



SAP Business Objects Attacks: Espionage and Poisoning of BI Platforms



Juan Perez-Etchegoyen
jppereze@onapsis.com
[@jp_pereze](https://twitter.com/jp_pereze)



onapsis

This presentation contains references to the products of SAP AG. SAP, R/3, xApps, xApp, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP Business ByDesign, and other SAP products and services mentioned herein are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world.

Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius and other Business Objects products and services mentioned herein are trademarks or registered trademarks of Business Objects in the United States and/or other countries.

SAP AG is neither the author nor the publisher of this publication and is not responsible for its content, and SAP Group shall not be liable for errors or omissions with respect to the materials.

Transforming how organizations protect the applications that manage their business-critical processes and information.

- **Founded:** 2009
- **Headquarters:** Boston, MA with Offices in South America and EMEA
- **Status:** Privately held. Backed by leading investors
- **Headcount:** 60+ which includes 30+ in R&D
- **Research:** 130+ SAP security advisories and presentations published

Who am I?



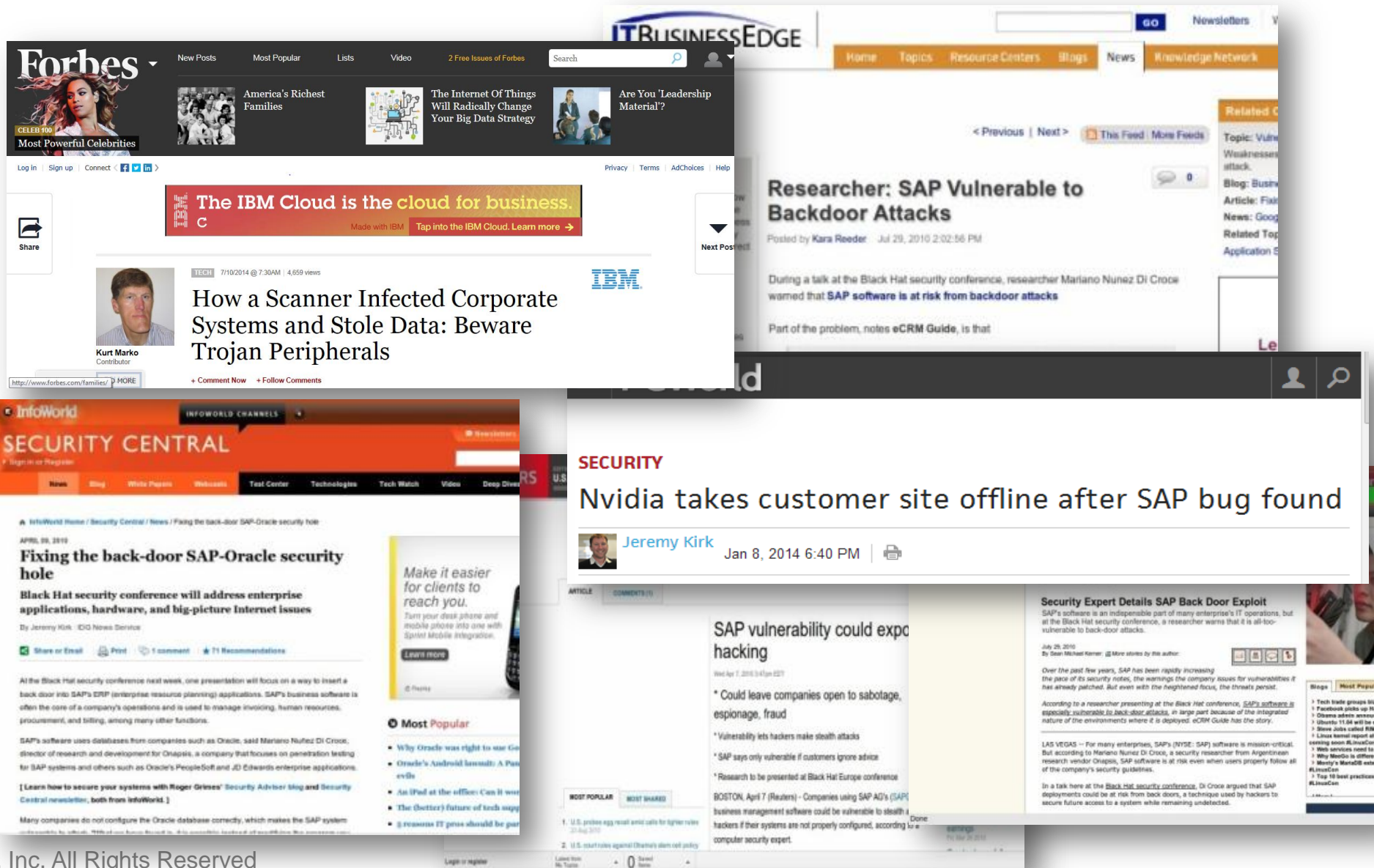
- Juan Perez-Etchegoyen (JP) – CTO @ Onapsis
- Background on Penetration Testing and vulnerabilities research
- Reported vulnerabilities in different SAP and Oracle Products
- Author/Contributor on diverse posts and publications
- Speaker and Trainer at Information Security Conferences
- <http://www.onapsis.com>



“

**“When performing security assessments I found that
95% of SAP systems are exposed to vulnerabilities.**

That is why I started Onapsis” — Mariano Nunez, CEO of Onapsis



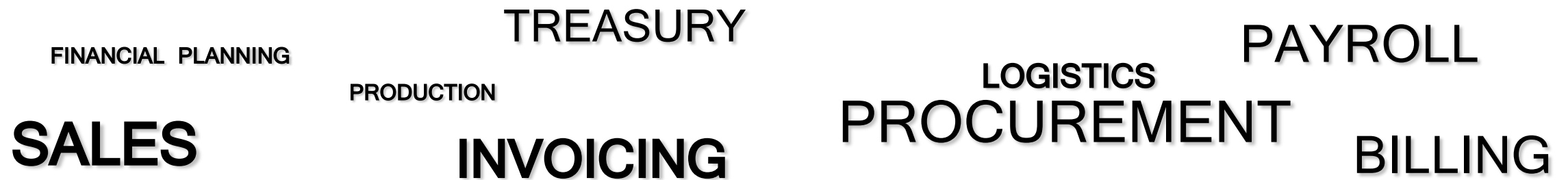
- SAP BusinessObjects Landscape
- The attacker lifecycle
- Abusing the Business Intelligence Process
- Conclusions

SAP BusinessObjects Landscape

What is SAP?



