خبرنامه الکترونیکی ۶۱

مرکز تخصصی آپا دانشگاه سمنان

شماره شصت و یکم، سال ششم، تیر ۱۴۰۲ | کاری از تیم تولید محتوای مرکز تخصصی آپا دانشگاه سمنان

در این شماره می‌خوانید:

وابسته‌های باج‌افزاری ،
اخاذی سه‌گانه،
و اکوسیستم وب تاریک

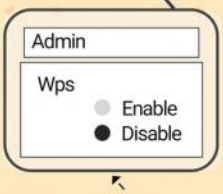
https://cert.semnan.ac.ir info.cert@semnan.ac.ir 023-31535019 @semcert

چگونه مودم Wi-Fi خود را امن کنیم؟

مرکز آپا دانشگاه سمنان

۱- نام (SSID) شبکه را مخفی کنید.

۲- قابلیت WPS را غیرفعال کنید.



۳- قدرت سیگنال مودم را تا حد امکان کم کنید.

۴- دیوار آتش مودم را فعال کنید

۵- در تنظیمات امنیتی از WPA۲ با رمزنگاری AES+TKIP استفاده کنید

۶- از SSID و پسورد پیچیده استفاده کنید.

۷- با استفاده از MAC Filtering تنها به دستگاه‌های شناخته شده اجازه ورود بدهید

چگونه در هنگام اتصال به شبکه‌های Wi-Fi امن بمانیم؟

۱- از افزونه HTTPS Everywhere استفاده کنید.

۲- ترجیحا در مکان‌های عمومی به شبکه‌های Wi-Fi متصل نشوید.

۳- از ضدویروس استفاده کنید.

۴- از یک VPN مطمئن استفاده کنید.

۵- در صورت عدم نیاز، Wireless را غیرفعال کنید.

فهرست

خبر

آموزش

مرکز آپا دانشگاه سمنان

خبر

آسیب‌پذیری بحرانی در SourceCodester HRM

یک آسیب‌پذیری بحرانی در SourceCodester Human Resource Management System 1.0 شناسایی شده است. مهاجم تایید هویت نشده، می‌تواند از راه دور دستورات SQL را در پایگاه داده اجرا کند.

این آسیب‌پذیری با شناسه CVE-2023-3391 و امتیاز 9.8 ارزیابی شده است و یک عملکرد ناشناخته از فایل detailview.php را تحت تاثیر قرار می‌دهد. دستکاری آرگومان employeeid با یک ورودی ناشناخته، منجر به آسیب‌پذیری تزریق sql و حمله از راه دور می‌شود. این محصول یک سیستم مدیریت منابع انسانی و یک web application است و هدف آن ارائه یک پلتفرم خودکار آنلاین برای مدیریت یا ارسال درخواست مرخصی کارمندان شرکت است.

نرم‌افزار، تمام یا بخشی از دستور SQL را با استفاده از ورودی تحت تاثیر خارجی از یک مولفه می‌سازد، اما عناصر خاصی را که می‌توانند دستور SQL موردنظر را هنگام ارسال به مولفه تغییر دهند، خنثی نمی‌کند و از این رو، بر محرمانگی، یکپارچگی و در دسترس بودن تاثیر می‌گذارد.

