

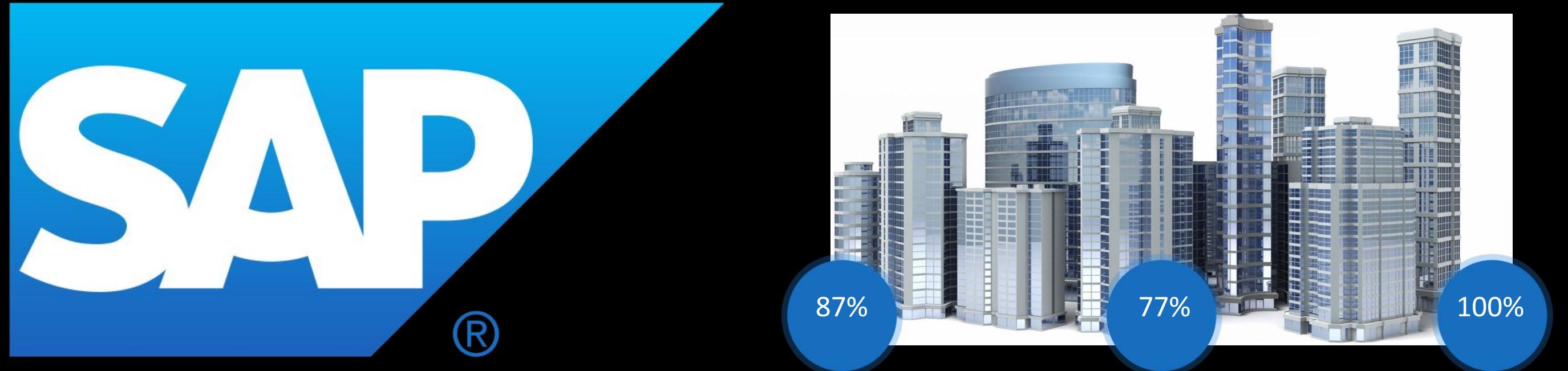


Exposing the dark corners of SAP

4-Years of Threat Intelligence data analyzed

Speaker: Yvan Genuer



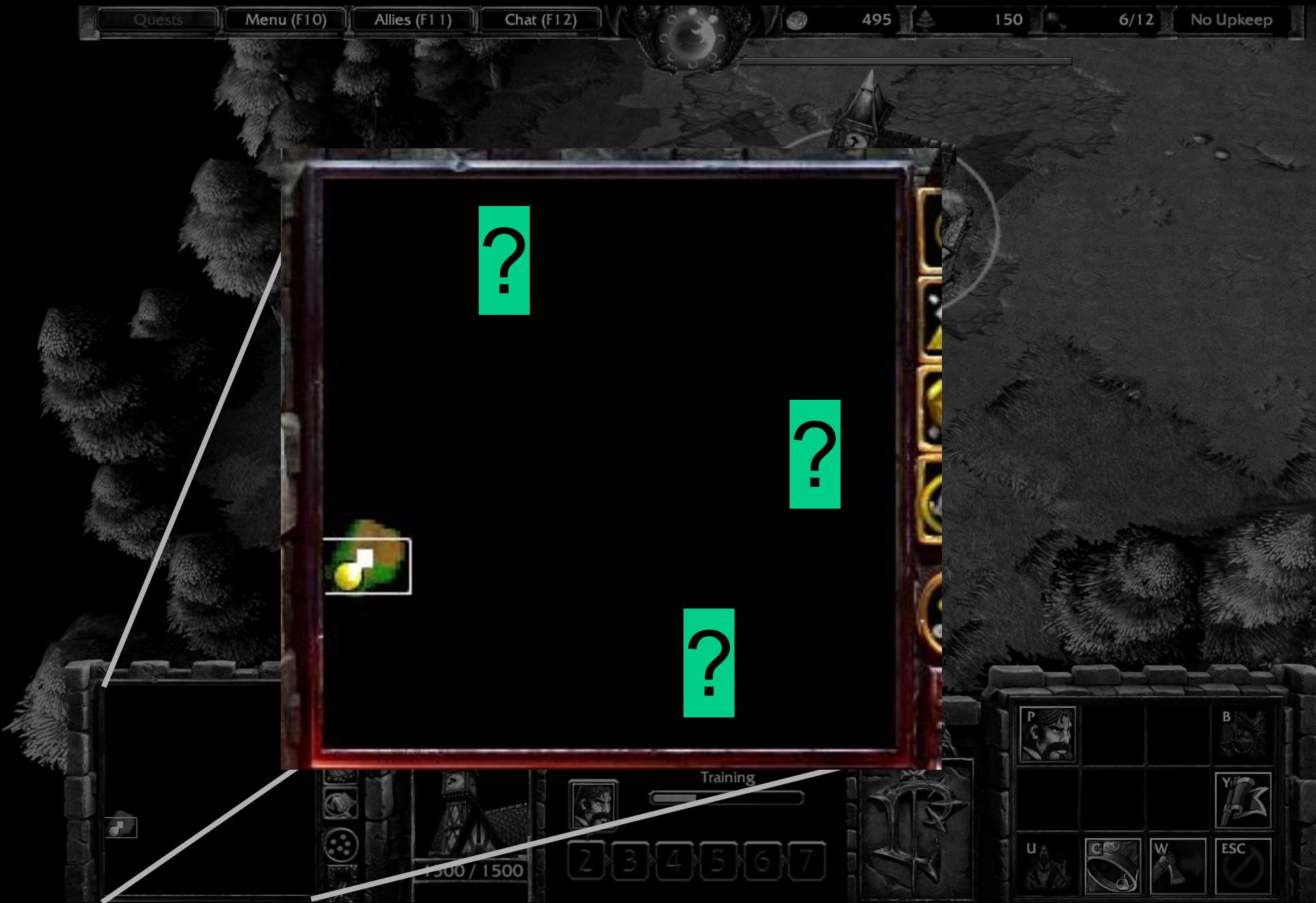


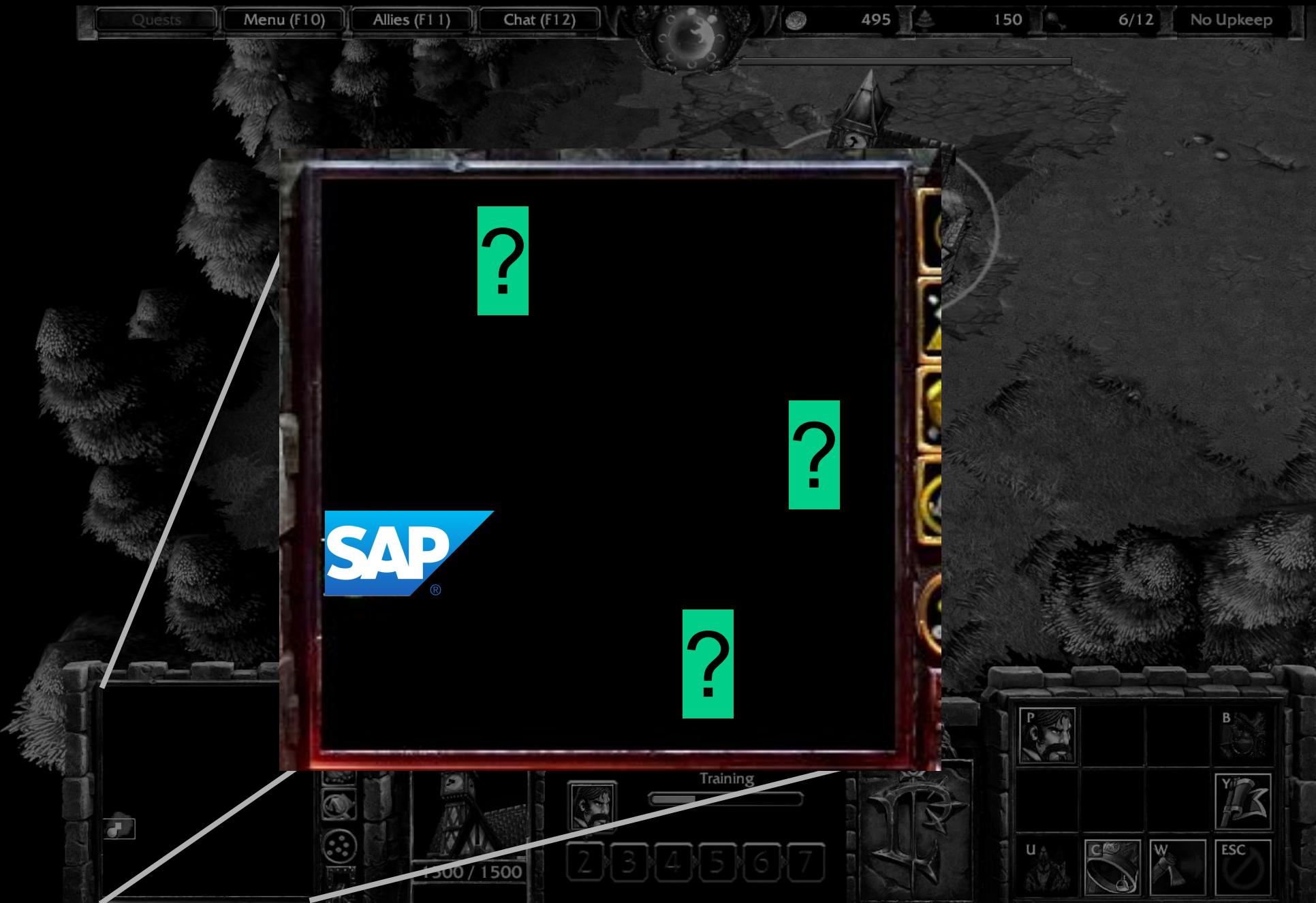
<https://www.sap.com/about/company.html#fast-facts>



