



سامانه تاقب

بدافزار ویژه سیستم عامل ویندوز





سامانه تاقب

بدافزار ویژه سیستم عامل ویندوز

معرفی

دسترسی پایدار به اطلاعات دارای طبقه بندی و حیاتی سیستم های اطلاعاتی مختلف همچون پایگاه های داده سازمان های دولتی و خصوصی و همچنین دسترسی به اطلاعات موجود در سیستم های رایانه ای با هدف بهره برداری از اطلاعات ، ایجاد تغییر و یا حذف آن به نفع خود همواره دارای اهمیت بالایی در جنگ سایبری بوده است. از این رو طراحی و ساخت سامانه بدافزار ویژه سیستم عامل ویندوز در دستور کار مؤسسه افق قرار گرفت.

بدافزار ثاقب جهت آلوده سازی سیستم های رایانه ای و سرور های اطلاعاتی با تمرکز بر سیستم های رایانه ای شخصی (PC) مبتنی بر سیستم عامل ویندوز طراحی و توسعه یافته است.





با توجه به اهمیت اطلاعات در اختیار اشخاص حقیقی، مقامات و اشخاص رده بالای دولتی و ...، با علم به آن که اکثر آنان به جهت سهولت بکارگیری، از سیستم عامل ویندوز بر روی رایانه های شخصی خود بهره می برند، این بدافزار جهت آلوده سازی رایانه های شخصی مبتنی بر سیستم عامل ویندوز گسترش یافته است. با توجه به این موضوع، برخی از قابلیت های گنجانده شده در بدافزار نیز متناسب با نسخه ویندوز PC در نظر گرفته شده است که می توان به استیلر تلگرام و مرورگر به دلیل اهمیت اطلاعات موجود و بر روی این دو ابزار اشاره کرد.

چالش عمده ای که در مورد سرورهای ویندوزی نیز مطرح می باشد، عدم وجود دسترسی پایدار با استفاده از "SHELL" بوده و این احتمال وجود دارد که با تغییر ساختار شبکه دسترسی موجود از طریق SHELL از بین رود. به همین جهت استفاده از بدافزار امکان ایجاد یک ارتباط اینترنتی فعال به سرور مورد نظر را در اختیار کاربر قرار می دهد.

چالش ها و نکات طراحی بدافزار ثاقب

چالش ها و نکات اصلی که در جریان طراحی بدافزار ثاقب به جهت دریافت بهترین عملکرد در نظر گرفته شده است به شرح ذیل می باشد:

۱. FUD

Fully UnDetected (FUD) یا غیرقابل شناسایی بودن یک بدافزار، مشهورترین و مهمترین چالش در طراحی آن است. بدافزار زمانی ارزشمند است که هیچ آنتی ویروسی نتواند آن را شناسایی و حذف نماید. مهمترین دغدغه شرکت های فعال در حوزه ضد بدافزار در سطح جهانی کشف و شناسایی و جلوگیری از فعالیت بدافزارها در کوتاه ترین زمان ممکن است. در این راستا امضای بدافزار (Malware Signature) به عنوان مفهومی در سیستم های ضد بدافزار شکل گرفته است. بدافزار به محض اینکه توسط نرم افزار امنیتی شناسایی گردد، نمونه ای از آن توسط نرم افزار امنیتی به مرکز تحلیل خود واقع در شرکت ارائه دهنده آن ارسال خواهد شد. کارشناسان شرکت مربوطه بدافزار را تحلیل و نهایتاً به الگوی ساختار بدافزار که به آن امضای



بدافزار گفته می شود دست خواهند یافت. این امضا در به روزرسانی های بعدی نرم افزار امنیتی مورد نظر گنجانده شده و پس از آن ، هر زمان که نسخه ای مشابه به بدافزار مربوطه در سطح جهانی مشاهده شود، به سرعت توسط نرم افزارهای امنیتی شناسایی شده و جلوی فعالیت آن گرفته می شود.

قابلیت FUD بدافزار ثاقب این مزیت را فراهم نموده است که هیچ امضایی از آن در نرم افزار های امنیتی وجود نداشته و این امکان را فراهم نموده است که بدافزار به مدت طولانی در سیستم های رایانه ای دارای نرم افزار های امنیتی به فعالیت خود بدون شناسایی توسط آنتی ویروس ادامه دهد.

۲. عدم وابستگی به Framework

چالش مطرح دوم در طراحی بدافزار ثاقب ، عدم وابستگی به یک چارچوب (Framework) خاص است. بدین معنا که بدافزار ثاقب در همه محیط های ویندوزی و فارغ از نصب بودن یا نبودن یک نرم افزار خاص امکان فعالیت داشته باشد. برای مثال بدافزارهایی که با استفاده از زبان برنامه نویسی C# نوشته شده اند وابسته به یک چارچوب نرم افزاری خاص بوده و لازم است برای اجرا شدن این نوع بدافزارها یکی از نسخه های Net Framework. روی سیستم هدف نصب شده باشد. مفهومی به نام Native بودن در دنیای بدافزار وجود دارد که طبق این مفهوم کلیه بدافزارها به دو دسته Native و غیر Native تقسیم بندی می شوند. بدافزارهای Native که ارزش بالاتری نسبت به بدافزارهای غیر Native دارند، هیچ گونه وابستگی به شرایط محیط اجرا ندارند و می توانند اجرا شوند. ولی بدافزارهایی که Native نیستند همیشه به نصب بودن یک چارچوب نرم افزاری خاص جهت اجرا شدن خود نیازمندند. بدافزارهایی که با زبانهای برنامه نویسی C، C++، Delphi و Assembly نوشته شده اند نمونه ای از بدافزارهای native هستند. در مقابل بدافزارهایی که با زبانهای برنامه نویسی مثل C#، Visual Basic و Java نوشته شده اند جزء بدافزارهای غیر Native بوده و ارزش پایین تری دارند. در طراحی بدافزار ثاقب نیز این موضوع در نظر گرفته شده و بدافزار فارغ از نصب بودن یا نبودن سایر نرم افزار ها بر روی سیستم هدف ، قادر به فعالیت می باشد.



