



گزارش تحلیلی تروجان Parallax

 <p>وزارت ارتباطات و فناوری اطلاعات سازمان فناوری اطلاعات ایران</p>	تحلیل تروجان Parallax		 <p>مرکز مالهانتر</p>
	تاریخ تدوین گزارش: بهمن ماه ۱۳۹۸	طبقه بندی سند: عادی	

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!

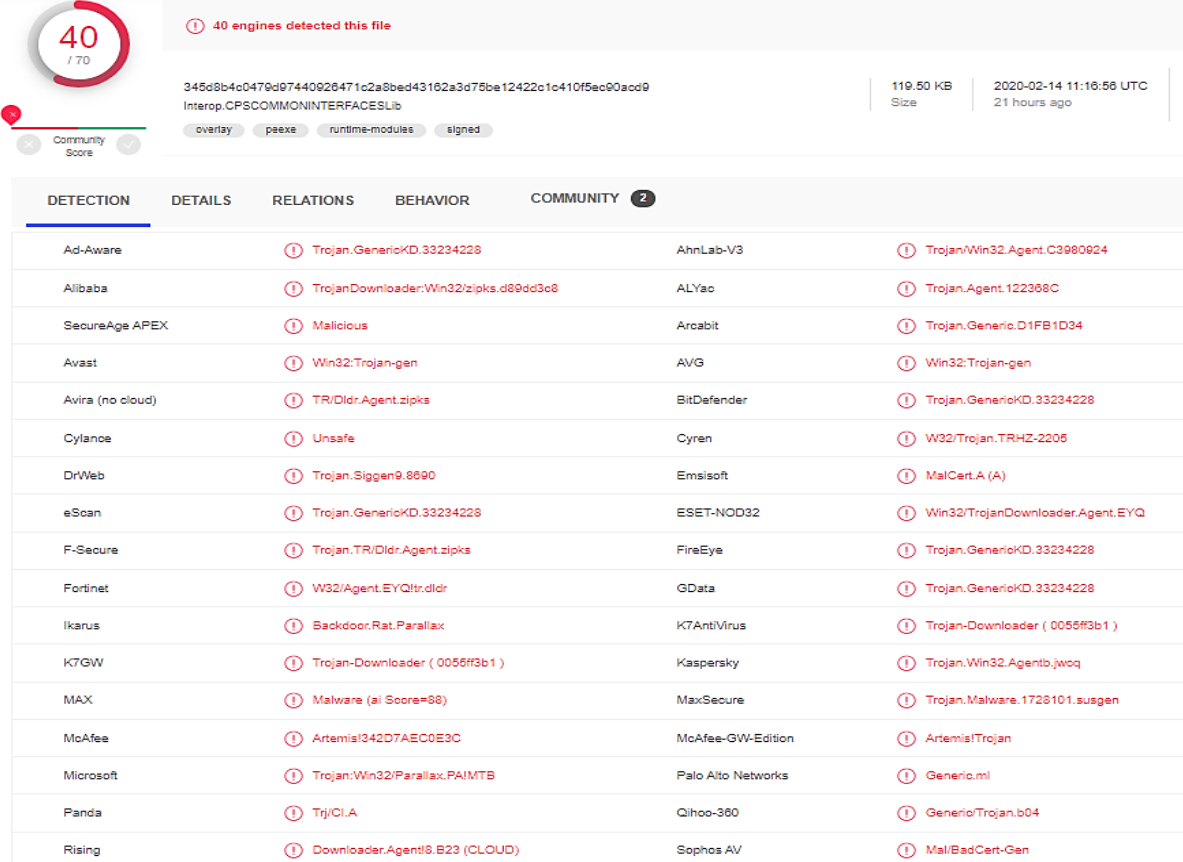
مشخصات بدافزار

در جدول زیر مشخصات کامل بدافزار Parallax را مشاهده می کنید.

جدول شماره ۱: مشخصات بدافزار

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

شکل زیر نتیجه اسکن فایل آلوده به بدافزار Parallax را توسط VirusTotal نشان می دهد که ۴۰ آنتی ویروس آن را تشخیص داده است.



