director of National Intelligence and [ ] State Department's intelligence unit, [ ] review showed. Additionally, products made by SAP, Symantec and McAfee and reviewed by Russian authorities are used in at least eight agencies. Some agencies use more than one of [ ] four products. (Graphic: tmsnrt.rs/2C30rp8)

McAfee, SAP, Symantec and Micro Focus, [ ] British firm that now owns ArcSight, all said that any source code reviews were conducted under [ ] software maker’s supervision in secure facilities where [ ] code could not be removed or altered. [ ] process does not compromise product security, they said. Amid growing concerns over [ ] process, Symantec and McAfee no longer allow such reviews and Micro Focus moved to sharply restrict them late last year.

[ ] Pentagon said in [ ] previously unreported letter (tmsnrt.rs/2C6o2p2) to Democratic Senator Jeanne Shaheen that source code reviews by Russia and China “may aid such countries in discovering vulnerabilities in those products."

Reuters has not found any instances where [ ] source code review played [ ] role in [ ] cyberattack, and some security experts say hackers are more likely to find other ways to infiltrate network systems.

But [ ] Pentagon is not alone in expressing concern. Private sector cyber experts, former U.S. security officials and some U.S. tech companies told Reuters that allowing Russia to review [ ] source code may expose unknown vulnerabilities that could be used to undermine U.S. network defenses.

“Even letting people look at source code for [ ] minute is incredibly dangerous,” said Steve Quane, executive vice president for network defense at Trend Micro, which sells TippingPoint security software to [ ] U.S. military.

Worried about those risks to [ ] U.S. government, Trend Micro has refused to allow [ ] Russians to conduct [ ] source code review of TippingPoint, Quane said.

Quane said top security researchers can quickly spot exploitable vulnerabilities just by examining source code.

“We know there are people who can do that, because we have people like that who work for us,” he said.

In contrast to Russia, [ ] U.S. government seldom requests source code reviews when buying commercially available software products, U.S. trade attorneys and security experts say.

OPENING THE DOOR

Many of [ ] Russian reviews have occurred since 2014, when U.S.-Russia relations plunged to new lows following Moscow’s annexation of Crimea. Western nations have accused Russia of sharply escalating its use of cyber attacks during that time, [ ] allegation Moscow denies.

Some U.S. lawmakers worry source code reviews could be yet another entry point for Moscow to wage cyberattacks.

“I fear that access to our security infrastructure - whether it be overt or covert - by adversaries may have already opened [ ] door to harmful security vulnerabilities,” Shaheen told Reuters.

In its Dec. 7 letter to Shaheen, [ ] Pentagon said it was “exploring [ ] feasibility” of requiring vendors to disclose when they have allowed foreign governments to access source code. Shaheen had questioned [ ] Pentagon about [ ] practice following [ ] Reuters report on ArcSight, which also prompted Micro Focus to say it would restrict government source code reviews in [ ] future. HPE said none of its current products have undergone Russian source code review.

Lamar Smith, [ ] Republican chairman of [ ] House Science, Space and Technology Committee, said legislation to better secure [ ] federal cybersecurity supply chain was clearly needed.

Responding to [ ] Reuters report on Thursday, Democratic Congressman Jim Langevin, [ ] senior member of [ ] House Armed Services Committee, said [ ] Pentagon must consider “any access adversaries may have to source code when it is making purchasing decisions.”

Most U.S. government agencies declined to comment when asked whether they were aware technology installed within their networks had been inspected by Russian military contractors. Others said security was of paramount concern but that they could not comment on [ ] use of specific software.

[ ] Pentagon spokeswoman said it continually monitors [ ] commercial technology

it uses for security weaknesses.

NO PENCILS ALLOWED

Tech companies wanting to access Russia's large market are often required to seek certification for their products from Russian agencies, including [ ] FSB security service and Russia's Federal Service for Technical and Export Control (FSTEC), [ ] defense agency tasked with countering cyber espionage.

