وزارة الاتصالات والتقانة

الهيئة الوطنية لخدمات الشبكة

مركـــز أمـن المعلومـــات

المخاطر المحدقة

بـنـظم تـخطيـط مـوارد المؤسسة

Enterprise Resources Planning

ERP Systems

إعداد

م. سلمان سليمان

رئيس مركز أمن المعلومات

أيلول-2018

مقدمة

مع وجود مئات الآلاف من التطبيقات البرمجية حول العالم، يقوم نظام تخطيط موارد المؤسسة ERP SYSTEM بتنفيذ إجرائيات العمل واستضافة البيانات الأكثر حساسية في المنظمات والشركات الكبرى في العالم، وفي ظل التوجهات المتنامية لاستخدام هذه النظم في الجهات الحكومية والشركات العامة والخاصة في بلدنا، قمنا في مركز أمن المعلومات بالتطرق لهذا الموضوع على أهميته من الناحية الأمنية من خلال هذه الدراسة التي اعتمدت في مصادرها على تقرير بحثي أعدته شركة Digital Shadows and Onapsis العالمية بهدف إلقاء نظرة عميقة على تطور مشهد التهديدات الأمنية لنظام تخطيط موارد المؤسسة بمرور الوقت، حيث تم تركيز الجهود والأبحاث على النظامين الأكثر انتشاراً واعتماداً على صعيد المؤسسات والشركات الكبيرة وهما تطبيقي SAP و Oracle E-Business Suite ، والمخاطر والتهديدات التي يجب أخذها على محمل الجد، ويمكن أن تعمم النتائج على جميع تطبيقات ERP الأخرى.

يساعد هذا التقرير كبار المسؤولين التنفيذيين لأمن المعلومات في المنظمات والشركات التجارية الخاصة والحكومية في فهم وإدارة تطبيقات تخطيط موارد المؤسسة الخاصة بهم وحمايتها من التعرض للهجمات السيبرانية، مما يمكنهم من تخفيف المخاطر المحتملة عن طريق اتباع توصيات معينة وبالتالي إلى مزيد من الأمان والمرونة في العمل.

التعريف بتطبيقات تخطيط موارد المؤسسات ERP

مجموعة من التطبيقات البرمجية التي تدعم وتشغل إجراءات العمل الأساسية للمنظمات والشركات بالإضافة للعمليات التجارية والمالية والإدارية، وفي هذه الدراسة سيتم استخدام مصطلح ERP للدلالة أيضاً إلى تطبيقات أخرى مثل:

- إدارة رأس المال البشري Human Capital Management HCM
- إدارة سلسلة التوريد Supply Chain Management SCM
- إدارة علاقات العملاء Customer Relationship Management CRM
- إدارة دورة حياة المنتج Product Lifecycle Management PLM
- إدارة علاقات الموردين Supplier Relationship Management SRM
- ذكاء الأعمال Business Intelligence BI
- إدارة دورة حياة الأصول Asset Lifecycle Management ALM
- تكامل الأعمال والتصنيع والعمليات

  Manufacturing and Operations MO and Process Integration PI.

في العديد من المؤسسات والشركات يقع نظام تخطيط موارد المؤسسة على عاتق فريق تقني مخصص لهذا النظام ولسوء الحظ إن أمن هذا النظام لا يعتبر أولوية لهذا الفريق، وبالنتيجة تبقى هذه النظم دون تحديث وتطوير ومعالجة للثغرات الأمنية لسنوات تحت مسمى أولوية الضرورة التشغيلية واستمرارية العمل.

فقد أصدر مركز الاستجابة للطوارئ المعلوماتية الأمريكي US-CERT في شهر أيار لعام 2016 تحذيرًا مفاده أن 36 منظمة عالمية على الأقل قد تعرضت لهجمات الكترونية عن طريق استغلال ثغرة أمنية مضى على اكتشافها خمس سنوات في نظام SAP وهذا فقط غيض من فيض، حيث واصلت الجهات المستهدِفة لهذه النظم تطويرها لأساليب مهاجمة نظم تخطيط موارد المؤسسات ERPs.

وعلى الرغم من أهمية هذه المنصات التجارية الحساسة لتشغيل الشركات والاقتصادات الحديثة، فقد عانى مجتمع الأمن المعلوماتي من نقص المعلومات المتعلقة بالتقنيات والتكتيكات والإجراءات المستخدمة TTPs من قبل الجهات التي تعمل على استهداف هذه النظم لأغراض التجسس السيبراني والتخريب والاحتيال المالي.

إن هذا التقرير يكشف النقاب عن أبحاث جديدة واستطلاعات للتهديدات التي تم استخلاصها من مواقع الويب المفتوحة و مواقع الويب العميق والويب المظلم، ويسلط الضوء على كيفية مشاركة جهات عديدة وبنشاط في مهاجمة هذه التطبيقات، وما ينبغي للمنظمات والشركات والمؤسسات القيام به لتخفيف أثر هذه المخاطر الحرجة.

الجهات التي تستهدف نظم إدارة المؤسسات

- مجموعات الاختراق: Hacktivist Groups تهاجم بفعالية تطبيقات تخطيط موارد المؤسسات لتعطيل العمليات التجارية الحرجة واختراق المنظمات المستهدَفة.
  حيث تم إيجاد الدليل على قيامها بأكثر من تسع هجمات إلكترونية على الأقل بالاشتراك مع منظمات أخرى مجهولة، تتضمن استهداف تطبيقات SAP وOracle EBS.
- المجرمون السيبرانيون Cybercriminals: الذين يقومون بتطوير برمجيات خبيثة لاستهداف نظم ERP لتعمل من الداخل خلف تجهيزات الحماية Firewalls من خلال سرقة بيانات الدخول لتمكينهم من التسلل إلى داخل هذه النظم.
- منظمات قومية مدعومة من بعض الدول: استهدفت هذه المنظمات نظم ERP بغرض التجسس الإلكتروني والتخريب، حيث تم إيجاد الدليل على قيام هذه المنظمات باختراق هذه النظم للحصول على بيانات حساسة جداً، وتعطيل بعض الأعمال التجارية الحرجة.

المؤشرات على تزايد التهديدات والمخاطر التي تستهدف تطبيقات ERP

- زيادة الاهتمام بشكل واضح من قبل المجرمين السيبرانيين في مواقع الويب العميق باستغلال ثغرات نظم تخطيط موارد المؤسسات، حيث تم الحصول على معلومات يتم تداولها على هذه المواقع عن قرصنة تطبيقات SAP، ولوحظت زيادة بنسبة 100% في عمليات القرصنة لتطبيقات SAP و Oracle EBS خلال السنوات الثلاث الماضية، كما لوحظت زيادة بنسبة 160% في الاهتمام باستغلال ثغرات معينة لتطبيقات ERP بين العامين 2016 و2017.
- تتطور الهجمات الالكترونية الموجهة ولا تزال تستفيد بشكل رئيسي من استغلال ثغرات مشهورة في هذه النظم بسبب النقص في درجة أمان هذه النظم وعدم تطبيق التحديثات الأمنية لمعالجة الثغرات، بالإضافة للثغرات الناتجة عن الإعدادات غير الصحيحة من الناحية الأمنية عند تنصيب هذه النظم. والملاحظ أن المهاجمين ليسوا بحاجة إلى اكتشاف واستغلال الثغرات الأحدث zero-day attacks بوجود ثغرات حرجة تعود لأكثر من 7 أعوام ولم يتم معالجتها بعد.
- إن التحولات الرقمية واستخدام الحوسبة السحابية وتطبيقات الهواتف الذكية تزيد من إمكانية استهداف منظوماتERP من قبل قراصنة المعلومات، حيث تم تحديد أكثر من 17000 نظام SAP وتطبيق من تطبيقات ERP متصل بشبكة الانترنت تعود لكبريات الشركات الحكومية والخاصة في العالم، في الولايات المتحدة وألمانيا والمملكة المتحدة الأكثر عرضة لهذه الهجمات.
- إن تسرب المعلومات من قبل أطراف أخرى كالموظفين العاملين على هذه التطبيقات والعملاء يمكن أن يعرض تطبيقات ERP للخطر ويسهل من مهمة الجهات المستهدِفة، كما تم اكتشاف وجود أكثر من 500 ملف من ملفات الإعدادات الخاصة بنظام SAP منتشرة عبر مواقع الويب، والخطر الناجم عن هذه الأطراف الأخرى في ازدياد مستمر.
- الضوابط التقليدية الأمنية الخاصة بتطبيقات ERP مثل إدارة هوية المستخدم وفصل الصلاحيات والواجبات غير مجدية في اكتشاف التقنيات المستخدمة من قبل الجهات المستهدِفة ومنع حصول اختراقات أمنية.

