گزارش اولیه سامانه RAT-2Ac2

اسفند ماه ۱۴۰۱

نسخه ۱.۰

فهرست

مقدمه

در اجرای حملات سایبری بعد از اجرای فرایند بهره کشی و ایجاد دسترسی به سیستم اهداف، یکی از مهم‌ترین امور ایجاد امکان دسترسی دائمی و طولانی مدت به سیستم اهداف با کمترین احتمال شناسایی است. امروزه با توجه به افزایش روزافزون دقت تشخیص نرم‌افزارهای ضدبدافزار، سطح حساسیت پیاده‌سازی و اجرای نرم‌افزارهای دسترسی از راه دور (Remote Access tool) در دسترس بسیار بالا بوده و باعث ایجاد هشدار برای راهبر سیستم هدف می‌شود. لذا با توجه حساسیت‌های موجود، الزام طراحی و توسعه محصولی که تا حد امکان کمترین میزان حساسیت برای نرم‌افزارهای ضدبدافزار و همچنین بیشترین امکان و سهولت برای استفاده و پیاده سازی در حملات، وجود دارد.

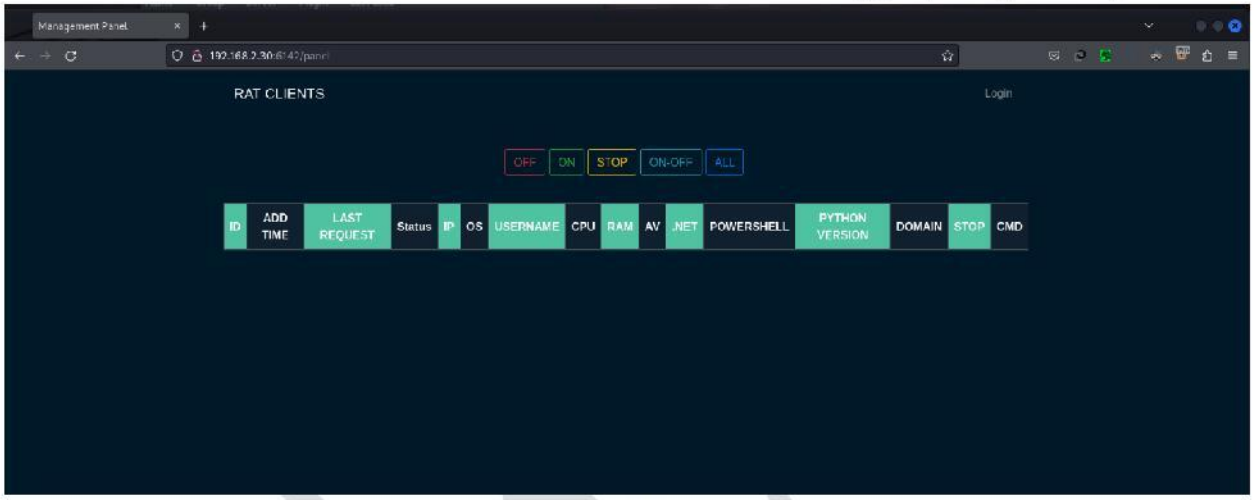
به همین خاطر تصمیم به طراحی و توسعه این محصول اتخاذ شد. در این گزارش به چگونگی استفاده و قابلیت های این محصول اشاره شده است.

ساختار و نحوه عملکرد

این محصول از دو بخش Client و Server تشکیل شده است. نسخه Client با زبان #C و Net Version 4. توسعه و طراحی شده است. نسخه Server با زبان Python و Flask Version 2 توسعه و پیاده سازی شده است. ارتباطات بین Client و Server تمامی از طریق پروتکل HTTP بوده و قابلیت جایگزینی با پروتکل HTTPS را نیز دارد. در ساختار پیش‌بینی شده برای اندازی و استفاده می‌توان از آدرس‌های DNS متعدد و Forwarder ها، به منظور جلوگیری از نشت آدرس IP سرور اصلی نیز استفاده کرد.

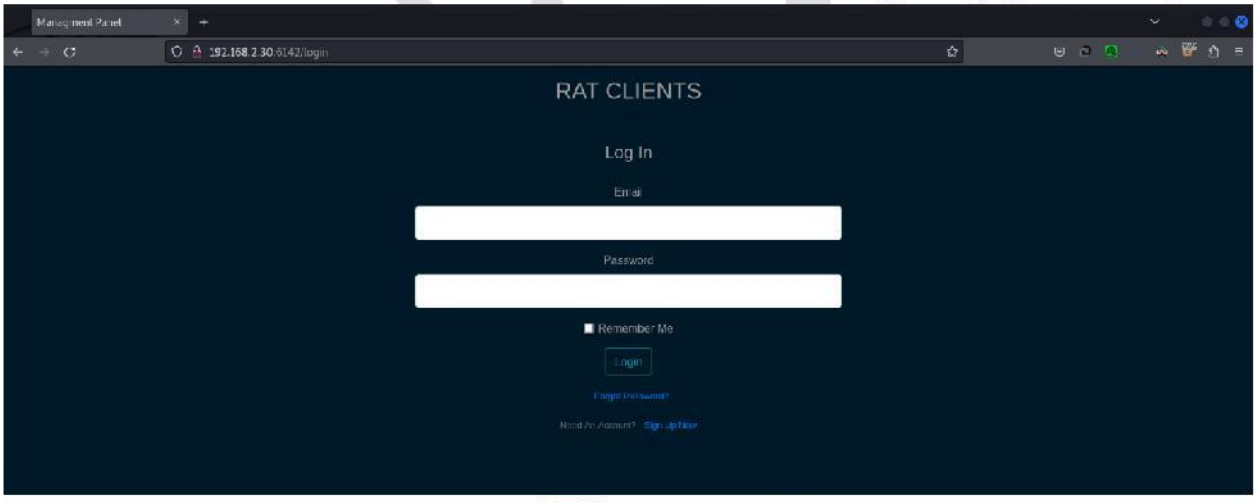
بخش‌های اصلی این سامانه عبارت‌اند از:

۱. Panel (صفحه اصلی سامانه) تصویر ۱



تصویر ۱ - صفحه اصلی سامانه

۲. Login (صفحه احرازهویت) تصویر ۲



تصویر ۲ – صفحه احراز هویتLOGIN

۳. API (صفحه احراز ثبت نام اولیه Client)

۴. CMD

۵. Image

۶. Keylogger (تصویر ۳)

تصویر ۳ – صفحه نتایج دریافتی از CLIENT و اطلاعات ثبت شده

۷. vncLauncher
۸. vncConnect
۹. vncTerminate
۱۰. file
۱۱. command
۱۲. result
۱۳. log
۱۴. download
۱۵. delete
۱۶. SysInfo
۱۷. uploadInDatabase

نحوه عملکرد

در زمان اجرای سامانه (Server) و شروع به کار ثبت نام و برقراری ارتباط بین کاربر(Client) و سامانه، در مرحله اول کاربر با استفاده از مسیر API، اقدام به ثبت نام و ارسال اطلاعات اولیه می‌کند. این اطلاعات اولیه شامل (تصویر۴):

۱. IP:

- آدرس IPv4 سیستم هدف در مقدار قرار می‌گیرد.

۲. OS:

- سیستم‌عامل و نسخه آن در مقدار ارسال می‌شود.

۳. CPU:

- مدل و تعداد پردازنده‌های موجود در این مقدار قرار می‌گیرد.

۴. RAM:

- شامل مقدار حافظه‌ی تصادفی سیستم هدف می‌باشد.

۵. AV:

- مدل و نوع ضدبدافزار استفاده شده سیستم هدف.

۶. NET:

- نسخه NET. موجود بر روی سیستم هدف.

۷. DOMAIN:

- نام دامنه در صورت عضویت ارسال می‌شود.

۸. POWERSHELL:

- نسخه POWERSHELL، موجود بر روی سیستم هدف در مقدار ارسال می‌شود.

۹. USERNAME:

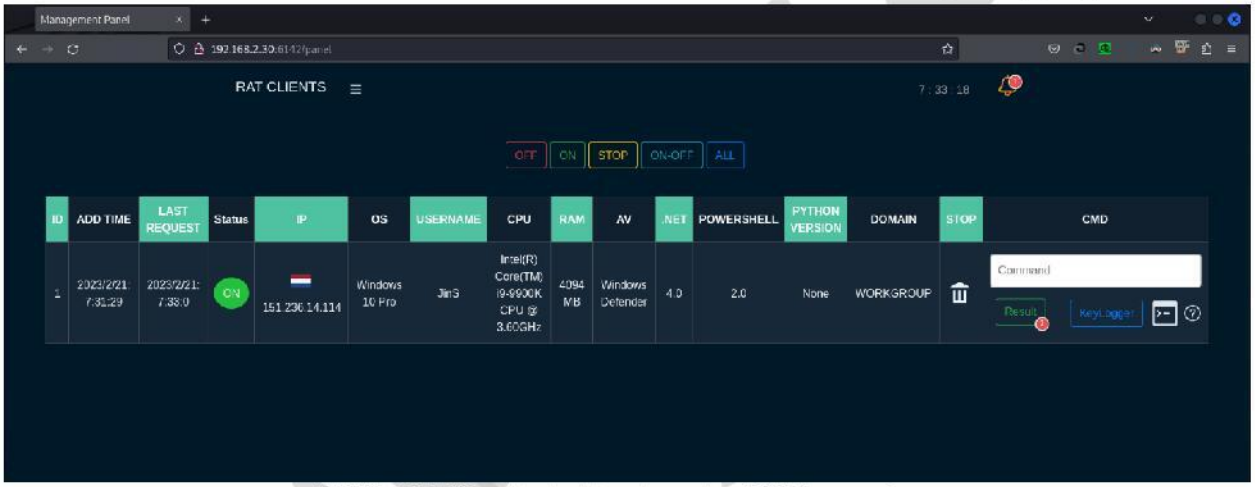
- نام کاربری که تحت دسترسی آن این نرم‌افزار اجرا شده است در مقدار ارسال می‌شود.

۱۰. PYTHON_VERSION:

- نسخه PYTHON، در صورت وجود بر روی سیستم هدف، ارسال می‌شود.

۱۱. COUNTRY:

- شامل کشور سیستم هدف است.