۳. پنهان کاری

پنهان کاری، اصلی مهم در طراحی بدافزار است. بدافزار چنانچه اصول پنهان کاری را رعایت ننماید پس از مدت کوتاهی می‌تواند توسط نرم افزارهای امنیتی و یا مدیر سیستم آلوده شده شناسایی شود. دور از چشم بودن و مخفی شدن در لایه‌های مختلف سیستم عامل می‌تواند نقش بسزایی در ماندگاری بدافزار داشته باشد.

۴. سطح دسترسی

داشتن بیشترین سطح دسترسی از سیستم عامل همیشه یکی از دغدغه‌های مهم طراحان بدافزار است. یک بدافزار ممکن است با سطح دسترسی یک کاربر مهمان اجرا شود که در این صورت کمترین گستره فعالیت را خواهد داشت. در مقابل چنانچه فردی که بدافزار را اجرا می‌کند مدیر یک سیستم باشد، بدافزار می‌تواند با حداکثر دسترسی فعالیت نموده و در این شرایط دست کاربر استفاده کننده از بدافزار برای دستکاری در سیستم آلوده شده بازتر خواهد بود.

اصول امنیتی در نظر گرفته شده در طراحی بدافزار ثاقب

در طراحی معماری یک بدافزار رعایت اصول امنیتی جهت عدم شناسایی شدن آن توسط هدف متخاصم از اهمیت بالایی برخوردار است. اگر معماری بدافزار دچار نقایص امنیتی باشد علاوه بر کشف و شناسایی خود بدافزار، مبدا تولید بدافزار نیز شناسایی خواهد شد که هزینه‌های آن به مراتب بیشتر از شناسایی شدن خود بدافزار است. از نظر معماری، یک بدافزار از دو قسمت RAT (Remote Administration Tool) یا ایجنت و پنل فرماندهی (Command & Control) تشکیل شده است. ایجنت همان برنامه‌ای است که بر روی سیستم هدف اجرا شده و آن را آلوده می‌سازد. در مقابل پنل فرماندهی وظیفه نظارت و صدور دستورات مختلف را به ایجنت بر عهده دارد.





در این نوع معماری دو پارچه ، رعایت برخی اصول امنیتی جهت عدم شناسایی شدن بدافزار ضروری است که مهمترین آنها به شرح ذیل می باشد:

۱. مخفی کردن اطلاعات سرور پنل در ایجنت تا حد امکان

هر بدافزار پس از شروع فعالیت در سیستم هدف و جمع آوری اطلاعات، نیازمند ارسال اطلاعات جمع آوری شده به سرور پنل (سرور کنترل و ارسال دستورات) است. در نتیجه اطلاعات سرور پنل سامانه ثاقب به شیوه های مختلف داخل بدافزار مخفی گردیده تا به راحتی و با یک تحلیل ساده نتوان به سرور اصلی دست یافت.

۲. رمزنگاری اطلاعات رد و بدل شده بین پنل و بدافزار (ایجنت)

اطلاعات جمع آوری شده توسط بدافزار، قبل از ارسال رمزنگاری می گردد تا در صورت شنود ترافیک ارسالی شبکه ، دسترسی به جزئیات اطلاعات امکان پذیر نباشد. در بدافزار ثاقب نیز این مهم در نظر گرفته شده است و کلیه اطلاعات قبل از ارسال با استفاده از الگوریتم XOR رمزنگاری شده تا امکان دسترسی و کشف محتوای آن وجود نداشته باشد.

۳. هدایت ترافیک بین پنل و بدافزار (ایجنت) از طریق مسیرهای چندگانه و طولانی همانند

شبکه TOR

هرچه مسیر رسیدن اطلاعات از ایجنت به سرور پنل طولانی تر باشد، احتمال شناسایی شدن سرور پنل پایین تر خواهد بود. همچنین اگر مسیرهای مختلفی را برای ارسال اطلاعات به پنل مرکزی انتخاب گردد ، احتمال شناسایی سرور پنل کاهش خواهد یافت. یکی از روش های پنهان کردن مقصد ترافیک بدافزار (ایجنت) ، هدایت اطلاعات از شبکه TOR است. شبکه TOR به علت قرار دادن چندین سرور واسط در مسیر بسته های ارسالی، کار شناسایی سرور مقصد را دشوار می کند. در حال حاضر بدافزار ثاقب جهت رسیدن به سرور پنل هفت گام (سرور واسط) را از طریق شبکه TOR می پیماید.





۴. استفاده از سرورهای رله و پروکسی در مسیر رسیدن به سرور پنل

سرور رله (Relay Server) و پروکسی وظیفه ای همانند شبکه TOR را انجام می دهند. با این تفاوت که کنترل سرورهای شبکه TOR در اختیار طراحان بدافزار نمی باشد. در مقابل چنانچه از سرور رله برای هدایت اطلاعات بدافزار (ایجنت) استفاده شود، در هر زمان می توان از سرورهای رله دیگر به عنوان جایگزین سرور رله اول استفاده نمود که این امر باعث کاهش احتمال شناسایی شدن بدافزار می گردد. در معماری بدافزار ثاقب از ترکیب سرورهای رله و شبکه TOR به منظور هدایت اطلاعات بدافزار (ایجنت) استفاده شده است. به این معنا که اطلاعات ابتدا وارد سرور رله شده و سپس از طریق شبکه TOR به مقصد نهایی (سرور کنترل بدافزار) می رسند.

