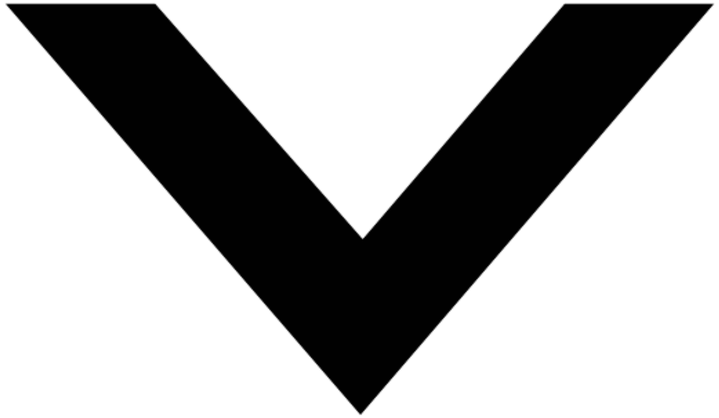


VICXER

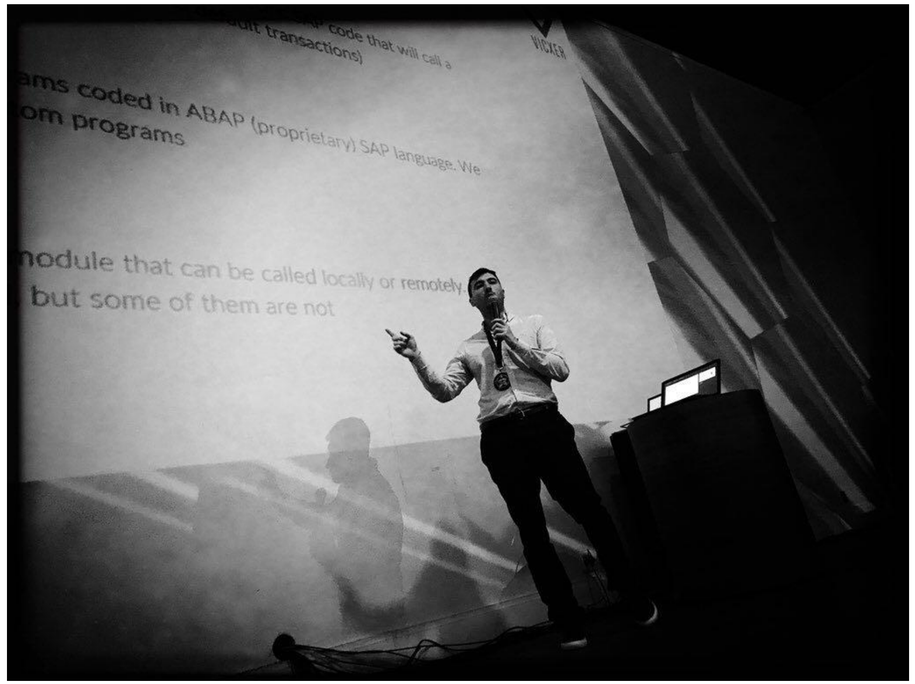
Spyware, Ransomware and Worms. How to Prevent the Next SAP Tragedy

HITCON 19

DISCLAIMER

- This publication contains references to the products of SAP AG. SAP, R/3, SAP NetWeaver and other SAP products.
- Products and services mentioned herein are trademarks or registered trademarks of SAP AG in Germany, in the US and in several other countries all over the world.
- SAP AG is neither the author nor the publisher of this publication and is not responsible for its content. The SAP Group shall not be liable for errors or omissions with respect to the materials.

VICXER



JORDAN SANTARSIERI

VICXER'S FOUNDER

Originally devoted to Penetration Testing, Vulnerability Research & Exploit writing, discovered several vulnerabilities in Oracle, SAP, IBM and many others.

Speaker and trainer at Black-Hat, OWASP-US, Hacker Halted, YSTS, Insomni'hack, AusCERT, Sec-T, RootCon, Ekoparty, etc.
I started researching ERP Software back in 2008.

Had the honor to secure more than 1000 SAP implementations all around the globe, including Fortune-500 companies, military institutions and the biggest ONG on the planet.

@JSANTARSIERI

VICXER

THE AGENDA

CHAPTER 01

Brief Introduction to SAP

CHAPTER 02

Project ARSAP is Born

CHAPTER 03

A Traditional Approach to Malware Distribution

CHAPTER 04

Ransomware and the Weaponization of Weaknesses

VICXER

CHAPTER 01

INTRODUCTION

A Brief Introduction to SAP

WHAT IS SAP?

VICXER

- SAP stands for ***Systems Applications and Products in Data Processing.*** It is a German company founded in 1972 by ex-IBM employees.

  - SAP counts 88,500+ Employees Worldwide
  - SAP Has 378,000+ Customers
  - Is Present in More Than 180 Countries
  - Dominate the Market With 87% of Forbes Global 2000

SAP

TWO TYPES OF SAP SOLUTIONS

VICXER

ENTERPRISE SOLUTIONS

- SAP ERP (Enterprise Resource Planning)
- SAP BI (Business Intelligence)
- SAP CRM (Customer Relationship Management)
- SAP SRM (Supplier Relationship Management)

These Solutions, provide direct services to end users

SUPPORTING SOLUTIONS

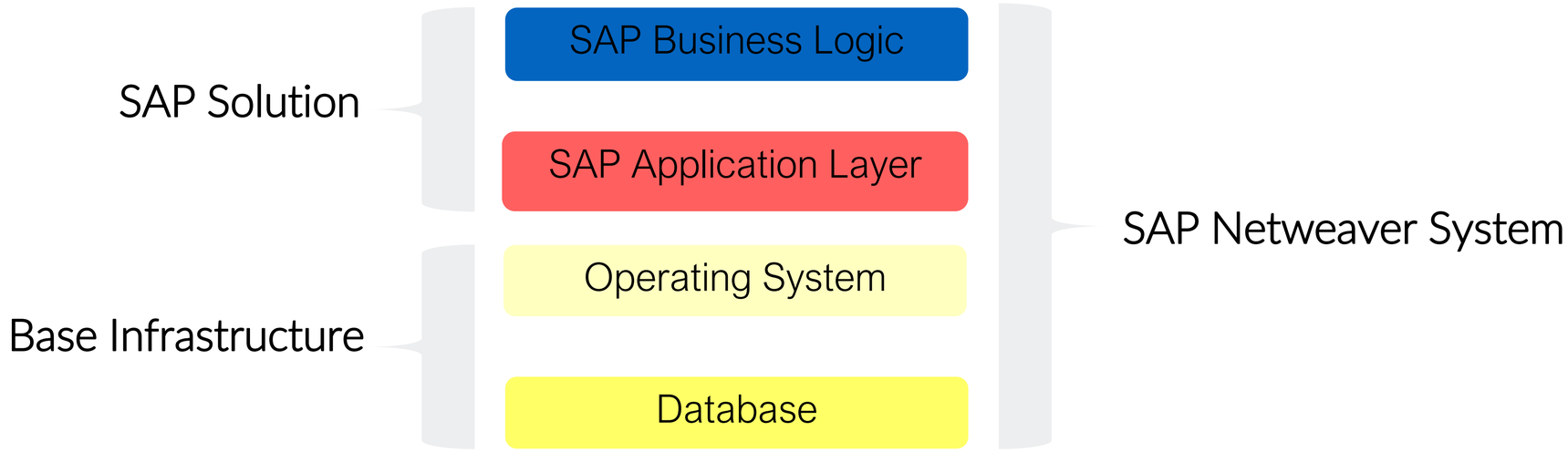
- SAP GRC (Government Risk and Compliance)
- SAP Business Objects
- SAP Mobile
- SAP Cloud Connectors

