مقالات علمی

سرقت از کیف‌پول‌های دیجیتالی سرد و گرم

روابط عمومی شرکت ایدکو (توزیع‌کننده‌ی محصولات کسپرسکی در ایران)؛ هرقدر محبوبیت جهانی رمزارزها بیشتر باشد و تعداد روش‌های ذخیره آن‌ها هم افزایش یابد، گستره‌ی ابزارهایی که عاملین تخریب با آن به دنبال پول دیجیتال می‌روند بیشتر می‌شود. اسکمرها بسته به نحوه محافظت شدن تارگت و اینکه مبلغ پول چقدر است و اگر حمله موفقیت‌آمیز باشد چه میزان می‌توانند سرقت کنند دست به ساخت فناورهای پیچیده می‌زنند. داستان امروز ما دو متود کاملاً متفاوت از حمله ایمیل را پوشش می‌دهد: سرقت از کیف‌پول‌های دیجیتالی سرد و گرم. با ما همراه بمانید.

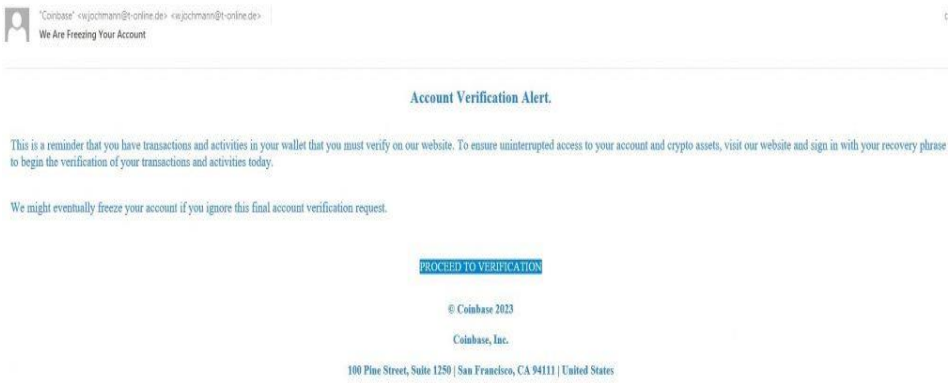
کیف‌پول‌های گرم و تلاش برای هک آن‌ها

کیف‌پول گرم یک کیف‌پول رمزارز است که دسترسی همیشگی به اینترنت دارد. این اساساً یعنی هر سرویس آنلاینی که ذخیره‌گاه رمزارز ارائه می‌دهد –از صرافی‌های کریپتو گرفته تا اپ‌های تخصصی. کیف‌پول‌های گرم گزینه‌ی بسیار محبوب ذخیره‌سازی کریپتو هستند. توجیه 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

مقالات علمی

سادگی کیف‌پول‌های 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 کیف‌پول‌ها به ندرت برای ذخیره‌سازی مقادیر بالا استفاده می‌شوند. از این رو مجرمان سایبری برای سرمایه‌گذاری سنگین روی کمپین‌های فیشینگ انگیزه کمی دارند پس تکنیک‌های استفاده‌شده در حملاتی که به کیف‌پول‌های گرم می شود کم پیش می‌آید بدعت‌گذارانه یا پیچیده باشند. در حقیقت، آن‌ها بیشتر بدوی به نظر می‌رسند و خوراکشان کاربران غیرپییده است. یک اسکم فیشینگ معمولی که کیف‌پول گرم را هدف گرفته چنین کار می‌کند:

هکرها ایمیل‌هایی را ارسال می‌کنند که آدرس آن از یک صرافی معروف ارز دیجیتال است و از کاربر می‌خواهد تراکنش را تأیید یا کیف پول خود را دوباره تأیید کند.


"Coinbase" <wjochmann@t-online.de> <wjochmann@t-online.de>
We Are Freezing Your Account

Account Verification Alert.