۵. رعایت اصول برنامه نویسی ایمن در ایجنت

یکی از روش های FUD کردن بدافزار، رعایت اصول برنامه نویسی ایمن و استاندارد است. دستکاری های خطرناک در سیستم عامل، فعالیت بیش از اندازه در سیستم فایل، رجیستری و دیگر منابع سیستم، ارسال گسترده اطلاعات در سطح شبکه و اشغال کردن پهنای باند سیستم هدف از جمله مثال های برنامه نویسی نا ایمن است که عمر بدافزار را به حداقل خواهد رساند. یک مثال از برنامه نویسی ایمن در بدافزار ثاقب، تکه تکه کردن اطلاعات در قالب چندین بسته کوچک و ارسال هر بسته با رعایت تاخیر زمانی مناسب است. با این کار ترافیک خروجی از سیستم متعادل تر خواهد بود که منجر کاهش احتمال شناسایی شدن بدافزار می گردد.

۶. استفاده از روش های Anti-Debug در ایجنت

یکی از روش ها جهت تحلیل بدافزار و شناسایی مقصد ارسال اطلاعات، دیباگ (Debug) بدافزار است. اگر یک بدافزار از هیچ روشی جهت مقابله با دیباگ شدن استفاده نکند، به راحتی و با یک تحلیل ساده نحوه عملکرد ایجنت و اطلاعات سرور مقصد قابل شناسایی است. در نتیجه استفاده از روش های Anti-Debug یک اصل اجتناب ناپذیر در طراحی بدافزار ثاقب بوده است که کار تحلیلگران بدافزار را جهت کشف آن دشوار تر می سازد.





پس از طراحی و ساخت بدافزار تاقب و حصول اطمینان از عملکرد آن ، FUD بودن آن نیز بررسی گردید. به همین جهت از یک آزمایشگاه بدافزار استفاده گردید. یک آزمایشگاه بدافزار، به ماشینی گفته می‌شود که در آن به تعداد آنتی‌ویروس‌های مطلوب چندین هاست نصب شده و روی هر هاست یک آنتی‌ویروس نصب گردد. کاربر قبل از استفاده از بدافزار در محیط عملیات، لازم است آن را در محیط ایزوله آزمایشگاه و در مقابل آنتی‌ویروس‌های به روز شده آزمایش نماید تا از FUD بودن بدافزار مطمئن گردد. رعایت نکات ایمنی در آزمایشگاه بدافزار و اجرای به ترتیب آنها بسیار ضروری است که فهرست آن در زیر آمده است:

۱. به روز رسانی آنتی‌ویروس‌ها و گرفتن Snapshot از ماشین ها قبل از آزمایش

۲. قطع اتصال به شبکه اینترنت در ماشین تحت آزمایش و اطمینان از ایزوله بودن آن

۳. قراردادن ایجنت در محیط ماشین تحت آزمایش و اجرای بدافزار

۴. مشاهده واکنش آنتی ویروس پس از اجرای بدافزار

۵. برگرداندن Snapshot ماشین تحت آزمایش به حالت قبل

۶. ایجاد تغییرات لازم در ایجنت در صورت FUD نبودن آن

گام های بالا آنقدر تکرار می گردد تا در نهایت بدافزار در برابر کلیه آنتی‌ویروس‌ها FUD گردد. پس از FUD شدن بدافزار لازم است با دقت و در محیطی ایزوله (عدم اتصال به اینترنت) و دور از دسترس آنتی‌ویروس‌ها نگهداری شود. بهترین محیط برای این منظور ویندوز ۷ است که در آن نرم‌افزار و سرویس امنیتی مهمی در حال اجرا نمی‌باشد.

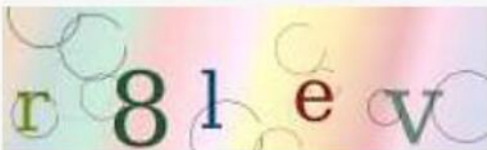


مطابق تصویر ۱، با وارد کردن نام کاربری و کلمه عبور در دامنه متصل بر بستر TOR که در اختیار کاربر قرار گرفته است، دسترسی به پنل کاربری امکانپذیر خواهد شد.

Login Form


Username

Password



enter captcha value

Log in

 Panel!

تصویر ۱ - صفحه ورود به پنل کاربری

ب) صفحه لیست کلاینت‌ها

اولین صفحه ای که کاربر پس از ورود به پنل آن را مشاهده می‌نماید، صفحه لیست کلاینت‌ها است. در این صفحه لیست کلیه کلاینت‌های آنلاین و آفلاین نمایش داده می‌شود. توضیحات هریک از موارد مذکور در تصویر ۲ مطابق شرح زیر است:

۱. Add new client

با کلیک روی این دکمه کاربر می‌تواند یک ایجنت جدید به منظور آلوده‌سازی یک کلاینت ایجاد نماید. لازم به ذکر است که ایجنت ایجاد شده فقط بر روی یک کلاینت اجرا می‌شود و پس از اولین اجرا و آنلاین شدن کلاینت، امکان اجرای ایجنت روی کلاینت دیگر وجود ندارد.

۲. Serial Number

برای هر ایجنتی که تولید می‌شود یک شناسه یکتا ایجاد می‌گردد که آن را از بقیه ایجنت‌ها متمایز می‌نماید.

۳. Status

این قسمت وضعیت کلاینت را از نظر آنلاین و آفلاین بودن آن نشان می‌دهد.

۴. Interval

ایجنت مورد نظر برای گرفتن دستورات جدید از پنل فرماندهی خود هر چند ثانیه یکبار به پنل رجوع می‌نماید. این مقدار بطور پیشفرض ۲۰ ثانیه در نظر گرفته شده است که قابل تغییر است.

