

جی‌بی‌سی که یکی از بزرگ‌ترین شرکت‌های گوشت در آمریکا به شمار می‌رود، حمله باج‌افزاری شد. این شرکت جی‌بی‌سی فعالیت پنج ساله خود را در آمریکا به صورت موقت متوقف کرد. همچنین این حمله باعث شد تا شرکت را در انگلستان هم مختل کرد. جی‌بی‌اس به به ارزش ۱۱ میلیون به وسیله پرداخت کرد تا از اختلالات و در مغازه‌ها و رستوران‌ها. اف‌بی‌ای این حمله را به های مشهور و ماهر در زمینه رای است، نسبت داد.

حمله به جی‌بی‌سی در سال ۲۰۲۱

در ۷ می ۲۰۲۱، بزرگ‌ترین خط لوله محصولات تصفیه‌شده در آمریکا توسط یک گروه به نام Darkside چهار حمله باج‌افزاری شد. خط لوله کولونیال بیشتر از ۵۵۰۰ مایل را تحت پوشش خود قرار داده است و بیش از ۱۰۰ میلیون گالن و سوخت به صورت روزانه انتقال می‌دهد، بنابراین در روزهای پس از حمله، متوسط قیمت هر گالن گاز برای اولین بار در هفت سال به بیش از سه دلار افزایش یافت. مدیران خط لوله کولونیال به رسانه‌ها گفت: ۴/۴ میلیون دلار به وسیله ارزهای دیجیتال به هکرها پرداخته‌اند. در ۷ ژوئن ۲۰۲۱، وزارت دادگستری آمریکا اعلام کرد بخشی از مبلغ باج را به خط لوله برگردانده است و پلیس سایبری آمریکا توانسته پرداخت را ردیابی کنند و ۲/۳ میلیون دلار آن را به وسیله یک کلید خصوصی برای یک کیف پول ارز دیجیتال پس بگیرد. در نتیجه حمله‌کنندگان توانستند تنها درآمدهای ۲/۱ میلیون دلار از این حمله کسب کنند.

حمله به خط لوله کولونیال در سال ۲۰۲۱

در ۲۸ آوریل ۲۰۲۱، شرکت آلمانی صنایع شیمیایی برنتاگ هدف حمله سایبری گروه Darkside بود. این گروه ۱۵۰ آگیاگابایت از اطلاعات را دزدید و تهدید کرد اگر شرکت مبلغ درخواست شده را نپردازد همه آنها را منتشر خواهد کرد. بعد از مذاکره با مجرمان، برنتاگ ۵/۵ میلیون دلار به جای ۷/۵ میلیون دلار در ۱۱ ماه می پرداخت کرد.

حمله به برنتاگ در سال ۲۰۲۱

در ۲۳ مارس ۲۰۲۱، شرکت CNA Financial که سومین شرکت بزرگ بیمه در آمریکاست، اعلام کرد دچار حمله سایبری شده است. گروهی به نام Phoenix این حمله را با باج‌افزاری به نام Phoenix Locker انجام داد. شرکت بیمه سی‌ان‌ای مجبور شد ۴۰ میلیون دلار در ماه می بپردازد و اطلاعات خود را پس بگیرد. این شرکت درباره جزئیات مذاکره و انتقال پول، ولی بیان کرد تمام سیستم‌هایش به طور کامل تعمیر شده است.