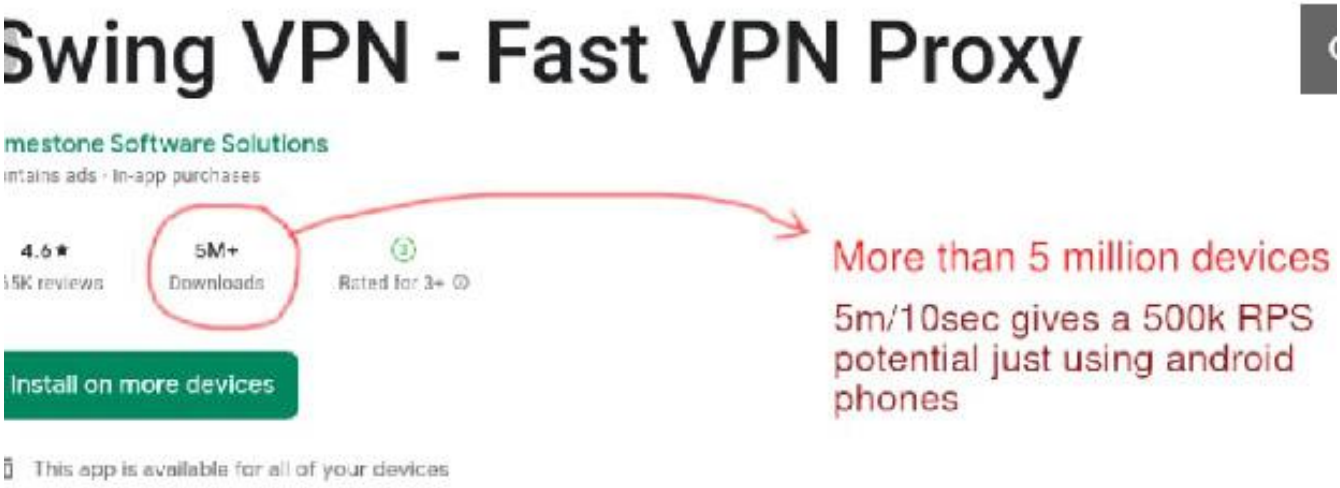
در ورودی‌های قابل کنترل توسط کاربر، پرس و جوی SQL تولید شده می‌تواند موجب تفسیر این ورودی‌ها بجای داده‌های کاربر معمولی شوند. این عامل می‌تواند برای تغییر منطق پرس و جو برای دور زدن بررسی‌های امنیتی، یا درج عبارات اضافی که پایگاه داده back-end را تغییر می‌دهد، استفاده شود. این آسیب پذیری موجب می‌شود SQL هیچ تمایزی بین صفحات کنترل و داده ایجاد نکند.

این آسیب‌پذیری به دلیل پاک سازی ناقص داده‌های ارائه شده توسط کاربر در اسکریپت detailview.php وجود دارد. کاربر از راه دور، می‌تواند یک درخواست ساختگی را به برنامه آسیب‌پذیر ارسال کند و دستورات SQL از راه دور را در پایگاه داده اجرا کند.

اکسپلویت موفق این آسیب‌پذیری ممکن است به مهاجم از راه دور اجازه دهد تا داده‌ها را در پایگاه داده بخواند، حذف کند، اصلاح کند و کنترل کاملی بر برنامه آسیب‌پذیر بدست آورد. این اکسپلویت بصورت عمومی افشا نشده است و ممکن است مورد استفاده قرار گیرد.

گزارش شناسایی باتنت DDoS در برنامه محبوب اندروید Swing VPN

با توجه به دسترس بودن برنامه Swing VPN در دستگاه های Android و iOS ، محققان تنها نسخه اندروید را به عنوان یک بات نت DDoS شناسایی کردند. برنامه Swing VPN که در فروشگاه رسمی گوگل پلی با نام Swing VPN - Fast VPN Proxy موجود است، بیش از ۵ میلیون بار و بخصوص توسط کاربران ایرانی دانلود شده است. نرم‌افزار Swing VPN یک برنامه VPN قانونی است که توسط Limestone Software Solutions برای سیستم‌های اندروید و iOS توسعه‌یافته است. بااین‌حال، به گفته محقق سایبری به نام لکرومی، نسخه اندروید این برنامه یک باتنت DDoS است و گفته می‌شود که دارای هدف مخربی است زیرا می‌تواند حملات Distributed Denial-of-Service[1] را انجام دهد.



۱- حملات DDoS

همه چیز از زمانی شروع شد که دوست لکرومی به او اطلاع داد که الگوی درخواست‌های غیرمعمولی روی گوشی همراهش را مشاهده کرده است. گوشی به صورت مداوم درخواست‌ها را هر 10 ثانیه به یک وبسایت خاص ارسال می‌کرد. ادعا می‌شد که اپلیکیشن از تاکتیک‌های مختلفی برای پنهان کردن اقدامات خبیثانه‌اش استفاده کرده است تا حمله به‌صورتی که قابل تشخیص نباشد، انجام شود. ابتدا، لکرومی این مشکل را به علت وجود نرم‌افزار مخرب یا ویروس می‌پنداشت. با این حال، بررسی‌های بیشتر نشان داد که تمام درخواست‌ها از اپلیکیشن Swing VPN ارسال می‌شوند که دوست لکرومی آن را در گوشی خود نصب کرده بود. درخواست‌ها به همان وبسایتی ارسال می‌شدند که دوست لکرومی تاکنون به آن دسترسی یا بازدیدی نداشته بود، که این امر باعث شک و تردید پژوهشگر نسبت به این اپلیکیشن شد. برای بررسی‌های بیشتر، لکرومی مشاهده کرد که اپلیکیشن Swing VPN برخی از درخواست‌ها را به یک وبسایت ارسال می‌کند.