الدراسة الإحصائية

تعتمد المنظمات والشركات والمؤسسات على هذه التطبيقات كما أشرنا، في العمليات التجارية مثل الرواتب، الموازنة، العمليات المستودعية، الإدارة والتصنيع والتخطيط المالي والمبيعات والخدمات اللوجستية والفواتير، لذلك تستضيف هذه التطبيقات معلومات وبيانات حساسة، بما في ذلك النتائج المالية، وصيغ التصنيع، والتسعير،

الملكية الفكرية، وبطاقات الائتمان والمعلومات الشـخصـية PII للموظفين والعملاء والموردين كما يبين الشـكل التالي:

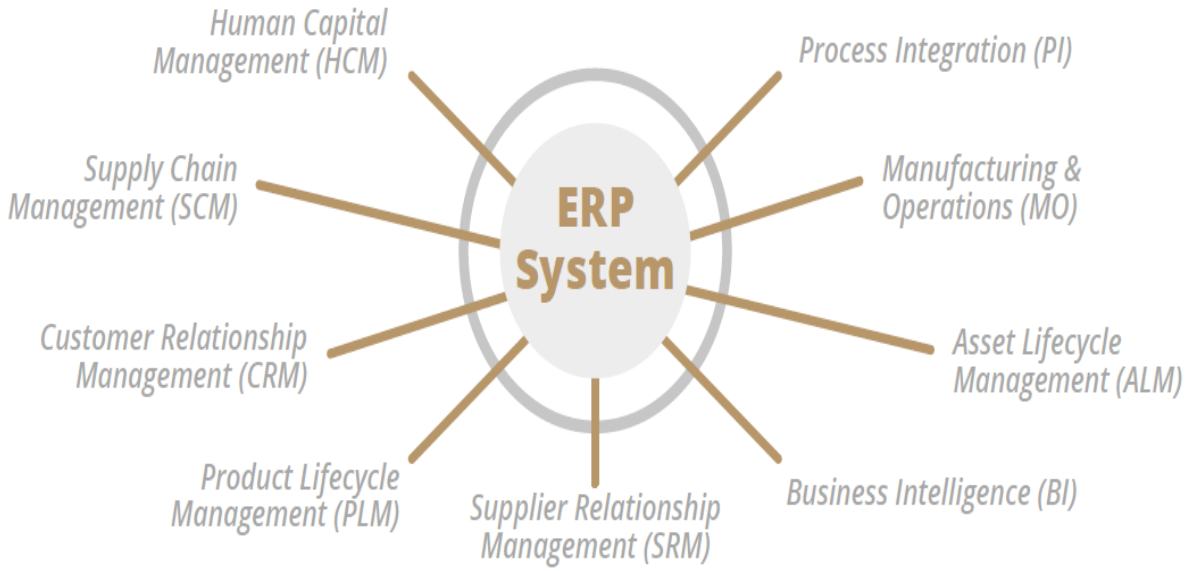


Figure 1: ERP Applications Hold Organizations' Sensitive Information, such as Payroll, Financials, Business Processes, etc.

تشير الاحصائيات إلى أن معظم كبريات الشركات في العالم تعتمد في تنصيب وتشغيل تطبيقات تخطيط موارد المؤسسة على مَوردين رئيسين كنواة للنظام هما:

SAP
SAP Business Suite and SAP S/4HANA

Oracle
Oracle E-Business Suite (EBS)

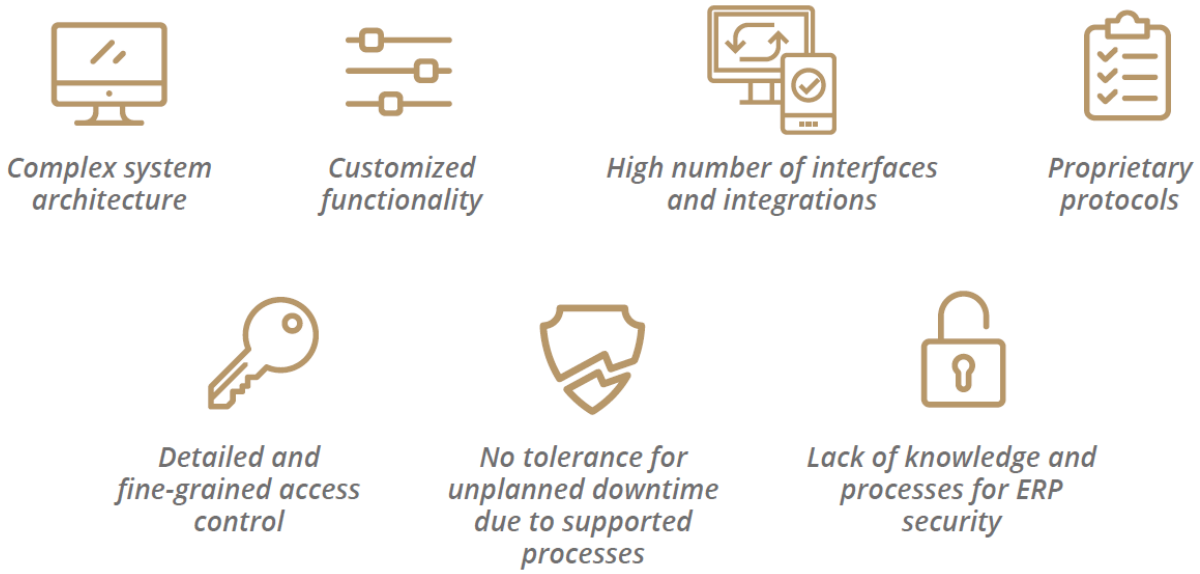
وبالتالي مئات الآلاف من منتجات هاتين الشـركتين تنتشـر عبر العالم وتهيمن على كبرى الشـركات في مجال المال والأعمال وتستضيف البيانات الأكثر حساسية وتأثيراً على عمل هذه الشركات لذلك ستركز الدراسة على منتجات هذين الموردين الأساسيين لمعظم تطبيقات تخطيط موارد المؤسسات ERP في العالم.

