دوشنبه 30 آبان 1390 - 07:57

چگونگي كنترل سيستم توسط هكر

هكرها از نقاط ضعف سيستم‌عامل رايانه‌ها استفاده مي‌كنند و با كمك برنامه‌هاي كوچك، رايانه‌هاي قربانيان را تحت كنترل مي‌گيرند.

جام جم آنلاين: هكرها از نقاط ضعف سيستم‌عامل رايانه‌ها استفاده مي‌كنند و با كمك برنامه‌هاي كوچك، رايانه‌هاي قربانيان را تحت كنترل مي‌گيرند.
تصور كنيد اينترنت يک شهر است و اين شهر پر از مكان‌هاي زيبا و گوناگون و همچنين مكان‌هاي خطرناک.

در اين شهر هر كس لزوما آن كسي نيست كه ادعا مي‌كند، حتي شما! ممكن است متوجه شويد بي‌آن‌كه بدانيد كارهاي غير قانوني مرتكب شده‌ايد.

اين يعني كارهايي كه انجام مي‌دهيد تحت كنترل شما نيست و نبوده و احتمال دارد حتي بعد از اين نيز نتوانيد جلوي آن را بگيريد.

يک رايانه زامبي (Zombie)، رايانه‌اي است كه فرمان‌هاي شخص ديگري را اجرا مي‌كند، بدون اين كه كاربران خبر داشته باشند و كنترل آن را به دست بگيرند.

يک هكر كه قصد انجام كارهاي غيرقانوني دارد، ممكن است از يک رايانه ديگر براي انجام خرابكاري‌هايش استفاده كند، بدون اين كه كاربر آن رايانه دخالتي در آنها داشته باشد.

در اين مواقع كاربر قرباني بي‌خبر از اتفاق‌هاي رخ داده، فقط با اين تصور كه سرعت پردازش رايانه‌اش بشدت كاهش يافته، مواجه مي‌شود.

هكرها از اين رايانه‌ها براي فرستادن اطلاعات يا حمله به سايت‌ها و سرورها استفاده مي‌كنند و در نتيجه اگر اين حمله ردياببي شود، رايانه قرباني، مقصر به حساب مي‌آيد؛ چرا كه همه سرنخ‌ها به آن ختم مي‌شود.

كاربر رايانه قرباني ممكن است متوجه شود كه ISP او ديگر اجازه دسترسي به اينترنت را نمي‌دهد.

با اين حال هكري كه كنترل اين رايانه را به دست گرفته بود، بي هيچ مشقتي به سراغ يارانه‌هاي ديگر مي‌رود چرا كه او در اين حمله هكري از چند رايانه زامبي ديگر استفاده مي‌كند.

شايد باور كردني نباشد كه يک هكر مي‌تواند در چنين مواقعي كنترل چند رايانه را در دست بگيرد. براي مثال در پيگيري يكي از همين حمله‌ها، هكري با استفاده از تنها يک رايانه كنترل يك ونيم ميليون رايانه ديگر را به دست آورده بود!

هک كردن رايانه قرباني

هكرها از نقاط ضعف سيستم‌عامل رايانه‌ها استفاده مي‌كنند و با كمك برنامه‌هاي كوچك، رايانه‌هاي قربانيان را تحت كنترل مي‌گيرند.

ممكن است تصور كنيد كه اين هكرها همه چيز را راجع به رايانه و اينترنت مي‌دانند، اما در واقع بيشتر آنها تجربه برنامه‌نويسي كمي‌دارند و حتي برخي فقط طرز استفاده از يک برنامه رايانه‌اي را ياد گرفته‌اند و از آن استفاده مي‌كنند.

براي آلوده كردن يک رايانه، برنامه مورد نظر بايد روي سيستم قرباني نصب شود. هكرها مي‌توانند به وسيله پست الكترونيک، شبكه‌هاي P2P و حتي يک سايت ساده اين كار را انجام دهند.

در بيشتر مواقع، هكر برنامه مورد نظر را در قالب يک فايل عادي مخفي مي‌كند و كاربر قرباني كه از همه چيز بي‌خبر است، گمان مي‌كند در واقع آنچه را خواسته به دست آورده است.

با افزايش اطلاعات كاربران درباره حمله‌هاي اينترنتي، هكرها نيز براي حمله از راه‌هاي جديدي استفاده مي‌كنند.

تا به حال در سایتی وارد شده‌اید که با ورود به آن پنجره‌ای خود به خود باز شود و یک دگمه روی آن باشد که روی آن نوشته است "No, Thanks"؟ امیدواریم که روی این دکمه کلیک نکرده باشید؛ چراکه این دگمه‌ها معمولا یک طعمه هستند. با فشار دادن آن دگمه، به جای این که پنجره مزاحم بسته شود، دانلود برنامه مخرب آغاز می‌شود.

در مرحله بعد، برنامه‌ای که در نرم‌افزار قربانی قرار گرفته است، باید فعال شود. معمولا کاربر فکر می‌کند که یک فایل عادی دانلود کرده است و آن را باز می‌کند و برنامه مخفی در آن اجرا می‌شود.

