باسمه تعالی

پیش‌بینی تهدیدات سایبری برای پول‌های رمزنگاری شده در سال ۲۰۱۸

مقدمه

امروزه، پول رمزنگاری شده تنها مختص افراد متخصص در حوزه کامپیوتر و فناوری اطلاعات نیست. پول رمزنگاری شده بیشتر از آنچه که مردم متوجه شده‌اند، بر زندگی روزمره آنها تأثیر گذاشته است و در عین حال، به سرعت به یک هدف جذاب برای مجرمان سایبری تبدیل شده است.

برخی از تهدیدات سایبری از پرداخت‌های الکترونیکی، نشأت گرفته شده‌اند مانند تغییر آدرس کیف پول مقصد در حین تراکنش‌ها، سرقت کیف پول الکترونیکی و موارد دیگر. با این حال، پول‌های رمزنگاری شده منجر به ایجاد روش‌های جدید و بی‌سابقه‌ای برای کسب درآمد از اقدامات خرابکارانه شده‌اند.

چشم‌انداز پول‌های رمزنگاری شده در سال ۲۰۱۷

در سال ۲۰۱۷، باج‌افزار تهدید اصلی جهانی برای کاربران بود و قربانیان به منظور بازیابی فایل‌ها و داده‌های رمزنگاری شده خود توسط مهاجمان، مجبور بودند که باج تقاضا شده را با استفاده از پول رمزنگاری شده پرداخت کنند. در هشت ماهه نخست سال ۲۰۱۷، محصولات آزمایشگاه کسپرسکی ۱/۶۵ میلیون کاربر را از استخراج‌کننده‌های[1] مخرب پول رمزنگاری شده محافظت نمودند و انتظار می‌رود که این رقم تا پایان این سال به بیش از دو میلیون نفر رسیده باشد. علاوه بر این، پس از گذشت چند سال در سال ۲۰۱۷ بازگشت سارقان بیت‌کوین دیده شد.

در سال ۲۰۱۸ چه انتظاری می‌توان داشت؟

با افزایش مداوم تعداد، پذیرش و ارزش بازاری پول رمزنگاری شده، نه تنها این پول‌ها به‌عنوان یک هدف جذاب برای مجرمان سایبری باقی خواهند ماند، بلکه منجر به استفاده از تکنیک‌ها و ابزارهای پیشرفته‌تری برای ایجاد پول‌های رمزنگاری شده بیشتر خواهند شد. مجرمان سایبری به سرعت توجه خود را به سمت سودآورترین طرح‌های پول‌سازی معطوف خواهند نمود. بنابراین، احتمالاً سال ۲۰۱۸ سال استخراج‌کنندگان مخرب در وب خواهد بود.

[1] miner

حملات باج‌افزار، کاربران را مجبور به خرید پول رمزنگاری شده خواهد کرد.

به دلیل بازار نابسامان و تقریباً بی‌نام و نشان پول رمزنگاری شده که نیازی به اشتراک‌گذاری هیچ اطلاعاتی با هیچ‌کس ندارد، کسی آدرس مجرم را مسدود نخواهد کرد و یا او را دستگیر نمی‌کند و همچنین احتمال کمی که برای ردیابی شدن شخص وجود دارد، مجرمان سایبری همچنان با پول رمزنگاری شده تقاضای باج می‌کنند. در عین حال، تسهیل بیشتر روند کسب درآمد، منجر به اشاعه گسترده‌تر رمزگذارها خواهد شد.

حملات هدفمند با استخراج‌کنندگان

انتظار می‌رود که حملات هدفمند به شرکت‌ها به منظور نصب استخراج‌کنندگان افزایش یابد. در حالی‌که باج‌افزار درآمدزایی زیاد اما فقط برای یک بار را دارد، استخراج‌کنندگان کسب درآمد پایین‌تر اما درازمدتی را خواهند داشت.

افزایش استخراج‌کنندگان ادامه خواهد یافت و افراد جدیدی را در بر خواهد گرفت.

