بسمه تعالی

تهدیدات امنیتی تروجان ها

Security Threats Trojans

فهرست مطالب

مقدمه

همانطور که می دانیم باجافزارها، سخت‌افزار و سیستم عامل، تهدیدات ابری، اینترنت اشیا و تهدیدات دیجیتالی از بیشترین تهدیدات امنیتی سال ۲۰۱۷ اعلام شده و آگاهی از مسائل امنیتی به قدرتمندتر شدن محصولات در برابر تهدیدات کمک خواهد کرد.

ویروس ها، تروجان ها و ... نیز روز به روز بر قدرت خود افزوده و با پیشرفت سیستم های حفاظتی و امنیتی برای نرم افزارها خود را به روز رسانی نموده اند. همانند ویروس های انسانی، ویروس های کامپیوتری نیز در انواع مختلفی وجود دارند و می توانند دستگاه های شما را از طریق راه های گوناگونی تحت تاثیر قرار دهند.

به صورت کاملا واضحی، کامپیوتر شما نیاز به بستری شدن به مدت یک هفته در تخت خواب و یا آنتی بیوتیک ندارد. اما با آلوده کردن کامپیوتر شما می توانند انتقام ویران کننده ای از شما و سیستم شما بگیرند. آنها می توانند فایل هایتان را حذف کنند، داده های شما را بدزدند، و به راحتی آنها را در اختیار دیگر دستگاه ها قرار دهند.

بنابراین نیاز هست که تهدیدهای امنیتی که روزانه منتشر می شود، کشف شده و اطلاع رسانی گردد تا در همان ابتدای راه، پیشگیری لازم انجام گیرد.

لذا در این گزارشات ما به بررسی تهدید های امنیتی روز می پردازیم در ابتدا جدولی از مشخصات تهدید ها شامل نام تهدید، نوع تهدید، تاریخ انتشار ، شدت و ... به طور کلی آورده شده است. در ادامه به جزئیات هر کدام و باید و نباید های آنها می پردازیم.

لازم به ذکر است که توصیه ها و پیشگیری های لازم برای هر کدام ارائه گردیده است که با توجه به کارکرد مشابه تروجان ها و ... این موارد ممکن است با هم، هم پوشانی داشته باشند.

تروجان چیست؟

لغت تروجان از یک داستان در یونان باستان گرفته شده است که معروف به جنگ تروی بوده در این جتگ دشمنان یک اسب بزرگ چوبی درست کرده و برای پیشکش به دشمنانشان هدیه دادند و در این اسب پر از سرباز جای گرفته بود و شب هنگام سربازها بیرون زده و در دروازه را باز کردند و به داخل قلعه نفوذ کرده و در جنگ پیروز شدند.

حال درست مثل یک اسب تروجان، آنها تا زمانی که قادر به دسترسی به کامپیوتر شما نیستند، مانند برنامه های بی ضرر هستند. تروجان ها یکی از خطرناک ترین انواع نرم افزارهای مخرب هستند، زیرا هکرها دسترسی به دستگاه و اطلاعات شخصی شما دارند.

تروجان ها بسیار پیچیده تر از یک ویروس متوسط هستند، بنابراین آنها سابقه طولانی مانند ویروس ندارند. تروجان ها بیشتر به عنوان نرم افزار معمولی در سیستم آسیب دیده قرار می گیرند و به اینترنت دسترسی پیدا می کنند، زیرا آنها نیاز به اتصال به شبکه برای ارسال فایل ها به هکر یا اجازه کنترل از راه دور کامپیوتر تخریب شده به هکر را دارند.

دو تروجان برجسته و قوی به نام های Back Orifice و Sub7 در دهه 90 میلادی به بعد برای نشان دادن نقص امنیتی در سیستم عامل های ویندوز، به ویژه ویندوز 95 و 98 ایجاد شد.

Back Orifice از اولین برنامه های کاربردی سرویس گیرنده و سرویس دهنده بود که در سکوت بر روی یک سیستم نصب می شد و اجازه می داد یک کاربر از راه دور سیستم را بر روی شبکه کنترل کند.

Sub7 یکی دیگر از تروجان های معروف است. اگرچه این برنامه از سال 2004 پشتیبانی نشده است، اما با سیستم عامل های ویندوز از جمله ویندوز 8.1 سازگار است. تروجان های

Back Orifice، Sub7 یک رابط کاربری گرافیکی داشتند که اجازه می داد مهاجم کنترل کامل هر دستگاه آلوده را در دست بگیرد.

با کنترل کامل کامپیوتر، هکر می تواند فایل ها را ارسال کند، فایل ها را حذف کند، کامپیوتر را مجددا راه اندازی کند یا اطلاعات را به مالک منتقل کند. اکثر هکرها در تلاشند تا چندین ماشین را در یک زمان کنترل کنند. هنگامی که یک هکر کنترل صدها نفر از رایانه های شخصی را به عهده دارد، آنها اغلب به عنوان رایانه های زامبی یا بوت نت شناخته می شوند. بوتنت ها دسترسی هکرها به یک دسته ی بزرگ از رایانه های شخصی را فراهم می کنند که بعدا می توانند برای حمله به سرورها یا شرکت های بزرگ استفاده کنند. تروجان ها اجازه می دهند هکرها حملات از دستگاه های زامبی را انجام دهند که مقدار زیادی از ترافیک را در منابع سرور قربانی هدف قرار می دهد. به طور خلاصه، هکرها می توانند وب سرورهای بزرگ شرکت را خراب کنند و خدمات را مختل کنند.

تروجانی موفقیت آمیز است که از سیستم های تشخیص نفوذ مخرب پنهان باشد. (Rootkits ها نوعی تروجان هستند که در برابر تشخیص محافظت می کنند. Rootkits آسیب پذیری ها را با اجازه دادن به هکرها برای نصب نرم افزارهای مخرب از راه دور بدون شناسایی ایجاد می کند.)

به طور کلی، تروجان ها بسیار خطرناک هستند که توانایی آنها برای دسترسی هکرها به یک سیستم با اضافه کردن نرم افزارهای مخرب یا کنترل از راه دور از روی دسکتاپ است. هکرها به همه چیز در کامپیوتر دسترسی دارند، بنابراین سرقت هویت شما یک مسئله مهم است. اگر آنها قادر به نصب سایر نرم افزارهای مخرب باشند، می توانند رمزهای عبور و اطلاعات شخصی مانند شماره کارت اعتباری را سرقت کنند.

تروجان ها در چند قالب قرار می گیرند. بعضی از تروجان ها در قالب ارتقاء یک برنامه به ورژن جدید موجود هستند، اما در واقع سیستم را آسیب پذیر می کنند. گاهی تروجان ها در قالب یک برنامه های آنتی ویروس هستند، اما به جای آن آسیب پذیری ها را باز می کنند. به همین دلیل هرگز فایل ها را از یک منبع غیر رسمی دانلود و نصب نکنید.

انواع مختلف تروجان ها

تروجان ها بر اساس نوع اقداماتی که می توانند بر روی رایانه شما اجرا شوند دسته بندی می شوند:

Backdoor

یک تروجان backdoor می تواند از برنامه های مخرب کنترل از راه دور بر روی کامپیوتر آلوده استفاده کند و کاری را که می خواهند بر روی کامپیوتر آلوده انجام دهند، از جمله ارسال، دریافت، راه اندازی و حذف فایل ها، نمایش داده ها و راه اندازی مجدد کامپیوتر. تروجان Backdoor اغلب برای متحد کردن یک گروه از رایانه های قربانی برای ایجاد یک botnet یا شبکه زامبی است که می تواند برای اهداف جنایی استفاده شود.

Exploits

Exploits برنامه هایی هستند که حاوی داده ها یا کد هایی هستند که از آسیب پذیری در نرم افزار کاربردی که در رایانه شما اجرا می شود استفاده می شود.

Rootkits

Rootkits ها برای مخفی کردن اشیاء خاص یا فعالیت ها در سیستم شما طراحی شده اند. اغلب هدف اصلی آنها جلوگیری از شناسایی برنامه های مخرب است - به منظور گسترش دوره ای که برنامه ها می توانند بر روی یک کامپیوتر آلوده اجرا شوند.

Trojan-Banker

برنامه های Trojan-Banker برای سرقت اطلاعات حساب شما برای سیستم های بانکی آنلاین، سیستم های پرداخت الکترونیکی و کارت های اعتباری یا بدهکاری طراحی شده اند.

Trojan-DDoS

این برنامه ها حملات DoS (Denial of Service) را علیه آدرس وب هدفمند انجام می دهند. با ارسال چندین درخواست - از کامپیوتر شما و چندین کامپیوتر آلوده دیگر – این حمله می تواند آدرس هدف را منحل کند و منجر به انکار سرویس می شود.

Trojan-Downloader

Trojan-Downloaders می توانید نسخه های جدیدی از برنامه های مخرب را بر روی کامپیوتر خود دانلود و نصب کنید - از جمله تروجان ها و ابزارهای تبلیغاتی.

Trojan-Dropper

این برنامه ها توسط هکرها برای نصب تروجان ها و / یا ویروس ها استفاده می شود و یا برای جلوگیری از شناسایی برنامه های مخرب. همه برنامه های آنتی ویروس قادر به اسکن تمام اجزای داخل این نوع تروجان نیستند.

Trojan-FakeAV

برنامه های Trojan-FakeAV شبیه سازی فعالیت نرم افزار آنتی ویروس. آنها برای جمع آوری پول از شما طراحی شده اند - در عوض برای شناسایی و رفع تهدیدات ... حتی اگر تهدیداتی که گزارش می کنند واقعا وجود نداشته باشند.

Trojan-GameThief

این نوع برنامه اطلاعات حساب کاربری کاربر را از بازیگران آنلاین دور می زند.