FSTEC declined to comment and [ ] FSB did not respond to requests for comment. [ ] Kremlin referred all questions to [ ] FSB and FSTEC.

FSTEC often requires companies to permit [ ] Russian government contractor to test [ ] software's source code.

SAP HANA, [ ] database system, underwent [ ] source code review in order to obtain certification in 2016, according to Russian regulatory records. [ ] software stores and analyzes information for [ ] State Department, Internal Revenue Service, NAS [ ] and [ ] Army.

[ ] SAP spokeswoman said any source code reviews were conducted in [ ] secure, company-supervised facility where recording devices or even pencils are "are strictly forbidden."

"All governments and governmental organizations are treated [ ] same with no exceptions," [ ] spokeswoman said.

While some companies have since stopped allowing Russia to review source code in their products, [ ] same products often remain embedded in [ ] U.S. government, which can take decades to upgrade technology.

Security concerns caused Symantec to halt all government source code reviews in 2016, [ ] company's chief executive told Reuters in October. But Symantec Endpoint Protection antivirus software, which was reviewed by Russia in 2012, remains in use by [ ] Pentagon, [ ] FBI, and [ ] Social Security Administration, among other agencies, according to federal contracting records reviewed by Reuters.

In [ ] statement, [ ] Symantec spokeswoman said [ ] newest version of Endpoint Protection, released in late 2016, never underwent [ ] source code review and that [ ] earlier version has received numerous updates since being tested by Russia. [ ] California-based company said it had no reason to believe earlier reviews had compromised product security. Symantec continued to sell [ ] older version through 2017 and will provide updates through 2019.

McAfee also announced last year that it would no longer allow government-mandated source code reviews.

[ ] cyber firm's Security Information and Event Management (SIEM) software was reviewed in 2015 by [ ] Moscow-based government contractor, Echelon, on behalf of FSTEC, according to Russian regulatory documents. McAfee confirmed this.

[ ] Treasury Department and Defense Security Service, [ ] Pentagon agency tasked with guarding [ ] military's classified information, continue to rely on [ ] product to protect their networks, contracting records show.

McAfee declined to comment, citing customer confidentiality agreements, but it has previously said [ ] Russian reviews are conducted at company-owned premises in [ ] United States.

‘YOU CAN‘T TRUST ANYONE’

On its website, Echelon describes itself as [ ] official laboratory of [ ] FSB, FSTEC, and Russia’s defense ministry. Alexey Markov, [ ] president of Echelon, which also inspected [ ] source code for ArcSight, said U.S. companies often initially expressed concerns about [ ] certification process.

“Did they have any? Absolutely!!” Markov wrote in [ ] email.

” [ ] less [ ] person making [ ] decision understands about programming, [ ] more paranoia they have. However, in [ ] process of clarifying [ ] details of performing [ ] certification procedure, [ ] dangers and risks are smoothed out.”

Markov said his team always informs tech companies before handing over any discovered vulnerabilities to Russian authorities, allowing [ ] firms to fix [ ] detected flaw. [ ] source code reviews of products “significantly improves their safety,” he said.

Chris Inglis, [ ] former deputy director of [ ] National Security Agency, [ ] United States’ premier electronic spy agency, disagrees.

“When you’re sitting at [ ] table with card sharks, you can’t trust anyone,” he said. “I wouldn’t show anybody [ ] code.”

Reporting by Dustin Volz and Joel Schectman in Washington and Jack Stubbs in Moscow.; Editing by Jonathan Weber and Ross Colvin

-- original text --

INSIGHT-Tech firms let Russia probe software widely used by U.S. government

https://ru.reuters.com/article/americasRegulatoryNes/idUKL2N1PK290?symbol=SAP

By Dustin Volz, Joel Schectman and Jack Stubbs

WASHINGTON/MOSCOW, Jan 25 (Reuters) - Major global technology providers SAP, Symantec and McAfee have allowed Russian authorities to hunt for vulnerabilities in software deeply embedded across the U.S. government, a Reuters investigation has found.