او مشخص کرد که اپلیکیشن بلافاصله پس از نصب، انتخاب زبان و پذیرش سیاست حفظ حریم خصوصی، آدرس IP واقعی را تشخیص می‌دهد. سپس یک درخواست با عنوان "What is my IP?" به بینگ و گوگل ارسال می‌کند. لکرومی همچنین فهمید که اصولاً برای یافتن فایل‌های پیکربندی جهت بارگذاری آدرس‌های IP را از پاسخ‌ها استخراج می‌کند.

بعد از شناسایی نوع پیکربندی مورد نیاز، اپلیکیشن درخواست‌هایی به دو فایل پیکربندی متفاوت که در حساب Google Drive شخصی توسعه دهنده ذخیره شده‌اند ارسال می‌کند. این فایل‌ها از سرورهای شخصی خاص، چند مخزن GitHub یا حساب‌های Google Drive درخواست می‌شوند. اپلیکیشن فرآیند مقدماتی خود را با اتصال به شبکه تبلیغاتی برای بارگذاری تبلیغات انجام می‌دهد و در نهایت پیش از رفتن به یک سایت داده‌ها را در حافظه محلی ذخیره می‌کند DDoS.

تا ژوئن ۲۰۲۳، این اپلیکیشن بیش از ۵ میلیون نصب بر روی اندروید داشته است و با تقسیم آن بر ده، پتانسیلی حدود ۵۰۰ هزار درخواست بر ثانیه[1] ایجاد می‌کند. این برای یک حمله DDoS به شدت قابل توجه است. لکرومی به گوگل انتقاد کرد که سیستم امنیتی ضعیفی دارد که به اپلیکیشن‌های مخرب امکان استفاده از دستگاه‌های کاربران بی‌گناه را می‌دهد.

1-RPS

افزایش جهانی حملات DDoS
زیرساخت دیجیتال را تهدید می‌کند

به گفته Nexusguard، در سال 2022، تعداد کل حملات DDoS در سراسر جهان 115.1 درصد نسبت به میزان مشاهده شده در سال 2021 افزایش یافته است.

این داده‌ها همچنین نشان داد که مهاجمان سایبری با هدف قرار دادن پلتفرم‌های کاربردی، پایگاه‌های داده آنلاین و سیستم‌های ذخیره‌سازی مبتنی بر ابر در ISP ها، به تغییر وکتورهای تهدید خود ادامه دادند. این منجر به تأثیر قابل توجه بیشتری در سطح جهانی شد زیرا سازمان‌ها همچنان به انتقال حجم بیشتری از کار خود به فضای ابری ادامه می‌دهند.

تعداد حملات DDoS در سراسر جهان

درحالی‌که تعداد کلی حملات DDoS بیش از دو برابر شد، حداکثر اندازه 361.9 گیگابیت در ثانیه[1] نشان‌دهنده کاهش 48.2 درصدی نسبت به موارد اندازه‌گیری شده در سال 2021 بود. اندازه متوسط حمله نیز 22.4 درصد کاهش یافت.

اکثر تهدیدات DDoS 85.6% در سال 2022 حملات تک وکتور بودند که تقریباً مشابه درصدی است که در سال 2021 مشاهده شد. حملات مبتنی بر UDP[2] و حملات مبتنی بر TCP[3] محبوب ترین‌ها بودند. حملات بر اساس نوع، به ترتیب 72.5% و 23.0% را تشکیل می‌دهند. سایر یافته‌های کلیدی عبارتند از:

سه وکتور اصلی حمله DDoS تقویت NTP[4]، حملات memcached و UDP بودند.