<https://warcraft3.blizzard.com>









2020 - 2023 (4 Years)

2020 - 2023 (4 Years)

Varied across the open - deep - dark web

2020 - 2023 (4 Years)

Varied across the open - deep - dark web

Criminal Forums
Chat Sites

Ransomware Incidents
Ransomware Group Sites and Chat

The Rise of Interest on SAP



GuardianeLinks

Удачного кода!



ФОРУМ

РЕСУРСЫ

ЧТО НОВОГО

ПОЛЬЗОВАТЕЛИ

ЧАТ

101010101001
011011001011101101110111010011011101000101010

На GitHub уже появился РоC-экспloit для опасной уязвимости RECON (CVE-2020-6287), которая представляет угрозу для большинства SAP-приложений.

Guardiane
уда

Posted on January 05, 2024 at 20:51:21 UTC

like making the exploit poc

Posted on January 05, 2024 at 20:51:42 UTC

or like wdyd work on it?

Posted on January 05, 2024 at 20:56:23 UTC

Yeah Im just analyzing the PoC. Seeing what sort of HTTP request needs to be made to exploit the vuln.

Looks like its just a request that resembles

```
'echo "print(\"GET /sap/public/bc/ur/Login/assets/corbu/sap_logo.png HTTP/1.1\\r\\nHost: 127.0.0.1:8443\\r\\nContent-Type: application/x-www-form-urlencoded\\r\\nAccept: */*\\r\\nUser-Agent: Chrome\\r\\n\\")'; print("A"*82642, end=""); print(" r\\n\\r\\nGET /sap/public/ping HTTP/1.1\\r\\nHost: 127.0.0.1:8443\\r\\n\\r\\n")' | gzip | base64'
```

сть которую продают чёрные хакеры, а удаляют белые [Открытые Редиректы]

24

Guard

Jan 5, 2024

Открытые Закрытые Редиректы

Эта статья о уязвимости, которую продают чёрные хакеры, а удаляют белые. Почему? Потому что она нам бесполезна. Как видите, она не принимается платформами безопасности, так как требует взаимодействия пользователя, или, как мы говорим, "фишинга". Я нашел открытый редирект для компании X, и компания X достаточно большая для наличия уязвимостей, очевидно, мне пришлось открыть ее сайт и исследовать, и пока этого достаточно. В любом случае, этот парень подал мне идею поиска открытых редиректов в организациях, которые не имеют собственных инструментов для обнаружения уязвимостей. Итак, давайте рассмотрим, как это сделать.

Открытый Редирект

Открытый Редирект - это уязвимость, возникающая, когда веб-приложение манипулируется для перенаправления пользователя на другой сайт. Уязвимости Открытых Редиректов эксплуатируют доверие пользователя к данному веб-сайту для перенаправления пользователя на другой сайт. Для демонстрации уязвимости Открытых Редиректов можно использовать сервис XSS-исследования XSS.is. Если в URL вставить ссылку, например, "xss.is/?redirectUrl=xss[.]bz", и нажать на нее, то пользователь будет перенаправлен на сайт XSS.is. Это является результатом неправильной проверки / отсутствия фильтрации при обработке URL, предоставленных пользователем. Таким образом, хакеры могут заменить его на свой злонамеренный URL.

made to exploit the vuln.

Ситуация в нашем мире

Уязвимости Открытых Редиректов часто игнорируются, хотя они представляют значительную угрозу из-за их косвенной природы. Программы раскрытия уязвимостей обращают внимание на прямые методы атаки (SQL/XSS и т.д.), а не на уязвимости, такие как открытые редиректы, которые подвергаются взлому простыми фишинговыми атаками.

\r\nHost: 127.0.0.1:8443\r\n

\n")

\r\n")" | gzip | base64'

Как работает открытый редирект?

ПОДДЕРЖКА
ПОДДЕРЖКА
ЧАТ

ПОДДЕРЖКА
ПОДДЕРЖКА
ПОДДЕРЖКА

ПОДДЕРЖКА
ПОДДЕРЖКА
ПОДДЕРЖКА

ПОДДЕРЖКА
ПОДДЕРЖКА
ПОДДЕРЖКА

сть которую продают чёрные хакеры, а удаляют белые [Открытые Редиректы]

Guard

Jan 5, 2024

Открытые Закрытые Редиректы

Эта статья о уязвимости, которую продают чёрные хакеры, а удаляют белые. Почему? Потому что она нам бесполезна. Как ви

Anonymous (None)

Posted on May 12, 2021 at 19:17:44 UTC

Server: 192.168.228.25 Instance: 00 ID: CTP SAP Router: /H/saprouter [REDACTED] n2 User: SC [REDACTED] S Pass: B [REDACTED] 5 Do it

является результатом неправильной проверки / отсутствия фильтрации при обработке URL, предоставленных пользователем
переадресации, хакеры могут заменить его на свой злонамеренный URL.

Ситуация в нашем мире

Уязвимости Открытых Редиректов часто игнорируются, хотя они представляют значительную угрозу из-за их косвенной природы. Программы раскрытия уязвимостей обращают внимание на прямые методы атаки (SQL/XSS и т.д.), а не на уязвимости, такие как подвергающиеся взлому простыми фишинговыми атаками.

Как работает открытый редирект?

\r\nHost: 127.0.0.1:8443\r\n\r\n")" | gzip | base64'

сть которую продают чёрные хакеры, а удаляют белые [Открытые Редиректы]

Guard

Jan 5, 2024

Открытые Закрытые Редиректы

Эта статья о уязвимости, которую продают чёрные хакеры, а удаляют белые. Почему? Потому что она нам бесполезна. Как ви

Anonymous (None)

Posted on May 12, 2021 at 19:17:44 UTC

Server: 192.168.228.25 Instance: 00 ID: CTP SAP Router: /H/saprouter [REDACTED] n2 User: SC [REDACTED] S Pass: B [REDACTED] 5 Do it

5 Do it

является результатом неправильной проверки / отсутствия фильтрации при обработке URL, предоставленных пользователем
переадресации, хакеры могут заменить его на свой злонамеренный URL.

