گزارش تحلیلی تروجان Parallax

مقدمه

یک تروجان با دسترسی از راه دور (RAT) به نام Parallax به طور گسترده در حال توزیع از طریق کمپین‌های مخرب اسپم می‌باشد. هنگامی که یک سیستم ویندوزی به این تروجان آلوده شود مهاجم می‌تواند کنترل کامل آن سیستم را در دست بگیرد.

مهاجم از این بدافزار برای دسترسی به سیستم قربانی استفاده می‌کند تا به نام کاربری و رمزهای عبور ذخیره شده در سیستم دسترسی پیدا کند و همچنین بتواند دستورات دلخواه خود را اجرا کند سپس از این اطلاعاتی که جمع‌آوری کرده است می‌تواند برای سرقت هویت قربانی، دسترسی به حساب‌های بانکی و توزیع بیشتر این تروجان استفاده کند.

یک محقق امنیتی MalwareHunterTeam از دسامبر سال ۲۰۱۹ نمونه‌هایی از تروجان Parallax را ردیابی کرده است.

ویژگی‌های بدافزار

این بدافزار می‌تواند فایل‌های مورد نظر خود را از سیستم آلوده دانلود کند و همچنین نام کاربری و رمزهای عبور ذخیره شده در مرورگرهای Firefox, Google Chrome, Thunderbird و Outlook را به سرقت ببرد.

یکی از کارهای مخربی که مهاجم با استفاده از این بدافزار می‌تواند انجام دهند این است که دستورات مخرب را از راه دور در سیستم قربانی اجرا کند از جمله خاموش کردن سیستم آلوده از راه دور و غیرفعال کردن آنتی‌ویروس و سایر نرم‌افزارهای امنیتی نصب شده در سیستم آلوده.

یکی دیگر از ویژگی‌های این بدافزار، keystroke logging می‌باشد. مهاجم با استفاده از این ویژگی می‌تواند هر کلیدی بر روی صفحه کلید که توسط قربانی فشرده می‌شود را ذخیره کند و اطلاعات مهم و حساس مانند نام کاربری و رمز عبور حساب‌های مختلف قربانی مانند اطلاعات حساب‌های بانکی را به سرقت ببرد. (قابلیت keylogger)

بنابراین با این توانایی‌هایی که برای این بدافزار نام برده شد مهاجم می‌تواند بدافزارهای دیگری را در سیستمی که به Parallax آلوده شده نصب کند به عبارت دیگر هر فعالیتی که قربانی در سیستم خود انجام دهد مهاجم قادر به دیدن آن است!