These Solutions support the operations of the Enterprise Solutions

SAP NETWEAVER

VICXER

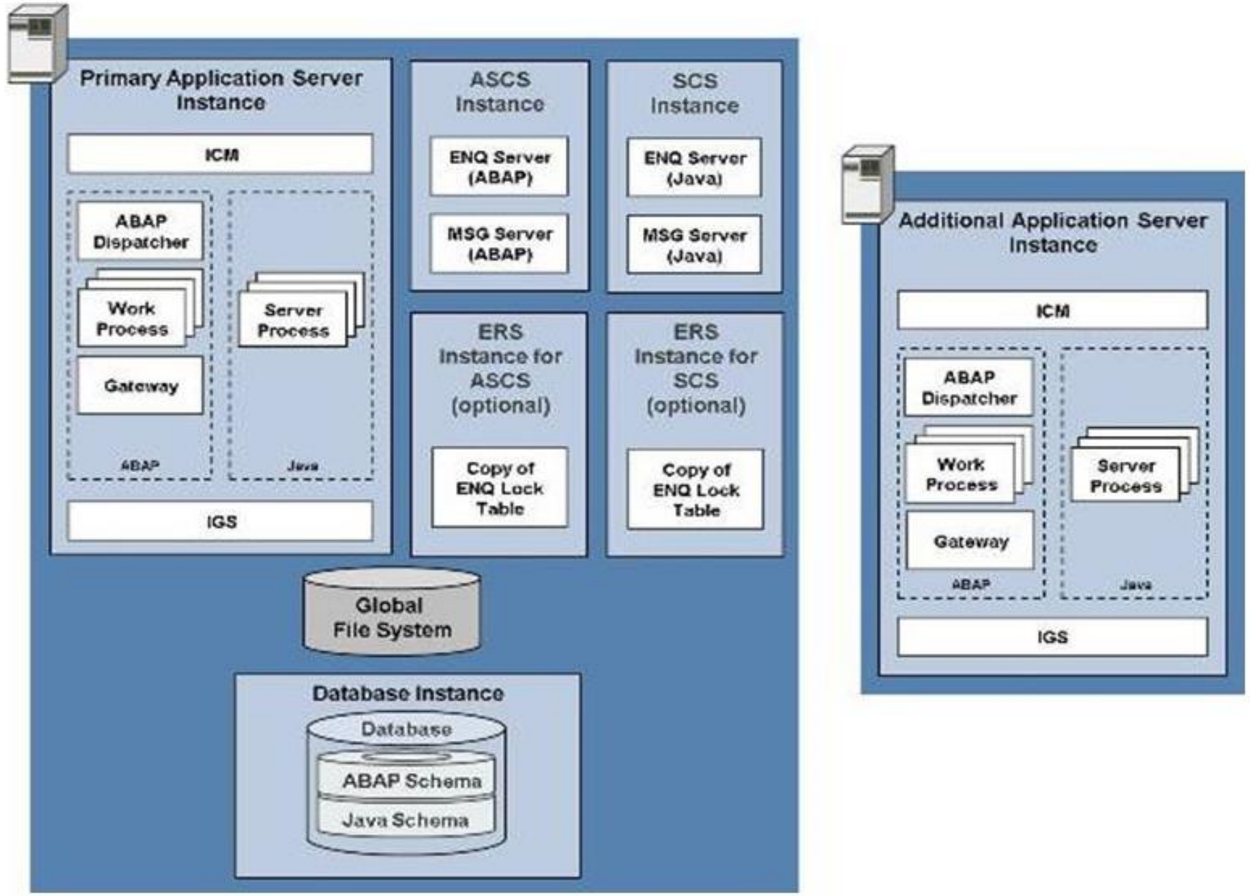
- Netweaver is the framework where SAP is built in. It is the most important technology so far as it synchronizes and regulates the operatory of the different SAP components
- Netweaver is **service** oriented! and it is divided in two different stacks, **ABAP** & **J2EE**.



SAP NETWEAVER

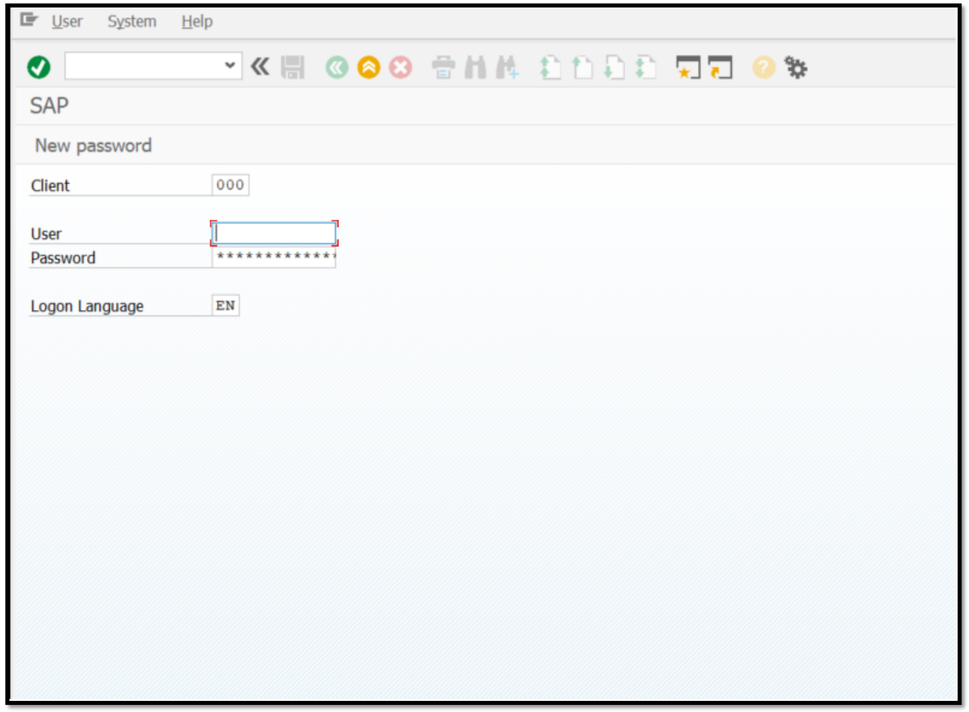
VICXER

- Each stack counts with different services, some of them are **shared between stacks**, some others are not
- Each one of those services will have **its own protocol** for communications. Some of them are **open**, but most of them **are proprietary**