حملات مبتنی بر UDP نسبت به سال گذشته 121.3 درصد افزایش یافته است. حملات مبتنی بر TCP و سایر حملات نیز به طور قابل توجهی رشد کردند.

حملات تقویتی سالانه 414.6 درصد رشد داشته است.

حملات برنامه رشد بسیار زیادی را تجربه کردند که سالانه 718.1 درصد افزایش یافت.

وکتورهای حمله DDoS مبتنی برهوش مصنوعی

اینترنت اشیا می‌تواند برای کاربران مفید باشد و از حملات DDoS جلوگیری کند. با این حال، این فقط گاهی اوقات برای دستگاه‌های IoT صدق می‌کند. آنها سطوح حمله بزرگی دارند و اغلب اصول امنیتی را در طراحی خود نادیده می‌گیرند. برخی از ویجت‌ها به مهاجمان اجازه ورود به سیستم را می‌دهند. کاربران ممکن است گاهی برای تغییر شناسه‌های خود به کمک نیاز داشته باشند.

همانطور که جهان ظهور ChatGPT و دیگر قابلیت‌های هوش مصنوعی و یادگیری ماشین را جشن می‌گرفت، برابری هکرها به سرمایه‌گذاری بر روی همان عملکرد ادامه داد. هکرها، همراه با سازمان‌های جهانی، مهندسان هوش مصنوعی و ML را استخدام می‌کنند. غالباً هکرها و سازمان‌های بین‌المللی رقیبی برای استعداد مشابه هستند.

1-Gbps

۲- پروتکل دیتاگرام کاربر
۳- پروتکل کنترل انتقال
٤- پروتکل زمان شبکه

سازمان‌های جهانی ارزش هوش مصنوعی و توانایی پردازش و منطقی کردن داده‌ها را تشخیص می‌دهند. هکرها ارزش پردازش پزشکی قانونی حملات DDoS گذشته یا فعلی را می‌بینند و از هوش مصنوعی و ML برای پیش بینی یک حمله موفقیت‌آمیز آینده استفاده می‌کنند.

Juniman Kasman، مدیر ارشد فناوری Nexusguard، می‌گوید: «اگرچه اندازه حملات DDoS در سال 2022 کاهش یافت اما شاهد جهش قابل توجهی در تعداد کلی حملات بودیم که نیاز به آگاهی و هوشیاری بیشتر را امروزه ضروری‌تر می‌کند».

Kasman در پایان گفت: «حمله‌کنندگان سایبری همچنین به هدف قرار دادن زیرساخت‌های حیاتی در ارائه دهندگان خدمات ارتباطی در سطح ASN، به‌ویژه ISPها، ادامه می‌دهند که منجر به تأثیر بسیار گسترده‌ای می‌شود زیرا سازمان‌های متکی به آن ارائه‌دهندگان نیز تحت تأثیر منفی قرار می‌گیرند».