تصویر ۴ – صفحه PANEL پس از ثبت نام و برقراری ارتباط بین SERVER و CLIENT

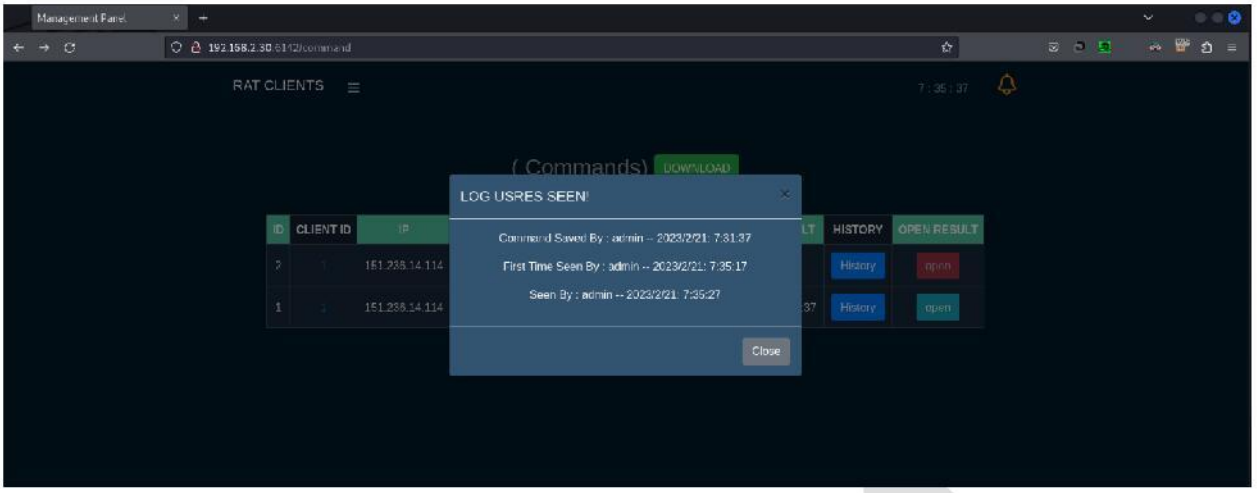
همانطور که در تصویر ۴ قابل مشاهده است،پس از ارسال این اطلاعات توسط کاربر، سامانه در پاسخ به درخواست، عددی را که به عنوان مقدار ID، تخصیص داده شده است را ارسال می‌کند. این عدد در ادامه فرایند برقراری ارتباط بین کاربر و سامانه مورد استفاده قرار می‌گیرد.

لازم به ذکر است به منظور ایجاد امنیت بیشتر در فرایند برقراری ارتباط بین سامانه و کاربر، مقداری از قبل تعیین شده می‌بایست در HEADER درخواست‌های ارسالی توسط کاربران وجود داشته باشد، در غیر اینصورت سامانه به هیچ یک از درخواست‌ها جواب صحیح نمی‌دهد و خطای Forbidden در پاسخ ارسال می‌کند(تصویر ۵). **همچنین برای مشاهده سامانه (Web Panel) نیز می‌بایست این مقدار در درخواست‌های ارسالی قرار گیرد. این مسئله‌بدین معناست که بعد از قرار دادن مقدار مذکور و پس از وارد کردن مقدار صحیح USERNAME و PASSWORD در صفحه LOGIN، اطلاعات موجود در پایگاه داده سامانه قابل مشاهده می‌باشد.**

تصویر ۵ – نمایش خطای FORBIDDEN در صورت عدم استفاده کلمه رمز در مقدار HEADER

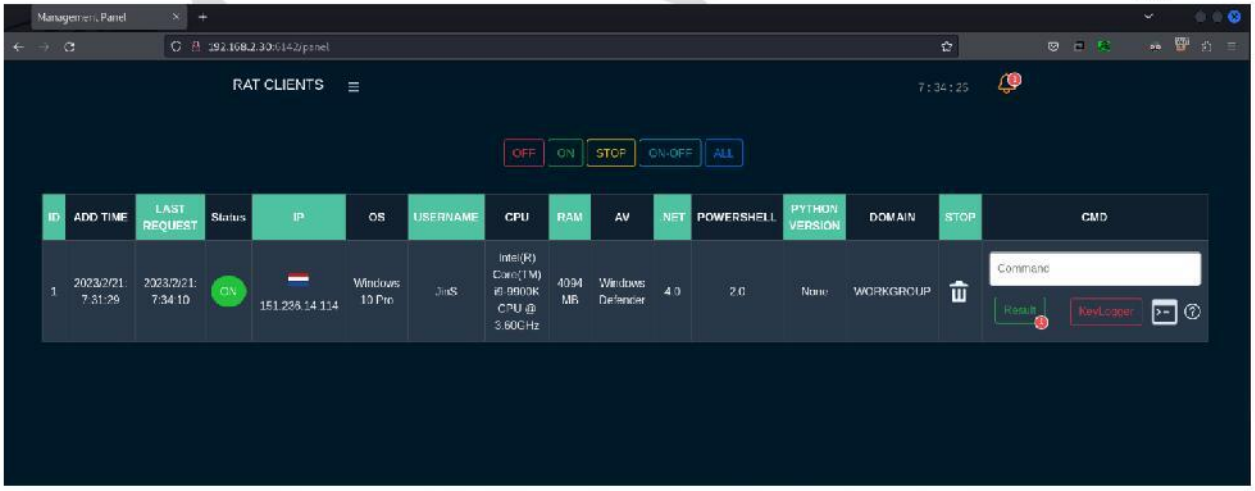
پس از انجام مرحله ثبت نام و تخصیص شماره ID، به کاربر احراز هویت شده، کاربران هر ۵ ثانیه یک‌بار اقدام به اعلام وضعیت خود، می‌کنند. در این فرایند کاربران از مسیر cmd/<id> می‌توانند دستورات ثبت شده برای اجرا را مشاهده کنند. این دستورات به صورت یکبار مصرف بوده و پس از بازدید، از بین می‌روند. تمامی دستورات ثبت شده در صفحه panel ، در پایگاه داده log می‌شوند.(لازم به ذکر است هر کاربر پس از انجام مراحل احراز هویت و ثبت اطلاعات در سامانه، در مرحله بعدی اقدام به ارسال نتیجه دستور systeminfo می‌کند. تصویر۶) اطلاعاتی که در پایگاه داده ثبت می‌شود شامل: زمان ثبت دستور، کاربر ثبت کننده دستور، زمان دریافت نتیجه دستور توسط سامانه، زمان مشاهده دستور راهبر، تعداد دفعات مشاهده نتیجه دستور و کاربر مشاهده کننده نتیجه ثبت و از طریق سامانه و گزینه history قابل مشاهده می‌باشد (تصویر۷).