SAP USER CLIENTS

- There are **MANY** ways that a regular user could use to connect to the SAP systems. The most popular ones are:
    - *SAP GUI (SAP proprietary protocol, extra thick client, around **1.4Gb** of size)*
    - *SAP Web Application Servers (ICM, Java HTTP, XSA)*



IN A FEW WORDS …

- Why would someone attack your SAP implementation? Easy….

"We don't like you"

"It's where the money is"

"Your organization highly depends on it"

VICXER

CHAPTER 02

A NEW BEGINNING

*“Project **ARSAP** is Born”*

ABOUT US

*WE ARE **VICXER!***

- A company focused in securing the business critical applications and its adjacent infrastructure (SAP, Oracle Siebel and others)
- All of our customers belong to the Fortune-500 Group
- We do:

  Oracle & SAP Penetration Testing

  Cyber-Security Trainings

  Vulnerability Assessment and Management

  SAP Forensics & Many More!

PROJECT ARSAP

VICXER

“Sometimes, reinventing the wheel makes sense” - Scenario

- As a young company, we had the same challenges that everyone else has when they just start, *getting new leads that could end-up in new customers*
- The approach that most companies take here, is to simply buy a list of businesses that are already running SAP, so they can try to “cold call” the CISO / security managers and pitch what they do
- The success rate of this procedure is 1%, same success rate that the spammers get. Coincidence? I think not!
- We said to ourselves, this cannot be the best possible way! there must be a more efficient way to tackle this challenge

……. and then the project ARSAP was born!

PROJECT ARSAP

VICXER

"Sometimes, reinventing the wheel makes sense" - Scenario

- We used search engines like *Shodan*, *Google*, *Bing*, *ZoomEye* to more **"sketchy"** and esoteric deep-web resources (deep-web search engines, private forums, etc.) in order to find the different SAP systems (**ABAP, Java, Business Objects, HANA**) that were already exposed to the Internet

- We ended-up creating one "**extractor**" per each data-source, as we knew since the very beginning that the SAP map that we would obtain would be "**alive**", meaning that the discovered SAP systems could come and go every-day ***(yes, people tend to expose non-productive SAP systems to the Internet too!)***

- Once we had a list of servers, we also had the necessity of categorizing and tagging the detected SAP systems for further analysis. Fortunately for us, the exposed SAP services were **QUITE verbose!**

```
server: SAP NetWeaver Application Server 7.21 / AS Java 7.31

     server: SAP NetWeaver Application Server 7.22 / AS Java 7.30

Server: SAP J2EE Engine/7.01
```

PROJECT ARSAP

VICXER

“Sometimes, reinventing the wheel makes sense” - Scenario

- At this point, we did not only have the list of exposed SAP systems, but we were also able to classify them per the exposed SAP services, country & continent (of the server hosting the SAP system), SSL support and the *different SAP / services version*!

- We used different techniques to discover what companies / individuals were behind the discovered assets.

- Now, of course, we needed a way to prioritize our efforts on which potential clients we would contact first, so what we did offline, was to analyze the detected SAP services versions and compare them to *our own vulnerability database.* This exercise allowed us to also classify the SAPs per “potential” risk *(as we did not actually trigger any attack probes)*

Are you intrigued about the results?

