هکرها با قصد و نیت سوءاستفاده و باج‌گیری از قربانیان دست به سرقت اطلاعات می‌زنند

بازیگران نقش منفی مجازی

| زهرا خلجی |
روزنامه‌نگار

هک عمل شناسایی و سپس بهره‌برداری از نقاط ضعف در یک سیستم یا شبکه کامپیوتری است که معمولا برای دسترسی غیرمجاز به داده‌های شخصی یا سازمانی است. البته هک همیشه یک فعالیت مخرب نیست، اما این اصطلاح به‌دلیل ارتباط آن با جرائم سایبری، بیشتر مفاهیم منفی دارد. پیش از این درباره حملات سایبری که نوعی از هک هستند نوشته‌ایم اما در این مطلب به شکل گسترده‌تری به آن می‌پردازیم.

هکرها چگونه کار می‌کنند؟

هکرها از تکنیک‌های مختلفی برای رسیدن به اهداف خود استفاده می‌کنند. برخی از رایج‌ترین روش‌ها عبارتند از:

رمزهای عبور

هکرها از راه‌های مختلفی برای به‌دست آوردن رمز عبور استفاده می‌کنند. روش آزمون و خطا به‌عنوان یک حمله brute force شناخته می‌شود که هکرها سعی می‌کنند هر ترکیب ممکن را حدس بزنند تا به رمز درست دسترسی پیدا کنند. هکرها همچنین ممکن است از الگوریتم‌های ساده برای تولید ترکیب‌های مختلف حروف، اعداد و نمادها استفاده کنند تا به آنها در شناسایی ترکیب‌های رمز عبور کمک کند. تکنیک دیگر به‌عنوان حمله دیکشنری شناخته می‌شود، برنامه‌ای که کلمات رایج را در فیلدهای رمز عبور وارد می‌کند تا ببیند آیا کار می‌کند یا خیر.

آلوده کردن دستگاه‌ها به بدافزار

هکرها ممکن است برای نصب بدافزار به دستگاه کاربر نفوذ کنند. به‌احتمال زیاد، آنها قربانیان را از طریق ایمیل، پیام‌های فوری و وب‌سایت‌هایی با محتوای قابل دانلود هدف قرار می‌دهند.

بهره‌برداری از شبکه‌های وای فای ناامن

هکرها به جای استفاده از کدهای مخرب برای نفوذ به کامپیوتر شخصی، ممکن است به سادگی از شبکه‌های وای فای استفاده کنند. همه روتر وای فای خود را ایمن نمی‌کنند و این می‌تواند توسط هکرهایی که به‌دنبال اتصال وای فای ناامن هستند مورد سوءاستفاده قرار گیرد. هنگامی که هکرها به شبکه ناامن متصل می‌شوند، فقط باید امنیت اولیه را دور بزنند تا به دستگاه‌های متصل به آن شبکه دسترسی پیدا کنند.

دسترسی به در پشتی

هکرها ممکن است برنامه‌هایی ایجاد کنند که مسیرهای محافظت نشده را در سیستم‌های شبکه و رایانه‌ها جست‌وجو کنند. آنها ممکن است با آلوده کردن یک کامپیوتر یا سیستم با بدافزاری به نام اسب تروا که برای به‌دست آوردن و سرقت داده‌های مهم بدون توجه به قربانی ایجاد شده است، به جایی که فکر می‌کنید امن‌ترین نقطه سیستم شماست دسترسی پیدا کنند.

ساخت کامپیوترهای زامبی

کامپیوتر زامبی یا روبات، کامپیوتری است که هکر می‌تواند از آن برای ارسال هرزنامه یا انجام حملات دی داس (DDoS) استفاده کند. پس از اینکه قربانی یک کد به ظاهر معمولی را روی سیستم خود اجرا می‌کند، یک ارتباط بین کامپیوتر او و سیستم هکر باز می‌شود. سپس هکر می‌تواند رایانه قربانی را مخفیانه کنترل و از آن برای ارتکاب جنایت یا انتشار هرزنامه استفاده کند.

