

سرقت از کیف پول های دیجیتالی سرد و گرم



روابط عمومی شرکت ایدکو (توزیع کننده ی محصولات کسپرسکی در ایران)؛ هر قدر محبوبیت جهانی رمزارزها بیشتر باشد و تعداد روش های ذخیره آن ها هم افزایش یابد، گستره ی ابزارهایی که عاملین تخریب با آن به دنبال پول دیجیتال می روند بیشتر می شود. اسکرها بسته به نحوه محافظت شدن تارگت و اینکه مبلغ پول چقدر است و اگر حمله موفقیت آمیز باشد چه میزان می توانند سرقت کنند دست به

ساخت فناوری های پیچیده می زنند. داستان امروز ما دو متود کاملاً متفاوت از حمله ایمیل را پوشش می دهد: سرقت از کیف پول های دیجیتالی سرد و گرم. با ما همراه بمانید.

کیف پول های گرم و تلاش برای هک آنها

کیف پول گرم یک کیف پول رمزارز است که دسترسی همیشگی به اینترنت دارد. این اساساً یعنی هر سرویس آنلاینی که ذخیره گاه رمزارز ارائه می دهد - از صرافی های کریپتو گرفته تا اپ های تخصصی. کیف پول های گرم گزینه ی بسیار محبوب ذخیره سازی کریپتو هستند. توجه این محبوبیت هم سادگی درست کردن آن (ثبت با سرویس کیف تنها کاری است که باید انجام دهید) و راحتی برداشت پول و تبدیل است. این محبوبیت و سادگی کیف پول های گرم باعث شده به طعمه چرب و نرمی برای مجرمان سایبری تبدیل شوند. به هر حال به این دلیل و نیز با توجه به این حقیقت که همیشه آنلاین هستند، این کیف پول ها به ندرت برای ذخیره سازی مقادیر بالا استفاده می شوند. از این رو مجرمان سایبری برای سرمایه گذاری سنگین روی کمپین های فیشینگ انگیزه کمی دارند پس تکنیک های استفاده شده در حملاتی که به کیف پول های گرم می شود کم پیش می آید بدعت گذاران یا پیچیده باشند. در حقیقت، آن ها بیشتر بدوی به نظر می رسند و خوراکشان کاربران غریبیده است. یک اسکم فیشینگ معمولی که کیف پول گرم را هدف گرفته چنین کار می کند:

هکرها ایمیل هایی را ارسال می کنند که آدرس آن از یک صرافی معروف ارز دیجیتال است و از کاربر می خواهد تراکنش را تأیید یا کیف پول خود را دوباره تأیید کند.

پس از اینکه کاربر روی لینک کلیک کرد، به صفحه ای هدایت می شود که از آنها خواسته می شود عبارت اولیه خود را وارد کنند. عبارت seed یا عبارت بازیابی دنباله ای از ۱۲ (به طور معمول ۲۴) کلمه برای بازیابی دسترسی به کیف پول رمزنگاری است. این در اصل رمز اصلی کیف پول است. عبارت seed را می توان برای به دست آوردن یا بازیابی دسترسی به حساب کاربر و انجام هر گونه تراکنش استفاده کرد. عبارت seed را نمی توان تغییر داد یا بازیابی کرد: با قرار دادن اشتباه آن، کاربر در خطر از دست دادن دسترسی به کیف پول خود برای همیشه قرار خواهد گرفت و با دادن آن به کلاهبرداران، حساب خود را برای همیشه به خطر می اندازد.

اگر کاربر عبارت بازیابی را روی وب پیج تقلبی وارد کند، اسکرها دسترسی کامل به کیف را پیدا خواهند کرد و نیز قادر خواهند شد همه وجوه را به آدرس خودشان منتقل کنند. کلاهبرداری هایی از این دست، بسیار ساده و بدون نرم افزار یا ترفندهای مهندسی اجتماعی، معمولاً کاربران غیر فنی را هدف قرار می دهند. فرم ورود عبارت اولیه معمولاً ظاهری ساده دارد: فقط یک فیلد ورودی و یک آرم صرافانی ارز دیجیتال.

