RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

SESSION ID: TECH-W05F

Understanding The “Why” In Enterprise Application Security Strategy

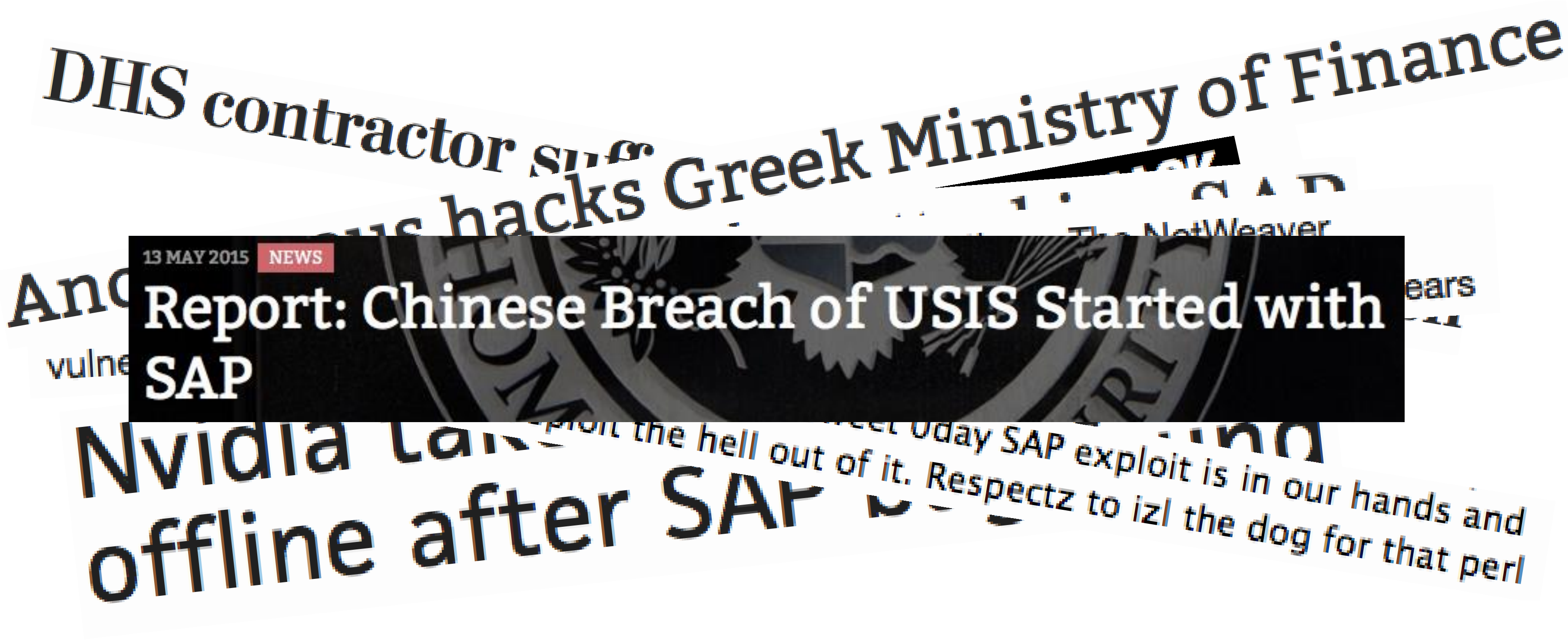
Connect to Protect

Troy Grubb

Information Security Manager,
GRC & SAP Security
The Hershey Company
@TroyRGrubb

#RSAC

SAP Security – The New Reality



DHS contractor suf

us hacks Greek Ministry of Finance

An

vulne

The NetWeaver

ears

13 MAY 2015 NEWS

Report: Chinese Breach of USIS Started with SAP

Nvidia tak

ind

offline after SAP

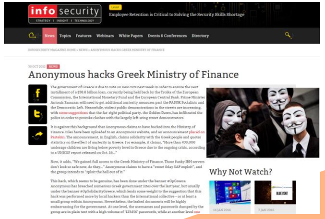
0day SAP exploit is in our hands and

xploit the hell out of it. Respectz to izl the dog for that perl

SAP Security – The New Reality

The Escalation of SAP Security Breaches

2012


info security
STRATEGY | INSIGHT | TECHNOLOGY
Latest
Employee Retention is Critical to Solving the Security Skills Shortage
News
Topics
Features
Webinars
White Papers
Events & Conferences
Directory
INFOSECURITY MAGAZINE HOME » NEWS » ANONYMOUS HACKS GREEK MINISTRY OF FINANCE
30 OCT 2012
NEWS
Why Not Watch?
BLUE COAT
14 JAN 2016
7 JAN 2016

Anonymous hacks Greek Ministry of Finance

The government of Greece is due to vote on new cuts next week in order to ensure the next installment of a $38.8 billion loan, currently being held back by the Troika of the European Commission, the International Monetary Fund and the European Central Bank. Prime Minister Antonis Samaras will need to get additional austerity measures past the PASOK Socialists and the Democratic Left. Meanwhile, violent public demonstrations in the streets are increasing, with some suggestions that the far-right political party, the Golden Dawn, has infiltrated the police in order to provoke clashes with the largely left-wing street demonstrators.

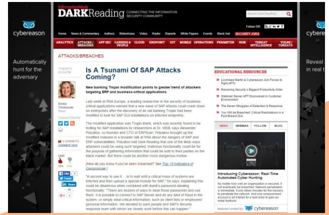
It is against this background that Anonymous claims to have hacked into the Ministry of Finance. Files have been uploaded to an Anonymous website, and an announcement placed on Pastebin. The announcement, in English, claims solidarity with the Greek people and quotes statistics on the effect of austerity in Greece. For example, it claims, "More than 439,000 underage children are living below poverty level in Greece due to the ongoing crisis, according to a UNICEF report released on Oct. 16..."

Now, it adds, "We gained full access to the Greek Ministry of Finance. Those funky IBM servers don't look so safe now, do they..." Anonymous claims to have a "sweet 0day SAP exploit", and the group intends to "sploit the hell out of it."

