# CHINESE ATTACK ON USIS EXPLOITING SAP VULNERABILITY

DETAILED REVIEW AND COMMENTS

## Introduction

On 11th of May, a security headline broke out in the news, it was about an attack on USIS (U.S. Investigations Services) conducted potentially by Chinese state-sponsored hackers via a vulnerability in SAP Software.

Hackers broke into third-party software in 2013 to open personal records of federal employees and contractors with access to classified intelligence, according to the government's largest private employee investigation provider [1].

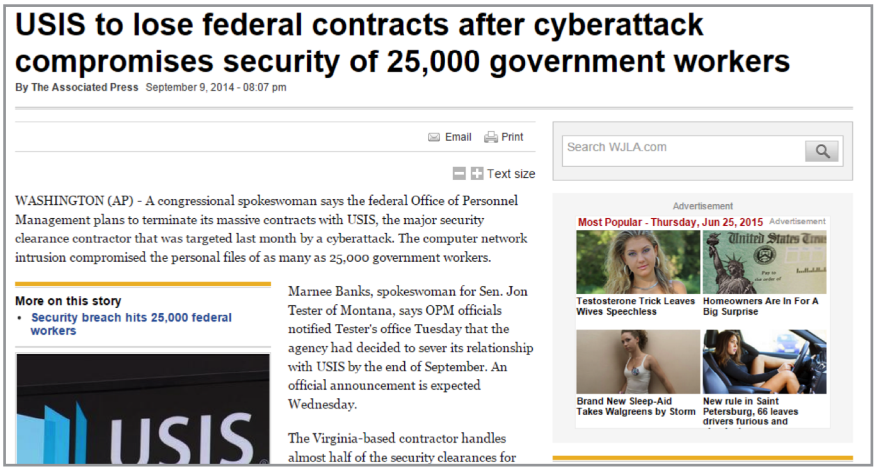
USIS is a federal contractor which conducts background checks for DHS - the largest commercial provider of background investigations to the federal government. It has more than 5,700 employees providing services in all 50 states and U.S. territories and overseas. As the result of the breach, more than 27,000 personnel seeking security clearances were likely to be affected. Similar hacks also affected servers at the Office of Personnel Management (OPM), which holds information on security clearance investigations. Once hackers have a list of employees who possess government security clearances, they can exploit other aspects of those employees' lives with a malicious intent.

### SAP RISKS

**In 2006 through 2010, according to the Association of Certified Fraud Examiners (ACFE), losses to internal fraud constituted 7% of yearly revenue on average. Global fraud loss is estimated at more than $3.5 trillion for 2010–2012. Thus, a typical entity loses 5% of annual revenue to fraud. The average value for 4 years is 6%. That is why we decided to increase awareness in this area.**

**25,000**

**Government workers have their files compromised**



### USIS to lose federal contracts after cyberattack compromises security of 25,000 government workers

By The Associated Press September 9, 2014 - 08:07 pm

Email Print

Text size

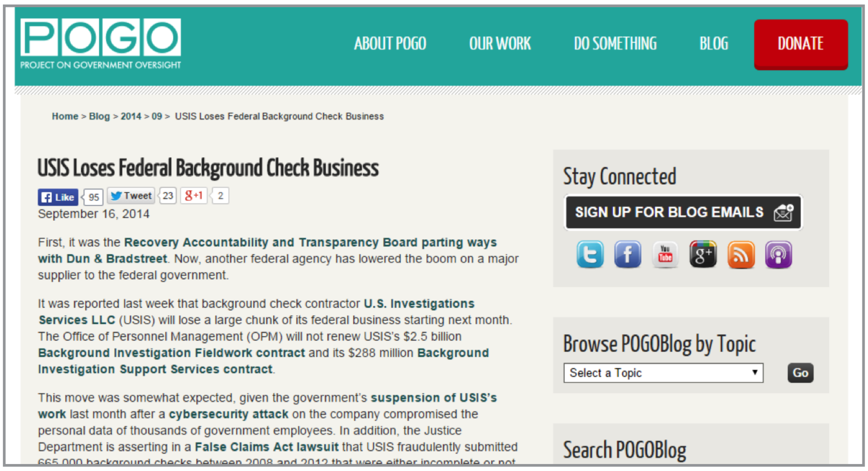
WASHINGTON (AP) - A congressional spokeswoman says the federal Office of Personnel Management plans to terminate its massive contracts with USIS, the major security clearance contractor that was targeted last month by a cyberattack. The computer network intrusion compromised the personal files of as many as 25,000 government workers.