اسکم های فیشینگی که کیف پول های سرد را هدف قرار می دهند

کیف پول سرد (ذخیره سرد) کیف پولی است بدون اتصال دائمی به اینترنت، مانند یک دستگاه اختصاصی یا حتی فقط یک کلید خصوصی که روی یک کاغذ نوشته شده است. ذخیره سازی سخت افزار رایج ترین نوع کیف پول سرد است. از آنجایی که این دستگاهها در اکثر مواقع آفلاین بوده و دسترسی از راه دور غیرممکن است، کاربران تمایل دارند مقادیر بسیار بیشتری را در این دستگاهها ذخیره کنند. با این اوصاف، باور اینکه کیف پول سخت افزاری بدون سرقت یا حداقل دسترسی فیزیکی به آن نمی تواند به خطر بیافتد، اشتباه خواهد بود. همانند کیف پول های گرم، کلاهبرداران از تکنیک های مهندسی اجتماعی برای دستیابی به وجوه کاربران استفاده می کنند. ما اخیراً یک کمپین ایمیل را مشاهده کردیم که به طور خاص برای دارندگان کیف پول های سرد سخت افزاری طراحی شده بود.

این نوع حمله به عنوان یک کمپین ایمیل کریپتو شروع می شود: کاربر ایمیلی دریافت می کند که آدرس آن از صرافانی ارزهای دیجیتال ریپل است و پیشنهاد پیوستن به توکن های XRP، ارز دیجیتال داخلی پلت فرم را می دهد.

اگر کاربر روی لینک کلیک کند، صفحه بلاگی به آن ها نمایش داده خواهد شد که در آن پستی است که قوانین «هدایا» را توضیح می دهد. این پست حاوی لینک مستقیمی است به بخش «ثبت نام».

در حال حاضر در این مرحله، کلاهبرداری چند تفاوت را با حملات انبوه به کیف پول های گرم نشان می دهد: کلاهبرداران به جای ارسال لینکی به صفحه فیشینگی برای کاربر، از ترفند غوطه وری [۱] پیچیده تری با یک پست وبلاگ استفاده کردند. آنها همچنین تا آنجا پیش رفتند که طراحی وب سایت ریپل را با دقت کپی کردند و نام دامنه ای را ثبت کردند که تقریباً مشابه دامنه رسمی صرافانی بود. این حمله فیشینگی Punycode نامیده میشود. در نگاه اول، دامنه سطح دوم با دامنه اصلی یکسان است، اما با نگاهی دقیق تر مشخص می شود که حرف r با یک کاراکتر یونیکد که از cedilla استفاده می کند، جایگزین شده است:

[https://app\[.\]xn--ipple-4bb\[.\]net](https://app[.]xn--ipple-4bb[.]net) - <[https://app\[.\]ripple\[.\]net](https://app[.]ripple[.]net)>

همچنین، سایت کلاهبرداری در دامنه سطح بالای .net میزبانی می شود، نه .com، جایی که وب سایت رسمی ریپل در آن قرار دارد. این ممکن است کاربر را مشکوک نکند زیرا هر دو دامنه به طور گسترده توسط سازمان های قانونی استفاده می شوند. پس از اینکه کاربر لینک را از "وبلاگ" به صفحه جعلی ریپل دنبال کرد، به آنها پیشنهاد می شود به آدرس [Web Socket wss://s2.ripple.com](https://s2.ripple.com) متصل شوند.

سپس به کاربر پیشنهاد می شود آدرس اکانت XRP خود را وارد کنند.

سپس وبسایت انتخاب متود احراز برای دریافت توکن های جایزه را پیشنهاد می دهد.

