خبرنامه الکترونیکی ۵۶

مرکز تخصصی آپا دانشگاه سمنان

شماره پنجاه و ششم، سال پنجم، بهمن ۱۴۰۱ | کاری از تیم تولید محتوای مرکز تخصصی آپا دانشگاه سمنان

https://cert.semnan.ac.ir info.cert@semnan.ac.ir 023-31535019 @semcert

مرکز آپا دانشگاه سمنان

امنیت تلفن همراه در سازمان ها(1)

رایج‌ترین و تاثیرگذارترین تهدیدات سایبری تلفن همراه

• باج‌افزار موبایل:
یکی از انواع برنامه‌های مخرب است که پس از نصب روی تلفن همراه، داده‌های آن را رمز کرده و از صاحب آن دستگاه باج‌خواهی می‌کند.

• برنامه‌ها و وب‌سایت‌های مخرب:
دستگاه‌های تلفن همراه می‌توانند از طریق نصب بدافزار تلفن همراه روی خودشان، به محتوای مخرب آنلاین دسترسی داشته باشند.

• فیشینگ:
دستگاه‌های تلفن همراه به تعدادی از رسانه‌های ارتباطی مختلف مانند پیامک، ایمیل و... دسترسی دارند و آنها را به یک پلتفرم ایده‌آل برای انجام حملات فیشینگ که داده‌ها را به سرقت می‌برند تبدیل می‌کنند.

• تکنیک‌های پیشرفته jailbreaking* و Rooting
jailbreaking و Rooting مجوزهای بالایی را در دستگاه تلفن همراه فراهم می‌کند و مهاجم را قادر می‌سازد تا طیف وسیع‌تری از اقدامات مخرب را انجام دهد.

• Exploitهای سیستم‌عامل:
مانند هر نرم‌افزار دیگری، سیستم‌عامل‌های تلفن همراه می‌توانند دارای آسیب‌پذیری‌های قابل بهره برداری باشند که آنها و کاربرانشان را در معرض خطر قرار می‌دهند.

• حمله مردی در میان:
ارتباطات سیار همیشه از فناوری‌های ایمن استفاده نمی‌کند و آنها را در برابر شنود برای استراق سمع یا تغییر داده‌ها آسیب‌پذیر می‌کند.

* jailbreak کردن فرآیندی است که طی آن یک سری تغییراتی در سیستم عامل IOS پیش فرض نصب شده در دستگاه اعمال می‌کند و به کاربر این امکان را می‌دهد که نسبت به نصب اپلیکیشن‌های غیر رسمی و خارج از اپ استور (App Store) اقدام کند. بنابراین به صورت کلی می‌توان jailbreak کردن را پروسه‌ای نسبتا مشابه با روت کردن دستگاه‌های اندرویدی دانست.

فهرست

خبر

مرکز آپا دانشگاه سمنان

خبر

هک ۳۵ هزار حساب پی‌پال

شرکت پی پال به ۳۵هزار کاربر خود اطلاع داد که حساب‌های آنها بین ٦ و ٨ دسامبر مورد نفوذ قرار گرفته است. روشی که مهاجمان برای کرک کردن حساب‌ها استفاده می‌کنند در این هک متفاوت است به گونه‌ای که خود پی پال هک نشده در عوض، بازیکنان مخرب از حمله‌ای به نام پر کردن اعتبار استفاده کردند(از اطلاعات ورودی که قبلاً فاش شده بود و مردم برای حساب‌های پی پال خود استفاده مجدد می‌کردند).

به گزارش فارس، به نقل از پی سی ورد، سایت Bleeping Computer گزارش می‌دهد: در طول دو روز، هکرها به نام کامل دارندگان حساب، تاریخ تولد، آدرس پستی، شماره بیمه و شماره شناسایی مالیات فردی دسترسی داشتند. سابقه تراکنش‌ها، جزئیات کارت اعتباری یا بدهی متصل و داده‌های صورت حساب پی پال نیز قابل دسترسی هستند.

پی پال نفوذ را در عرض دو روز متوقف و رمزهای عبور کاربران آسیب دیده را بازنشانی کرد و گفت که هیچ تراکنش غیرمجازی انجام نشده است. همچنین به کاربران آسیب‌دیده دو سال نظارت رایگان اعتباری از طریق مرکز اعتبارسنجی اکوئیفاکس ارائه می دهد.