More on this story
- Security breach hits 25,000 federal workers

Marnee Banks, spokeswoman for Sen. Jon Tester of Montana, says OPM officials notified Tester's office Tuesday that the agency had decided to sever its relationship with USIS by the end of September. An official announcement is expected Wednesday.

The Virginia-based contractor handles almost half of the security clearances for

Search WJLA.com



Home > Blog > 2014 > 09 > USIS Loses Federal Background Check Business

### USIS Loses Federal Background Check Business

Like 95 Tweet 23 g+1 2

September 16, 2014

First, it was the **Recovery Accountability and Transparency Board parting ways with Dun & Bradstreet**. Now, another federal agency has lowered the boom on a major supplier to the federal government.

It was reported last week that background check contractor **U.S. Investigations Services LLC** (USIS) will lose a large chunk of its federal business starting next month. The Office of Personnel Management (OPM) will not renew USIS's $2.5 billion **Background Investigation Fieldwork contract** and its $288 million **Background Investigation Support Services contract**.

This move was somewhat expected, given the government's **suspension of USIS's work** last month after a **cybersecurity attack** on the company compromised the personal data of thousands of government employees. In addition, the Justice Department is asserting in a **False Claims Act lawsuit** that USIS fraudulently submitted 665,000 background checks between 2008 and 2012 that were either incomplete or not

Stay Connected

SIGN UP FOR BLOG EMAILS

Browse POGOBlog by Topic

Select a Topic ▾ Go

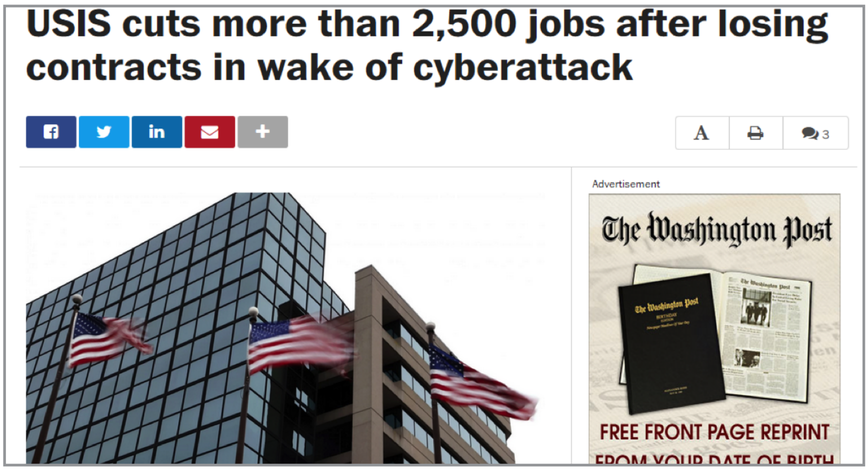
Search POGOBlog

**$2.8**

**Billion dollar worth of contracts were not renewed**

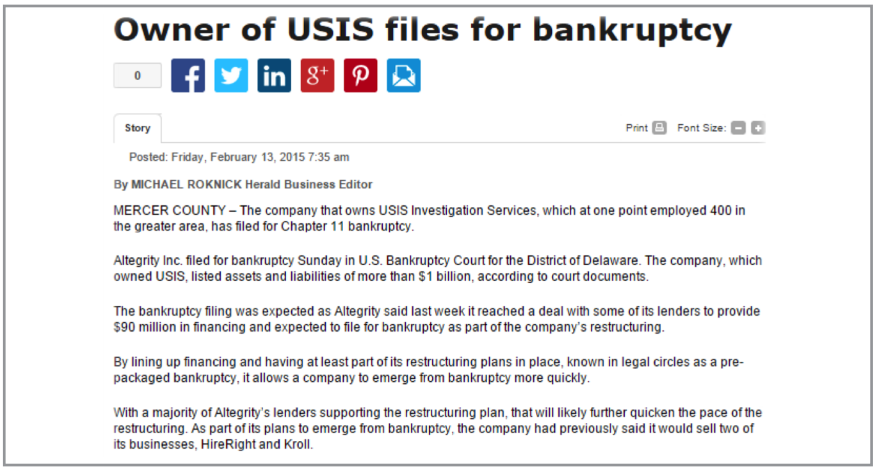
**2,500**

**Employees fired**



### USIS cuts more than 2,500 jobs after losing contracts in wake of cyberattack

A 3



### Owner of USIS files for bankruptcy

0

Story Print Font Size:

Posted: Friday, February 13, 2015 7:35 am

By MICHAEL ROKNICK Herald Business Editor

MERCER COUNTY – The company that owns USIS Investigation Services, which at one point employed 400 in the greater area, has filed for Chapter 11 bankruptcy.