هکرها چه آسیبی می‌توانند به قربانی وارد کنند؟

هک امنیت سایبری می‌تواند یک ویرانی واقعی ایجاد کند. هکرها پس از اینکه از هر تکنیکی برای دسترسی به داده‌ها یا دستگاه‌های شما استفاده کردند، می‌توانند: ■ پول شما را بدزدند و کارت اعتباری و حساب‌های بانکی را به نام خود باز کنند ■ رتبه اعتباری شما را از بین ببرند ■ شماره‌های شناسایی شخصی (PIN) یا کارت‌های اعتباری بیشتری درخواست کنند ■ از طرف شما خرید انجام دهند ■ خودشان یا نام مستعاری را که به‌عنوان کاربر مجاز کنترل می‌کنند اضافه کنند تا استفاده از اعتبار شما آسان‌تر شود ■ پیش‌پرداخت نقدی دریافت کنند ■ از شماره تامین اجتماعی شما سوءاستفاده کنند ■ اطلاعات شما را به دیگران بفروشند که از آن برای اهداف مخرب استفاده می‌کنند ■ فایل‌های مهم کامپیوتر شما را حذف کنند یا به آنها آسیب بزنند ■ اطلاعات شخصی حساس را به‌دست آورند و آن را به اشتراک بگذارند یا تهدید کنند که آن را به اشتراک می‌گذارند.

هکرها چه کسانی هستند و چرا هک می‌کنند؟

شاید برای بیشتر مردم این سؤال پیش بیاید که چرا برخی افراد سعی می‌کنند به سیستم‌ها و اطلاعات آنها دست پیدا کنند. انگیزه‌های هک متفاوت است. برخی از رایج‌ترین‌ها عبارتند از:

پول

بزرگ‌ترین انگیزه اغلب هکرها سود مالی است. هکرها می‌توانند با سرقت رمزهای عبور شما، دسترسی به اطلاعات بانک یا کارت اعتباری شما، نگهداری اطلاعات شما به‌عنوان باج، یا فروش داده‌های شما به سایر هکرها یا در وب تاریک درآمد کسب کنند.

جاسوسی شرکتی

گاهی اوقات، هکرها با سرقت اسرار تجاری از شرکت‌های رقیب انگیزه می‌گیرند. جاسوسی شرکتی نوعی هک است که برای دسترسی به داده‌های طبقه‌بندی شده یا مالکیت معنوی به‌منظور کسب مزیت رقابتی نسبت به رقبای شرکتی طراحی شده است.

جاسوسی سیاسی

دولت‌ها می‌توانند از هکرها برای مقاصد سیاسی استفاده کنند. این ممکن است شامل سرقت داده‌های طبقه‌بندی شده، مداخله در انتخابات، دسترسی به اسناد دولتی یا نظامی، یا تلاش برای ایجاد ناآرامی سیاسی باشد.

انتقام

گاهی اوقات، هکرها با خشم تحریک می‌شوند؛ تمایل به انتقام‌گرفتن از افراد یا سازمان‌هایی که احساس می‌کنند به‌نحوی به آنها ظلم کرده‌اند.

نافرمانی مدنی

هک می‌تواند نوعی نافرمانی مدنی باشد. برخی از هکرها از مهارت‌های خود برای ترویج یک برنامه سیاسی خاص یا جنبش اجتماعی استفاده می‌کنند.

بدنامی

هکرها می‌توانند با احساس موفقیت، یعنی شکستن «سیستم» انگیزه داشته باشند. آنها می‌توانند با ایجاد حس رقابت، یکدیگر را به چالش بکشند و با انجام این کار از سوی سایر رقبا به رسمیت شناخته شوند. رسانه‌های اجتماعی به آنها بستری می‌دهند تا درباره فعالیت‌هایشان به‌خود ببالند.