Trojan-IM

برنامه های Trojan-IM سرقت ورود و رمز عبور خود را برای برنامه های پیام رسانی فوری مانند ICQ، MSN Messenger، AOL Instant Messenger، Yahoo Pager، Skype و بسیاری دیگر ارسال می کند.

Trojan-Ransom

این نوع تروجان می تواند داده ها را بر روی کامپیوتر شما تغییر دهد - به طوری که کامپیوتر شما به درستی اجرا نمی شود و یا دیگر نمی توانید از داده های خاص استفاده کنید. و برای بازگرداندن اطلاعات شما پول درخواست می کنند.

Trojan-Spy

برنامه های Trojan-Spy می توانند بر روی نحوه استفاده از رایانه خود جاسوسی کنند - به عنوان مثال، از طریق ردیابی داده هایی که از طریق صفحه کلید وارد می کنید، گرفتن عکس های روی صفحه یا گرفتن لیستی از برنامه های در حال اجرا.

Trojan-Mailfinder

این برنامه ها می توانند آدرس های ایمیل شما را از رایانه تان برداشت کنند.

انواع دیگر تروجان ها عبارتند از:

Trojan-ArcBomb

Trojan-Clicker

Trojan-Notifier

Trojan-PSW

چگونه از سیستم های خود در مقابله با تروجان محافظت کنیم؟

در حالی که بیشتر نرم افزارهای مخرب فقط نیاز به آنتی ویروس دارند، بزرگترین محافظت در برابر تروجان ها فایروال است. ویندوز فایروال نصب شده و فایروال ها روی یک روتر نیز می توانند در مقابل این حملات کمک کنند. فایروال ها به شما اجازه می دهد قوانین مربوط به ترافیک ورودی و خروجی را تنظیم کنید. این بدان معنی است که اگر هکر تلاش کند تا

از طریق روتر خود به کامپیوتر متصل شود، برنامه فایروال ویندوز با تنظیماتی که در خود دارد و با set کردن آن جلوی ورودی ها را می گیرد.

به همان شیوه که فایروال ها ترافیک ورودی را مسدود می کنند، اتصالات خروجی را نیز می تواند مسدود کنند. برخی از نرم افزارهای مخرب تروجان فایل ها و سایر اطلاعات را به هکر ارسال می کنند. اگر این ترافیک را در سطح فایروال متوقف کنید، هشدار دریافت خواهید کرد که رایانه شما در حال تلاش برای اتصال به یک پورت مسدود شده است. به عنوان مثال، هکر ممکن است تلاش کند فایل های خصوصی را به یک سرور FTP ارسال کند. FTP از پورت 21 استفاده می کند. اگر فایروال شما پورت 21 را متوقف کند، هنگامی که کامپیوتر تلاش می کند فایل ها را بدون دانش خود ارسال کند، یک هشدار دریافت خواهید کرد. انتقال مسدود شده است، و اطلاعات خصوصی شما محافظت می شود.

نرم افزار آنتی ویروس همچنین اکثر تروجان ها را شناسایی می کند. با این حال، هکرها همچنان به ایجاد تروجان های جدید و همچنین نصب روت کیت ها بر روی ماشین ها برای دسترسی به سیستم شما هستند. همیشه software definition files آنتی ویروس خود را به روز نگه دارید. این فایل ها برای شناسایی اثر انگشت تروجان و جلوگیری از آلوده شدن دستگاه شما مورد استفاده قرار می گیرند.

در نهایت، برای جلوگیری از تروجان ها، فقط نرم افزار را از وب سایت رسمی توسعه دهنده دانلود کنید.

حذف تروجان ها

تروجان ها معمولا در سیستم جاسازی شده اند، بنابراین کاربران نهایی باید آخرین نرم افزار آنتی ویروس خود را برای تمیز کردن دستگاه دانلود کنند. اکثر کاربران قادر به دستی حذف

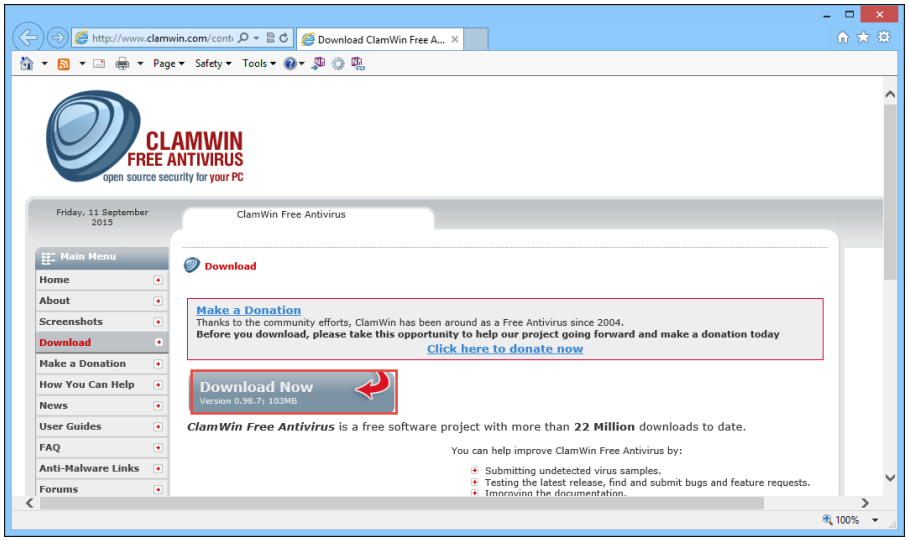
تروجان ها نمی شوند، زیرا نیاز به ویرایش رجیستری سیستم و احتمالا راه اندازی مجـدد در حالت امن است.

به جای حذف دستی آنها، آخرین فایل های تعریف شده برای آنتی ویـروس خـود را دانلـود کنید و یک بررسی کامل روی دستگاه انجام دهید. این احتمالا امن ترین و مطمئن ترین راه برای حذف یک تروجان است.

معرفی یک راه حل

یک راه حل ساده برای رهایی از ویروس ها ی تروجان از سیستم استفاده از نرم افزار رایگان ClamWin است.که کار اصلی آن پیدا کردن ویروس هـای تروجـان و حـذف آن هـا مـی باشد. و استفاده ازین نرم افزار با وجود رابط گرافیکی ساده بسیار آسان است.

که در این بخش به نصب و چگونگی استفاده از آن می پردازیم:



گام اول

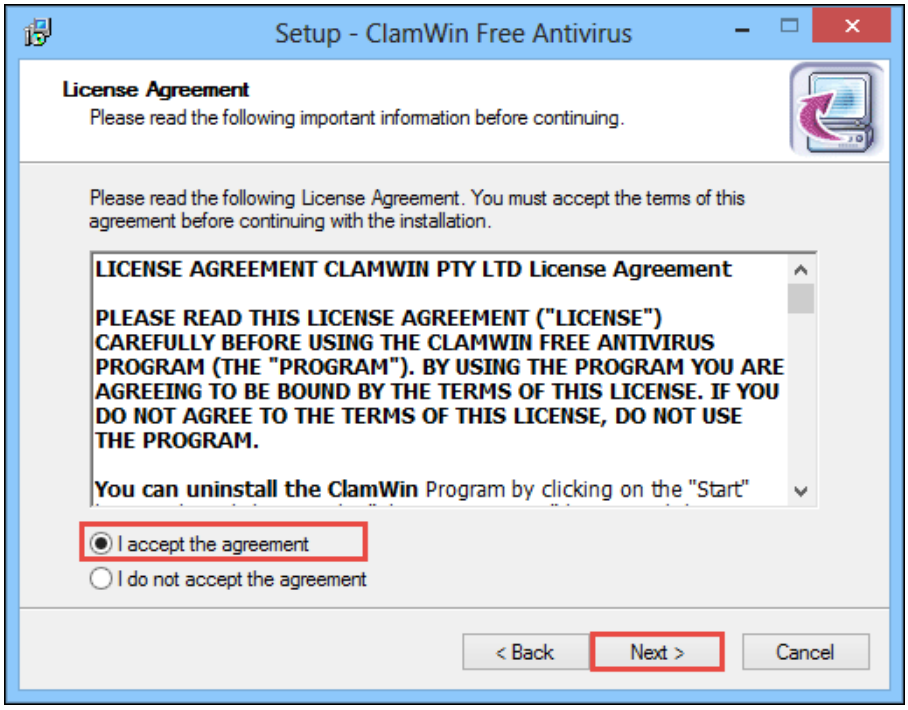
در بـروزر خـود لینـک http://www.clamwin.com/content/view/18/46/ را وارد کـرده سـپس روی دکمـه ی دانلـود کلیک کنید تا نرم افزار برای شما دانلود شوئد.

گام دوم

روی فایل دانلود شده کلید کنید سپس صفحه ی خوش آمدید و نصب نرم افزار برای شما باز می شود.