Altegrity Inc. filed for bankruptcy Sunday in U.S. Bankruptcy Court for the District of Delaware. The company, which owned USIS, listed assets and liabilities of more than $1 billion, according to court documents.

The bankruptcy filing was expected as Altegrity said last week it reached a deal with some of its lenders to provide $90 million in financing and expected to file for bankruptcy as part of the company's restructuring.

By lining up financing and having at least part of its restructuring plans in place, known in legal circles as a pre-packaged bankruptcy, it allows a company to emerge from bankruptcy more quickly.

With a majority of Altegrity's lenders supporting the restructuring plan, that will likely further quicken the pace of the restructuring. As part of its plans to emerge from bankruptcy, the company had previously said it would sell two of its businesses, HireRight and Kroll.

**BANCRYPTSY**

**Altegrity Inc. - company-owner of USIS has filed for Chapter 11 bankrupsy.**

## Who else were affected?

USIS has told Congress in a letter obtained by The Washington Post that the breach may have been even more damaging affecting:

- ✓ OPM
- ✓ Customs and Border Protection (DHS)
- ✓ Immigration and Customs Enforcement (DHS)
- ✓ U.S. Capitol Police
- ✓ National Geospatial-Intelligence Agency

## Attacks on SAP can lead not only to stealing your data. The possible outcomes are:

### Espionage

- Theft of financial information
- Corporate trade secret theft
- Theft of supplier and customer lists
- HR data, Employee Data Theft

### Fraud

- Fake vendors
- Modification of master data
- Stealing money

### Sabotage

- Denial of service
- Tampering with financial reports
- DOS attacks on technology network (SCADA/ICS) by trust relations
- Modification of data in Plant Management and Asset Management

Below you can find the timeline of this attack investigation, the collection of historical facts from different resources, and our comments on the topic.

# Attack Timeline

## Late 2013

Initial Attack against USIS Supplier potentially started [2].

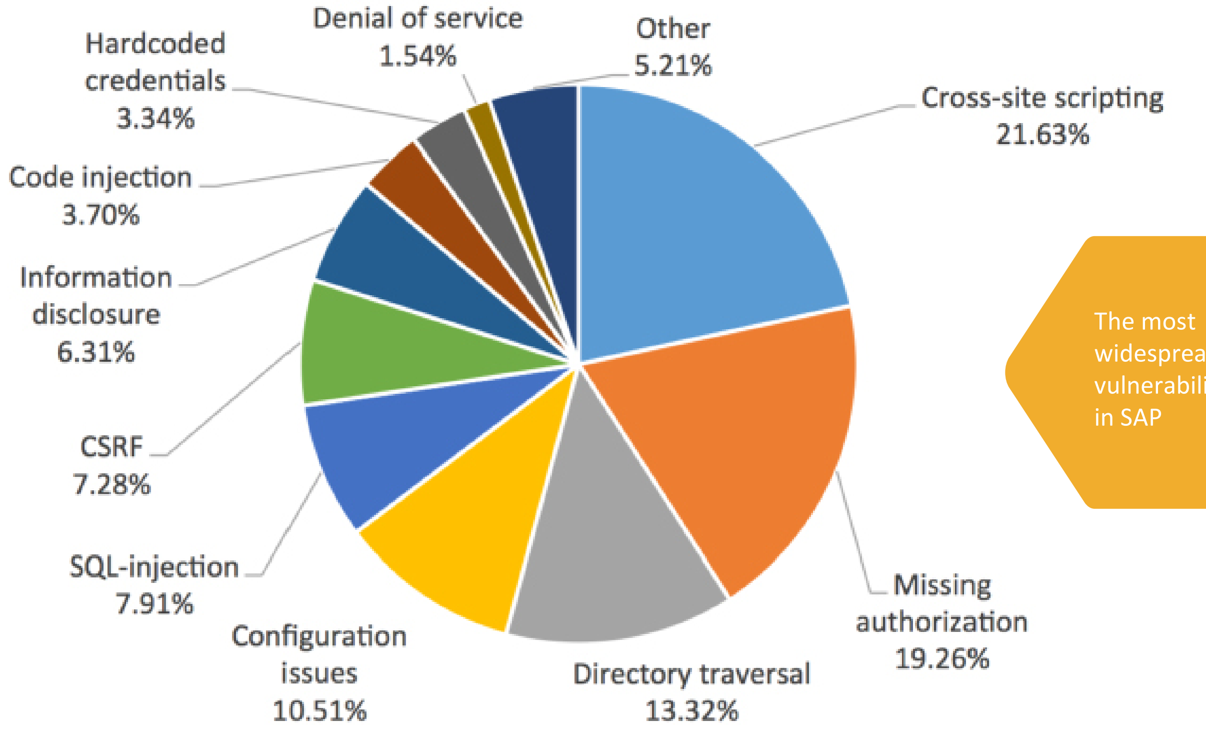
> *Both USIS and OPM were hacked around March 2014, and while the security controls in place at OPM's networks shielded employee information, the networks at USIS were not as secured. At USIS, hackers deployed spyware designed to capture screenshots when a background check window was open,"*
>
> ***- Stroz Friedberg,***
> ***spokesperson from Digital Forensic agency.***

## March 2014

Attack continued against USIS [3].