This is a reminder that you have transactions and activities in your wallet that you must verify on our website. To ensure uninterrupted access to your account and crypto assets, visit our website and sign in with your recovery phrase to begin the verification of your transactions and activities today.

We might eventually freeze your account if you ignore this final account verification request.

PROCEED TO VERIFICATION

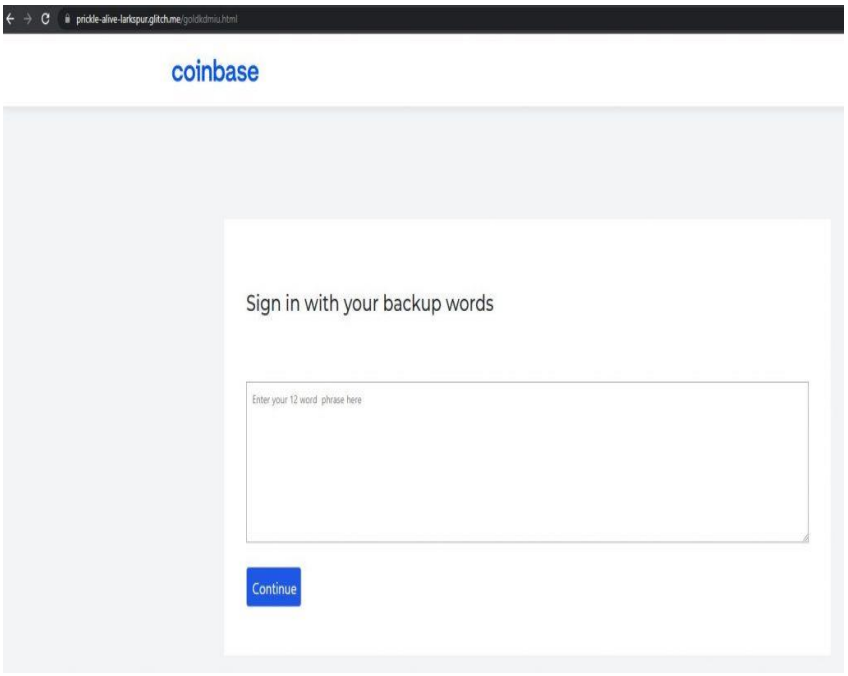
© Coinbase 2023

Coinbase, Inc.

100 Pine Street, Suite 1250 | San Francisco, CA 94111 | United States

پس از اینکه کاربر روی لینک کلیک کرد، به صفحه ای هدایت می‌شود که از آنها خواسته می‌شود 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 می‌توان برای به دست آوردن یا بازیابی دسترسی به حساب کاربر و انجام هر گونه تراکنش استفاده کرد. عبارت seed را نمی‌توان تغییر داد یا بازیابی کرد: با قرار دادن اشتباه آن، کاربر در خطر از دست دادن دسترسی به کیف‌پول خود برای همیشه قرار خواهد گرفت و با دادن آن به کلاهبرداران، حساب خود را برای همیشه به خطر می‌اندازد.