تصویر ۶ – نتیجه دستور SYSTEMINFO ارسال شده توسط CLIENT



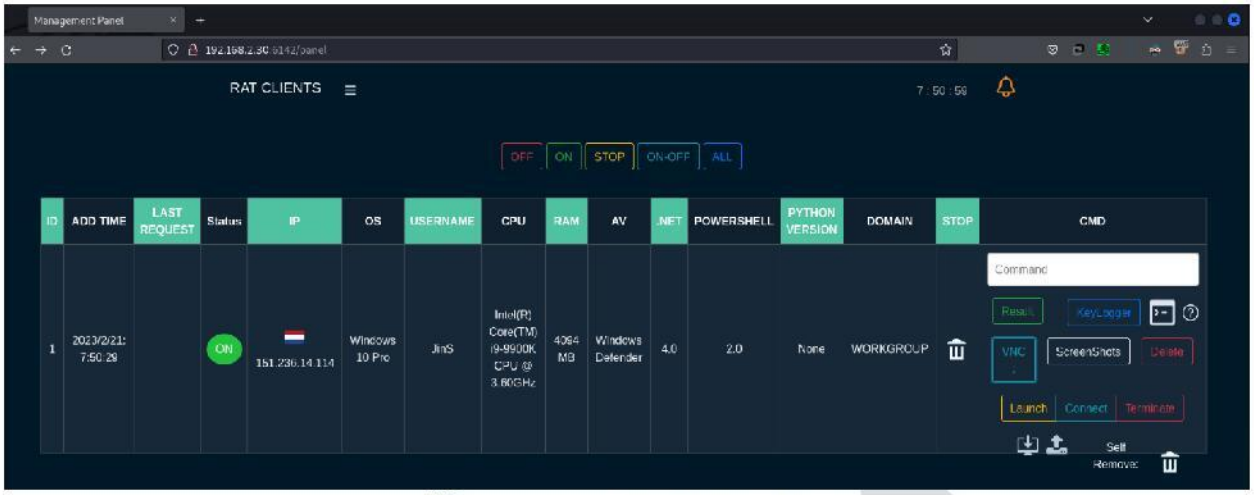
تصویر ۷- گزارش ثبت و مشاهدات دستور

قابلیت‌های موجود در سامانه شامل: vnc، keylogger، screenshot، file upload، file download می‌باشد.
برای اجرا و راه‌اندازی امکان keylogger، می‌بایست در سامانه دستور keylogger ثبت شود. سپس دکمه keylogger در صفحه به رنگ قرمز در آمده و منتظر دریافت نتایج می‌شود. کاربر (Client) پس از دریافت این دستور اقدام به ثبت اطلاعات صفحه کلید در یک فایل به صورت مخفی کرده و نتایج را در پاسخ برای سامانه ارسال می‌کند. پس از دریافت این اطلاعات دکمه keylogger در سامانه به رنگ آبی در می‌آید و در صورت کلیک بر روی دکمه نتایج دریافتی نمایش داده می‌شود. (تصویر۸)



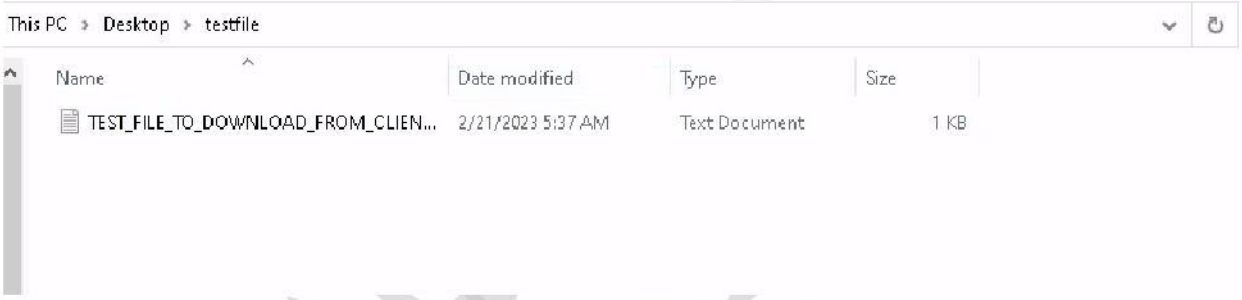
تصویر ۸ – دستور KEYLOGGER پس از ثبت در سامانه و در حالت انتظار برای دریافت نتایج