- **Largest** provider of **business management solutions** in the world.
 - More than 250.000 customers around the globe.
 - More than 70.000 employees.
- Used by **Global Fortune-1000 companies, governmental organizations and defense agencies** to run their every-day business processes.
 - Such as Revenue / Production / Expenditure business cycles.



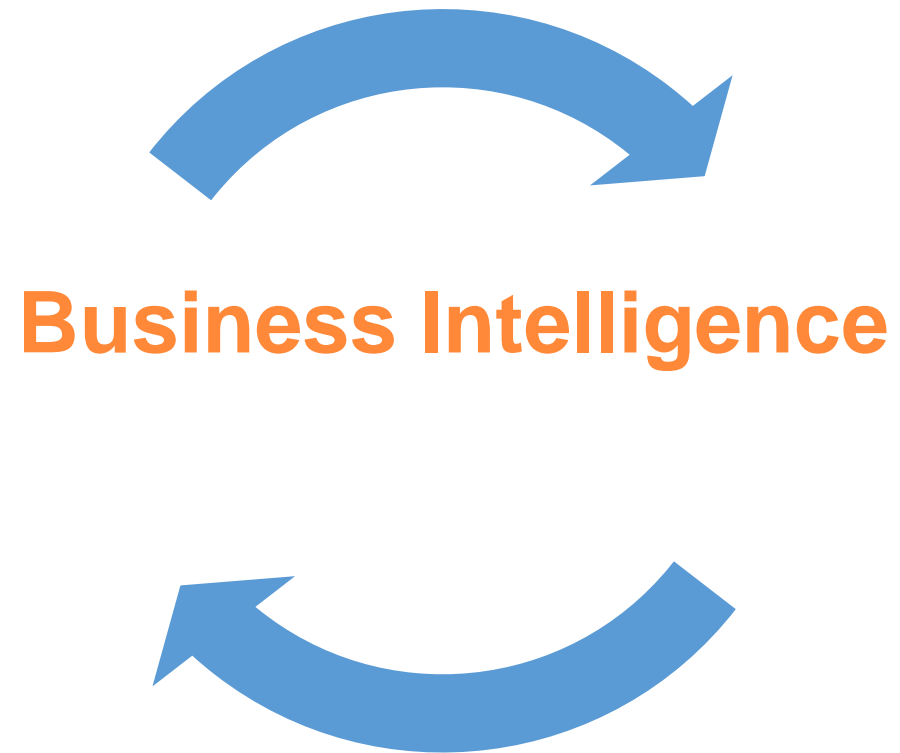
- Purchased by SAP in 2007
- Business Analysis and Intelligence is the Core Functionality
 - Produces Reports, Dashboards and KPI consumed by **decision makers**
 - Simplifies analysis of data for users
 - Usually pulling information from products such as ERP or CRM

While for traditional SAP systems (ERP,CRM,SCM...) it is easier to **understand** the impact of a security breach...

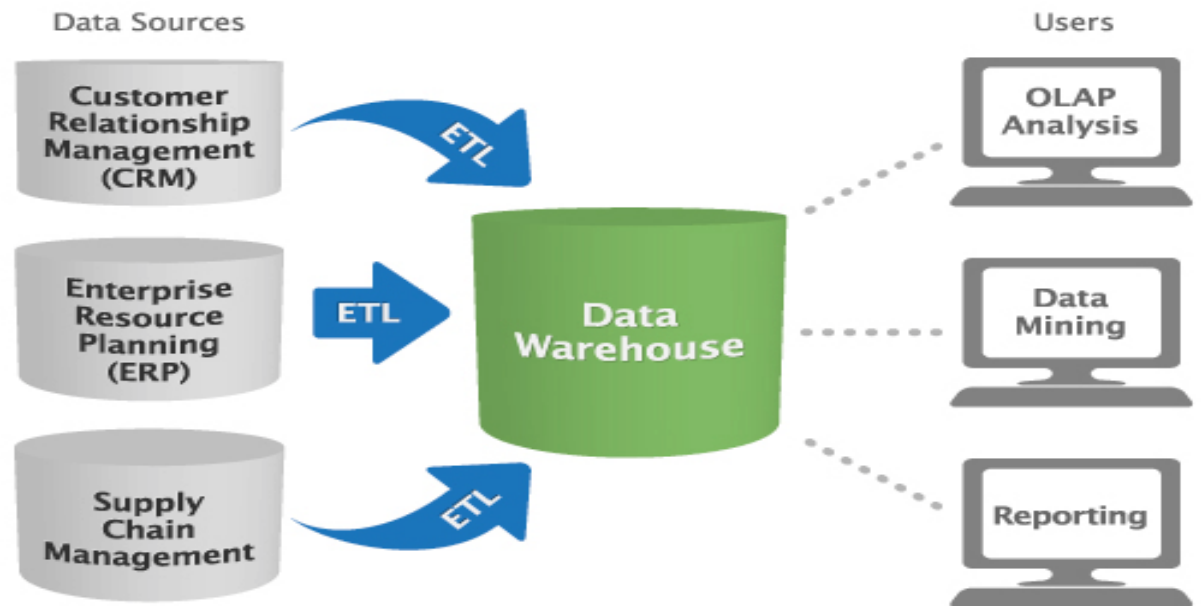
- **ESPIONAGE:** Obtain customers/vendors/human resources data, financial planning information, balances, profits, sales information, manufacturing recipes, etc.
- **SABOTAGE:** Paralyze the operation of the organization by shutting down the SAP system, disrupting interfaces with other systems and deleting critical information, etc.
- **FRAUD:** Modify financial information, tamper sales and purchase orders, create new vendors, modify vendor bank account numbers, etc.

