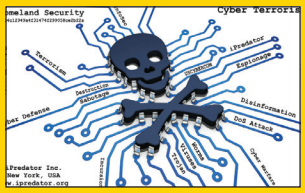
جنگ به سبک سایبری



در سال‌های اخیر جنگ سایبری به یک جنگ متداول بین دولت‌های متخاصم تبدیل شده است. در این نوع جنگ از تکنیک‌های دفاع و حمله به اطلاعات و شبکه‌های کامپیوتری در فضای مجازی استفاده می‌شود که اغلب از طریق یک کارزار سایبری یا مجموعه‌ای از کمپین‌های مرتبط رخ می‌دهد. این کار توانایی حریف را در زیرساخت‌ها از بین می‌برد، ضمن اینکه از ابزارهای جنگی فناورانه برای حمله به سامانه‌های مهم رایانه‌ای حریف استفاده می‌کند. از طرف دیگر، سایبرتروریسم استفاده از ابزارهای شبکه رایانه‌ای برای خاموش کردن زیرساخت‌های مهم ملی (مانند انرژی، حمل و نقل، عملیات دولتی) یا اجبار یا ارعاب یک دولت یا جمعیت غیرنظامی است. این یعنی اینکه نتیجه نهایی هم جنگ سایبری و هم سایبرتروریسم یکسان است تا به زیرساخت‌های مهم و سامانه‌های کامپیوتری که در محدوده فضای مجازی با یکدیگر ارتباط دارند، آسیب برساند.

عوامل حمله‌های سایبری

۳عامل در ایجاد حمله‌های سایبری علیه یک دولت یا یک فرد نقش دارند: عامل ترس، عامل تماشایی و عامل آسیب‌پذیری. ضریب تماشایی، معیاری از خسارت واقعی حاصل از حمله است، به این معنی که این حمله ضرر مستقیم ایجاد می‌کند (معمولاً از دست‌دادن دسترسی یا از دست‌دادن درآمد) و تبلیغات منفی را منجر می‌شود. در ۸ فوریه ۲۰۰۰، یک حمله انکار سرویس (DDOS) به شدت ترافیک مراجعه به بسیاری از سایت‌های مهم از جمله Amazon , Buy.com , CNN و eBay را کاهش داد.

این در حالی است که عامل آسیب‌پذیری از چگونگی آسیب‌پذیری یک سازمان یا سازمان دولتی در برابر حمله‌های سایبری سوءاستفاده می‌کند. سازمان‌های بدون سامانه تعمیر و نگهداری ممکن است روی سرورهای قدیمی کار کنند که از سامانه‌های به‌روز آسیب‌پذیرتر هستند. یک سازمان می‌تواند در برابر حمله DDOS آسیب‌پذیر باشد یا یک نهاد دولتی در صفحه وب خود متوجه حمله سایبری شود. حمله به شبکه رایانه‌ای، یکپارچگی یا صحت اطلاعات را مختل می‌کند که معمولاً از طریق کد مخرب که منطق برنامه و داده‌ها را کنترل می‌کند، منجر به خطا در خروجی می‌شود.

عمل هک از زمان پیدایش تا اکنون از یک فعل مثبت به فعالیتی کاملا مجرمانه تبدیل شده است

تاریخچه هک

در حال که هک کردن این روزها بیشتر مفهومی منفی دارد اما باید بدانید که همیشه اینطور نبوده است. در روزهای اولیه فعالیت به نام هک کامپیوتر، هکرها به‌عنوان متخصصان فناوری در نظر گرفته می‌شدند که انگیزه اصلی آنها شخصی‌سازی و بهینه‌سازی سیستم‌ها بود. همانطور که جرائم سایبری تکامل یافت و پیچیده‌تر و گسترده‌تر شد، هک هم بیشتر با فعالیت‌های مخرب همراه شد. مروری کوتاه داریم بر تاریخچه هک در جهان.

