

# Enterprise Defense and why you're most likely doing it all wrong





# "SAP has released 3300+ security patches to date. In 2014 alone, 391 were released - averaging 30+/month. Over 46 percent of them were ranked as "high priority".

- Onapsis Research Labs

Source: <u>http://www.onapsis.com/blog/sap-security-advisories-a-preview-of-a-year-in-review-and-future-trends/</u>

Over 95% of the SAP systems we have assessed, were exposed to vulnerabilities that could lead to full compromise of the company's business processes and information. Most vulnerabilities could be exploited **anonymously and remotely.** 

# In most scenarios, anyone that can "ping" an SAP server, can break into it.

BlackHat EU 2012 – "Cyber Attacks & SAP Systems" by Mariano Nunez



- "Our SAP platform is only accessible through internal networks"
  - There is no such thing as an "Internal" Network anymore
  - There are no more "perimeters" (spear-phishing, rough contractors, malicious employees)
  - Many SAP systems are directly connected to the Internet (Web apps, Mobile, cloud-deployments, etc.)

### www.shodanhq.com/search?q=SAP

🔏 SHODAN	SAP	Searc	h
	*	*	
		Results 1 - 10 of about 13332 for SAP	



- "This can only be performed by highly-skilled attackers"
  - Who is the Threat Actor? Most likely an unethical competitor, disgruntled employee, hacktivist, or foreign state.
  - Even script kiddies the information is out there!

SAP R/3 on Oracle: vulnerable Default Installation	-
From: Jochen Hein ( <u>lochen@jochen.org</u> ) Date: 04/27/02	Date: Sat, 27 Apr 2002
Previous message: <u>Trish Lynch: "Response to KF about Listar/Ecartis Vulnerability"</u> Messages sorted by: <u>[date]</u> [ <u>thread]</u> [ <u>subject]</u> [ <u>author]</u> [ <u>attachment]</u>	
To: <u>bugtraq@securityfocus.com</u> From: Jochen Hein < <u>iochen@jochen.org</u> > Date: Sat, 27 Apr 2002 09:06:19 +0200	
SAP R/3 on Oracle: vulnerable Default Installation	
Topic: SAP R/3 on Oracle: vulnerable Default Installation Module: Default Oracle Listener Configuration Announced: 2002-04-27	
Affects: All R/3 Releases using SQL*net V2 (3.x, 4.x, 6.10) Vendor: [1]SAP AG, Walldorf, Germany Vendor-Status: 2002-03-03: Informed 2002-03-05: problem acknowledged	
Synopsis	

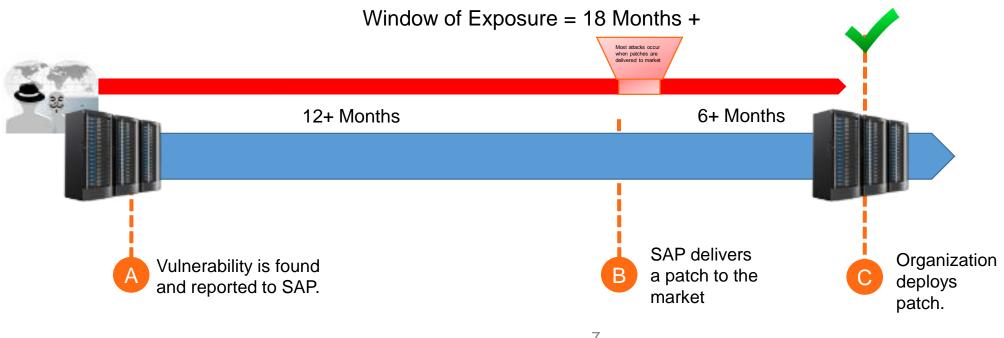
- **o**napsis
- "Our SAP system has never been hacked"
  - Most companies do not enable (security) logging due to the <u>negative impact</u> on performance
  - Traditional SIEMs or log correlators won't help. Even with the standard Security Audit features enabled, certain type of cyber security attacks can't be detected through log files.
  - Furthermore, several vulnerabilities have been discovered that could be used for anti-forensics purposes