In a BusinessObjects implementation it is more difficult to **understand** the impact of a security breach...

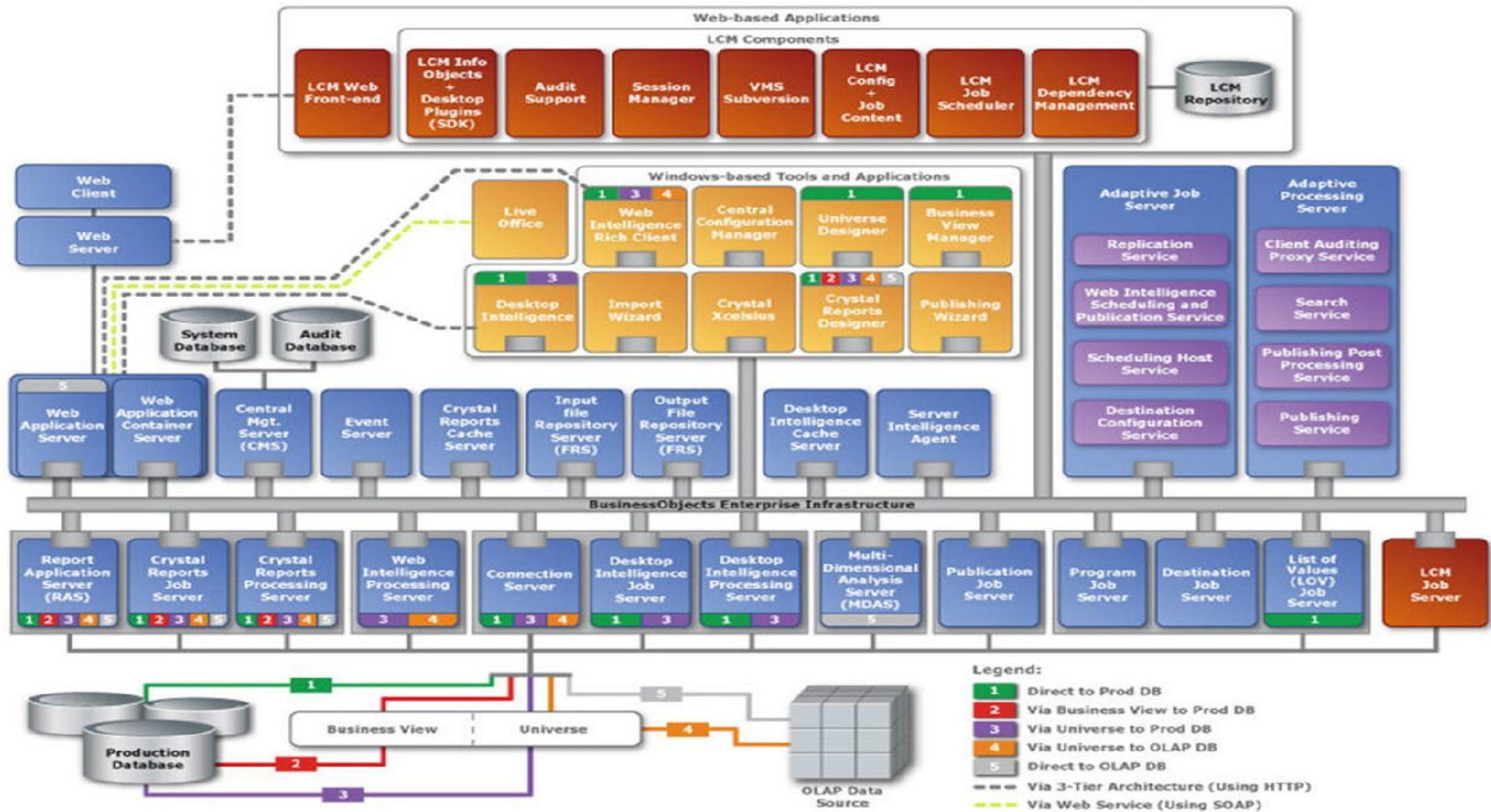
- **FINANCIAL STATEMENT**: Incorrect reporting to authorities such as SEC. Access the information in advance.
- **BUDGETING AND STAFFING**: Incorrect allocating of resources for the achievement of targets.
- **SALES FORECAST**: Critical to determine the budget and to understand how much the company will grow, quantity of products to be produced, purchasing requirements...
- **LIQUIDITY PLANNING**: Affect the understanding of the available cash that the company will have during a period of time.



