ایران
IRAN PLUS NEWSPAPER

خطرناک‌ترین هک‌های سال ۲۰۲۲

HACKED

میترا جلیلی
روزنامه‌نگار

در عصر دیجیتال که از خرید و آموزش گرفته تا درمان و سفر به اینترنت گره خورده، هکرها و مجرمان سایبری نیز فرصت را غنیمت شمرده و تلاش می‌کنند تا از این وضعیت بیشترین بهره را ببرند. کارشناسان حوزه سایبری تخمین می‌زنند که تا سال ۲۰۲۵ میزان خسارت جرایم سایبری به حدود ۱۰ تریلیون دلار برسد. در سال ۲۰۲۲ نیز همچون سال‌های گذشته بیشترین درصد خسارات و جرایم سایبری به حملات فیشینگ، نشتِ داده و باج‌افزارها اختصاص داشت. اما خطرناک ترین و بزرگ ترین هک‌های سال ۲۰۲۲ کدام بود؟

وانواتو : یکی از بزرگ‌ترین هک‌های سال ۲۰۲۲، حمله باج‌افزاری معروف به وانواتو (Vanuatu) بود. هکرها اول نوامبر ۲۰۲۲، جمهوری «وانواتو» با مجموعه‌ای متشکل از ۸۰ جزیره در اقیانوس آرام را هدف یک حمله سنگین سایبری قرار دادند طوری که تقریباً تمام شبکه‌های دیجیتال دولت از بین رفت. در نتیجه این اتفاق تمام سامانه‌ها ازجمله سیستم‌های اورژانس، ثبت سوابق پزشکی، ثبت وسایل نقلیه، پایگاه‌های اطلاعاتی گواهینامه رانندگی و سیستم‌های مالیاتی از کار افتاد. همه کارهای دیجیتال تا مدت‌ها به‌صورت دستی انجام می‌شد. هرچند عنوان شد که این، یک حمله باج‌افزاری بوده ولی دولت هرگز میزان باج پرداختی به هکرها برای پس گرفتن اطلاعات سرقت شده و همچنین نام گروه هکری یا مجرم پشت این حمله را افشا نکرد.

پرنده آبی در دام هکرها : در ۲۷ جولای سال ۲۰۲۲ توئیتر هدف یک حمله سایبری بزرگ قرار گرفت و سرقت اطلاعات ۵/۴ میلیون حساب کاربری این شبکه اجتماعی تأیید شد. مرکز امنیت سایبری گزارش داد یک هکر با نام مستعار شیطان(devil) ادعا کرده است که جزئیات ۵/۴ میلیون حساب توئیتری را برای فروش در اختیار دارد و این اطلاعات را با استفاده از یک آسیب‌پذیری که قبلاً کشف کرده بود جمع‌آوری کرده است. توئیتر نیز در ۵ اوت این نشتی داده‌ها را تأیید و پیشنهاد کرد که کاربران احراز هویت دو مرحله‌ای را فعال کنند تا از حساب‌های آنها در برابر ورودهای غیرمجاز محافظت شود.

دردسر یک بازی بلاک چینی : شرکت بازی‌های ویدیویی کریپتو Axie Infinity که یکی از محبوب‌ترین بازی‌های بلاک چینی است در دام یک حمله باج‌افزاری افتاد و درنهایت ۶۲۰ میلیون دلار ارز دیجیتال غارت شد. این بازی یک زنجیره جانبی به نام شبکه رونین (Ronin) دارد که کاربران با کمک بریج (Bridge) رونین، می‌توانستند دارایی‌های خود را بین شبکه اتریوم و رونین انتقال دهند. اما مشکل اینجاست که در مارس سال گذشته، بریج رونین هدف حمله هکری قرار گرفت. محققان معتقدند مجرمان سایبری کره شمالی مرتبط با گروه هکری لازاروس(Lazarus)، پشت این سرقت گسترده بوده‌اند هرچند اطلاعات زیادی از این گروه در دست نیست.