برای اجرای vnc، می‌بایست در ابتدا گزینه vncLaunch فعال شود. پس از فعالسازی این قابلیت در سامانه، کاربر(Client) اقدام به بارگیری نرم‌افزار bore و راه اندازی نرم‌افزار noVNC، و اجرای فرایند port forward با استفاده نرم افزار bore می‌نماید. پس از اجرای تمامی این مراحل آدرس bore.pub و شماره port به وجود آمده، برای سامانه ارسال می‌شود. سپس با استفاده از دکمه vncConnect می‌توان از طریق مرورگر به سیستم هدف متصل شد. برای پایان دادن به این فرایند می‌بایست از دکمه vncTerminate در سامانه استفاده کرد. این دکمه سرویس novncproxy راه اندازی شده بر روی سرور و novnc و bore را از روی سرور هدف غیرفعال می‌کند.(تصویر۹)

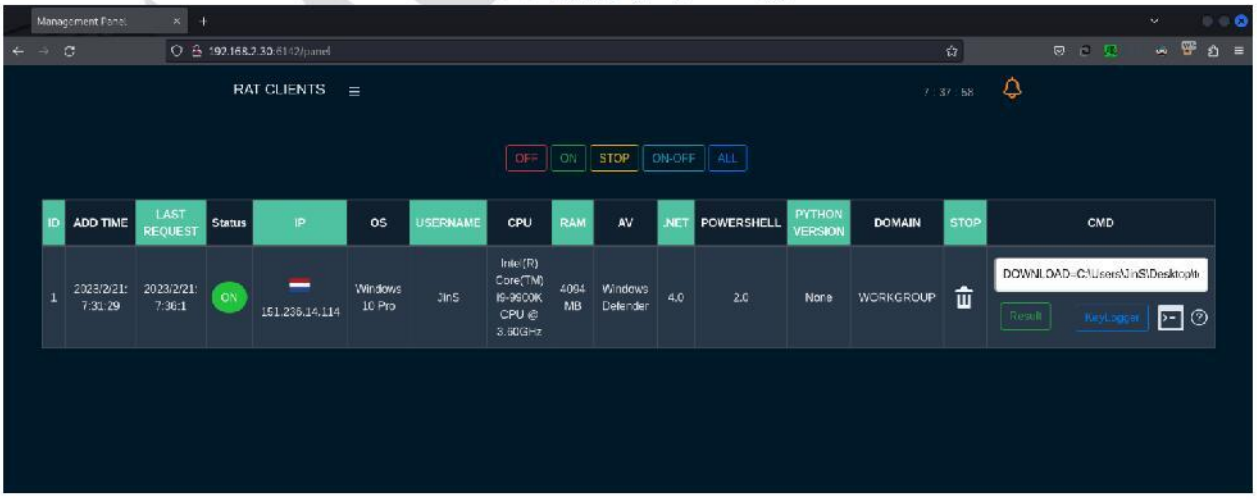


تصویر ۹ – دستورات قابل استفاده در دسته بندی VNC

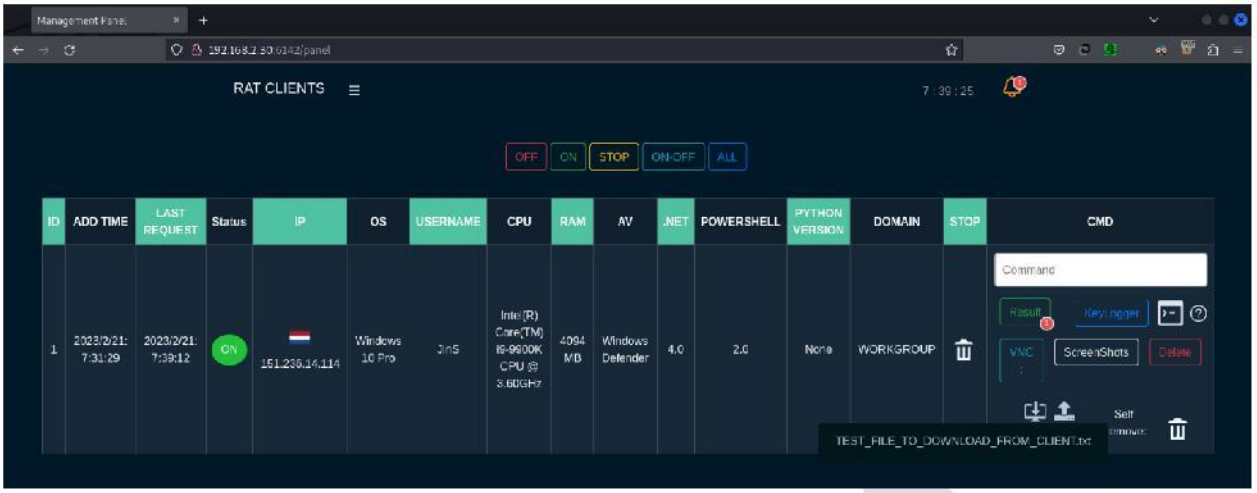
قابلیت بعدی امکان باگیری و بارگذاری file بر روی سیستم هدف است. به منظور بارگیری فایل می‌بایست در سامانه دستور DOWNLOAD=/path/to/file، و به جای عبارت path to file مسیر فایل مدنظر را وارد کرد. Client پس از دریافت این دستور اقدام به ارسال فایل مدنظر به سامانه می‌نماید. فایل‌های ارسالی توسط Client، در سامانه قابل مشاهده می‌باشد. (تصویر ۱۰ و ۱۱ و ۱۲)