۵. Clients

با کلیک روی این دکمه می‌توان به لیست کلاینت‌های آنلاین و آفلاین بطور مجزا دسترسی داشت.

۶. Users

کلیک روی این لینک کاربر را به بخش مدیریت کاربران هدایت می‌کند.

۷. Home

کاربر هر زمان که در قسمتی دیگر از پنل حضور داشته باشد با کلیک بر روی این گزینه به صفحه اصلی (صفحه کلاینت‌ها) هدایت خواهد شد.



۸. Log Off

منجر به خروج کاربر از پنل می‌شود.

۹. Lock Screen

پنل کاربری را قفل می‌کند که پس از کلیک بر روی آیکن موجود در صفحه Lock Screen کاربر می‌تواند دوباره صفحه پنل کاربری را مشاهده نماید.

۱۰. Fullscreen

جهت نمایش تمام صفحه سامانه به کار برده می‌شود.

#PELAK-1

Panel!

GENERAL FEATURES

- Home → 7
- Clients → 5
- Users → 6

10 9 8

List Of Targets

Search:

i	SN	Comp-Name	User-Name	OS	Cpu-Arch	IP	Time-Zone	Interval	Status	Users	Homes
3	30011THHZNS	null	null	null	null	null	null	30 s	off	Users (0)	Homes (0)
4	3PBV87PT3E0Y	INETSrvH	we9puulacul	8	x64	::ffff:127.0.0.1	UTC+2	0 s	off	Users (0)	Homes (0)
5	D363B28105/r	WIN10-PC	win10	7	x64	::ffff:127.0.0.1	UTC-0	20 s	off	Users (1)	Homes (0)
6	15DF0EFE5A00	WIN-FRKJCR6F-H2H	win8	8	x64	::ffff:127.0.0.1	UTC-8	20 s	off	Users (1)	Homes (0)
7	337381E3B/4B	WIN10-PC	win10	7	x64	::ffff:127.0.0.1	UTC-8	20 s	on	Users (1)	Homes (0)

تصویر ۲ - صفحه اصلی سامانه تاقب



پ) پنل راهبری بدافزار

مطابق تصویر ۳، پس از دوبار کلیک بر روی یک کلاینت کاربر به صفحه‌ای هدایت می‌شود که در آن می‌تواند از وضعیت بدافزار آگاهی پیدا کرده و دستورات مختلف را برای آن صادر نماید که دارای قابلیت‌های زیر است:

۱. Client Info

این بخش اطلاعات کلی سیستم کلاینت مانند نام رایانه، نام سیستم عامل و نام کاربری به کاربر نمایش می‌دهد.

۲. Interval

با استفاده از دکمه لغزنده می‌توان میزان زمانی را که بدافزار بصورت متناوب برای دریافت دستورات جدید به پنل مراجعه می‌نماید بر حسب ثانیه تنظیم نمود. برای مثال اگر این مقدار برابر ۲۰ باشد، بدافزار هر ۲۰ ثانیه یکبار دستورات جدید را از پنل فرماندهی خواهد خواند. برای اعمال تنظیم مورد نظر لازم است بر روی دکمه روبروی آن (Set) کلیک نماید.

۳. Auto Run

با کلیک بر روی منوی بازشونده کاربر می‌تواند بدافزار (ایجنت) را در حالت اجرای خودکار قرار دهد. بدین معنا که چنانچه سیستم کلاینت به هر دلیلی راه اندازی مجدد شود ایجنت مورد نظر از کار خواهد افتاد، اما با تنظیم راه اندازی خودکار ایجنت روی هفتگی یا روزانه، در زمانی مشخص در یک روز از هفته یا بصورت روزانه چنانچه سیستم روشن بوده و بدافزار (ایجنت) در حال اجرا نباشد شروع به کار خواهد کرد.

۴. Kill RAT

هر زمان که کاربر نیازی به وجود دسترسی بر روی سیستم هدف نداشته و یا احتمال دهد که بدافزار امکان دارد توسط سیستم هدف کشف گردد، با انتخاب این گزینه بدافزار را از روی سیستم هدف حذف می‌نماید.



۵. Ask Current Info

اطلاعات جاری بدافزار مانند مشخصات سرورهای رله و ورژن بدافزار را بازیابی می نماید.

۶. Update RAT

اگر نسخه جدیدی از بدافزار موجود باشد ، کلیک روی این دکمه، بدافزار جدید را جایگزین نسخه قدیمی خواهد کرد.

The screenshot displays the SAMANAH web interface. On the left is a sidebar with 'GENERAL FEATURES' and navigation links for 'Home', 'Clients', 'Online', 'Offline', and 'Users'. The main content area is divided into two sections: 'Target Details' and 'Target Modules'.

Target Details: This section contains a box with the following information:

- Serial No.: 337E81E3BA4B
- Comp-Name: WIN10-PC
- User Name: win10
- OS: 7
- Cpu-Arch: x64
- IP: 127.0.0.1
- Time-Zone: UTC-8

 A red dashed box highlights this information, with a red arrow and the number 1 pointing to it.

Target Modules: This section shows a list of modules with tabs for 'Explore', 'Cmd', 'Stealer', 'Screen Shot', 'Key Logger', and 'History'. Below the tabs is a file explorer view showing a directory structure: 'Disk / Z: / shared / test'. A search bar is present.