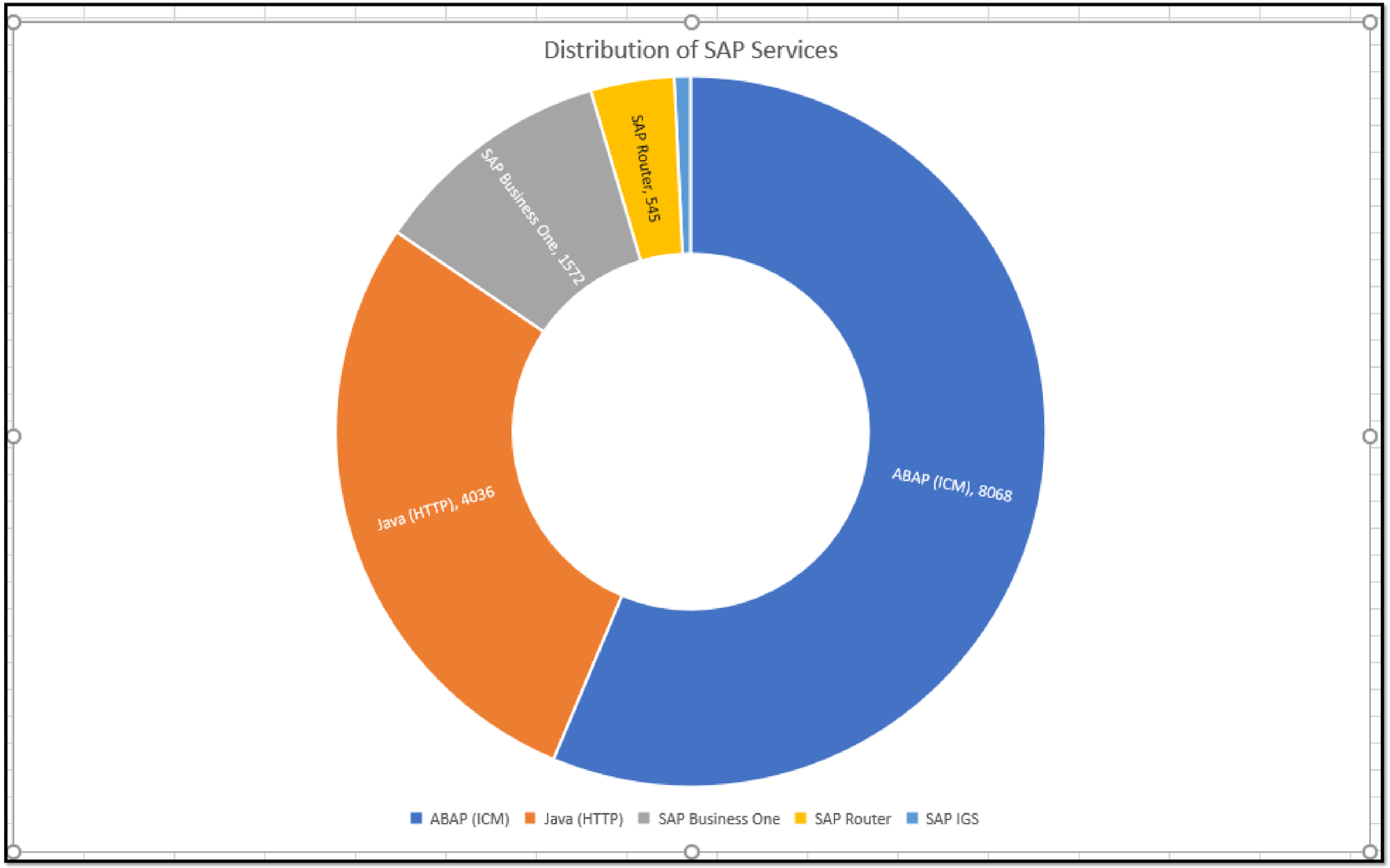
PROJECT ARSAP

VICXER

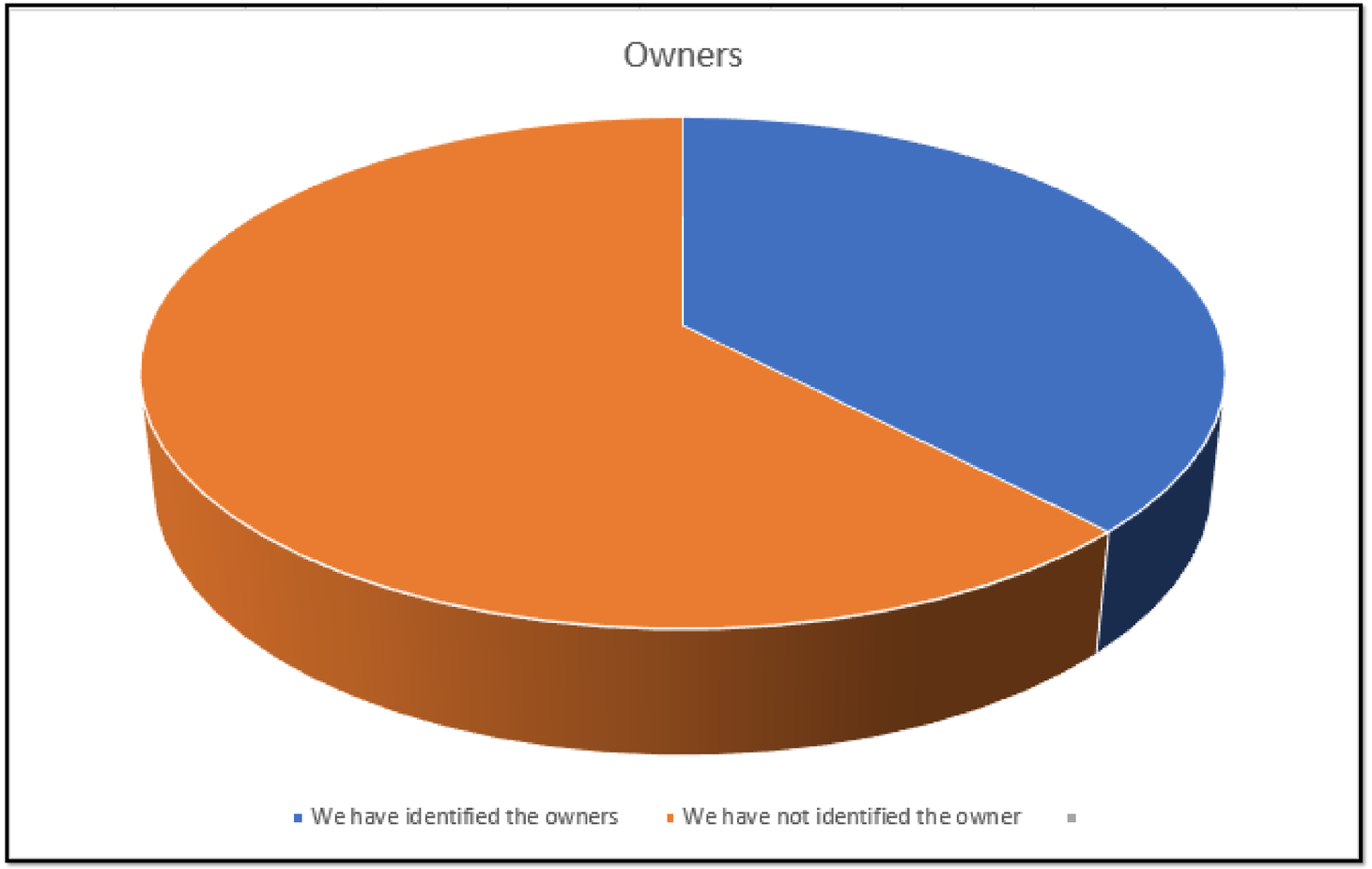
"ARSAP By the Numbers"

- We found more than **14k**

SAP Services



PROJECT ARSAP



"ARSAP By the Numbers"

- We have identified the owners of 37.86% of the detected assets

PROJECT ARSAP

VICXER

"ARSAP By the Numbers"

- We also discovered that at least **27%** of the detected assets were **potentially** vulnerable to **critical** and **high** criticity vulnerabilities like **RCE, Directory Transversal, Arbitrary File uploads / Arbitrary File Reads**
- We ended up being **highly surprised** by our discoveries and we immediately started to think that a sufficiently skilled attacker could provoke the **"next SAP tragedy"** without much effort
- How? you say, well, keep watching …

CHAPTER 03

YOU GOT EMAIL!

“A traditional approach to malware distribution”

YOU GOT EMAIL!

VICXER

“A traditional approach to Malware distribution” – Thinking Like an Attacker

- Think about it, if you were an attacker who has recollected the information that we highlighted on the previous slides, it would be trivial for you to enumerate email addresses from the people that works at the target company
- You know that the target organization uses SAP, probably across the board
- You know that the target organization has enough resources to acquire and use an SAP system. This indicates that the level of resources belonging to the company are high and the head-count is significant
- Almost all the big companies, with good amount of resources and a lot of employees use SSO (Single Sign-on) to facilitate access to SAP

YOU GOT EMAIL!