Ситуация в нашем мире

Уязвимости Открытых Редиректов часто игнорируются, хотя они представляют значительную угрозу из-за их косвенной природы.
Программы раскрытия уязвимостей обращают внимание на прямые методы атаки (SQL/XSS и т.д.), а не на уязвимости, такие как подвергшиеся взлому простыми фишинговыми атаками.

Как работает открытый редирект?

\r\n")" | gzip | base64'

Trigona Ransomware Blog



Created By: [Trigona](#)

URL: <http://trigonax2zb3fw34rbaap4cqep76zofxs53zakrdgcxzq6xzt24l5lqd.onion/leak/3649f5c9>

First Observed On October 01, 2023

Last Observed On October 05, 2023

[Trigona](#) on Oct 01, 2023 12:47:34

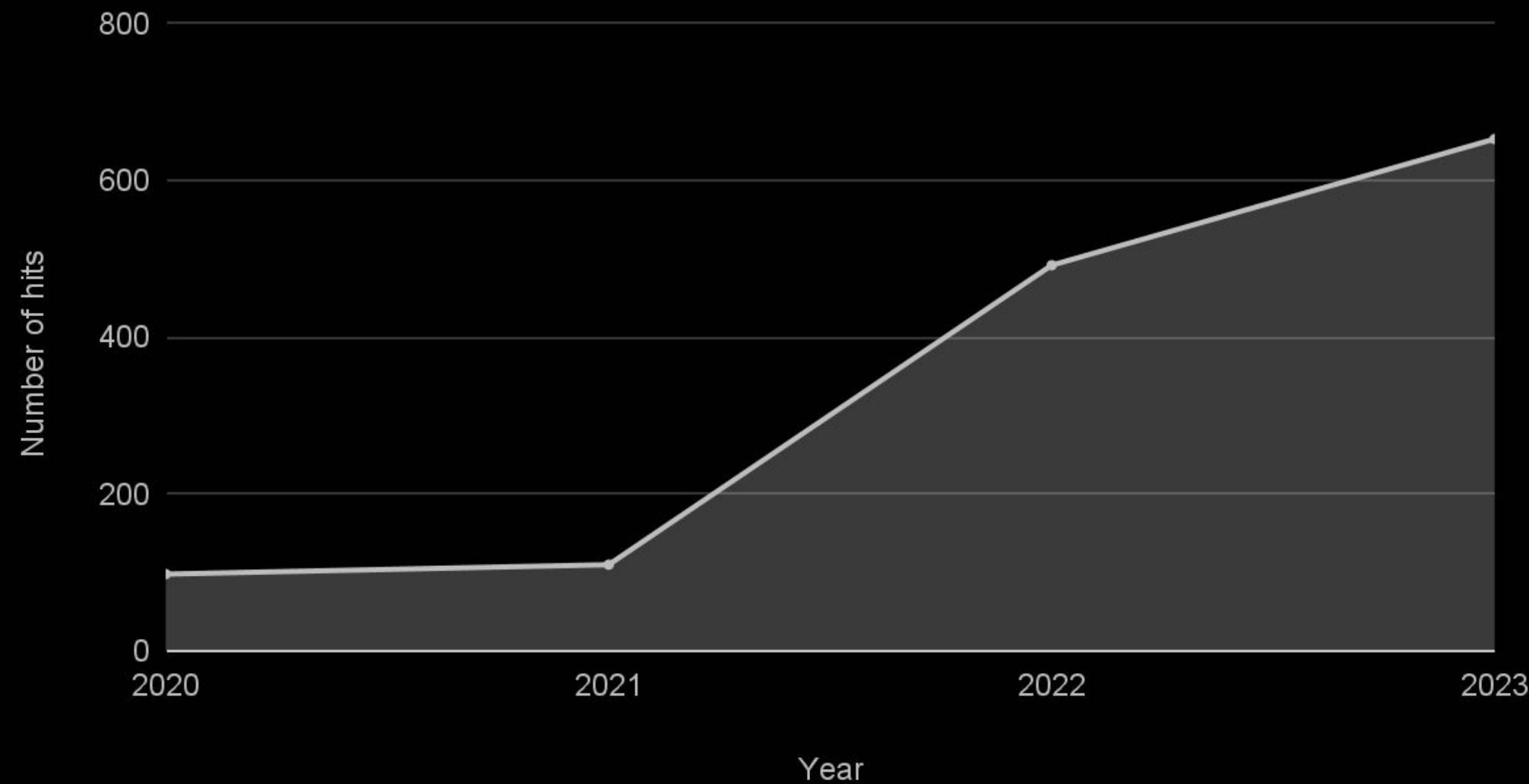


1930

I is a leading global post-sales service support partner for original equipment manufacturers (OEMs) across various industries, founded in 1982. Company offers services supporting OEM customers through depot repairs, field services, supply-chain logistics, and other professional services.

By acquiring this company's confidential data (including in full SAP data), you will get access to valuable information that can help you grow your business. You will learn about the company's strategies, strengths, weaknesses, opportunities and threats. You will also discover the needs, pain points, motivations and behaviors of its customers. You will be able to use this information to create better products and services, target the right prospects, craft compelling sales pitches and close more deals.

SAP exploits or vulnerabilities



Good and easy to understand indicator

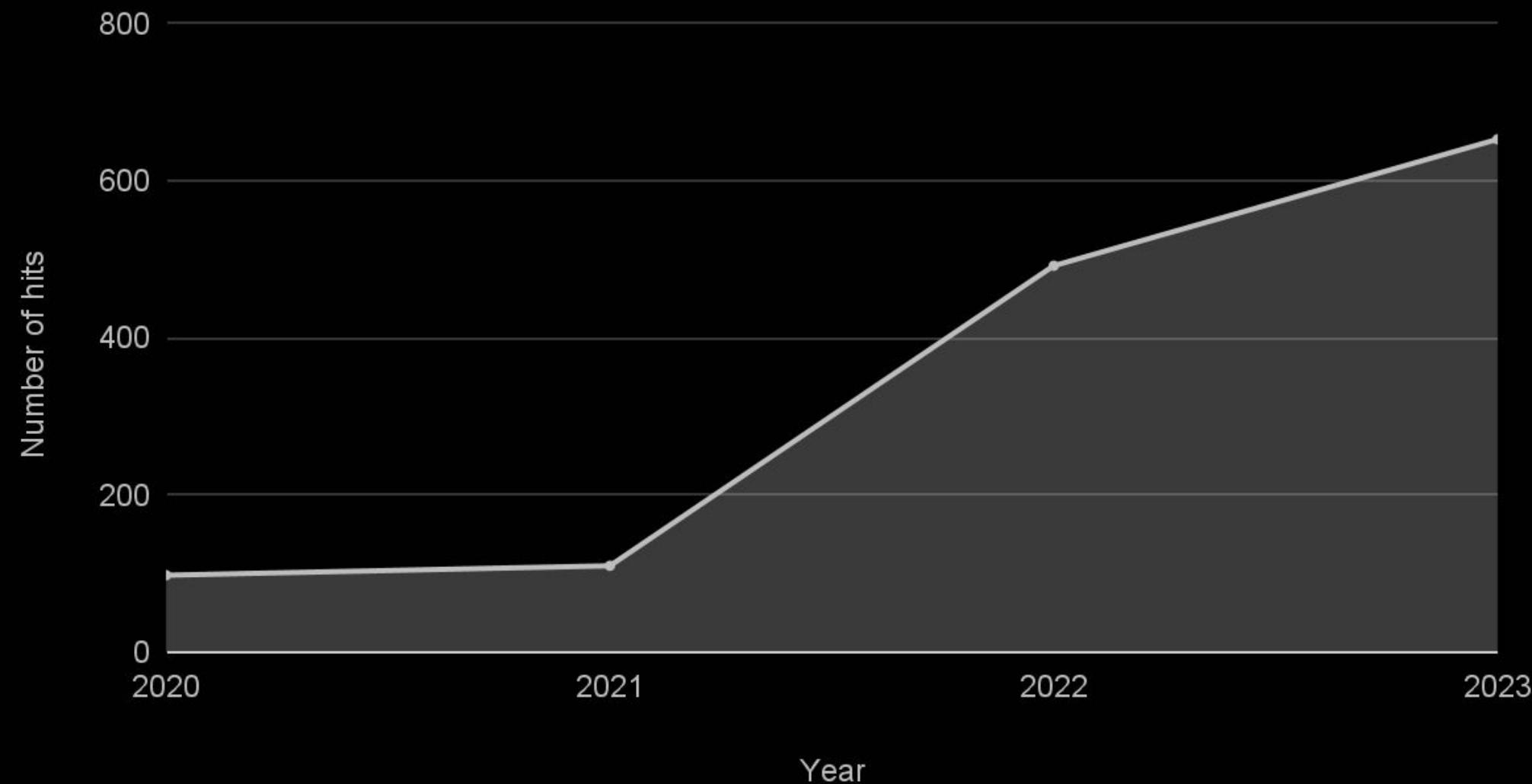


Good and easy to understand indicator
What threat actors speak about is not for fun...