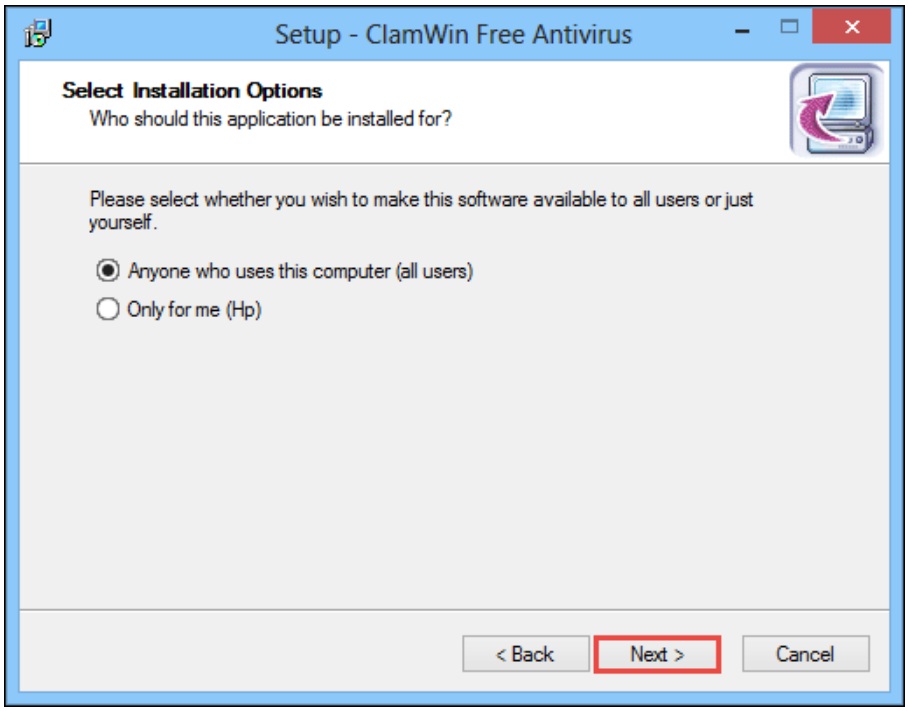
گام سوم

روی دکمه ی **Next کلیک کنید.**



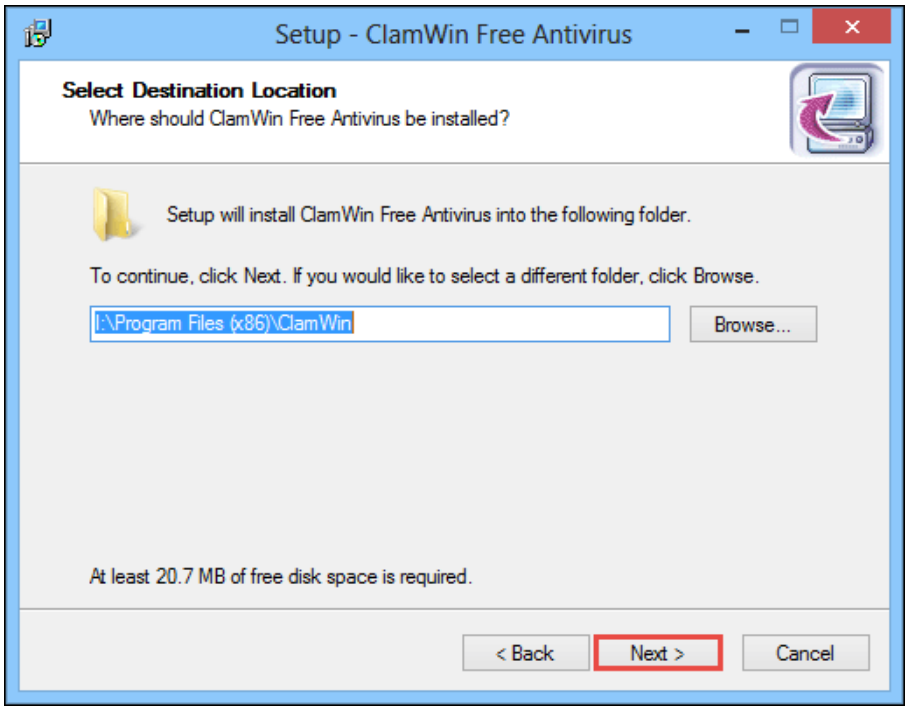
گام چهارم

روی **I accept the agreement** کلیک کرده سپس دکمه Next را وارد کنید.



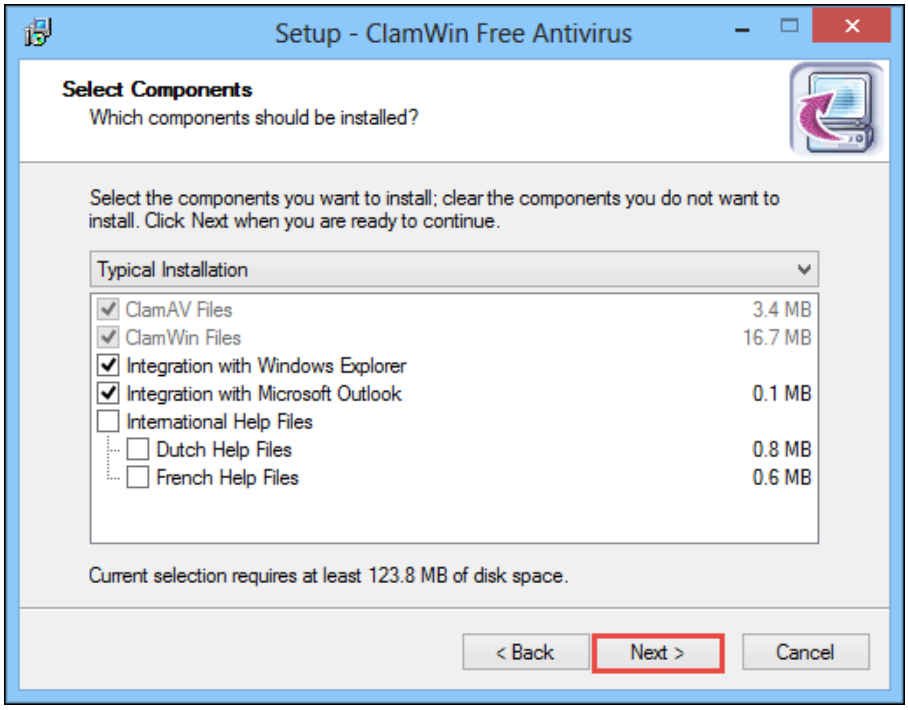
گام پنجم

روی **Select Installation Options** کلیک کرده سپس دکمه Next را وارد کنید.



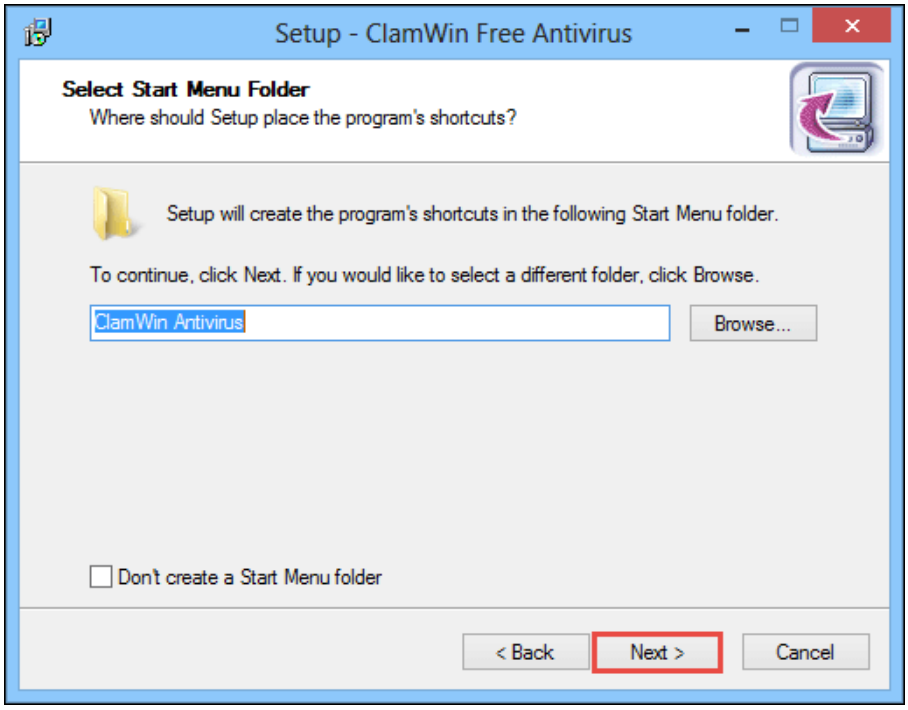
گام ششم

مسیر مورد نظر خود را انتخاب کرده و دکمه ی Next را وارد کنید.



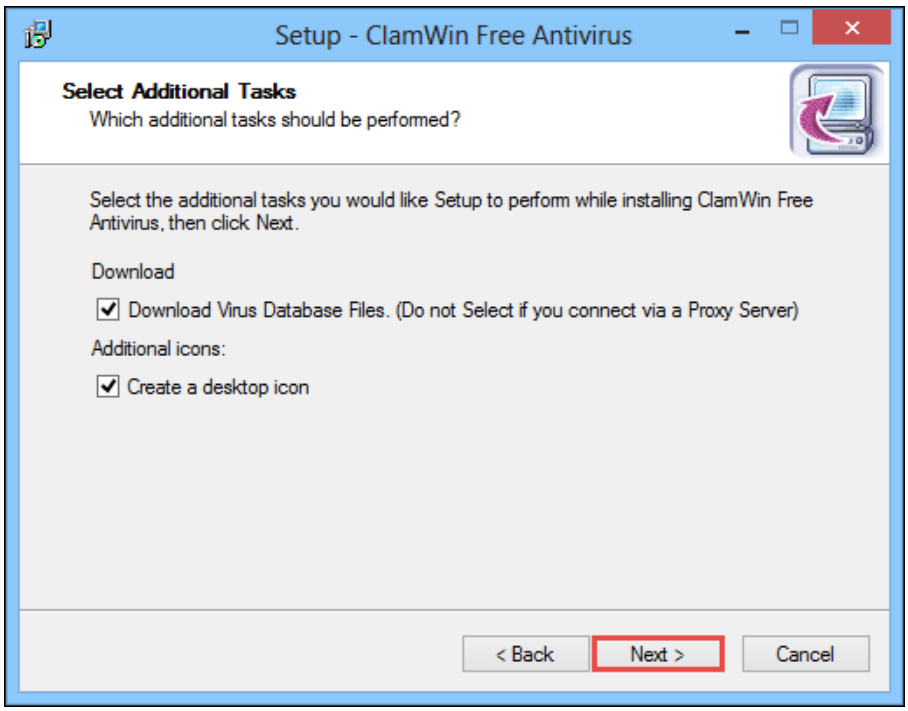
گام هفتم

مطابق شکل عمل کرده و دکمه ی Next را وارد کنید.