This hack, which seems to be genuine, has been done under the banner #OpGreece. Anonymous has breached numerous Greek government sites over the last year, but usually under the banner #OpSolidarityGreece, which lends some weight to the suggestion that this hack was performed more by local hackers than the international collective – or at least a small group within Anonymous. Nevertheless, the leaked documents will be highly embarrassing for the government. At one level, the usernames and passwords dumped by the group are in plain text with a high volume of '123456' passwords, while at another level one

Anonymous claimed breach to Greek Ministry of Finance using SAP zero-day exploit.

2013



Is A Tsunami Of SAP Attacks Coming?

New banking Trojan modification points to greater trend of attackers targeting ERP and business-critical applications

Last week at RSA Europe, a leading researcher in the security of business-critical applications warned that a new wave of SAP attacks could crash down on enterprises after the discovery of an old banking Trojan had been modified to look for SAP GUI installations on infected endpoints.

The modified application was Trojan.ibank, which was recently found to be trolling for SAP installations by researchers at Dr. WEB, says Alexander Polyakov, co-founder and CTO of ERPScan. Polyakov brought up the modified malware in a broader talk at RSA about the dangers of SAP and ERP vulnerabilities. Polyakov told Dark Reading that one of the likely ways attackers could be using such targeted, malicious functionality could be for the purpose of gathering information that could be sold to third parties on the black market. But there could be another more dangerous motive.

[How do you know if you've been breached? See Top 15 Indicators of Compromise.]

"A second way to use it ... is to wait until a critical mass of systems are infected and then upload a special module for SAP," he says, explaining this could be disastrous when combined with ibank's password-stealing functionality. "There are dozens of ways to steal those passwords and use them. It is possible to connect to SAP Server and do any kind of fraud in the system, or simply steal critical information, such as client lists or employees' personal information. We decided to warn people and SAP's Security response team with whom we closely work before this can happen."

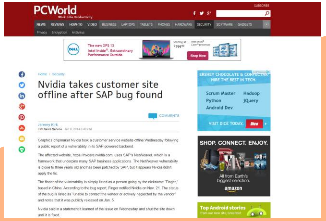
- Lockheed Martin & Cybereason Join Forces to Fight APTs
- Resolving Security's Biggest Productivity Killer
- Webmail Server APT Discovered in Customer Environment
- The Seven Struggles of Detection & Response
- You Will be Breached: Critical Realizations in a Post-Breach Era

Introducing Cybereason: Real-Time Automated Cyber Hunting

No matter how well an organization is secured, it will eventually be breached. Network penetration is immediate. It only takes minutes for the hackers to penetrate the network. And one compromised account is all it takes for a bad actor to gain an initial foothold.

A malware targeting SAP systems discovered in the wild – A "Tsunami of SAP Attacks Coming?"

2014



Nvidia takes customer site offline after SAP bug found

Jeremy Kirk
IDG News Service Jan 8, 2014 6:40 PM

Graphics chipmaker Nvidia took a customer service website offline Wednesday following a public report of a vulnerability in its SAP-powered backend.

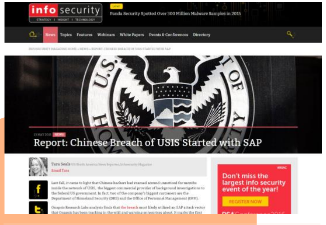
The affected website, https://nvcare.nvidia.com, uses SAP's NetWeaver, which is a framework that underpins many SAP business applications. The NetWeaver vulnerability is close to three years old and has been patched by SAP, but it appears Nvidia didn't apply the fix.

The finder of the vulnerability is simply listed as a person going by the nickname "Finger," based in China. According to the bug report, Finger notified Nvidia on Nov. 21. The status of the bug is listed as "unable to contact the vendor or actively neglected by the vendor" and notes that it was publicly released on Jan. 5.

Nvidia said in a statement it learned of the issue on Wednesday and shut the site down until it is fixed.

A Chinese hacker exploited a vulnerability in a corporate SAP NetWeaver Portal.

May 2015


info security
STRATEGY | INSIGHT | TECHNOLOGY
Latest
Panda Security Spotted Over 300 Million Malware Samples in 2015
News
Topics
Features
Webinars
White Papers
Events & Conferences
Directory
INFOSECURITY MAGAZINE HOME » NEWS » REPORT: CHINESE BREACH OF USIS STARTED WITH SAP
13 MAY 2015
NEWS
Tara Seals US/North America News Reporter, Infosecurity Magazine
Email Tara
#RSAC
Don't miss the largest info security event of the year!
REGISTER NOW

Report: Chinese Breach of USIS Started with SAP

Last fall, it came to light that Chinese hackers had roamed around unnoticed for months inside the network of USIS, the biggest commercial provider of background investigations to the federal US government. In fact, two of the company's biggest customers are the Department of Homeland Security (DHS) and the Office of Personnel Management (OPM).

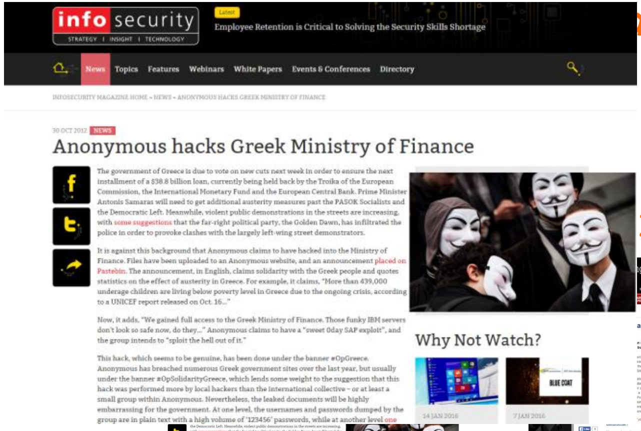
Onapsis Research Labs analysis finds that the breach most likely utilized an SAP attack vector that Onapsis has been tracking in the wild and warning enterprises about. It marks the first

Report: A Chinese Breach of USIS targeted SAP. Went unnoticed for over six months and compromised over 48,000 employee records of DHS and OPM.

