Security in knowledge

If I want a perfect cyberweapon, I'll target ERP

Alexander Polyakov / ERPScan

RSA CONFERENCE
EUROPE 2013

Session ID: ADS-R07

Session Classification: Advanced

Intro

- I hate “CYBER” talks and all that buzz
- I usually do more technical presentations
- But everyone talks about it, why skip this area?
- My research is about Business Applications and ERP systems

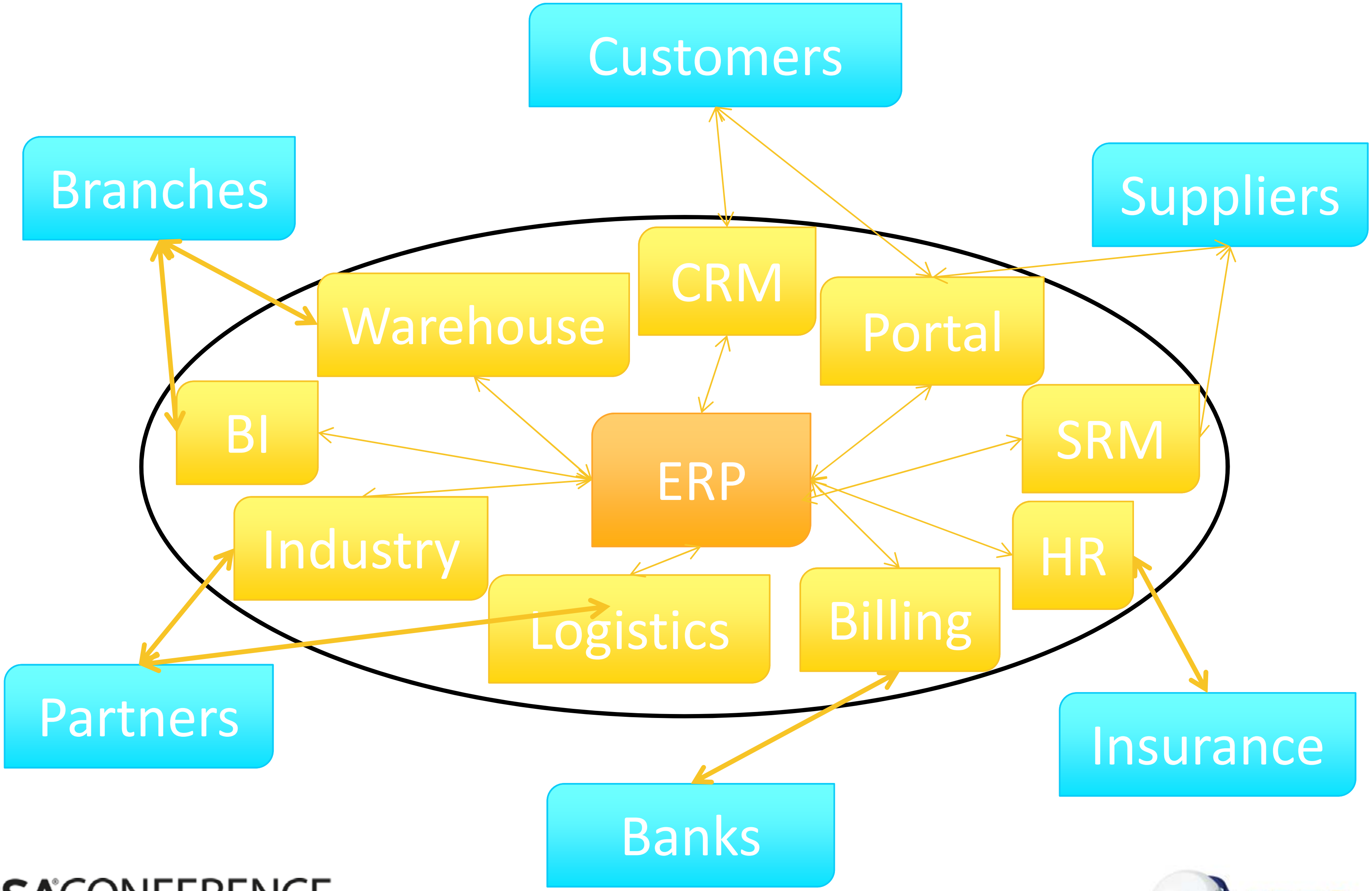
Agenda

- Intro
- Big companies and critical systems
- What used to happen?
- How easy is that?
- What can happen?
- Forensics
- What can we do?
- Conclusion

Big companies

- Oil and Gas
- Manufacturing
- Logistics
- Financials
- Nuclear
- Retail
- Telecommunication
- etc.

What do they look like?



Are business applications popular?

SAP

- More than 248,500 customers in 188 countries
- 86 % of Forbes 500

Oracle

- 100 % of Fortune 100

Microsoft

- More than 300000 businesses worldwide choose Microsoft Dynamics ERP and CRM software

What can happen?