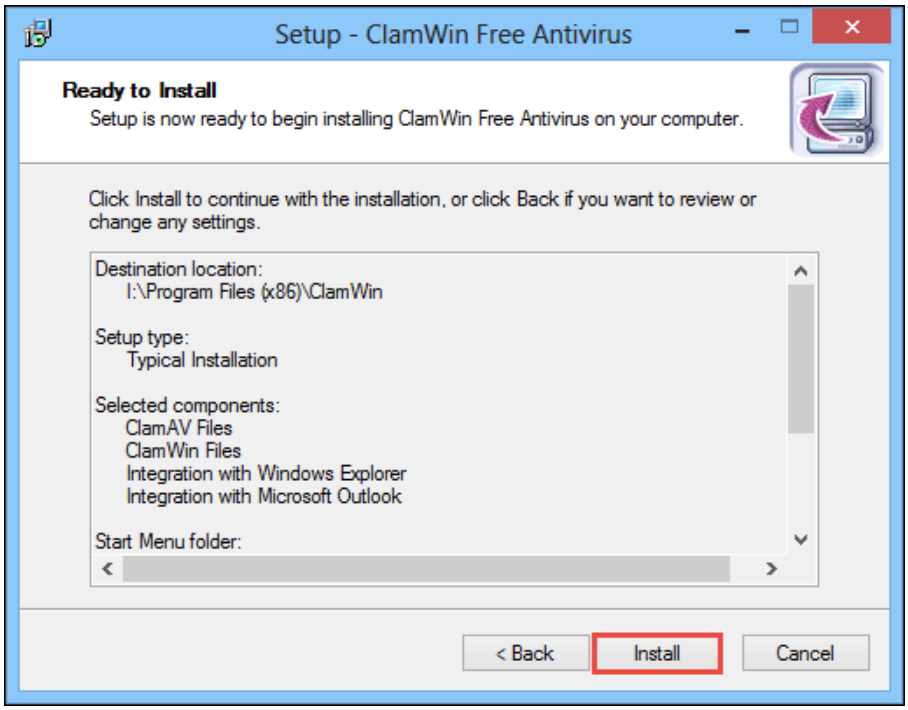
گام هشتم

فولدر مورد نظر را انتخاب کرده و دکمه Next را فشار می دهیم.



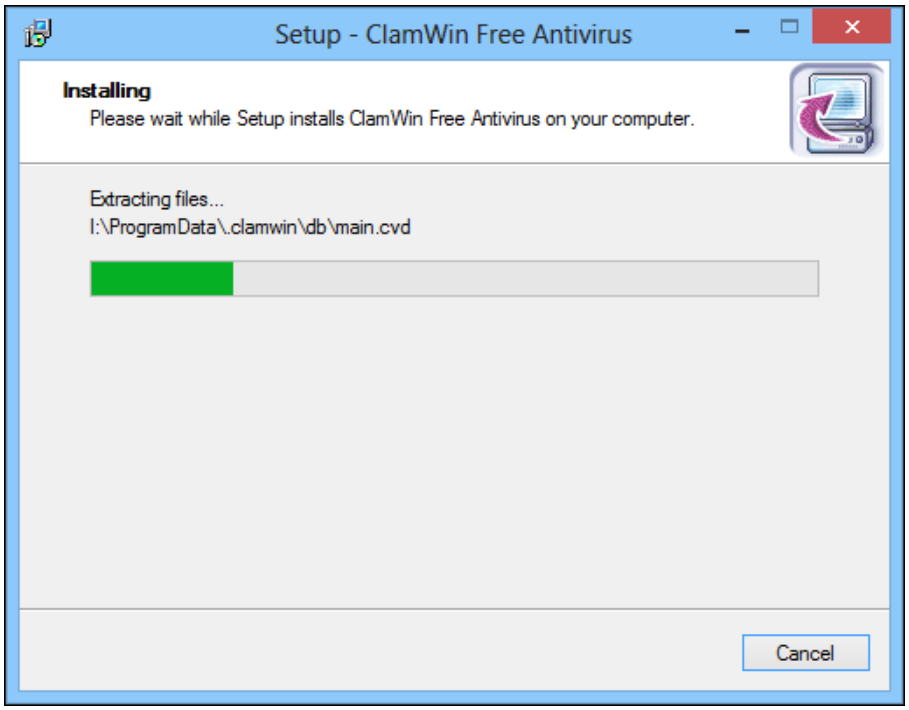
گام نهم

روی دکمه Next کلیک کنید.



گام دهم

روی دکمه Install کلیک کرده تا برنامه شروع به نصب کند.

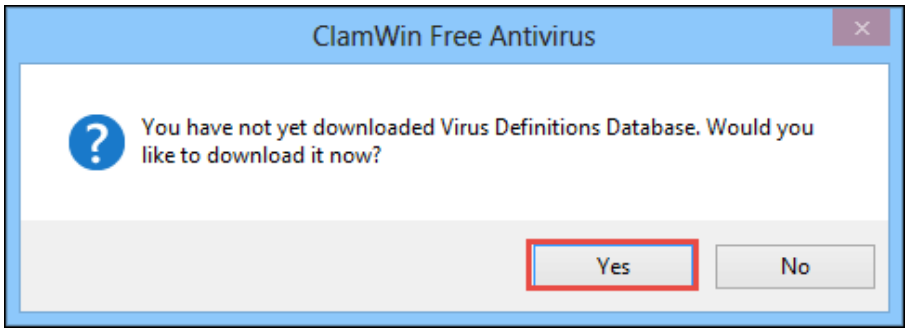


گام یازدهم

پروسه ی نصب در این مرحله انجام می شود.

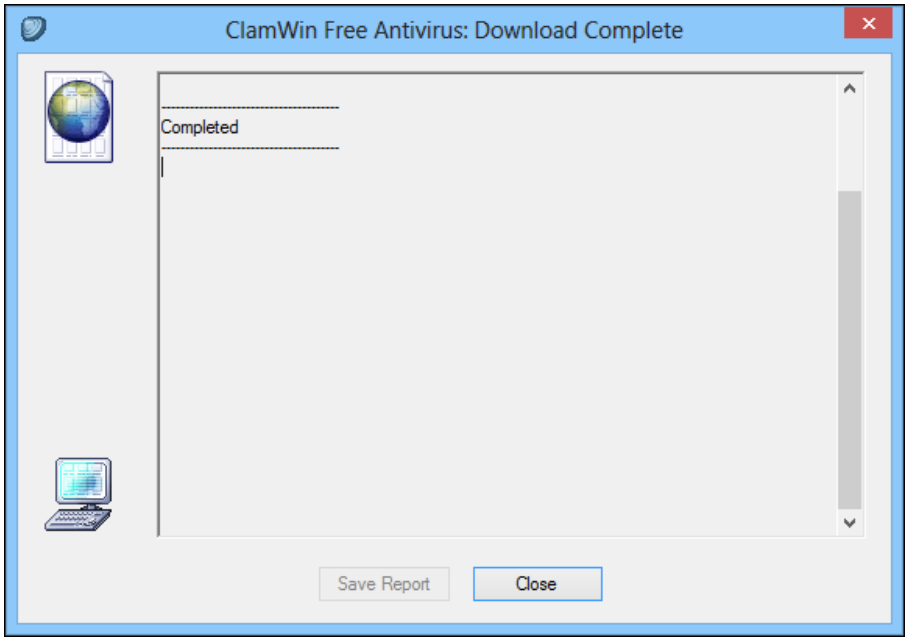
گام دوازدهم

دکمه ی Finish را فشار دهید.



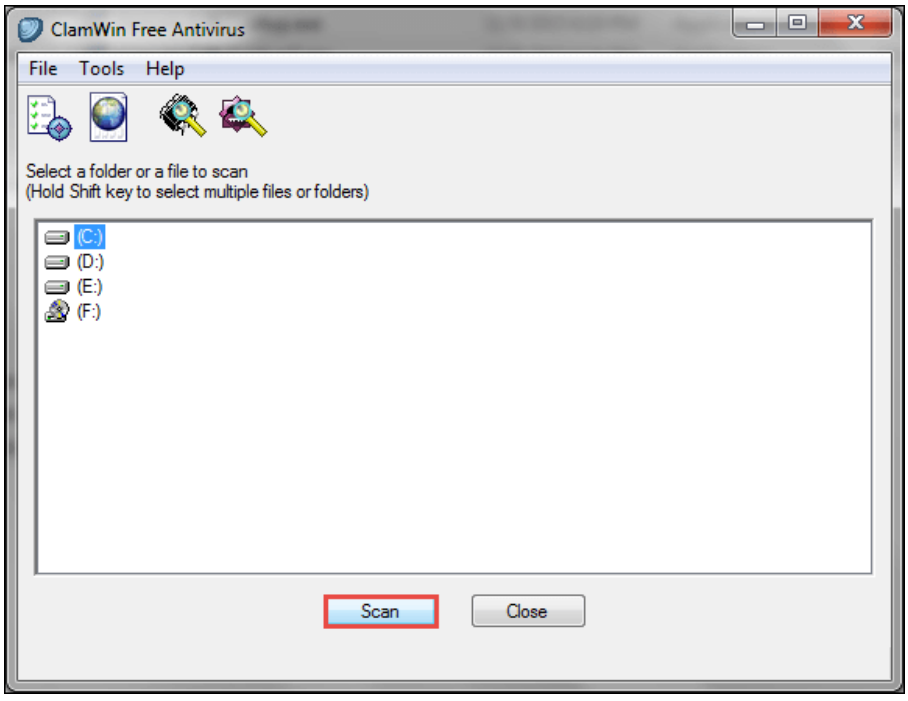
گام سیزدهم

روی دکمه ی Yes کلیک کنید.