الثغرات الأمنية في نظم ERP

كباقي التطبيقات البرمجية، فإن تطبيقات ERP لا تخلو من الثغرات الأمنية التي يمكن أن تســـتغل من قبل جهات عديدة، وعدد هذه الثغرات في ازدياد دائم، ونســـرد فيما يلي أهم العوامل التي تجعل من تطبيقات ERP عرضة للتهديدات والمخاطر الأمنية:

- **عدم الاهتمام بالتحديثات الأمنية بالشكل الكافي:**

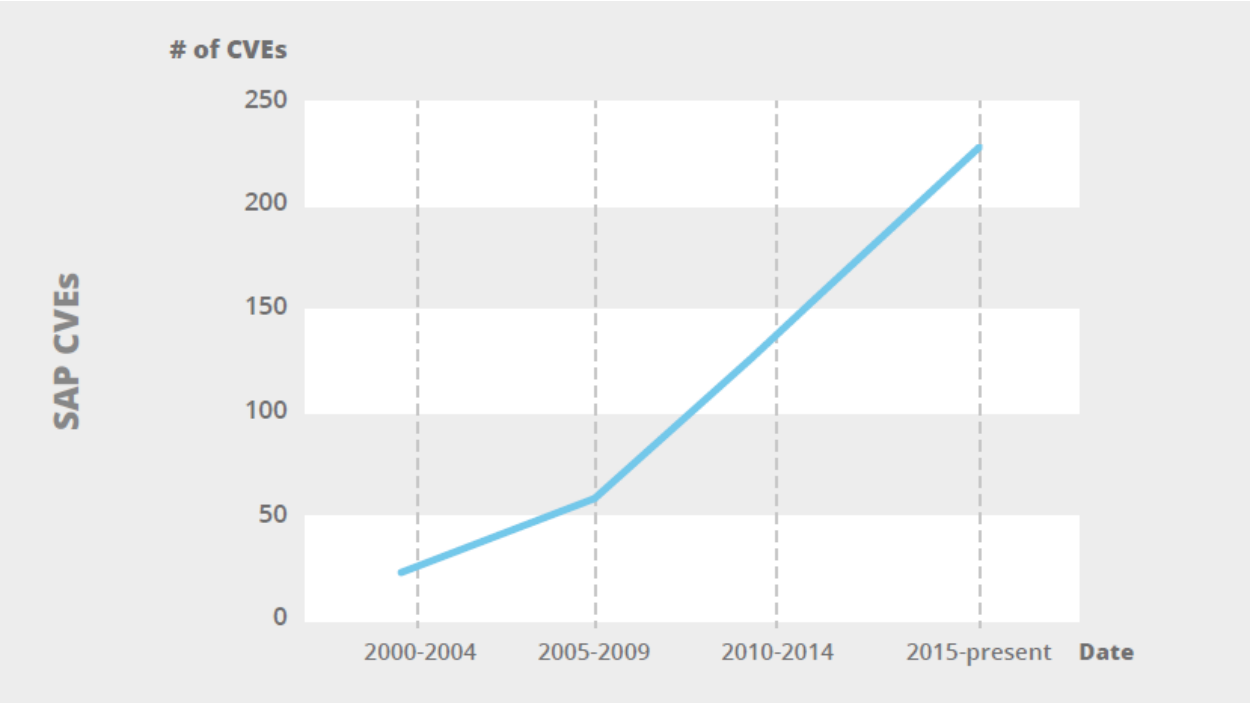
يكافح مستثمرو هذه التطبيقات لتطبيق التحديثات الأمنية لهذه الثغرات، لكن توجد مجموعة من الأسباب التي تصعب مهمة المستثمرين في تنصيب أحدث الترقيعات الأمنية وضبط الإعدادات الصحيحة لمعالجة هذه الثغرات، والنتيجة تشغيل تطبيقاتERP غير مؤمنة جيداً ضد الاختراق وأهم هذه الأسباب:



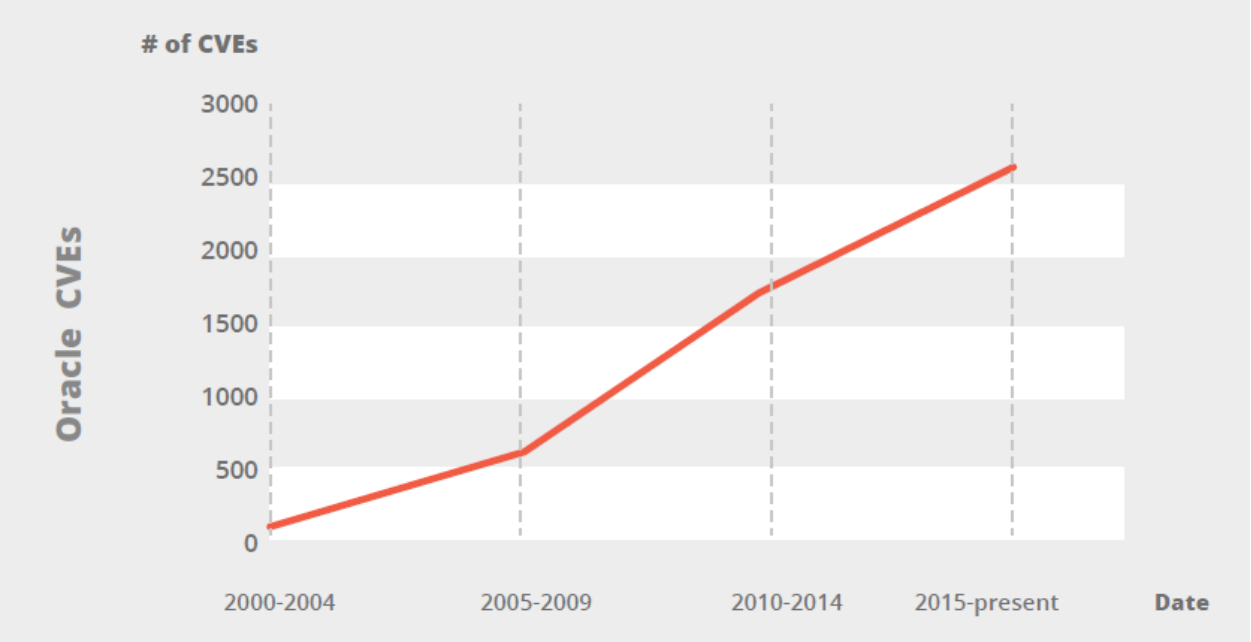
كذلك الأمر، يسعى مستثمرو هذه النظم للاختيار الأفضل لأهم الثغرات التي يجب معالجتها من قبلهم لتخفيف الضرر الناجم عنها، وفي الحالة المثالية يجب معالجة جميع الثغرات الأمنية بلا استثناء وفي الوقت المناسب، لكن في كثير من الأحيان يتعارض ذلك مع أولوية العمل والتنافس القائم بين هذه الشركات.

سوف نستخدم مصطلح معرف للثغرات الأمنية CVE الذي يستخدم لتعريف كل ثغرة أمنية وتصنيفها وفق معيار عالمي.

وكما يمكن اســـتنتاجه من المخطط التالي، الثغرات الأمنية وترقيعاتها في ازدياد مســـتمر، وحتى الآن أكثر من 4000 ترقيع أمني لتطبيقات SAP و5000 ترقيع أمني للتطبيقات الموردة من قبل شركة Oracle.



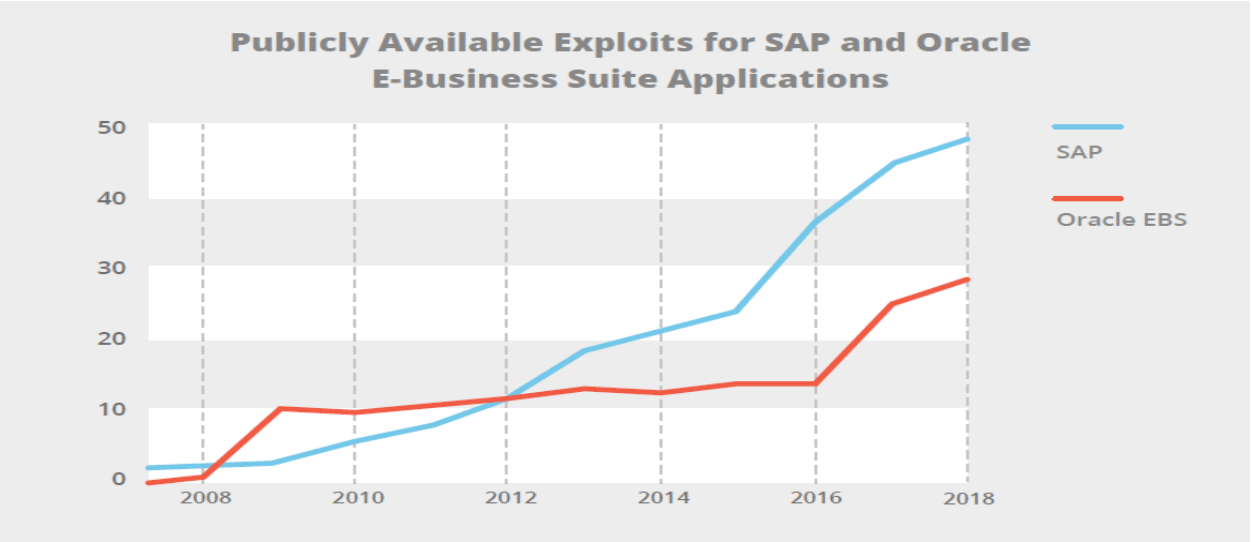
Graph 1: Evolution of SAP CVEs [6]