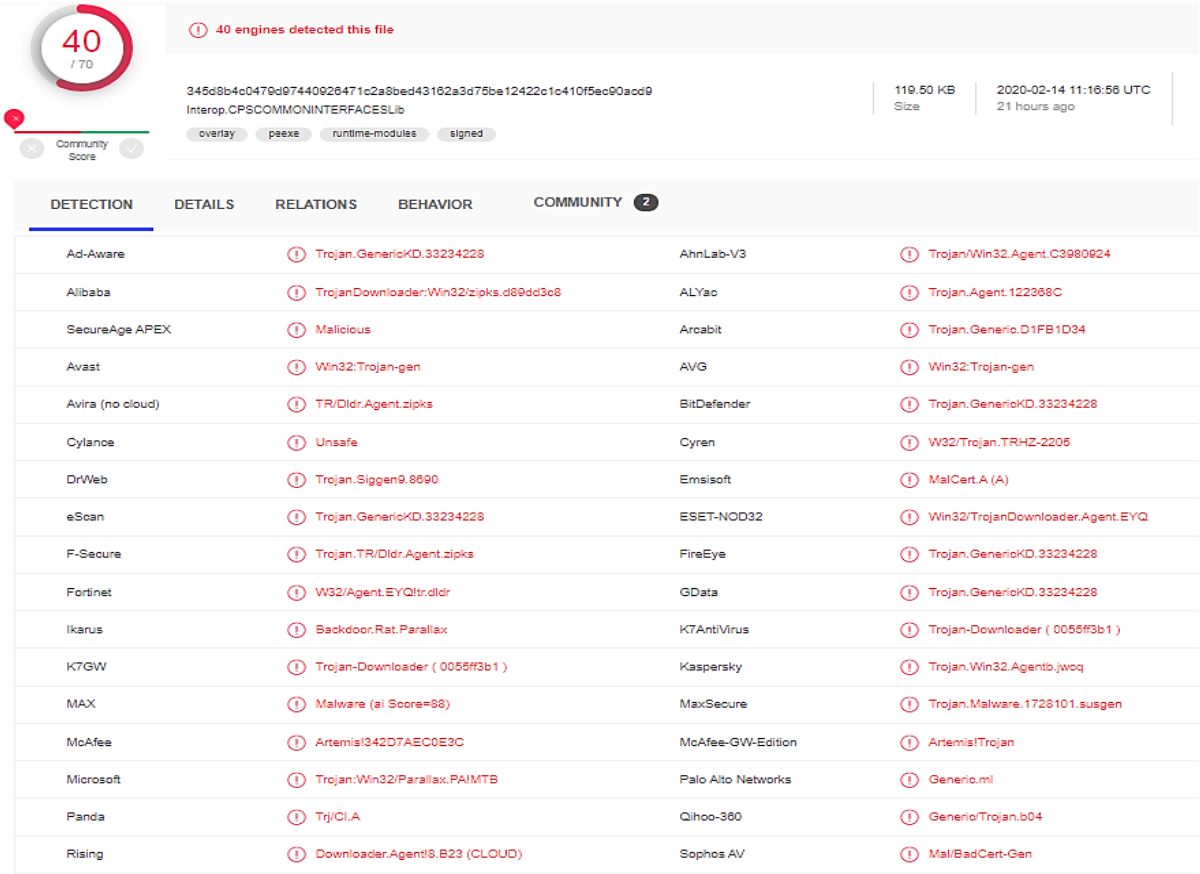
مشخصات بدافزار

در جدول زیر مشخصات کامل بدافزار Parallax را مشاهده می‌کنید.

جدول شماره ۱: مشخصات بدافزار

نام بدافزار	Parallax remote access trojan
نوع بدافزار	Trojan, password-stealing virus, banking malware, spyware
شناسایی توسط آنتی‌ویروس	Avast, BitDefender, ESET-NOD32, Kaspersky,…
Payload	بدافزارها از نوع RAT می توانند به عنوان ابزاری برای آلوده کردن سیستم با انواع برنامه های مخرب استفاده شوند.
علائم آلودگی	این بدافزار بعد از آلوده کردن سیستم هیچ علائمی از خود نشان نمی دهد.
نحوه انتشار	ضمیمه آلوده ایمیل، تبلیغات های مخرب، نرم افزارهای crack و مهندسی اجتماعی
میزان تخریب	سرقت رمزهای عبور و اطلاعات بانکی و اضافه کردن سیستم به botnet

شکل زیر نتیجه اسکن فایل آلوده به بدافزار Parallax را توسط VirusTotal نشان می‌دهد که ۴۰ آنتی‌ویروس آن را تشخیص داده است.

