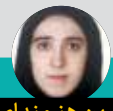
طبق آمار Chainanalysis، حدود ۳۵۰ میلیون دلار به وسیله ارزهای دیجیتال در سال ۲۰۲۰ باج داده شده است اما در قانون آمریکا کسب و کارها حملات سایبری را فقط در صورتی که اطلاعات خصوصی کاربران در خطر باشد می‌توانند گزارش کنند

حملات باج افزارها سال گذشته ۳۰۰ درصد رشد داشته است

باج‌های میلیون دلاری



شیرین هنرمنداصل
روزنامه‌نگار

در سال‌های اخیر ارزهای دیجیتال به‌ویژه بیت‌کوین به ابزاری کلیدی در جرایم آنلاین تبدیل شده‌اند. تاریخ فناوری پر از اتفاقات ناخواسته و عواقب پرحاشیه است.گرچه ارزهای دیجیتال برای واسطه بودن در پرداخت‌های مربوط به حملات باج‌افزاری ساخته نشده‌اند، ولی به‌سرعت به یک ابزار اساسی برای جرایم آنلاین تبدیل شده‌اند. باج‌افزارها گونه‌ای از بدافزارها هستند و تا زمانی که قربانی،پول درخواست شده را به هکرها پرداخت نکند، ارتباط کامپیوتر با شبکه را مسدود می‌کند. با وجود تلاش دولت‌ها برای کنترل ارزهای دیجیتال و حذف نقش آنها در پرداخت‌های مربوط به حملات باج‌افزاری، این حملات هنوز متوقف نشده است. طبق آمار Chainanalysis، حدود ۳۵۰ میلیون دلار به وسیله ارزهای دیجیتال در سال ۲۰۲۰ باج داده شده است. جالب است بدانید این رقم رشدی ۳۰۰درصدی نسبت به سال قبلش داشته است. البته شرکت‌های آمریکایی باید طبق قانون، حملات سایبری را فقط در صورتی که اطلاعات خصوصی کاربران در خطر باشد، گزارش کنند. استدلال دولت ایالات متحده این است که ممکن است شرکت‌ها رقم باج‌ها را بیشتر از رقم اصلی اعلام کنند. در ادامه به پرسودترین یا بزرگ‌ترین حملات باج‌افزاری تاریخ خواهیم پرداخت.

حمله به کاسیا در سال ۲۰۲۱

در دوم ژوئن، یک شرکت ارائه کننده خدمات آی تی به نام کاسیا اعلام کرد، باج‌افزاری به نام REvil به سیستم‌هایش حمله کرده است. شرکتی که به کسب‌وکارهای مختلفی خدمات ارائه می‌دهد، یک هدف ایده‌آل برای حمله‌کنندگان به شمار می‌رود، زیرا طبق گزارش رویترز، این حمله توانست مانند دومینو بر ۱۵۰۰شرکت در کشورهای مختلف اثر بگذارد و از چندهزار تا میلیون‌ها دلار درخواست کند.
مشخص نیست چه تعداد از این ۱۵۰۰شرکت مبلغ درخواستی را پرداخت کرده‌اند ولی Revil از کاسیا خواست ۷۰میلیون دلار به‌وسیله بیت‌کوین پرداخت کند. البته کاسیا از پرداخت خودداری کرد و با اف‌بی‌آی و پلیس سایبری آمریکا همکاری کرد. در ۲۱جولای۲۰۲۱، کاسیا توانست کلید جهانی را به دست آورد و آن را بین شرکت‌هایی که قربانی حمله بودند، پخش کرد.

