INTEGRIGY

Oracle Database

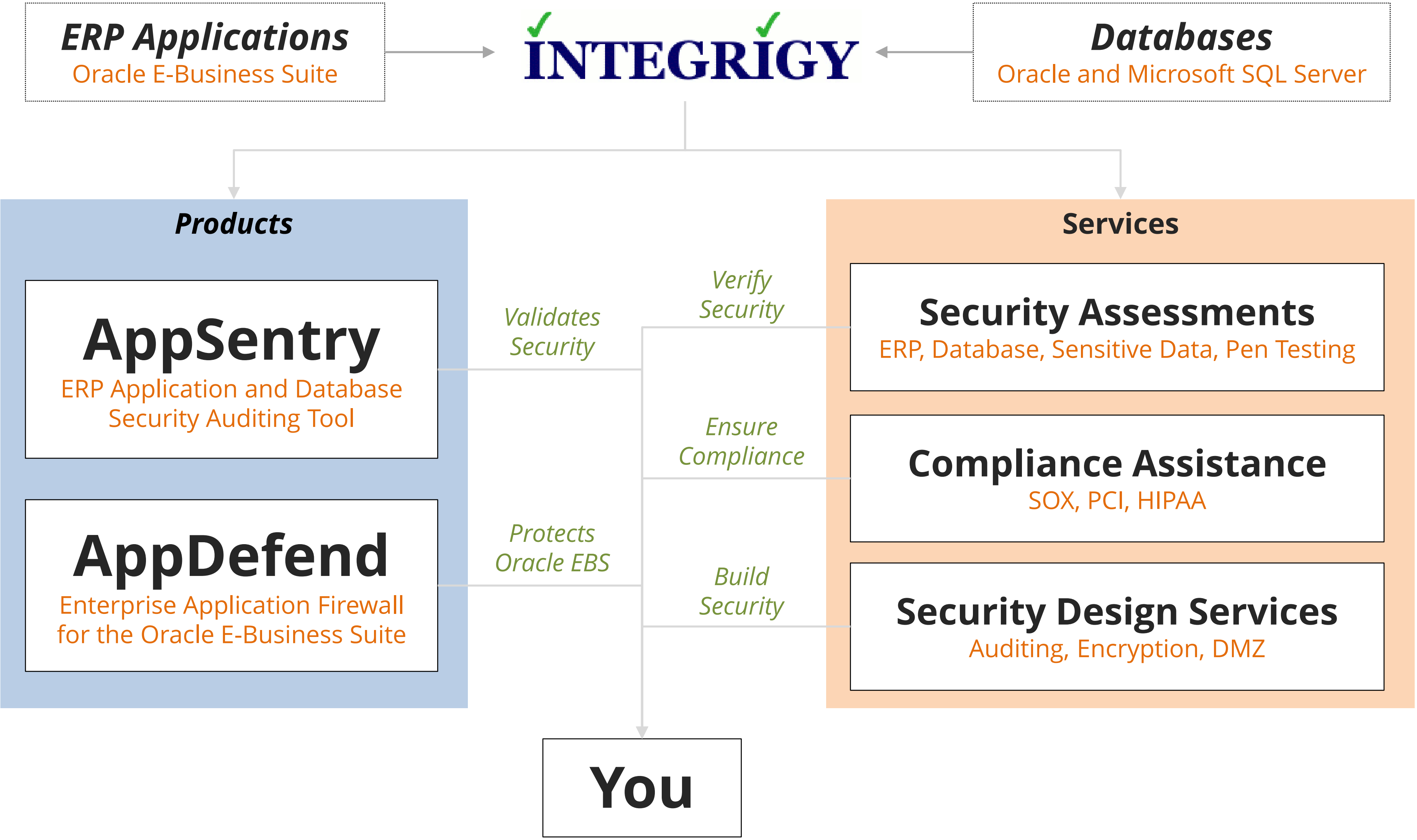
TNS Poisoning Attacks (CVE-2012-1675)