Hackers infiltrated a network belonging to one of USIS's suppliers that stored ERP software. That network was connected to USIS's network.

> *The attacker was able to navigate from the third-party-managed environment into the USIS network by successfully brute-forcing a password on an application server. Once the attacker was able to log in to that server, the attacker installed a malicious backdoor."*
>
> ***- Padres (NextGov), referring to a hacking technique***
> ***that systematically checks all possible passwords.***



The most widespread vulnerabilities in SAP

## June 5, 2014

USIS reported about the cyberattack to federal authorities on June 5, more than two months before acknowledging it publicly [4].

## July 9, 2014

It was published, that Chinese hackers in March broke into the computer networks of some United States government agency that houses the personal information of all federal employees. But officials also said that neither the personnel agency nor Homeland Security had identified any loss of personally identifiable information [5].

## August 6, 2014

USIS published the press release stating that they were hacked. And potentially it was a state-sponsored attack. They also hired independent Forensic investigation company - Stroz Friedberg to perform an investigation [6].

## August 22, 2014

Detailed information about the breach appeared in the news.

> *The agency has identified some 25,000 employees whose information it believes were exposed in the breach. While the number of employees affected is relatively small compared to breaches at retailers such as Target or Home Depot which have affected tens of millions of customers, nonetheless quite serious.*
>
> ***– one of DHS officials to Reuters***

Files on background checks contain highly sensitive data that foreign intelligence agencies could attempt to exploit to intimidate government workers with access to classified information.

This information includes Social Security numbers, education and criminal history, birth dates along with information about spouses, other relatives and friends including their names and addresses. [7]

## November 3, 2014

First detailed information about the attack appeared on Associated Press website. At this time without any details that attack on SAP ERP System was used to carry out the attack [8].

> *A cyberattack similar to previous hacker intrusions from China penetrated computer networks for months at USIS, the government's leading security clearance contractor, before the company noticed, officials and others familiar with an FBI investigation and related official inquiries. The breach, first revealed by the company and government agencies in August, compromised the private records of at least 25,000 employees at the Homeland Security Department and cost the company hundreds of millions of dollars in lost government contracts. In addition to trying to identify the perpetrators and evaluate the scale of the stolen material, the government inquiries have prompted concerns about why computer detection alarms inside the company failed to quickly notice the hackers and whether federal agencies that hired the company should have monitored its practices more closely."*
>
> ***– The Associated Press*** [9]

In the private analysis prepared for USIS by Stroz Friedberg, a digital risk management firm, managing director Bret A. Padres said the company's computers had government-approved "perimeter protection, antivirus, user authentication and intrusion-detection technologies." But Padres said his firm did not evaluate the strength of USIS' cybersecurity measures before the intrusion. So, what can we learn from the following statement: **"government inquiries have prompted concerns about why computer detection alarms inside the company failed to quickly notice the hackers"?**

As we have mentioned in many reports, SAP Security, much like any business application security area is rarely covered by traditional security tools such as vulnerability management and intrusion detection systems. SAP has very specific vulnerabilities and configuration issues that should be assessed by high-quality experts. To give you an example, there are thousands of parameters related to security in each SAP System just in application server. In addition to that, there were 3300+ vulnerabilities found in SAP from 2001 till 2015. Also, if we continue to speak about complexity, there are 1200 web services installed by default on SAP NetWeaver 7.2 (SAP's application server), each web service is like a small website. So, you beggin to get an idea of the complexity of this system and the magnitude of potential issues. Needless to say that "complexity kills security". Even after the latest SAP's marketing campaign "SAP is Simple" (which is a great idea), it will take you years to make it really simple with such amount of legacy systems.

## November 4, 2014

New information appeared in the news [10].

> *The hackers attacked a vulnerable computer server in a connected but separate network, managed by a third party not affiliated with USIS,"*
>
> ***- Bret Padres from Stroz Friedberg, Digital Forensic agency.***

### SAP NOTES

Every month on SAP Critical Patch Day (every second Tuesday), SAP releases one or more internal advisories called SAP Security Notes. Such an advisory usually stores information about one or more vulnerabilities found in SAP products or misconfigurations that bear some risk to SAP systems. The first SAP Security Note was published in 2001. In 2007, the number of published notes began to grow exponentially having its peak in 2010. Later, the number of SAP security notes began to fall, but still remain on quite high value.