مقالات علمی

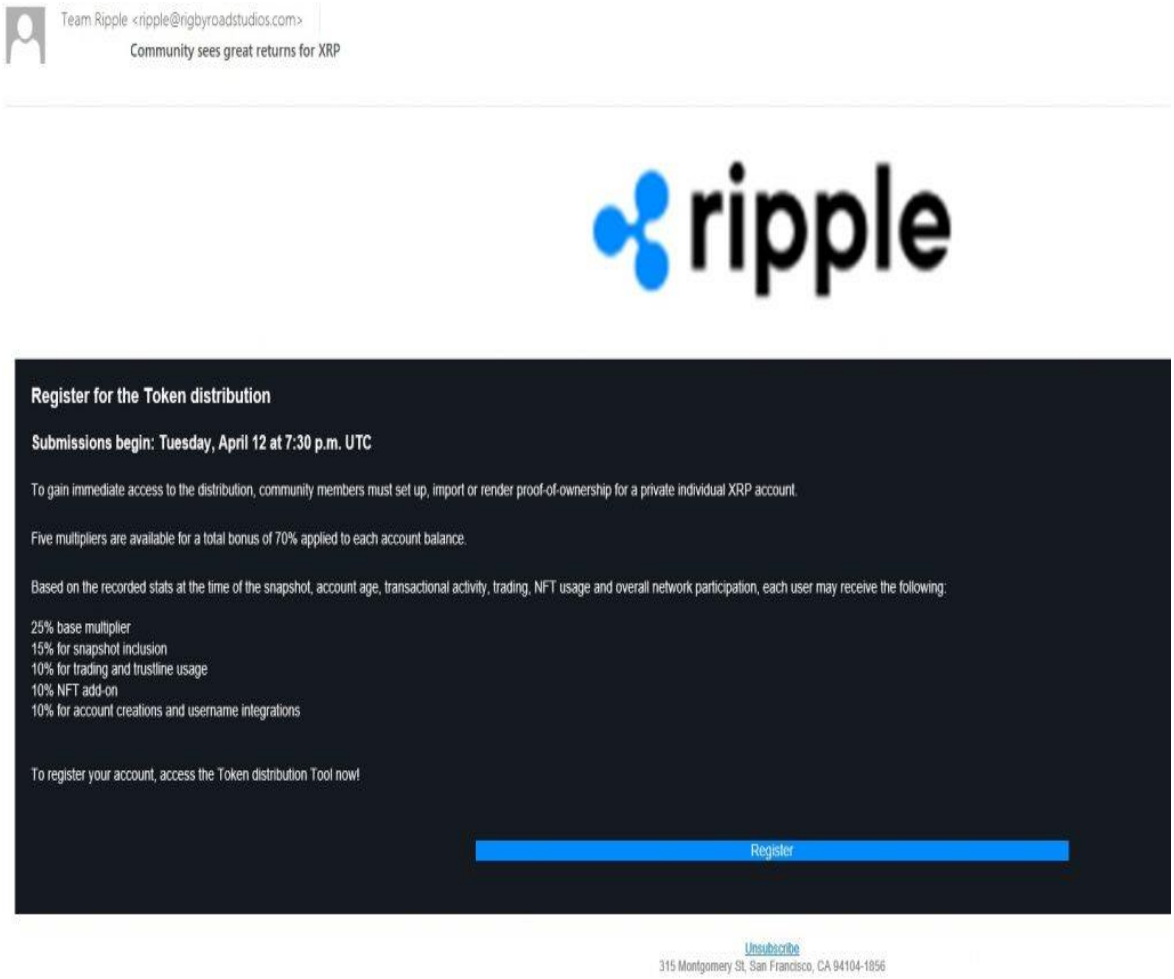


اگر کاربر عبارت بازیابی را روی وب‌پیج تقلبی وارد کند، اسکمرها دسترسی کامل به کیف را پیدا خواهند کرد و نیز قادر خواهند شد همه وجوه را به آدرس خودشان منتقل کنند. کلاهبرداری‌هایی از این دست، بسیار ساده و بدون نرم‌افزار یا ترفندهای مهندسی اجتماعی، معمولاً کاربران غیر فنی را هدف قرار می‌دهند. فرم ورود عبارت اولیه معمولاً ظاهری ساده دارد: فقط یک فیلد ورودی و یک آرم صرافی ارز دیجیتال.