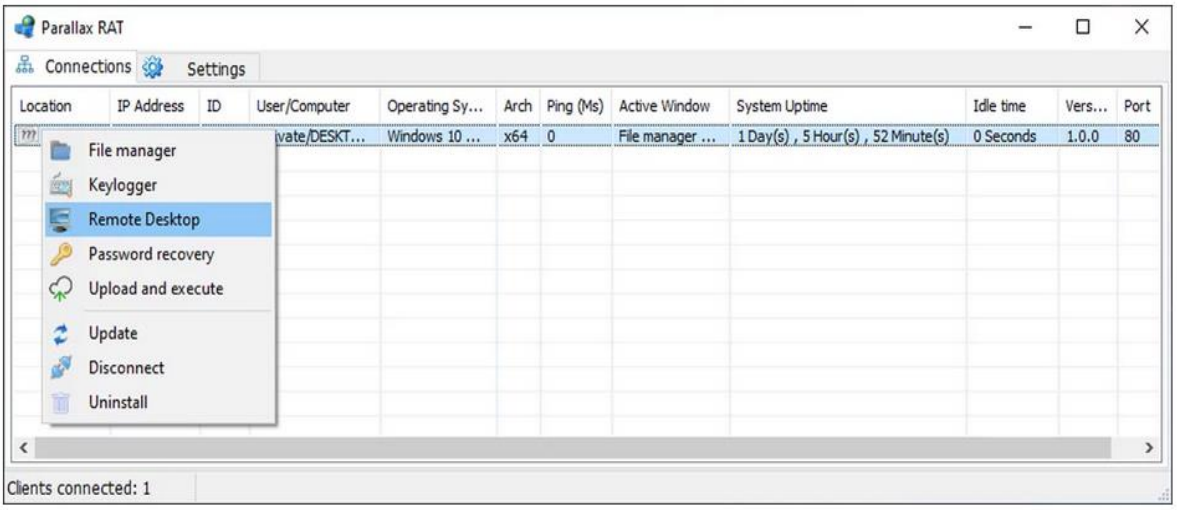


شکل ۱: اسکن فایل آلوده توسط VirusTotal

این بدافزار از دسامبر ۲۰۱۹ در فروم‌های هکرها به فروش می‌رسد و سایر مهاجمان می‌توانند license آن را برای مدت یک ماهه به قیمت ۶۵ دلار و برای مدت سه ماهه به قیمت ۱۷۵ دلار خریداری کنند. با خرید license این بدافزار ویژگی‌های زیر را خواهد داشت:

- سرقت اطلاعات login
- برقراری ارتباط با سیستم قربانی از طریق Remote Desktop
- آپلود و دانلود فایل
- اجرای دستورات از راه دور در سیستم آلوده
- ارتباط رمزنگاری شده با سیستم آلوده
- پشتیبانی از ویندوز XP از طریق ویندوز ۱۰

به عنوان مثال در شکل زیر مشاهده می‌کنید که مهاجم با استفاده از بدافزار Parallax توانسته است ارتباط Remote Desktop را با سیستم قربانی برقرار کند.