Graph 2: Evolution of Oracle CVEs [6]

- **تزايد الاهتمام بتطوير أساليب استغلال ثغرات تطبيقات ERP**

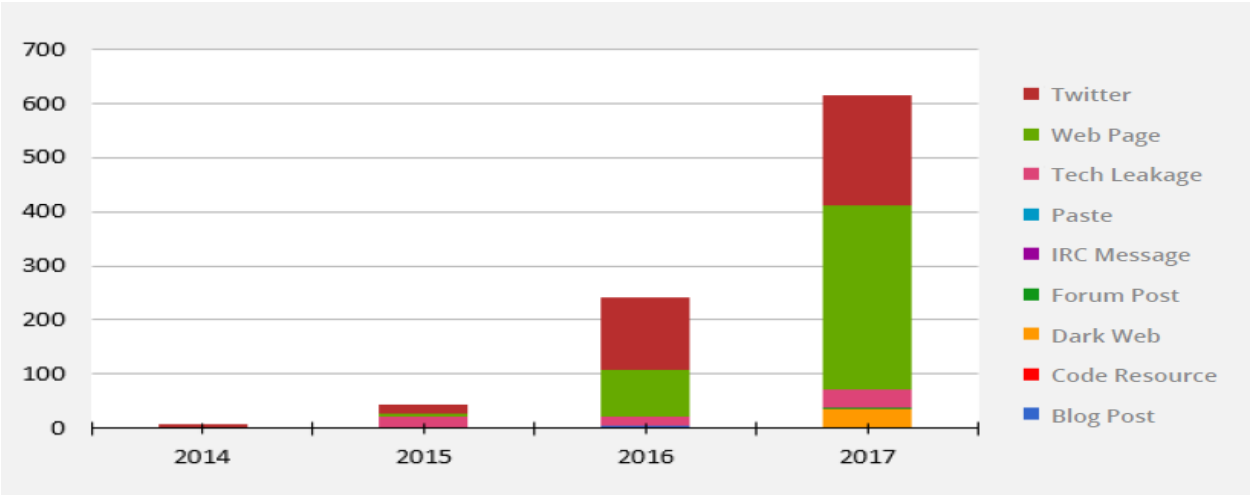
العديد من الثغرات الأمنية المكتشفة في هذه التطبيقات لا تزال قابلة للاستغلال رغم مضي زمن طويل على اكتشافها، ويتم تداول هذه الثغرات وطرق استغلالها بالإضافة لبيعها على مواقع الويب العميق ومنظمات القرصنة الالكترونية ومن لف لفيفهم، وعلى سبيل المثال على أحد هذه المواقع https://0day.today تم إيجاد ما يقارب 50 رماز برمجي لاستغلال ثغرات تطبيقات SAP و 30 رماز برمجي لاستغلال ثغرات تطبيقات Oracle EBS حتى عام 2018:



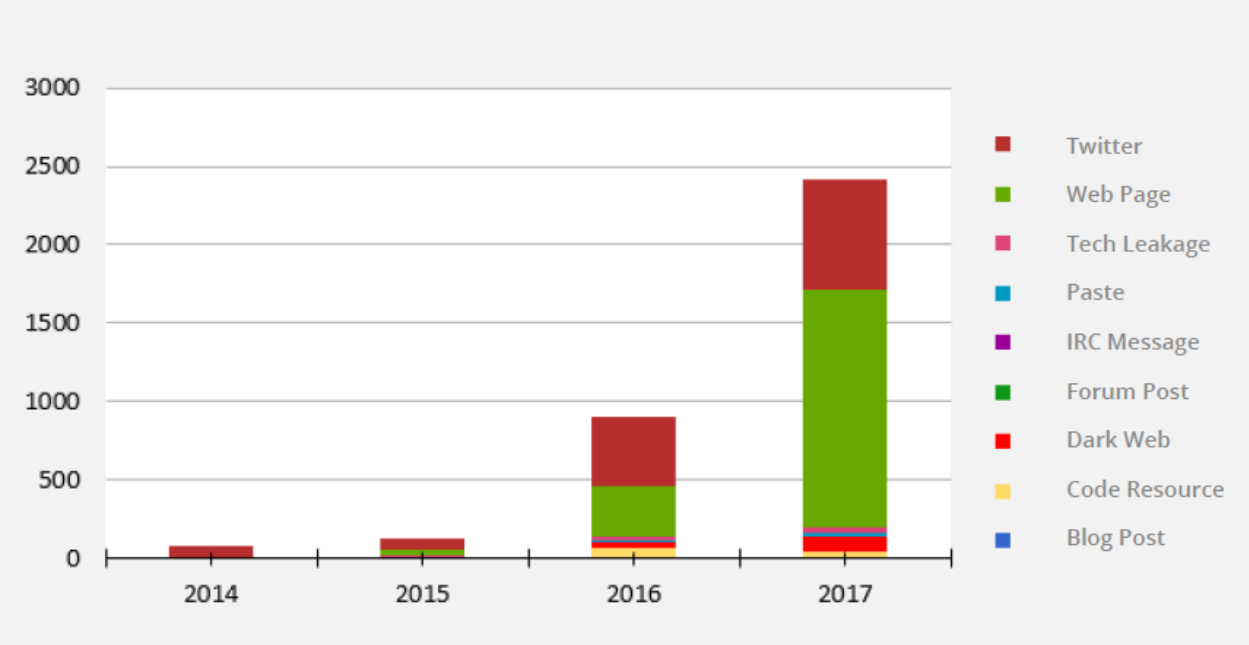
Graph 3: Evolution of SAP and Oracle EBS Publicly-Available Exploits [7]

ومن خلال تحليل البيانات حول الثغرات الأمنية في نظم ERP والتي تم جمعها من مصادر متنوعة مثل الويب المظلم والويب العميق ومواقع منظمات إجرامية ومواقع التواصل الاجتماعي، نستطيع أن نؤكد التنامي المتزايد لتركيز الاهتمام بالثغرات الأمنية في تطبيقات ERP وعلى وجه الخصوص تطبيقات SAP and Oracle EBS technologies ويعتبر تزايد عدد معرفات هذه الثغرات CVEs مؤشراً واضحاً على ذلك.

ويوضح المخططين التاليين تزايد نسبة الاهتمام بهذه الثغرات وفقاً للمواقع والمصادر التي تم تداولها من خلالها:



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



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

- **الآلاف من تطبيقات ERP تعمل على تماس مباشر مع شبكة الانترنت Online**

تسمح تطبيقات ERP للشركات والمنظمات بإتاحة إجرائيات العمل لشريحة واسعة ومتعددة من العملاء، وفي كثير من مجالات عالم المال والأعمال، وهذا يستدعي وجود متطلبات معينة للعملاء للعمل على التطبيق عبر شبكة الانترنت، إن إمكانية الوصول لهذه التطبيقات عبر واجهات معينة على شبكة الانترنت لا يعد مخاطرة بحد ذاته، لكن لتجنب أن يتحول هذا الأمر إلى وضع عالي الخطورة يجب أن تتخذ التدابير الأمنية الصحيحة من قبل المنظمات والشركات.

إن أحد مواضيع هذا المشروع البحثي هو فهم مدى توافرية وانكشاف تطبيقات ERP بشقيها SAP and Oracle EBS على شبكة الانترنت وبيان ذلك باستخدام أدوات برمجية شائعة ومتاحة للجميع.