در سال ۲۰۱۸، استخراج در سراسر جهان گسترش خواهد یافت و افراد بیشتری را به سمت خود جذب خواهد کرد. مشارکت استخراج‌کنندگان جدید بستگی به توانایی آنها در دسترسی به منبع برق رایگان و پایدار خواهد داشت. بنابراین، افزایش "استخراج‌کنندگان داخلی" مشهود خواهد بود، به طوریکه کارمندان بیشتری در سازمان‌های دولتی شروع به استخراج با کامپیوترهای دولتی می‌کنند و همچنین کارکنان شرکت-های تولیدی بیشتری از امکانات متعلق به شرکت استفاده خواهند نمود.

استخراج در وب

استخراج در وب، یک تکنیک استخراج پول رمزنگاری شده است که به طور مستقیم با نصب یک اسکریپت خاص بر روی یک صفحه وب در مرورگر صورت می‌گیرد. مهاجمان قبلاً ثابت کرده‌اند که بارگذاری یک اسکریپت بر روی یک وب‌سایت آلوده ساده است و با این اقدام، کامپیوترهای بازدیدکنندگان را برای استخراج به کار می‌گیرند؛ در نتیجه، سکه‌های بیشتری به کیف پول مجرمان افزوده می‌شود. در سال ۲۰۱۸، استخراج در وب به طرز چشمگیری بر ماهیت اینترنت تأثیر خواهد گذاشت و منجر به راهکارهای جدیدی برای کسب درآمد وب‌سایت خواهد شد. یکی از این موارد، جایگزینی تبلیغات خواهد بود: در صورتی که کاربر موافق پرداخت هزینه محتوا باشد، وب‌سایت‌ها اسکریپت استخراج را به صورت دائمی حذف خواهند

کرد. از سوی دیگر، انواع مختلف سرگرمی مانند فیلم، به صورت رایگان در ازای استخراج شما ارائه خواهد شد. یکی از روش‌های دیگر، مبتنی بر یک سیستم بررسی امنیت وب‌سایت است. تأیید Captcha برای تشخیص انسان از ربات با روش‌های استخراج در وب جایگزین خواهد شد و مهم نخواهد بود که یک بازدیدکننده ربات است یا انسان؛ چرا که آنها با استخراج منفعت خواهند رساند.

کاهش ICO[۲] (عرضه اولیه سکه)

عرضه اولیه سکه به معنی سرمایه‌گذاری جمعی از طریق پول‌های رمزنگاری شده است. سال ۲۰۱۷ از این لحاظ، رشد فوق‌العاده‌ای را داشت که با جمع‌آوری بیش از ۳ میلیارد دلار توسط پروژه‌های مختلف، به نوعی با زنجیره بلوک[۳] بیشترین ارتباط را داشت. باید انتظار داشت که در سال ۲۰۱۸ با دنباله‌ای از شکست‌ها (عدم توانایی برای تولید محصول سرمایه‌گذاری شده توسط عرضه اولیه سکه) و انتخاب دقیق‌تر پروژه‌های سرمایه‌گذاری، تب و تاب عرضه اولیه سکه کاهش یابد. تعدادی از پروژه‌های ناموفق عرضه اولیه سکه ممکن است بر نرخ پول‌های رمزنگاری شده مبادله‌ای (Bitcoin، Ethereum و ...) که در سال ۲۰۱۷ رشد بی‌سابقه‌ای را تجربه کردند، تأثیر منفی بگذارد. بنابراین، تعداد حملات فیشینگ و هک برای هدف قرار دادن عرضه اولیه سکه، قراردادهای هوشمند و کیف‌های پول کاهش خواهد یافت.

نتیجه‌گیری

فناوری‌های ارتباطی، امکان ایجاد زندگی بهتر و امن‌تری را فراهم می‌آورند، اما آنها آسیب‌پذیری‌های جدیدی را نیز به وجود می‌آورند که مهاجمان سایبری به سرعت از آن بهره می‌برند. این پیش‌بینی‌ها بر اساس تجربیات محققان و متخصصان امنیت در سال گذشته به دست آمده است. این پیش‌بینی‌ها نظرات کارشناسی هستند و ممکن است که همه آنها تحقق نیابند. اما آماده شدن نیمی از نبرد است.

[2] Initial Coin Offering
[3] blockchain

منابع:

[1] Kaspersky Labs, "*Threat Predictions for Cryptocurrencies*", Kaspersky Security Bulletin: Threat Predictions for 2018, 15 November 2017.