September 29, 2016

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

About Integrigy



ERP Applications
Oracle E-Business Suite

INTEGRIGY

Databases
Oracle and Microsoft SQL Server

Products

AppSentry
ERP Application and Database Security Auditing Tool

Validates Security

AppDefend
Enterprise Application Firewall for the Oracle E-Business Suite

Protects Oracle EBS

Services

Verify Security

Security Assessments
ERP, Database, Sensitive Data, Pen Testing

Ensure Compliance

Compliance Assistance
SOX, PCI, HIPAA

Build Security

Security Design Services
Auditing, Encryption, DMZ

You

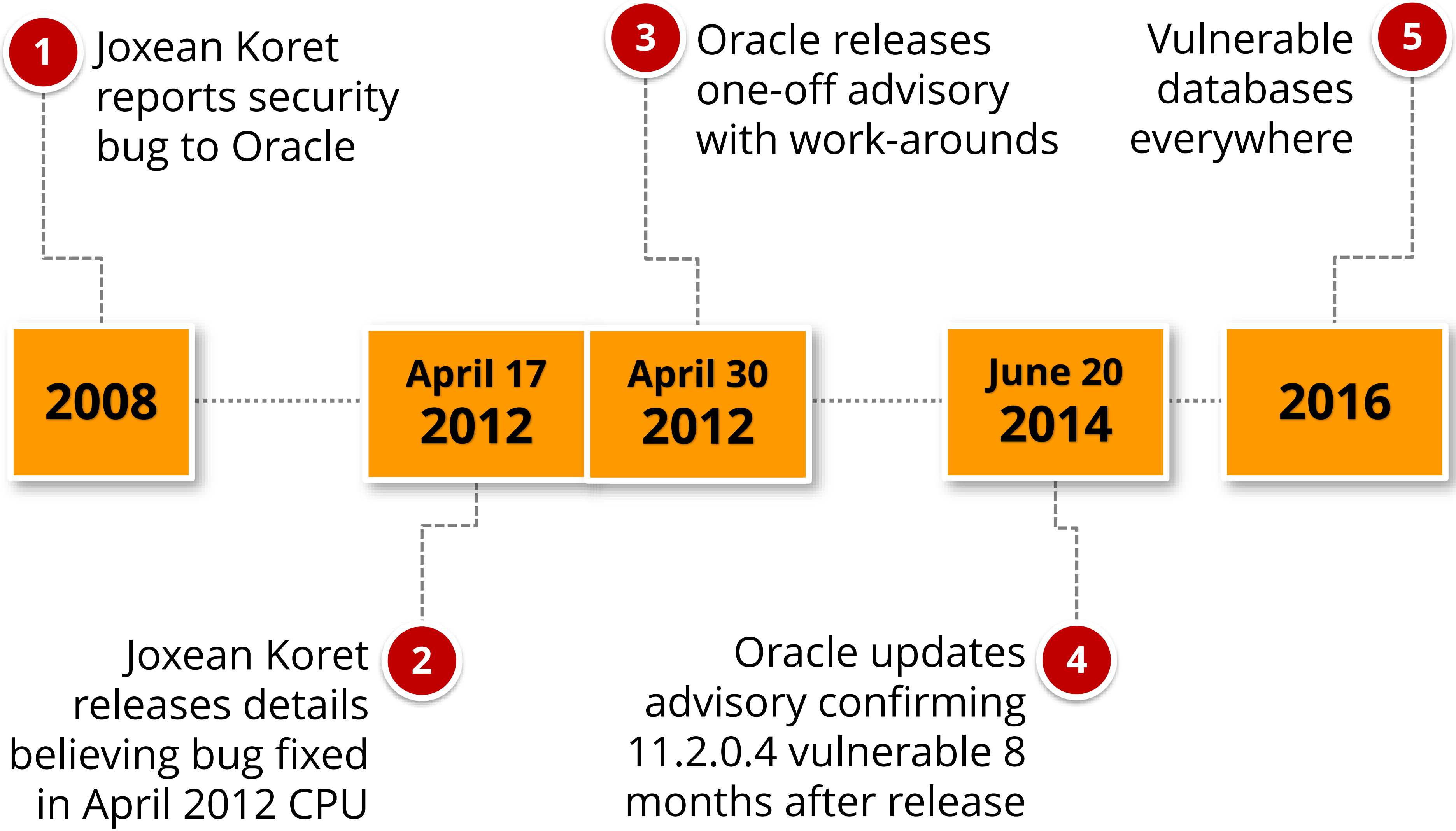
Why are we talking about an Oracle Database **security vulnerability** reported to Oracle in

2008?

60% of databases assessed by Integrigy are **vulnerable**

Not fixed or enabled by default in **11.2.0.4 and prior**

Vulnerability Timeline



2008

1 Joxean Koret reports security bug to Oracle

April 17 2012

2 Joxean Koret releases details believing bug fixed in April 2012 CPU

April 30 2012

3 Oracle releases one-off advisory with work-arounds

June 20 2014

4 Oracle updates advisory confirming 11.2.0.4 vulnerable 8 months after release

2016

5 Vulnerable databases everywhere

Oracle Database Listener Registration

Listener registration allows a database to register dynamically with the TNS listener

- Static service entries not required in listener.ora for ease of management – **Local Registration**
- Controlled by initialization parameters **LOCAL_LISTENER, REMOTE_LISTENER , DISPATCHERS**

Remote registration used by **RAC** to register databases in a clustered environment

TNS Poisoning Attack – One-off – April 30, 2012

Vuln #	Component	Protocol	Package and/or Privilege Required	Remote Exploit without Auth.?
CVE-2012-1675	**Listener**	**Oracle Net**	**None**	**Yes**

CVSS VERSION 2.0 RISK							
Base Score	Access Vector	Access Complexity	Authentication	Confidentiality	Integrity	Availability	Last Affected Patch set (per Supported Release)
7.5	**Network**	**Low**	**None**	**Partial+**	**Partial+**	**Partial**	**ALL VERSIONS**

- **This vulnerability is not patched by a SPU or PSU.** The TNS Listener configuration must be secured.
- **ALL VERSIONS** of the Oracle Database are affected.
- 12c (12.1.0.1 and 12.1.0.2) are protected by default, but vulnerable if Valid Node Checking Registration (VNCR) is disabled.