- Espionage
  - Stealing financial information
  - Stealing corporate secrets
  - Stealing supplier and customer lists
  - Stealing HR data
- Sabotage
  - Denial of service
  - Modification of financial reports
  - Access to technology network (SCADA) by trust relations
- Fraud
  - False transactions
  - Modification of master data

AutoCAD virus (Industrial espionage)

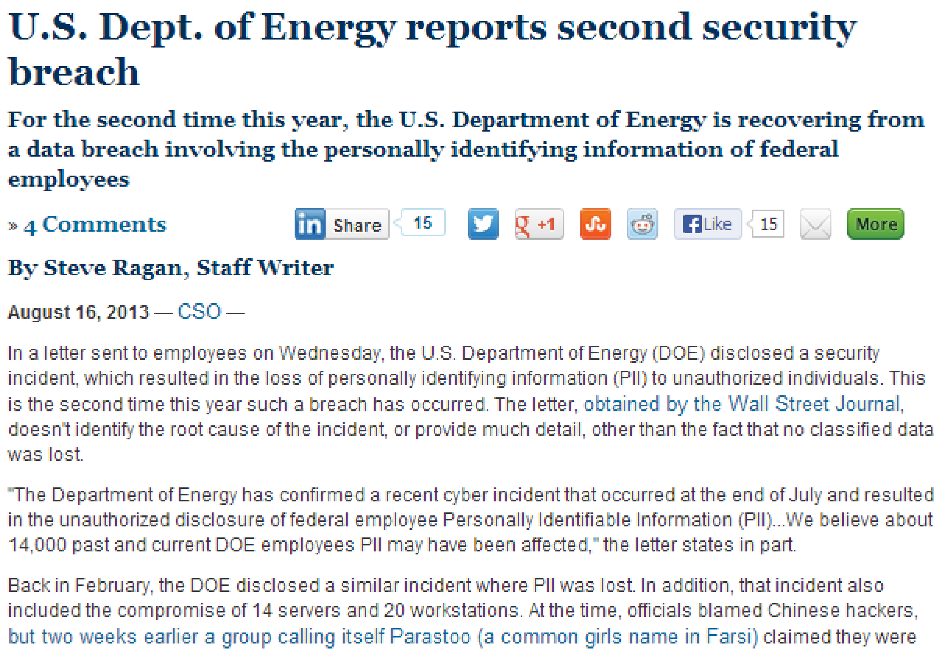
- AutoCAD virus
- Stealing critical documents
- Sending them potentially to China
  - http://www.telegraph.co.uk/technology/news/9346734/Espionage-virus-sent-blueprints-to-China.html

PeopleSoft vulnerabilities (Sabotage)

- Presented at BlackHat USA
- Old and new issues
- The old one was a buffer overflow in a login page
- Over 500 systems can be found by googling
- New issues ranged from information disclosure to unauthorized system access
- Potential to steal the data of 20 million customers

US Department of Energy breached

- Sabotage
- Real example of stealing 14000 records
- Target: HR system (maybe PeopleSoft)
- Unauthorized disclosure of personally identifiable information about federal employees



U.S. Dept. of Energy reports second security breach

For the second time this year, the U.S. Department of Energy is recovering from a data breach involving the personally identifying information of federal employees

» 4 Comments

By Steve Ragan, Staff Writer

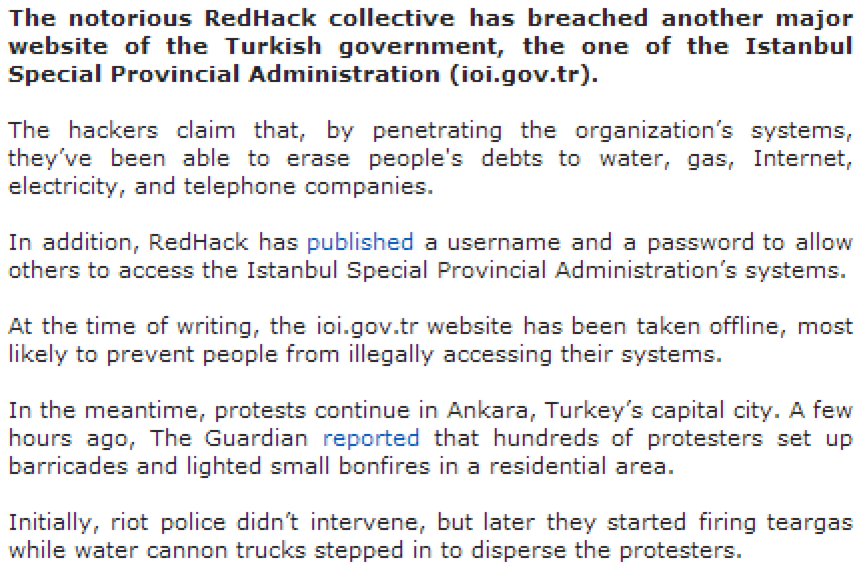
August 16, 2013 — CSO —

In a letter sent to employees on Wednesday, the U.S. Department of Energy (DOE) disclosed a security incident, which resulted in the loss of personally identifying information (PII) to unauthorized individuals. This is the second time this year such a breach has occurred. The letter, obtained by the Wall Street Journal, doesn't identify the root cause of the incident, or provide much detail, other than the fact that no classified data was lost.