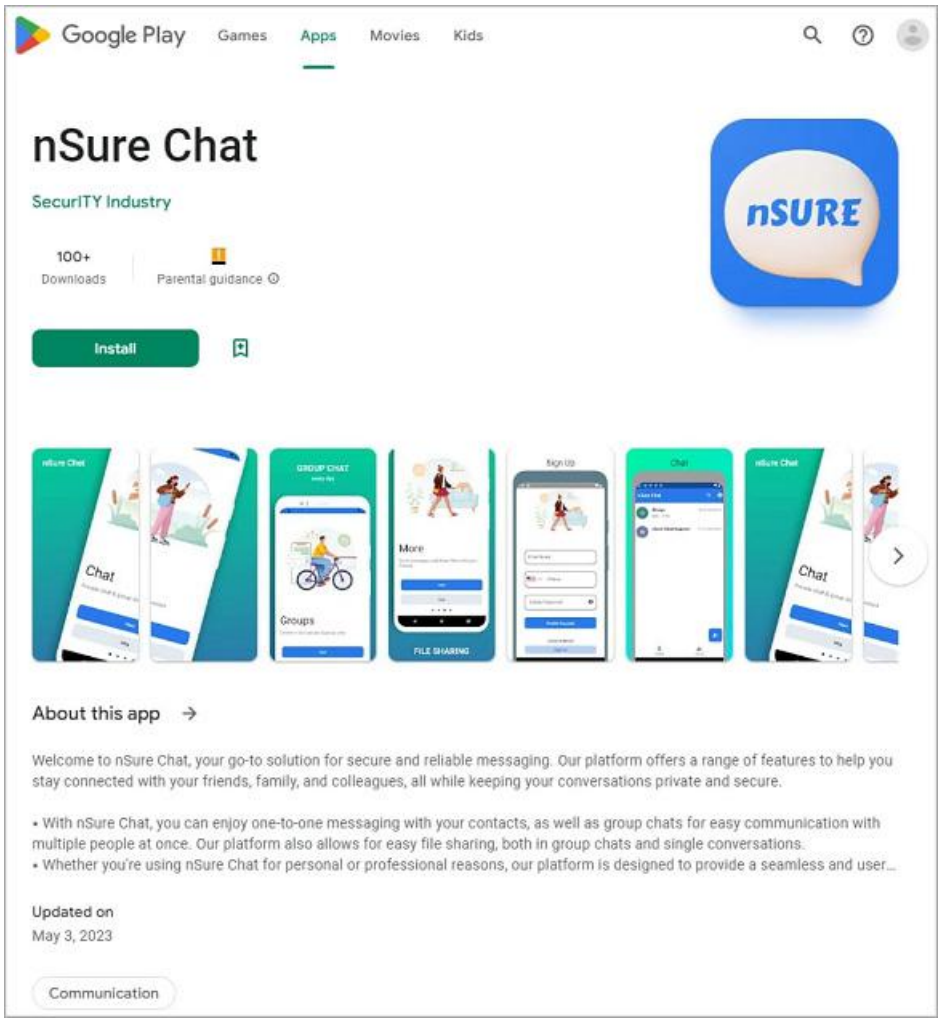
1-CSP

افزایش جهانی حملات DDoS زیرساخت دیجیتال را تهدید می‌کند

نرم افزارهای جاسوسی اندروید استتار شده به عنوان VPN و برنامه های چت در Google Play

سه برنامه اندروید در Google Play توسط عوامل تهدید مورد حمایت دولت برای جمع‌آوری اطلاعات از دستگاه‌های مورد نظر، مانند داده‌های موقعیت مکانی و فهرست‌های مخاطبین استفاده شده‌اند. برنامه‌های مخرب اندروید توسط Cyfirma کشف شدند که این عملیات را با اطمینان متوسط به گروه هکر هندی «DoNot» نسبت داد که با نام APT-C-35 نیز ردیابی می‌شود که حداقل از سال ۲۰۱۸ سازمان‌های برجسته در جنوب شرقی آسیا را هدف قرار داده است. برنامه‌های مورد استفاده در آخرین کمپین DoNot جمع‌آوری اطلاعات اولیه را انجام می‌دهند تا زمینه را برای آلودگی‌های بدافزاری خطرناک‌تر آماده کنند که به نظر می‌رسد اولین مرحله از حملات گروه تهدید باشد.

برنامه‌های مشکوک یافت شده توسط Cyfirma در Google Play عبارتند از nSure Chat و iKHfaa VPN که هر دو از «SecurITY Industry» آپلود شده‌اند. هر دو برنامه و یک برنامه دیگر از همان ناشر که طبق Cyfirma مخرب به نظر نمی‌رسند، در Google Play در دسترس هستند.



تعداد دانلود برای همه برنامه‌های SecurITY Industry کم است که نشان می‌دهد آنها به طور انتخابی علیه اهداف خاص استفاده می‌شوند. این دو برنامه در حین نصب، مجوزهای خطرناکی مانند دسترسی به لیست مخاطبین کاربر[1] و اطلاعات مکان دقیق[2] درخواست می‌کنند تا این اطلاعات را به عامل تهدید منتقل کنند.