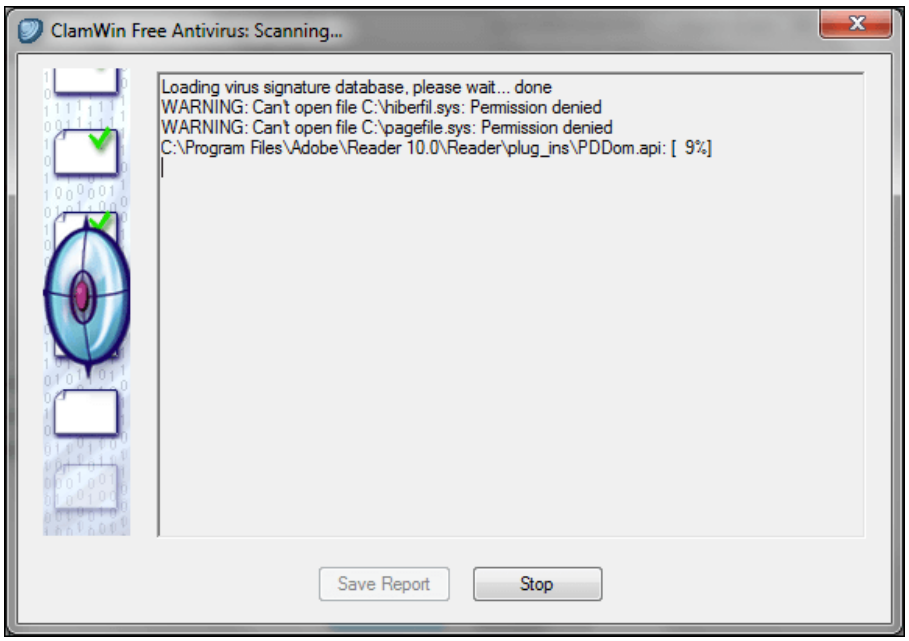
گام چهاردهم

ClamWin شروع به به روز رسانی پایگاه داده آنتی ویروس می کند.



گام پانزدهم

پس از اتمام به روز رسانی، یک یا چند درایو را برای اسکن انتخاب کنید. شما می توانید Shiftkey را برای انتخاب چندین درایو برای اسکن نگه دارید. روی دکمه Scan کلیک کنید.



گام آخر

ClamWin فرآیند اسکن را برای شناسایی و حذف نرم افزارهای مخرب از کامپیوتر شما آغاز می کند.

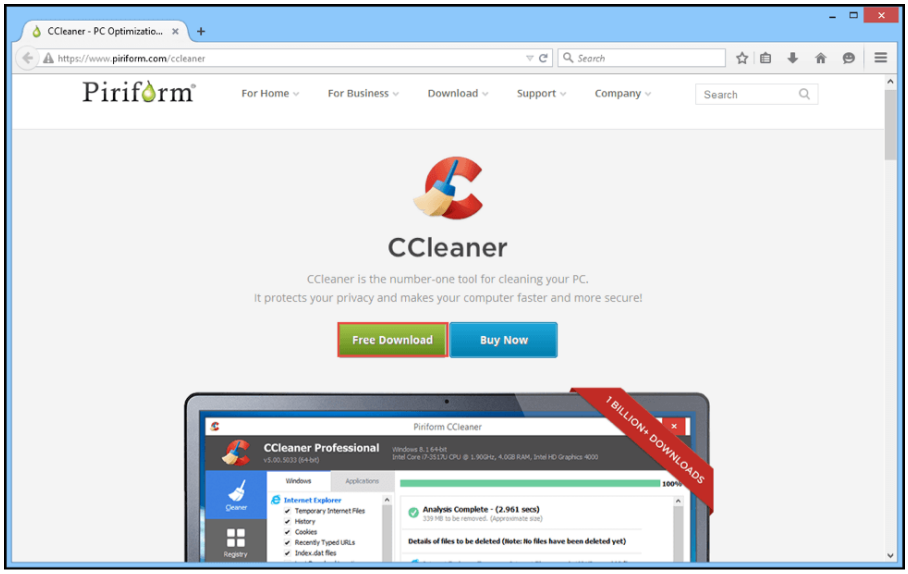
اگر چه تروجان ها از کامپیوتر شما حذف شده است، به همان اندازه مهم است که شما رجیستری ویندوز خود را از هر گونه نوشته های مخرب ایجاد شده پاک کنید.

تمیزکردن رجیستری ویندوز

عفونت گرفته شده از تروجان ها می تواند رجیستری ویندوز کامپیوتر شما را تغییر دهد. بنابراین، حتی پس از حذف کامل تروجان ها از کامپیوتر شما، بسیار مهم است که رجیستری خود را تمیز کنید.

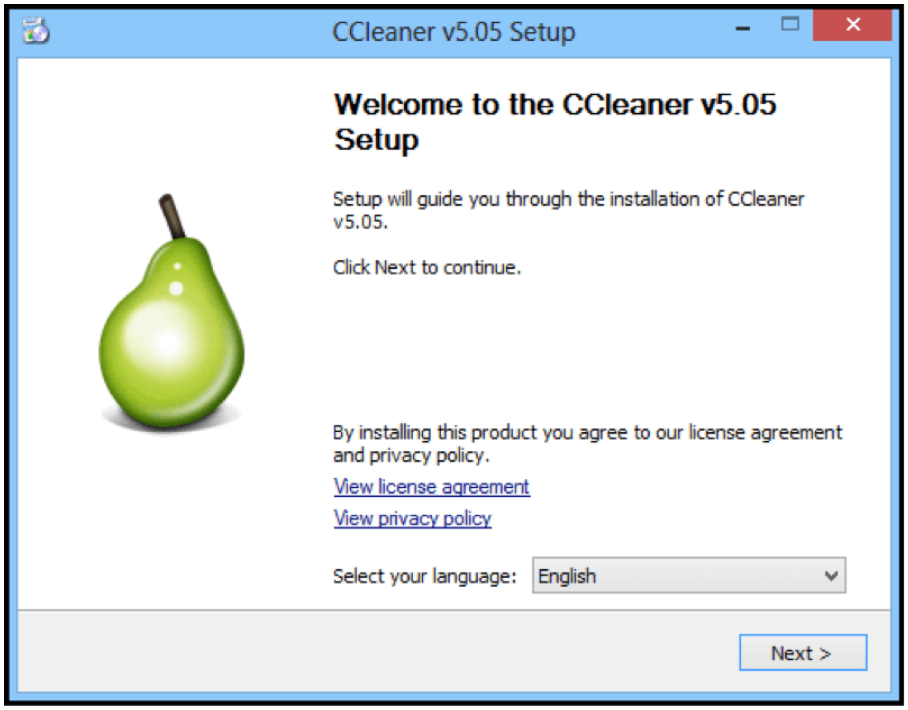
توصیه می کنیم دانلود و استفاده ازCCleaner ، یک ابزار پاک کننده رجیستری ویندوز رایگان برای تمیز کردن رجیستری است. برای پاک کردن رجیستری با استفاده ازCCleaner ، لطفا وظایف زیر را

انجام دهید:



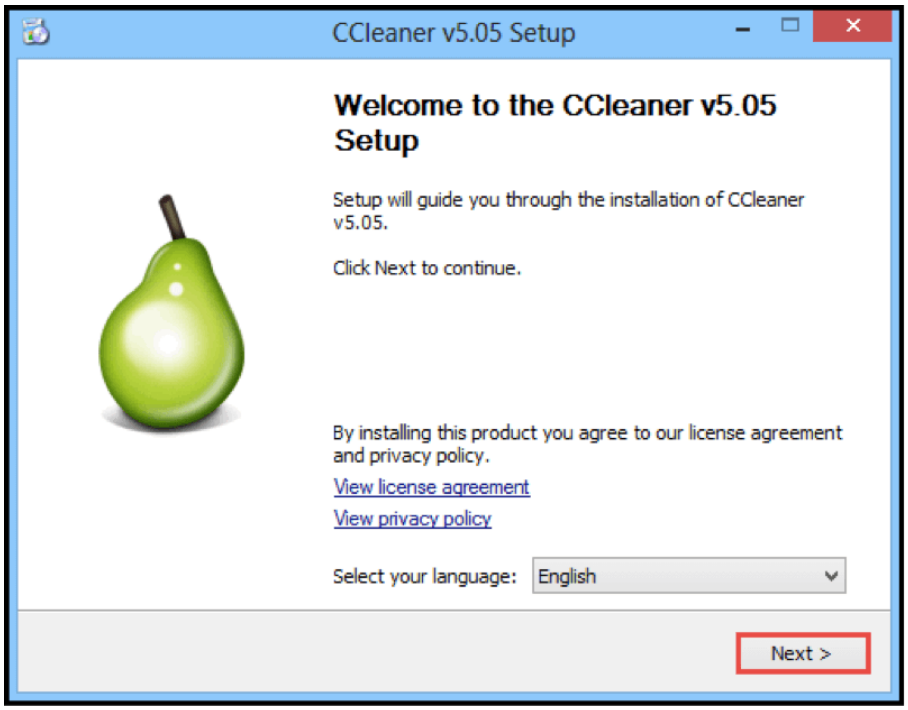
گام اول

در بروزر خود خود لینک https://www.piriform.com/ccleaner را باز کنید صفحه ی بالا برای شما نمایش داده می شود سپس بر روی دانلود رایگان کلیک کرده تا نرم افزار دانلود شود.