TNS Poisoning Attack – One-off – April 30, 2012

Vuln #	Component	Protocol	Package and/or Privilege Required	Remote Exploit without Auth.?
CVE-2012-1675	**Listener**	**Oracle Net**	**None**	**Yes**

CVSS VERSION 2.0 RISK							
Base Score	Access Vector	Access Complexity	Authentication	Confidentiality	Integrity	Availability	Last Affected Patch set (per Supported Release)
7.5	**Network**	**Low**	**None**	**Partial+**	**Partial+**	**Partial**	**ALL VERSIONS**

- **This vulnerability is not patched by a SPU or PSU.** The TNS Listener configuration must be secured.
- **ALL VERSIONS** of the Oracle Database are affected.
- 12c (12.1.0.1 and 12.1.0.2) are protected by default, but vulnerable if Valid Node Checking Registration (VNCR) is disabled.

TNS Poisoning Attack – One-off – April 30, 2012

Vuln #	Component	Protocol	Package and/or Privilege Required	Remote Exploit without Auth.?
CVE-2012-1675	**Listener**	**Oracle Net**	**None**	**Yes**

CVSS VERSION 2.0 RISK							
Base Score	Access Vector	Access Complexity	Authentication	Confidentiality	Integrity	Availability	Last Affected Patch set (per Supported Release)
7.5	**Network**	**Low**	**None**	**Partial+**	**Partial+**	**Partial**	**ALL VERSIONS**

- **This vulnerability is not patched by a SPU or PSU.** The TNS Listener configuration must be secured.
- **ALL VERSIONS** of the Oracle Database are affected.
- 12c (12.1.0.1 and 12.1.0.2) are protected by default, but vulnerable if Valid Node Checking Registration (VNCR) is disabled.

TNS Poisoning Attack – One-off – April 30, 2012

Vuln #	Component	Protocol	Package and/or Privilege Required	Remote Exploit without Auth.?
CVE-2012-1675	**Listener**	**Oracle Net**	**None**	**Yes**

CVSS VERSION 2.0 RISK							Last Affected Patch set (per Supported Release)
Base Score	Access Vector	Access Complexity	Authenticatio	Confidentiality	Integrity	Availability	
7.5	**Network**	**Low**	**None**	**Partial+**	**Partial+**	**Partial**	**ALL VERSIONS**

- **This vulnerability is not patched by a SPU or PSU.** The TNS Listener configuration must be secured.
- **ALL VERSIONS** of the Oracle Database are affected.
- 12c (12.1.0.1 and 12.1.0.2) are protected by default, but vulnerable if Valid Node Checking Registration (VNCR) is disabled.

TNS Poisoning Attack – One-off – April 30, 2012

Vuln #	Component	Protocol	Package and/or Privilege Required	Remote Exploit without Auth.?
CVE-2012-1675	**Listener**	**Oracle Net**	**None**	**Yes**

CVSS VERSION 2.0 RISK							Last Affected Patch set (per Supported Release)
Base Score	Access Vector	Access Complexity	Authentication	Confidentiality	Integrity	Availability	
7.5	**Network**	**Low**	**None**	**Partial+**	**Partial+**	**Partial**	**ALL VERSIONS**

- **This vulnerability is not patched by a SPU or PSU.** The TNS Listener configuration must be secured.
- **ALL VERSIONS** of the Oracle Database are affected.
- 12c (12.1.0.1 and 12.1.0.2) are protected by default, but vulnerable if Valid Node Checking Registration (VNCR) is disabled.

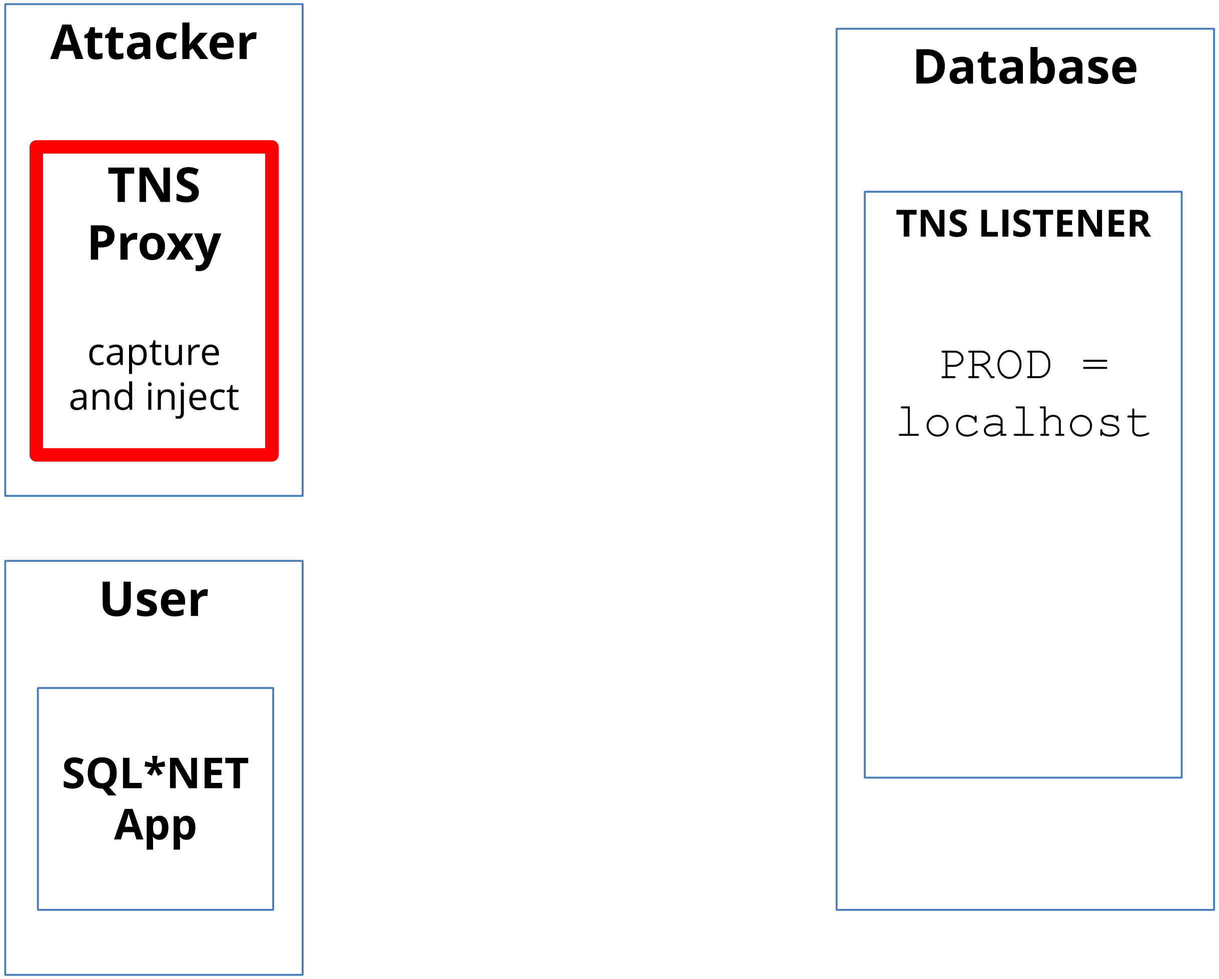
TNS Poisoning Attack – One-off – April 30, 2012

