ویروسها ، کرمها و تروجان ها چه هستند؟

ویروسها ، کرمها و تروجان ها برنامه های بدی هستند که می توانند باعث خطر برای کامپیوتر شما واطلاعات آن شوند. آنها می توانند سرعت اینترنت را پایین بیاورند وآنها حتی ممکن ا ست از کامپیوتر شما برای بخش کردن خودشان برای دوستانتان، آشنایان، شرکت محل کار استفاده کنند ودرآدرس مجازی باقی بمانند. خبرهای خوب آن است که با یک جلوگیری اندک وتعدادی مفهوم رایج خوب شما احتمالا کمترقربانی اینها هستید . به نظر می رسد این پیش قدم شدن شما برای جلوگیری تمام فامیل شما را محافظت می کند. بخوانید برای یادگرفتن درباره مشخصه ها وتفاوتهای ویروسها ، کرمها وتروجان ها .

- ویروس چیست؟
- کرم چیست؟
- تروجان چیست؟
- چطورکرمها وویروسهای دیگر پخش می شوند؟
- چطورمی توان اثرکرم یا ویروس داشت؟

مرحله بعدی : کاهش خطر ویروس

ویروس چیست؟

ویروس یک تکه کد کامپیوترا ست که خودش وابسته به یک برنامه یا فایل ا ست بنابراین آن می تواند ازکامپیوتر به کامپیوتر پخش شود.ویروسها می توانند موجب خطر نرم افزار، سخت افزار وفایلهای شما باشند.

ویروس : کد نو شته شده با مفهوم رو شن. تکرار خودش . یک ویروس برای پخش از کامپیوتربه کامپیوترتو سط وابستگی خودش به یک دسته برنامه تلاش می کند. آن ممکن است برای سخت افزار، نرم افزاریا اطلاعات خطرناک باشد. فقط دامنه ویروسهای انسانی درشدت از 1 بولا به 24 ساعت فلو، دامنه ویروسهای کامپیوتر ازرنج آوری مختصر تا مخرب محض. اخبار جدید آن هست که یک ویروس واقعی بدون اقدام انسان برای حرکت آن پخش نمی شود، مثل اشتراک فایل یا فرستادن ای میل.

کرم چیست؟

یک کرم، مثل یک ویروس برای کپی خودش از یک کامپیوتر روی دیگری طراحی شـــده اســـت، اما آن بطور اتوماتیک خصـیصــه کنترل روی کامپیوتر را می گیرد که می تواند فایلها واطلاعات را ببرد. وقتی شــما یک کرم درسیستمتان دارید آن میتواند به تنهایی حرکت کند.

یک خطر بزرگ کرمها تواناییشان برای بازگرداندن درصدای بلند است.برای مثال، یک کرم می تواند کپی خودش رابرای هرکسی که درآدرس ای میل شما ثبت شده بفرستد وسپس کامپیوترهایشان همان عمل را انجام خواهند داد ، باعث یک ترافیک شبکه سنگین می شود که سرعت شبکه ها پایین خواهد آمد واینترنت هم. موقعیکه، کرمهای جدید آزاد هستند، آنها خیلی سریع پخش می شوند، شبکه ها را کند می کند وممکن است باعث شوند که تومدت طولانی منتظرباشی برای دیدن هرصفحه سایت اینترنت.

کرم بخش اولیه ویروس . یک کرم بطورکلی بدون اقدام کاربر پخش می شود وکپی های خودش را در سرتا سر شبکه ها به طور کامل توزیع می کند یک کرم می تواند حافظه یا پهنای باند شبکه را مصرف کند، سپس باعث توقف پاسـخ دهی کامپیوتر شـود. چون کرمها برای حرکت نیاز به یک دسـته برنامه یا فایل ندارند، آنها همچنین می توانند در داخل سیستم شما تونل بزنند واجازه دهند هرکس دیگری کنترل سیستم شما رابگیرد اخیرا نمونه های کرمها شامل سایسر وبلاستر است.

تروجان چیست؟

اندکی پیش ازاین اســب تروجان اســاطیری یک هدیه بود، اما با دربرداشــتن ســربازان وخارج شــدن آنها هنگام رسیدن به شهر تروی . امروزه ، تروجان ها برنامه های کامپیوتری هستند که ظاهرا برای نرم افزارمفید می باشند، اما درعوض آنها امنیت تورا مصالحه می کنند . باعث خطر زیادی می شوند. اخیرا تروجان ازپیغام ای میل می آید که مدعی اســت جزء متعلقات امنیت برزو مایکروســافت اســت، اما ســرانجام یک ویروس می شــود که برای ازکار انداختن آنتی ویروس ونرم افزار دیوار آتش (نرم افزار حفاظتی) تلاش می کند.