- Callout 2 points to the 'Interval' dropdown menu.
- Callout 3 points to the 'Auto Run' dropdown menu.
- Callout 4 points to the 'KILL R.A.T.' button.
- Callout 5 points to the 'Ask Current Info' button.
- Callout 6 points to the 'Update R.A.T.' button.
- Callout 7 points to the 'reScan Folder' button.
- Callout 8 points to the 'reScan Disk' button.
- Callout 9 points to the 'Download' icon in the file list.
- Callout 10 points to the 'Upload' icon in the file list.
- Callout 11 points to the 'Delete' icon in the file list.

The file list at the bottom shows four items:

#	Path	Size
1	2	
2	٦١٦٥	
3	Antivirus Lab.txt	
4	C:\p_480_5sec_6mops_n234.mp4	3771577 Bytes

تصویر ۳ - پنل راهبری بدافزار تاقب



ت) File Explorer

با استفاده از قابلیت فایل اکسپلورر بدافزار ثاقب ، امکان مدیریت ، حذف و یا ایجاد تغییر در فایل های رایانه هدف با دسترسی بالا امکانپذیر می باشد. گزینه های موجود در این بخش به شرح ذیل می باشند. (تصویر ۳)

۷. Rescan Disk

به محض اجرای بدافزار ثاقب بر روی سیستم هدف ، لیست کلیه فایل های موجود بر روی آن به پنل کاربری و فرمان بدافزار ارسال می گردد. با کلیک دوباره بر روی این گزینه ، فرآیند تکرار می گردد.

۸. Rescan Folder

جهت بروزرسانی لیست فایل های موجود در یک دایرکتوری خاص به همراه تمامی زیر شاخه های آن از این گزینه استفاده می گردد.

۹. Upload

جهت آپلود فایل بر روی سیستم هدف ، از این گزینه استفاده می گردد. پس از انتخاب این گزینه ، صفحه انتخاب فایل مورد نظر باز شده و امکان انتخاب و ارسال فایل بر روی سیستم هدف را فراهم می سازد. لازم به ذکر است با توجه به این که بدافزار با میزان دسترسی کاربر رایانه اجرا می شود، آپلود فایل تنها روی مسیرهایی امکان پذیر خواهد بود که بدافزار مجوز دسترسی بر روی آن را داشته باشد.

۱۰. Encrypt Files

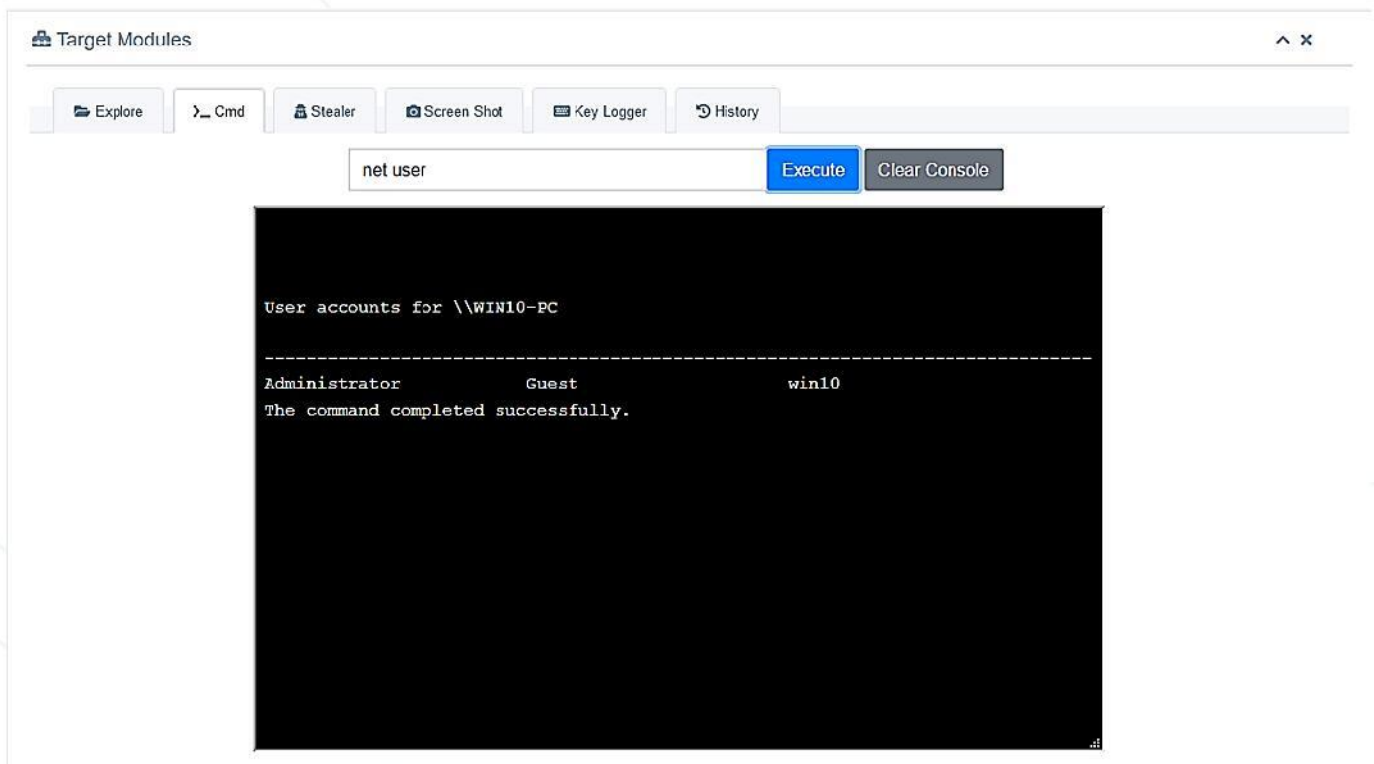
با استفاده از این قابلیت فایل های موجود بر روی یک دایرکتوری خاص بصورت یک طرفه رمز شده و پس از رمز نگاری ، امکان رمز گشایی آن وجود نخواهد داشت و فایل مورد نظر قابل استفاده نخواهد بود. این عملکرد نیز همانند Upload File تابع میزان دسترسی بدافزار به سیستم هدف است.