40 / 70

40 engines detected this file

345d8b4c0479d97440926471c2a8bed43162a3d75be12422c1c410f5e090acd9
Interop.CPSCOMMONINTERFACESLib

119.50 KB Size | 2020-02-14 11:16:56 UTC 21 hours ago

Community Score

overlay ps.exe runtime-modules signed

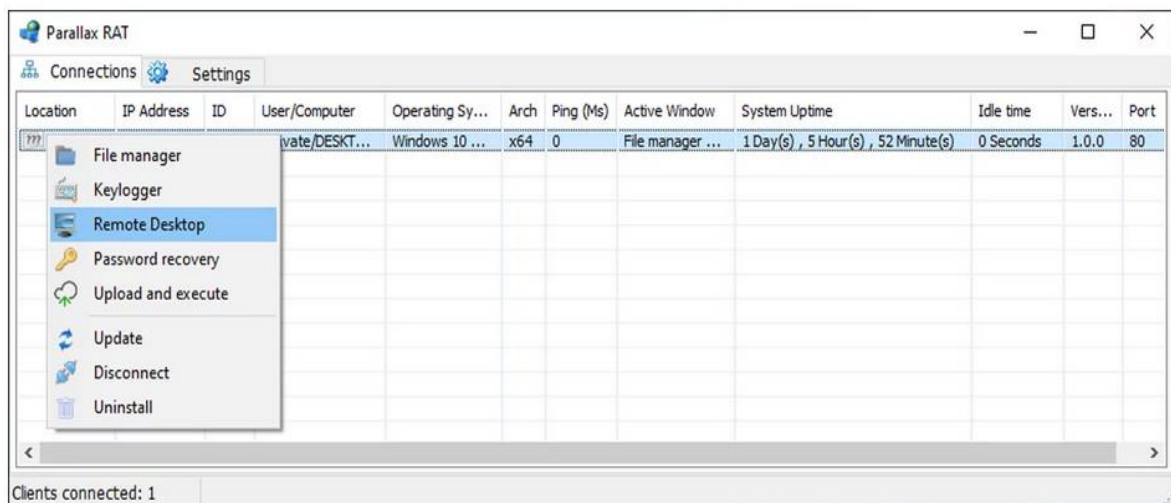
DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Ad-Aware		Trojan.GenericKD.33234228	AhnLab-V3	Trojan/Win32.Agent.C3980624
Alibaba		Trojan/Downloader.Win32/zipks.d89dd3c8	ALYac	Trojan.Agent.122368C
SecureAge APEX		Malicious	Arcabit	Trojan.Generic.D1FB1D34
Avast		Win32:Trojan-gen	AVG	Win32:Trojan-gen
Avira (no cloud)		TR/Dldr.Agent.zipks	BitDefender	Trojan.GenericKD.33234228
Cylance		Unsafe	Cyren	W32/Trojan.TRHZ-2205
DrWeb		Trojan.Siggen9.8690	Emsisoft	MalCert.A.(A)
eScan		Trojan.GenericKD.33234228	ESET-NOD32	Win32/Trojan/Downloader.Agent.EYQ
F-Secure		Trojan.TR/Dldr.Agent.zipks	FireEye	Trojan.GenericKD.33234228
Fortinet		W32/Agent.EYQlfr.dldr	GData	Trojan.GenericKD.33234228
Ikarus		Backdoor.Rat.Parallax	K7AntiVirus	Trojan-Downloader (0055ff3b1)
K7GW		Trojan-Downloader (0055ff3b1)	Kaspersky	Trojan.Win32.Agentb.jwoq
MAX		Malware (ai Score=88)	MaxSecure	Trojan.Malware.1728101.susgen
McAfee		Artemis!342D7AEC0E3C	McAfee-GW-Edition	Artemis!Trojan
Microsoft		Trojan:Win32/Parallax.PA!MTB	Palo Alto Networks	Generic.ml
Panda		Trj/CI.A	Qihoo-360	GenericTrojan.b04
Rising		Downloader.Agent!8.B23 (CLOUD)	Sophos AV	MaliBadCert-Gen

