

هکرها چگونه سیستم شما را کنترل می کنند؟



محمدعلی زارعی فر

تصور کنید اینترنت یک شهر است و این شهر پر از مکان های زیبا و گوناگون و همچنین مکان های خطرناک. در این شهر هر کس لزوماً آن کسی نیست که ادعا می کند، حتی شما! ممکن است متوجه شوید بی آن که بدانید کارهای غیر قانونی مرتکب شده اید. این یعنی کارهایی که انجام می دهید تحت کنترل شما نیست و نبوده و احتمال دارد حتی بعد از این نیز نتوانید جلوی آن را بگیرید.

یک رایانه زامبی (Zombie)، رایانه ای است که فرمان های شخص دیگری را اجرا می کند، بدون این که کاربران خبر داشته باشند و کنترل آن را به دست بگیرند. یک هکر که قصد انجام کارهای غیر قانونی دارد، ممکن است از یک رایانه دیگر برای انجام خرابکاری هایش استفاده کند، بدون این که کاربر آن رایانه دخالتی در آنها داشته باشد. در این مواقع کاربر قربانی بی خبر از اتفاق های رخ داده، فقط با این تصور که سرعت پردازش رایانه اش بشدت کاهش یافته، مواجه می شود. هکرها از این رایانه ها برای فرستادن اطلاعات یا حمله به سایتها و سرورها استفاده می کنند و در نتیجه اگر این حمله ردیابی شود، رایانه قربانی، مقصر به حساب می آید؛ چرا که همه سر نخها به آن ختم می شود.

کاربر رایانه قربانی ممکن است متوجه شود که ISP او دیگر اجازه دسترسی به اینترنت را نمی دهد. با این حال هکری که کنترل این رایانه را به دست گرفته بود، بی هیچ مشقتی به سراغ پارانه های دیگر می رود؛ چرا که او در این حمله هکری از چند رایانه زامبی دیگر استفاده می کند. شاید باور کردنی نباشد که یک هکر می تواند در چنین مواقعی کنترل چند رایانه را در دست بگیرد. برای مثال در پیگیری یکی از همین حمله ها، هکری با استفاده از تنها یک رایانه کنترل ۱/۵ میلیون رایانه دیگر را به دست آورده بود!

هک کردن رایانه قربانی

هکرها از نقاط ضعف سیستم عامل رایانه ها استفاده می کنند و با کمک برنامه های کوچک، رایانه های قربانیان را تحت کنترل می گیرند. ممکن است تصور کنید که این هکرها همه چیز را راجع به رایانه و اینترنت می دانند، اما در واقع بیشتر آنها تجربه برنامه نویسی کمی دارند و حتی برخی فقط طرز استفاده از یک برنامه رایانه ای را یاد گرفته اند و از آن استفاده می کنند.

برای آلوده کردن یک رایانه، برنامه مورد نظر باید روی سیستم قربانی نصب شود. هکرها می توانند به وسیله پست الکترونیک، شبکه های P2P و حتی یک سایت ساده این کار را انجام دهند. در بیشتر مواقع، هکر برنامه مورد نظر را در قالب یک فایل عادی مخفی می کند و کاربر قربانی که از همه چیز بی خبر است، گمان می کند در واقع آنچه را خواسته به دست آورده است. با افزایش اطلاعات کاربران درباره حمله های اینترنتی، هکرها نیز برای حمله از راه های جدیدی استفاده می کنند. تا به حال در سایتی وارد شده اید که با ورود به آن پنجره ای خود به خود باز شود و یک دکمه روی آن باشد که روی آن نوشته است "No, Thanks"؟! امیدواریم که روی این دکمه کلیک نکرده باشید؛ چرا که این دکمه ها معمولاً یک طعمه هستند. با فشار دادن آن دکمه، به جای این که پنجره مزاحم بسته شود، داندلود برنامه مخرب آغاز می شود.

آنتی ویروس ها باید همیشه به روز باشند تا مؤثر واقع شوند.

برنامه های فایروال نیز از اهمیت بالایی برخوردارند. این برنامه ها از رد و بدل اطلاعات ناشناس از درگاه های شبکه شما جلوگیری می کنند. معمولاً هر سیستم عامل دارای یک سرویس فایروال است و همین سرویس جوابگوی نیازهای شماست. اما می توانید برای امنیت بیشتر از برنامه های موجود برای سیستم عامل خود استفاده کنید.

همچنین شما باید برای رایانه تان یک کلمه عبور امن درست کنید. حدس زدن این رمز عبور نباید کار آسانی باشد. هر چند استفاده از کلمه های عبور برای حساب های مختلف در سایتها و برنامه های مختلف و به خاطر سپردن همه آنها ممکن است کار دشواری باشد، اما این موضوع امنیت سیستم شما را چند برابر می کند.