اسکمرهای فیشینگی که کیف‌پول‌های سرد را هدف قرار می‌دهند

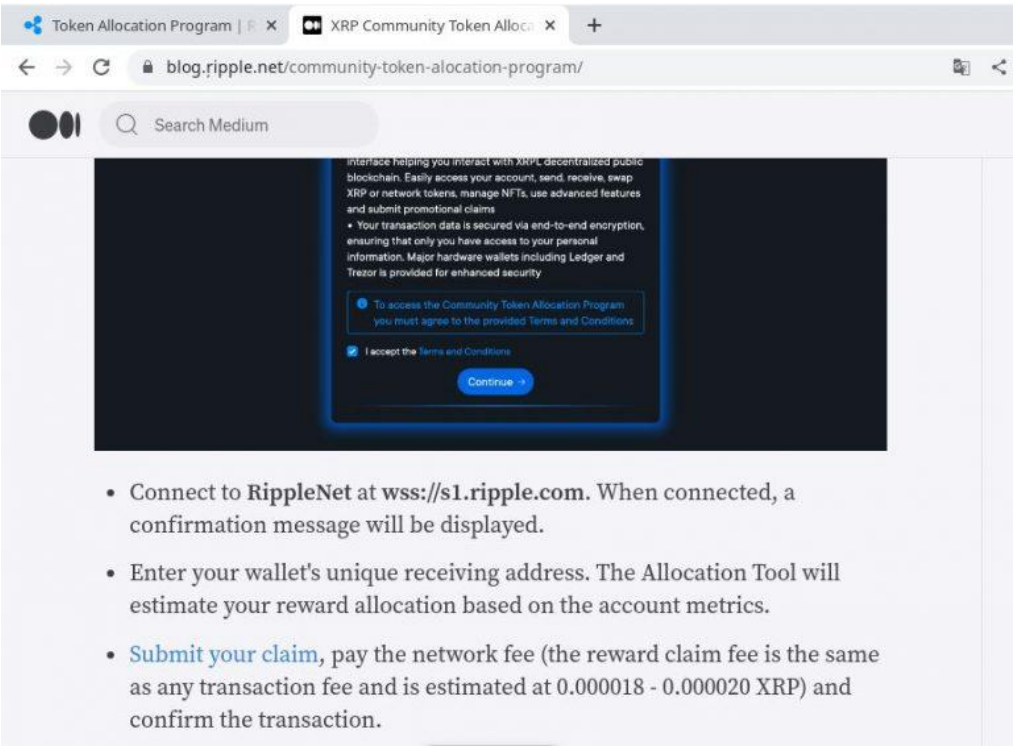
کیف پول سرد (ذخیره سرد) کیف پولی است بدون اتصال دائمی به اینترنت، مانند یک دستگاه اختصاصی یا حتی فقط یک کلید خصوصی که روی یک کاغذ نوشته شده است. ذخیره سازی سخت افزار رایج‌ترین نوع کیف‌پول سرد است. از آنجایی که این دستگاه‌ها در اکثر مواقع آفلاین بوده و دسترسی از راه دور غیرممکن است، کاربران تمایل دارند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

این نوع حمله به عنوان یک کمپین ایمیل کریپتو شروع می‌شود: کاربر ایمیلی دریافت می‌کند که آدرس آن از صرافی ارزهای دیجیتال ریپل است و پیشنهاد پیوستن به توکن‌های XRP، ارز دیجیتال داخلی پلت‌فرم را می‌دهد.