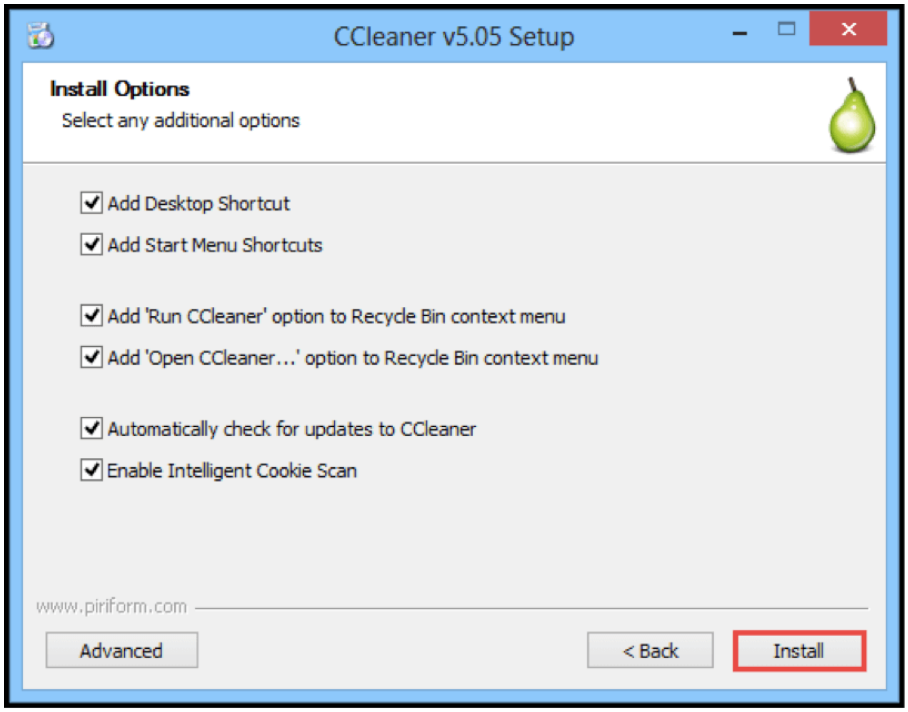
گام دوم

برای شروع فرآیند نصب بر روی فایل دانلود دو بار کلیک کنید.صفحه خوش آمدید نمایش داده می شود.



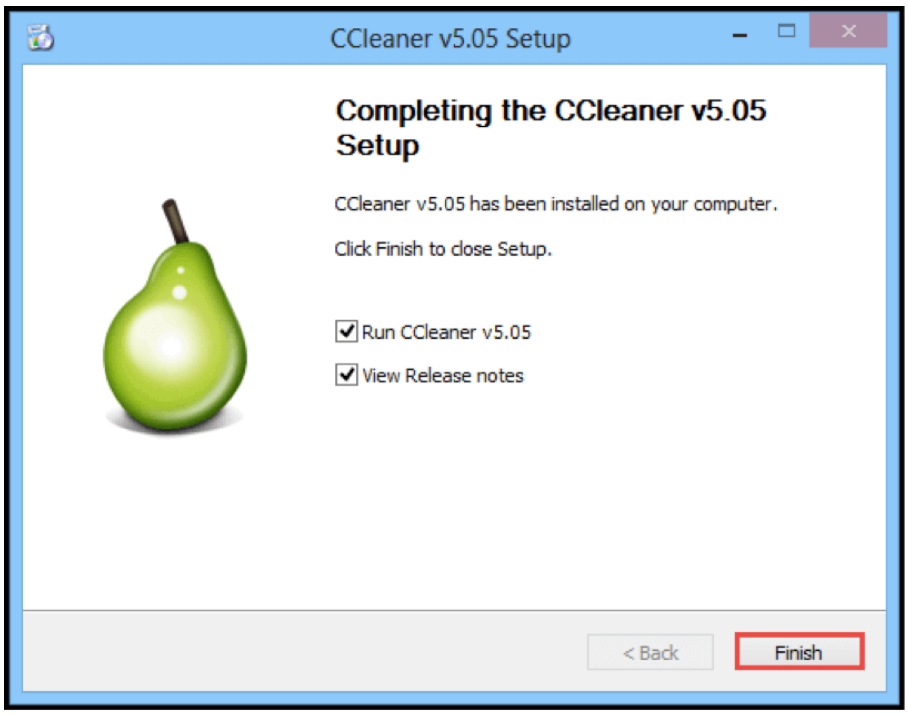
گام سوم

روی دکمه Next کلیک کنید.



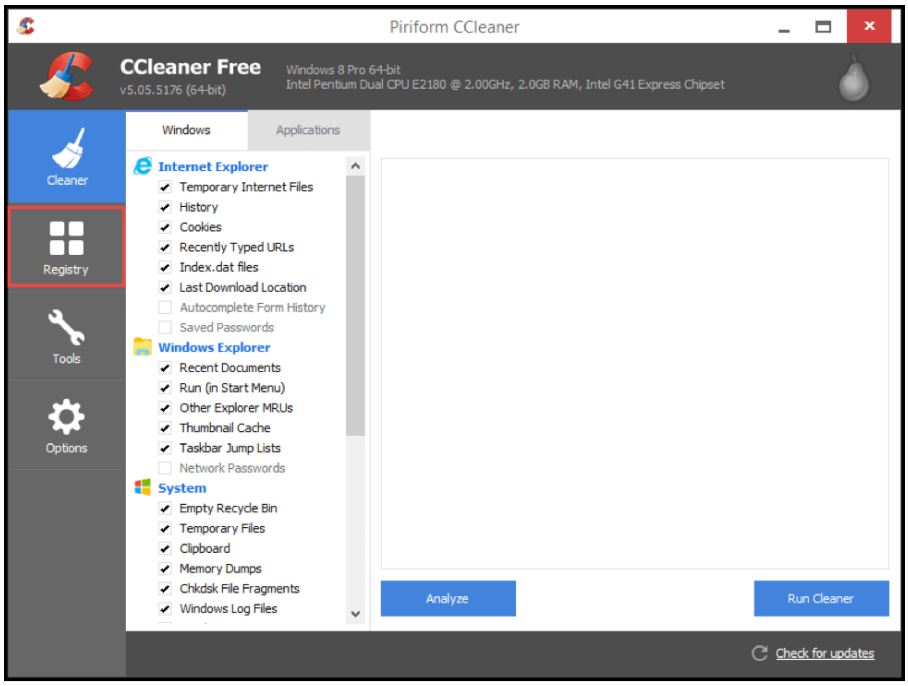
گام چهارم

روی دکمه Install کلیک کنید تا نصب شروع شود.



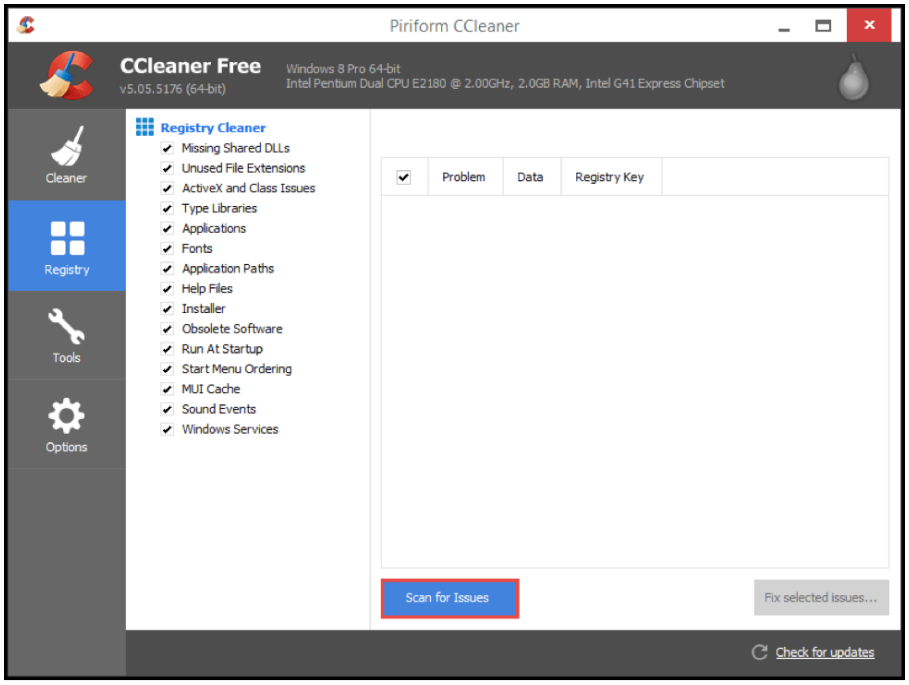
گام پنجم

دکمه Finish را برای تکمیل فرآیند نصب و راه اندازی CCleaner کلیک کنید.



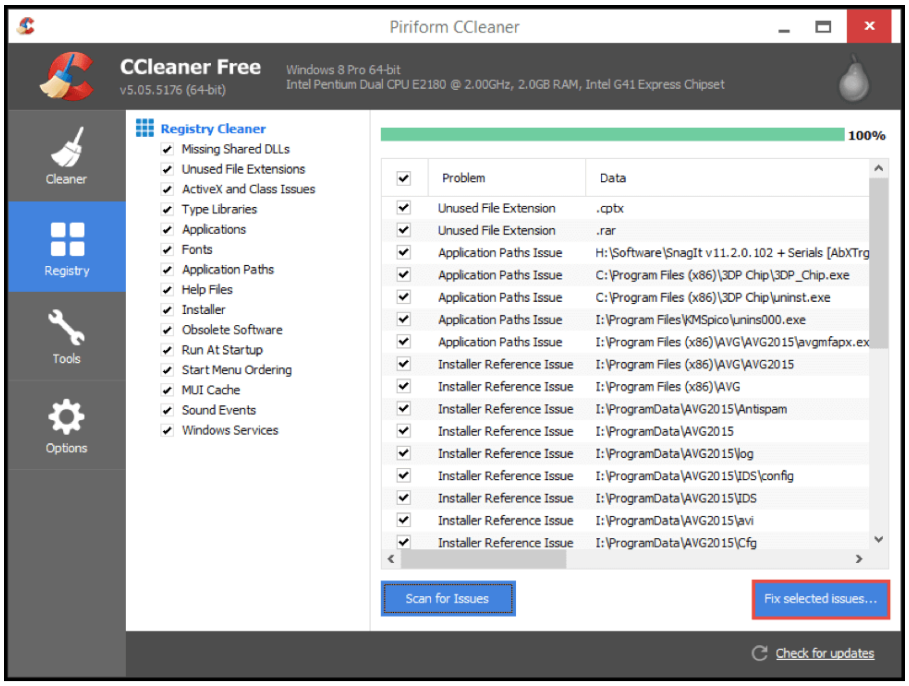
گام ششم

روی دکمه Registry در پنجره CCleanermain کلیک کنید.