VICXER

“SAP Gui Scripts”

- In SAP Words

> *“SAP GUI Scripting is an automation interface that enhances the capabilities of SAP GUI. By using this interface, end users may automate repetitive tasks by running macro-like scripts”*

- By default, the execution of SAP GUI scripts is disabled, but in our experience, **90%** of corporate users use this functionality to do performance and functional testing

```
//-Set connection = application.Children(0)-----------------------
Connection = new ActiveXComponent(
  GUIApp.invoke("Children", 0).toDispatch()
);
//-Set session = connection.Children(0)---------------------------
Session = new ActiveXComponent(
  Connection.invoke("Children", 0).toDispatch()
);

//-Open SE16------------------------------------------------------
Obj = new ActiveXComponent(Session.invoke("findById",
  "wnd[0]/tbar[0]/okcd").toDispatch());
Obj.setProperty("text", "/nse16");
Obj = new ActiveXComponent(Session.invoke("findById",
  "wnd[0]").toDispatch());
Obj.invoke("sendVKey", 0);
```

YOU GOT EMAIL!

VICXER

“SAP Gui Scripts”

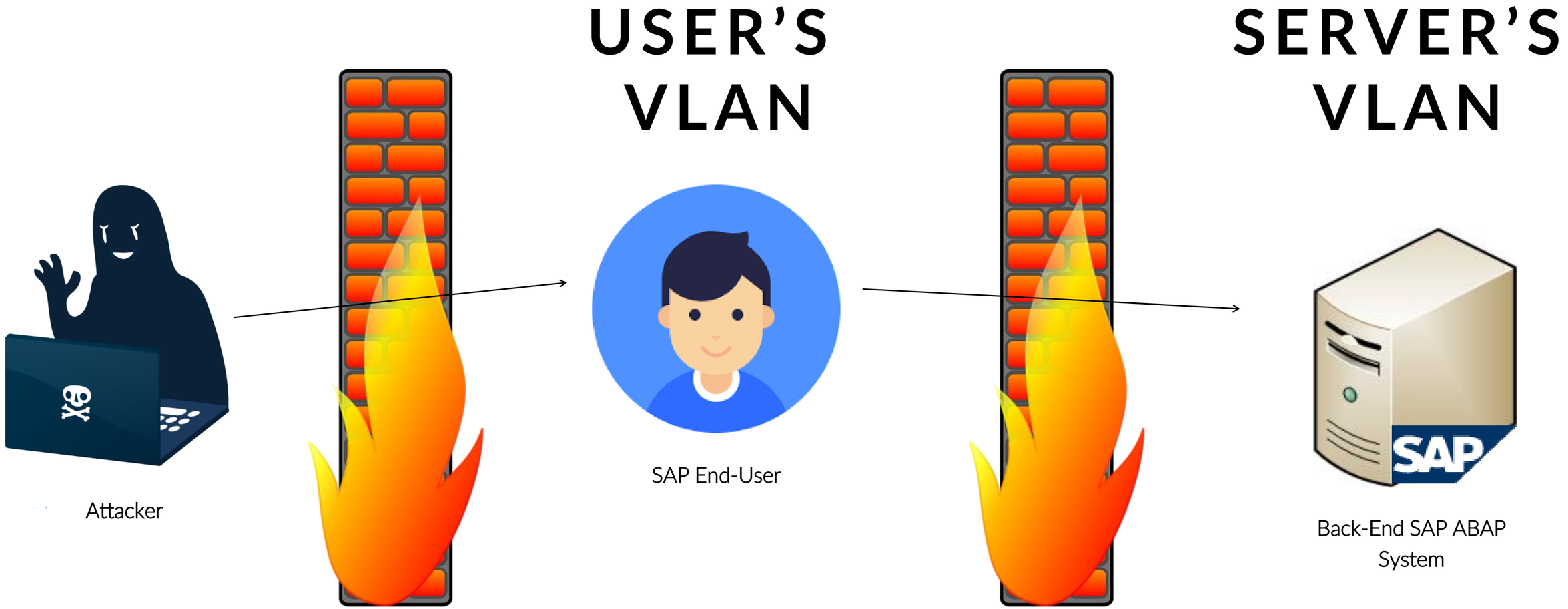
- The attacker has already harvested some corporate email accounts and is ready to send some malware
- The distribution channel will be an email with a malicious SAP GUI Script attached to it
- The attacker will leverage the privileges of the victim and use them to completely delete a table containing public debt, Robin Hood Style!

DEMO TIME!

WEAPONIZATION

VICXER

“You Got Email!” - Scenario



YOU GOT EMAIL!

VICXER

“SAP Gui Scripts” - Prevention

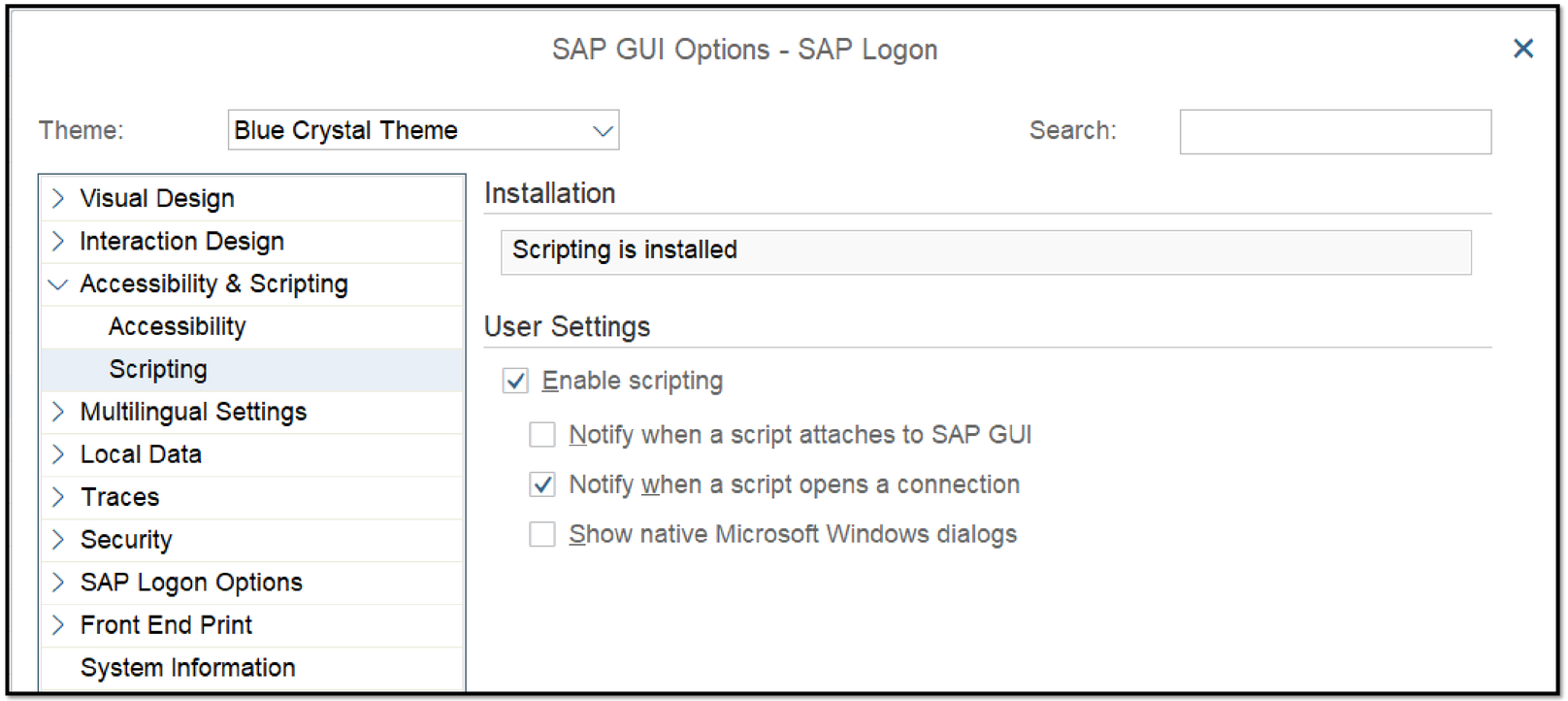
- If your organization is lucky enough to **not need SAP Gui scripts**, you could disable this functionality by making sure that the **sapgui/user_scripting** profile parameter is set to **FALSE**
- As we mention before, **most organizations cannot afford disabling SAP Gui scripts**, but fear not, there is a valid workaround!
- Leave the SAP Gui scripts enable and configure the **script/user_scripting_per_user** parameter to **TRUE**, then, just assign the authorization object **S_SCR** with value **16** to **(only)** the users that are allowed to use this functionality