توجه داشته باشید که برای دسترسی به مکان هدف، GPS باید فعال باشد، در غیر این صورت، برنامه آخرین مکان شناخته شده دستگاه را واکشی می‌کند. داده‌های جمع‌آوری شده به صورت محلی با استفاده از کتابخانه ROOM اندروید ذخیره می‌شود و بعداً از طریق یک درخواست HTTP به سرور C2 مهاجم ارسال می‌شود.

```
try {
   this.locationManager.requestLocationUpdates("gps", 60000L, 10.0F, this);
   var3 = this.locationManager;
} catch (Exception var6) {
   var10000 = var6;
   var10001 = false;
   break label158;
}

if (var3 == null) {
   return this.loc;
}

Location var9;
try {
   var9 = var3.getLastKnownLocation("gps");
   this.loc = var9;
} catch (Exception var5) {
   var10000 = var5;
   var10001 = false;
   break label158;
}

if (var9 == null) {
   return this.loc;
}

try {
   this.latitude = var9.getLatitude();
   this.longitude = this.loc.getLongitude();
   this.Accu = (double)this.loc.getAccuracy();
   return this.loc;
} catch (Exception var4) {
   var10000 = var4;
   var10001 = false;
}
}

Exception var10 = var10000;
var10.printStackTrace();
return this.loc;
```

C2 مورد استفاده برنامه “https[:]ikhfaavpn[.]com“، “vpn” است. «در مورد nSure Chat، آدرس سرور مشاهده شده سال گذشته در عملیات Cobalt Strike مشاهده شد». تحلیلگران Cyfirma دریافتند که پایه کد برنامه VPN هکرها مستقیماً از محصول قانونی Liberty VPN گرفته شده است.

انتساب این کمپین به گروه تهدید DoNot توسط Cyfirma بر اساس استفاده خاص از رشته‌های رمزگذاری شده با استفاده از الگوریتم AES/CBC/PKCS5PADDING و مبهم سازی Proguard است که هر دو تکنیک مرتبط با هکرهای هندی هستند. علاوه بر این، برخی شباهت‌ها در نام‌گذاری فایل‌های خاص تولیدشده توسط برنامه‌های مخرب وجود دارد که آنها را به کمپین‌های DoNot گذشته مرتبط می‌کند.

محققان بر این باورند که مهاجمان تاکتیک ارسال ایمیل‌های فیشینگ حاوی پیوست‌های مخرب را به نفع حملات پیام‌رسانی نیزه‌ای (هدفمند) از طریق واتس‌اپ و تلگرام کنار گذاشته‌اند. پیام‌های مستقیم در این برنامه‌ها، قربانیان را به فروشگاه Google Play هدایت می‌کند، یک پلتفرم قابل اعتماد که به حمله مشروعیت می‌بخشد، بنابراین می‌توان آنها را به راحتی فریب داد تا برنامه‌های پیشنهادی را دانلود کنند.