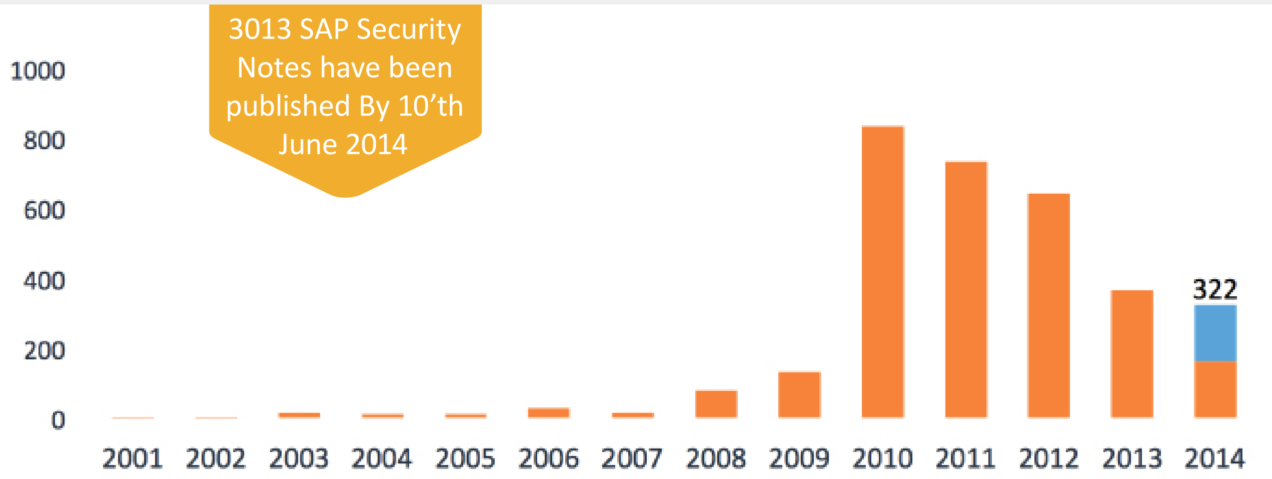
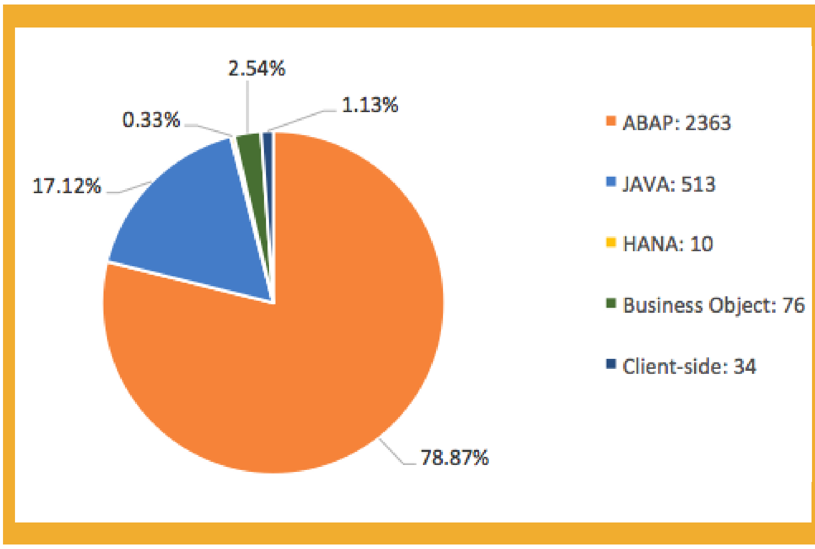


*Figure 3.1-1. Number of Sap Security Notes per year: 2001-2014*



**Vulnerabilities sorted by engine**

**In the SAP systems there are several large popular platforms on which different systems are based. Among them there are 5 most popular areas:**

- **NetWeaver ABAP engine**
- **NetWeaver J2EE engine**
- **SAP HANA**
- **SAP Business Object**
- **Frontend applications**

Now we learned, that the actual attack was conducted via separate network owned by 3rd party, but still nothing special about how exactly it was executed.