"The Department of Energy has confirmed a recent cyber incident that occurred at the end of July and resulted in the unauthorized disclosure of federal employee Personally Identifiable Information (PII)...We believe about 14,000 past and current DOE employees PII may have been affected," the letter states in part.

Back in February, the DOE disclosed a similar incident where PII was lost. In addition, that incident also included the compromise of 14 servers and 20 workstations. At the time, officials blamed Chinese hackers, but two weeks earlier a group calling itself Parastoo (a common girls name in Farsi) claimed they were

Istanbul Provincial Administration



The notorious RedHack collective has breached another major website of the Turkish government, the one of the Istanbul Special Provincial Administration (ioi.gov.tr).

The hackers claim that, by penetrating the organization's systems, they've been able to erase people's debts to water, gas, Internet, electricity, and telephone companies.

In addition, RedHack has published a username and a password to allow others to access the Istanbul Special Provincial Administration's systems.

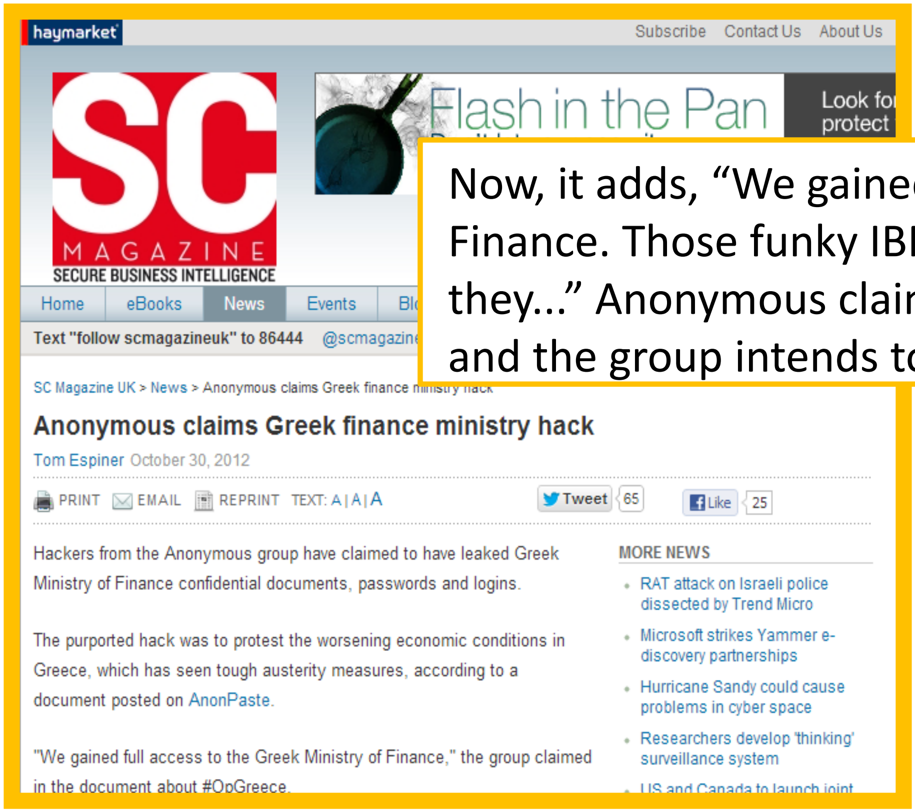
At the time of writing, the ioi.gov.tr website has been taken offline, most likely to prevent people from illegally accessing their systems.

In the meantime, protests continue in Ankara, Turkey's capital city. A few hours ago, The Guardian reported that hundreds of protesters set up barricades and lighted small bonfires in a residential area.

Initially, riot police didn't intervene, but later they started firing teargas while water cannon trucks stepped in to disperse the protesters.

- Unauthorized disclosure of personally identifiable information about federal employees
- Debts of people erased

Media gossip about a potential Anonymous attack



haymarket

Subscribe Contact Us About Us

SC MAGAZINE

SECURE BUSINESS INTELLIGENCE

Flash in the Pan

Look fo
protect

Home eBooks News Events Bl

Text "follow scmagazineuk" to 86444 @scmagazine

SC Magazine UK > News > Anonymous claims Greek finance ministry hack

Anonymous claims Greek finance ministry hack

Tom Espiner October 30, 2012

PRINT EMAIL REPRINT TEXT: A | A | A Tweet 65 Like 25

Hackers from the Anonymous group have claimed to have leaked Greek Ministry of Finance confidential documents, passwords and logins.

The purported hack was to protest the worsening economic conditions in Greece, which has seen tough austerity measures, according to a document posted on AnonPaste.

"We gained full access to the Greek Ministry of Finance," the group claimed in the document about #OpGreece.