۱۹۶۰

اصطلاح «هک» با اعضای باشگاه راه‌آهن مدل فناوری MIT آمریکا که مجموعه‌های قطارهای پیشرفته‌شان اسباب‌بازی را برای تغییر عملکردشان «هک» می‌کردند، مرتبط شد. هکرهای اولیه به این موضوع علاقه‌مند بودند که چگونه می‌توانند محدودیت‌های برنامه‌های موجود را کشف و آزمایش کنند. تلاش‌های آنها اغلب نتیجه داد زیرا برنامه‌هایی بهتر از برنامه‌های موجود تولید کردند.

۱۹۷۰

هک کامپیوتر در دهه ۱۹۷۰ادامه یافت اما با هک تلفنی متنوع شد. هکرهای تلفن که به «phreakers» نیز معروف هستند، سعی کردند از ویژگی‌های عملیاتی در شبکه سوئیچینگ تلفن که در آن زمان تازه الکترونیکی شده بود سوءاستفاده کنند. با این کار آنها شبکه تلفنی را فریب دادند و تماس‌های طولانی مدت رایگان برقرار کردند.

۱۹۸۰

در دهه ۱۹۸۰، کامپیوترهای شخصی دیگر محدود به کسب‌وکارها یا دانشگاه‌ها نبودند بلکه بیشتر در دسترس عموم قرار گرفتند. این افزایش در دسترس‌بودن منجر به افزایش قابل توجه هک شد. ماهیت هک نیز تغییر کرد. پیش از این، هک اغلب در مورد بهبود رایانه‌ها بود، اما نسل جدید تر هکرها عمدتا برای منفعت شخصی، از جمله دزدی نرم‌افزار، ایجاد ویروس‌ها و نفوذ به سیستم‌ها برای سرقت اطلاعات، انگیزه داشتند.

۱۹۹۰

هک واقعاً در دهه ۱۹۹۰با برخی جرائم سایبری و دستگیری‌های معروف به شهرت رسید. هکرهای قابل توجه در این دهه شامل کوین میتنیک، کوین پولسن، رابرت موریس و ولادیمیر لوین بودند که به جرائمی از سرقت نرم‌افزارهای اختصاصی و فریب ایستگاه‌های رادیویی برای به‌دست آوردن اتومبیل‌های گرانقیمت تا راه‌اندازی نخستین کرم رایانه‌ای و اجرای نخستین بانک دیجیتال محکوم شدند.

۲۰۰۰

سازمان‌های دولتی و شرکت‌های بزرگ به‌طور فزاینده‌ای در معرض هک امنیت سایبری قرار گرفتند. قربانیان برجسته شامل مایکروسافت، eBay، Yahoo و آمازون بودند که همگی قربانی حملات Distributed Denial of Service به اختصار دی داس شدند. وزارت دفاع ایالات متحده و ایستگاه فضایی بین‌المللی هر دو توسط یک پسر ۱۵ ساله مورد حمله هکری قرار گرفتند.

۲۰۱۰ ۲۰۲۰

با توجه به اینکه اینترنت در حال حاضر بخش اصلی زندگی روزمره است، هک کردن پیچیده‌تر از همیشه شده است. تهدیدهای سایبری جدید به‌طور منظم ظاهر می‌شوند. در طول این دهه، گروه هکتیویست معروف به Anonymous به شهرت رسید و اسرار دولتی را افاش کرد و جنگ‌های صلیبی دیجیتال را رهبری کرد که به اعتقاد آنها منافع عمومی را بیشتر می‌کرد. دولت‌ها، شرکت‌های بزرگ و غول‌های رایانه‌ای در واکنش به هک بیوست‌ها و افزایش جرائم سایبری، سخت تلاش کردند سیستم‌های خود را بهبود بخشند. البته کارشناسان امنیت سایبری به نوآوری خود ادامه می‌دهند تا یک قدم جلوتر از هکرها باشند.