SAP Security – The New Reality

alation of SAP Security Breaches

2012



info security
STRATEGY | INSIGHT | TECHNOLOGY

Latest
Employee Retention is Critical to Solving the Security Skills Shortage

News Topics Features Webinars White Papers Events & Conferences Directory

INFOSECURITY MAGAZINE HOME » NEWS » ANONYMOUS HACKS GREEK MINISTRY OF FINANCE

30 OCT 2012 NEWS

Anonymous hacks Greek Ministry of Finance

The government of Greece is due to vote on new cuts next week in order to ensure the next installment of a $38.8 billion loan, currently being held back by the Troika of the European Commission, the International Monetary Fund and the European Central Bank. Prime Minister Antonis Samaras will need to get additional austerity measures past the PASOK Socialists and the Democratic Left. Meanwhile, violent public demonstrations in the streets are increasing, with some suggestions that the far-right political party, the Golden Dawn, has infiltrated the police in order to provoke clashes with the largely left-wing street demonstrators.

It is against this background that Anonymous claims to have hacked into the Ministry of Finance. Files have been uploaded to an Anonymous website, and an announcement placed on Pastebin. The announcement, in English, claims solidarity with the Greek people and quotes statistics on the effect of austerity in Greece. For example, it claims, "More than 439,000 underage children are living below poverty level in Greece due to the ongoing crisis, according to a UNICEF report released on Oct. 16..."

Now, it adds, "We gained full access to the Greek Ministry of Finance. Those funky IBM servers don't look so safe now, do they..." Anonymous claims to have a "sweet 0day SAP exploit", and the group intends to "sploit the hell out of it."

This hack, which seems to be genuine, has been done under the banner #OpGreece. Anonymous has breached numerous Greek government sites over the last year, but usually under the banner #OpSolidarityGreece, which lends some weight to the suggestion that this hack was performed more by local hackers than the international collective – or at least a small group within Anonymous. Nevertheless, the leaked documents will be highly embarrassing for the government. At one level, the usernames and passwords dumped by the group are in plain text with a high volume of '123456' passwords, while at another level one

Why Not Watch?

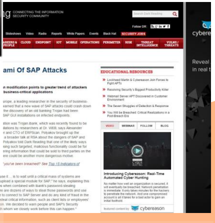
14 JAN 2016

7 JAN 2016

Anonymous claimed breach to Greek Ministry of Finance using SAP zero-day exploit.

Anonymous claimed breach to Greek Ministry of Finance using SAP zero-day exploit.

2013



CONNECTING THE INFORMATION SECURITY COMMUNITY

Slideshows Video Radio Reports White Papers Events Black Hat SECURITY JOBS

AREERS & PEOPLE CLOUD ENDPOINT IOT MOBILE OPERATIONS PERIMETER RISK THREAT INTELLIGENCE VULNS / THREATS

ami Of SAP Attacks

n modification points to greater trend of attackers business-critical applications

urope, a leading researcher in the security of business- warned that a new wave of SAP attacks could crash down the discovery of an old banking Trojan had been SAP GUI installations on infected endpoints.

ation was Trojan.ibank, which was recently found to be llations by researchers at Dr. WEB, says Alexander r and CTO of ERPScan. Polyakov brought up the a broader talk at RSA about the dangers of SAP and Polyakov told Dark Reading that one of the likely ways sing such targeted, malicious functionality could be for ering information that could be sold to third parties on the ere could be another more dangerous motive.

'you've been breached? See Top 15 Indicators of'

"A second way to use it … is to wait until a critical mass of systems are infected and then upload a special module for SAP," he says, explaining this could be disastrous when combined with ibank's password-stealing functionality. "There are dozens of ways to steal those passwords and use them. It is possible to connect to SAP Server and do any kind of fraud in the system, or simply steal critical information, such as client lists or employees' personal information. We decided to warn people and SAP's Security response team with whom we closely work before this can happen."

EDUCATIONAL RESOURCES

- Lockheed Martin & Cybereason Join Forces to Fight APTs
- Resolving Security's Biggest Productivity Killer
- Webmail Server APT Discovered in Customer Environment
- The Seven Struggles of Detection & Response
- You Will be Breached: Critical Realizations in a Post-Breach Era

VIDEO WEBINAR FOLLOW BLOG

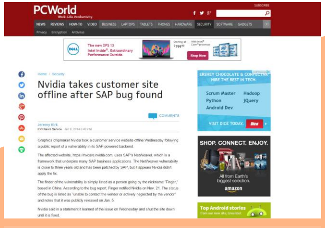
Introducing Cybereason: Real-Time Automated Cyber Hunting

No matter how well an organization is secured, it will eventually be breached. Network penetration is immediate. It only takes minutes for the hackers to penetrate the network. And one compromised account is all it takes for a bad actor to gain an initial foothold.

featured content by cybereason

A malware targeting SAP systems discovered in the wild – "Tsunami of SAP Attacks Coming?"

2014



PCWorld
Work. Life. Productivity.

NEWS REVIEWS HOW-TO VIDEO BUSINESS LAPTOPS TABLETS PHONES HARDWARE SECURITY SOFTWARE GADGETS

Privacy Encryption Antivirus

Home / Security

Nvidia takes customer site offline after SAP bug found

Jeremy Kirk
IDG News Service Jan 8, 2014 6:40 PM

Graphics chipmaker Nvidia took a customer service website offline Wednesday following a public report of a vulnerability in its SAP-powered backend.

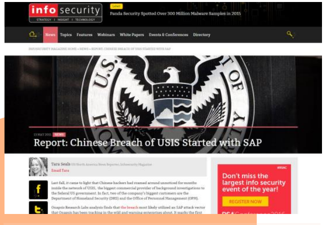
The affected website, https://nvcare.nvidia.com, uses SAP's NetWeaver, which is a framework that underpins many SAP business applications. The NetWeaver vulnerability is close to three years old and has been patched by SAP, but it appears Nvidia didn't apply the fix.