تروجان برنامه کامپیوتر که ظاهرا مفید می باشـــد اما واقعا خطرناک اســـت. تروجان مردم را درهنگام باز کردن برنامه گول می زند وپخش می شود، چون آنها فکر می کنند که آن از یک منبع قانونی آمده است. برای محافظت بهتر کاربر، مایکرو سافت اغلب بیانیه های امنیتی تو سط میل می فر ستد، اما این بیانیه ها هرگز شامل وابستگی نیستند. ما همچنین همه مشدار دهنده های امنیتی مان را روی وب سایت امنیتی منتشرمی کنیم قبل ازاینکه

ما آگهی آنها را برای مشـــتریانمان بفرســـتیم. تروجان می تواند همچنین جزئی درنرم افزاری باشـــد که شـــما به طوررایگان دانلود می کنید. هرگز نرم افزاری راکه از یک منبع در ست نی ستند دانلود نکنید. همی شه برنامه ها به روزهای مایکروسافت را از ویندوز به روز یا شرکتهای به روز مایکروسافت دانلود کنید.

کرمها وویروسهای دیگر چگونه منتشر می شوند؟

واقعا همه ویروسها وتعداد زیادی ازکرمها نمی توانند منتشر شوند مگراینکه شما باز کنید یا اجرا کنید یک برنامه آلوده را .

تعداد زیادی ازاین ویرو سهای خطرناک ا صولا ازطریق متعلقات ای میل فایلها که همراه با پیغام ای میل فر ستاده شده ، منتشر می شوند. شما می توانید معمولا اگر ای میل شما ، شامل پیوستگی ای هست بگویید . چون شما آیکن کلیپی می بینید که متعلقات ونامهای آن را نشـــان می دهد. عکســـها ، نامه های نوشـــته شـــده در word مایکروسافت وحتی صفحه های گسترده excel فقط تعدادی ازانواع فایلهای شما هستند که ممکن است هر روز ازطریق ای میل بر سد . ویرو سها موقعیکه شما متعلقات فایل را باز می کنید شروع می شوند . اگربه شما پیغام ای میلی برسـد با متعلقاتش از کسـی که شـما نمی شـناسـید، شـما باید فورا آن را پاک کنید. متاسـفانه ، شـما ازمتعلقات ای میل ک سی را هم که می شنا سید ایمنی ندارید. ویرو سها وکرمها توانایی دزدیدن اطلاعات خارج برنامه های ای میل را دارند وخودشان را برای همه لیست آدرس های ثبت شده می فرستند . بنابراین اگربه شما ای میلی ازکسی با یک پیغامی که نمی فهمید یا فایلی که شما منتظرآن نبودید رسید، همیشه با شخصی تماس بگیرید ومحتویات متعلقات را قبل ازاینکه آن را باز کنید بپذیرید . ویروســـهای دیگر می توانند پخش شـــوند از طریق برنامه دانلود شده ازاینترنت یا دیسکتهای پاک کننده ویروس کامپیوتر که شما از دوستان قرض می گیرید یا از فروشگاه خریداری می کنید . اینها هستند کمترین راه رایج برای منقبض کردن ویروس کامپیوتر . اکثرمردم از طریق باز کردن واجرای متعلقات ای میل ناشناخته ویروسی می شوند .

چطور می توان گفت اگر کرم یا ویروسهای دیگر داشت؟

موقعی که شما باز می کنید یا اجرا می کنید یک برنامه آلوده را، شما ممکن ا ست ندانید منقبض کردن ویروس را . کامپیوتر شما ممکن ا ست سرعتش پایین بیاید، پا سخ دهی اش متوقف شود یا از کار بیفتد و ری ا ستارت

شـــود . گاهی اوقات یک ویروس به فایلی که شـــما برای بالا آمدن کامپیوترنیاز دارید حمله خواهد کرد. در این حالت، شما ممکن است دکمه power را فشار دهید ودرصفحه خالی آیکن start را جستجو کنید .

- همه این علامتها هســتند علامت رایج که کامپیوترشــما ویروس دارد، اگرچه که آنها می توانند معلول برنامه های نرم افزاری وسخت افزاری باشند که هیچ عملی با دارنده ویروس ندارند. جدی بگیرید پیغامی را که کامپیوتر مبنی بر وجود ویروس می دهد. این ممکن است به معنی آن باشد که ویروس به عنوان فرستنده آلوده به آدرس ای میل های لیست شده فرستاده می شود. این لزوما به معنی داشتن ویروس نیست. بعضی از ویروسها توانایی تغییرآدرس ای میل را دارند. مگر اینکه شــما نرم افزارآنتی ویروس جدید را نصــب کرده باشــید، وجود ندارد راه مطمئنی برای اینکه شما بدانید که آیا ویروس دارد یا نه. اگر شما ندارید نرم افزارآنتی ویروس رایج را یا اگر شما علاقه ای به نصب انواع مارک نرم افزار آنتی ویروس ندارید، از صفحه نرم افزارامنیتی ما دیدن کنید.

مرحله های بعدی : کاهش خطر ویروس شما

هیچ ضــمانتی، کامپیوترشــما را صــد درصــد ایمن نمی کند. با وجود این شــما میتوانید بهبود دهید امنیت کامپیوترتان توسط نرم افزارهای نگه دارنده جدید ونگه داشتن آبونمان نرم افزارآنتی ویروس رایج .

