معرفی شایع ترین حملات سایبری در دنیا

شرکت رهاکو

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

فهرست

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

انواع حملات متداول سایبری کدامند؟

جرائم سایبری روز به روز بیشتر می‌شود و هکرها در حال قوی‌تر شدن هستند. حملات سایبری به دلایل مختلف و به روش‌های مختلفی انجام می‌شوند. مجرمان سایبری با برنامه ریزی این حملات به دنبال سو استفاده از آسیب پذیری‌ها در سیاست‌ها و فناوری‌های امنیتی سازمان‌ها هستند. روش ها و راه‌های مختلفی برای حملات سایبری وجود دارد که مهاجم می‌تواند با استفاده از آن‌ها به یک سیستم نفوذ کند. البته بیشتر این حملات سایبری بر تکنیک‌های مشابهی متکی هستند که در این مقاله به معرفی آن‌ها می‌پردازیم.

حملات اسکریپت بین سایتی (XSS)

حملات اسکریپت بین سایتی کاملا شبیه حمله تزریق کد اس کیو ال هستند؛ اگرچه به جای استخراج داده‌ها از پایگاه داده، برای آلوده کردن بازدید کنندگان وبسایت استفاده می‌کند. یک مثال ساده در این مورد بخش نظرات در وبسایت‌هاست. حملات XSS زمانی اتفاق می‌افتد که مهاجم از یک برنامه تحت وب برای ارسال کدهای مخرب (عموما در قالب یک اسکریپت جانبی مرورگر) برای کاربر استفاده می‌کند. عواملی که باعث موفقیت این حملات می‌شوند بسیار گسترده هستند و در هر جایی که یک برنامه تحت وب بدون اعتبارسنجی یا رمزگذاری استفاده شود، رخ خواهد داد.

اسکریپت به معنی فایل‌هایی است که بر روی هاست قابل نصب و راه اندازی هستند و یک وظیفه مشخص را تحت وب یا سرور انجام می‌دهند. مهاجم می‌تواند از XSS برای ارسال یک اسکریپت مخرب به کاربر استفاده کند. کاربر خبر ندارد که اسکریپت قابل اعتماد نیست و آن را اجرا می‌کند. این اسکریپت مخرب می‌تواند به کوکی‌ها یا سایر اطلاعات حساسی که در تاریخچه مرورگر وجود دارد، دسترسی داشته باشد. حتی می‌توانند محتوای صفحه HTML را بازنویسی کنند!

حمله درایو

حمله drive-by-download جایی است که دستگاه کاربر هنگام بازدید از وب سایت با بدافزار آلوده می‌شود. وب سایت مورد نظر می‌تواند وب سایتی باشد که مستقیما توسط مهاجم کنترل می‌شود یا در معرض خطر قرار گرفته است. در برخی موارد، بدافزار در محتوایی مانند بنرها و تبلیغات ارائه می‌شود. این روزها کیت‌هایی در دسترس هستند که به هکرهای تازه کار اجازه می‌دهند تا به راحتی وب سایت‌های مخرب را راه اندازی کنند یا محتوای مخرب را با روش‌های دیگر توزیع نمایند.

Cryptojacking

مجرمان سایبری، رایانه یا دستگاه کاربر را به خطر می‌اندازند و از آن برای استخراج ارزهای دیجیتال مانند بیت کوین استفاده می‌کنند. این روش به اندازه سایر حملات شناخته شده نیست، اما نباید آن را دست کم گرفت. سازمان‌ها دید خوبی به این نوع حمله ندارند، یعنی هکر می‌تواند از منابع ارزشمند یک شبکه برای استخراج ارز دیجیتال استفاده کند؛ بدون این که سازمان هیچ اطلاعی از آن داشته باشد.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

سازش ایمیل تجاری (BEC)

حملات BEC یکی از مضرترین حملات سایبری است و مهاجم در این روش افراد خاصی را هدف قرار می‌دهد. معمولا کارمندی که مجوز تراکنش‌های مالی را دارد فریب می‌دهد تا پول را به حساب مورد نظر منتقل کند. حملات BEC شامل برنامه ریزی و تحقیق است. به عنوان مثال هرگونه اطلاعات در مورد مدیران، کارکنان، مشتریان، شرکای تجاری سازمان هدف به مهاجم کمک می‌کند. او با استفاده از این اطلاعات کارمند را متقاعد می‌کند که وجه را به حساب مد نظر تحویل دهد.

حملات با هوش مصنوعی

استفاده از هوش مصنوعی برای راه اندازی حملات سایبری پیچیده کمی نگران کننده است زیرا هنوز مشخص نیست این حملات چه تاثیراتی داشته باشند. مهم‌ترین حمله مبتی بر هوش مصنوعی که تا به امروز مورد بررسی قرار گرفته استفاده از بات نت‌های مجهز به هوش مصنوعی است که از ماشین‌ها برای انجام یک حمله DDoS استفاده می‌کنند. (botnet برای اجرای حملات سایبری مانند DDOS، بر علیه یک هدف یا سرقت اطلاعات حساس استفاده می‌شود).

نرم افزار مجهز به هوش مصنوعی نشان می‌دهد که چه نوع رویکردهایی مناسب ترند و روش‌های حمله خود را بر همان اساس تطبیق می‌دهند. آن‌ها می‌توانند از فیدهای هوشمند برای شناسایی بخش‌های آسیب پذیر نرم افزار و همچنین اسکن خود سیستم برای تشخیص آسیب پذیری‌های احتمالی استفاده کنند.