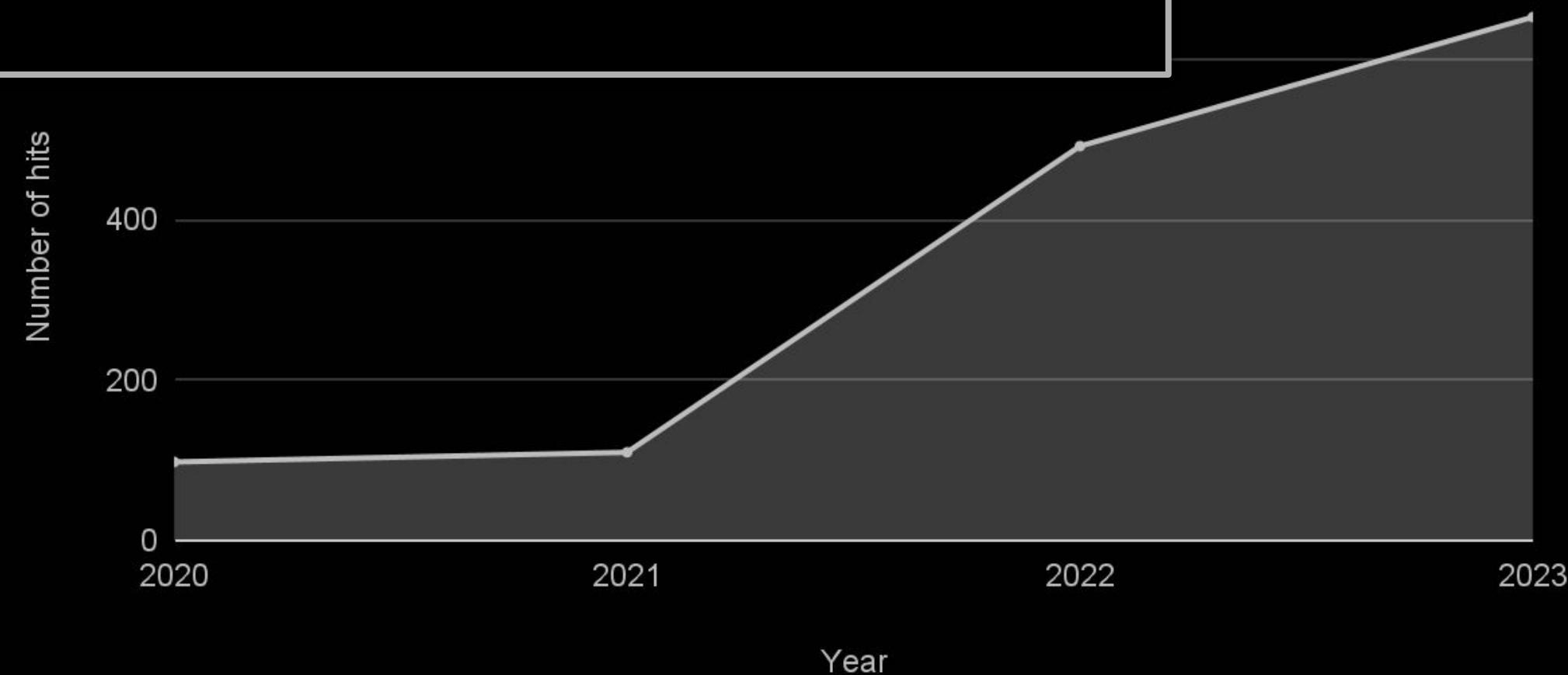


Good and easy to understand indicator
What threat actors speak about is not for fun...
... it is for profit

SAP exploits or vulnerabilities



What happened in 2021 ?



RECON

Posted on July 15, 2020 at 00:00:00 UTC

Hi,

just been published:
CVE-2020-6287

<https://securityaffairs.co/wordpress/105861/hacki>

Anyone up to work with this?

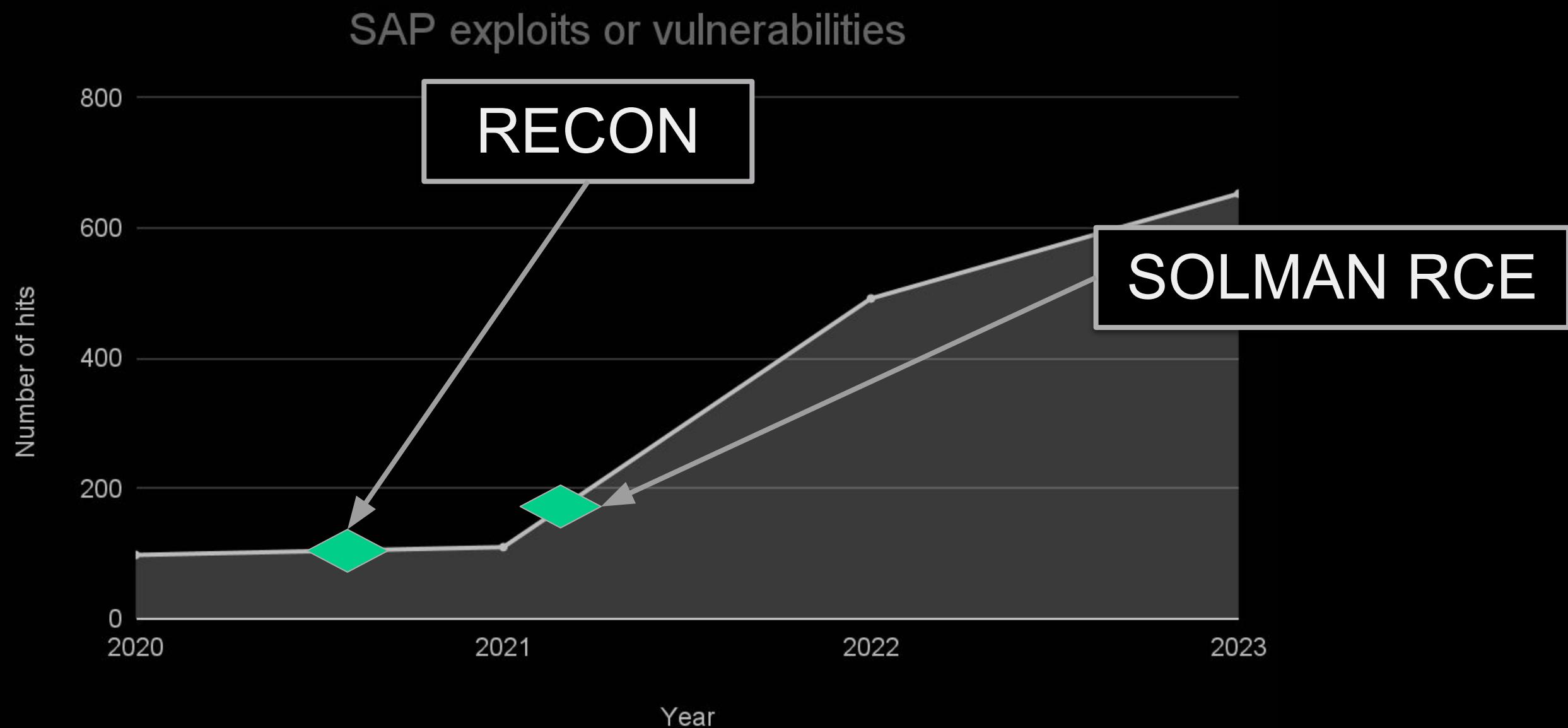
```
print(f"Something wrong with setServer")
exit(1)
if args.list:
    getAllAgentsPretty()
```