در ۳۱می۲۰۲۱، ح
تأمین‌کنندگار
می‌رود، دچا
حمله باعث
کارخانه بزرگ
موقت متوقف
فعالیت‌های
و استرالیا ه
هکرها مبلغی
بیت‌کوین پر
اثرات بیشتر
جلوگیری کن
REvil که حلق
حملات باج‌افز

حم

حمله تروجان ایدز با PC Cyborg در سال ۱۹۸۹

تروجان ایدز که الگوی حملات سال‌های بعدی شناخته می‌شود، اولین باج‌افزار شناخته‌شده تاریخ است. در سال ۱۹۸۹، یک دهه پیش از ساخته شدن بیت‌کوین، یک زیست‌شناس به‌نام جوزف پوپ ۲۰هزار فلاپی‌دیسک را در کنفرانس ایدز سازمان جهانی سلامت در استکهلم پخش کرد. نام این فلاپی دیسک‌ها، اطلاعات مقدماتی درباره ایدز بود که حاوی یک ویروس تروجان بودند و در سیستم‌های ام‌اس‌داس نصب می‌شدند. ویروس تعداد دفعات روشن‌شدن رایانه را می‌شمرد و زمانی که رایانه ۹۰ بار روشن می‌شد، تمام دایرکتوری‌ها و نام فایل‌های رمزگذاری‌شده را مخفی می‌کرد. سپس یک صفحه از شرکت PC Cyborg نمایش داده می‌شد و از کاربران می‌خواست ۱۸۹ دلار را به یک آدرس پستی در پاناما ارسال کنند. فرآیند رمزگشایی ساده بود و محققان امنیتی یک ابزار رایگان برای کمک به قربانیان منتشر کردند.

حمله CryptoWall در سال ۲۰۱۴

Widespread گزارش کرد سیستم‌های رایانه‌ای آلوده‌شده با باج‌افزار Crytowall در سال ۲۰۱۴ مشاهده شده‌است. صاحب رایانه‌های آلوده‌شده نمی‌توانستند به فایل‌های خود دسترسی پیدا کنند. قربانیانی که در سراسر جهان هدف قرار داده شده بودند، باید مبلغی برای برنامه رمزگشایی پرداخت می‌کردند. حمله‌کنندگان از قربانیان می‌خواستند مبلغ را به‌صورت بیت‌کوین به کارت‌های پیش‌پرداخت پرداخت کنند. طبق گفته‌های Help Net Security، این باج‌افزار حدود ۱۸میلیون دلار درآمد کسب کرد. نسخه‌های متفاوتی از Crytowall منتشر شدند که ردیابی باج‌افزار را سخت‌تر می‌کرد.

حمله TeslaCrypt در سال ۲۰۱۵

نمونه‌های اولیه این باج‌افزار در نوامبر ۲۰۱۴ مشاهده شد ولی تا ماه مارس سال بعدی هیچ حمله گسترده‌ای انجام نشد. این باج‌افزار ابتدا گیمرها را هدف قرار می‌داد. پس از آلوده‌کردن رایانه، یک صفحه ظاهر می‌شد و از کاربر می‌خواست ۵۰۰هزار دلار به‌صورت بیت‌کوین برای بازگشایی قفل سیستم بپردازد. منابع دیگری گزارش کردند که این باج‌افزار مبالغی از ۲۵۰هزار دلار تا هزار دلار به‌صورت بیت‌کوین درخواست کرده است. در ماه می ۲۰۱۶، توسعه‌دهندگان TeslaCrypt یک رمزگشایی برای باز کردن رایانه‌های آلوده‌شده منتشر کردند.

حمله باج‌افزار لاکی (Locky) در سال ۲۰۱۶

این باج‌افزار در فوریه سال ۲۰۱۶ توانست تعداد قابل‌توجهی از شبکه‌های رایانه‌ای را هدف قرار دهد. حمله‌ها به وسیله فاکتور ضمیمه‌شده یک ایمیل که در آن فردی ادعا می‌کرد کارمند شرکتی است انجام می‌گرفت. در ۱۶ فوریه سال ۲۰۱۶، تحقیقات Check Point بیش از ۵۰هزار حمله لاکی را در یک روز شناسایی کرد.
لاکی شکل‌های گوناگونی دارد ولی هدف آنها یکی است: قفل فایل‌های رایانه برای مجبور کردن صاحبان آنها به پرداخت مبلغی به وسیله ارزهای دیجیتال و گرفتن ابزاری برای دسترسی دوباره به فایل‌های قفل‌شده. بیشتر قربانیان لاکی در آمریکا به‌ویژه شرکت‌های خدمات‌درمانی بودند ولی کانادا و فرانسه نیز نرخ آلودگی قابل‌توجهی را تجربه کردند.