حيث يمكن استخدام محرك البحث Google لإيجاد محتوى محدد لنظام معين باستخدام أساليب البحث المتقدم لإيجاد ما يسمى بـــ Google Dorks المعروفة جيداً لدى الجهات المستهدِفة لهذه التطبيقات، ومن بعض الأمثلة التي نستخدم فيها السياق التالي للبحث المتقدم:

”intitle:”ITS System Information” “Please log on to the SAP System”

والنتيجة عدد كبير من واجهات الدخول:

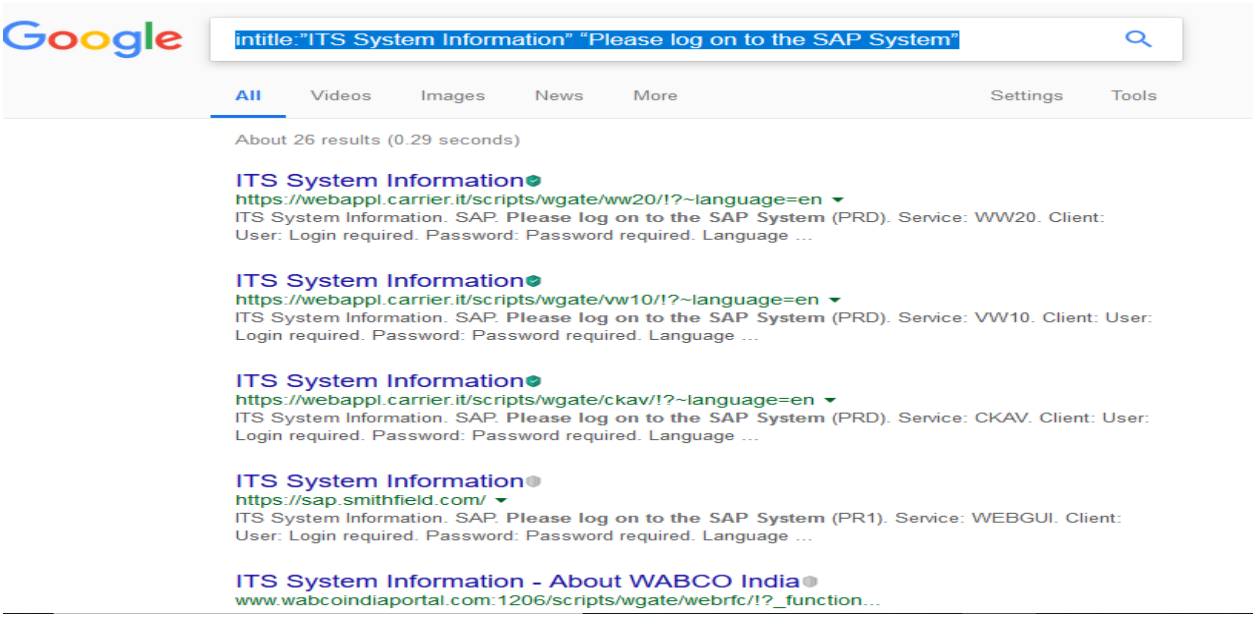


Figure2: findings by Google Dorks statements

كذلك تنتشر هذه التعليمات للبحث المتقدم على مواقع الويب العميق ومن الأمثلة:

```
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:box
```

Figure3: Example of Google Dork for SAP Identified in Cybercrime Underground Site (Cebolla Chan)

إحدى هذه التعليمات يمكن استخدامها لإيجاد مخدم الويب لتطبيق SAP للمعاملات التجارية SAP Internet Transaction Server، ووفق الشـــركة المطورة فإن هذا المخدم لم يعد يخضـــع لعمليات الصـــيانة والدعم والترقيعات الأمنية.

ويمكن باســـتخدام تعليمات البحث المتقدم لمحرك البحث غوغل تحديد أكثر من 100 مكون برمجي لتطبيقات SAP تعمل وجهاً لوجه مع شبكة الانترنت، وهذا المؤشر كافٍ للشركات لتعلم مدى انكشاف تطبيقات SAP على الشبكة.

كمثال آخر، يمكننا إيجاد كم هائل من الرمازات البرمجية المعدّة لاستغلال الثغرات الأمنية لتطبيقات SAP على موقع www.exploit-db.com وهو متاح للجميع:

EXPLOIT DATABASE

Home Exploits Shellcode Papers Google Hacking Database Submit Search

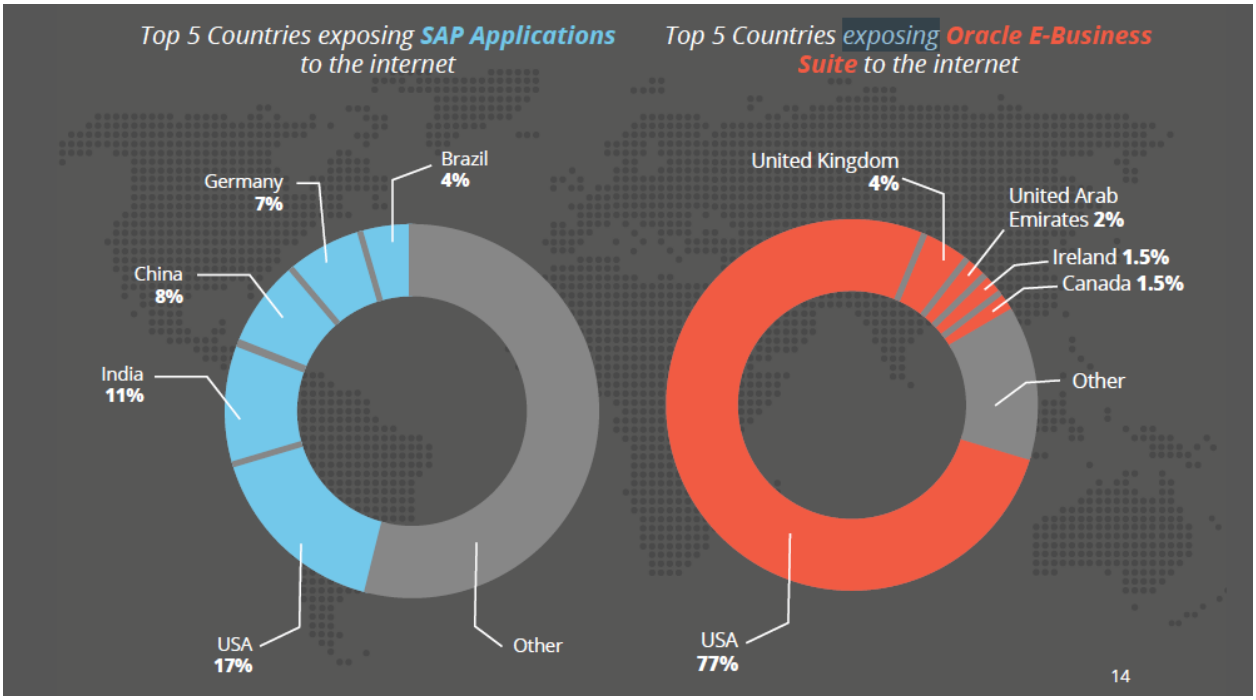
153 total entries

<< prev 1 2 3 4 next >>

Date	D	A	V	Title	Platform	Author
2018-05-25		-		SAP Internet Transaction Server 6200.x - Session Fixation / Cross-Site Scripting	Multiple	J. Carrillo...
2018-05-18		-		SAP B2B / B2C CRM 2.x < 4.x - Local File Inclusion	Linux	Richard...
2018-05-18		-		SAP NetWeaver Web Dynpro 6.4 < 7.5 - Information Disclosure	Linux	Richard...
2018-05-16		-		WhatsApp 2.18.31 - Memory Corruption	iOS	Juan Sacco
2018-03-14		-		SAP NetWeaver AS JAVA CRM - Log injection Remote Command Execution	Windows	erp scan team
2018-01-23		-	-	Hardcore SAP Penetration Testing	Papers	Vahagn...
2018-01-10		-		SAP NetWeaver J2EE Engine 7.40 - SQL Injection	Multiple	Vahagn...
2017-12-27		-		SAP BusinessObjects launch pad - Server-Side Request Forgery	Multiple	Ahmad Mahfouz
2017-11-01		-		WhatsApp 2.17.52 - Memory Corruption	iOS	Juan Sacco
2017-05-19		-		SAP Business One for Android 1.2.3 - XML External Entity Injection	XML	Ravindra Singh...
2017-05-10		-		SAP SAPCAR 721.510 - Heap Buffer Overflow	Linux	Core Security
2016-12-28		-		SapLPD 7.40 - Denial of Service	Windows	Peter Baris
2016-11-22		-		SAP NetWeaver AS JAVA - 'BC-BMT-BPM-DSK' XML External Entity Injection	XML	ERPScan
2016-10-20		-		SAP Adaptive Server Enterprise 16 - Denial of Service	Windows	ERPScan