### So ... the most honest answer is probably: "we don't know"

© 2015 Onapsis, Inc. All Rights Reserved

# What Is the Probability? Killing Some Myths O onapsis

- "We are applying SAP patches regularly"
  - Most patches that are applied are "functional", not security-related.
  - Applying security patches without the proper analysis introduces operational risk (more sensitive in business-critical platforms!).
  - Another risk: <u>The Window of Vulnerability</u>



NEWS

New banking Trojar

Ericka Chickowski

See more from Erick

SAP GUI installations on infected endpoints

### 2012



### Anonymous claimed breach and stated: "A sweet Oday SAP exploit is in our hands and oh boy we're gonna sploit the hell out of it."

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

2013

Connect directly with Ericka: 🌄 🛐 Bio | Contac

Is A Tsunami Of SAP Attacks Coming?

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

The modified application was Trojan. bank, which was recently found to be trolling for SAP installations by researched

The monthe application was replanitoring interfusion of the second replanet of the second replanet in the second replanet was received at Dr. WEB, says Alexander Polyakov, co-founder and CTO of ERPScan. Polyakov told Dark Reading that one of the 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 dan

Follow Dark Reading

Dark Reading R

How Cybercrimin Knowing your enemy is t against him. In this Dark

examine the world of cy

recommend what enter their data and computir of an ever-growing and

A Data Breach E

Cyber attackers of all typ

this special compendium coverage, we offer a lool

recent breaches, includ

and how they affected

The 8 Most Com

motivated, nation-state continue to hammer av masse, and once in a

💽 🕇 🖬

F 🔽

- 🕰

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

### 2014

onapsis



© 2015 Onapsis, Inc. All Rights Reserved

### What Could Be the Impact?



### "IF OUR COMPANY'S SAP SYSTEM IS BREACHED, IT WILL COST US \$22 MILLION PER MINUTE."

**CISO OF FORTUNE 500 COMPANY** 





# **Attack Scenarios**

### **Attack Scenarios**





HTTP Request with Verbitampering

and Step

Login with created

SAP CTC service

**XAP Portal with busines** 

SAP OFFICIAL

SAP J2EE

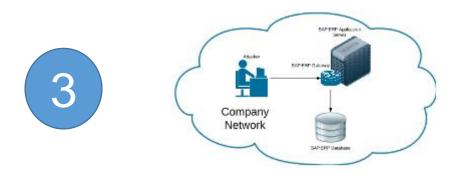
exposed to internet

#### **Pivoting between SAP systems:**

Pivot from a system with lower security (Development or QA system) to a critical system (Production system), to execute SAP remote function modules in the destination system

#### **Customer and Supplier Portal Attacks:**

Create users in the SAP J2EE User Management Engine using the CTC servlet, by exploiting a vulnerability through HTTP verb tampering, and obtaining access to the SAP Portal business information (and internal systems).



#### Attack on SAP services configuration:

Execute Operating System commands under the privileges of the user <sid>adm by exploiting vulnerabilities in the SAP Gateway. Get and potentially modify credit card information stored in the SAP database.

# **Attack Scenario 1**



1. Attacker connecting to non-prod systems (Dev/QA)

### 2. List of RFC destinations and its properties

Configuration of RFC Connections	Data Browser: Table RFCDES Select Entries 1			
় Generate RFC Callback Positive Lists				
CO RFC callback check not secure	Table: RFCDES Displayed Fields: 15 of 20	Fixed Columns:	List Width 1023	
	Destination	Connection Type	e Options	
IFC Connections     Ty     PL     Comment       ABAP Connections     3     3     3		3	H=192.168.0.83, S=00, M=800, U=ZONAPSIS, Y=2, h=2, z=-2, v=%_PWD, W=Y, B=N, C=N, E=	
B DM1 3 - DYNAMIC_DEST_CALLBACK_WHITELIST 3 - Callback Positive List for Dynamic Destinations G74 3 - SM59	SE16 - RFCDE	S		