MORE NEWS

- RAT attack on Israeli police dissected by Trend Micro
- Microsoft strikes Yammer e-discovery partnerships
- Hurricane Sandy could cause problems in cyber space
- Researchers develop 'thinking' surveillance system
- US and Canada to launch joint

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 attack has not been confirmed by the customer nor by the police authorities in Greece investigating the case. SAP does not have any indication that it happened.*

Fraud

"There are several different methods used by vendors to defraud a company. Some of the more common methods include:

- Invoice company for a greater number of hours than worked
- Ghost employees of the vendor
- Vendor employees billed at amounts higher than contract rate
- Vendor employees billed at higher job classification than actual work performed (skilled vs. non-skilled labor rates)
- Invoice company for incorrect equipment or materials charges
- Vendor charges for equipment not needed or used for the job performed
- Vendor charges for materials not used or materials are for the personal benefit of company employee
- Vendor charges for equipment or material at higher prices than allowed by the contract
- Invoice company incorrectly for other services
- Vendor charges for services performed where work is not subject to audit clause
- Vendor charges include material purchases from or for work performed by related companies at inflated prices"

http://www.padgett-cpa.com/insights/articles/fraud-risks-oil-and-gas-industry

Fraud

- The Association of Certified Fraud Examiners (**ACFE**) survey showed that US organizations lose an estimated **7**% of annual revenues to fraud.
- Real examples that we met:
  - Salary modification
  - Material management fraud
  - Mistaken transactions

Fraud

- PWC survey: out of 3000 organizations in 54 countries, 30 % were the victims of economic crime within the previous 12 months
- Average loss per organization for fraud: $ 500k + collateral damage
- Asset misappropriation: 83%
- Accounting fraud: 33%

Internet-Trading virus (Fraud)

- Internet-Trading virus (Fraud)
  - Ranbys modification for QUIK
  - trojan-spy.win32.**broker.j** for QUIK (stealing keys)
  - http://www.welivesecurity.com/2012/12/19/win32spy-ranbyus-modifying-java-code-in-rbs/
  - http://www.securitylab.ru/news/439695.php

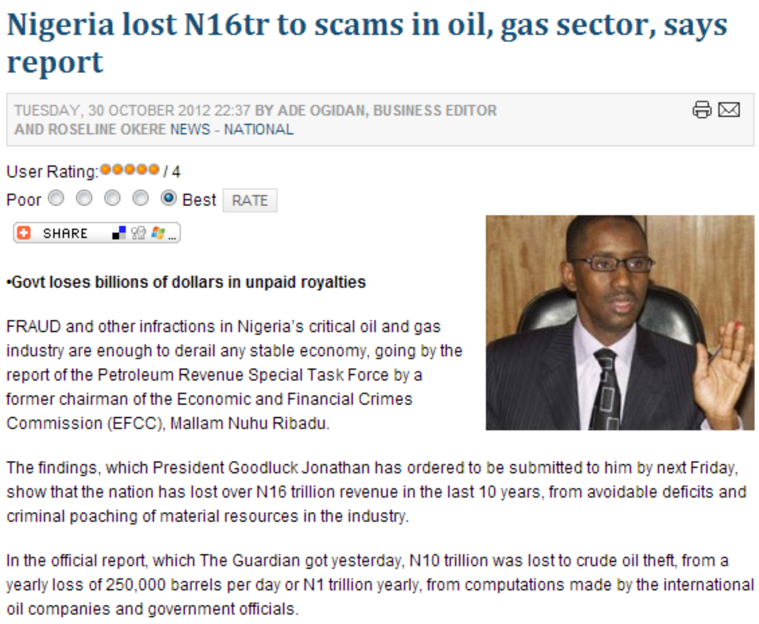
Project Mayhem (Fraud)

“Hacker could manipulate financial data and change entries to move funds to an outside account:

- alter the remittance address on vendor records
- create a new vendor and manual check entry
- change general ledger accounting records
- increase customer credit limit
- credit the balance in a customer account in order to get a refund”

http://www.csoonline.com/article/723430/researchers-show-proof-of-concept-microsoft-erp-hack

Fraud in Oil And Gas



Nigeria lost N16tr to scams in oil, gas sector, says report

TUESDAY, 30 OCTOBER 2012 22:37 BY ADE OGIDAN, BUSINESS EDITOR AND ROSELINE OKERE NEWS - NATIONAL

User Rating: ●●●●● / 4

Poor ○ ○ ○ ○ ● Best RATE

•Govt loses billions of dollars in unpaid royalties

FRAUD and other infractions in Nigeria's critical oil and gas industry are enough to derail any stable economy, going by the report of the Petroleum Revenue Special Task Force by a former chairman of the Economic and Financial Crimes Commission (EFCC), Mallam Nuhu Ribadu.

The findings, which President Goodluck Jonathan has ordered to be submitted to him by next Friday, show that the nation has lost over N16 trillion revenue in the last 10 years, from avoidable deficits and criminal poaching of material resources in the industry.

In the official report, which The Guardian got yesterday, N10 trillion was lost to crude oil theft, from a yearly loss of 250,000 barrels per day or N1 trillion yearly, from computations made by the international oil companies and government officials.

"FRAUD and other infractions in Nigeria's critical oil and gas industry are enough to derail any stable economy, going by the report of the Petroleum Revenue Special Task Force by a former chairman of the Economic and Financial Crimes Commission (EFCC), Mallam Nuhu Ribadu"

What can happen?