Vuln #	Component	Protocol	Package and/or Privilege Required	Remote Exploit without Auth.?
CVE-2012-1675	**Listener**	**Oracle Net**	**None**	**Yes**

CVSS VERSION 2.0 RISK							
Base Score	Access Vector	Access Complexity	Authentication	Confidentiality	Integrity	Availability	Last Affected Patch set (per Supported Release)
7.5	**Network**	**Low**	**None**	**Partial+**	**Partial+**	**Partial**	**ALL VERSIONS**

- **This vulnerability is not patched by a SPU or PSU.** The TNS Listener configuration must be secured.
- **ALL VERSIONS** of the Oracle Database are affected.
- 12c (12.1.0.1 and 12.1.0.2) are protected by default, but vulnerable if Valid Node Checking Registration (VNCR) is disabled.

TNS Poisoning Attack Illustrated



Attacker

TNS Proxy

capture and inject

User

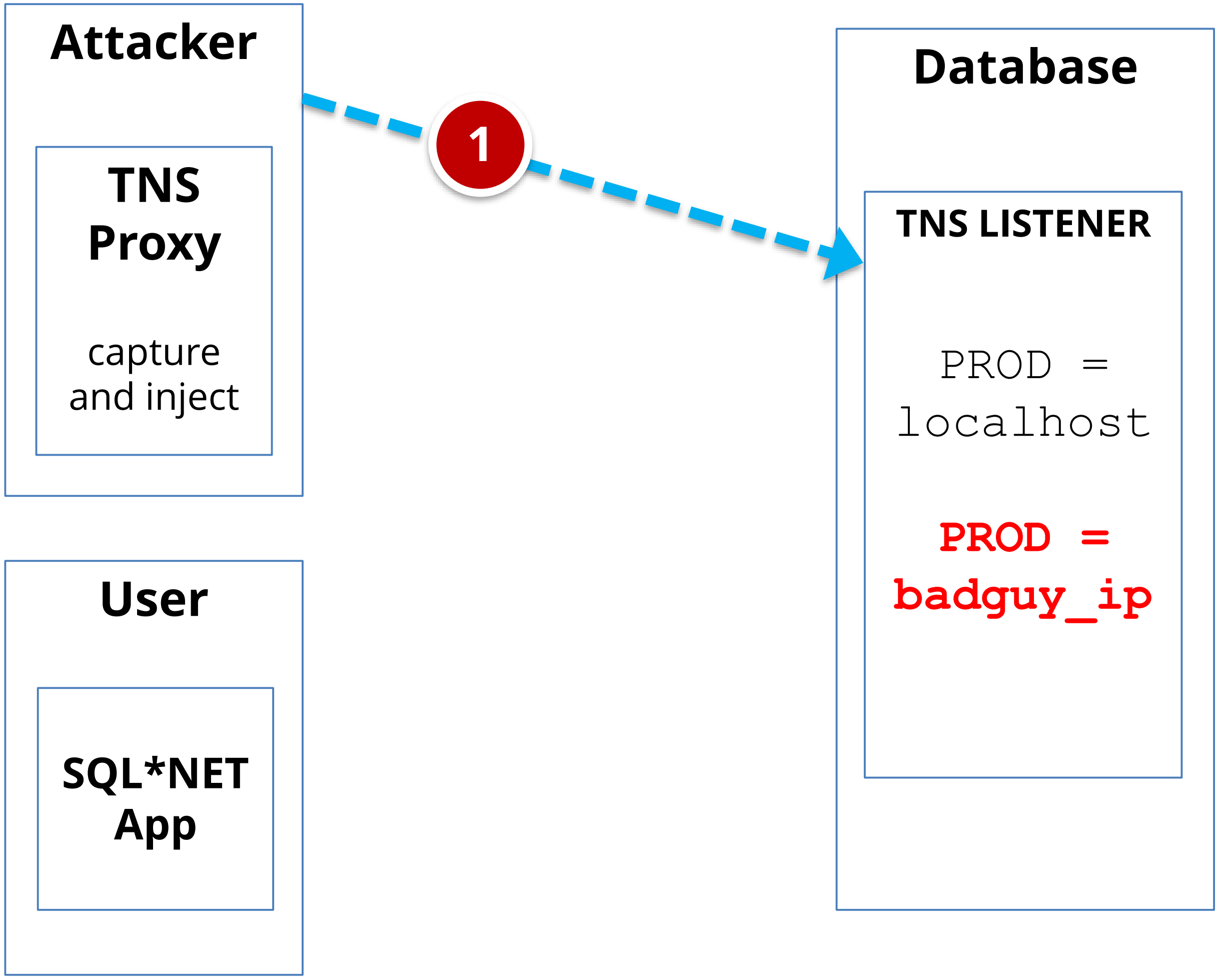
SQL*NET App

Database

TNS LISTENER

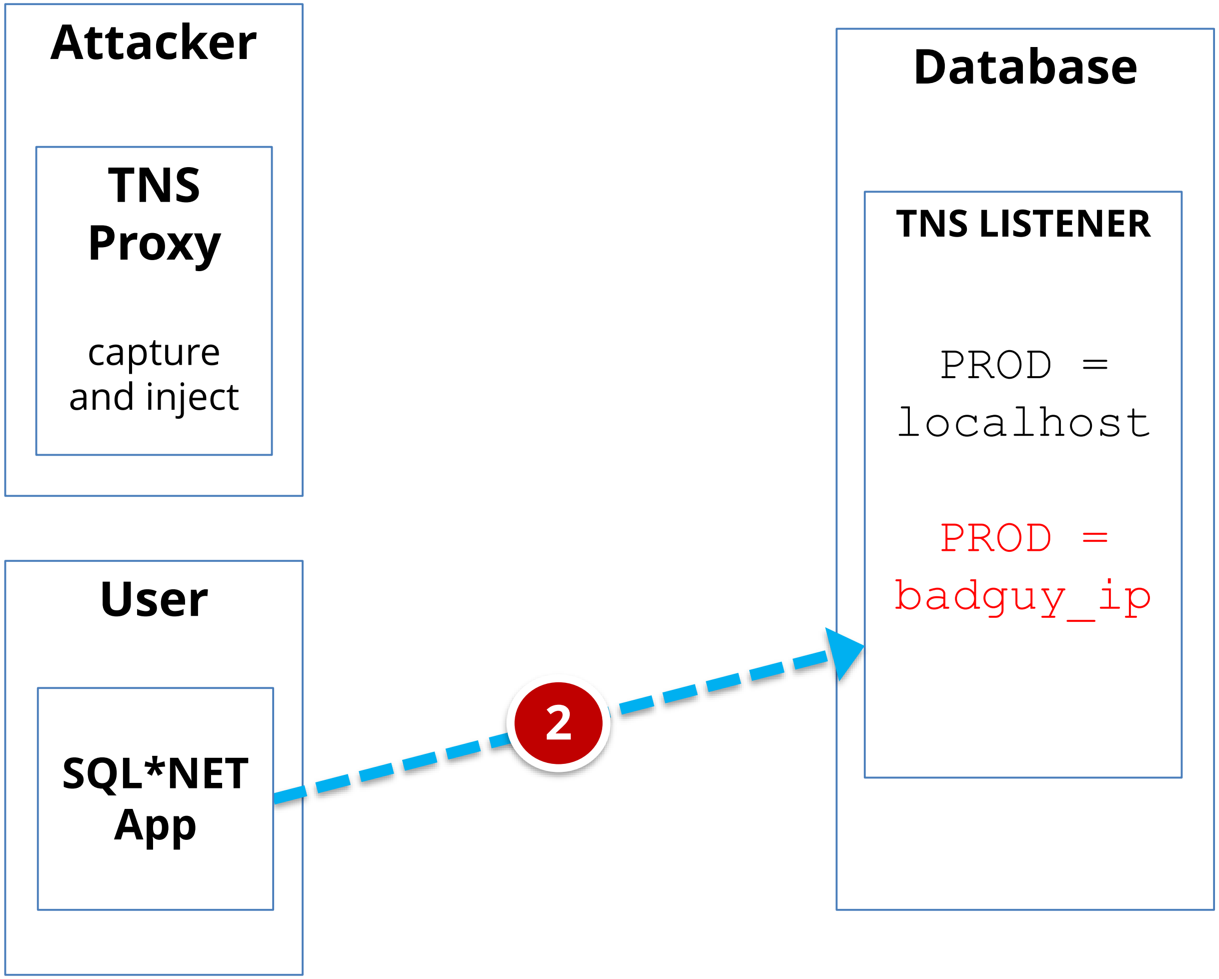