The practice potentially jeopardizes the security of computer networks in at least a dozen federal agencies, U.S. lawmakers and security experts said. It involves more companies and a broader swath of the government than previously reported. In order to sell in the Russian market, the tech companies let a Russian defense agency scour the inner workings, or source code, of some of their products. Russian authorities say the reviews are necessary to detect flaws that could be exploited by hackers. (Graphic: tmsnrt.rs/2sZudWT)

But those same products protect some of the most sensitive areas of the U.S government, including the Pentagon, NASA, the State Department, the FBI and the intelligence community, against hacking by sophisticated cyber adversaries like Russia.

Reuters revealed in October that Hewlett Packard Enterprise software known as ArcSight, used to help secure the Pentagon’s computers, had been reviewed by a Russian military contractor with close ties to Russia’s security services.

Now, a Reuters review of hundreds of U.S. federal procurement documents and Russian regulatory records shows that the potential risks to the U.S. government from Russian source code reviews are more widespread.

Beyond the Pentagon, ArcSight is used in at least seven other agencies, including the Office of the Director of National Intelligence and the State Department's intelligence unit, the review showed. Additionally, products made by SAP, Symantec and McAfee and reviewed by Russian authorities are used in at least eight agencies. Some agencies use more than one of the four products. (Graphic: tmsnrt.rs/2C30rp8)

McAfee, SAP, Symantec and Micro Focus, the British firm that now owns ArcSight, all said that any source code reviews were conducted under the software maker’s supervision in secure facilities where the code could not be removed or altered. The process does not compromise product security, they said. Amid growing concerns over the process, Symantec and McAfee no longer allow such reviews and Micro Focus moved to sharply restrict them late last year.

The Pentagon said in a previously unreported letter (tmsnrt.rs/2C6o2p2) to Democratic Senator Jeanne Shaheen that source code reviews by Russia and China “may aid such countries in discovering vulnerabilities in those products."

Reuters has not found any instances where a source code review played a role in a cyberattack, and some security experts say hackers are more likely to find other ways to infiltrate network systems.

But the Pentagon is not alone in expressing concern. Private sector cyber experts, former U.S. security officials and some U.S. tech companies told Reuters that allowing Russia to review the source code may expose unknown

vulnerabilities that could be used to undermine U.S. network defenses.

“Even letting people look at source code for a minute is incredibly dangerous,” said Steve Quane, executive vice president for network defense at Trend Micro, which sells TippingPoint security software to the U.S. military.

Worried about those risks to the U.S. government, Trend Micro has refused to allow the Russians to conduct a source code review of TippingPoint, Quane said.

Quane said top security researchers can quickly spot exploitable vulnerabilities just by examining source code.

“We know there are people who can do that, because we have people like that who work for us,” he said.

In contrast to Russia, the U.S. government seldom requests source code reviews when buying commercially available software products, U.S. trade attorneys and security experts say.

OPENING THE DOOR

Many of the Russian reviews have occurred since 2014, when U.S.-Russia relations plunged to new lows following Moscow’s annexation of Crimea. Western nations have accused Russia of sharply escalating its use of cyber attacks during that time, an allegation Moscow denies.

Some U.S. lawmakers worry source code reviews could be yet another entry point for Moscow to wage cyberattacks.

“I fear that access to our security infrastructure - whether it be overt or covert - by adversaries may have already opened the door to harmful security vulnerabilities,” Shaheen told Reuters.

In its Dec. 7 letter to Shaheen, the Pentagon said it was “exploring the feasibility” of requiring vendors to disclose when they have allowed foreign governments to access source code. Shaheen had questioned the Pentagon about the practice following the Reuters report on ArcSight, which also prompted Micro Focus to say it would restrict government source code reviews in the future. HPE said none of its current products have undergone Russian source code review.