How to make it more “Cyber/Danger”

- Breach + worm
- Multiple attacks of the same type
- Against one country

What can happen next?

- Just imagine what could be done by breaking:
  - One ERP system
  - All business applications of a company
  - All ERP systems in a particular country

How easy is that?

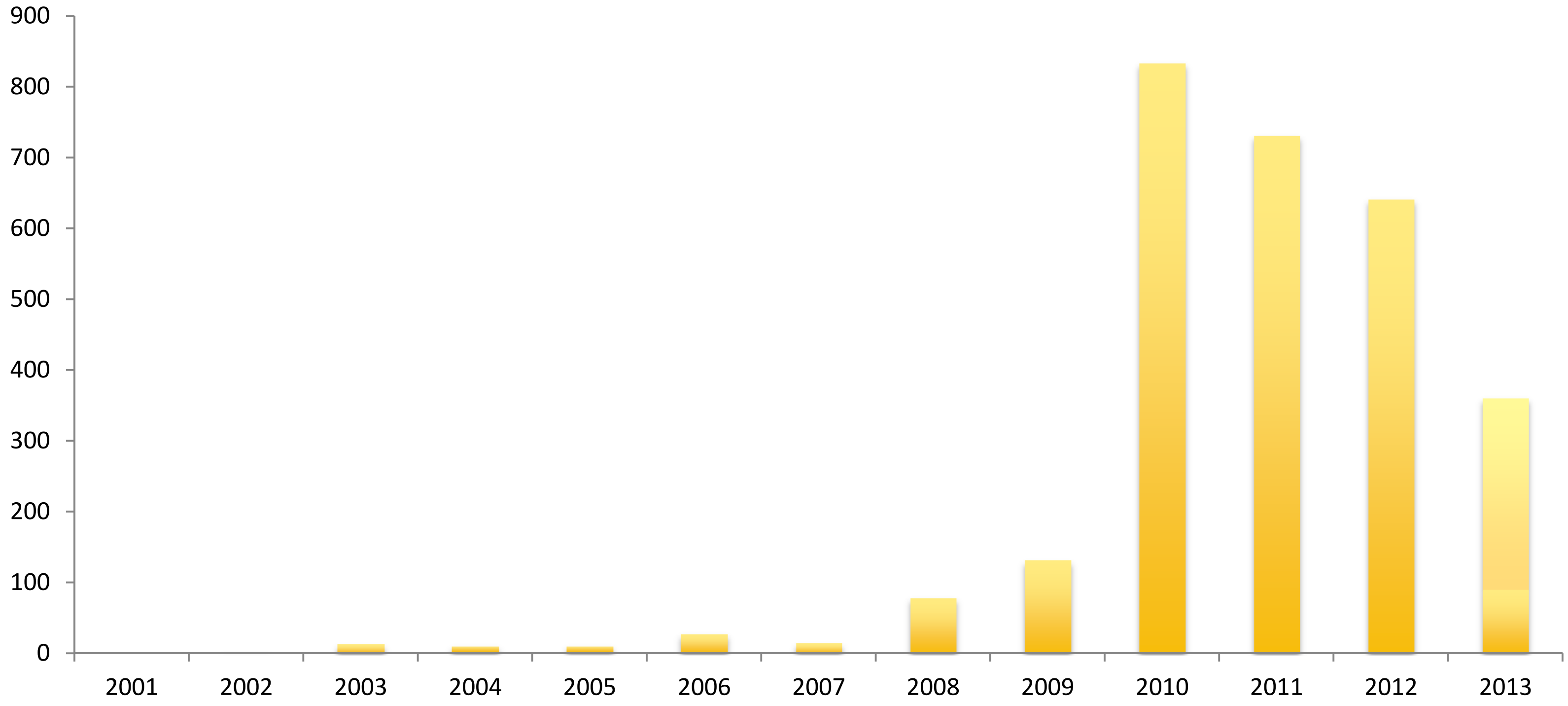
Ease of development

- Price of vulnerability is low
- Patching it is a nightmare
- Vaporization is easy
- Interconnection is high
- Availability via the Internet

Price of vulnerability

- Price of typical vulnerabilities in Flash and browsers goes higher
- Security of applications and OS is increasing
- It is much easier to find an architecture issue in ERP
- 2000 vulnerabilities closed only by SAP within 3 years
- And this kind of issue will work for years!