Figure4: exploitation codes for SAP

وحسب الاحصائيات يمكننا أن نتبين الدول التي تمتلك أكبر نسبة من تعرض تطبيقات ERP العاملة ضمنها لمخاطر الانكشاف على شبكة الانترنت وتقع الولايات المتحدة الأمريكية في مقدمة هذه الدول:



Graph6: Top 5 Countries exposing SAP & Oracle EBS to the internet

- **تسرب معلومات تطبيقات ERP بشكل غير مقصود**

بالإضافة لما تتعرض له تطبيقات ERP من أخطار انكشاف المعلومات نتيجة عملها مباشرة على الشبكة، هناك أطراف أخرى تسهم في هذا الانكشاف مثل الموظفين العاملين على هذه التطبيقات أنفسهم، والأطراف الأخرى المتعاملة مع هذه التطبيقات، حيث تم اكتشاف أطراف متعاقدة تقوم بمشاركة بيانات دخول على بعض تطبيقات

الحوسبة السحابية، إذا سمحت المنظمات والشركات بهكذا نوع من انكشاف المعلومات فلن يكون هنالك أي حاجة للجهات المستهدِفة لهذه التطبيقات لتكبد عناء استغلال الثغرات الأمنية.

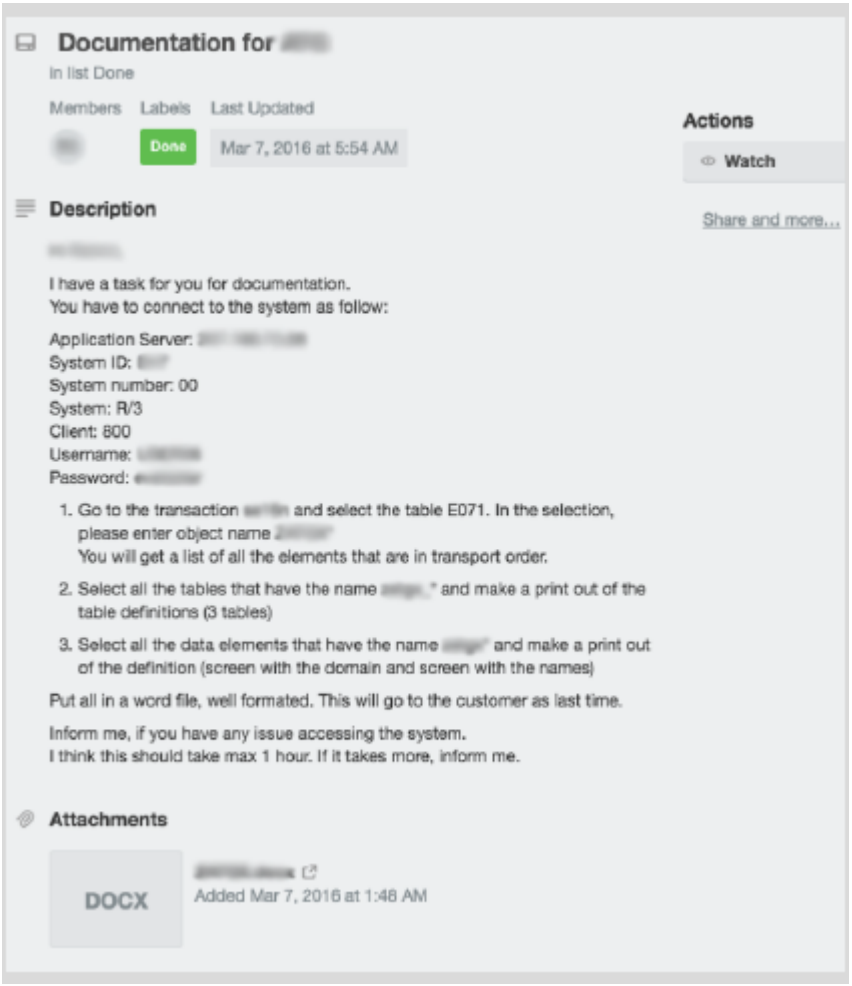
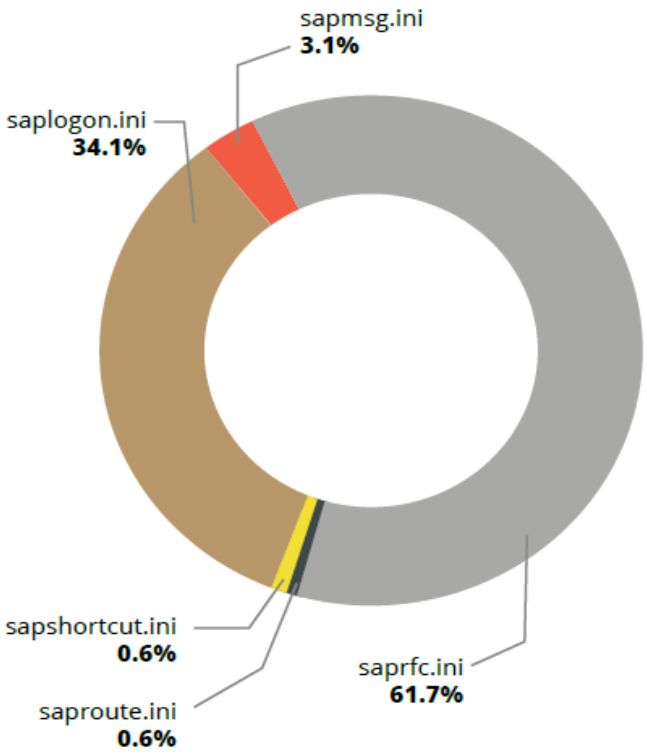


Figure5: Trello Board Revealing SAP Credentials and ULR

وأكثر من ذلك، أثناء البحث ضمن مستودعات الملفات التي تعود لبعض البروتوكولات التي تعتمد عليها هذه التطبيقات مثل SMB،FTP والمواجهة مباشرة للشبكة تم اكتشاف 186 ملف "saplogon.ini" و3 ملفات "sapshortcut.ini" و 336 ملف "saprfc.ini" و17 ملف "saproute.ini" و "sapmsg.ini".

هذه الملفات وما تحتويه من معلومات حساسة، يمكن أن يستغلها أي مهاجم في الولوج إلى منصات عمل هذه التطبيقات، وهذا تحذير لجميع الشركات والمنظمات لضرورة الأخذ بعين الاعتبار الخطر الناجم عن تسرب المعلومات من خلال الموظفين والأطراف الأخرى وضرورة مراعاة ذلك عند وضع خطط التصدي للتهديدات الأمنية.