باج‌افزاری علیه کاستاریکا

: یکی دیگر از خطرناک‌ترین هک‌های سال ۲۰۲۲، حمله باج‌افزاری Conti بود که دولت کاستاریکا را مورد حمله قرار داد. این حملات سیستم‌های واردات و صادرات این کشور را برای ماه‌ها فلج کرد و خسارات مالی زیادی به بار آورد. میزان تجارت بین‌المللی این کشور به نصف رسید و بیشتر کارمندان مجبور شدند دوباره به کاغذ و خودکار روی بیاورند. Conti ۲۷ دستگاه دولتی، بیش از ۸۰۰سرور با چندین ترابایت داده و همچنین مراکز سلامت را مورد حمله قرارداد و بخش خصوصی روزانه ۳۸میلیون دلار خسارت دید. هکرها خواستار ۱۰میلیون دلار برای پس دادن اطلاعات شدند و وقتی دولت کاستاریکا امتناع کرد، رقم را تا ۲۰میلیون دلار بالا بردند و درنهایت اطلاعات را بر وب سایت Conti منتشر کردند. امریکا نیز جایزه ۱۰میلیون دلاری برای یافتن رهبر گروه هکری Contiقرار داد و بارها اعلام کرد که منشأ این حمله هکری روسیه است هرچند این کشور هرگز این اتهام را نپذیرفت.

ردپای هکرهای نوجوان

در ۲۰ مارس ۲۰۲۲، مایکروسافت توسط یک گروه هکری به نام Lapsus$ مورد هدف قرار گرفت. اعضای این گروه ظاهراً نوجوانانی هستند که حمله‌های موفقی به بزرگ ترین شرکت‌های جهان ازجمله مایکروسافت، سامسونگ، Nvidia، یوبی‌سافت و اوبر داشتند و اطلاعات کاربران این شرکت‌ها را به سرقت بردند. این گروه هکری دردسرهای دیگری هم ایجاد کرد. در ۱۹ سپتامبر سالی که گذشت، Rockstar Games، کمپانی توسعه‌دهنده سری بازی محبوب Grand Theft Auto (GTA) هدف یک حمله هکری بزرگ قرار گرفت و نشت داده‌ها برایش دردسرساز شد. در این ماجرا هم ردپای گروه هکری Lapsus$ دیده شد و یکی از قسمت‌های این بازی که هنوز به بازار عرضه نشده و در حال توسعه بود لو رفت. درحالی که در مارس ۲۰۲۲ یک نوجوان در بریتانیا به عنوان رهبر فرضی باند دستگیر شد، ولی هنوز اطلاعات زیادی در مورد این گروه یا اعضای آن وجود ندارد.

هک‌های رکوردشکن صنعت کریپتو

ارزهای دیجیتال نیز سال گذشته بسیار مورد توجه هکرها قرار داشت و بزرگ‌ترین هک‌های این رمزارزها اتفاق افتاد. هکرهای صنعت کریپتو با سرقت ۳ میلیارد دلار رمزارز در سال ۲۰۲۲ رکوردشکنی کردند. تنها در ۵ حمله سایبری بیش از ۱/۴۸ میلیارد دلار به سرقت رفت که از این رقم ۶۲۵ میلیون دلار را هکرهای کره‌شمالی از طریق شبکه Ronin ربوده‌اند. شبکه Wormhole نیز بیش از ۳۲۵ میلیون دلار از دست داد. ۱۹۰ میلیون دلار از مبلغ سرقت‌شده به Nomad ارتباط دارد که تقریباً چند ماه قبل به آن حمله شد. سرقت ۱۹۰ میلیون دلاری Nomad سومین سرقت بزرگ کریپتو در سال ۲۰۲۲ بود و Beanstalk Farms و Wintermute با ۱۸۲ میلیون دلار و ۱۶۰ میلیون دلار به‌ترتیب در رتبه‌های چهارم و پنجم قرار گرفتند. این ۵ حمله سایبری در مجموع تقریباً نیمی از کل رمزارز سرقت‌شده در سال ۲۰۲۲ را تشکیل دادند.

سرقت ۵۰۰ کیف پول ارز دیجیتال

: هکرها در ۱۷ ژانویه سال گذشته با دور زدن احراز هویت دومرحله‌ای، موفق شدند به کیف پول ارزهای دیجیتال کاربران Crypto.comدسترسی پیدا کنند و در نهایت نیز ۱۸ میلیون دلار بیت‌کوین و ۱۵ میلیون دلار اتریوم و سایر ارزهای رمزنگاری شده را سرقت کردند. این موضوع نشان می‌دهد مدیریت رمز عبور تا چه حد اهمیت دارد. Crypto.com ابتدا موضوع سرقت را رد کرد ولی بعد با قبول این اتفاق، خبر داد که پول به سرقت رفته را به کاربران آسیب دیده بازپرداخت کرده است. این شرکت همچنین اعلام کرد که سیستم‌ها را ممیزی کرده و وضعیت امنیتی سازمان را بهبود بخشیده است ولی بهترین راه برای محافظت در برابر این نوع کلاهبرداری، اطمینان از رمزگذاری تمام داده‌های حساس است و کسب و کارها باید به این موضوع توجه داشته باشند.