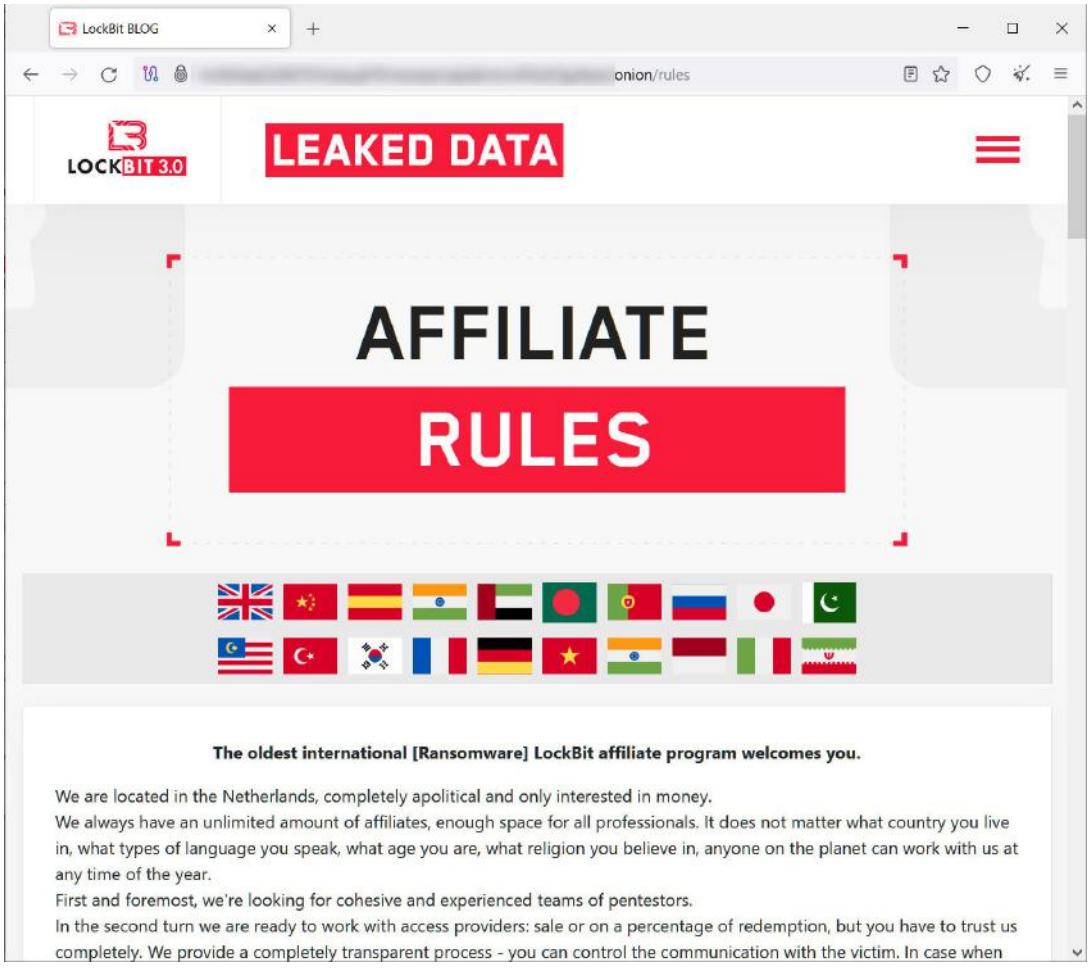
1-READ_CONTACTS
2-ACCESS_FINE_LOCATION

مرکز آپا دانشگاه سمنان

آموزش

وابسته‌های باج‌افزاری، اخاذی سه‌گانه، و اکوسیستم وب تاریک

بسیاری از مردم فقط وب تاریک را با مواد مخدر، جنایت و اعتبارنامه‌های لو رفته می‌شناسند، اما در سال‌های اخیر یک اکوسیستم جرائم سایبری پیچیده و وابسته به هم در سراسر Tor و کانال‌های غیرقانونی در تلگرام ظاهر شده است. این روند را می‌توان با بررسی گروه‌های باج‌افزار، وابستگان آنها و روش‌های پیچیده‌تر فزاینده‌ای که برای اخاذی از شرکت‌ها استفاده می‌کنند، نشان داد. باج‌افزار بیش از یک دهه است که نگرانی حادی برای سازمان‌ها بوده است اما یکی از روندهای اخیری که می‌بینیم این است که گروه‌ها اکنون در حال ایجاد زیرساخت هستند، اما آلوده سازی واقعی (و در برخی موارد مذاکره) را به «وابستگان»[1] که عملاً نقش پیمانکار گروه باج‌افزار به عنوان سرویس[2] را دارند، برون‌سپاری می‌کنند و در پایان حملات موفقیت‌آمیز، سود را تقسیم می‌کنند. این «کالاسازی جرائم سایبری» امکان آلودگی بیشتر، قربانیان بیشتر و پرداخته‌ای بیشتر را فراهم می‌کند.



صفحه قوانین وابسته به گروه باج‌افزار Lockbit

1-affiliates
2-RaaS

در عین حال، گروه‌هایی را دیده‌ایم که به تاکتیک‌های اخاذی پیچیده‌تر متوسل می‌شوند. گروهی که فقط داده‌های یک شرکت را رمزگذاری می‌کنند، اکنون امری نادر است (اخاذی منفرد)، و برخی از گروه‌ها به طور کامل از رمزگذاری صرف نظر می‌کنند و در عوض بر استخراج داده‌ها و باج‌گیری از کارکنان تمرکز می‌کنند.

انواع مختلف اخاذی باج‌افزار

حال، ببینیم حملات اخاذی یک، دو و سه‌گانه چیست؟

اخاذی واحد

این حمله باج‌افزار "سنتی" است که در آن گروهی داده‌های یک شرکت را رمزگذاری می‌کنند و برای انتشار داده‌ها به پرداخت نیاز دارند.