Lamar Smith, the Republican chairman of the House Science, Space and Technology Committee, said legislation to better secure the federal cybersecurity supply chain was clearly needed.

Responding to the Reuters report on Thursday, Democratic Congressman Jim Langevin, a senior member of the House Armed Services Committee, said the Pentagon must consider “any access adversaries may have to source code when it is making purchasing decisions.”

Most U.S. government agencies declined to comment when asked whether they were aware technology installed within their networks had been inspected by Russian military contractors. Others said security was of paramount concern but that they could not comment on the use of specific software.

A Pentagon spokeswoman said it continually monitors the commercial technology it uses for security weaknesses.

NO PENCILS ALLOWED

Tech companies wanting to access Russia's large market are often required to seek certification for their products from Russian agencies, including the FSB security service and Russia's Federal Service for Technical and Export Control (FSTEC), a defense agency tasked with countering cyber espionage.

FSTEC declined to comment and the FSB did not respond to requests for comment. The Kremlin referred all questions to the FSB and FSTEC.

FSTEC often requires companies to permit a Russian government contractor to test the software's source code.

SAP HANA, a database system, underwent a source code review in order to obtain certification in 2016, according to Russian regulatory records. The software stores and analyzes information for the State Department, Internal Revenue Service, NASA and the Army.

An SAP spokeswoman said any source code reviews were conducted in a secure, company-supervised facility where recording devices or even pencils are "are strictly forbidden."

"All governments and governmental organizations are treated the same with no exceptions," the spokeswoman said.

While some companies have since stopped allowing Russia to review source code in their products, the same products often remain embedded in the U.S. government, which can take decades to upgrade technology.

Security concerns caused Symantec to halt all government source code reviews in 2016, the company's chief executive told Reuters in October. But Symantec Endpoint Protection antivirus software, which was reviewed by Russia in 2012, remains in use by the Pentagon, the FBI, and the Social Security Administration, among other agencies, according to federal contracting records reviewed by Reuters.

In a statement, a Symantec spokeswoman said the newest version of Endpoint Protection, released in late 2016, never underwent a source code review and that the earlier version has received numerous updates since being tested by Russia. The California-based company said it had no reason to believe earlier reviews had compromised product security. Symantec continued to sell the older version through 2017 and will provide updates through 2019.

McAfee also announced last year that it would no longer allow government-mandated source code reviews.

The cyber firm's Security Information and Event Management (SIEM) software was reviewed in 2015 by a Moscow-based government contractor, Echelon, on behalf of FSTEC, according to Russian regulatory documents. McAfee confirmed this.

The Treasury Department and Defense Security Service, a Pentagon agency tasked with guarding the military's classified information, continue to rely on the product to protect their networks, contracting records show.

McAfee declined to comment, citing customer confidentiality agreements, but it has previously said the Russian reviews are conducted at company-owned premises in the United States.

'YOU CAN'T TRUST ANYONE'

On its website, Echelon describes itself as an official laboratory of the FSB, FSTEC, and Russia's defense ministry. Alexey Markov, the president of Echelon,

which also inspected the source code for ArcSight, said U.S. companies often initially expressed concerns about the certification process.

“Did they have any? Absolutely!!” Markov wrote in an email.

”The less the person making the decision understands about programming, the more paranoia they have. However, in the process of clarifying the details of performing the certification procedure, the dangers and risks are smoothed out.”

Markov said his team always informs tech companies before handing over any discovered vulnerabilities to Russian authorities, allowing the firms to fix the detected flaw. The source code reviews of products “significantly improves their safety,” he said.

Chris Inglis, the former deputy director of the National Security Agency, the United States’ premier electronic spy agency, disagrees.

“When you’re sitting at the table with card sharks, you can’t trust anyone,” he said. “I wouldn’t show anybody the code.”

Reporting by Dustin Volz and Joel Schectman in Washington and Jack Stubbs in Moscow.; Editing by Jonathan Weber and Ross Colvin