The finder of the vulnerability is simply listed as a person going by the nickname "Finger," based in China. According to the bug report, Finger notified Nvidia on Nov. 21. The status of the bug is listed as "unable to contact the vendor or actively neglected by the vendor" and notes that it was publicly released on Jan. 5.

Nvidia said in a statement it learned of the issue on Wednesday and shut the site down until it is fixed.

A Chinese hacker exploited a vulnerability in a corporate SAP NetWeaver Portal.

May 2015



info security
STRATEGY | INSIGHT | TECHNOLOGY

Latest
Panda Security Spotted Over 300 Million Malware Samples in 2015

News Topics Features Webinars White Papers Events & Conferences Directory

INFOSECURITY MAGAZINE HOME » NEWS » REPORT: CHINESE BREACH OF USIS STARTED WITH SAP

13 MAY 2015 NEWS

Report: Chinese Breach of USIS Started with SAP

Tara Seals US/North America News Reporter, Infosecurity Magazine
Email Tara

Last fall, it came to light that Chinese hackers had roamed around unnoticed for months inside the network of USIS, the biggest commercial provider of background investigations to the federal US government. In fact, two of the company's biggest customers are the Department of Homeland Security (DHS) and the Office of Personnel Management (OPM).

Onapsis Research Labs analysis finds that the breach most likely utilized an SAP attack vector that Onapsis has been tracking in the wild and warning enterprises about. It marks the first

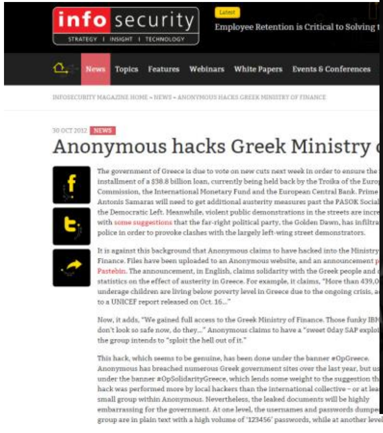
Don't miss the largest info security event of the year!
REGISTER NOW

Report: A Chinese Breach of USIS targeted SAP. Went unnoticed for over six months and compromised over 48,000 employee records of DHS and OPM.

HERSHEY

SAP Security – The New Reality

2012


info security
STRATEGY | INSIGHT | TECHNOLOGY
Latest
Employee Retention is Critical to Solving t

News Topics Features Webinars White Papers Events & Conferences

INFOSECURITY MAGAZINE HOME » NEWS » ANONYMOUS HACKS GREEK MINISTRY OF FINANCE

30 OCT 2012 NEWS

Anonymous hacks Greek Ministry o

The government of Greece is due to vote on new cuts next week in order to ensure the installment of a $38.8 billion loan, currently being held back by the Troika of the Europ Commission, the International Monetary Fund and the European Central Bank. Prime Antonis Samaras will need to get additional austerity measures past the PASOK Social the Democratic Left. Meanwhile, violent public demonstrations in the streets are incre with some suggestions that the far-right political party, the Golden Dawn, has infiltra police in order to provoke clashes with the largely left-wing street demonstrators.

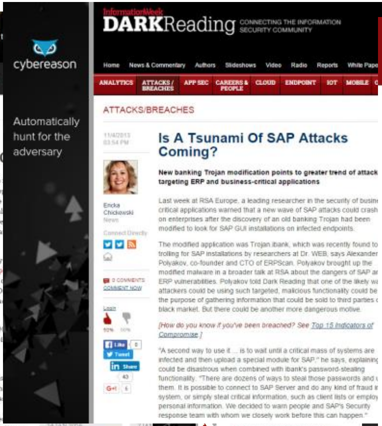
It is against this background that Anonymous claims to have hacked into the Ministry Finance. Files have been uploaded to an Anonymous website, and an announcement p Pastebin. The announcement, in English, claims solidarity with the Greek people and statistics on the effect of austerity in Greece. For example, it claims, "More than 439,0 underage children are living below poverty level in Greece due to the ongoing crisis, a to a UNICEF report released on Oct. 16..."

Now, it adds, "We gained full access to the Greek Ministry of Finance. Those funky IBM don't look so safe now, do they..." Anonymous claims to have a "sweet 0day SAP exploi the group intends to "sploit the hell out of it."

This hack, which seems to be genuine, has been done under the banner #OpGreece. Anonymous has breached numerous Greek government sites over the last year, but us under the banner #OpSolidarityGreece, which lends some weight to the suggestion th hack was performed more by local hackers than the international collective – or at lea small group within Anonymous. Nevertheless, the leaked documents will be highly embarrassing for the government. At one level, the usernames and passwords dumpe group are in plain text with a high volume of '123456' passwords, while at another level one

Anonymous claimed breach to Greek Ministry of Finance using SAP zero-day exploit.

2013


cybereason
Automatically hunt for the adversary

InformationWeek
DARKReading CONNECTING THE INFORMATION SECURITY COMMUNITY

Home News & Commentary Authors Slideshows Video Radio Reports White Pape
ANALYTICS ATTACKS / BREACHES APP SEC CAREERS & PEOPLE CLOUD ENDPOINT IOT MOBILE

ATTACKS/BREACHES

11/4/2013 03:54 PM

Ericka Chickowski
News
Connect Directly

0 COMMENTS
COMMENT NOW

Is A Tsunami Of SAP Attacks Coming?

New banking Trojan modification points to greater trend of attack targeting ERP and business-critical applications

Last week at RSA Europe, a leading researcher in the security of busine critical applications warned that a new wave of SAP attacks could crash on enterprises after the discovery of an old banking Trojan had been modified to look for SAP GUI installations on infected endpoints.

The modified application was Trojan.ibank, which was recently found to trolling for SAP installations by researchers at Dr. WEB, says Alexander Polyakov, co-founder and CTO of ERPScan. Polyakov brought up the modified malware in a broader talk at RSA about the dangers of SAP ar ERP vulnerabilities. Polyakov told Dark Reading that one of the likely wa attackers could be using such targeted, malicious functionality could be the purpose of gathering information that could be sold to third parties c black market. But there could be another more dangerous motive.