PROD = localhost

TNS Poisoning Attack Illustrated



1 Attacker dynamically registers Service with database.

TNS Poisoning Attack Illustrated



Attacker

TNS Proxy

capture and inject

User

SQL*NET App

2

Database

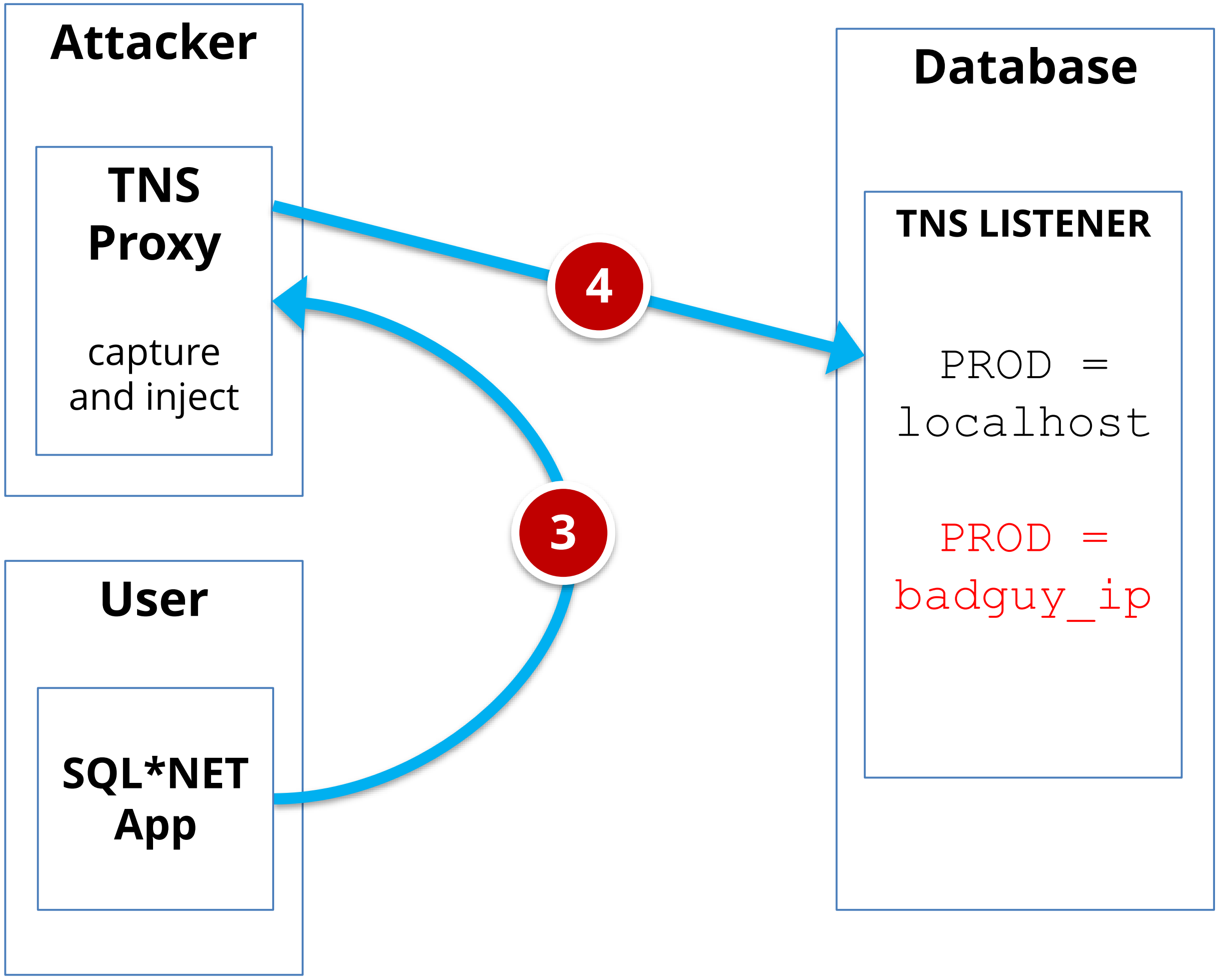
TNS LISTENER

PROD = localhost

PROD = badguy_ip

2 User connects and is “Load Balanced” to attacker.

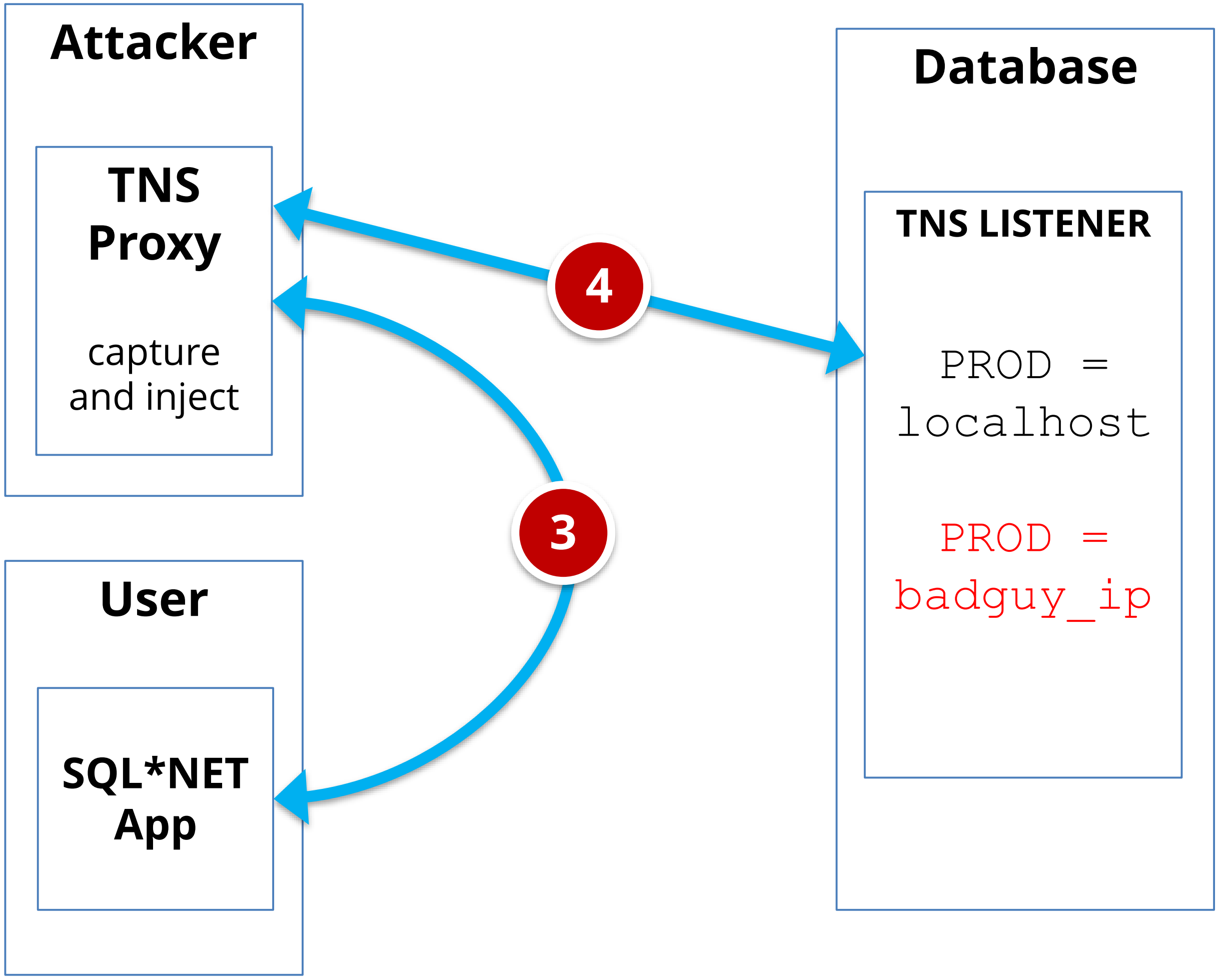
TNS Poisoning Attack Illustrated



3 User connect to attacker rather than database.

4 Attacker forwards to database.

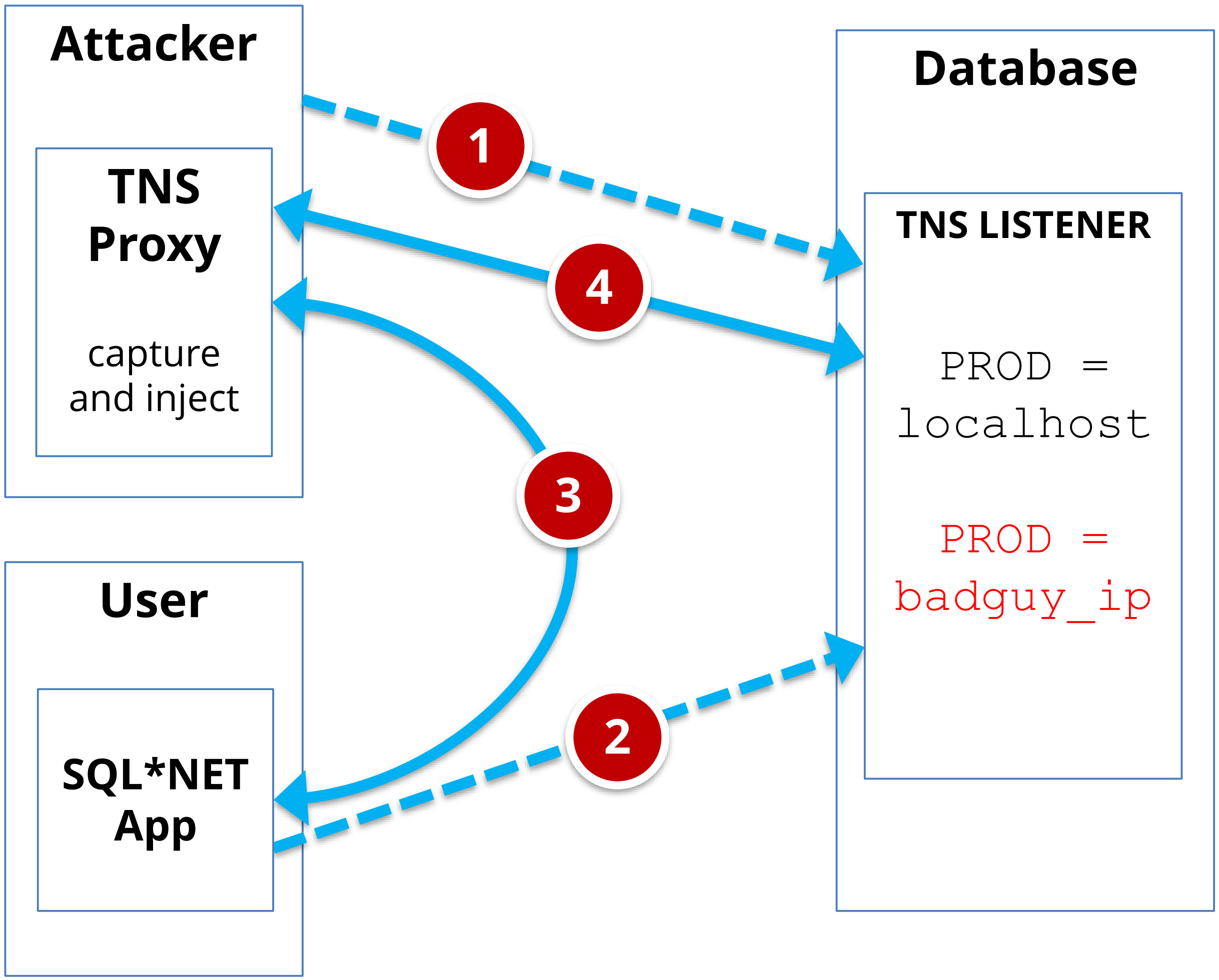
TNS Poisoning Attack Illustrated



3 User connect to attacker rather than database.

4 Attacker forwards to database.

TNS Poisoning Attack Illustrated



1. Attacker dynamically registers Service with database.
2. User connects and is “Load Balanced” to attacker.
3. User connect to attacker rather than database.