شکل ۲: ارتباط Remote Desktop

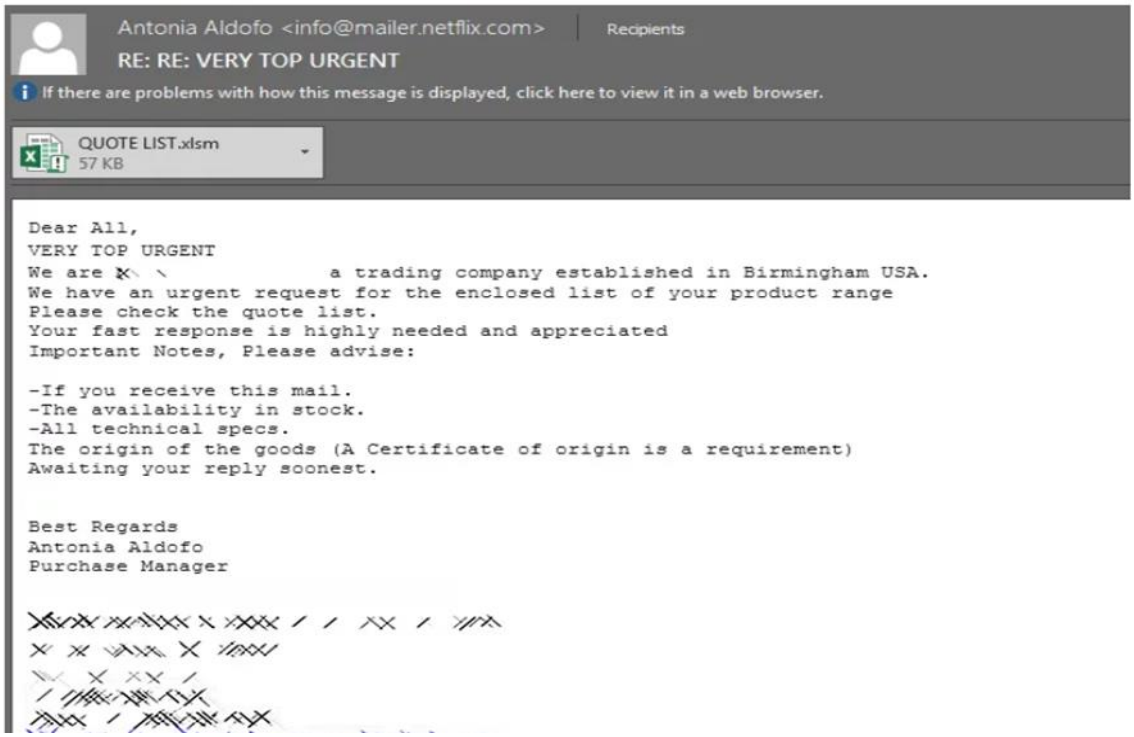
نحوه آلودگی سیستم توسط بدافزار

این بدافزار بیشتر از طریق موارد زیر باعث آلوده شدن سیستم‌ها می‌شود:

- ایمیل‌های spam
- تروجان
- کانال‌های غیر قابل اعتماد دانلود نرم‌افزار
- به روز رسانی‌های جعلی نرم‌افزارها
- ابزارهای crack نرم‌افزار

مهاجمان اغلب برای انتشار این بدافزار و آلوده کردن سیستم‌ها ایمیل‌هایی را که حاوی یک فایل ضمیمه آلوده به Parallax است برای قربانیان ارسال می‌کنند. این فایل‌های آلوده شامل اسناد مخرب office، فایل‌های Java Script، فایل‌های PDF، فایل‌های اجرایی مانند exe. و فایل‌های فشرده با پسوند zip. و rar. .

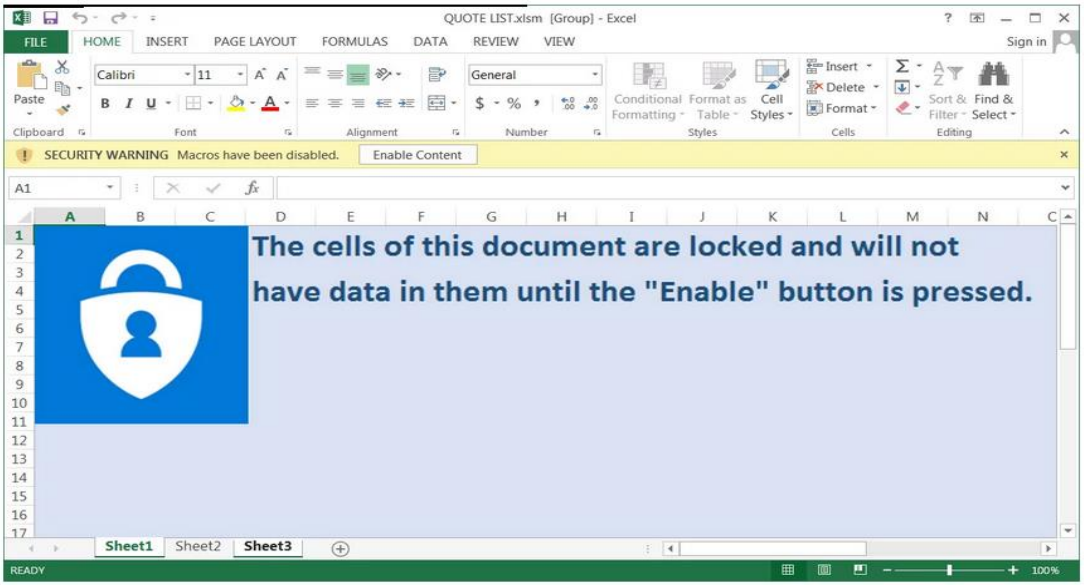
شکل زیر یک نمونه از ایمیلی را نشان می‌دهد که حاوی فایل آلوده به بدافزار Parallax است.