جهت دانلود فایل از روی سیستم هدف ، بر روی فایل مورد نظر کلیک کرده تا به حالت انتخاب درآید. سپس با کلیک بر روی آیکن دانلود ، فرآیند انتقال فایل از سیستم کلاینت به سرور آغاز می گردد. پس از اتمام دانلود، پیغام اتمام آن برای کاربر نمایش داده خواهد شد.

ث) Command Execute

برای اجرای دستورات تحت خط فرمان ویندوز (Cmd) مطابق تصویر ۴ ، کاربر دستور مورد نظر را در باکس مربوطه وارد و با کلیک بر روی دکمه Execute ، دستور مورد نظر توسط بدافزار اجرا شده و پس از گذشت چند ثانیه که حداکثر برابر با زمان Interval است ، نتیجه اجرای دستور در صفحه کنسول پایینی نمایش داده خواهد شد.

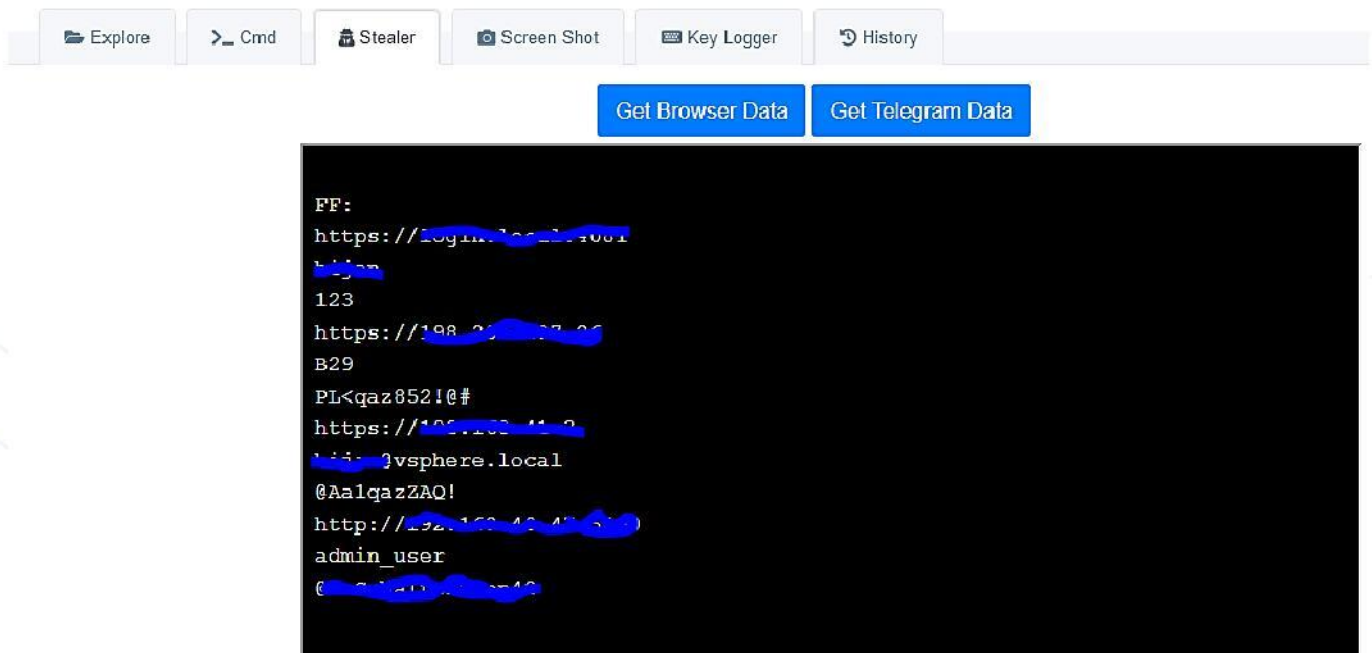


تصویر ۴ - بخش ارسال دستورات (Cmd) در پنل راهبری بدافزار تاقب



قابلیت Stealer شامل دو بخش Telegram و مرورگر فایرفاکس است. با کلیک بر روی دکمه Get Telegram Data چنانچه نرم افزار تلگرام دسکتاپ روی سیستم کلاینت نصب باشد، بدافزار اقدام به جستجوی فایل‌های ضروری این نرم افزار روی سیستم هدف کرده و پس از بسته‌بندی این فایل‌ها، آن‌ها را به سمت سرور ارسال می‌نماید. پس از دریافت فایل‌های تلگرامی، جایگزین کردن آن با فایل‌های نظیرشان در یک سیستم دیگر که نرم افزار تلگرام دسکتاپ روی آن نصب است، امکان دسترسی به تلگرام هدف را میسر خواهد نمود.

مطابق تصویر ۵ با کلیک بر روی دکمه Get Browser Data تمامی اطلاعات کاربری ذخیره شده در مرورگر فایرفاکس سیستم هدف توسط بدافزار به پنل راهبری ارسال می‌گردد. با توجه به ذخیره اطلاعات صفحات بازدید شده و نام‌های کاربری و پسورد ورود به سیستم‌های مختلف عمومی و سازمانی مانند مشخصات دسترسی به حساب‌های اجتماعی و ایمیل، دسترسی به اطلاعات مرورگر حائز اهمیت می‌باشد.