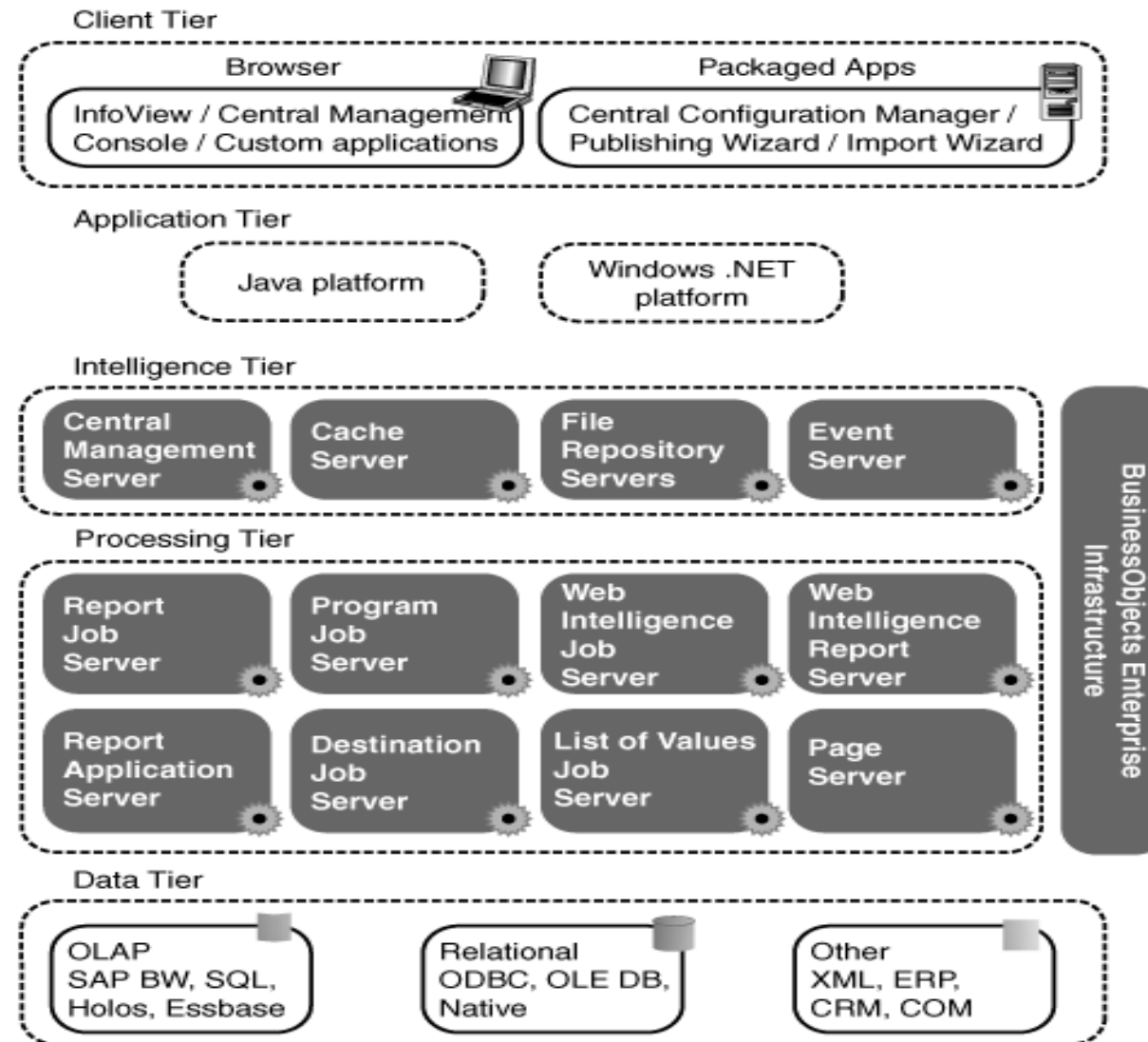
- BW is an analytical, reporting and data warehousing product
- Structured by layers. ETL (Extract, Transform, Load) is probably the most important layer
- The process of extracting data from other SAP Systems is usually performed by RFC Function Calls.
- SAP **BusinessObjects** are usually connected to **SAP BW**