4. Attacker forwards to database.

Demo

TNS Poisoning Attack

http://joxeankoret.com/research.html

“Oracle TNS Poison un-auth proof on concept (Oracle 9i, 10g and 11g)”

Exploit Information

- **Joxean Koret**
  - http://joxeankoret.com/research.html
  - Oracle TNS Poison proof on concept
  - Oracle 9i, 10g and 11g
- **tnspoisonv1.py**
  - Used to poison the remote database listener
- **proxy.py**
  - Proxy on attacker machine to accept client connections and forward to database server

Identifying Vulnerable Databases

- **Check listener.ora for mitigation steps**
- **Use nmap (nmap.org)**
  - oracle-tns-poison script from https://gist.github.com/JukArkadiy/3d6cff222d1b87e963e7

```
nmap -Pn -sT --script=+oracle-tns-poison
-p 1521 192.168.2.18
```

TNS Poisoning Mitigation

Database Version	***SSL Encrypt with Cert***	***COST*** *class of secure transport*	***VNCR*** *valid node checking registration*
References	See ASO	1453883.1 1340831.1 (RAC)	1600630.1
8.1.7.x – 10.2.0.3	✓		
10.2.0.3 – 10.2.0.5	✓	✓	
11.1.0.x	✓	✓	
11.2.0.1 – 11.2.0.3	✓	✓	
11.2.0.4	✓	✓	✓
12.1.0.x*	✓	✓	✓ (Enabled by default)

* 12c does not allow remote registration by default.

VNCR – Valid Node Checking Registration

Valid Node Checking For Registration (VNCR) (Doc ID 1600630.1)

VALID_NODE_CHECKING_REGISTRATION_<listener_name>

Setting	*Description*
OFF **0**	**Disable VNCR** **11.2.0.4 default value**
ON **LOCAL** **1**	**Enable VNCR** **12.1.0.x default value**
SUBNET **2**	**All machines in the subnet are allowed registration**

VNCR – Problems

- Many examples on Oracle and other web sites use VALID_NODE_CHECKING_REGISTRATION_LISTENER – if the listener name is not LISTENER it does not work. The listener name must be used.
- VALID_NODE_CHECKING_REGISTRATION without the listener name does not work.
- 12c is secure by default, however, some My Oracle Support (MOS) notes recommended disabling.

VNCR – Valid Node Check Registration

REGISTRATION_INVITED_NODES_<listener-name>

Values are valid IPs, valid hosts, a subnet using CIDR notation (for ip4/6), or wildcard (*) for ipv4.

```
REGISTRATION_INVITED_NODES_Listener=

(net-vm1, 127.98.45.209, 127.42.5.*)
```

COST – Class of Secure Transport

- Using Class of Secure Transport (COST) to Restrict Instance Registration (Doc ID 1453883.1)
- Using Class of Secure Transport (COST) to Restrict Instance Registration in Oracle RAC (Doc ID 1340831.1)
- Required for 10.2.0.3 through 11.2.0.3

Contact Information

Stephen Kost

Chief Technology Officer

Integrigy Corporation

web: **www.integrigy.com**

e-mail: **info@integrigy.com**

blog: **integrigy.com/oracle-security-blog**

youtube: **youtube.com/integrigy**