اخاذی مضاعف

یک گروه باج‌افزار داده‌های یک شرکت را رمزگذاری می‌کند، اما ابتدا داده‌ها را استخراج می‌کند، که اگر قربانی پرداخت نکند، در تاریخ خاصی در وبلاگ‌های باج‌افزار پست می‌شوند.

اخاذی سه‌گانه

این گروه نه تنها داده‌ها را رمزگذاری و استخراج می‌کند، بلکه همچنین تلاش می‌کند:

- کارکنان خاص را هدف قرار دهد
- یک حمله DDoS به شرکت انجام دهد
- به اشخاص ثالث شرکت اطلاع دهد

یا در غیر این صورت تلاش می‌کند اهرمی اضافی ایجاد کند تا قربانی را مجبور به پرداخت کند.

خطر حملات باج‌افزار چقدر است؟

در سال 2022 ما شاهد افشای اطلاعات 2947 شرکت در وبلاگ‌های باج‌افزار بودیم. بدون شک صدها یا هزاران شرکت دیگر قربانی شدند و برای جلوگیری از افشای اطلاعات، باج پرداخت کردند.

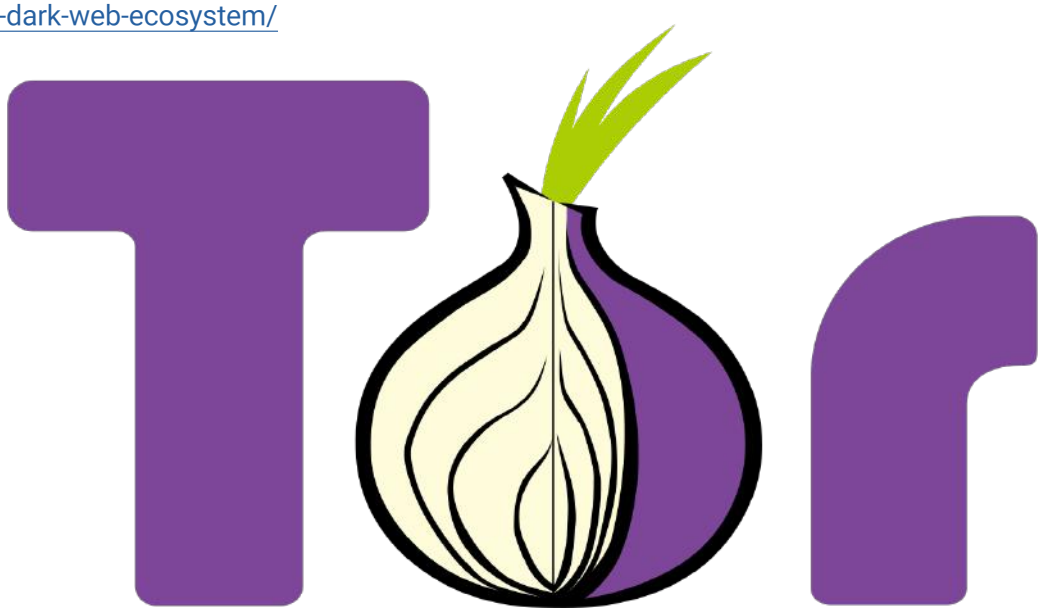
در سال 2023، در شش ماه اول سال شاهد بیش از 2000 نشت داده در وبلاگ‌های باج‌افزار بوده‌ایم که به احتمال زیاد سال 2023 یک سال رکورد برای افشای داده‌های باج‌افزار خواهد بود.

چگونه باج‌افزار سه‌گانه اخاذی از اکوسیستم جرائم سایبری استفاده می‌کند

ظهور باج‌افزار سه‌گانه اخاذی نیز مستقیماً با تغییر قابل توجه دیگری در چشم‌انداز تهدید همزمان است: ظهور بدافزار سرقت اطلاعات. انواع Infostealer مانند Redline، Vidar و Racoon رایانه‌های فردی را آلوده می‌کنند و اثر انگشت مرورگر، داده‌های میزبان، و مهمتر از همه، تمام اطلاعات کاربری ذخیره‌شده در مرورگر را استخراج می‌کنند.

منبع:

https://www.bleepingcomputer.com/news/security/ransomware-affiliates-triple-extortion-and-the-dark-web-ecosystem/



تلاش ما
حفظ امنیت
شماست...