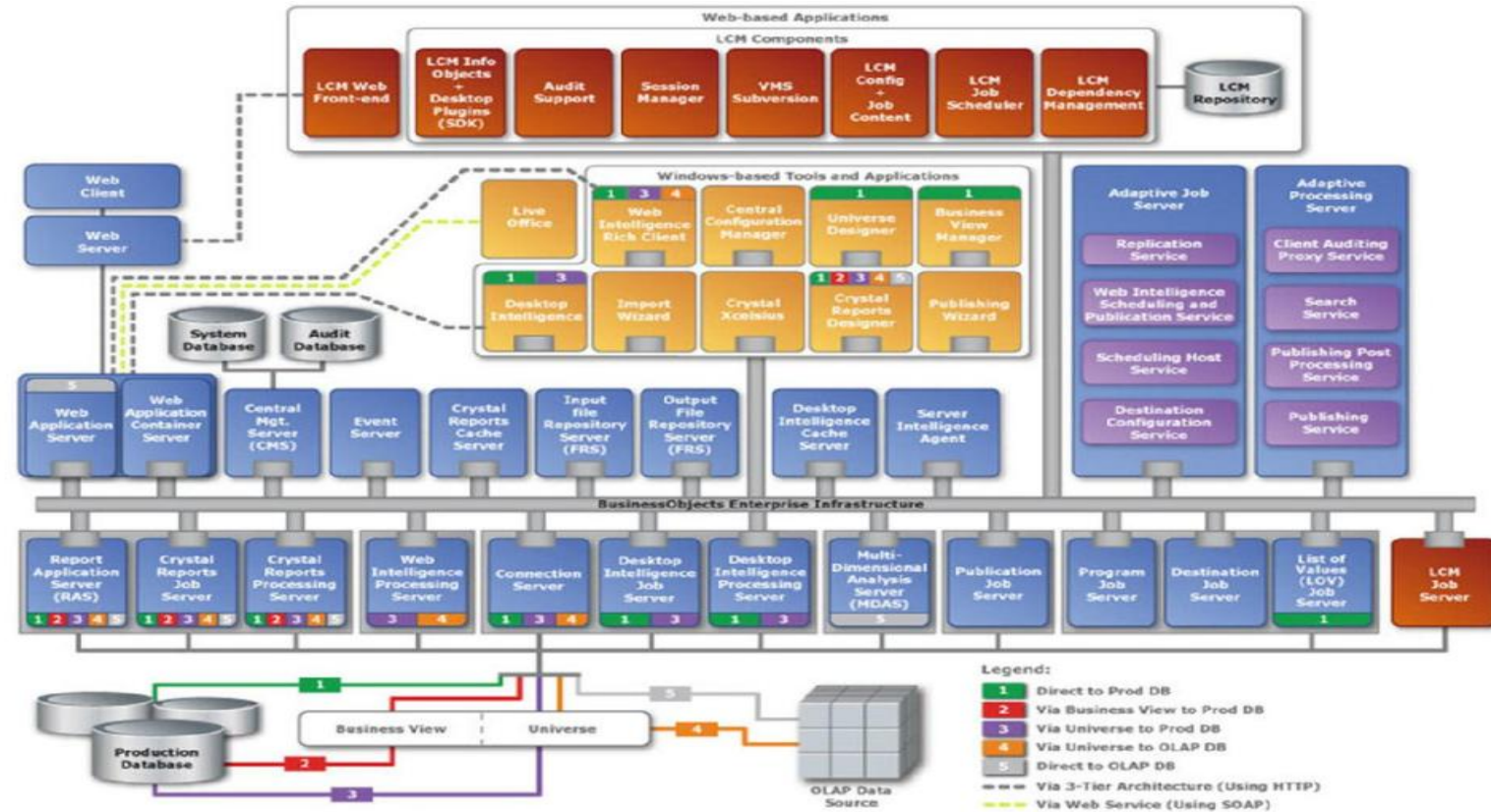
Architecture of SAP BO



Architecture of SAP BO



- Central Management Server
- File Repository Server
 - Report Templates
 - Resulting Reports
- Server Intelligence Agent
- Client Endpoints
 - Web Applications: CMC
 - Web Services

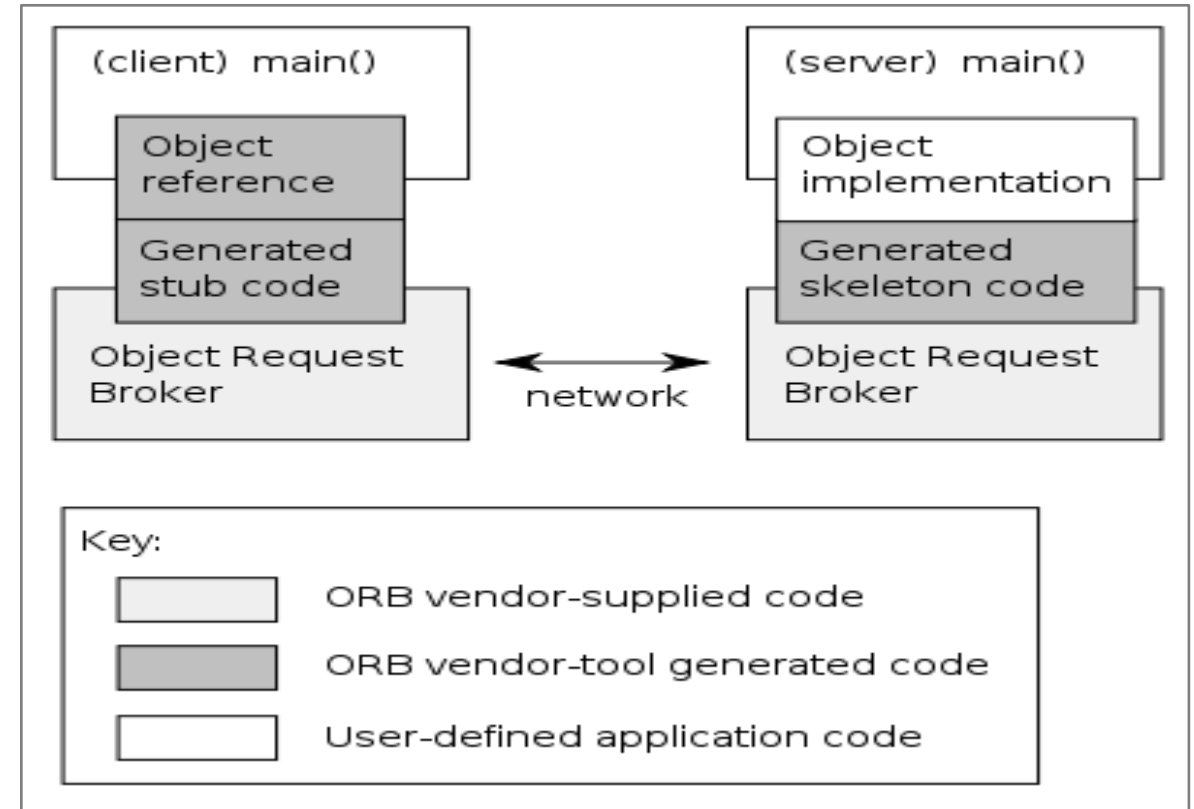


- From the Client browser tier to the Application tier, SOAP and HTTP are the most common methods of communication (REST is also available)



- Most of the Inter “Process” communication is done using CORBA on the BO Service Bus

- Standard defined by OMG (“Similar” to JAVA RMI)
- Uses IIOP Network Protocol
- Uses IDL to define interfaces exposed
- Designed to facilitate the communication of systems that are deployed on diverse platforms.