SAP security notes by year



More than 2600 in total

Patching them is a nightmare

- You need to stop the processes
- Sometimes, you need to update multiple parts
- Examples of huge architectural issues in:
  - Microsoft Dynamics
  - Oracle JDE
  - SAP SDM

Microsoft Dynamics authentication

- Dynamics security = only visual restrictions of fat client
- All users have rights in corporate databases
- The only obstruction: ~~im~~possible to connect to the SQL server directly
- Reverse engineering to understand the password "encryption" algorithm
- Create a tool
- Every user can become an Administrator
- **NO PATCH! Only new architecture can help (but there is none)**

Oracle JD Edwards authentication

- All the security of JD Edwards relies on the visual restrictions of the fat client
- In fact, all users have rights to corporate data because the client connects using a special JDE account
- Then the username and password is checked on the fat client
- User can connect directly to database using a JDE account and modify their rights on table level
- Every user can become an Administrator
- **NO PATCH! Only moving to 3-tier architecture**

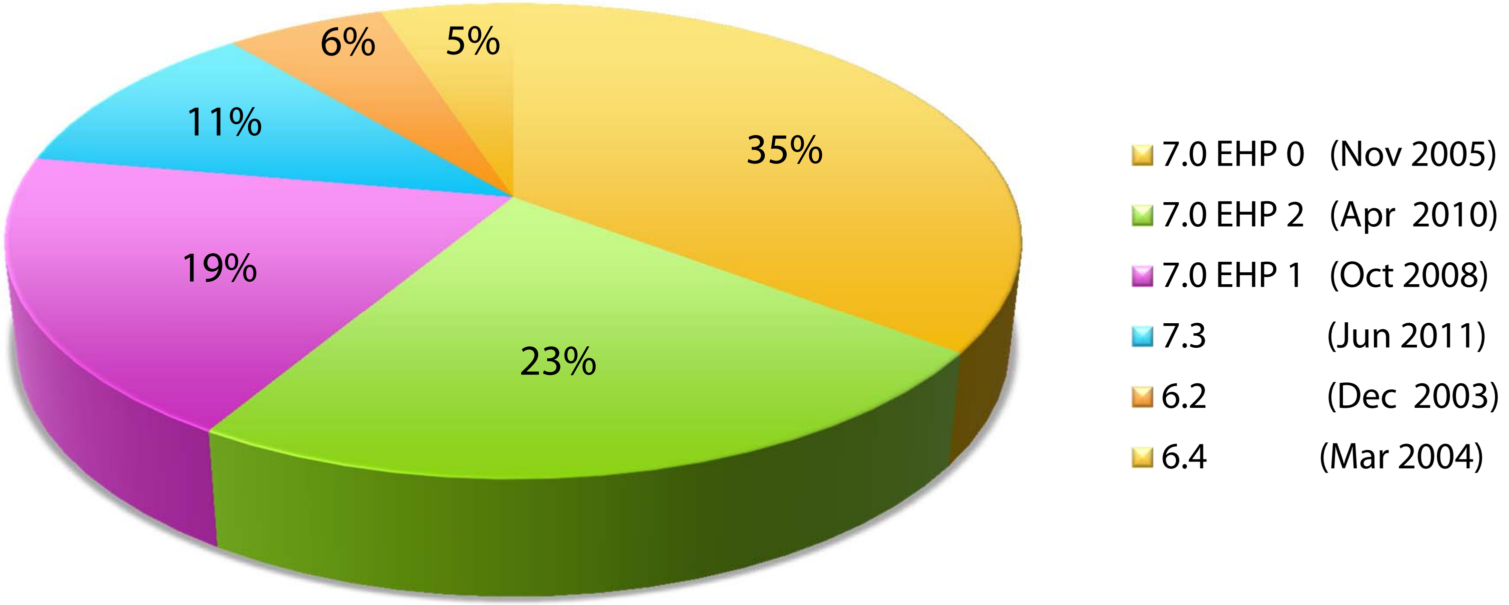
SAP SDM authentication

- Authentication is done by password hash
- It means that PassTheHash is possible
- First, hash can be simply sniffed, so it is like authenticating using a clear password
- Second, hashes are stored in an OS file so they can be accessed by using other vulnerabilities
- After getting a hash, it is possible to upload any backdoor into SAP
- To patch it:
  - Modify client and server at the same time
  - Install SAP Note 1724516

DEMO

Patching is a nightmare

NetWeaver ABAP versions by popularity



The most popular release (35 %, previously 45 %) is still NetWeaver 7.0, and it was released in 2005!

Special payload is not needed

- Remember Verb Tampering user creation?
- Just one request, and you are inside the system
- Another request, and you are the admin
- Then you can do whatever you want with simple HTTP requests
- If it is just a technical system, you can jump to connected systems

Systems are highly connected

- Systems are highly connected with each other by trust relations
- Even different companies are connected by ESB systems
- Remember SSRF?
  - http://cwe.mitre.org/data/definitions/918.html
  - Second place in the top 10 web application techniques of 2012
  - Allows bypassing firewall restrictions and directly connecting to protected systems via connected systems

Business applications on the Internet

- Companies have Portals, SRMs, CRMs remotely accessible
- Companies connect different offices by ESB
- SAP users are connected to SAP via SAProuter
- Administrators open management interfaces to the Internet for remote control