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

مقالات علمی

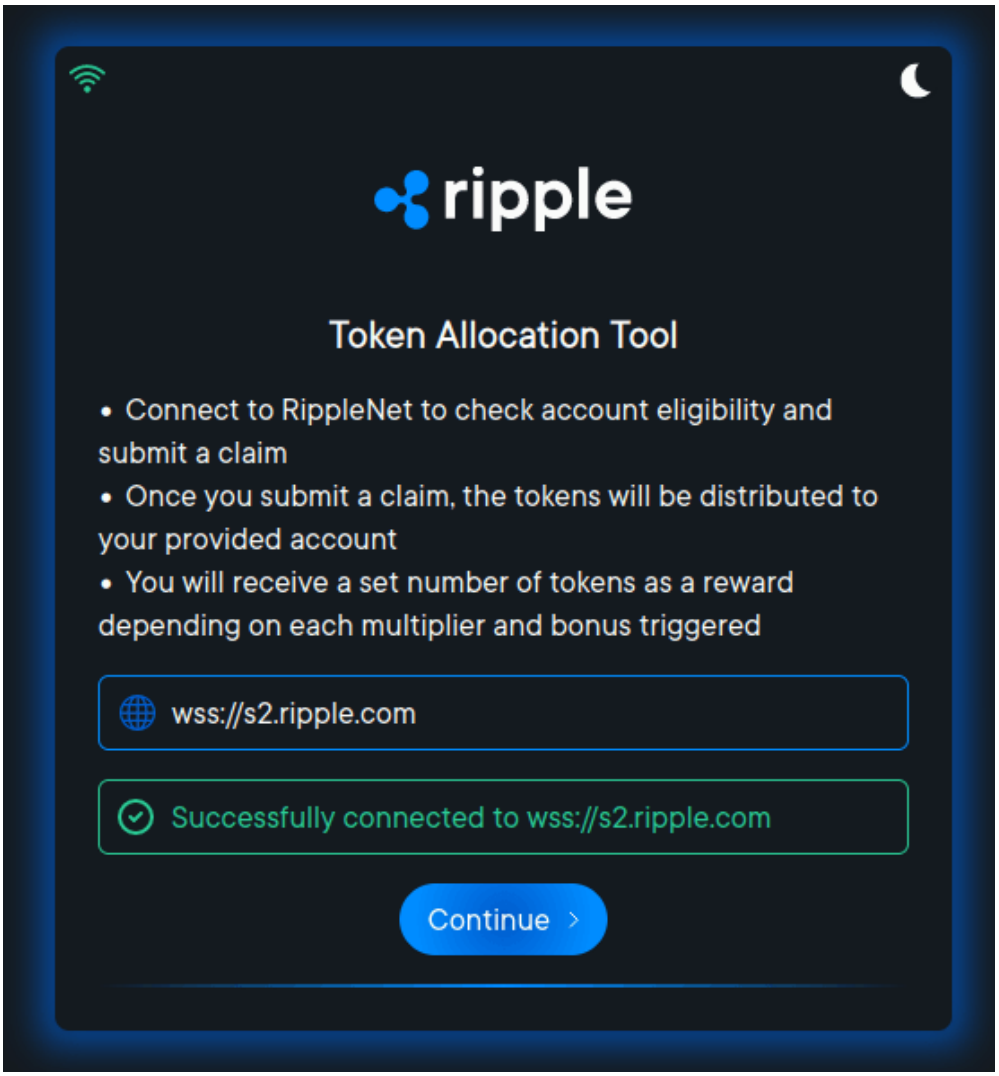


در حال حاضر در این مرحله، کلاهبرداری چند تفاوت را با حملات انبوه به کیف‌پول‌های گرم نشان می‌دهد: کلاهبرداران به جای ارسال لینکی به صفحه فیشینگ برای کاربر، از ترفند غوطه‌وری[۱] پیچیده‌تری با یک پست وبلاگ استفاده کردند. آنها همچنین تا آنجا پیش رفتند که طراحی وب سایت ریپل را با دقت کپی کردند و نام دامنه ای را ثبت کردند که تقریباً مشابه دامنه رسمی صرافی بود. این حمله فیشینگ Punycode نامیده میشود. در نگاه اول، دامنه سطح دوم با دامنه اصلی یکسان است، اما با نگاهی دقیق‌تر مشخص می‌شود که حرف r با یک کاراکتر یونیکد که از cedilla استفاده می‌کند، جایگزین شده است:

https://app[.]ripple[.]net/ <https://app[.]xn--ipple-4bb[.]net -

همچنین، سایت کلاهبرداری در دامنه سطح بالای .net میزبانی می‌شود، 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 سازمان‌های قانونی استفاده می‌شوند. پس از اینکه کاربر لینک را از "وبلاگ" به صفحه جعلی ریپل دنبال کرد، به آنها پیشنهاد می‌شود به آدرس wss://s2.ripple.com WebSocket متصل شوند.