YOU GOT EMAIL!

VICXER

"SAP Gui Scripts" - Prevention

- Also, **at the client level**, make sure you select the **"Notify when a script attaches to SAP GUI"** option, to get a warning from the SAP GUI whenever a scripts tries to be executed



VICXER

CHAPTER 04

WEAPONIZATION & PREVENTION

“Ransomware and the weaponization of weaknesses”

WEAPONIZATION

VICXER

"The Ransomware Approach"

- One of our recurrent thoughts after having the complete picture of the SAPs that were exposed to the Internet was ***"If a ransomware hits the SAP systems exposed to the Internet, the results would be catastrophic"***

- **We wanted to help**, but before we could recommend some countermeasures, we needed to think how an attacker could try to take over these assets…. (in SAP, that is no easy tasks)

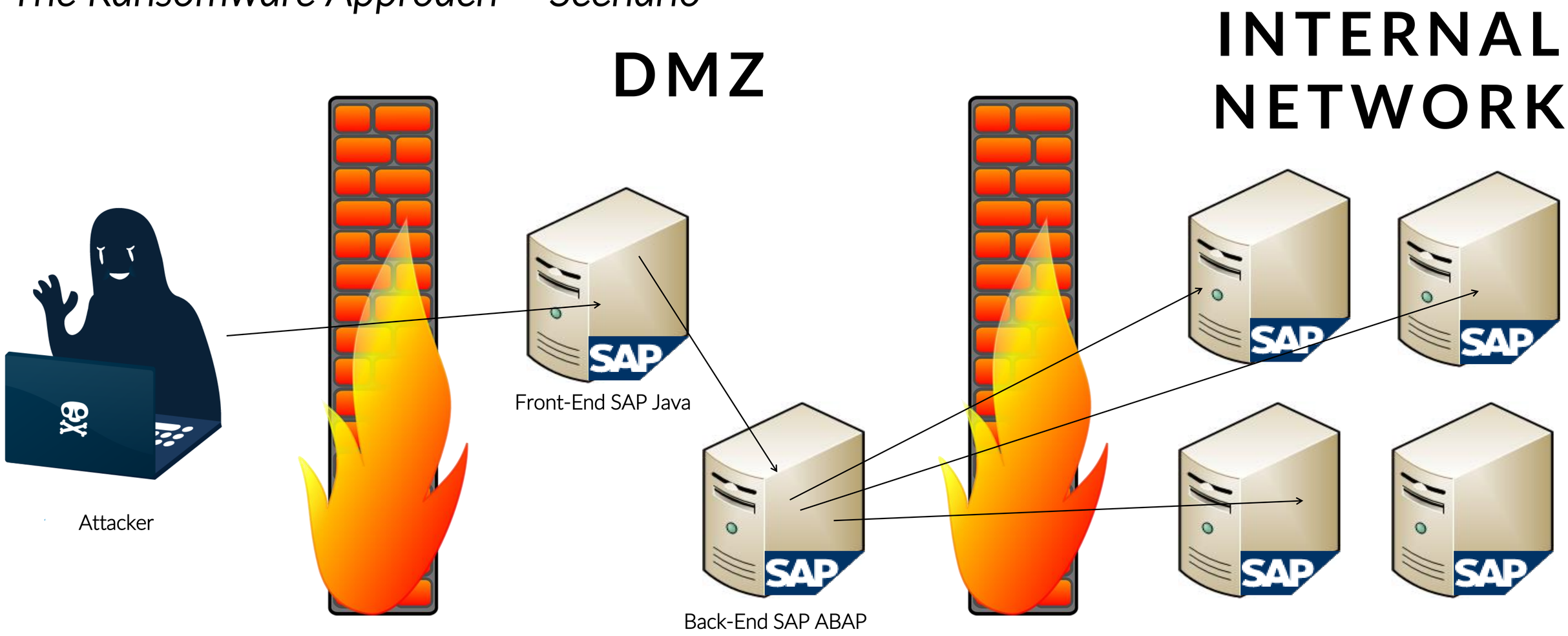
- By studying past ransomwares, we discovered that **most of them shared some "personality traits"**

    - They were designed to hit hard
    - Quick lateral movement was gold
    - Avoiding "making noise" was not a priority
    - Open to **"weaponize"** (aka reutilize) previously reported vulnerabilities

WEAPONIZATION

VICXER

“The Ransomware Approach” - Scenario



WEAPONIZATION

VICXER

"The Ransomware Approach"

- The hypothetical malware will be divided in **5 phases**

Stage	Action
Intrusion	*Remote Command Execution via SAP Java Invoker Servlet*
Credential Gathering	*Decrypting SAP Secure Storage*
Lateral Movement Around DMZ	*SSH / Password Guessing / Brute-force via RFC*
DMZ Escape / Lateral Movement Around Adjacent Network	*Credential Reutilization using SOAPRFC / Master Password*
Ransom & Expansion	*Encrypt all the things!!! And bonus!*