3. Attacker goes to transaction SE37 and leverages a destination and "data read" function module.

RFC target sys:	DM1	WA		
		 800AMEX37000000000002	John Taylor	200501019999123101
Import parameters	Value	800MC 51000000000008	John Taylor	200306019999123101
Import parameters	Value	 800MC 51200000000004	Uncle John's Bagel Factory	2008022899991231
OUEDV TABLE	VCNUM	 800MC 512000000100002	Carpenter Works	2008022899991231
QUERY_TABLE	LACNOW	 800VISA410000000000000	Andrew Sands	200307022005053101
DELIMITER		800VISA4111111111111111	Alex Lynch	200809012008123101
NO_DATA		800VISA4200000000000000	Tech Inc.	200411192007123101
ROWSKIPS ROWCOUNT	0			

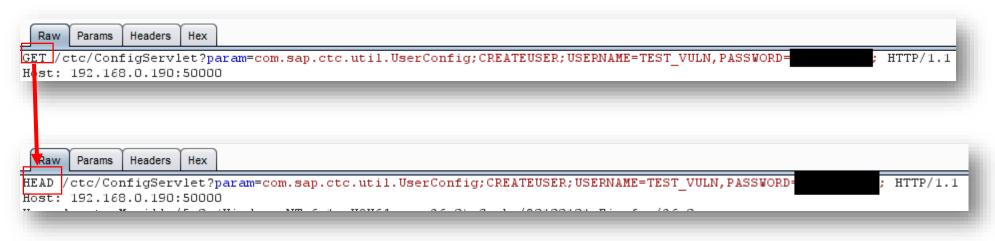
## Attack Scenario 2



1. Vulnerable systems are also connected to Internet!

	Google	inurl:/irj/portal	Ŷ	٩	1
•	Attacker s	sending HTTP request to the CTC servlet and crea	ating a	user –	Filtered
	192.168.0.190:50000/	ctc/ConfigServlet?param=com.sap.ctc.util.UserConfig;CREATEUSER;USERNAME=TEST_VULN,PASSWORD=			

3. Using a local proxy, the attacker changes the HTTP verb from GET to HEAD and forwards it to the server. This command will send the user creation request to the CTC servlet