تصویر ۱۰– file و مسیر آن بر روی سیستم هدف

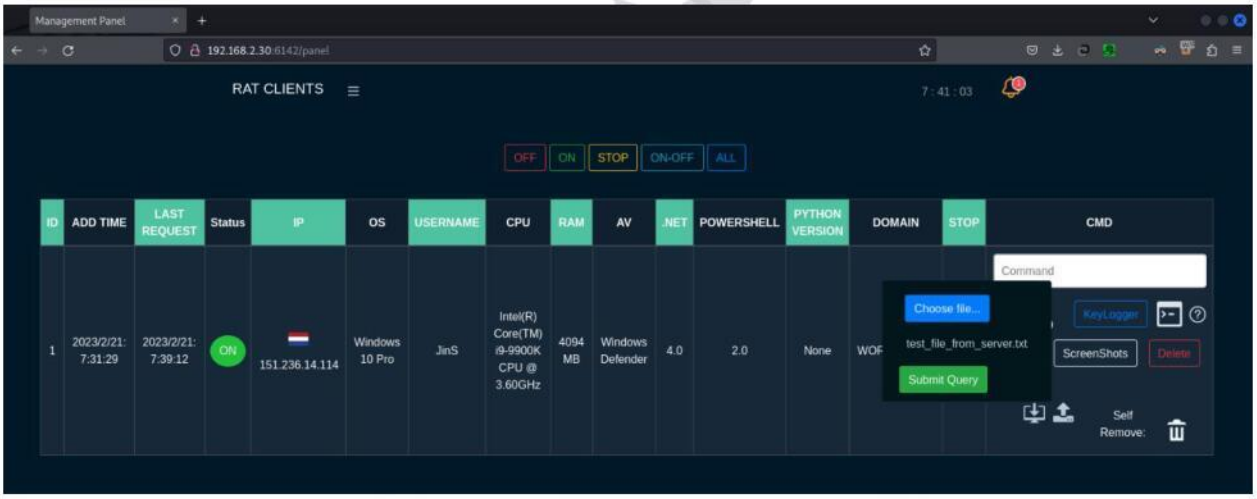


تصویر ۱۱ – دستور بارگیری file مدنظر

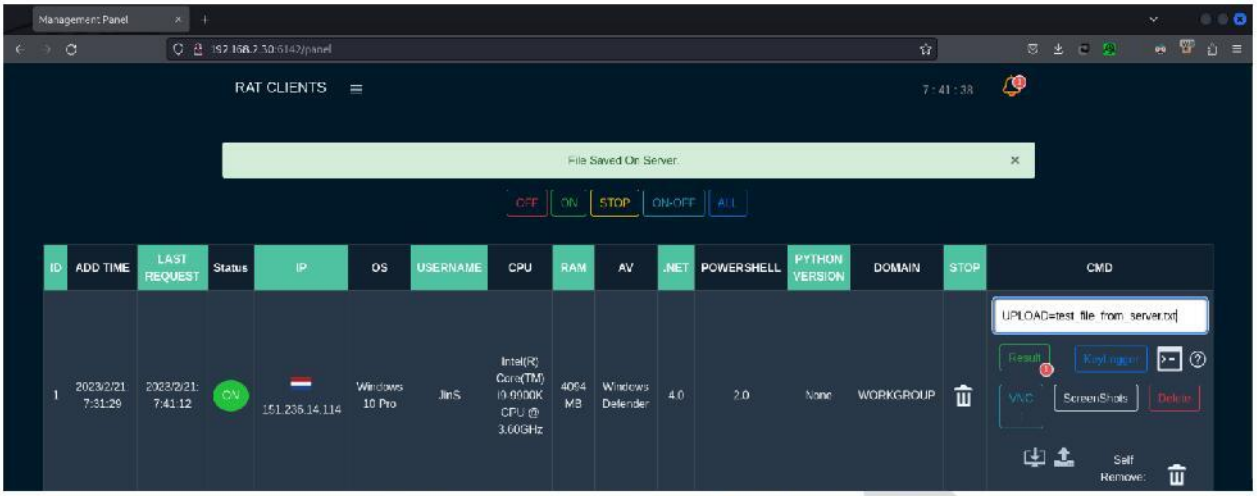


تصویر ۱۲ – file بارگیری شده از روی سیستم هدف قابل مشاهده در سامانه

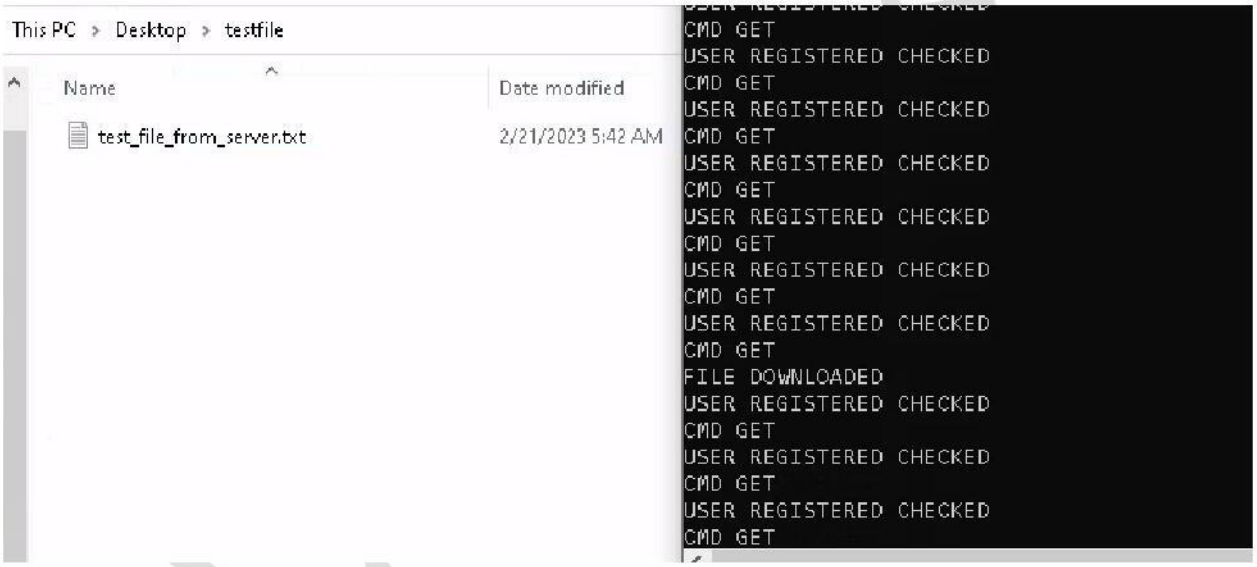
برای استفاده از قابلیت بارگذاری file بر روی سیستم هدف، ابتدا می‌بایست در سامانه اقدام به باگذاری file مدنظر و در قسمت ثبت دستورات در panel اقدام به وارد کردن عبارت UPLOAD=/path/to/file/yourfile.format، و به جای عبارت path to file آدرس و مسیر قرار گیری فایل مدنظر و نام فایل مدنظر قرار می‌گیرد. پس از ثبت این دستور فایل از روی سامانه توسط client بارگیری و در مسیر مدنظر قرار می‌گیرد.(تصویر ۱۳ ، ۱۴ و ۱۵)