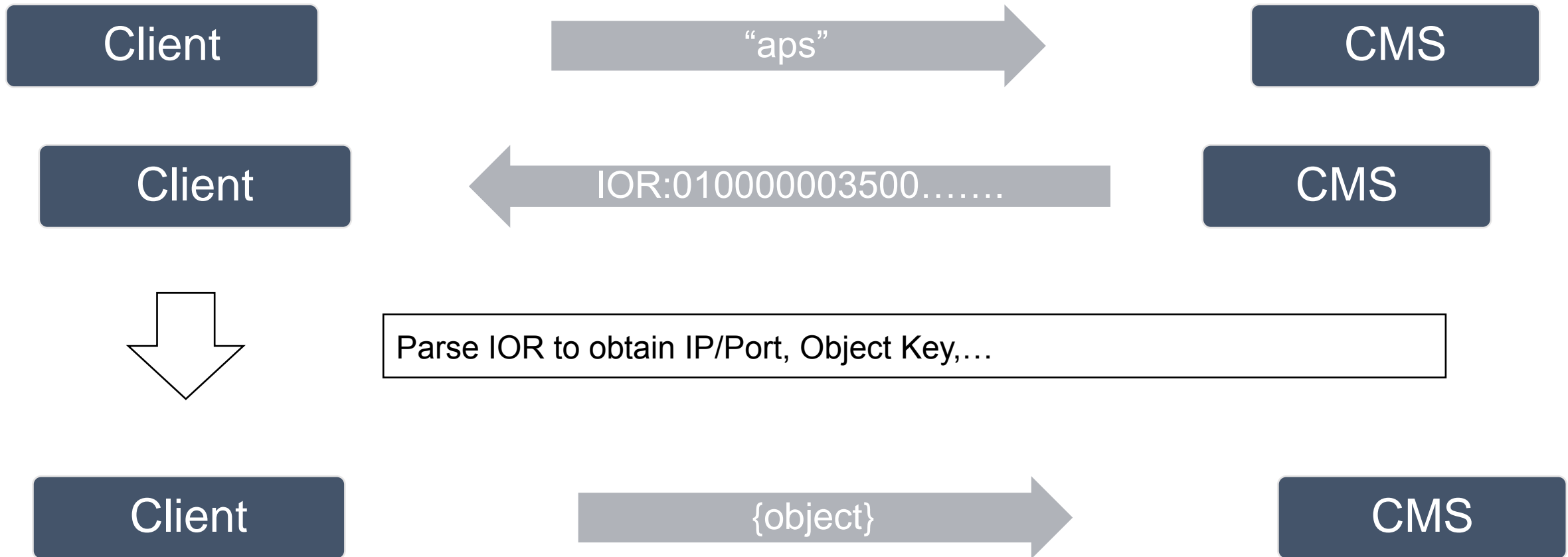


Source: Wikipedia

- Interoperable Object Reference (IOR)
 - Reference to a remote object
 - Provided by the server, consumed by the client to communicate using remote object
 - Example Components
 - “IDL:Hello/HelloWorld”
 - “Host: www.remotecorba.com”
 - “Port: 4678”

- Each BO server has a number of services available via CORBA
- A client needs to know the IOR of the remote service to initiate communication
 - They also need to know (or reverse engineer) the IDL to communicate meaningfully

BO CORBA Example – Client to CMS



BO and the Attacker Lifecycle

- Many Different Types of attackers
 - Internal/External
 - Advanced/Script kiddies
 - Just for fun/Criminal organizations
- Identifying the threat actor is an obvious key to defense
 - Define monitoring processes
 - Define configuration and security standards

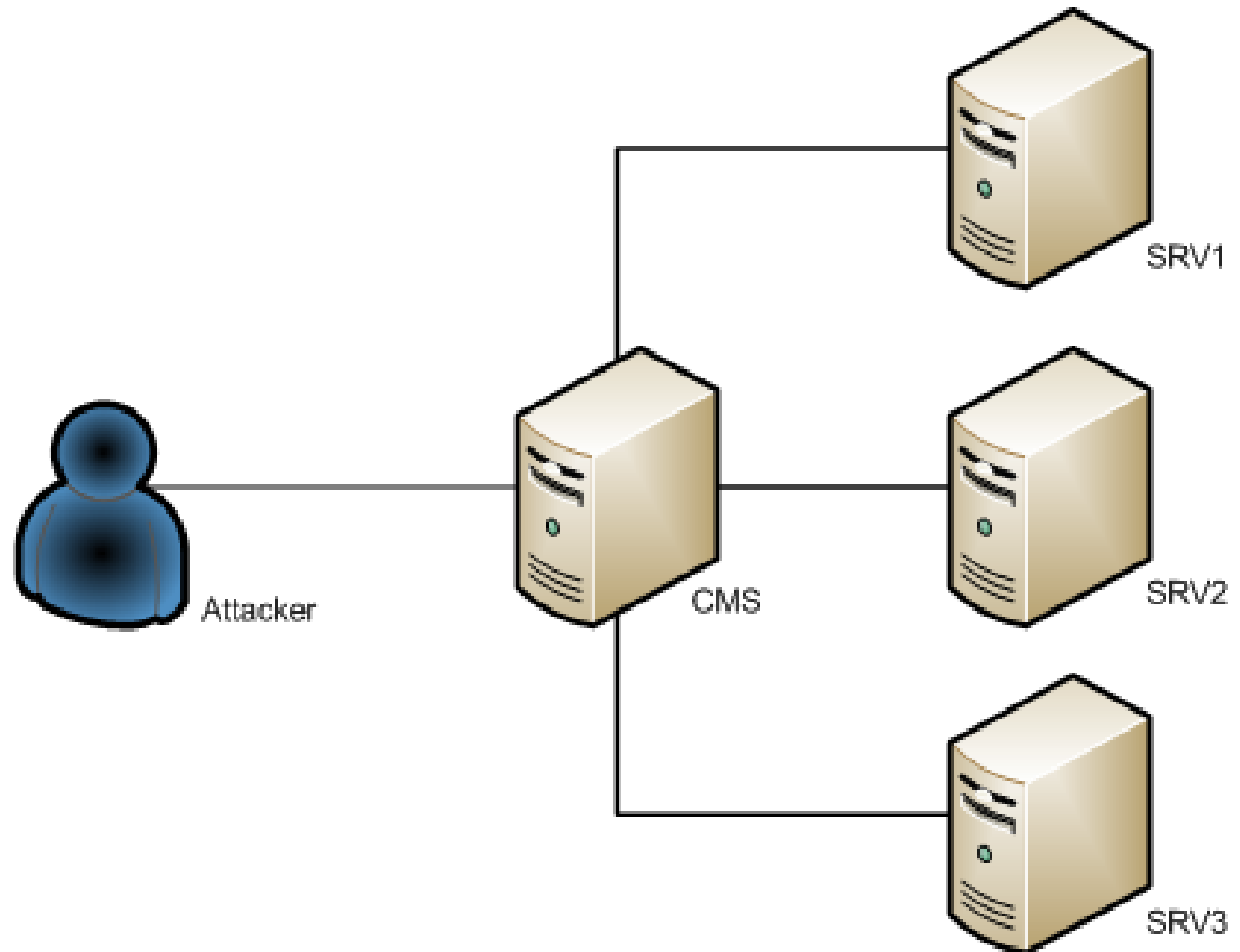
Reconnaissance (Default Ports)