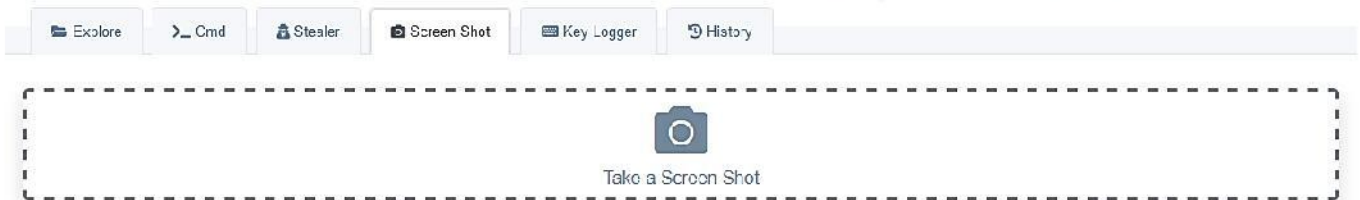


تصویر ۵ - صفحه Stealer در پنل راهبری بدافزار تاقب



Screen Shot (ج)

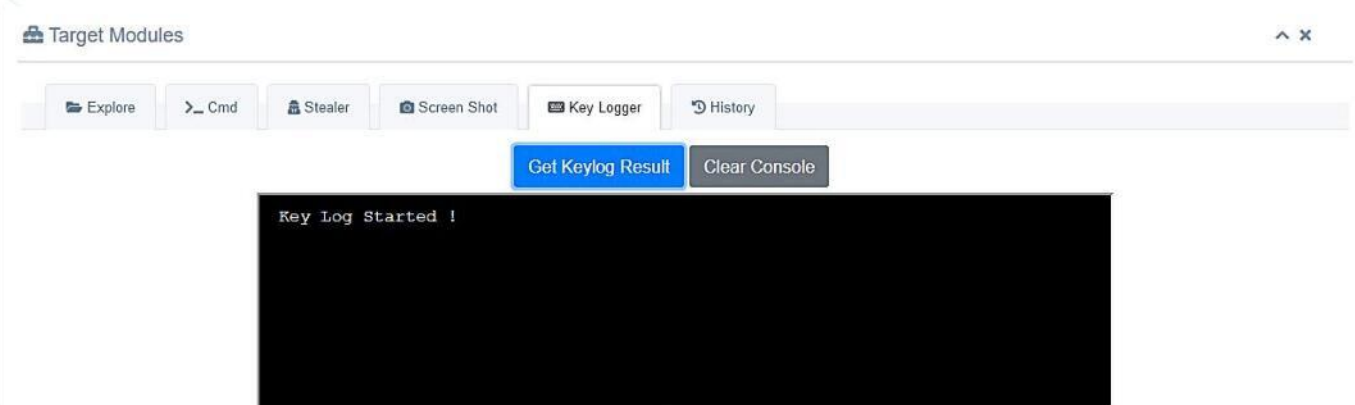
کاربر جهت دریافت تصویر از صفحه نمایش سیستم هدف ، میتواند از گزینه Take a Screen Shot مطابق تصویر ۶ استفاده نماید. تصویر دسکتاپ سیستم هدف پس از چند ثانیه در پایین این صفحه نمایش داده خواهد شد.



تصویر ۶ - صفحه Screen Shot در پنل راهبری بدافزار تاقب

Key Logger (ح)

مطابق تصویر ۷ قابلیت Keylog این امکان را در اختیار کاربر قرار می دهد که گزارش کلیدهای فشرده شده توسط کلاینت را در صورت وجود دریافت نماید. بدین منظور لازم است ابتدا با کلیک روی دکمه Start Keylog ، فرآیند مذکور راه اندازی شده و چنانچه موفقیت آمیز باشد پیغام Key log started! به نمایش درخواهد آمد. از این زمان به بعد کلیه کلیدهای فشرده شده توسط کلاینت ضبط خواهند شد. همچنین متن دکمه Start Keylog به Get Keylog Result تغییر می یابد و گزارش کلیدهای فشرده شده با کلیک بر روی این دکمه دریافت خواهد شد. این گزارش شامل نام پنجره در حال استفاده توسط سیستم هدف و کلید های فشرده شده در آن می باشد.



تصویر ۷ - صفحه Key Logger در پنل راهبری بدافزار تاقب



در این بخش کاربر میتواند به تاریخچه دستوراتی که اجرا شده‌اند دسترسی یابد. برای مشاهده نتیجه اجرای دستوری که در گذشته اجرا شده است، کفایت مطابق تصویر ۸ روی دکمه Result کلیک نموده تا نتیجه اجرای دستور مورد نظر در بخش مربوط به آن دستور نمایش داده شود.

Target Modules

Explore
Cmd
Stealer
Screen Shot
Key Logger
History

Log Start Date: dd-mm-yyyy
Log End Date: dd-mm-yyyy
Task Type: Any
Task Status: Any
Filter

Show 50 entries
Search:

i	task ID	Client	Task Type	Status	Inserted at:	Received at:	Completed at:	Result
1	30	F37C20CF5B6F	Browser Stealer	Success. Run	2020-12-26 15:54:33	2020-12-26 15:54:36	2020-12-26 15:54:37	Result
2	31	F37C20CE5B6F	Browser Stealer	Success. Run	2020-12-26 16:07:15	2020-12-26 16:07:56	2020-12-26 16:07:57	Result
3	32	F37C20CE5D6F	Telegram Stealer	Success. Run	2020-12-26 16:08:22	2020-12-26 16:08:41	2020-12-26 16:09:20	Result