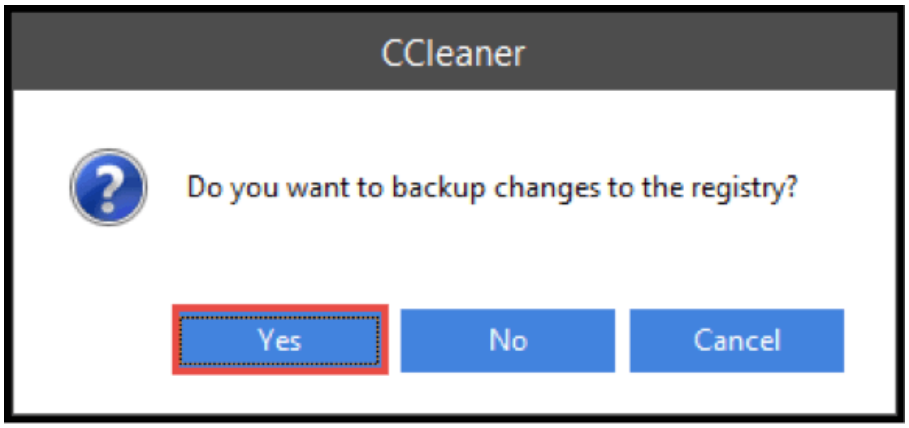
گام هفتم

بر روی دکمه Scan for Issues کلیک کنید تا مسائل مربوط به رجیستری تروجان را بررسی کند.



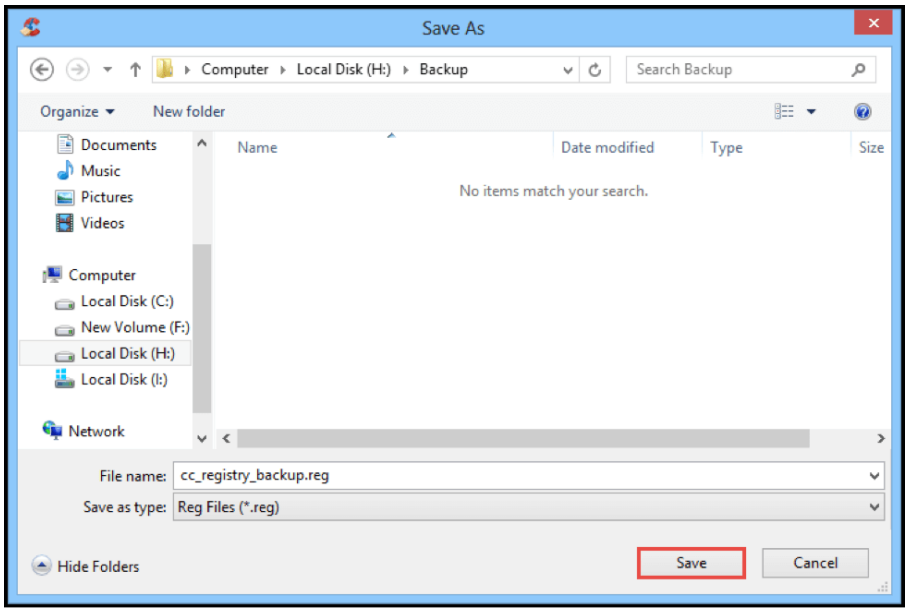
گام هشتم

دکمه Fix selected issues را کلیک کنید تا مسائل مربوط به رجیستری را که CCleaner گزارش می کند، رفع کنید.



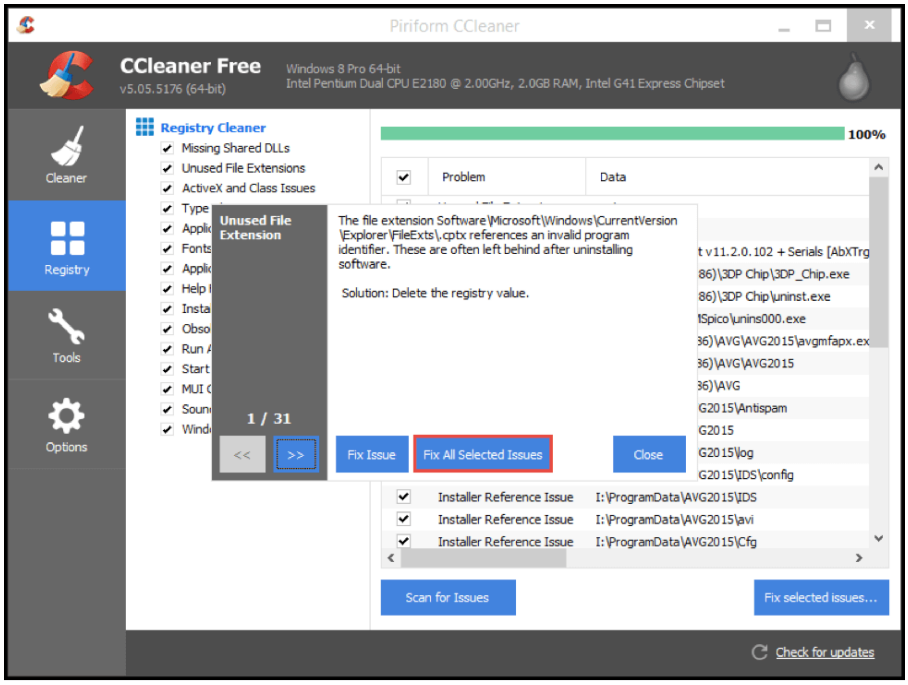
گام نهم

وقتی CCleaner شما را به تهیه نسخه پشتیبان از رجیستری دعوت می کند، روی دکمه Yes کلیک کنید.



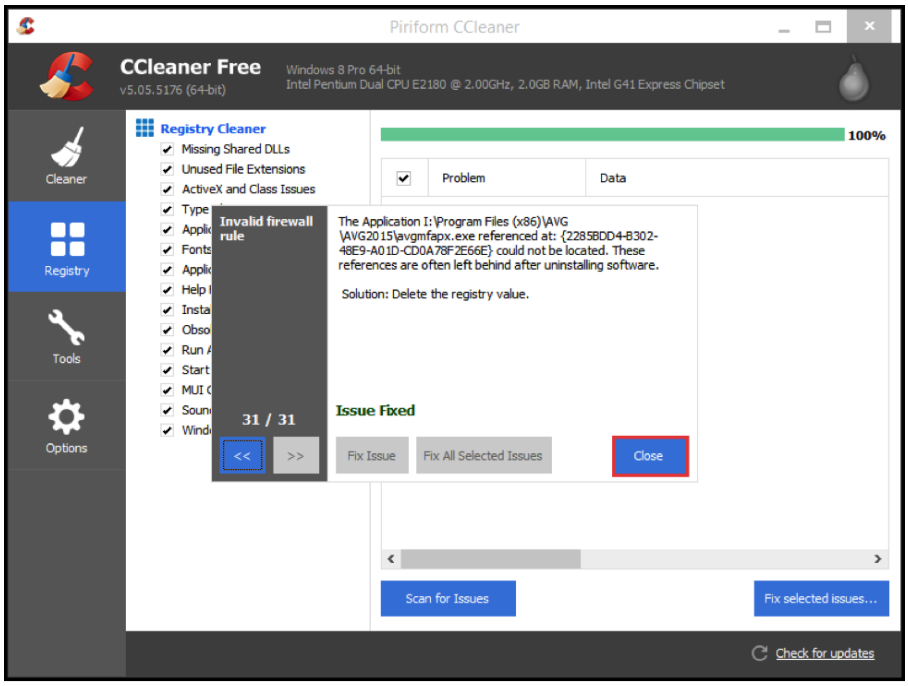
گام دهم

نام فایل را برای پشتیبان گیری از رجیستری در جعبه متن File Name در کادر Save Asdialog بنویسید و سپس روی دکمه Saveکلیک کنید.



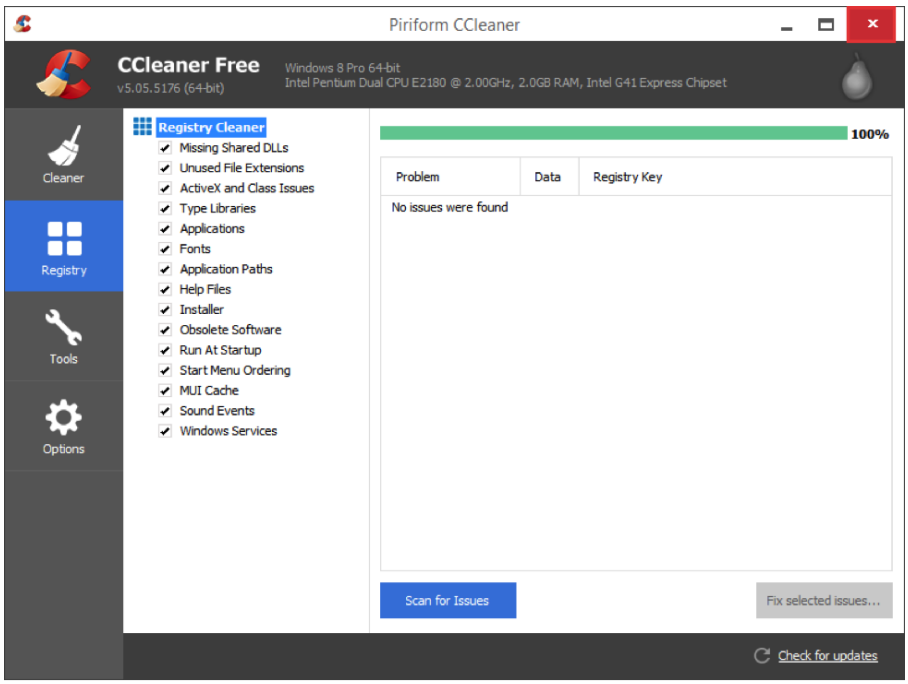
گام یازدهم

برای رفع همه مسائل، روی دکمه **Fix All Selected Issues** کلیک کنید.