Graph7: Number of Different Config Files Exposed across Misconfigured rsync, SMB, FTP and s3 Buckets

Figure 6: Sapmsg.ini Configuration File for a Large Oil Company, Exposed On Misconfigured FTP Server

- **تطور التهديدات الأمنية**

من خلال الشـــكل أدناه والذي يمثل التهديدات الأمنية الموثقة التي تعرضـــت لها تطبيقات ERP على مدى السنوات الخمس الماضية، نستطيع أن نتبين أن جهات متعددة تستمر في استهداف هذه التطبيقات من خلال أساليب متعددة ومتنوعة.

إن هجوم منع الخدمة DoS هو هجوم مفضل لدى بعض منظمات الاختراق مثل SudoHackers و Anonymous و Ghost Squad Hackers وقد تم اكتشاف عدة حالات استهداف لتطبيقات SAP من قبلها في قطاعات مثل الإعلام والشركات المالية وشركات التكنولوجيا، وهنالك على الأقل 10 نقاط ضعف لتطبيقات SAP يمكن من خلال استغلالها شن هجوم منع الخدمة وهي موجودة على موقع 0day[.]today.

كذلك في العام 2013 تم اكتشـــاف هجمات الكترونية من نوع هجمات منع الخدمة الموزعة DDoS قامت بها منظمة ANONYMOUS على تطبيقات SAP تعود لمؤسسات مالية.

وكمثال جيد عن عدم تأمين تطبيقات ERP التي تعمل على تماس مباشر مع شبكة الانترنت بالشكل الكافي، نشر موقع الاستجابة للطوارئ المعلوماتية الأمريكي تحذيراً يحمل الرقم TA16-132A والذي يتعلق باستغلال ثغرة أمنية في المكون Servlet invoker تسمح للمهاجم تنفيذ أوامر سطرية خاصة بنظام التشغيل الذي تعمل عليه تطبيقات SAP وتُمكن المهاجم من السيطرة على هذا التطبيق وبياناته بشكل تام تقريباً.

وقد مضى سنتين على نشر هذا التحذير ومازال بالإمكان استغلال هذه الثغرة.

كما تم نشر عدة نجاحات قامت بها مجموعات مختلفة من عدة دول مثل الصين في اختراق هذه التطبيقات.

- **توسع استخدام برمجيات أحصنة طروادة المصرفية لاستهداف بيانات دخول زبائن البنوك**

تم برمجة هذه الأحصنة الطروادية خصيصاً لاستهداف النظم المعلوماتية الخاصة بالبنوك والمؤسسات المالية من خلال البحث عن عناوينها على الشـــبكة وجمع المعلومات عنها وعن بيانات زبائنها وطبعاً تطبيقات ERP التي تعتمد عليها هذه البنوك.

وحصـــل أول اســـتهداف موثق لتطبيقات SAP باســـتخدام الأحصـــنة الطروادية البنكية عام 2013 عن طريق حصان طروادي يحمل خصائص مشابهة للحصان الطروادي Carberp variant.

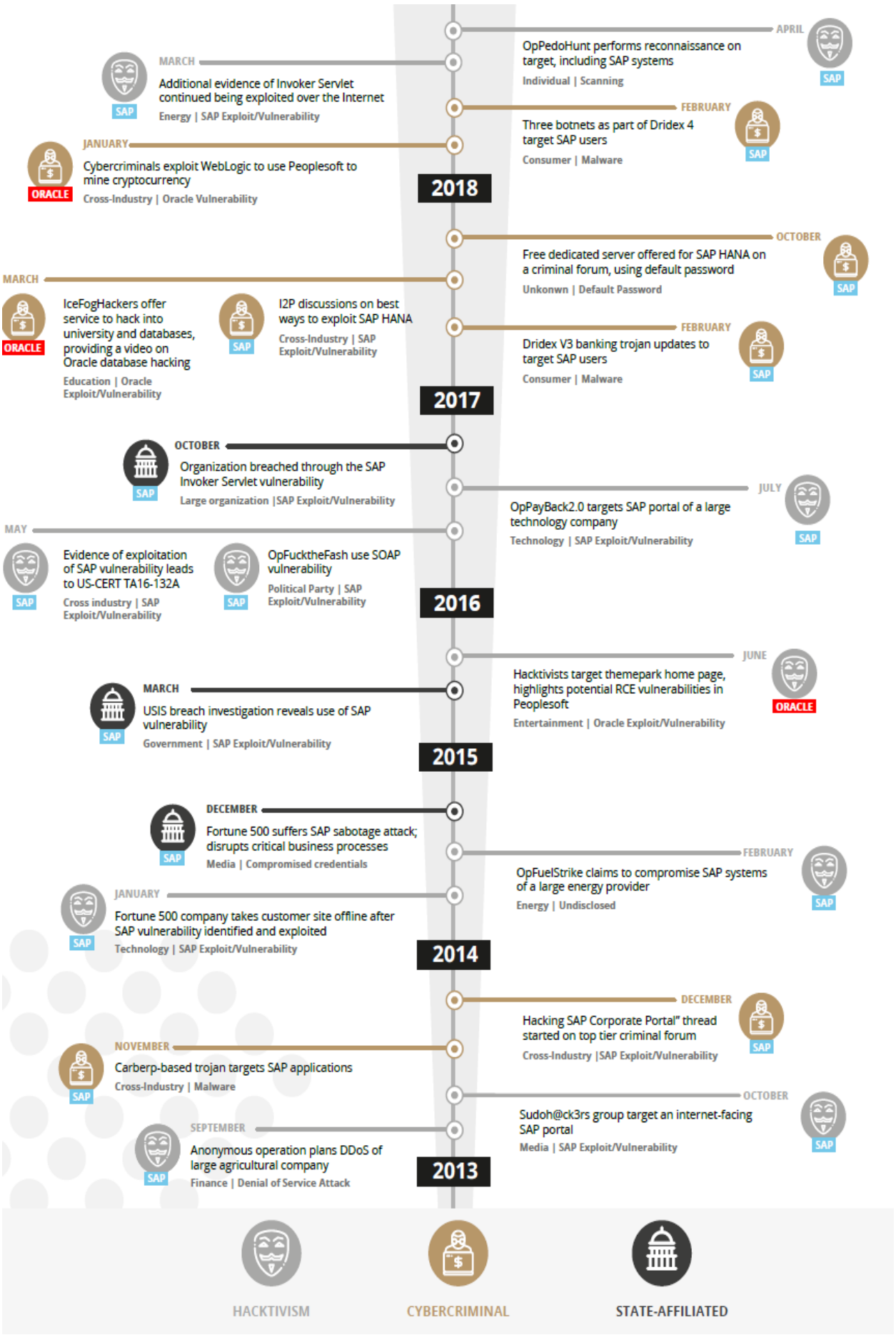
كان الحصـــان الطروادي البنكي Dridex الأشـــهر بينها، والذي أُعيد اســـتخدامه بأكثر من نســـخة مطورة منذ ظهوره لأول مرة عام 2014، وينتشـر عن طريق تحميل ملف نصـي على جهاز الضـحية، وبعد الإصـابة يقوم

هذا البرنامج الخبيث بالبحث عن مســتخدمي تطبيقات SAP، ويجمع بياناتهم المتعلقة بهذا التطبيق مثل بيانات الدخول وبيانات الأعمال الحساسة.

Figure7: A Posted Configuration file of Dridex 4 Trojan Feb 2018

كما حدثت عدة حالات اختراق لتطبيقات ERP كانت أسبابها استخدام كلمات مرور ضعيفة للحسابات المعرفة على هذه التطبيقات أو حسابات لخدمات أخرى مثل خدمة الوصول لسطح المكتب عن بعد RDP والتي مكن استغلالها من زرع برمجيات خبيثة لتسجيل ضربات لوحة المفاتيح وبالتالي سرقة بيانات الدخول لواجهات دخول تطبيقات ERP من خلال هذه الأجهزة.