این شرکت تأیید کرد که اشخاص ثالث غیرمجاز با اعتبارنامه‌های معتبر وارد حساب‌ها شده‌اند. پلتفرم پرداخت‌های الکترونیکی ادعا می‌کند که این به دلیل نقض سیستم‌های آن نبوده و هیچ مدرکی دال بر اینکه اعتبار کاربر مستقیماً از آنها به دست آمده وجود ندارد.

با توجه به گزارش نقض داده ۳۴هزار و۹۴۲ کاربر آن تحت تأثیر این حادثه قرار گرفته‌اند. پی پال می‌گوید که اقدام به موقع برای محدود کردن دسترسی متجاوزان به پلتفرم و بازنشانی رمز عبور حساب‌ها را انجام داده است. همچنین، این شرکت ادعا می‌کند که مهاجمان موفق به انجام هیچ تراکنشی از حساب‌های پی پال نشده‌اند.

در اطلاعیه پی پال به کاربران آسیب دیده آمده است: «اطلاعاتی دال بر اینکه در نتیجه این حادثه از داده‌های شخصی شما سوء استفاده شده یا تراکنش‌های غیرمجاز در حساب شما وجود ندارد. ما گذرواژه‌های حساب‌های آسیب‌دیده را بازنشانی کردیم و کنترل‌های امنیتی پیشرفته‌تری را اجرا کردیم که از شما می‌خواهد دفعه بعد که وارد حساب خود می‌شوید رمز عبور جدیدی ایجاد کنید.»

این شرکت توصیه می‌کند که دریافت‌کنندگان اعلان‌ها رمز عبور سایر حساب‌های آنلاین را با استفاده از یک رشته منحصر به فرد و طولانی تغییر دهند. به طور معمول، یک رمز عبور خوب حداقل ۱۲ کاراکتر طول دارد و شامل کاراکترها و نمادهای الفبایی عددی است. علاوه بر این، به کاربران اعلام کرد که محافظت دو مرحله‌ای[1] را از منوی تنظیمات حساب فعال کنند، تا از دسترسی افراد غیرمجاز به یک حساب، (حتی اگر نام کاربری و رمز عبور معتبری داشته باشد) جلوگیری کند.

به کاربران توصیه شده که از گذرواژه‌های تکراری در حساب‌ها استفاده نکنند، به‌ویژه آنهایی که اطلاعات خصوصی یا بانکی فوق‌العاده حساسی دارند. یک مدیر رمز عبور این کار را آسان می کند. فعال بودن احراز هویت دو مرحله ای نیز این حملات را متوقف می کند؛ پی پال گزینه امنیتی را در منوی تنظیمات حساب خود ارائه داده است.

1-2FA

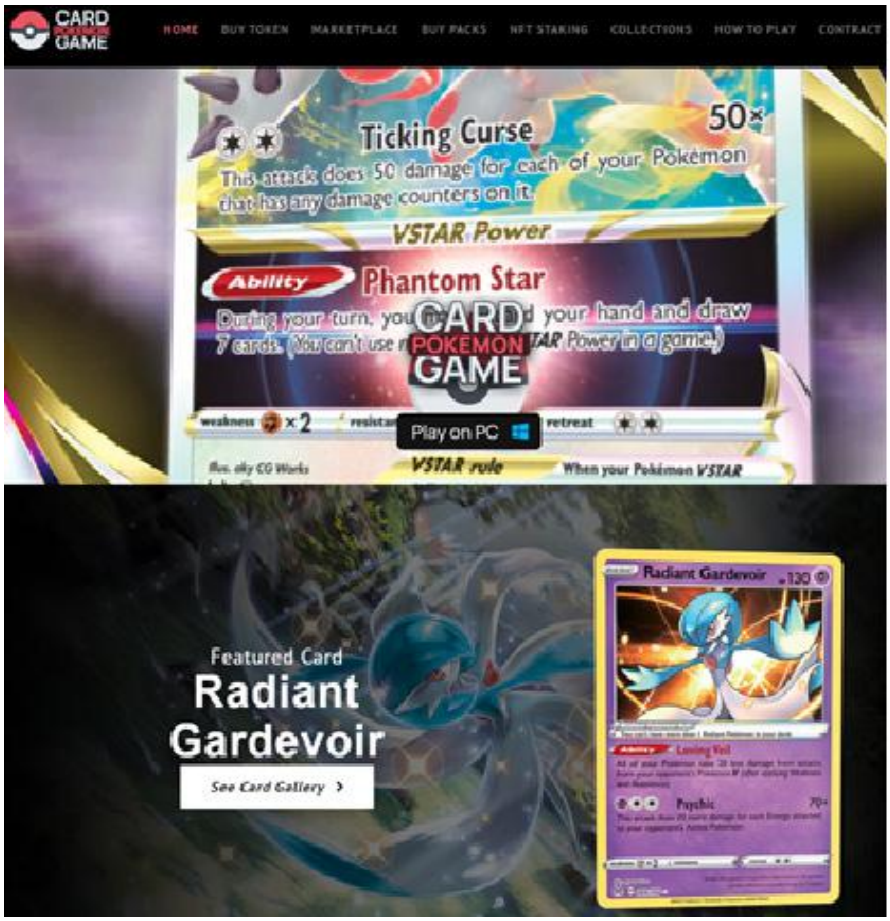
هکرها با push کردن NFT با بازی pokemon دستگاه‌های ویندوزی را تحت فشار قرار می‌دهند