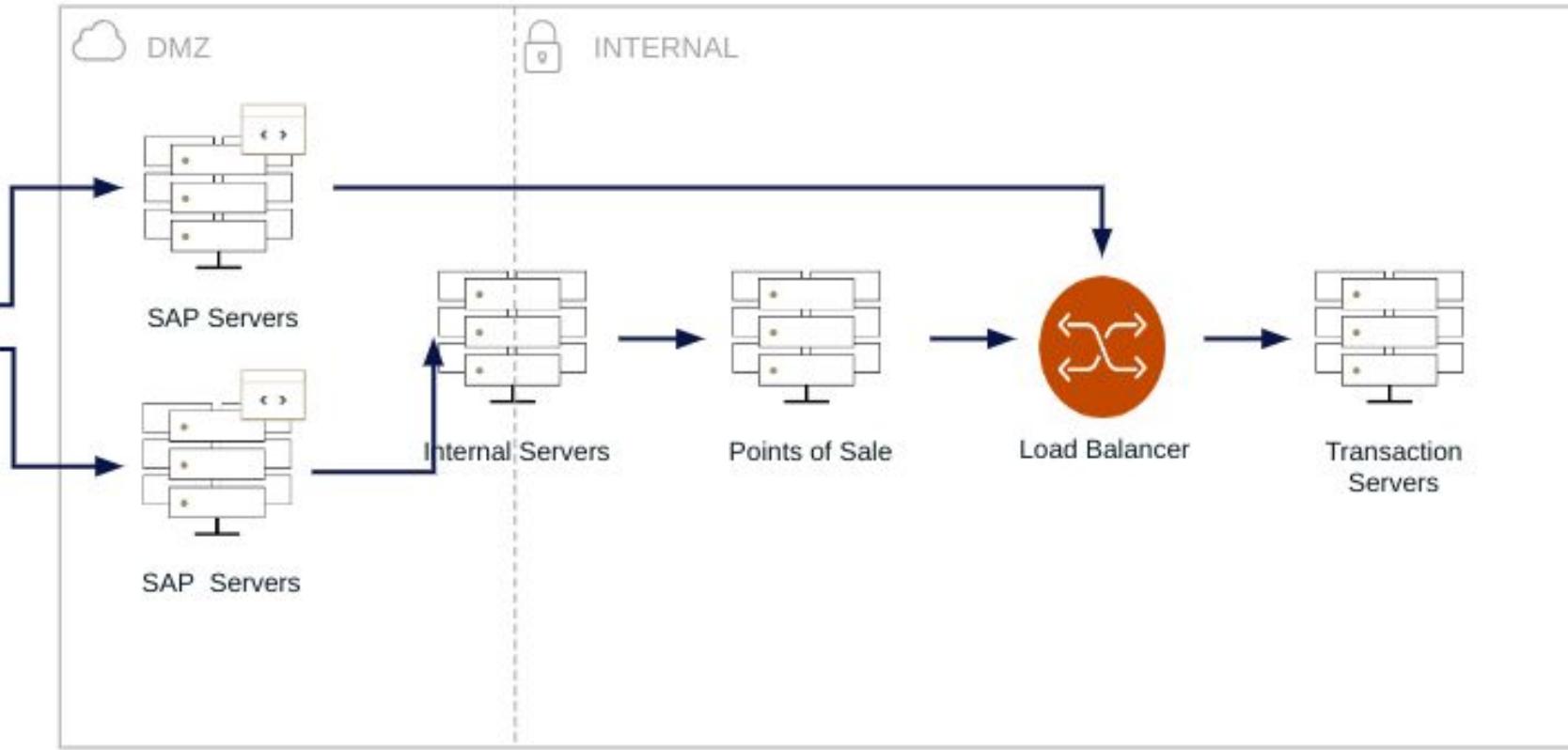
Источник: https://github.com/chipik/SAP_EEM_CVE-2020-6207

SOLMAN RCE

Posted on February 03, 2021 at 12:02:00 UTC

@reaver : did you try it? because i can't get success with this.