كشفت إحدى هذه الهجمات الإلكترونية افتقار هذه التطبيقات لوسائل الاستجابة والملاحقة للنشاطات غير الشرعية، وفيما يلي يبين الشكل أهم الهجمات التي تعرضت لها تطبيقات ERP خلال الخمس سنوات الماضية والجهات المستهدِفة:


APRIL
OpPedoHunt performs reconnaissance on target, including SAP systems
Individual | Scanning
FEBRUARY
Three botnets as part of Dridex 4 target SAP users
Consumer | Malware
MARCH
Additional evidence of Invoker Servlet continued being exploited over the Internet
Energy | SAP Exploit/Vulnerability
JANUARY
Cybercriminals exploit WebLogic to use Peoplesoft to mine cryptocurrency
Cross-Industry | Oracle Vulnerability
2018
OCTOBER
Free dedicated server offered for SAP HANA on a criminal forum, using default password
Unkonwn | Default Password
MARCH
IceFogHackers offer service to hack into university and databases, providing a video on Oracle database hacking
Education | Oracle Exploit/Vulnerability
I2P discussions on best ways to exploit SAP HANA
Cross-Industry | SAP Exploit/Vulnerability
FEBRUARY
Dridex V3 banking trojan updates to target SAP users
Consumer | Malware
2017
OCTOBER
Organization breached through the SAP Invoker Servlet vulnerability
Large organization |SAP Exploit/Vulnerability
JULY
OpPayBack2.0 targets SAP portal of a large technology company
Technology | SAP Exploit/Vulnerability
MAY
Evidence of exploitation of SAP vulnerability leads to US-CERT TA16-132A
Cross industry | SAP Exploit/Vulnerability
OpFucktheFash use SOAP vulnerability
Political Party | SAP Exploit/Vulnerability
2016
JUNE
Hacktivists target themepark home page, highlights potential RCE vulnerabilities in Peoplesoft
Entertainment | Oracle Exploit/Vulnerability
MARCH
USIS breach investigation reveals use of SAP vulnerability
Government | SAP Exploit/Vulnerability
2015
DECEMBER
Fortune 500 suffers SAP sabotage attack; disrupts critical business processes
Media | Compromised credentials
FEBRUARY
OpFuelStrike claims to compromise SAP systems of a large energy provider
Energy | Undisclosed
JANUARY
Fortune 500 company takes customer site offline after SAP vulnerability identified and exploited
Technology | SAP Exploit/Vulnerability
2014
DECEMBER
Hacking SAP Corporate Portal" thread started on top tier criminal forum
Cross-Industry |SAP Exploit/Vulnerability
NOVEMBER
Carberp-based trojan targets SAP applications
Cross-Industry | Malware
OCTOBER
Sudoh@ck3rs group target an internet-facing SAP portal
Media | SAP Exploit/Vulnerability
SEPTEMBER
Anonymous operation plans DDoS of large agricultural company
Finance | Denial of Service Attack
2013
HACKTIVISM
CYBERCRIMINAL
STATE-AFFILIATED

حماية تطبيقات ERP

قمنا حتى الآن بتسليط الضوء على المخاطر التي تتعرض لها أشهر تطبيقات ERP في العالم وأكثرها شيوعاً واستخداماً، ومهما كان نوع أو مصدر تطبيق ERP الذي تستخدم، تتشابه الأساليب التي يتبعها المخترقون على اختلاف دوافعهم لمحاولة استهداف هذه التطبيقات، ولذلك تتشابه إجراءات الحماية ويمكن تعميمها على جميع هذه التطبيقات التي تعمل في مختلف البيئات سواء على تماس مباشر مع الشبكة أو ضمن شبكات خاصة VPN وحتى في البيئات السحابية وأهمها:

- **تحديد وتخفيف عدد ثغرات تطبيقات ERP، على مستوى طبقة التطبيقات والإعدادات غير الآمنة والإفراط بمنح الصلاحيات للمستخدمين قدر الإمكان وذلك من خلال:**
  - التقييم المستمر للثغرات الأمنية على مستوى التطبيق، من خلال متابعة الترقيعات الأمنية التي يصدرها مطور التطبيق بشكل دوري، بالإضافة لثغرات نظم التشغيل التي تنصب عليها هذه التطبيقات وثغرات قواعد البيانات.
  - التقييم المستمر والمراجعة للإعدادات البنيوية Configuration لتطبيقات ERP والبحث عن الخلل في هذه الإعدادات مثل الإعدادات الافتراضية لكلمات المرور التي تعتمد كلمات مرور ضعيفة ومعروفة.
  - المراجعة المستمرة للسماحيات الممنوحة للمدراء المشرفين على هذه التطبيقات، القائمين على تطويرها، بما يشمل المسؤولين عن عمليات دمجها مع تطبيقات أخرى.
  - تطبيق عملية تحقق تكرارية لضمان أن أي خلل أمني في هذه التطبيقات يتم اكتشافه وتصحيحه وفي الوقت المناسب.
- **تحديد وإزالة واجهات الربط البينية وواجهات برمجة التطبيقات APIs بين مكونات تطبيقات ERP التي تشكل خطر على التطبيق خصوصاً تلك التي تعمل على تماس مباشر مع شبكة الانترنت وتستخدمها أطراف أخرى Third-Party وذلك من خلال:**
  - الاستمرار في تفقد واجهات الربط البينية وواجهات برمجة التطبيقات بما يتضمن قنوات الربط مع الجهات المطوِرة، والأطراف المعنية بضمان الجودة، والتي يمكن أن يتم إساءة استخدامها وتحويلها إلى نقاط ارتكاز لهجمات مستقبلية.
  - التقييم المستمر للإعدادات البنيوية لواجهات الربط البينية والواجهات البرمجية والتأكد من فعالية استخدام التشفير وصلاحيات الحسابات المعرفة على الخدمات.
  - المراجعة المستمرة لواجهات تطبيقات ERP التي تعمل على تماس مباشر مع شبكة الانترنت والتأكد من عدم السماح بذلك دون وجود سبب تجاري مشروع وكافٍ.

- **المراقبة الدائمة والاستجابة الفورية لنشاطات المستخدمين الحساسة ومؤشرات محددة تدل على أي تهديد وذلك من خلال:**
  - المراقبة المستمرة لأي نشاط مشبوه لأي مستخدم لهذه التطبيقات ولمختلف الصلاحيات التقنية أو الممنوحة لضرورات العمل.
  - المراقبة المستمرة لأي مؤشرات قد تظهر على النظم والتطبيقات تتعلق بمحاولات استغلال للثغرات الأمنية.
  - تنفيذ إجراءات دورية للتأكد من إمكانية الاستجابة لأي حدث طارئ قد يصيب هذه التطبيقات والإمكانات المتاحة للمعالجة.
- **مراقبة تسرب المعلومات والبيانات وبيانات الدخول الخاصة بالمستخدمين وذلك من خلال:**
  - المراقبة المستمرة لمصادر نشر التهديدات الأمنية ومواقع المنظمات الإجرامية بحثاً عن تسرب بيانات الدخول، وأي بيانات أخرى أو ملفات حساسة وأي معلومات عن حالات اختراق أو تهديد لتطبيقات ERP، وخصوصاً التي تتعرض لها تطبيقات تماثل التطبيقات العاملة في مؤسستك أو شركتك.

إن تطبيق وتنفيذ هذه التوصيات يجب أن يشمل جميع أجزاء المنظومة وعدم ترك أي جزء من المنظومة بلا حماية ومراقبة مهما قل شأنه، لأن أي ضعف في مكون معين يمكن أن يؤدي إلى اختراق كامل النظام.

ومما يجب أخذه بعين الاعتبار عند عمل تطبيقات ERP في البيئات السحابية أن مزودي هذه الخدمات لا يأخذون على عاتقهم إجراءات الحماية على مستوى التطبيقات بل يركزون جهدهم واهتمامهم على حماية الشبكة ونظم التشغيل وقواعد البيانات.

يمكن أن تنجز هذه العمليات بتعاون جهات عدة بشكل وثيق بين فرق التدقيق المعلوماتي والمدراء المشرفين على التطبيقات وطبعاً المسؤولين عن أمن المعلومات في المنشأة.