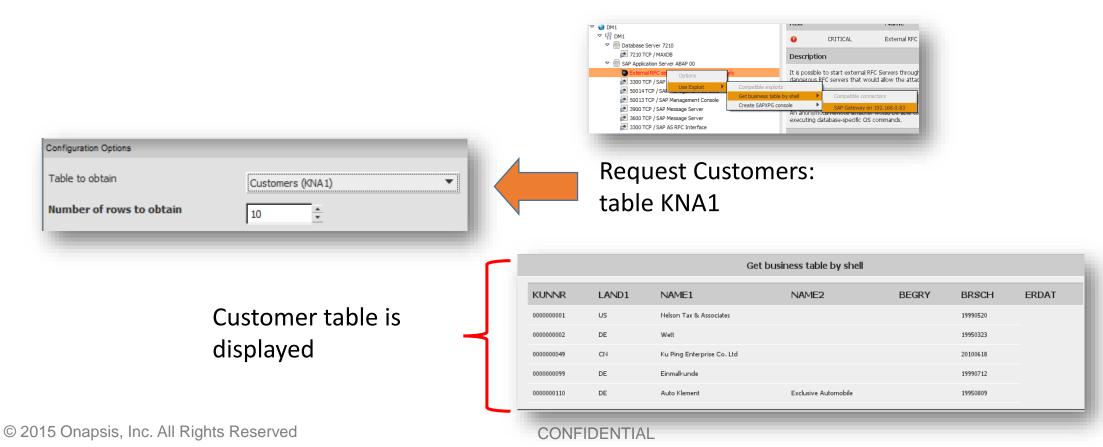
2

# **Attack Scenario 3**



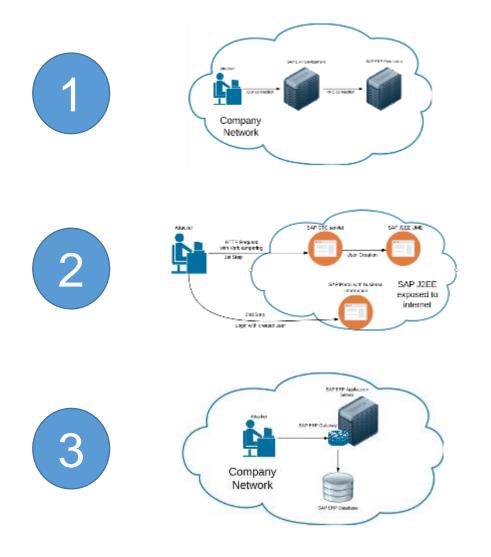
By abusing of insecure configurations in the SAP systems, there are different ways an attacker would use to get business data:

1. Exploits the SAP RFC Gateway -> OS control -> SAP DB schema control.



# **Attack Scenarios**





In these attack scenarios, <u>any</u> business information in SAP can be displayed:

- PA00\*: group of tables with HR Information
- LFA1: Vendor Master Data
- KNA1: Customer Master Data
- VCNUM & MKNUM: Customer Credit Cards
- BKPF & BSEG: Financial Documents
- EKKO & EKPO: Purchase Orders
- AUFK: Production Orders
- KALC: Material quantity calculation formulas

# **Onapsis Security Platform**





### **Onapsis Security Platform**

Provides organizations a holistically adaptive approach to focus on the factors that matter most to their business – critical applications running on SAP that house vital data and run missioncritical business processes.

**SAP**<sup>®</sup> Certified Integration with SAP NetWeaver<sup>®</sup>

### Vulnerability and Compliance

- Identify all SAP infrastructure and generate graphical topology maps along with the interfaces between systems and applications.
- Assess risks based on vulnerabilities and tie business context into remediation planning processes.
- Performs audits to Identify compliance gaps and report when systems don't meet requirements based on policies and industry regulations.

### **Detection and Response**

- Continuous monitoring of advanced threats and anomalous user behavior on SAP infrastructure.
- Provides visibility into attacks, with context, to determine if the attack is likely to be successful.
- Leverages real-time reporting on the likelihood and impact of threats from SAP exploits.
- Delivers attack signatures to identify anomalous user behaviors.
- Detects system changes that make organizations more vulnerable to attack.

### **Advanced Threat Protection**

- Provides protection against SAP security issues for which no SAP note has been released.
- Eliminates the window of exploitability and protects customers against known but unpublished vulnerabilities.
- Customers who subscribe to Advanced Threat Protection receive signatures for exploitation attempts against zero day vulnerabilities.

# **Engage with Onapsis**



### YouTube Video



1 minute Onapsis Security Platform Demo on SAP Cybersecurity

https://youtu.be/38T-\_yvTroc





Visit our Blog – The source For SAP Cybersecurity Expertise

Onapsis.com/blog

# Training

0	633	XXY.	Yes .	
black	hat	X X	REGISTE	RNOW
	2015			5T 1 - 6, 2015 BAY I LAS VEGAS, NV
REGISTRATION	BRIEFINGS TRAINING	CHEDULE SPONSORS	SPECIAL EVENTS	CFP TRAVEL
	PLATFORMS DNAPSIS INC. 1 AUGUST 3-4			
AND DESCRIPTION OF THE OWNER OF T	EARLY			
OVERVIEW WHO SHOULD TAKE THIS COURSE	\$3,000 ENDSJUNE 5 2359 EST	\$ <b>3,200</b>		
STUDENT REQUIREMENTS				
WHAT STUDENTS SHOULD BRING	OVERVIEW			
WHAT STUDENTS WILL BE	Neur CAR chafferer sectors the b	usiness crown jewels of your com	name Manifesta udda Inc.	

BlackHat USA 2015 ERP Security Training – Aug. 3-4

http://ubm.io/1MbaYe3



Thank You @marianonunezdc