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 این license 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

 <p>وزارت ارتباطات و فناوری اطلاعات سازمان فناوری اطلاعات ایران</p>	تحلیل تروجان Parallax		 <p>مرکز ملی امنیت سایبری</p>
	تاریخ تدوین گزارش: بهمن ماه ۱۳۹۸	طبقه بندی سند: عادی	

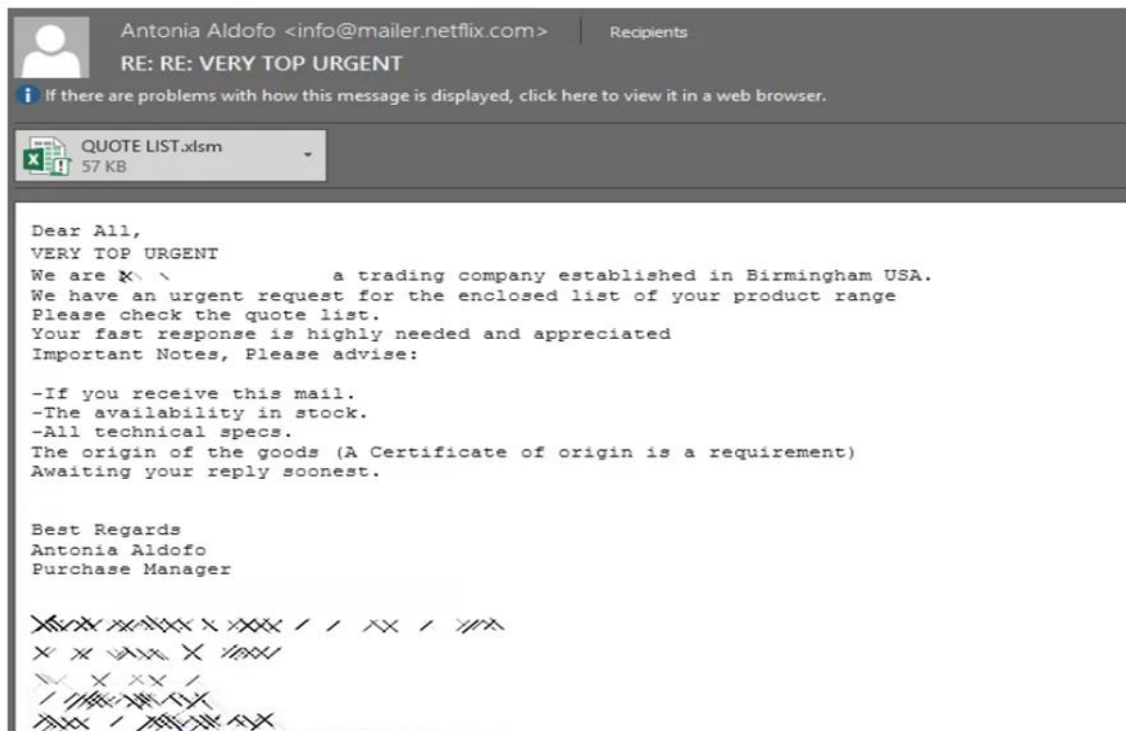
نحوه آلودگی سیستم توسط بدافزار

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 .