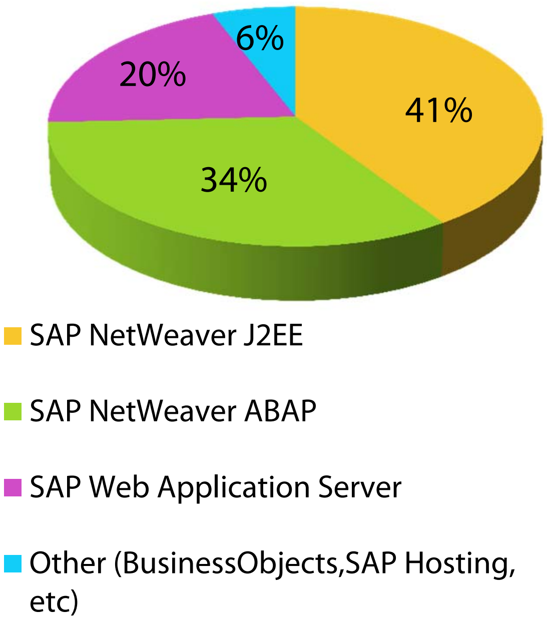
Business applications on the Internet

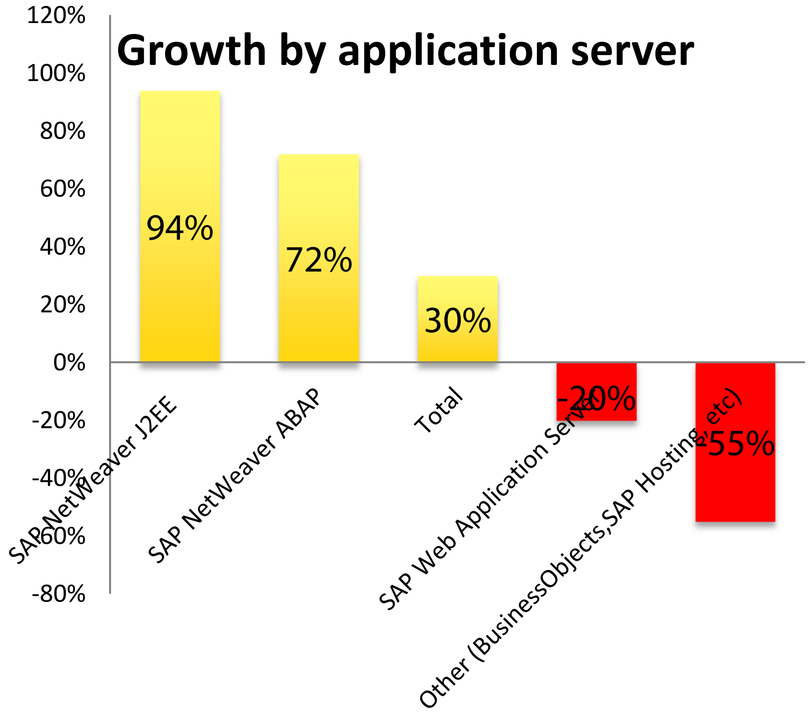
SAP HTTP services can be easily found on the Internet:

- inurl:/irj/portal
- inurl:/IciEventService sap
- inurl:/IciEventService/IciEventConf
- inurl:/wsnavigator/jsps/test.jsp
- inurl:/irj/go/km/docs/

Shodan scan

A total of 3741 server with different SAP web applications was found





SAProuter

- Special application proxy
- Transfers requests from the Internet to SAP (and not only)
- Can work through VPN or SNC
- Almost every company uses it for connecting to SAP to download updates
- Usually listens to port 3299
- Internet accessible (Approximately 5000 IPs)
- http://www.easymarketplace.de/saprouter.php