حمله تزریق SQL

یک حمله تزریقی ساختاریافته (SQL) زمانی رخ می‌دهد که هکر، یک استاندارد SQL را دستکاری می‌کند. این حمله با تزریق یک کد مخرب به جعبه جستجوی آسیب پذیر وب‌سایت انجام می‌شود و در نتیجه باعث می‌شود سرور اطلاعات مهمی را فاش کند. این حمله باعث می‌شود که مهاجم اطلاعات موجود در پایگاه داده را مشاهده، ویرایش و حذف کند. همچنین مهاجمان می‌توانند از این طریق از حقوق اداری برخوردار شوند.

حمله شنود Eavesdropping attack

حمله استراق سمع که گاهی اوقات به آن snooping نیز می‌گویند، حمله‌ای است که به دنبال ارتباطات شبکه نا امن، برای رهگیری و دسترسی به داده‌ها در سراسر شبکه ارسال می‌شود. حمله استراق سمع زمانی رخ می‌دهد که هکر قصد دارد، داده‌هایی که بین دو دستگاه منتقل می‌شود را حذف کند یا تغییر دهد. استراق سمع، همچنین به عنوان sniffing یا snooping شناخته می‌شود و برای دسترسی به داده‌های میان دستگاه‌ها به ارتباطات ناامن شبکه متکی است.

برای توضیح بیشتر تعریف حمله استراق سمع بهتر است بگوییم این حمله زمانی اتفاق می‌افتد که کاربر به شبکه‌ای لدون رمزگذاری متصل می‌شود و داده‌های تجاری حساس را برای همکار ارسال می‌کند. داده‌ها از طریق یک شبکه باز منتقل می‌شوند که به مهاجم این فرصت را می‌دهد تا از این آسیب پذیری سو استفاده کند. تشخیص حملات استراق سمع اغلب دشوار است.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

برخلاف سایر حملات سایبری، ممکن است وجود باگ یا یک دستگاه شنود بر عملکرد دستگاه‌ها و شبکه‌ها تاثیر چندانی نداشته باشد.

بد افزار Malware

اصطلاح "بدافزار" انواع مختلفی از حملات را در بر دارد که شامل: نرم افزارهای جاسوسی و ویروس‌ها می‌باشد. بدافزار از یک ویژگی آسیب پذیر برای نفوذ به شبکه استفاده می‌کند. زمانی که کاربر روی Link خطرناک یا پیوست ایمیل کلیک می‌کند، نرم‌افزار مخرب در داخل سیستم نصب می‌شود و اطلاعات را استخراج می‌کند. بدافزارها و فایل‌های مخرب داخل یک سیستم کامپیوتری می‌توانند:

- دسترسی به اجزای حیاتی شبکه را ممنوع کنند.
- اطلاعات را از هارد دیسک بازیابی کنند.
- سیستم را مختل یا حتی آن را غیرفعال کنند.

رایج‌ترین انواع بدافزارها عبارتند از:

ویروس‌ها: ویروس‌ها برنامه‌ها را آلوده می‌کنند. ویروس خودش را تکثیر می‌کند و سایر کدها را در سیستم کامپیوتری آلوده می‌کند. همچنین می‌توانند کد را در خود اجرا کنند، و یا با ایجاد یک فایل ویروسی با پسوند exe خود را در یک فایل مرتبط جای دهند. در این صورت یک طعمه که حامل ویروس است ایجاد می‌شود.

تروجان‌ها: تروجان برنامه‌ای است که با اهداف مخرب در داخل یک برنامه دیگر پنهان می‌شود. برخلاف ویروس‌ها، تروجان خودش را تکثیر نمی‌کند و معمولا برای ورود از روش‌های پنهان استفاده می‌شود.

کرم‌ها: کرم‌ها برخلاف ویروس‌ها به میزبان حمله نمی‌کنند، زیرا برنامه‌های مستقلی هستند که در شبکه‌ها و رایانه‌ها منتشر می‌شوند. کرم‌ها اغلب از طریق پیوست‌های ایمیل نصب می‌شوند و یک نسخه از خود را برای هر مخاطبی که در لیست ایمیل وجود دارد، ارسال می‌کنند.

باج افزار: نوعی بدافزار که دسترسی به داده‌ها را قطع می‌کند و کاربر را تهدید به انتشار یا حذف داده‌ها می‌کند، تا بتواند باج بگیرد. باج افزار پیشرفته داده‌های کاربر را رمزگشایی می‌کند تا بدون کلید رمزگشایی غیر ممکن باشد.

جاسوس‌افزار: نوعی برنامه نصب شده برای جمع‌آوری اطلاعات در مورد کاربران و سیستم‌هاست. مهاجم می‌تواند از اطلاعات خاصی برای باج خواهی استفاده کند یا سایر برنامه‌های مخرب را از وب دانلود و بر کامپیوتر کاربر نصب کند.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

نتیجه گیری

حملات سایبری زمانی است که فرد یا سازمانی عمدا و با سو قصد به سیستم اطلاعاتی یک فرد یا سازمان خاص نفوذ کند. تخریب داده‌ها به عنوان یک هدف در نظر گرفته می‌شود؛ در حالی که معمولا یک هدف اقتصادی برای این حملات وجود دارد. حملات سایبری زیادی وجود دارد اما به اندازه همان حملات سایبری راهکار یا روش‌های برای جلوگیری هم وجود دارد.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net