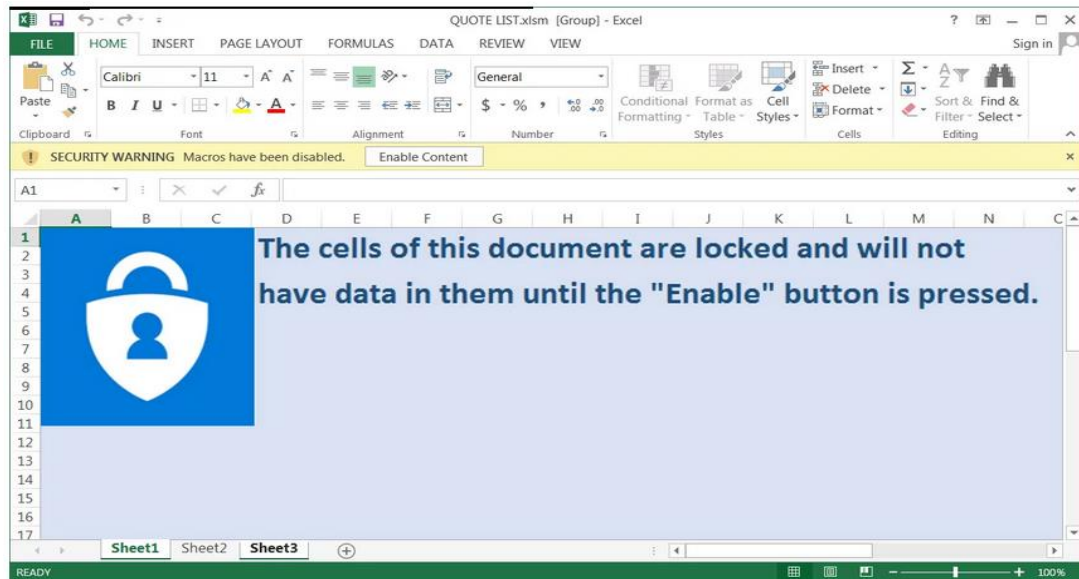
شکل زیر یک نمونه از ایمیلی را نشان می‌دهد که حاوی فایل آلوده به بدافزار Parallax است.



شکل ۳: نمونه‌ای از ایمیل حاوی فایل آلوده به Parallax

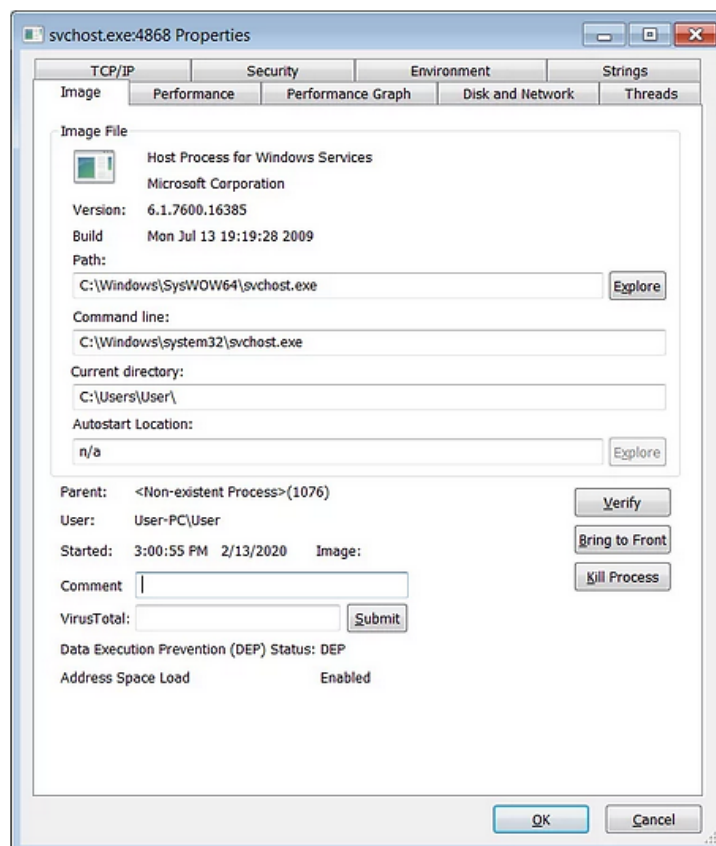
هنگامی که قربانی این ایمیل را دریافت کرد با توجه به محتوای آن ترغیب می‌شود تا فایل ضمیمه را باز کند. با باز کردن فایل و یا کلیک بر روی لینک آن فایل و یا نرم‌افزاری که از طریق این لینک نصب کرده است به بدافزار Parallax آلوده می‌شود. بدافزار Parallax این قابلیت را دارد تا مهاجم با استفاده از آن سایر بدافزارهای 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