یکی از بحث‌های داغ و به روز در حوزه اینترنت و شبکه بین الملل NFT[1] یا رمز غیرمثلی است. در این قسمت توجه شما را به نحوه سوء استفاده از این توکن جلب میکنیم:

هکرها از وب سایت بازی کارتی Pokemon NFT که به خوبی ساخته شده برای توزیع ابزار دسترسی از راه دور NetSupport و کنترل دستگاه‌های قربانیان استفاده می‌کنند.

وب‌سایت «pokemon-go[.]io» که در زمان نگارش این مقاله هنوز آنلاین است، ادعا می‌کند که میزبان یک بازی کارتی جدید NFT است که براساس امتیاز Pokemon ساخته شده است و به کاربران یک بازی استراتژیک همراه با سود سرمایه‌گذاری NFT ارائه می‌کند.

با توجه به محبوبیت هر دو یعنی هم پوکمون و هم NFT، برای اپراتورهایی با پورتال مخرب، جذب مخاطبان به سایت از طریق malspam، پست‌های رسانه‌های اجتماعی و غیره نباید سخت باشد.



(سایتی که یک بازی تقلبی Pokemon NFT را تبلیغ می‌کند.)

1-non-fungible Token

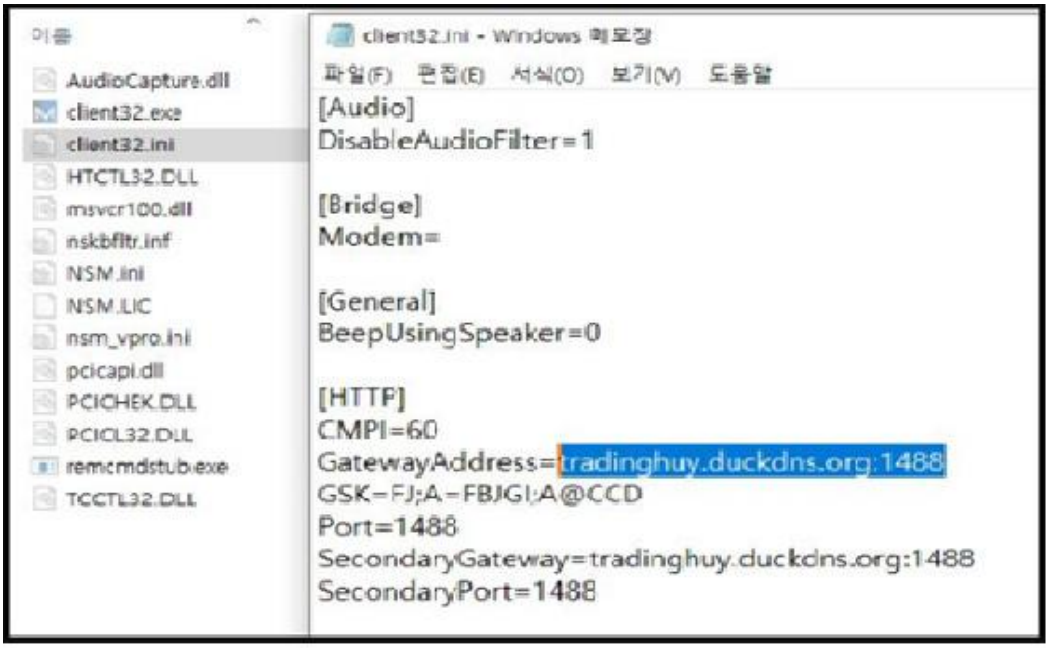
کسانی که روی دکمه «Play on PC» کلیک می‌کنند یک فایل اجرایی را دانلود می‌کنند که شبیه نصب‌کننده بازی قانونی است، اما در واقع، ابزار دسترسی از راه دور NetSupport[1] را روی سیستم قربانی نصب می‌کند.