برای یاد گرفتن چیزهای بیشتردرباره آنچه که می توانید انجام دهید، این صفحات راببینید.

* یادگرفتن درباره رویدادهای امنیتی اخیروخطرات ویروس
* جستجوبرای اینکه چرا شما نیازبه دیوارآتش (نرم افزار محافظتی) کامپیوتر دارید.
* دیدن آنچه از ویندوز که می تواند به شما کمک کند.
* 3 مرحله محافظتpc شما.

آنچه که شما باید درباره بلاستربدانید.

کرم بلاستر هدف گیری می کند با یک انتشار امنیتی مربوط به کارپردازنده که مایکروسافت با آزاد کردن امنیت به روز متوجه ی شود.

بلاستر کامپیوترهایی با نرم افزارمنسوخ راهدف گیری می کند وآن کامپیوترها

درخطرآلودگی تا نصب به روزباقی می مانند.

ما پیشنهاد می کنیم که مصرف کننده ها نصب کنند به روز را از بولتن امنیتی

MS03 – 039 برای کمک به حفاظت در برابراین نرم افزار بد. اگر کامپیوتر شما آلوده شده است، کامپیوترشما ممکن است نرمال عمل کند، ممکن است که ظاهر شود یا ممکن است ری استارت شود بدون دادن ورودی. اگر کامپیوتر شما آلوده شده است ، شما ممکن است این پیغام خطا را ببینید.

- اگر سیستم شما shutt down است، مطابق این مراحل برای توقف دوره، سپس به مرحله 2 برای توقف گرم پیش روید.

01 فشار دهید : CTRL+ ALT+Delete

02 کلیک کن روی Task Manoger

03 کلیک کن رویprocesses

04 کلیک کن رویImage Name مرتب کردن به ترتیب حروف الفبا

05 جستجوی فرآیند نامیده می شود Msblast .exe اگر شما پیدا کنید آن را، کلیک نام برای انتخاب فرآیند وسپس کلیک رویd process

06 ببندید Task Manager

2 0 چک کردن وبرطرف کردن بلاستر : استفاده ابزار متوقف نرم افزاربد ویندوزمایکروسافت برای جستجوی هاردتان وتوقف بلاسترمختلف.

3 0 حفاظت pc شما : کمک به امن بودن کامپیوترتان دربرابر بلاستر و خطرهای دیگر در اینترنت، برطبق دستورالعمل محافظ pc برای برقرار کردن دیوارآتش ورسیدن به نرم افزار به روز واستفاده ازنرم افزارآنتی ویروس بروز.

کرم ساسر هدف گیری می کند با یک انتشارامنیتی با سرویس زیر سیستم نفوذ امنیتی که مایکروسافت با آزاد کردن امنیت بروز متوجه می شود. هدف ساسر کامپیوترهایی با نرم افزار منسوخ است وآن کامپیوترها با خطر آلودگی تانصب شدن به روز باقی میمانند .

ما پیشنهاد می کنیم که مصرف کننده ها نصب کنند به روز را از بولتن امنیتی مایکروسافت MS04 – 011 برای کمک به حفظ دربرابر این نرم افزارهای بد.

قبل از اینکه شـــما مراحل دیگر را طی کنید، مطمئن باشـــید ازفعالیت دیوارآتش برای کمک به حفاظت کامپیوترتان در برابرآلودگی. اگر شما یک سخت افزار دیوارآتش دارید درخانه یا محل کار یا اگر شما استفاده می کتید ازدیوارآتش با ویندوزXP ، کرم ساسر احتمالا مسدود شده است. اگر کامپیوترشما آلوده شده، یک دیوار آتش به محدود کردن اثرات کرم کامپیوتر شما کمک خواهد کرد. برای دستور العمل جامع نصب وفعال ساختن دیوارآتش از دستور العمل محافظ PC دیدن کنید.

کمک برای حفاظت کامپیوترتان دربرابر ساسر، شما باید ابتدا دانلود کنید و نصب

کنید835732 به روز امنیتی را که آزاد شده بود با بولتن امنیتی مایکرو سافت011 - MS04 . شما می توانید پیدا کنید 835732 به روز را روی وب سایت به روز ویندوز که لیست شده دربه روز مهم و سرویس بخش فشرده . شما می توانید همچنین دانلود کنید ونصب کنید این مقررات بروز را از Microsoft . com برای پیدا کردن دانلود برای ســیســتم عملیات شــما، مراجعه کنید به بولتن امنیتی Technical 011 – MS04

یادداشت : اگر شما نصب کنید به روز را برای مقررات 011 - MS04 یا از طریق به روز کردن اتوماتیک قبل از 30 بهار 2004 ، سپس شما آماده هستید برای محافظت دربرابر این انتشار.

استفاده از ویندوز مایکروسافت، ابزار توقف نرم افزار برای جستجو هارد شما وتوقف ساسر گوناگون .