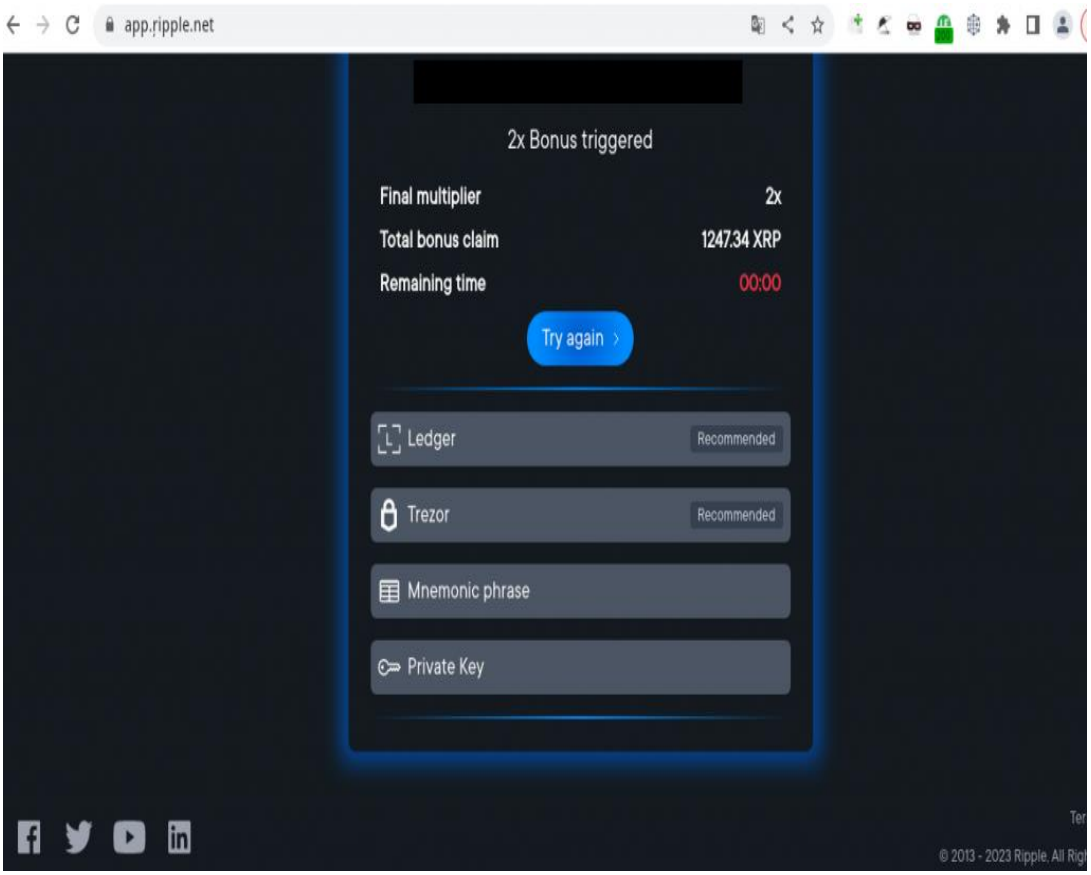
مقالات علمی



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

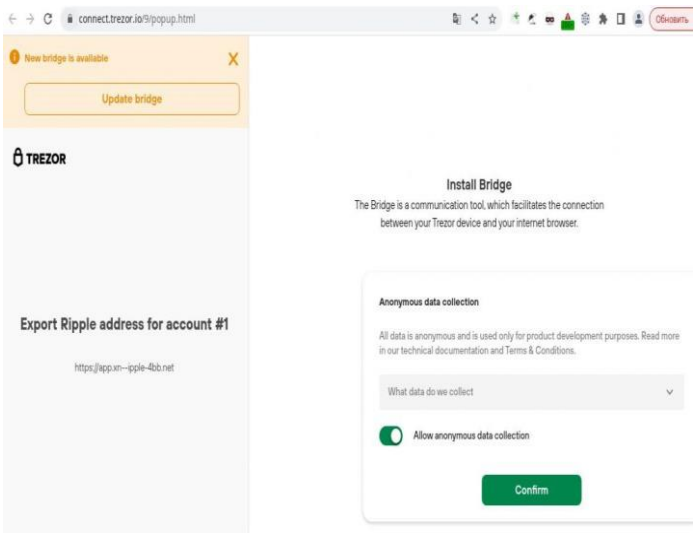
سپس وبسایت انتخاب متود احراز برای دریافت توکن‌های جایزه را پیشنهاد می‌دهد.