شکل ۳: نمونه‌ای از ایمیل حاوی فایل آلوده به Parallax

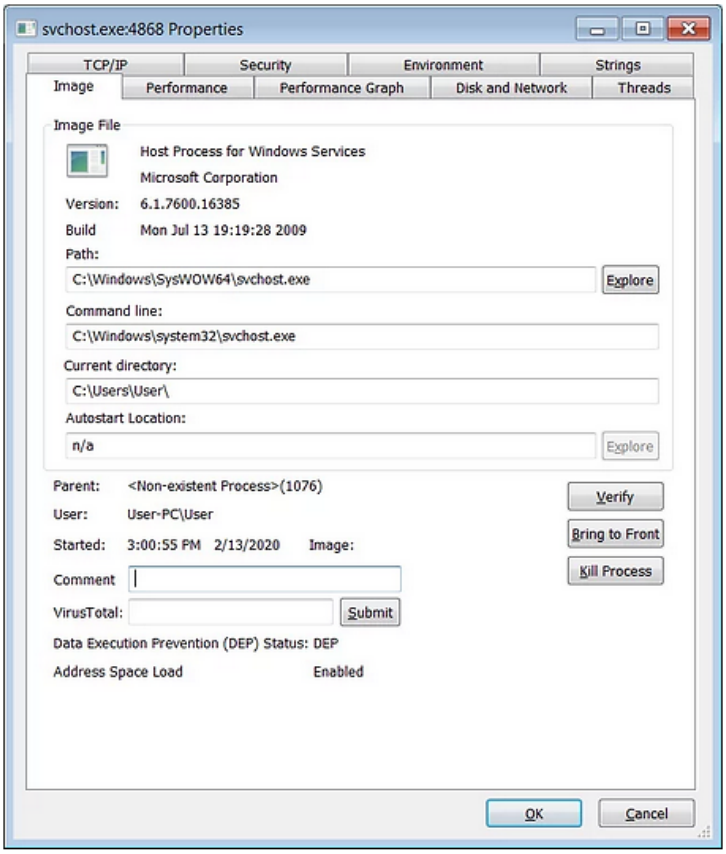
هنگامی که قربانی این ایمیل را دریافت کرد با توجه به محتوای آن ترغیب می‌شود تا فایل ضمیمه را باز کند. با باز کردن فایل و یا کلیک بر روی لینک آن فایل و یا نرم‌افزاری که از طریق این لینک نصب کرده است به بدافزار Parallax آلوده می‌شود. بدافزار Parallax این قابلیت را دارد تا مهاجم با استفاده از آن سایر بدافزارهای مورد نیاز خود را نیز در سیستم آلوده نصب کند و همچنین بتواند از آسیب‌پذیری‌های موجود در سیستم بهره‌برداری کند.

شکل زیر یک نمونه از فایل Excel آلوده را نشان می‌دهد.