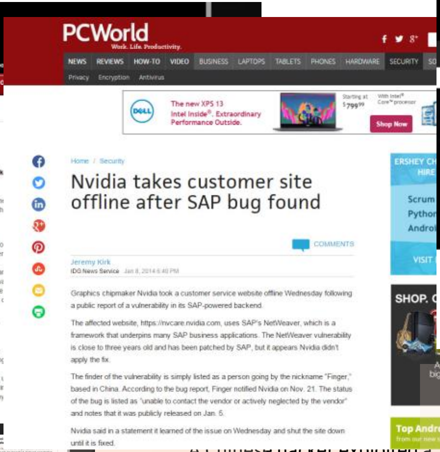
[How do you know if you've been breached? See Top 15 Indicators of Compromise.]

"A second way to use it ... is to wait until a critical mass of systems are infected and then upload a special module for SAP," he says, explaining could be disastrous when combined with ibank's password-stealing functionality. "There are dozens of ways to steal those passwords and u them. It is possible to connect to SAP Server and do any kind of fraud i system, or simply steal critical information, such as client lists or employ personal information. We decided to warn people and SAP's Security response team with whom we closely work before this can happen."

A malware targeting SAP systems discovered in the wild – A "Tsunami of SAP Attacks Coming?"

A malware targeting SAP systems discovered in the wild "Tsunami of SAP Attacks Coming?"

2014


PCWorld
Work. Life. Productivity.

NEWS REVIEWS HOW-TO VIDEO BUSINESS LAPTOPS TABLETS PHONES HARDWARE SECURITY SO
Privacy Encryption Antivirus

Home / Security

Nvidia takes customer site offline after SAP bug found

COMMENTS

Jeremy Kirk
IDG News Service Jan 8, 2014 6:40 PM

Graphics chipmaker Nvidia took a customer service website offline Wednesday following a public report of a vulnerability in its SAP-powered backend.

The affected website, https://nvcare.nvidia.com, uses SAP's NetWeaver, which is a framework that underpins many SAP business applications. The NetWeaver vulnerability is close to three years old and has been patched by SAP, but it appears Nvidia didn't apply the fix.

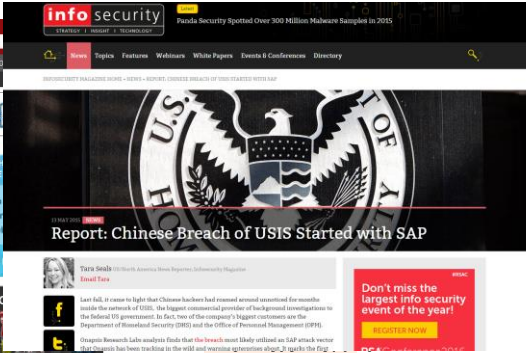
The finder of the vulnerability is simply listed as a person going by the nickname "Finger," based in China. According to the bug report, Finger notified Nvidia on Nov. 21. The status of the bug is listed as "unable to contact the vendor or actively neglected by the vendor" and notes that it was publicly released on Jan. 5.

Nvidia said in a statement it learned of the issue on Wednesday and shut the site down until it is fixed.

A Chinese hacker exploited a vulnerability in a corporate SAP NetWeaver Portal

A Chinese hacker exploited a vulnerability in a corporate SAP NetWeaver Portal.

May 2015


info security
STRATEGY | INSIGHT | TECHNOLOGY
Latest
Panda Security Spotted Over 300 Million Malware Samples in 2015

News Topics Features Webinars White Papers Events & Conferences Directory

INFOSECURITY MAGAZINE HOME » NEWS » REPORT: CHINESE BREACH OF USIS STARTED WITH SAP

13 MAY 2015 NEWS

Report: Chinese Breach of USIS Started with SAP

Tara Seals US/North America News Reporter, Infosecurity Magazine
Email Tara

Last fall, it came to light that Chinese hackers had roamed around unnoticed for months inside the network of USIS, the biggest commercial provider of background investigations to the federal US government. In fact, two of the company's biggest customers are the Department of Homeland Security (DHS) and the Office of Personnel Management (OPM).

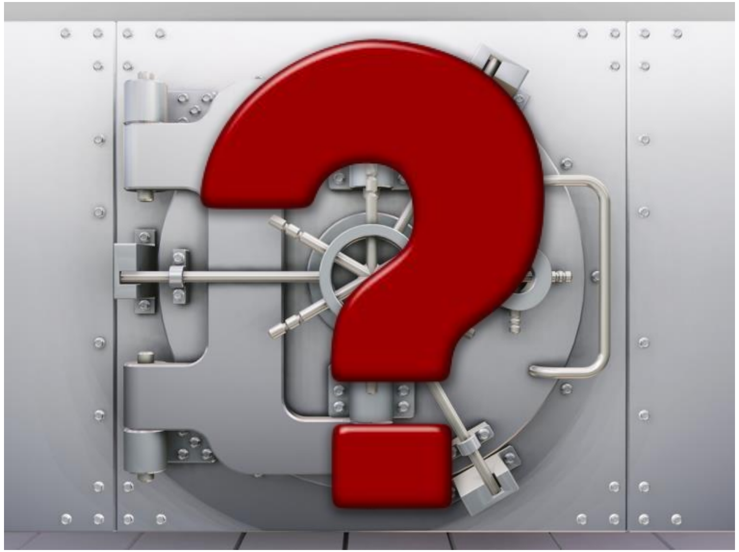
Onapsis Research Labs analysis finds that the breach most likely utilized an SAP attack vector that Onapsis has been tracking in the wild and warning enterprises about. It marks the first

targeted SAP. Went
ed for over six months
mpromised over 48,000
records of DHS and
OPM

Report: A Chinese Breach of USIS targeted SAP. Went unnoticed for over six months and compromised over 48,000 employee records of DHS and OPM.