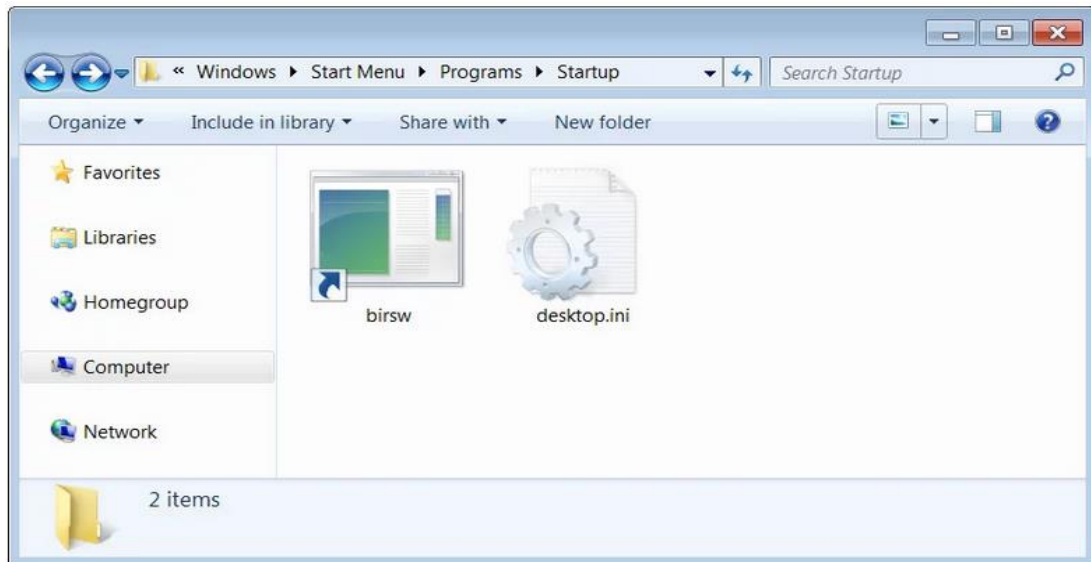
علاوه بر روش آلوده شدن سیستم از طریق ایمیل، یک محقق، بدافزار Parallax را به فرآیند svchost.exe تزریق کرده است تا از این طریق سیستم را آلوده کند. شکل زیر فرآیند svchost.exe آلوده به بدافزار را نشان می‌دهد.



شکل ۵: تزریق بدافزار Parallax به فرآیند svchost.exe

 وزارت ارتباطات و فناوری اطلاعات سازمان فناوری اطلاعات ایران	تحلیل تروجان Parallax		 مرکز ملی امنیت سایبری
	تاریخ تدوین گزارش: بهمن ماه ۱۳۹۸	طبقه بندی سند : عادی	

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 می‌شود 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

 <p>وزارت ارتباطات و فناوری اطلاعات سازمان فناوری اطلاعات ایران</p>	تحلیل تروجان Parallax		 <p>مرکز سایبر</p>
	تاریخ تدوین گزارش: بهمن ماه ۱۳۹۸	طبقه بندی سند : عادی	

راه کارهای جلوگیری از آلوده شدن سیستم به بدافزار

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

- ضمیمه ایمیل های ناشناس را باز نکنید.
- اگر ایمیلی از طرف فردی آشنا برای شما ارسال شده ابتدا با آن فرد تماس بگیرید 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.
- نرم افزارهای مورد نیاز خود را فقط از سایت های معتبر دانلود کنید.
- سیستم عامل و نرم افزارهای سیستم خود را به روز نگه دارید و فایل های به روز رسانی را از سایت معتبر آن نرم افزار دانلود کنید.
- نرم افزارهای anti-Virus و anti-Malware را در سیستم خود نصب کنید و همیشه آن ها را به روز رسانی کنید.
- از فایل های 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>