## April 28, 2015

After almost 5 months of silence, finally some new information appeared, and this was the first resource where we found information that pointed us to the fact that the initial attack was against ERP System. And this ERP System was on the separate network managed by separate company. [11]

> *The attacker was able to navigate from the third-party-managed environment into the USIS network by successfully brute-forcing a password on an application server,”*
>
> ***– Padres.***

Hackers infiltrated a network belonging to one of USIS’s suppliers, which stored enterprise resource planning software. That network was connected to USIS’s network. [12]

When we speak about business applications, we need to consider their highly interconnected nature. You can’t just implement dozens of business applications in a company and leave them unconnected. For example, to automate business processes, your ERP system should be able to automatically create an invoice in banking system, so these systems should be somehow connected on application layer even if they are separated by network. In the real life we see dozens or even hundreds of connections between different SAP Systems, and some of these connections (so-called RFC Destinations) store usernames and passwords (according to our statistics, average number of connections in SAP System is about 50 while 30% of them usually store usernames and passwords).

Once an attacker gets an access to the weakest SAP System, he can easily get access to connected systems and from them to others, so on and so forth spreading his access like a spider’s web.

Another way how business applications can be connected is via Enterprise Service Bus, such as SAP PI, or process integration system, these systems also have vulnerabilities as reported by ERPScan Research team during BlackHat 2013 conference.

Even if direct connections don’t exist, there was a research conducted by ERPScan experts, with explanation of SSRF attack that can be used to bypass firewall restriction and attack systems using their trust connections [13].

Taking into account those connections, it comes as no surprise that attackers were able to get access to the connected network of another company.

Finally we would like to say that those connections can be even more dangerous if we talk about Manufacturing, Oil and Gas and Nuclear Energy sectors, where SAP can be connected with Field Devices and Plant Floor.

## May 10, 2015

From the above paragraphs one can conclude that this ERP system was most probably SAP as it happenes to be the most popular, and the new article confirmed this fact. NextGov became the first resource to point out the fact that it was actually SAP.

> *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,"*
>
> ***- internal investigation by NextGov.***

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." [14]

**5%** SAP

Number of vulnerabilities closed by SAP is about 5% of all existing vulnerabilities.

**70%** 3RD PARTIES

Number of vulnerabilities found by 3rd parties comparing to vulnerabilities patched by SAP.

This report also includes an attempt to look deeper into SAP vulnerabilities and analyze what has transpired:

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 [15].

From our point of view, real figures about potential vulnerabilities are much larger. If we assume that real attack was conducted in 2013, let's say in the beginning of the year, the actual number of vulnerabilities patched by SAP from 2001 to the middle of 2013 were about 2000, according to the research "SAP Security in figures 2013" [16] based on information from SAP Support portal about all vulnerabilities.

> *The number of SAP vulnerabilities would have given attackers many options to target SAP directly, based on how USIS deployed the ERP tool,"*
>
> ***- Richard Barger, chief intelligence officer at ThreatConnect, former Army intelligence analyst.***

This is more than true. In addition, more than 2000 potential vulnerabilities existed in SAP Applications, there also can be some vulnerabilities in custom programs developed by USIS subcontractor or even another 3rd party.

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.

## May 11, 2015

Some other details appeared. [17]

Lawmakers have been pressing for answers about the breach since last year. Suspected Chinese hackers got into the USIS systems in late 2013 but weren't discovered until June 2014. This comes as a no big surprize to us. Some of the companies that we had a chance to assess don't have any visibility to their systems. According to our research, only 10% of customers really configure and analyze SAP Security logs and other events.

## May 12, 2015

An article from DarkReading where we gave our first comments regarding this breach.[18]

So now, you can get the full picture of attack, and there is only one question left – how this attack was conducted. Let's try to answer it.

# What kind of vulnerability was exploited?

The news states that the vulnerability is “present in a widely-used and highly-regarded enterprise resource planning (‘ERP’) software package”

No other details about the vulnerability were provided.

Let’s try to understand what kind of vulnerabilities were used in this attack, but, first of all, let’s look at the history. We provide annual reviews about SAP Vulnerabilities, these reports usually called “SAP Security in figures”

- 2011. SAP SECURITY IN FIGURES 2007-2011 [19]
- 2013. SAP SECURITY IN FIGURES 2007-2013 [20]
- 2014. Analysis of 3000 SAP Security notes [21]
- 2015. Blog post with latest review [22]

From those reports we can get information about most critical vulnerabilities. Taking into account that the attack has happened in late 2013, only the first three reports will be relevant for us.

Another guideline provided by ERPScan Research team is focused on most popular vulnerabilities, taking into consideration their criticality as well. So, combining data from these reports we can give an overview of vulnerabilities that were most probably used in this attack. And even if this assumption won’t be true, we will anyway get the list of most critical and popular vulnerabilities affecting SAP ERP Systems. The fact that we are mostly looking for SAP ERP vulnerabilities also should be taken into account.