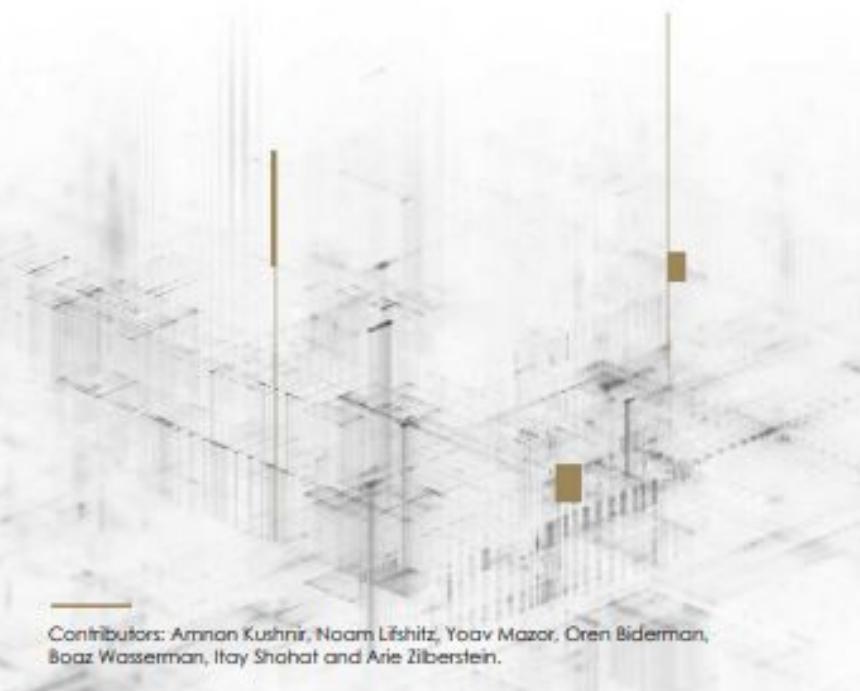




S Y G N I A

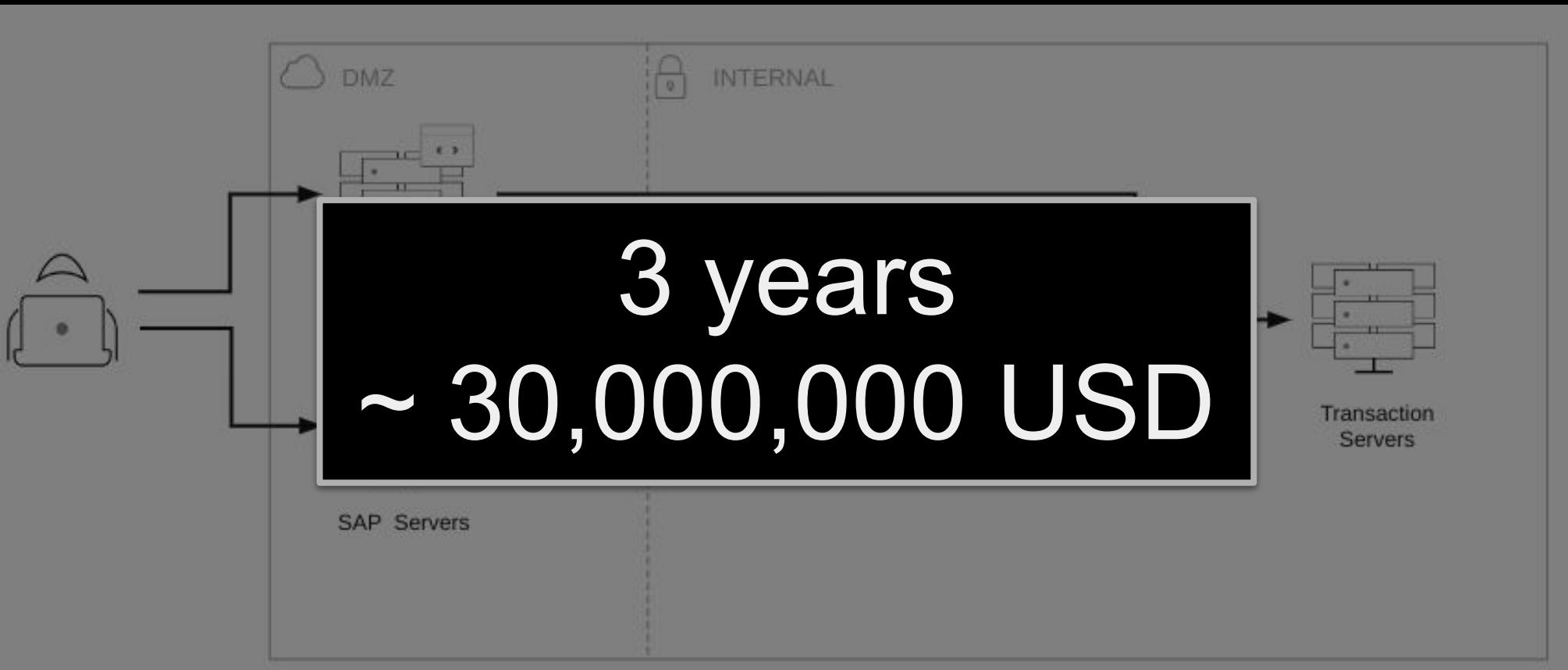
TG2003: Elephant Beetle
UNCOVERING AN ORGANIZED
FINANCIAL-THEFT OPERATION

January 2022



<https://www.sygnia.co/threat-reports-and-advisories/elephant-beetle-an-organized-financial-theft-operation/>
<https://onapsis.com/blog/elephant-beetle-older-unpatched-sap-vulnerabilities-are-still-threat/>

Contributors: Amnon Kushnir, Noam Lifshitz, Yoav Mazor, Oren Biderman, Boaz Wasserman, Itay Shahat and Arie Zilberman.



S Y G N / A

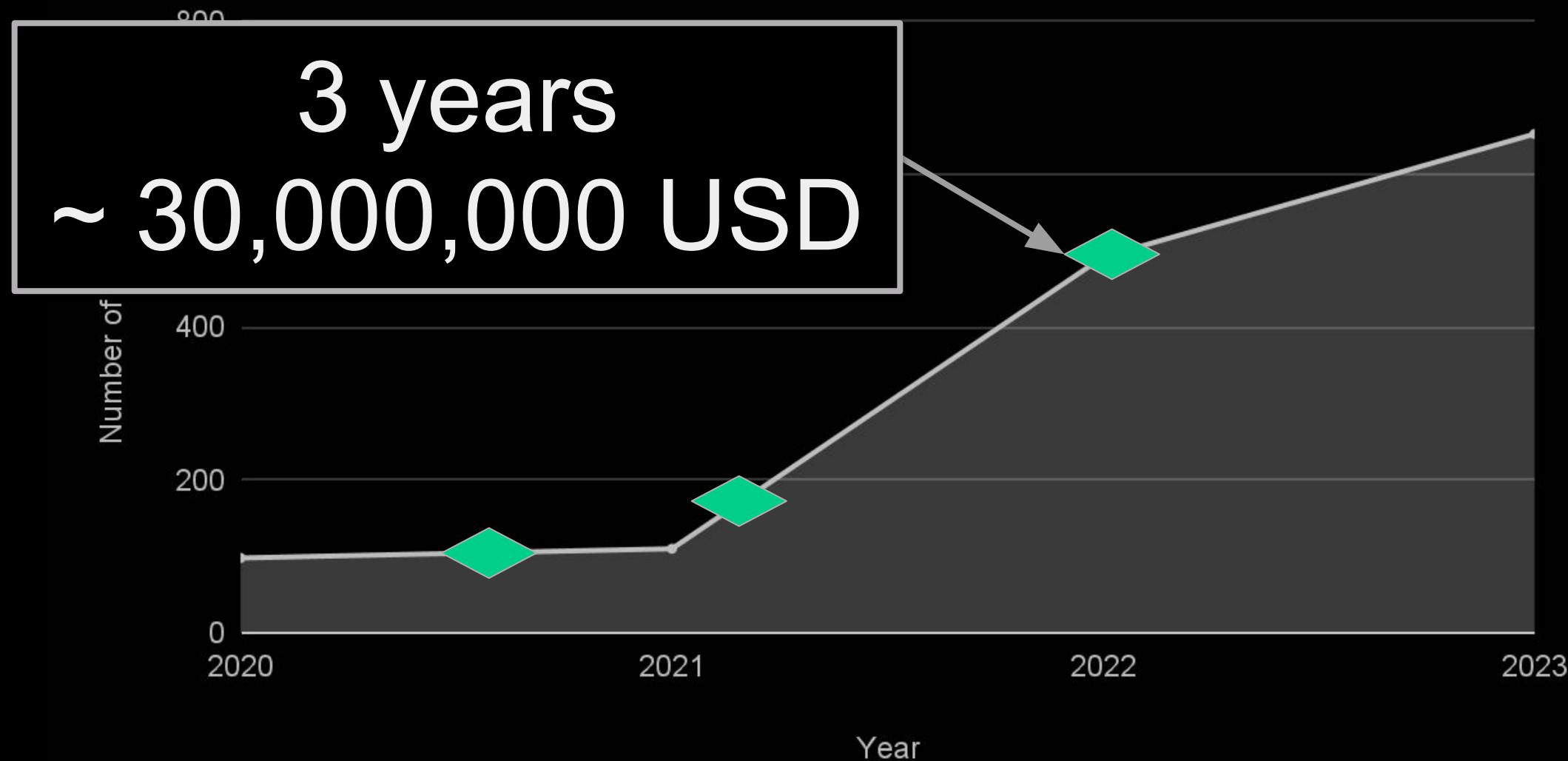
TG2003: *Elephant Beetle*
UNCOVERING AN ORGANIZED
FINANCIAL-THEFT OPERATION

January 2022

<https://www.sygnia.co/threat-reports-and-advisories/elephant-beetle-an-organized-financial-theft-operation/>
<https://onapsis.com/blog/elephant-beetle-older-unpatched-sap-vulnerabilities-are-still-threat/>

Contributors: Amnon Kushnir, Noam Lifshitz, Yoav Mazor, Oren Biderman,
Boaz Wasserman, Itay Shahar and Arie Zilberman.

SAP exploits or vulnerabilities



Public exploits

Public exploits

FIN13 set a precedent

Public exploits

FIN13 set a precedent

Threat actors realized that SAP target could have great ROI

Pu

FI

The

Which companies / agencies
already run SAP ?

have great ROI

Who are interested by SAP



Name	Particularity
FIN13	Financial companies target
FIN7	Financial companies target

Name	Particularity
FIN13	Financial companies target
FIN7	Financial companies target
Cobalt Spider	Point Of Sales target

Name	Particularity
FIN13	Financial companies target

PoC for CVE-2020-6207 [Fixed] (Missing Authentication Check in SAP Solution Manager)

Author Message

PoC for CVE-2020-6207 [Fixed] (Missing Authentication Check in SAP Solution Manager) 01-22-2021, 08:45 PM #1

Yesterday i was reading a article in zdnet about a fresh exploit and PoC that allow remote code execution with the possibility to completely automate the exploitation. The PoC is easy to use and it only require some command lines to check if a host is vulnerable or not. If vulnerable it can execute exes.

View the article:
<https://www.zdnet.com/article/automated---the-wild/>

Note: The file is almost equal to the original but there is some fixes. Credits removed, User-Agent in the payload had a tracking code which was removed too.