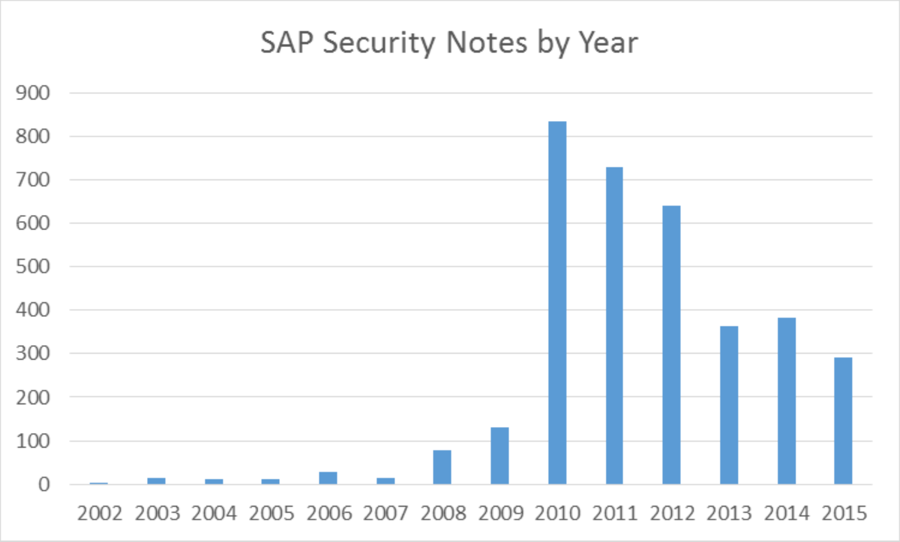
Risk of SAP Insecurity

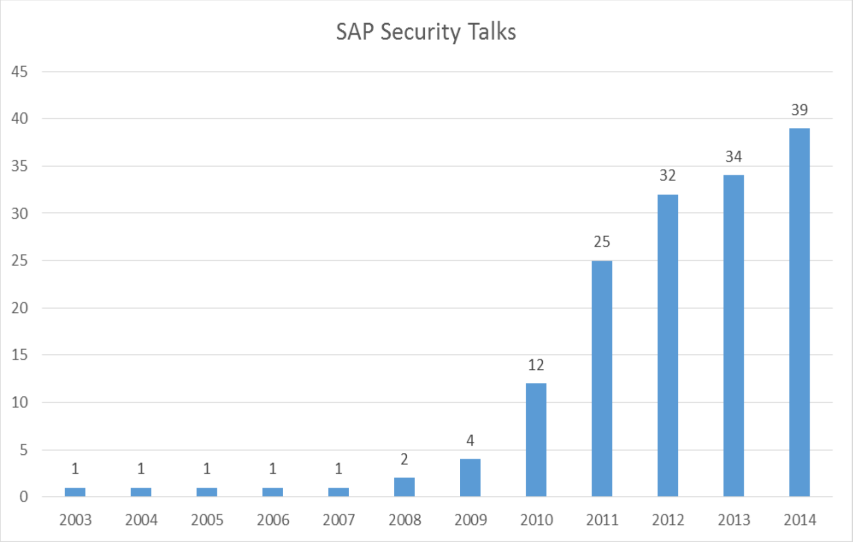
- Risk = Loss (Threat + Vulnerability)
  - Sensitive Information
    - Tangible Assets – Tech IP, Customer/Vendor Data, Financial Records, Personnel Records (PII)
  - Loss is significant
    - 74% of world's financial transactions touch and SAP System
    - 86% of global fortune 500 run SAP software
    - SAP serves > 263,000 customers in 190 countries
    - "The impact of an SAP breach is serious to catastrophic in 92% of organizations" – Ponemon Institute
    - Average cost of breach involving SAP systems if $4.5 Million Dollars



We identify SAP in the scope of our "crown jewels"

Changes in SAP Environment





Security Gap

- SAP Security Team
  - Operations and Infrastructure ERP teams
  - Reactive/Tactical service oriented
  - Success defined by audit and compliance
  - Other risks were out of scope
- Information Security Team
  - Vulnerability Management/Malware Defense
  - Cyber Defense/Incident Response
  - Weak in SAP Knowledge
- Both groups identified the other as responsible making it difficult to pursue an SAP Security Strategy

SO LIKE I WAS SAYING... I WAS AUDITING LAST YEAR'S AUDIT AND I DETERMINED WE NEED ANOTHER AUDIT... PHEW!... LUCKY I CAUGHT THAT...
HUH? IS IT GETTIN HOT IN HERE?

Are our SAP Systems Secure?

- **Common Responses**
  - Patch Management/ System Recommendations
  - Configuration Management/Configuration Validation
  - Early Watch/ SOSS
  - Service Market Place/SAP Security Guides
  - RAL/UCON

  - **End State**
    - SAP Security Team Solely Responsible
    - The unknown?

Transition to Information Security

Speaking a common language

SAP Critical Controls	SANS Top 20
Reduce Attack Surface	3 - Secure Configurations for Hardware and Software on Servers
Gateway Security	10 - Secure Configurations for Network Devices such as Firewall, Routers, and Switches
Protect Default Users	12- Controlled Use of Administrative Privileges
Secure RFC Management	11 - Limitation and Control of Network Services
Secure Communications	3 - Secure Configurations for Hardware and Software on Servers
Password Management / SSO	16 - Account Monitoring and Control
Maintain Security Logs	18 - Incident Response and Mgmnt 14 - Maintenance, Monitoring and Analysis of Audit Logs
Patch Management / SDLC	6 - Application Software Security
System Configurations	3 - Secure Configurations for Hardware and Software on Servers
Access Management	15 - Controlled Access Based on the Need to Know
Secure Code	6 - Application Software Security
Data Classification	1 - Device Inventory 2 - Application / Software Inventory
Critical Access	12- Controlled Use of Administrative Privileges

SAP Security Framework

Vulnerability Management
- Secure communications
- Attack surface
- Gateway
- Default users
- Secure RFCs
- Password Management
- Security Logs
- Configuration
- Patch Management
- System Configuration