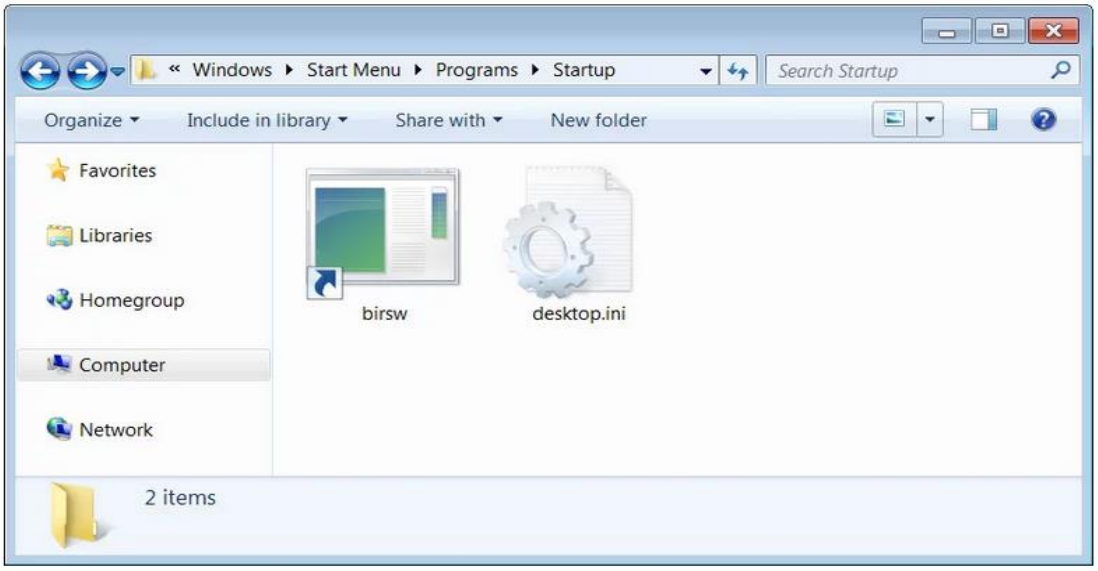
شکل ۴: نمونه‌ای از فایل آلوده Excel

علاوه بر روش آلوده شدن سیستم از طریق ایمیل، یک محقق، بدافزار Parallax را به فرآیند svchost.exe تزریق کرده است تا از این طریق سیستم را آلوده کند. شکل زیر فرآیند svchost.exe آلوده به بدافزار را نشان می‌دهد.



شکل ۵: تزریق بدافزار Parallax به فرآیند svchost.exe

هنگامی که این بدافزار در سیستم نصب شد یک shortcut از launcher این بدافزار در پوشه startup ویندوز (مطابق شکل زیر) قرار می‌گیرد تا با هر بار راه اندازی سیستم توسط قربانی به صورت خودکار شروع به کار کند. همین امر موجب می شود تا دسترسی مهاجم به سیستم قربانی پایدار بماند و بتواند سیستم را از راه دور کنترل کند.



شکل ۶: وجود فایل بدافزار در پوشه startup ویندوز

راه‌کارهای جلوگیری از آلوده شدن سیستم به بدافزار

برای جلوگیری از آلوده شدن سیستم به این بدافزار باید موارد امنیتی زیر رعایت شود:

- ضمیمه ایمیل‌های ناشناس را باز نکنید.
- اگر ایمیلی از طرف فردی آشنا برای شما ارسال شده ابتدا با آن فرد تماس بگیرد تا از صحت ارسال ایمیل از سمت او مطمئن شوید.
- اگر ایمیل حاوی لینک بود قبل از کلیک بر روی آن ابتدا آن لینک را در سایت VirusTotal اسکن کنید.
- نرم‌افزارهای مورد نیاز خود را فقط از سایت‌های معتبر دانلود کنید.
- سیستم‌عامل و نرم‌افزارهای سیستم خود را به روز نگه دارید و فایل‌های به روز رسانی را از سایت معتبر آن نرم‌افزار دانلود کنید.
- نرم‌افزارهای anti-Virus و anti-Malware را در سیستم خود نصب کنید و همیشه آن‌ها را به روز رسانی کنید.
- از فایل‌های مهم خود backup بگیرید و در جایی غیر از سیستم خود ذخیره کنید.

منابع

- https://www.bleepingcomputer.com/news/security/parallax-rat-common-malware-payload-after-hacker-forums-promotion/
- https://www.pcrisk.com/removal-guides/17041-parallax-rat