اگر رایانه شما آلوده و به یک رایانه زامبی تبدیل شده است، راه های کمی برای بهبود اوضاع پیش رو دارید. اگر اطلاعات کافی در زمینه رایانه ندارید، بهتر است کار را به یک متخصص واگذار کنید. اما اگر به چنین شخصی دسترسی ندارید، می توانید با استفاده از یک برنامه آنتی ویروس، ارتباط هکر را با رایانه تان قطع کنید. متأسفانه بعضی اوقات تنها راه، پاک کردن اطلاعات موجود روی رایانه و نصب مجدد سیستم عامل است. همچنین بهتر است به طور منظم از اطلاعات هارد دیسک بک آپ بگیرید که در صورت نصب مجدد سیستم عامل اطلاعاتتان را از دست ندهید. به یاد داشته باشید که این فایل های پشتیبانی باید به طور منظم با آنتی ویروس اسکن شوند و از پاک بودن آنها اطمینان حاصل کنید. با به کار بردن این دستورالعمل ها می توانید با خاطری آسوده رایانه خود را در مقابل حمله ها محافظت کنید.

منبع: www.howstuffworks.com

اختیار هکر قرار دهد تا او دستوراتش را به رایانه هک شده منتقل کند. وقتی برنامه به این مرحله برسد، هکر تقریباً می تواند به همه اهدافش دست یابد. اگر در این مرحله کاربر از حضور هکر با خبر شود، ممکن است هکر یکی از رایانه های زامبی را از دست بدهد.

جلوگیری از حمله

برای جلوگیری از آلوده شدن، همیشه باید از سیستم خود حفاظت کنید. از سوی دیگر باید توجه داشته باشید که تقویت امنیت سیستم تنها قسمتی از حفاظت است. شما باید در محیط اینترنت نیز با احتیاط رفتار کنید. استفاده از یک نرم افزار آنتی ویروس یک ضرورت مطلق است. شما می توانید یک آنتی ویروس تجاری مانند McAfee VirusScan را خریداری یا یک آنتی ویروس مجانی مانند AVG را داندلود کنید، اما همیشه در نظر داشته باشید که آنتی ویروس شما باید فعال و به روز باشد. به عبارتی دیگر، این که شما از چه آنتی ویروسی استفاده می کنید اهمیتی چندانی ندارد. مهم این است که آنتی ویروس شما همیشه به روز باشد و از سیستم تان محافظت کند.

همچنین شما باید یک نرم افزار ضد

جاسوسی نیز نصب کنید. این نرم افزارها الگوی انتقال داده های شما را در اینترنت تحت نظر می گیرند. حتی بعضی از آنها فعالیت شما در سیستم عامل را نیز کنترل می کنند و با شناسایی یک فعالیت غیرعادی در دستگاه شما، جلوی آن را می گیرند. این برنامه ها نیز مانند

در مرحله بعد، برنامه ای که در نرم افزار قربانی قرار گرفته است، باید فعال شود. معمولاً کاربر فکر می کند که یک فایل عادی داندلود کرده است و آن را باز می کند و برنامه مخفی در آن اجرا می شود. ممکن است این فایل با پسوند MPEG باشد و مانند یک عکس به نظر آید یا یک پسوند شناخته شده دیگر باشد. وقتی کاربر این فایل را باز می کند، در ابتدا به نظر می آید که فایل مورد نظر خراب است یا هیچ اتفاقی رخ نمی دهد. این موضوع برای بعضی افراد که اطلاعات رایانه ای دارند، می تواند یک هشدار باشد؛ بنابراین برای جلوگیری از آلوده شدن به ویروس، می توانند با استفاده از یک آنتی ویروس، رایانه را پاکسازی کنند. اما متأسفانه بعضی دیگر که اطلاعات چندانی ندارند گمان می کنند که فایل مورد نظر درست داندلود نشده است و کار خاصی برای پاکسازی انجام ندهند.

با فعال شدن برنامه مخرب، آن به یکی از برنامه های سیستم عامل وصل می شود و به این ترتیب هر وقت رایانه قربانی روشن شود، برنامه هکر نیز فعال می شود. البته هکرها همیشه

برنامه سیستمی برای این کار استفاده نمی کنند، تا پراحتی شناسایی نشوند و تشخیص آن برای کاربر و برنامه های ضد جاسوسی دشوارتر شود. برنامه مخرب می تواند به ۲ صورت فعالیت کند. این برنامه ممکن است حاوی دستوراتی باشد که فرمان های لازم را در زمانی مشخص اجرا کند یا ممکن است کنترل رایانه قربانی را در