Download:
https://anonfiles.com/X5QfD9Bap8/SAP_CVE-2020-6207_zip

(This post was last modified: 01-22-2021, 08:51 PM by hacxx.)

hacxx •
Posting Freak

Eight Years of Service

Posts: 6,766
Threads: 3,219
Reputation: 71
Currency: 12,443 NSP

Name	Particularity
FIN13	Financial companies target
FIN7	Financial companies target
Cobalt Spider	Point Of Sales target
APT10	Mainly known for espionage

Name	Particularity
FIN13	Financial companies target
FIN7	Financial companies target

Добрового времени суток, дамы и господа!

Буду краток. Удалось получить доступ к 4 сетям разных компаний через CVE-2020-6287 и CVE-2020-6207, погуглив удалось узнать, что одна из них вроде сеть ресторанов, а другая телефонная компания. Две других установить не удалось. Соответственно имею доступ через админку Netweaver, а так же могу добавлять свои скрипты через CVE-2020-6207. Так вот вопрос, что с этим делать? Продать? А за сколько? Шифровать? А чем? Возможно мои вопросы покажутся глупыми, но прошу строго не судить т.к с сетками работаю впервые.

Report

Like + Quote Reply

“Good day, ladies and gentlemen!
I'll be brief. We managed to gain access to 4 networks of different
companies through CVE-2020-6287 [RECON] and
CVE-2020-6207 [SAP Solution Manager missing authentication],
after googling I found out that one of them was like a restaurant
chain, and the other was a telephone company [...] What to do
about it? Sell? How much? Encrypt? [...]”

“Good day, ladies and gentlemen!
I'll be brief. We managed to gain access to 4 networks of different
companies through CVE-2020-6287 [RECON] and
CVE-2020-6207 [SAP Solution Manager missing authentication],
after googling I found out that one of them was like a restaurant
chain, and the other was a telephone company [...] What to do
about it? Sell? How much? Encrypt? [...]”

“Good day, ladies and gentlemen!
I'll be brief. We managed to gain access to 4 networks of different
companies through CVE-2020-6287 [RECON] and
CVE-2020-6207 [SAP Solution Manager missing authentication],
after googling I found out that one of them was like a restaurant
chain, and the other was a telephone company[...] **What to do**
about it? Sell? How much? Encrypt? [...]”

Name	Particularity
FIN13	Financial companies target
FIN7	Financial companies target
Cobalt Spider	Point Of Sales target
APT10	Mainly know for espionage
Script Kiddies	Various threats

Name

FIN13

Particularity

Financial companies target

What can we learn from this result ?

APT10

Mainly known for espionage

Script Kiddies

Various threats

Name	Particularity
FIN13	Financial companies target
Why are they interested ?	
APT10	Mainly known for espionage
Script Kiddies	Various threats

Name	Particularity
FIN13	Financial companies target
FIN7	Financial companies target
Cobalt Spider	Point Of Sales target
Because of what SAP processes... \$\$	

Name	Particularity
FIN13	Because of what SAP holds
FIN7	
Cobalt Spider	
APT10	Mainly known for espionage
Script Kiddies	Various threats

Name	Particularity
FIN13	Financial companies target
APT 10	Mainly known for espionage
Script Kiddies	Various threats

Highlight wide range of SAP components

Cobalt Spider

Point Of Sales target

APT10

Mainly know for espionage

Script Kiddies

Various threats

Major units [edit]

- SAP S/4HANA (Enterprise Resource Planning on-premise and cloud)
- SAP Business ByDesign (SME Cloud Enterprise Resource Planning)
- SAP Business One (B1 on HANA) (Small enterprise Enterprise Resource Planning)
- SAP CRM (Customer Relationship Management) (legacy product)
- SAP ERP (Enterprise Resource Planning) (legacy product, see S/4HANA)
- SAP PLM (Product Lifecycle Management) (legacy product)
- SAP SCM (Supply Chain Management) (legacy product)
- SAP SRM (Supplier Relationship Management) (legacy product)

Business software [edit]

- SAP Advanced Data Migration (ADP)
- SAP Advanced Planner and Optimizer
- SAP Analytics Cloud (SAC)
- SAP Advanced Business Application Programming (ABAP)
- SAP Apparel and Footwear Solution (AFS)
- SAP Business Information Warehouse (BW)
- SAP Business ByDesign (ByD)
- SAP Business Explorer (Bex)
- SAP BusinessObjects Lumira
- SAP BusinessObjects Web Intelligence (Webi)
- SAP Business One
- SAP Business Partner Screening
- SAP Business Intelligence (BI)
- SAP Business Workflow
- SAP Catalog Content Management ()
- SAP Cloud for Customer (C4C)

- SAP Cost Center Accounting (CCA)
- SAP Convergent Charging (CC)
- SAP Converged Cloud
- SAP Data Warehouse Cloud (DWC)
- SAP Design Studio
- SAP PRD2(P2)
- SAP Enterprise Buyer Professional (EBP)
- SAP Enterprise Learning
- SAP Portal (EP)
- SAP Exchange Infrastructure (XI) (From release 7.0 onwards, SAP XI has been replaced by SAP Integration Suite)
- SAP Extended Warehouse Management (EWM)
- SAP FICO
- SAP BPC (Business Planning and Consolidation, formerly OutlookSoft)
- SAP GRC (Governance, Risk and Compliance)
- SAP EHSM (Environment Health & Safety Management)
- Enterprise Central Component (ECC)
- SAP ERP
- SAP HANA (formerly known as High-performance Analytics Appliance)
- SAP Human Resource Management Systems (HRMS)
- SAP SuccessFactors
- SAP Information Design Tool (IDT)
- SAP Integrated Business Planning (IBP)
- SAP Internet Transaction Server (ITS)
- SAP Incentive and Commission Management (ICM)
- SAP IT Operations Analytics (ITOA)^[1]
- SAP Jam
- SAP Knowledge Warehouse (KW)
- SAP Manufacturing
- SAP Marketing Cloud
- SAP Materials Management (MM)

- SAP Master Data Management (MDM)
- SAP Plant Maintenance (PM)
- SAP Production Planning (PP)
- SAP Product Lifecycle Costing (PLC)
- SAP Profitability and Cost Management (PCM)
- SAP Project System (PS)
- SAP Rapid Deployment Solutions (RDS)
- SAP Service and Asset Management
- SAP Supply Network Collaboration (SNC)
- SAP Solutions for mobile business
- SAP Sales and Distribution (SD)
- SAP Solution Composer
- SAP Strategic Enterprise Management (SEM)
- SAP Test Data Migration Server (TDMS)
- SAP Training and Event Management (TEM)
- SAP Transportation Management (TM)
- SAP NetWeaver Application Server (Web AS)
- SAP xApps
- SAP Sales Cloud (previously: CallidusCloud)
- SAP Supply Chain Performance Management (SCPM)
- SAP Supply Chain Management (SCM)
- SAP Sustainability Performance Management (SUPM)
- SAP S/4HANA
- SAP Master Data Governance (MDG)
- SAP S/4HANA Cloud

Industry software [edit]

- SAP for Retail
- SAP for Utilities (ISU)
- SAP for Public Sector (IS PSCD)
- SAP for Oil & Gas (IS Oil & Gas)

- SAP for Media (ISM)
- SAP for Telecommunications (IST)
- SAP for Healthcare (ISH)
- SAP Banking (SAP Banking)
- SAP for Insurance (SAP for Insurance)
- SAP Financial Services Network (FSN)
- SAP Shipping Services Network (SSN)
- Engineering Construction & Operations (EC&O)
- SAP IS Airlines & Defense
- SAP for Discrete Industries and Mill Products (IS DIMP)

Software for small and midsize enterprises [edit]

- SAP Business One (Small enterprise ERP 6.2, 6.5, 2004, 2005, 2007, 8.8x, 9.X)
- SAP Business ByDesign (SME Cloud ERP)

Platforms and frameworks [edit]