ممکن است این فایل با پسوند MPEG باشد و مانند یک عکس به‌نظر آید یا یک پسوند شناخته شده دیگر باشد. وقتی کاربر این فایل را باز می‌کند، در ابتدا به نظر می‌آید که فایل مورد نظر خراب است یا هیچ اتفاقی رخ نمی‌دهد.

این موضوع برای بعضی افراد که اطلاعات رایانه‌ای دارند، می‌تواند یک هشدار باشد؛ بنابراین برای جلوگیری از آلوده شدن به ویروس، می‌توانند با استفاده از یک آنتی‌ویروس، رایانه را پاکسازی کنند اما متأسفانه بعضی دیگر که اطلاعات چندانی ندارند گمان می‌کنند که فایل مورد نظر درست دانلود نشده است و کار خاصی برای پاکسازی انجام ندهند.

با فعال شدن برنامه مخرب، آن به یکی از برنامه‌های سیستم‌عامل وصل می‌شود و به این ترتیب هر وقت رایانه قربانی روشن شود، برنامه هکر نیز فعال می‌شود البته هکرها همیشه از یک برنامه سیستمی برای این کار استفاده نمی‌کنند، تا براحتی شناسایی نشوند و تشخیص آن برای کاربر و برنامه‌های ضدجاسوسی دشوارتر شود.

برنامه مخرب می‌تواند به دو صورت فعالیت کند. این برنامه ممکن است حاوی دستوراتی باشد که فرمان‌های لازم را در زمانی مشخص اجرا کند یا ممکن است کنترل رایانه قربانی را در اختیار هکر قرار دهد تا او دستوراتش را به رایانه هک شده منتقل کند.

وقتی برنامه به این مرحله برسد، هکر تقریبا می‌تواند به همه اهدافش دست یابد اگر در این مرحله کاربر از حضور هکر با خبر شود، ممکن است هکر یکی از رایانه‌های 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 نرم‌افزار آنتی‌ویروس یک ضرورت مطلق است. شما می‌توانید یک آنتی‌ویروس تجاری مانند McAfee VirusScan را خریداری یا یک آنتی‌ویروس مجانی مانند AVG را دانلود کنید، اما همیشه در نظر داشته باشید که آنتی‌ویروس شما باید فعال و به‌روز باشد.

به عبارتی دیگر، این که شما از چه آنتی‌ویروسی استفاده می‌کنید اهمیتی چندانی ندارد. مهم این است که آنتی‌ویروس شما همیشه به‌روز باشد و از سیستم‌تان محافظت کند.

همچنین شما باید یک نرم‌افزار ضد جاسوسی نیز نصب کنید. این نرم‌افزارها الگوی انتقال داده‌های شما را در اینترنت تحت نظر می‌گیرند حتی بعضی از آنها فعالیت شما در سیستم‌عامل را نیز کنترل می‌کنند و با شناسایی یک فعالیت غیرعادی در دستگاه شما، جلوی آن را می‌گیرند. این برنامه‌ها نیز مانند آنتی‌ویروس‌ها باید همیشه به‌روز باشند تا مؤثر واقع شوند.

برنامه‌های فایروال نیز از اهمیت بالایی برخوردارند. این برنامه‌ها از رد و بدل اطلاعات ناشناس از درگاه‌های شبکه شما جلوگیری می‌کنند.

معمولا هر سیستم‌عامل دارای یک سرویس فایروال است و همین سرویس جوابگوی نیازهای شماست. اما می‌توانید برای امنیت بیشر از برنامه‌های موجود برای سیستم‌عامل خود استفاده کنید.

همچنین شما باید برای رایانه‌تان یک کلمه عبور امن درست کنید. حدس زدن این رمز عبور نباید کار آسانی باشد.

هر چند استفاده از کلمه‌های عبور برای حساب‌های مختلف در سایت‌ها و برنامه‌های مختلف و به خاطر سپردن همه آنها ممکن است

کار دشواری باشد، اما این موضوع امنیت سیستم شما را چندبرابر می‌کند.

اگر رایانه شما آلوده و به یک رایانه زامبی تبدیل شده است، راه‌های کمی‌برای بهبود اوضاع پیش‌رو دارید. اگر اطلاعات کافی در زمینه رایانه ندارید، بهتر است کار را به یک متخصص واگذار کنید اما اگر به چنین شخصی دسترسی ندارید، می‌توانید با استفاده از یک برنامه آنتی‌ویروس، ارتباط هکر را با رایانه‌تان قطع کنید.

متأسفانه بعضی اوقات تنها راه، پاک کردن اطلاعات موجود روی رایانه و نصب مجدد سیستم‌عامل است. همچنین بهتر است به طور منظم از اطلاعات هارد دیسک بک‌آپ بگیرید که در صورت نصب مجدد سیستم‌عامل اطلاعاتتان را از دست ندهید.

به یاد داشته باشید که این فایل‌های پشتیبانی باید به‌طور منظم با آنتی‌ویروس اسکن شوند و از پاک بودن آنها اطمینان حاصل کنید.

با به کار بردن این دستورالعمل‌ها می‌توانید با خاطری آسوده رایانه خود را در مقابل حمله‌ها محافظت کنید.