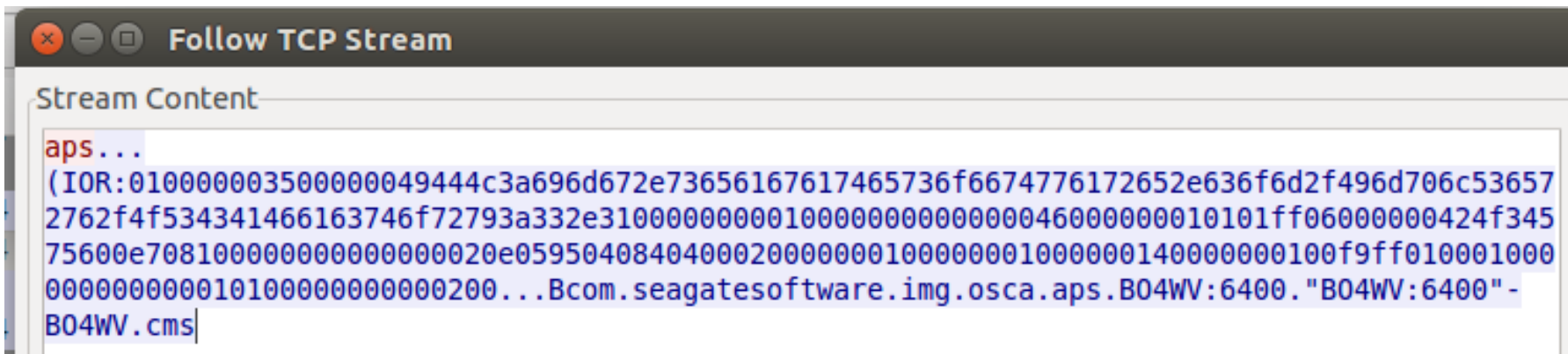
Name	Default Port	Function
Central Management Server	6400 Name Port (CORBA), dynamic	Most Important Component. Manages user sessions, other servers, and many other core components. Administration is essentially performed through here.
Server Intelligence Agent	6410	Starts and Stops the servers used by BO
CMS Database	Depends (SQL Server by default)	Stores data for BO
Version Management	3690	BO supports a version control system
Web Application Frontend	8080 or 6405	8080 – Tomcat 6405 – Web Application Container Server

What would an attacker use to target a BO implementation ? onapsis

- CMS IP
- CMS Static Port
- CMS IOR
- SRV's IORs



- In default state, 15 dynamic ports
 - Example Use Case
 - One service needs to know the IP:PORT of another service.
How does it get this information?
 - Asks the CMS via CORBA



```
Follow TCP Stream

Stream Content

aps...
(IOR:010000003500000049444c3a696d672e73656167617465736f6674776172652e636f6d2f496d706c53657
2762f4f534341466163746f72793a332e310000000001000000000000046000000010101ff06000000424f345
75600e70810000000000000020e059504084040020000000100000001000000140000000100f9ff010001000
000000000010100000000000200...Bcom.seagatesoftware.img.osca.aps.B04WV:6400."B04WV:6400" -
B04WV.cms|
```

Demo

Attacker discovering service ports

As discussed in the Administrators guide, limiting network access to every BusinessObjects component is the best method to protect against pulling information from these services.

- Enterprise
- SAP
- LDAP
- WindowsAD

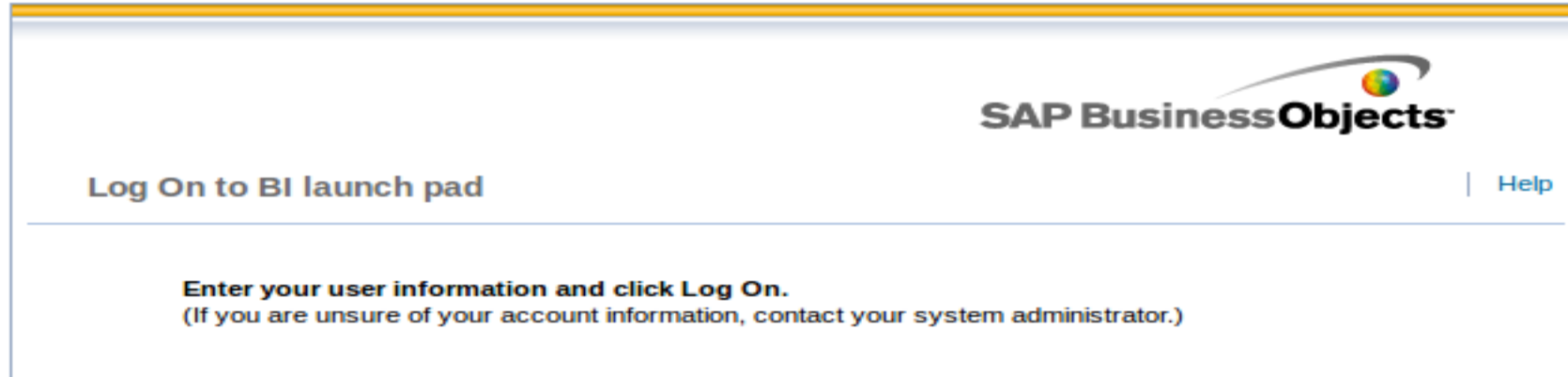
Default Accounts (Reconnaissance)



Username	Notes
Administrator	Administrator, default but can be changed
SMAAdmin	Disabled by default in BO4
QaaWSServletPrincipal	Enabled by default in BO4
Guest	Disabled by default in BO4
boeuser	DB account which stores BO stuff
sa	Hardcoded DB Account
LCMuser	Hardcoded SVN user, password stored in cleartext on the FS and in the web app