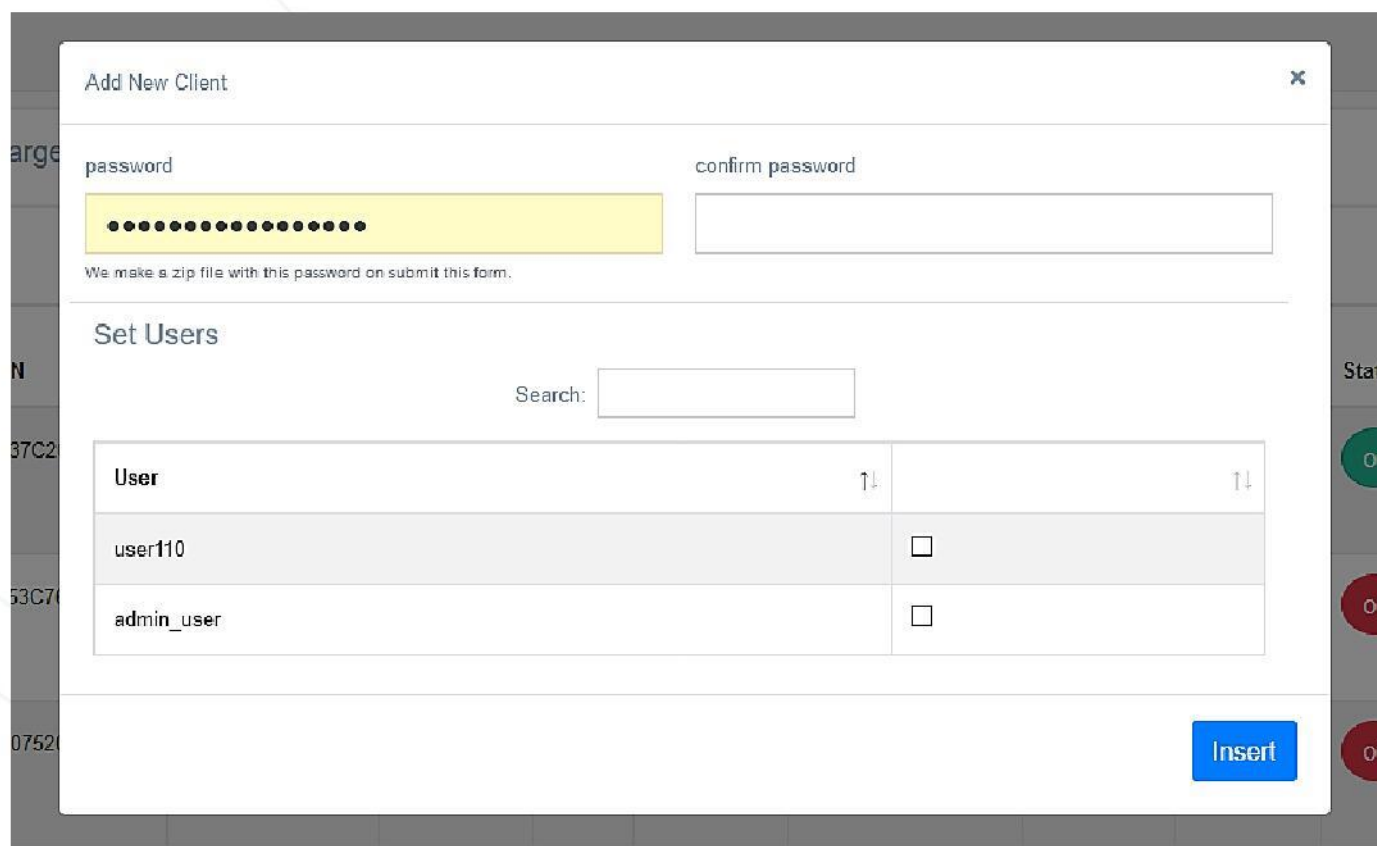
Showing 1 to 3 of 3 entries
Previous
Next

تصویر ۸ - صفحه History در پنل راهبری بدافزار تاقب



د) پنجره ساخت بدافزار (ایجنت) جدید

مطابق تصویر ۲ پس از کلیک بر روی دکمه Add New Client نسخه ای از بدافزار ایجاد خواهد شد. بدافزار بصورت فشرده شده در یک فایل ZIP و رمزنگاری شده در دسترس خواهد بود تا امکان آشکار شدن آن بر روی سیستم کاربر به دلیل اتصال به اینترنت و استفاده از نرم افزارهای امنیتی وجود نداشته باشد. مطابق تصویر ۹ کاربر می‌بایست رمزی دلخواه را که حداقل طول آن ۸ کاراکتر است انتخاب نماید. با کلیک بر روی دکمه Insert بدافزار ساخته شده و پنجره دانلود برای کاربر به نمایش درخواهد آمد. همچنین امکان انتخاب کاربرانی که مجاز به استفاده از بدافزار تولید شده می باشند در بخش پایین همین فرم وجود دارد.



The screenshot shows a web application window titled "Add New Client". It contains two input fields for "password" and "confirm password". Below the password fields, a note states: "We make a zip file with this password on submit this form." Below this, there is a section titled "Set Users" with a "Search:" input field. A table lists two users: "user110" and "admin_user", each with a checkbox for selection. An "Insert" button is located at the bottom right of the form.

User	
user110	<input type="checkbox"/>
admin_user	<input type="checkbox"/>

تصویر ۹ - صفحه ساخت نسخه ای از بدافزار در پنل راهبری بدافزار تاقب



مطابق تصویر ۱۰، کاربر با دسترسی مدیر با استفاده از گزینه Add New User و انتخاب نام کاربری و رمز مناسب، میتواند اقدام به ساخت کاربر جدید نماید.

List Of Targets

Add New User ^ x

Search:

i	SN	Creation	Last Login	Edit
1	user_110	2020-12-23 15:33:57		Users
2	admin_user	2020-12-24 10:33:12		Users

تصویر ۱۰ - صفحه مدیریت و ایجاد کاربران سامانه تاقب