حمله به شرکت بیمه سی‌ان‌ای در سال ۲۰۲۱

حمله باج‌افزار WannaCry در سال ۲۰۱۷

در می ۲۰۱۷، باج‌افزاری به نام WannaCry، رایانه‌های سراسر جهان را از طریق آسیب‌پذیری موجود در رایانه‌های سیستم‌عامل ویندوز هدف قرار داد. یک گروه به نام Shadow Brokers در آوریل ۲۰۱۷، این آسیب‌پذیری را هنگام انتشار گسترده اسناد NSA و ابزار هک فاش کرده بود. گرچه تعداد دقیق قربانیان و اناکرای ناشناخته مانده است، بیش از ۲۰۰ هزار رایانه در سراسر دنیا و حتی در ایران هدف حمله این باج‌افزار قرار گرفتند. در فهرست قربانیان و اناکرای، نام یک شرکت مخابراتی اسپانیایی به نام تلفونیا و هزاران بیمارستان در انگلستان به چشم می‌خورد. سیستم‌های رایانه‌ای در ۱۵۰ کشور تحت تأثیر حمله قرار گرفتند و نزدیک به چهار میلیارد دلار در سراسر جهان از دست رفت. هکرها برای بازگشایی قفل کامپیوترهای قربانیان، به ارزش ۳۰۰ دلار بیت‌کوین درخواست کردند. این مبلغ بعدها به ۶۰۰ دلار افزایش یافت. محققان ادعا کردند با وجود پرداخت مبلغ درخواستی، هیچ کس نتوانست اطلاعات خود را به دست آورد. در فوریه سال ۲۰۲۱، وزارت دادگستری ایالات متحده آمریکا سه برنامه‌نویس در کره شمالی را متهم کرد. از آنجا که هکرها و اناکرای فقط بیت‌کوین دریافت می‌کردند، پس از گذشت سه سال هنوز ردیابی نشده‌اند.

حمله به تراولکس در سال ۲۰۱۹

در جشن سال نوی میلادی، یک شرکت خدمات معامله ارز در لندن به نام تراولکس هدف حمله باج‌افزاری یک گروه به نام Sodnikibi که با نام REVil نیز شناخته می‌شود، قرار گرفت. حمله‌کنندگان با سرعت پنج گیگابایت از اطلاعات مشتریان شامل تاریخ تولد، جزئیات بیمه و اطلاعات کارت بانکی آنها را دزدیدند. تراولکس سایت خود را در ۳۰ کشور غیرفعال کرد تا این حمله باج‌افزاری را مهار کند. مجرمان ابتدا شش میلیون دلار درخواست کردند. پس از مذاکرات، تراولکس ۲/۳ میلیون دلار به وسیله بیت‌کوین که آن زمان این مبلغ برابر با ۲۸۵ بیت‌کوین بود، پرداخت کرد و اطلاعات خود را پس گرفت.

حمله به دانشگاه کالیفرنیا در سال ۲۰۲۰

در سوم ژوئن ۲۰۲۰، دانشگاه کالیفرنیا اعلام کرد به وسیله باج‌افزاری به نام Netwalker در اول ژوئن به سیستم‌های آیتی دانشکده پزشکی حمله کرده‌اند. این مرکز برای یافتن درمانی برای کووید-۱۹ فعالیت می‌کرد. طبق گزارش بی‌بی‌سی، Netwalker حداقل به دو دانشگاه دیگر در سال ۲۰۲۰ حمله کرده و تقاضای باج کرده است. به نظر می‌رسد گروه مجرمانه Netwalker درباره این دانشگاه تحقیق کرده تا درباره وضعیت مالی آن اطلاعاتی به دست آورد. آنها با بیان این که دانشگاه کالیفرنیا سالانه میلیاردها دلار درآمد دارد از دانشگاه خواستند سه میلیون دلار پرداخت کند. بعد از مذاکرات، دانشگاه کالیفرنیا چیزی حدود ۱/۱ میلیون دلار به وسیله ارز دیجیتال بیت‌کوین پرداخت کرد تا این حمله سایبری را مهار کند.

حمله به CWT در سال ۲۰۲۰

در ۳۱ جولای ۲۰۲۰، یک شرکت مسافرتی آمریکایی به نام سی‌دی‌لوتی اعلام کرد سیستم‌هایش هدف حمله باج‌افزاری قرار گرفته و مبلغ باج را پرداخته است. هکرها به وسیله یک باج‌افزار به نام Ragnar Locker این حمله را انجام دادند. آنها اسناد محرمانه همکاری را دزدیدند و ۳۰ هزار کامپیوتر شرکت را از کار انداختند. از آنجا که این شرکت به یک سوم از شرکت‌های فهرست S&P500 خدمات ارائه می‌کند، انتشار اطلاعات دزدیده شده می‌توانست کسب‌وکار شرکت را نابود کند، بنابراین شرکت چند روز قبل از گزارش رویترز، ۴/۵ میلیون دلار به هکرها در ۲۸ جولای پرداخت کرد.