We also excluded most of the vulnerabilities that can be used only with combination with others, most of the specific vulnerabilities, and those vulnerabilities that require some user’s actions such as XSS. So finally we narrowed down to 15 vulnerabilities that most likely were used against USIS’s ERP System in this period of time and can give attacker and easy way to get full access to vulnerable SAP System.

And finally we limited the list of vulnerabilities by publication date and selected only those that were published before Q2 2013.

**Questions? Comments? Brilliant ideas?**

We want to hear them. Drop us a line at
info@erpscan.com,
find us on LinkedIn,
or tweet @erpscan

We add a couple of parameters to each vulnerability to calculate the final likelihood as to which particular vulnerability was exploited.

- **Criticality –** Real impact to system, such as full administrative access or just an information disclosure.
- **Frequency** – Amount of information in public sources such as presentations, whitepapers, and advisories with vulnerability description.
- **Ease of exploitation** – If there is a publically available free tool with exploit, or exploit, or POC, or advisory, or some kind of details.
- **Applicability** – our personal thoughts if this vulnerability is applicable to particular system that has been used in organization.
- **Likehood** – overall probability that this particular vulnerability was exploited based on previously mentioned parameters.

Here is the table with details of our analysis

| Vulnerability Title | Year | Likehood | Popularity | Criticality | Ease of exploitation: | Applicability | CVSSv2: | Patch |
|---|---|---|---|---|---|---|---|---|
| Default passwords for administrative users | 2002 | 100,00% | 5 | 5 | 5 | 5 | 7,5 | 1414256 |
| RFC Gateway remote command execution | 2007 | 80,00% | 5 | 5 | 4 | 5 | 7,5 | 1425765, 1408081, 1473017, 1069911, 1480644 ,614971, 1525125 |
| SAP/Oracle REMOTE_OS_AUTHENT | 2003 | 40,96% | 4 | 4 | 4 | 4 | 7,5 | 1622837, 1639578 |
| Remote code execution via TH_GREP | 2011 | 38,40% | 4 | 5 | 3 | 4 | 6.0 | 1620632 |
| Unauthorized access to SAP Management console | 2011 | 38,40% | 4 | 3 | 4 | 5 | 5,6 | 1439348 |
| SAP Host Control – Code Injection | 2012 | 36,00% | 3 | 5 | 5 | 3 | 10 | 1341333 |
| SAP Dispatcher – DIAG protocol Buffer Overflow | 2012 | 24,00% | 3 | 5 | 2 | 5 | 9,3 | 1687910 |

| Vulnerability Title | Year | Likehood | Popularity | Criticality | Ease of exploitation: | Applicability | CVSSv2: | Patch |
|---|---|---|---|---|---|---|---|---|
| Authentication bypass through Verb Tampering | 2011 | 20,00% | 5 | 5 | 5 | 1 | 10 | 1589525,<br>1624450 |
| Authentication bypass through the Invoker servlet | 2011 | 20,00% | 5 | 5 | 5 | 1 | 10 | 1585527 |
| SAP Message Server – Buffer Overflow | 2012 | 16,00% | 2 | 5 | 2 | 5 | 10 | 1649840 |
| SAP NetWeaver DI – Arbitrary file upload | 2013 | 10,24% | 2 | 4 | 2 | 4 | 9,3 | 1757675 |
| Message Server Auth Bypass | 2008 | 7,68% | 3 | 4 | 1 | 4 | 7,5 | 1421005 |
| SAP GRMGApp – XXE and authentication bypass | 2013 | 5,76% | 2 | 3 | 2 | 3 | 7,3 | 1729293,<br>1725390 |
| SAP NetWeaver J2EE – DilbertMSG SSRF [14] | 2012 | 4,32% | 3 | 3 | 3 | 1 | 7,3 | 1707494 |
| Buffer overflow in ABAP Kernel call | 2011 | 3,20% | 1 | 5 | 1 | 4 | 4,8 | 1487330,<br>1529807 |

So, most likely the vulnerability exploited was one of the following:

1. Default passwords for administrative users
2. RFC Gateway remote command execution
3. SAP/Oracle REMOTE_OS_AUTHENT
4. Remote code execution via TH_GREP
5. Unauthorized access to SAP Management console

# Prevention

We recommend you to implement some of the most critical SAP Security Notes, which were probably used during this attack, these are listed in the table provided above.

Secondly, follow our guidelines [23] for initial assessment of SAP NetWeaver ABAP Application server – 33 Most critical security checks.

Thirdly, check this presentation, as well as all other slides and guidelines [24] about SAP Security and you are also welcome to follow us during security conferences worldwide. Here is the list of upcoming events http://erpscan.com/category/press-center/future-events/.