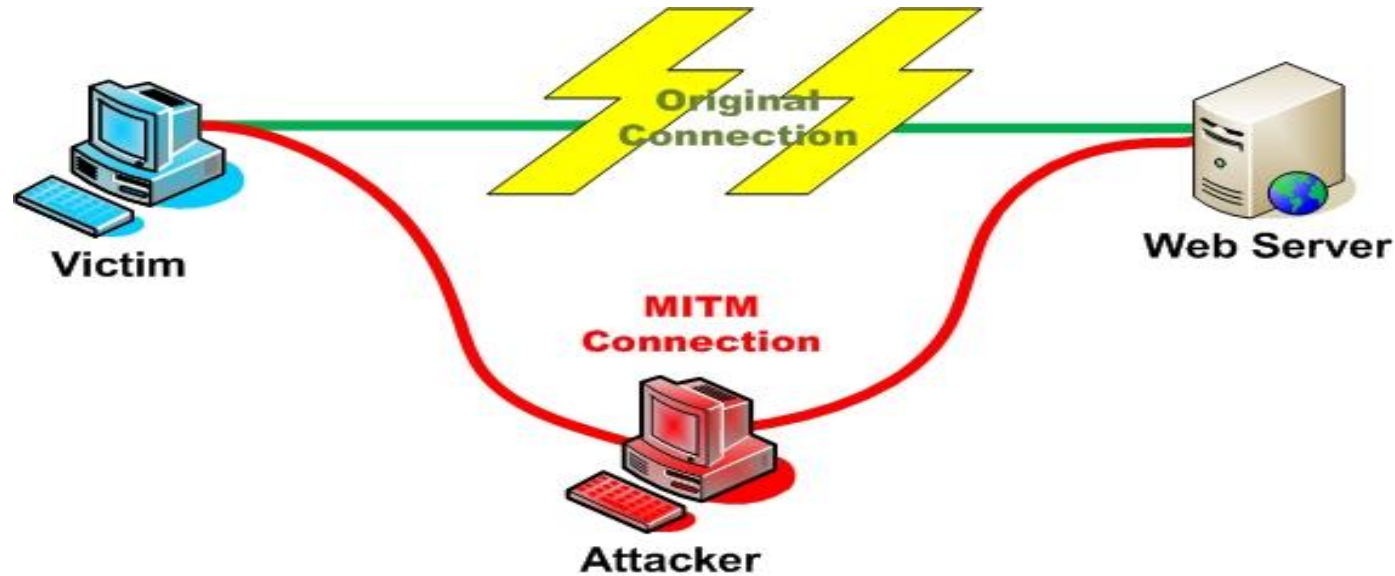
It is critically important to apply the most up to date security notes. Furthermore, disabling unused web applications and services limits the attack surface.

Major Version Info (Reconnaissance)



- What Web Interfaces are available?
- Web Services also has valuable information

A warning about MitM



- Communication is Unencrypted by default
- An Attacker can hijack a Session via **HTTP** or **CORBA**

Poisoning and Intercepting Business Intelligence

- We are discussing an attacker that wishes to access or poison the Business Intelligence Process
- Intercepting vs. Poisoning

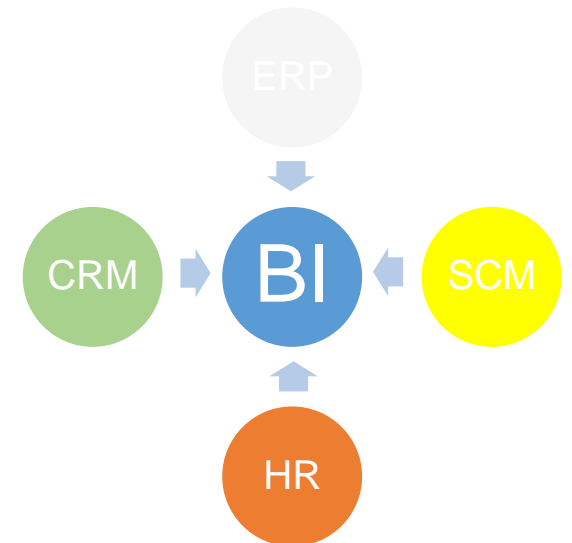
Information disclosure

Any information in the data sources
Generated Reports

Information Tampering

Switching data source system
Changes on the business data
Changes on the generated reports

- BO processes and groups information from many systems (ERP, SCM, CRM, HR, etc).
- By compromising BO/BW/BI the attacker will have almost all of the company critical information in a central repository.
- Access to Business Reports
- Access to Financial Statements



- Change data source
 - Point to a different SAP system (ERP,BW...)
 - Changing Infoproviders (InfoSet, SAP Queries...)
- Modify BO contents
 - Reports
 - Dashboards
 - KPI



Demo

Attacker connecting to Source System

- Commonly an attacker will focus on a client with access
 - Obvious ways to access data
 - Check the FS
 - Browser cookies
 - How else?
- Network Sniffing!
- Active Traffic is best
- But, the Client will auto ping the Server on a set schedule (SESSION_ID is given in the ping)

Demo

Sniffing traffic to hijack sessions

- Power Shell
 - Made available in the Client or Server BusinessObjects installation
 - SDK Like functionality
 - Reporting Access
 - InfoQuery
 - Session Handling

Available to BO clients... and to attackers too!

- File Repository Server
 - Input
 - Output
- What is a report to BO?
 - File on the Filesystem
 - Entry in the InfoStore
- Not all files will stay overwritten

Demo

Changes on existing business reports

Conclusions



- Read the **Admin Guide!**
- Many of these attacks can be prevented or detected
- Keep the systems **updated!**
- Enable Auditing
- Periodically **scan**/monitor the systems
- Secure the system and the **critical data**



Questions?

Thanks to Will Vandevanter and the ORL