- SAP Cloud Platform (Its brand name is removed^[2] in January 2021 in favor of SAP Platform)
- SAP Enterprise Services Architecture
- SAP NetWeaver Platform
 - SAP NetWeaver Portal (formerly SAP Enterprise Portal)
 - SAP NetWeaver BI (formerly SAP NetWeaver BW- "BW" is still used to describe components)
 - SAP NetWeaver Visual Composer
 - SAP Auto-ID Infrastructure
 - SAP Composite Application Framework



Groups are very heterogeneous

Groups are very heterogeneous

SAP target is not reserved individually to
Hacktivist
Nation State
Criminal

Groups are very heterogeneous

SAP target is not reserved individually to
Hacktivist
Nation State
Criminal

SAP is so huge, that it has interest for all groups

Price inflation



Posted on August 09, 2020 at 03:26:00 UTC

Предлагаю exploit для горизонтального перемещения в системах SAP (никогда ранее не реализовался в такой функциональности)

- необходим предварительный доступ к серверу, используется для перемещения на другие ресурсы экосистемы SAP.
- базовая теория описана тут <https://www.cert-devoteam.fr/en/the-security-of-sap-secure-storage/>

SAP Secure Storage to find credentials, elevate privileges and eventually compromise another SAP System behind the first target.

- +Namespace key(s).
- +Developer Key.
- +Object Key.
- +Hardware key. ABAP hardware key.
- +Generates MAC Address for the Message Server ABAP/JAVA

25,000 USD

Target:	SAP NetWeaver	We are looking for pre-authentication RCEs or authentication bypass exploits affecting recent versions of SAP NetWeaver.
Bounty:	Up to \$50,000	The exploit should allow either remote code execution or authentication bypass, work with default installations and should not require any authentication or user interaction.
Start Date:	26 August 2020	
End Date:	30 September 2020	

50,000 USD

Target: SAP NetWeaver

We are looking for pre-authentication RCEs or authentication bypass exploits affecting recent versions of SAP NetWeaver.

Bounty: Up to \$50,000

The exploit should allow either remote code execution or authentication bypass, work with default installations and should

not require any user interaction.

Start Date: 26 August 2020

End Date: 30 September 2020

50,000 USD



HOME

BOUNTIES

Exploit Acquisition Program

PLM and EPR

- **SAP (RCE)**: 250k USD
- **Siemens Teamcenter (RCE)**: 250k USD
- **Oracle ERP (RCE)**: 200k USD

250,000 USD



SSD Secure Disclosure

@SecuriTeam_SSD

...

Found a vulnerability in SAP NetWeaver?
Submit your findings today at ssd-disclosure.com/sap-netweaver-... and
get the BIG payouts you deserve

The image is a composite of two photographs. On the left, a woman with long hair and glasses is seen from the side, looking at a computer screen. On the right, a close-up view of a computer monitor displays a complex SAP NetWeaver application interface with multiple windows and data grids. The SAP logo is visible in the bottom left corner of the main image area.

SAP
**Netweaver
exploits**
are now in high-demand!

SAP ssd-disclosure.com

10:30 AM · May 26, 2024 · 1,113 Views



SSD Secure Disclosure ✅

@SecuriTeam_SSD

...

Found a vulnerability in SAP NetWeaver?
Submit your findings today at ssd-disclosure.com/sap-netweaver-... and
get the BIG payouts you deserve 💰💰💰

The image is a composite of several elements. On the left, there's a large SAP logo in blue and white. Next to it, the text "Netweaver exploits" is displayed in a large, bold, dark font, with "are now in high-demand!" in a smaller font below it. A horizontal red bar is positioned under the second line of text. On the right side, there's a photograph of a person with long hair wearing glasses, looking at a computer screen. The screen shows what appears to be a database or log entry. Below the photograph is the URL "ssd-disclosure.com".

10:30 AM · May 26, 2024 · 1,113 Views

“Why do you still report your findings to SAP instead of selling them to me !!??”

Around event in 2021

~~“Why do you still report your findings to SAP instead of selling them to me !!??”~~

Around event in 2021

What do these prices tell us ?



Confident of what they can get back

Confident of what they can get back

Pay more to win time

Finding SAP vulnerabilities... takes time

Creating reliable exploit... takes time

Confident of what they can get back

Pay more to win time

Finding SAP vulnerabilities... takes time

Creating reliable exploit... takes time

Public critical exploits are 4 years old

→ Exploit lose their effectiveness

→ Seek for “fresh” weapons

Takeaways





SAP Interest is growing... From heterogeneous groups

SAP Interest is growing... From heterogeneous groups

The demand for SAP 0day is growing... Because of ROI

SAP is no longer a black box
→ Consider SAP applications targeted

SAP is no longer a black box
→ Consider SAP application targeted

No 0days found
→ Mainly public vulnerabilities

CVE	CVSS	Exploit	KEV / Active	Ransomware Risk	SAP Security Note
CVE-2010-5326	10.0	Public	Yes / ACTIVE	High	1445998
CVE-2016-2386	9.8	Public	Yes / ACTIVE	High	2101079
CVE-2016-2388	5.3	Public	Yes	Low	2256846
CVE-2016-3976	7.5	Public	Yes / ACTIVE	High	2234971
CVE-2016-9563	6.5	Public	Yes	Low	2296909
CVE-2018-2380	6.6	Public	Yes / ACTIVE	High	2547431
CVE-2020-6207	10.0	Public	Yes / ACTIVE	Medium	2890213
CVE-2020-6287	10.0	Public	Yes / ACTIVE	Medium	2934135
CVE-2021-38163	9.9	Public	Yes / ACTIVE	Medium	3084487
CVE-2021-33690	9.9	Public	No / ACTIVE	High	3072955
CVE-2021-42063	8.8	Public	No / ACTIVE	Medium	3102769
CVE-2022-22536	10.0	Public	Yes / ACTIVE	Medium	3123396

SAP is no longer a black box
→ Consider SAP application targeted

No 0days found
→ Mainly public vulnerabilities
→ Patch them all !

SAP is no longer a black box
→ Consider SAP application targeted

No 0days found
→ Mainly public vulnerabilities
→ Patch them all !

Not only internet exposed vulnerabilities

SAP is no longer a black box
→ Consider SAP application targeted

No 0days found
→ Mainly public vulnerabilities
→ Patch them all !

Not only internet exposed vulnerabilities
→ SAP systems are widely connected
→ Manage SAP security **globally**

SAP is no longer a black box
→ Consider SAP application targeted

No 0days found
→ Mainly public vulnerabilities
→ Patch them all !

Not only internet exposed vulnerabilities
→ SAP systems are widely connected
→ Manage SAP security globally



Thank You!

Yvan Genuer
info@onapsis.com



THIS DOCUMENT CONTAINS CONFIDENTIAL INFORMATION & IS SUBJECT TO THE CONFIDENTIALITY AGREEMENT BETWEEN THE PARTIES

All data submitted in this document is solely for the use of the recipient and cannot be disclosed to any third party or used by the recipient for any other purpose than cooperation with Onapsis. This data shall not be duplicated, used or disclosed in whole or in part for any purpose. If a contract is awarded to Onapsis as a result of, or in connection with the submission of this data, the customer or prospective customer shall have the right to duplicate, use or disclose this data to the extent provided in the contract. This restriction does not limit the customer's or prospective customer's right to use the information contained in the data if it is obtained from another source without restriction. The data contained in this presentation does not constitute legal advice and is for informational purposes only. An attorney-client relationship is not presumed or intended by receipt or review of this presentation. Onapsis does not make any representations or warranties, express or implied, with respect to the accuracy or completeness of the data included in this presentation. Onapsis will have no liability with respect to the use or reliance upon this data by recipient. The following information is being shared in order to outline some of Onapsis' current product plans, but it is important to understand that it is being shared for informational purposes only, and not as a binding commitment. Please do not rely on this information in making purchasing decisions because Onapsis makes no representations about future functionality, and ultimately, the development, release, and timing of any products, features or functionality remains at the sole discretion of Onapsis and is subject to change.