# Recommendations

Since all steps discussed previously can be manhour intensive, we recommend you to check automatic solutions to assess and secure your system as soon as possible, as nobody knows, if your system is not under attack.

### Takeaways for CISOs are:

As you see, when some researchers start flagging security loopholes by publishing information about one or another system's security vulnerability, it's only a matter of time before cyber criminals actually exploit it. Who will fall victim is anybody's guess. So, apart from the fact that it's better to take precautionary actions before a real example surfaces, we started highlighting this 8 years back.

Our lessons are simply three:

1. When it comes to advanced cyber attacks you can't rely only on traditional security solutions.
2. You can't be sure that everything is ok in your network unless you really monitor it from all angles, if we talk about SAP it means that VA, Custom code security, SOD and event monitoring - all areas should be on the radar.
3. And the most important for business applications is that they are highly connected within each other, and as you see in this example, and it's not only the problem of your infrastructure security, it's also a problem of all your external connections and 3rd party security

So what it boils down to is that "a system is only as secure as its weakest link".

# References

1. http://www.nextgov.com/cybersecurity/2015/05/third-party-software-was-entry-point-background-check-system-hack/112354/

2. http://www.nextgov.com/cybersecurity/2015/05/third-party-software-was-entry-point-background-check-system-hack/112354/

3. www.homelandsecuritynewswire.com%2Fdr20150430-breach-of-backgroundchecks-database-may-lead-to-blackmail

4. http://www.theblaze.com/stories/2014/11/04/cyberattack-on-top-u-s-govt-security-contractor-went-unnoticed-for-months/

5. http://www.nytimes.com/2014/07/10/world/asia/chinese-hackers-pursue-key-data-on-us-workers.html?_r=0

6. http://www.usis.com/media-release-detail.aspx?dpid=151

7. http://www.reuters.com/article/2014/08/22/us-usa-security-contractor-cyberattack-idUSKBN0GM1TZ20140822

8. http://bigstory.ap.org/article/427fbd5d88f5481eab35f5a8bbc534be/security-contractor-breach-not-detected-months

9. http://bigstory.ap.org/article/427fbd5d88f5481eab35f5a8bbc534be/security-contractor-breach-not-detected-months.

10. http://www.theblaze.com/stories/2014/11/04/cyberattack-on-top-u-s-govt-security-contractor-went-unnoticed-for-months/

11. http://www.ladailypost.com/content/background-checks-database-breach-heightens-blackmail-risk

12. http://www.nextgov.com/cybersecurity/2015/05/third-party-software-was-entry-point-background-check-system-hack/112354/

13. http://erpscan.com/wp-content/themes/supercms/Publications/SSRF%20vs%20Businness%20critical%20applications%20final%20edit.pdf

14. http://www.nextgov.com/cybersecurity/2015/05/third-party-software-was-entry-point-background-check-system-hack/112354/

15. http://www.nextgov.com/cybersecurity/2015/05/third-party-software-was-entry-point-background-check-system-hack/112354/

16. http://erpscan.com/wp-content/themes/supercms/Publications/SAP%20Security%20in%20figures%20-%20A%20global%20survey%202013%20RC.pdf

17. http://thehill.com/policy/cybersecurity/241588-report-hackers-infiltrated-security-contractor-using-third-party

18. http://www.darkreading.com/attacks-breaches/first-example-of-sap-breach-surfaces/d/d-id/1320382

19. http://erpscan.com/wp-content/themes/supercms/Publications/SAP-Security-in-figures-a-global-survey-2007-2011-final.pdf

20. http://erpscan.com/wp-content/themes/supercms/Publications/3000-SAP-notes-Analysis-by-ERPScan.pdf

21. http://erpscan.com/wp-content/themes/supercms/Publications/3000-SAP-notes-Analysis-by-ERPScan.pdf

22. http://erpscan.com/press-center/blog/sap-vulnerabilities-highlighted-in-many-reports-such-as-hp-cyber-risk-report-2015/#more-7858

23. http://erpscan.com/wp-content/themes/supercms/Publications/EASSEC-PVAG-ABAP.pdf

24. http://erpscan.com/white-papers/

# Our Contacts

**Global Headquarters:** 228 Hamilton Avenue, Fl. 3,
Palo Alto, CA. 94301
Phone: 650.798.5255

**EMEA Headquarters:** Luna ArenA 238 Herikerbergweg,
1101 CM Amsterdam
Phone: +31 20 8932892

Twitter: @erpscan
Web: www.erpscan.com
Contact: info@erpscan.com
PR: pr@erpscan.com