گام دوازدهم

برروی دکمه Close کلیک کنید.



گام سیزدهم

برای خروج از CCleaner روی پنجره ( ) Closeدر پنجره اصلی کلیک کنید.

رجیستری ویندوز شما باید از هر گونه بقایای آلوده مربوط به تروجان پاک شود.

مشخصات کلی از چند نمونه تروجان

ردیف	نام باج افزار	تاریخ انتشار	شدت
1	Xtrat Trojan Activity	2017June 20	Critical
2	RDN/Generic.bfr!dq	-	Medium
3	Win32:SdBot-DMG	-	Moderate

تروجان Xtrat Trojan Activity

	گزارش 1
Xtrat Trojan Activity	نام تروجان
2017June 20	تاریخ انتشار
--	CVE
Critical	شدت تهدید
سیستم عامل های ویندوز	سیستم های آسیب دیده

گزارش 1	
معرفی مختصر	نوعی تروجان است که به صورت backdoor Remote Access عمل می کند.
بررسی آسیب پذیری	راه توزیع شدن این تروجان از وب سایت های به اشتراک گذاری فایل آسیب دیده و از درایو های آلوده USB است. گزارش ها نشان می دهد که تروجان برای نصب نرم افزارهای مخرب در یک کامپیوتر هدفمند مورد استفاده قرار می گیرد و می تواند برای ضبط اطلاعات حساس در یک سیستم هدفمند، از جمله کلمه کاربر و کلمه عبور سیستم استفاده شود. علاوه بر این، Xrat برای گرفتن عکس از کاربران unsuspecting با استفاده از وب کم سیستم هدف قرار گرفته است. Xrat با استفاده از یک loadload برای ضبط اطلاعات حساس در یک سیستم هدفمند استفاده می کند. تروجان ممکن است کلاینتگر را بر روی سیستم هدف قرار داده، که می تواند برای ضبط رمزهای کاربر و سیستم استفاده شود. تروجان همچنین می تواند تصاویر دسکتاپ، تصاویر از وبکم سیستم و

گزارش 1	
	صدا از میکروفون سیستم هدف را ضبط کند. اطلاعات جمع آوری شده سپس به سرور راه دور برای مهاجم برای مشاهده ارسال می شود.

گزارش 1	
توصیه های امنیتی و راهکارهای جلوگیری از آسیپ پذیری	1. به کاربران توصیه می شود از USB های ناخواسته یا درایوهای قابل جابجایی استفاده نکنند. 2. به مدیران توصیه می شود برای جلوگیری از حملات که برای استفاده از RAT انجام می شوند، از یک سیستم پیشگیری از نفوذ IPS یا سیستم تشخیص نفوذ IDS استفاده کنند. 3. گرفتن نسخه ی پشتیبانی از سیتم به صورت مداوم در یک حافظه ی جدا گانه 4. اگر کامپیوتر شما به شبکه وصل است در صورت مشاهده آلوده شدن سیستم حتما آن را از شبکه خارج کنید. 5. به روز نگه داشتن سیستم عامل و نرم افزار ها از لینک های معتبر. 6. استفاده از آنتی ویروس و به روز نگهداری آن. 7. استفاده از فایروال های ویندوز و بستن یا مسدود کردن پورت های ورودی و خروجی که مورد استفاده نیستند. 8. استفاده از راه حل های نام برده شده در این گزارش مربوط به حذف تروجان.

تروجان RDN/Generic.bfr!dq

گزارش 2	
نام تروجان	RDN/Generic.bfr!dq
تاریخ انتشار	-
CVE	--
شدت تهدید	Medium
سیستم های آسیب دیده	سیستم عامل های ویندوز
معرفی مختصر	RDN / Generic.bfr! dq یک تروجان است که در برنامه های مخرب پنهان شده است. هنگامی که شما برنامه منبع (برنامه ی حاوی ویروس تروجان) را نصب می کنید، این تروجان تلاش می کند بدون دانستن شما دسترسی root را به کامپیوتر خود

	برساند.
بررسی آسیب پذیری	تروجان ها از جمله RDN / Generic.bfr! dq پیچیده هستند زیرا خود را با ادغام به سیستم عامل مخفی می کنند. هنگامی که کامپیوتر شما توسط این تروجان آلوده شد، با هر بار اجرا شدن برنامه کامپیوتر خود را چک می کند و تلاش برای دانلود و نصب فایل های مخرب دیگر. پس از اجرای موفق، برنامه منبع را پاک می کند و تشخیص آن را دشوار می کند. علائم اولیه ویروس RDN / Generic.bfr! Dq عبارتند از: فعالیت های غیر طبیعی شبکه: این تروجان ممکن است فعالیت های غیر طبیعی شبکه را به سرعت افزایش دهد، زیرا تروجان تلاش می کند به سایر برنامه های مخرب خود دسترسی پیدا کند. تغییر رجیستری RDN / Generic.bfr! dq تلاش برای اضافه کردن رجیستری جدید و اصلاح آن است. در نتیجه، شما به تدریج متوجه رفتارهای رایانه ای آهسته و غیر معمول خواهید شد.

	تغییر تنظیمات مرورگر: نصب فایل های سرکش، به خصوص با تغییر تنظیمات مربوط به پروکسی مرورگر شما. به عنوان مثال، دسترسی به اینترنت شما کم می شود و وب سایت های ناخواسته از طریق پنجره های بازشو یا به طور مستقیم در پنجره مرورگر فعال بارگیری می شوند. آهسته شدن کامپیوتر: به علت برنامه های راه اندازی شده و ناشناخته که توسط RDN / Generic.bfr! dq دانلود شده اند، شما ممکن است بوت شدن کامپیوتر شما بسیار آهسته شود.
توصیه های امنیتی و راهکارهای جلوگیری از آسیب پذیری	1. به کاربران توصیه می شود از USB های ناخواسته یا درایوهای قابل جابجایی استفاده نکنند. 2. به مدیران توصیه می شود برای جلوگیری از حملات که برای استفاده از RAT انجام می شوند، از یک سیستم پیشگیری از نفوذ IPS یا سیستم تشخیص نفوذ IDS استفاده کنند. 3. گرفتن نسخه ی پشتیبانی از سیتم به صورت

مداوم در یک حافظه ی جدا گانه

4. اگر کامپیوتر شما به شبکه وصل است در صورت مشاهده آلوده شدن سیستم حتما آن را از شبکه خارج کنید.
5. به روز نگه داشتن سیستم عامل و نرم افزار ها از لینک های معتبر.
6. استفاده از آنتی ویروس و به روز نگهداری آن.
7. استفاده از فایروال های ویندوز و بستن یا مسدود کردن پورت های ورودی و خروجی که مورد استفاده نیستند.
8. استفاده از راه حل های نام برده شده در این گزارش مربوط به حذف تروجان.

تروجان Win32:SdBot-DMG

گزارش 3	
نام تروجان	Win32:SdBot-DMG

تاریخ انتشار	==
CVE	--
شدت تهدید	Moderate
سیستم های آسیب دیده	سیستم عامل های ویندوز
معرفی مختصر	این تروجان خود را در سیستم پنهان می کند و دسترسی های از راه دور را برای هکر ایجاد می کند تا هکر بتواند از راه دور وارد اطلاعات سیستم شود.

بررسی آسیب پذیری	پس از فعال شدن، تروجان ها می توانند مجرمان اینترنتی را به جاسوسی بر روی سیستم شما متصل کنند، اطلاعات حساس شما را سرقت کنند و دسترسی به سیستم شما را به دست بیاورند. این اقدامات می تواند شامل موارد زیر باشد: • حذف داده ها • مسدود کردن داده ها • اصلاح داده ها • کپی کردن داده ها • اختلال عملکرد کامپیوترها یا شبکه های کامپیوتری بر خلاف ویروس های کامپیوتری و کرم ها، تروجان ها قادر به تکثیر خود نیستند.

توصیه های امنیتی و راهکارهای جلوگیری از آسیب پذیری	1. به کاربران توصیه می شود از USB های ناخواسته یا درایوهای قابل جابجایی استفاده نکنند. 2. به مدیران توصیه می شود برای جلوگیری از حملات که برای استفاده از RAT انجام می شوند، از یک سیستم پیشگیری از نفوذ IPS یا سیستم تشخیص نفوذ IDS استفاده کنند. 3. گرفتن نسخه ی پشتیبانی از سیتم به صورت مداوم در یک حافظه ی جدا گانه 4. اگر کامپیوتر شما به شبکه وصل است در صورت مشاهده آلوده شدن سیستم حتما آن را از شبکه خارج کنید. 5. به روز نگه داشتن سیستم عامل و نرم افزار ها از لینک های معتبر. 6. استفاده از آنتی ویروس و به روز نگهداری آن. 7. استفاده از فایروال های ویندوز و بستن یا مسدود کردن پورت های ورودی و خروجی که مورد استفاده نیستند. 8. استفاده از راه حل های نام برده شده در این گزارش مربوط به حذف تروجان.