مقالات علمی



همانطور که می‌بینید، کیف‌پول‌های سخت افزاری در صدر لیست قرار دارند و توسط کلاهبرداران پیشنهاد می‌شوند. انتخاب Trezor کاربر را به وب‌سایت رسمی trezor.io هدایت می‌کند، که اجازه می‌دهد دستگاه‌ها را از طریق Trezor Connect API به برنامه‌های وب متصل کند. API برای ساده کردن تراکنش‌ها با کمک کیف‌پول سخت‌افزاری استفاده می‌شود. کلاهبرداران از قربانی می‌خواهند به وبسایت آنها متصل شود تا بتوانند وجوه خود را از حساب قربانی برداشت کنند. هنگامی که کاربر تلاش می‌کند به وبسایت طرف سوم متصل شود، Trezor Connect از آنها می‌خواهد که با جمع آوری ناشناس داده‌ها موافقت کنند و تأیید کنند که می‌خواهند به وبسایت متصل شوند. آدرس سایت کلاهبرداری در نمای Punycode به صورت: https://app[.]xn--ipple-4bb[.]net نمایش داده می‌شود. امید کلاهبردار این است که کاربر حواسش به آدرسی که با حروف کوچک در کنار صفحه ارائه شده نباشد.

مقالات علمی



اتصال از طریق Ledger بسیار شبیه به Trezor است، اما از رابط WebHID استفاده می‌کند و سایر مراحل بدون تغییر است.

پس از اتصال کاربر کیف‌پول سخت افزاری خود چه اتفاقی می‌افتد؟ 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 می‌شود. این از دو API استفاده می‌کند:

- wss://s2.ripple.com, the official WebSocket address for Ripple transactions
- The phishing site API, for example: app[.]xn--ipple-4bb[.]net/api/v1/action

کلاهبرداران از این دو API برای تعامل با حساب XRP قربانی استفاده می‌کنند. API سایت فیشینگ با آدرس WebSocket ارتباط گرفته، جزئیات حساب را تأیید و درخواست وجه می‌کند. برای این منظور، کلاهبرداران کیف‌پول‌های میانجی را به راه می‌اندازند.

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

آمار

بهار سال ۲۰۲۳، راهکارهای آنتی اسپم کسپرسکی ۸۵۳۶۲ ایمیل کلاهبرداری را که کاربران ارزهای دیجیتال را هدف قرار می‌دادند شناسایی و مسدود کرد. کمپین‌های 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

مقالات علمی

اسکمرها یک چیز را خوب درک می‌کنند و آن هم این است: هر قدر غنایم سخت‌تر بدست بیایند یعنی بزرگ‌تر و رب و نرم‌تر هستند. از این رو حمله به کیف‌پول‌های سخت‌افزاری که خیلی‌ها آن‌ها را نفوذناپذیر می‌پندارند بیشتر به چشم اسکمرها می‌آید. آن‌ها برای چنین طعمه‌هایی همه همت و اندیشه شرورانه خود را به کار می‌بندند. گرچه کیف‌پول‌های سخت‌افزاری بسیار از کیف‌پول های گرم امن‌تر هستند اما کاربران نباید سپر خود را زمین بیاندازند. قبل از دادن دسترسی وبسایت به کیف‌پول‌تان هر جزئیاتی را با دقت مورد بررسی قرار داده و اگر هر چیزی برایتان مشکوک بود از اتصال سر باز بزنید.

Immersion trick [۱]

منبع: کسپرسکی آنلاین (ایدکو)

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