- Each action / stage will be complemented with the **technical attack / technique** and the respective **countermeasure**

- The full Ransomware / Malware **wont be distributed for obvious reasons ;-) but we will show some code!**

WEAPONIZATION

VICXER

“The Ransomware Approach” - Intrusion

- As other malwares like **WannaCry**, we will use a previously reported vulnerability and just **weaponize** the publicly available exploit. This makes sense as many sophisticated attackers already have **“malware frameworks”**, they just need a silver bullet and some vulnerable victims
- Per our network diagram, on the **first phase**, we are going to take over the **front-end SAP system** that is located inside the **DMZ**
- The exploit that we are going to use will allow us to execute operating system commands under the privileges of the operating system user that is running the SAP system. This vulnerability is due to a combination of **a default misconfiguration** and **a security vulnerability** in SAP
- Modern versions of SAP **are not vulnerable** to this exploit, but according to our research, finding a vulnerable systems is easy enough **(almost 3 out of 10!!!!)**

DEMO TIME!

PREVENTION

VICXER

“The Ransomware Approach” - Countermeasures

- To prevent the abuse of the **InvokerServlet** and the unauthenticated command execution, **SAP Notes 1445998**, **1589525** and **1624450 must** be implemented on the affected assets

- After the SAP security notes have been implemented, you need to be sure that the **Invoker Servlet functionality is globally disabled**. For that, use the *SAP Java config-tool* or open the *Netweaver administrator webpage (nwa)*, go to **Server Configurations,** locate the **servlet_jsp** option and make sure **EnableInvokerServletGlobally** is set to **False**

- WARNING !!! There is a known issue / bug in SAP that will prevent old versions to start after implementing this fix. Please read **SAP Note 1467771**, before disabling the **InvokerServlet**

- Unfortunately, changes will only take effect **once you restart your SAP systems**

WEAPONIZATION

VICXER

"The Ransomware Approach" – Getting some creds!

- Once the ransomware's target has been breached, the first thing that it needs to do is lateral movement
- The easiest way to extract credentials from a SAP Java system is by opening an encrypted file called SAP J2EE Secure Storage
- In the SAP Java systems, the secure storage is an encrypted container that lays on the file-system. This container is encrypted using 3-DES, a hardcoded key and an user key phrase which is defined at the installation time
- The container holds the SAP's database password and depending on the version, the SAP Java administrator password *(which is usually the same one, aka Master Password)*
- The container is extremely trivial to decrypt ……..

DEMO TIME!

PREVENTION

VICXER

“The Ransomware Approach” – Countermeasures

- Access to the SAP J2EE Secure Storage must be protected at all cost!
- Files:
    - /usr/sap/<SID>/SYS/global/security/data/SecStore.properties,
    - /usr/sap/<SID>/SYS/global/security/data/SecStore.key

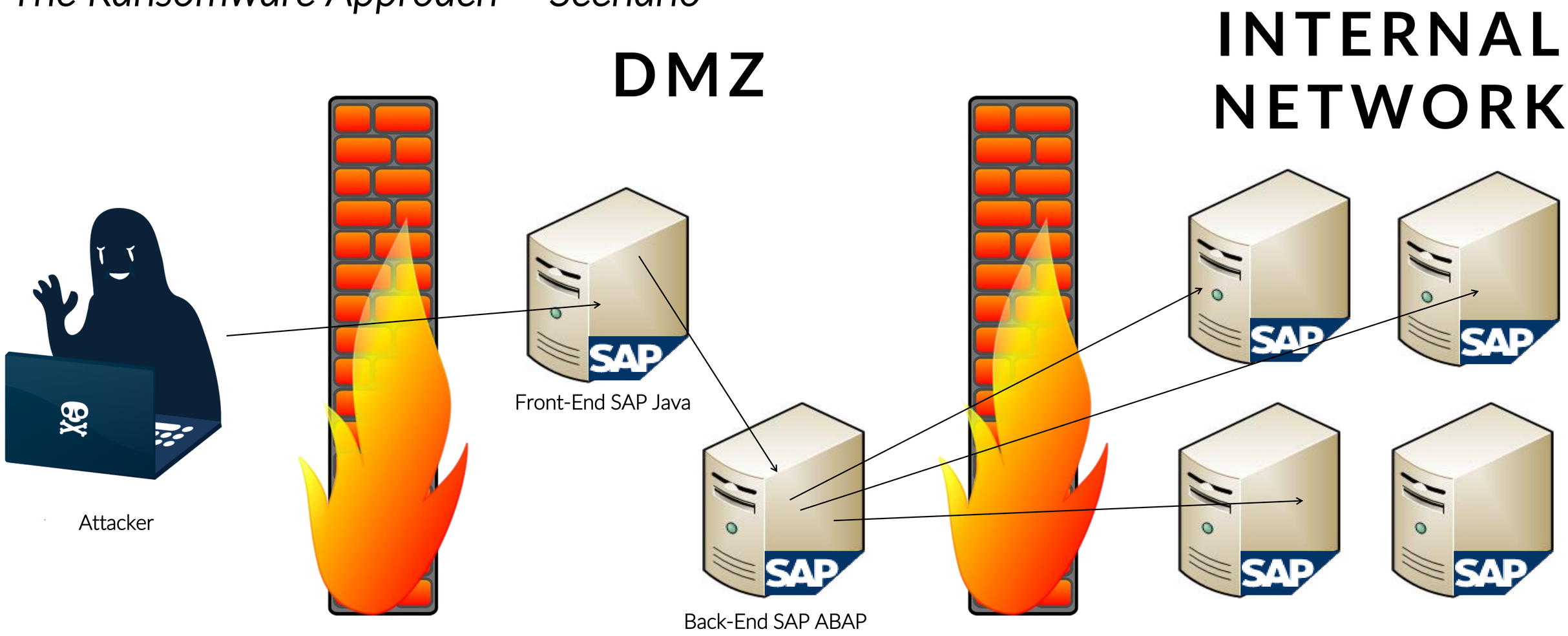
Should only be accessible by the SAP’s operating system user, local administrators and global admins

- Our selected encryption key phrase must be different from the SAP master password
- The password for the SAP Administrator must be different from the SAP database user

WEAPONIZATION

VICXER

“The Ransomware Approach” - Scenario



WEAPONIZATION

VICXER

“The Ransomware Approach” – Getting some creds!