این عملیات توسط تحلیلگران ASEC فاش شد ،آنها گزارش دادند که سایت دومی نیز در این کمپین مورد استفاده قرار گرفته است، به نام beta-pokemoncards[.]io، اما از آن زمان به بعد آفلاین شده است.

اولین نشانه‌های فعالیت این کمپین در دسامبر ۲۰۲۲ ظاهر شد، در حالی که نمونه‌های قبلی بازیابی شده از VirusTotal نشان می‌داد که همان اپراتورها یک فایل Visual Studio جعلی را به جای بازی Pokemon جا زده‌اند(عوض کردند).

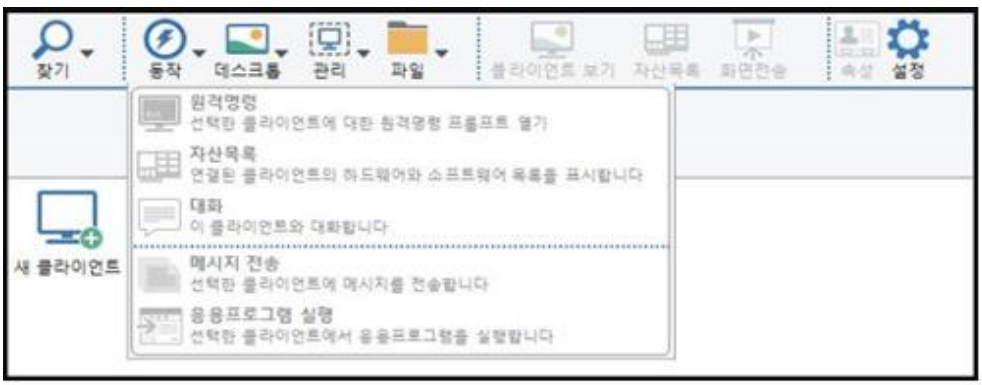
حذف NetSupport RAT

فایل اجرایی %APPDATA% و برنامه های کمکی آن در یک پوشه جدید در مسیر (“client32.”) NetSupport RAT %exe نصب می‌شوند. آنها روی حالت «مخفی» تنظیم می‌شوند تا از شناسایی قربانیانی که سیستم خود را به صورت دستی بازرسی می‌کنند، در امان باشند و به چشم نیا یند .



(فایل‌های حذف شده و محتویات فایل پیکربندی (ASEC))

علاوه بر این، نصب کننده یک ورودی در پوشه شروع اولیه[2] ویندوز ایجاد می‌کند تا مطمئن شود RAT پس از بوت شدن سیستم اجرا می‌شود. از آنجایی که Net-[3] Support RAT یک برنامه قانونی است، هکرها معمولاً از آن استفاده می‌کنند به این امید که از نرم افزار امنیتی فرار کنند.



1-RAT
2-Startup
3-NetSupport Manager

هکرها اکنون می‌توانند از راه دور به دستگاه کاربر متصل شوند تا داده ها را سرقت کنند، بدافزارهای دیگر را نصب کنند یا حتی تلاش کنند تا بیشتر در شبکه پخش شوند.

در حالی که NetSupport Manager یک محصول نرم افزاری قانونی است، معمولاً توسط هکرها به عنوان بخشی از برنامه و هدف مخربی که دارند استفاده می‌شود.

در سال 2020، مایکروسافت در مورد عوامل فیشینگ با استفاده از فایل‌های اکسل با مضمون COVID-19 که NetSupport RAT را روی رایانه‌های گیرندگان انداخته بود، هشدار داد.

در آگوست 2022، کمپینی که سایت‌های وردپرس را با صفحات حفاظتی جعلی Cloudflare DDoS هدف قرار می‌داد، NetSupport RAT و Raccoon Stealer را روی کامپیوتر های قربانیان نصب کرد.

NetSupport Manager از کنترل صفحه نمایش از راه دور، ضبط صفحه نمایش، نظارت بر سیستم، گروه بندی سیستم از راه دور برای کنترل بهتر و گزینه های اتصال زیادی از جمله رمزگذاری ترافیک شبکه پشتیبانی می‌کند. با این حال، عواقب چنین عفونتی ، گسترده و شدید است که عمدتاً مربوط به دسترسی غیرمجاز به داده‌های حساس کاربر و دانلود بدافزار است.

تلاش ما
حفظ امنیت
شماست...