تصویر ۱۳- بارگذاری file مدنظر بر روی سامانه به منظور بارگیری آن توسط CLIENT



تصویر ۱۴- پس از ثبت file، میبایست دستور بارگذاری آن در سامانه ثبت شود

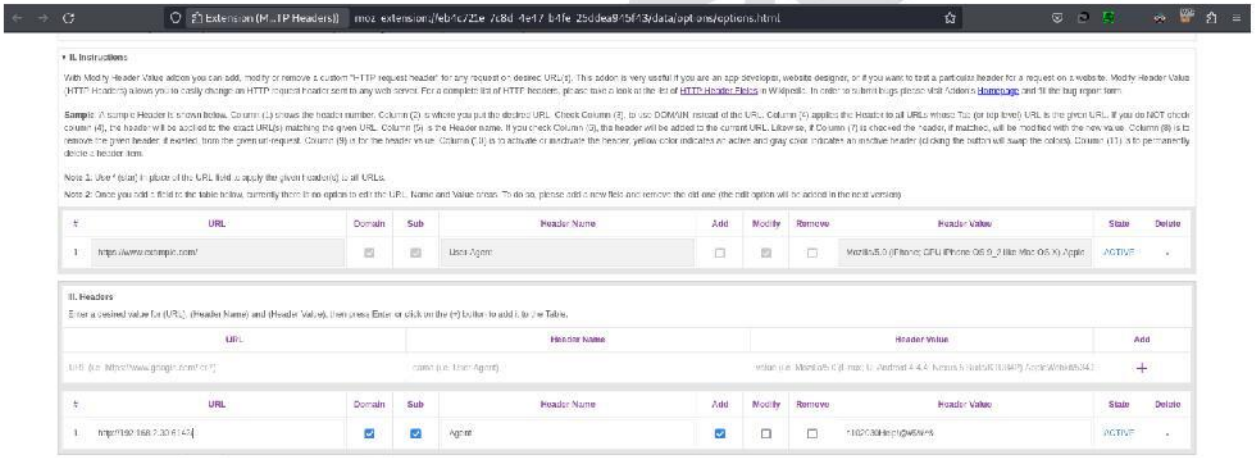


تصویر ۱۵ – پس از ثبت درخواست CLIENT اقدام به بارگیری file می‌نماید.

تمامی دستورات ثبت شده و نتایج آن در سامانه، قابل استخراج با فرمت CSV میباشد. (تصویر ۱۶)

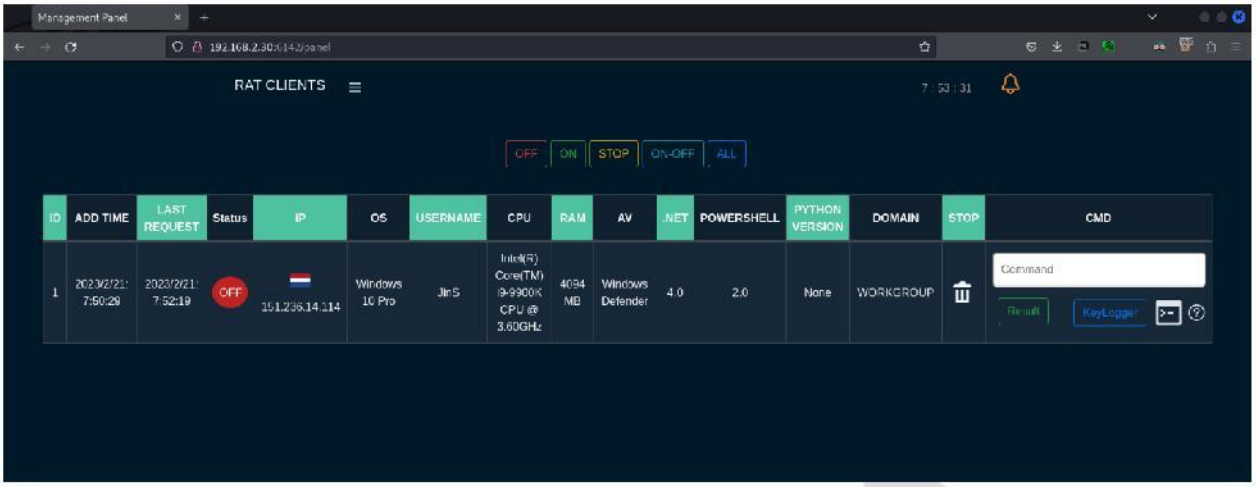
تصویر ۱۶ – نتایج تمامی دستورات با فرمت BASE64 در پایگاه داده ذخیره می‌شود. (نمونه دستورات و جزئیات آن در فایل استخراج شده.)