SAProuter: known issues

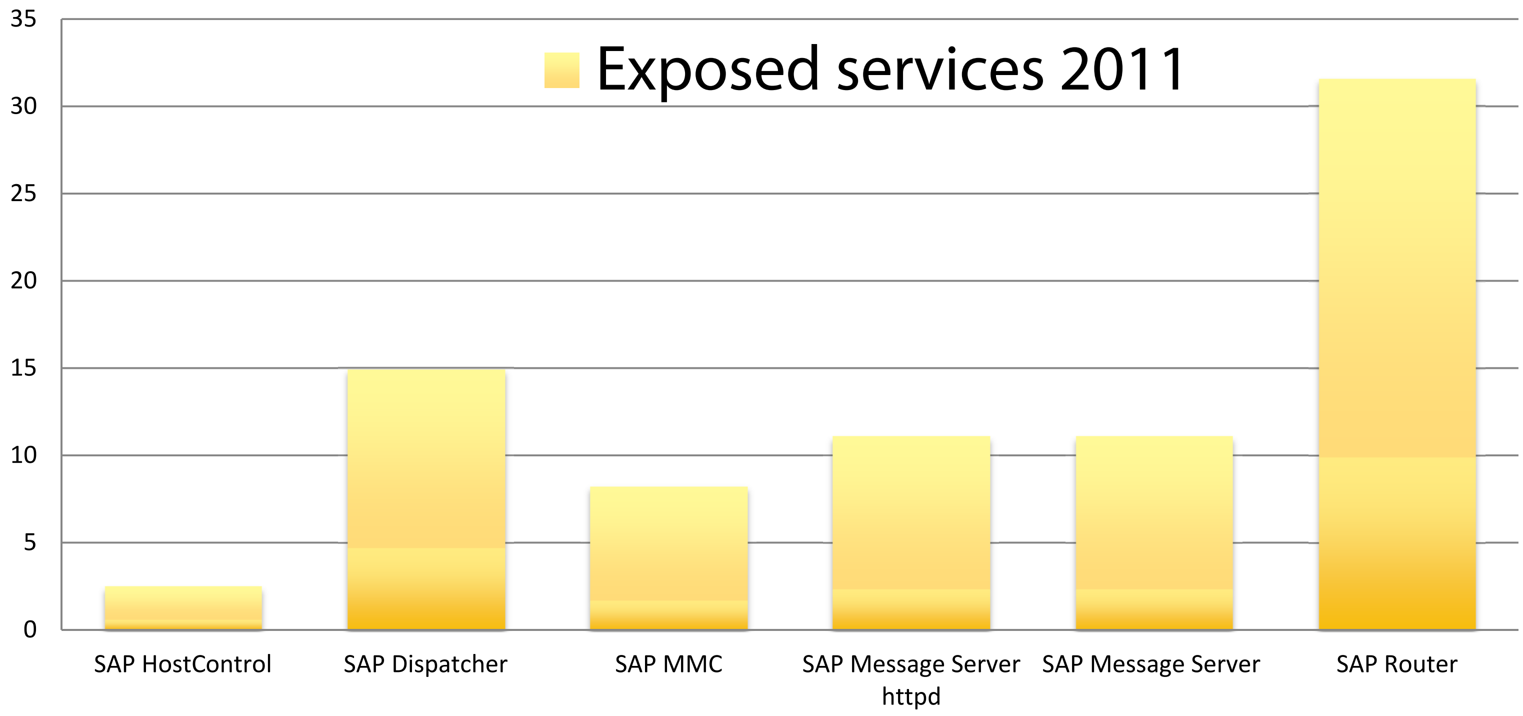
- Absence of ACL: 15%
  - Possible to proxy any request to any internal address
- Information disclosure about internal systems: 19%
  - Denial of service by specifying many connections to any of the listed SAP servers
  - Proxy requests to internal network if there is no ACL
- Insecure configuration, authentication bypass: 5%
- **Heap corruption vulnerabilities: lots of them!**
- To secure SAProuter, use SAP Note 1895350

DEMO

Port scan results

- Are you sure that only the necessary SAP services are exposed to the Internet?
- We were not
- In 2011, we ran a global project to scan all of the Internet for SAP services
- It is not completely finished yet, but we have the results for the top 1000 companies
- We were shocked when we saw them first

Port scan results



Listed services should not be accessible from the Internet

Why are there not many **public** examples of breaches if the situation is so bad?

Examples

- Fraud – very popular inside companies but you see only some incidents
- Sabotage – at this moment, it may be easier to DDoS than DoS, but we'll see
- Espionage – here is what we don't see a lot of, because it is designed to be unseen. You will never know about it, especially if you don't enable logging

SAP security forensics

- There is not so many info in public
- Companies are not interested in publishing compromise
- But the main problem is:
  - **How can you be sure that there was no compromise?**
  - Only 10% of systems have Security Audit Log enabled
  - Only few of them analyze those logs
  - And much less do central storage and correlation

** Based on the assessment of over 250 servers of companies that allowed us to share results*

Percent of enabled log options

ICM log icm/HTTP/logging_0	70%
Security audit log in ABAP	10%
Table access logging rec/client	4%
Message Server log ms/audit	2%
SAP Gateway access log	2%

** Based on the assessment of over 250 servers of the companies that allowed us to share results*

Weapons

Weapons

- DoS for bank
- Fraud for oil, then manipulate prices and economy
- Multiple money transfer fraud

Prevention

EAS-SEC.org

EAS-SEC

- Resource which combines
  - Guidelines for assessing enterprise application security
  - News and articles about enterprise application security

EAS-SEC guidelines

1. Lack of patch management
2. Default passwords
3. Unnecessary enabled functionality
4. Remotely enabled administrative services
5. Insecure configuration
6. Unencrypted communications
7. Internal access control and SoD
8. Insecure trust relations
9. Monitoring of security events

Conclusion

It is possible to be protected from almost all those kinds of issues, and we are working hard to make it secure

Guides

Regular security assessments

Monitoring technical security

Code review

Segregation of duties

EAS-SEC project

Conclusion

Issues are everywhere

but the risks and price

of mitigation are different

Future work

I'd like to thank SAP Product Security Response Team for their great cooperation to make SAP systems more secure. Research is always ongoing, and we can't share all of it today. If you want to be the first to see new attacks and demos, follow us at @erpscan and attend future presentations:

- *November 7-8 ZeroNights (Moscow, Russia)*
- *November 10 G0S (New Delhi, India)*

Questions?

Security in knowledge

#RSAC

RSA CONFERENCE EUROPE 2013

Security in knowledge

Thank you!

Alexander Polyakov

ERPScan

@sh2kerr

a.polyakov@erpscan.com

erpscan.com