- The ransomware now has the ability to **execute operating system commands** under the privileges of the user running the SAP system, has **full access to the local database** and **some important credentials for an eventual brute force**
- But this is not all….. In order to connect to other SAP systems of “different stacks” the SAP Java systems have a mechanism called **JCO Destinations,** these **destinations might contain sensitive data** such as **client, username** and **password** for remote systems (inside or outside the **DMZ**)
- Finally, we should always test if the passwords that we got so far correspond to the **SAP Master Password**. We could do this via **SSH** or **SMB**

DEMO TIME!

WEAPONIZATION

VICXER

“The Ransomware Approach” – Master Password!

- At the installation time, SAP will ask the user if he / she wants to assign **a different password for the most important SAP accounts** or use a **Master Password**
- **By default**, the installer suggests the implementation of **a Master Password**
- If the **Master Password** is selected, **the most powerful** SAP users like **SAP*, DDIC,** the **SAP’s database user** and the **SAP OS administrator** and the **SAP OS service user** *will all share the same password*
- **95%** of the surveyed companies **use** the **SAP Master Password** mechanism
- If one password is compromised ….

THE FINAL RESULT

VICXER

"A Screen that no one wants to see on their SAPs"

PREVENTION

VICXER

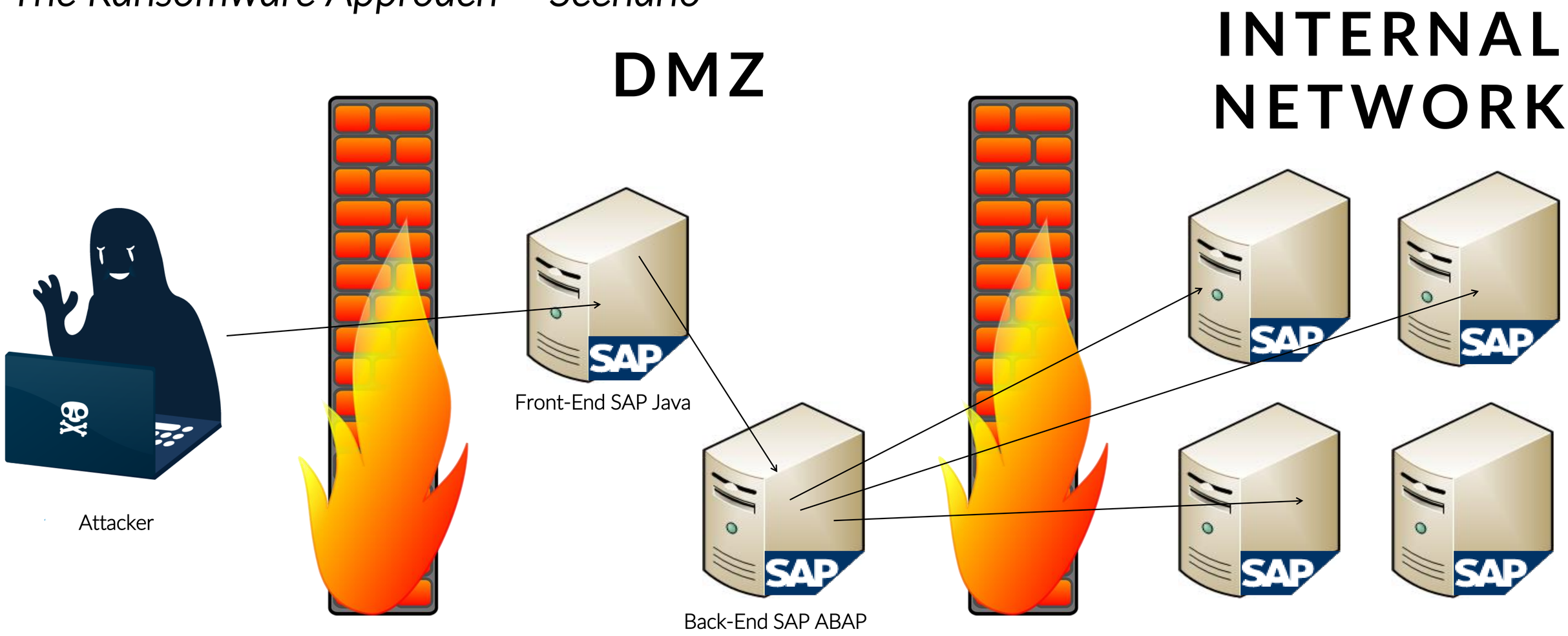
“The Ransomware Approach” – Countermeasures

- In order to protect your RFC destinations, first ask yourself the following question, do I have **a real business need** to create an RFC destination **with hardcoded** credentials?
- If the answer is **“Yes”** because you need to interact with a poorly designed interface (quite common on the SAP world) the **least privileged** approach must be follow
- Avoid the utilization of an **SAP Master Password**, each key account must have its own password, with such be in compliance to your local password policy
- Review your firewall strategy, how are you connecting your SAP systems on the DMZ and from the DMZ to the adjacent network. Allow traffic to **ONLY** the services that you require and nothing else

WEAPONIZATION

VICXER

“The Ransomware Approach” - Scenario



WEAPONIZATION

VICXER

“The Ransomware Approach” – Bonus Track

- **Now is time to leave the DMZ!**. One of the most notable characteristics of SAP is that it has been born to be interconnected
- We can safely assume that the **RFC** and the **ICM** ports will be accepting connections from the already compromised SAP systems on the **DMZ**
- The malware will attack the ICM services on the adjacent network by trying to reutilize the obtained credentials. The attack will target a particularly vulnerable service called **SOAPRFC**
- The malware will send **fake messages** from the SAP servers on the adjacent network to all the end-users (human beings) pretending to be the SAP administrators
- The users will receive a pop-up saying that a new **SAP add-on MUST be installed** and if they do not proceed with the installation, they will **“disrupt the SAP system”**

DEMO TIME!

VICXER

WRAPPING-UP!

WHAT DID WE LEARN TODAY?

WRAPPING-UP

VICXER

A Few Take-Aways …

- Always ask yourself, do I really need to expose my SAP system to the internet? If the answer is yes, you must **ONLY expose the bare minimum**
- Use an **SAP Web-dispatcher** to restrict access to **ALL the webpages that are not required by the business**
- Your Internet facing SAP systems must be patched! **follow SAP's security notes release cycle!** (New patches are available the second Tuesday of each month)
- Do not forget about the audit trails! **They will be invaluable in case the worst happens**
- Make sure your **SOC is "SAP Aware"**
- ***And finally….. Prevent, Prevent, Prevent***, conduct penetration testings regularly, distrust default configurations and always use the least privileged approach when in doubt! It will pay-off in the future!

THAT IS ALL...

VICXER

QUESTIONS?

To find out more about SAP, visit us at *https://vicxer.com* or follow us on Twitter

@VICXERSECURITY

@JSANTARSIERI