برای مشاهده صفحه webpanel میتوان از افزونه‌ی Modify Header Values استفاده کرد. (تصویر ۱۷)

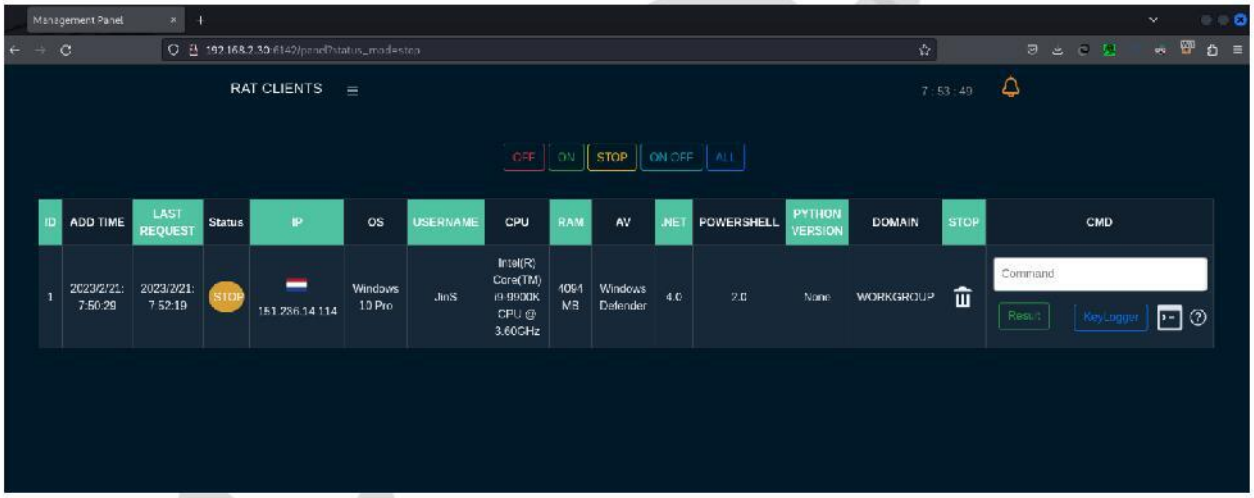


تصویر ۱۷ – صفحه تنظیمات و ثبت کلید مدنظر در مقدار HEADER

تمامی CLIENTهای ثبت شده در سامانه، دارای وضعیت بوده و دسته بندی آن‌ها، شامل : ON، OFF و STOP می‌باشد. در سامانه بر اساس وضعیت لیست CLIENT ها قابل filter می‌باشد.(تصویر ۱۸و ۱۹)



تصویر ۱۸- وضعیت OFFLINE یک CLIENT در سامانه. (تمامی CLIENT های ثبت نام شده در سامانه می‌بایست هر ۱۰ ثانیه اقدام به اعلام وضعیت خود به سامله کنند. در صورتی که بیشتر از ۱۰ ثانیه (یا هر مقداری که تعریف شده باشد) گذشته و درخواستی از سوی CLIENT دریافت نشده باشد، وضعیت CLIENT از ON به OFF تغییر می‌کند.



تصویر ۱۹- امکان STOP کردن CLIENT از طریق سامانه امکان پذیر است. به منظور انجام اینکار در سامانه و ستون STOP و کلیک کردن بر روی دکمه موجود CLIENT به حالت STOP در آمده و دیگر درخواست ارسال نمیکند. لازم به ذکر است این قابلیت به معنای حذف و از بین بردن نرم‌افزار بر روی سیستم هدف نمی‌باشد و به منظور حذف کامل نرم‌افزار دکمه‌ای دیگر با نام Self Remove در نظر گرفته شده است که با استفاده از آن نرم‌افزار به صورت کامل حذف شده و تمامی اطلاعات خود را از روی سیستم هدف پاکسازی می‌کند. در تصویر بالا وضعیت کاربر از حالت ON به STOP تغییر کرده است.

نصب و راه اندازی

به منظور نصب و راه‌اندازی سامانه (SERVER)، پیشنهاد می‌شود از سیستم‌عامل‌های مبتنی بر Linux و Debian استفاده شود. پیش‌نیازهای راه‌اندازی Python Version 3.x می‌باشد. برای نصب Flask و سایر کتابخانه‌های استفاده شده از دستور pip3 install -r requirement.txt استفاده شود. این دستور تمامی کتابخانه‌های مورد نیاز را نصب و آماده استفاده می‌کند. برای اجرا و راه‌اندازی سرور، با استفاده از دستور python3 app.py می‌توان استفاده کرد.

لازم به ذکر است برای تغییر آدرس و port سامانه میبایست این مقدار در ابتدای source code، app.py در خط پایانی تغییر کند.