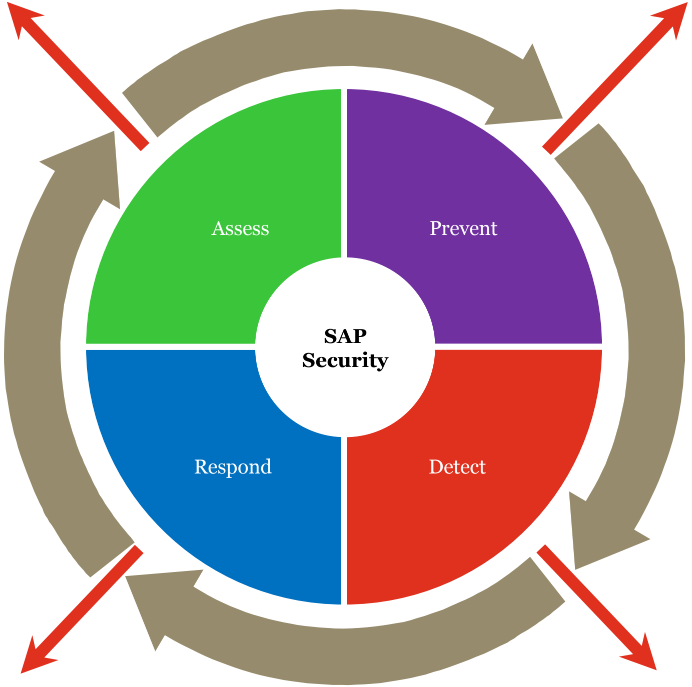
Crown Jewels
- Identification
- Inventory
- Data/Asset Classification

Application Security
- Code reviews
- Architecture

GRC Access Control
- Administrative Privilege
- System administration
- Transport management
- SODs/Fraud Protection

Control Enhancements
Solution Development
Architecture
- Network segmentation

Investigate Issues
Resolve Problems
Incident Response



Role Design
- Production
- Non-production

GRC Access Control / IDM
- Automated workflows w/ integrated risk checks

Governance
- Access attestation
- Role recertification
- Critical access reviews

Control implementation
- Password management
- Default accounts
- Secure comms (SNC, https)
- Gateway security
- RFC security (UCON)
- Configuration standards
- Logging activities

Configuration validation
- Password management
- Default accounts
- Attack surface
- Gateway
- Configuration

Log monitoring
- Network
- System
- Table
- Document
- Security

Onapsis D&R

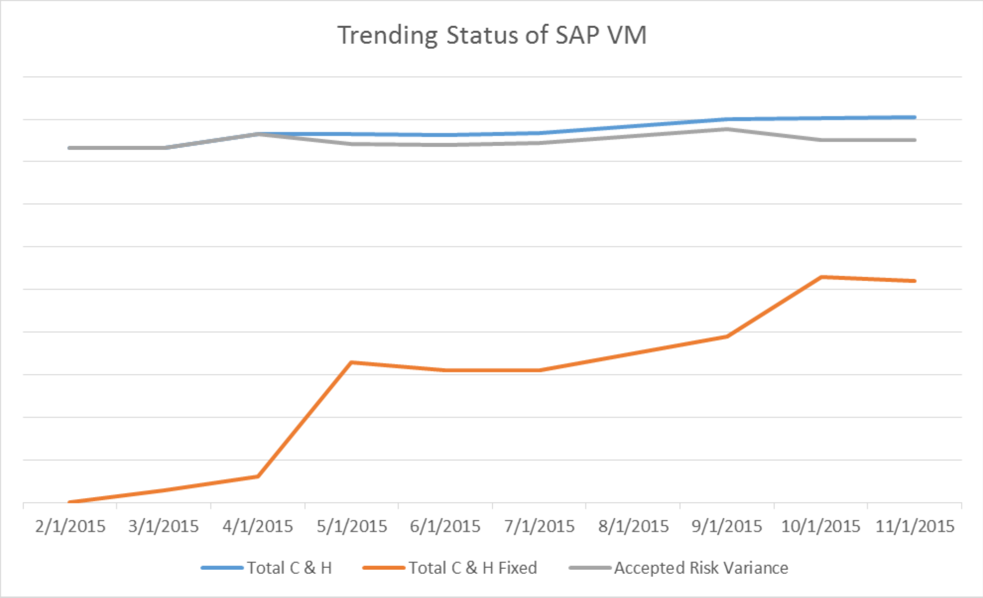
SAP VM Program Overview

SAP VM Program

- POC in 2014 established context
- Leadership support based on business driver of differential protection of critical assets
- Founded program in February of 2015
- Core team members from SAP Security, Basis, and Information Security
- Meet on regular schedule to identify, prioritize, and remediate risk
- Communicate to management on monthly basis
- Founded on external intelligence by partnering with 3rd Party SAP Security Research and Vulnerability Management Company
  - Holistic, Complete, Scalable Intelligence

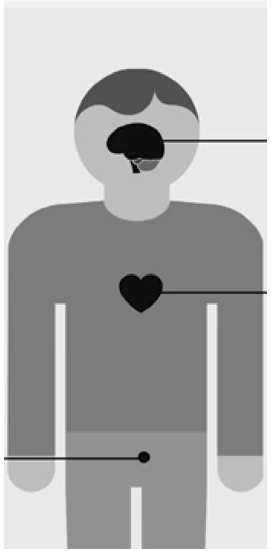
SAP VM Program Impacts

- **Operational Impacts**
  - Identification of previously unrecognized risk
  - > 60% Reduction in 12 months
- **Strategic Impacts**
  - Holistically, completely, and accurately define **risk** posture
  - **Risk** visualization and analysis can be used to communicate up, down, and across the organization
  - Leadership interest and support put risk into business context

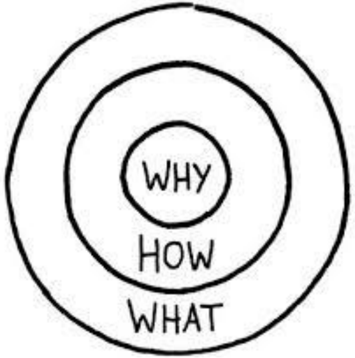


Strategy of "Why"