همانطور که می بینید، کیف پول های سخت افزاری در صدر لیست قرار دارند و توسط کلاهبرداران پیشنهاد می شوند. انتخاب Trezor کاربر را به وبسایت رسمی trezor.io هدایت می کند، که اجازه می دهد دستگاهها را از طریق Trezor Connect API به برنامه های وب

متصل کند. API برای ساده کردن تراکنش ها با کمک کیف پول سخت افزاری استفاده می شود. کلاهبرداران از قربانی می خواهند به وبسایت آنها متصل شود تا بتوانند وجوه خود را از حساب قربانی برداشت کنند. هنگامی که کاربر تلاش می کند به وبسایت طرف سوم متصل شود، Trezor Connect از آنها می خواهد که با جمع آوری ناشناس داده ها موافقت کنند و تأیید کنند که می خواهند به وبسایت متصل شوند. آدرس سایت کلاهبرداری در نمای Punycode به صورت: [https://app\[.\]xn--ipple-4bb\[.\]net](https://app[.]xn--ipple-4bb[.]net) نمایش داده می شود. امید کلاهبردار این است که کاربر حواسش به آدرسی که با حروف کوچک در کنار صفحه ارائه شده نباشد.

اتصال از طریق Ledger بسیار شبیه به Trezor است، اما از رابط Web HID استفاده می کند و سایر مراحل بدون تغییر است.

پس از اتصال کاربر کیف پول سخت افزاری خود چه اتفاقی می افتد؟ ما مجبور شدیم برای پاسخ به این سوال کمی کد سایت فیشینگ را بررسی کنیم. این وبسایت توسط یک برنامه کاربردی نوشته شده در Node.js پشتیبانی می شود. این از دو API استفاده می کند:

- <wss://s2.ripple.com>, the official Web Socket address for Ripple transactions

- The phishing site API, for example: [app\[.\]xn--ipple-4bb\[.\]net/api/v1/action](app[.]xn--ipple-4bb[.]net/api/v1/action)

کلاهبرداران از این دو API برای تعامل با حساب XRP قربانی استفاده می کنند. API سایت فیشینگ با آدرس Web Socket ارتباط گرفته، جزئیات حساب را تأیید و درخواست وجه می کند. برای این منظور، کلاهبرداران کیف پول های میانجی را به راه می اندازند.

حساب میانجی فقط برای دو مورد استفاده می شود: دریافت وجوه قربانی و ارسال آن به حساب دائمی کلاهبرداران. این به پنهان کردن مقصد نهایی کمک می کند.

آمار

بهار سال ۲۰۲۳، راهکارهای آنتی اسپم کسپرسکی ۸۵۳۶۲ ایمیل کلاهبرداری را که کاربران ارزهای دیجیتال را هدف قرار می دادند شناسایی و مسدود کرد. کمپین های ایمیل کلاهبرداری در ماه مارس با ۳۴۶۴۴ پیام به اوج خود رسید. ما ۱۹۹۰۲ ایمیل را در آوریل و ۳۰۸۱۶ ایمیل را در ماه می مسدود کردیم.

نتیجه

اسکمرها یک چیز را خوب درک می کنند و آن هم این است: هر قدر غنایم سخت تر بدست بیایند یعنی بزرگ تر و رب و نرم تر هستند. از این رو حمله به کیف پول های سخت افزاری که خیلی ها آن ها را نفوذناپذیر می پندارند بیشتر به چشم اسکمرها می آید. آن ها برای چنین طعمه هایی همه همت و اندیشه شروانه خود را به کار می بندند. گرچه کیف پول های سخت افزاری بسیار از کیف پول های گرم امن تر هستند اما کاربران نباید سپر خود را زمین ببندند. قبل از دادن دسترسی وبسایت به کیف پول تان هر جزئیاتی را با دقت مورد بررسی قرار داده و اگر هر چیزی برایتان مشکوک بود از اتصال سر باز بزنید.

منبع: کسپرسکی آنلاین (ایدکو)

پژوهش های محسن خندان دل



کسپرسکی اسم یکی از بزرگترین شرکتهای امنیتی و سازنده آنتی ویروس است که برخی از کاربران اشتبهاً این شرکت و محصولات آنتی ویروس آن را با عناوینی نظیر کسپرسکای ، کاسپرسکی ، کسپراسکای ، کسپراسکای ، و یا کاسپراسکای نیز می شناسد. همچنین لازم به ذکر است مدیرعامل این شرکت نیز یوجین کسپرسکی نام دارد.

پژوهشگر : محسن خندان دل

مدیر عامل خدمات مالی و کامپیوتری حساب رایانه