- **"Why" people buy** -
  - The Four Horsemen: Amazon/Apple/Facebook & Google--Who Wins/Loses
    - Scott Galloway – Clinical Professor of Marketing, NYU Stern



- **Start with "Why" – Simon Sinek**
  - Provide a platform for success and drive purpose

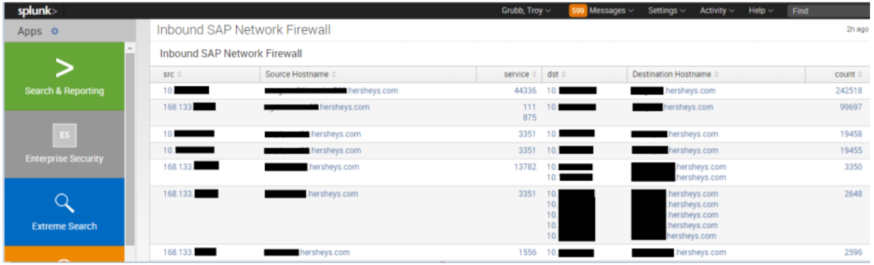


Prevention

- Mitigation and reductions via SAP Vulnerability Management Program
  - Configuration Management
- Configuration Validation
  - 2 Target Systems
    - ZSEC - Alerting
    - ZSECGOLD – Gold client
- Patch Management
- System Recommendations
  - Used in combination with ConfVal for new system implementations
- New Standards for new system implementations
  - UCON, RAL, Network Segmentation

Detection and Response

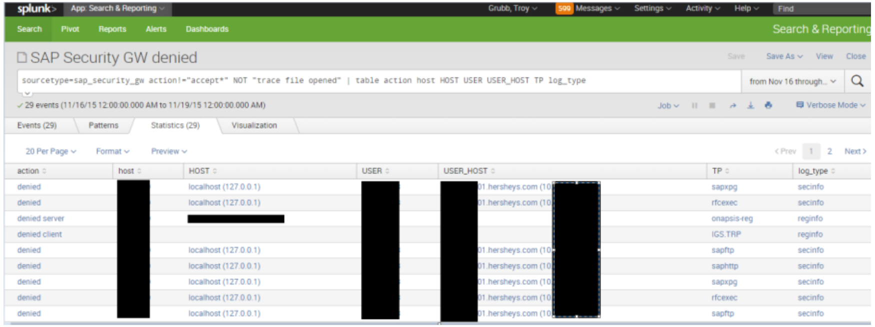
- Configuration Validation
- Log Monitoring/Alerting
- Splunk
  - SAP Audit Logs
  - SAP ICM logs
  - SAP Gateway Logs
  - Enterprise Firewall Logs
- IDS Signatures
- SAP RAL
  - Read Access Logging
- Expanded partnership with 3rd party to provide scale



Inbound SAP Network Firewall

Inbound SAP Network Firewall

src	Source Hostname	service	dst	Destination Hostname	count
10.[redacted]	[redacted]hersheys.com	44336	10.[redacted]	[redacted]hersheys.com	242518
168.133.[redacted]	[redacted]hersheys.com	111 875	10.[redacted]	[redacted]hersheys.com	99697
10.[redacted]	[redacted]hersheys.com	3351	10.[redacted]	[redacted]hersheys.com	19458
10.[redacted]	[redacted]hersheys.com	3351	10.[redacted]	[redacted]hersheys.com	19455
168.133.[redacted]	[redacted]hersheys.com	13782	10.[redacted] 10.[redacted]	[redacted]hersheys.com hersheys.com	3350
168.133.[redacted]	[redacted]hersheys.com	3351	10. 10. 10. 10. 10.[redacted]	[redacted]hersheys.com hersheys.com hersheys.com hersheys.com hersheys.com	2648
168.133.[redacted]	[redacted]hersheys.com	1556	10.[redacted]	[redacted]hersheys.com	2596



SAP Security GW denied

```
sourcetype=sap_security_gw action!="accept*" NOT "trace file opened" | table action host HOST USER USER_HOST TP log_type
```

✓ 29 events (11/16/15 12:00:00.000 AM to 11/19/15 12:00:00.000 AM)

action	host	HOST	USER	USER_HOST	TP	log_type
denied	[redacted]	localhost (127.0.0.1)	[redacted]	[redacted]01.hersheys.com (10[redacted]	sapxpg	secinfo
denied	[redacted]	localhost (127.0.0.1)	[redacted]	[redacted]01.hersheys.com (10[redacted]	rfcexec	secinfo
denied server	[redacted]	[redacted]	[redacted]	[redacted]	onapsis-reg	reginfo
denied client	[redacted]		[redacted]	[redacted]	IGS.TRP	reginfo
denied	[redacted]	localhost (127.0.0.1)	[redacted]	[redacted]01.hersheys.com (10[redacted]	sapftp	secinfo
denied	[redacted]	localhost (127.0.0.1)	[redacted]	[redacted]01.hersheys.com (10[redacted]	saphttp	secinfo
denied	[redacted]	localhost (127.0.0.1)	[redacted]	[redacted]01.hersheys.com (10[redacted]	sapxpg	secinfo
denied	[redacted]	localhost (127.0.0.1)	[redacted]	[redacted]01.hersheys.com (10[redacted]	rfcexec	secinfo
denied	[redacted]	localhost (127.0.0.1)	[redacted]	[redacted]01.hersheys.com (10[redacted]	sapftp	secinfo

“Apply” Slide

- Identify your business critical applications and who is responsible for system security
- Bridge the gap between SAP Security and Information Security teams
- Review the maturity and efficiency of your SAP Control Framework and build/redesign your SAP control framework based on risk
- Don’t attempt to scale to fix all issues but instead work to influence others around you but showing progress towards realistic goals
- Transfer the risk by deploying a holistic and complete assessment and communication capability

Q&A

- Troy Grubb, Information Security Manager, GRC and SAP Security
- tgrubb@hersheys.com
- @TroyRGrubb