مرکز آپا دانشگاه سمنان

خبرنامه الکترونیکی ۵۲

مرکز تخصصی آپا دانشگاه سمنان

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

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

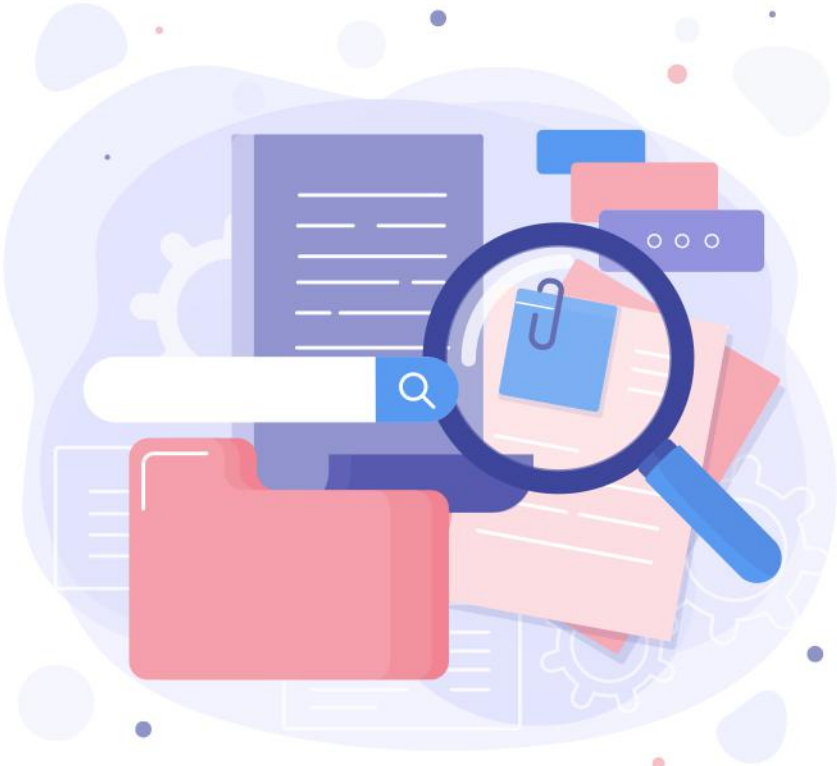
هـــر تمـــاس و پیامـــی از طـرف هـر موسسـه‌ای کـه شـــما را پـــای خودپـــرداز بکشـــاند حتما **کلاهبرداری** است.

فهرست

خبر

آموزش

خبرکوتاه



مرکز آپا دانشگاه سمنان

خبر

تبدیل Discord به بدافزار سرقت رمز عبور توسط بسته‌های مخرب PyPi

ده‌ها بسته مخرب PyPi کشف شده است که با نصب بدافزار، کلاینت Discord را تغییر می‌دهد تا به یک درب پشتی سرقت اطلاعات تبدیل شود و داده‌ها را از مرورگرهای وب و Roblox به سرقت می‌برد.

دوازده بسته در تاریخ ۱ آگوست ۲۰۲۲ توسط کاربری به نام «scarycoder» در فهرست بسته پایتون[1] آپلود شد و توسط محققان Snyk کشف شد.

بسته‌های پایتون وانمود می‌کنند که ابزارهای Roblox، مدیریت رشته‌ها و ماژول‌های اصلی هک هستند، اما هیچ‌کدام عملکرد وعده داده شده را ندارند. در عوض، بسته‌ها بدافزار سرقت رمز عبور را روی دستگاه‌های توسعه‌دهندگان نصب می‌کنند.

به عنوان بخشی از گزارش جدید Snyk، محققان یکی از این بسته‌های مخرب پایتون به نام «cyphers» را تجزیه و تحلیل می‌کنند که نشان می‌دهد چگونه کد مخرب پنهان شده در فایل «setup.py» برای نصب دو فایل اجرایی بدافزار «ZYXMN.exe» و «ZYRBX.exe.» از یک سرور Discord CDN استفاده می‌شود.

اولین باینری، ZYXMN.exe، برای سرقت اطلاعات از گوگل کروم، کرومیوم، مایکروسافت اج، فایرفاکس و اپرا، از جمله رمزهای عبور ذخیره شده، تاریخچه مرورگر، کوکی‌ها و سابقه جستجو استفاده می‌شود.

برای سرقت اطلاعات از مرورگرها، این بدافزار کلید اصلی پایگاه داده محلی مرورگر وب را رمزگشایی می‌کند تا داده‌های متن اصلی سابقه جستجو، سابقه مرور، کوکی‌ها، نشانک‌ها، رمزهای عبور ذخیره شده و کارت‌های اعتباری ذخیره شده را بازیابی کند. سپس این اطلاعات از طریق وب هوک Discord برای عوامل تهدید بارگذاری می‌شود.

1-PyPI

با این حال، حتی جالب‌تر، این بدافزار فایل‌های جاوا اسکریپت واقعی مورد استفاده توسط مشتری Discord را تغییر می‌دهد تا یک درب پشتی تزریق کند که می‌تواند اطلاعات را مستقیماً از حساب Discord شما بدزدد.

بدافزار دوم، ZYRBX.exe، تنها بر روی Roblox تمرکز می‌کند و تلاش می‌کند کوکی حساب، شناسه کاربری، موجودی Robux و وضعیت Premium حساب پلتفرم بازی آنلاین را بدزدد و آن را به وب‌هوک Discord منتقل کند.

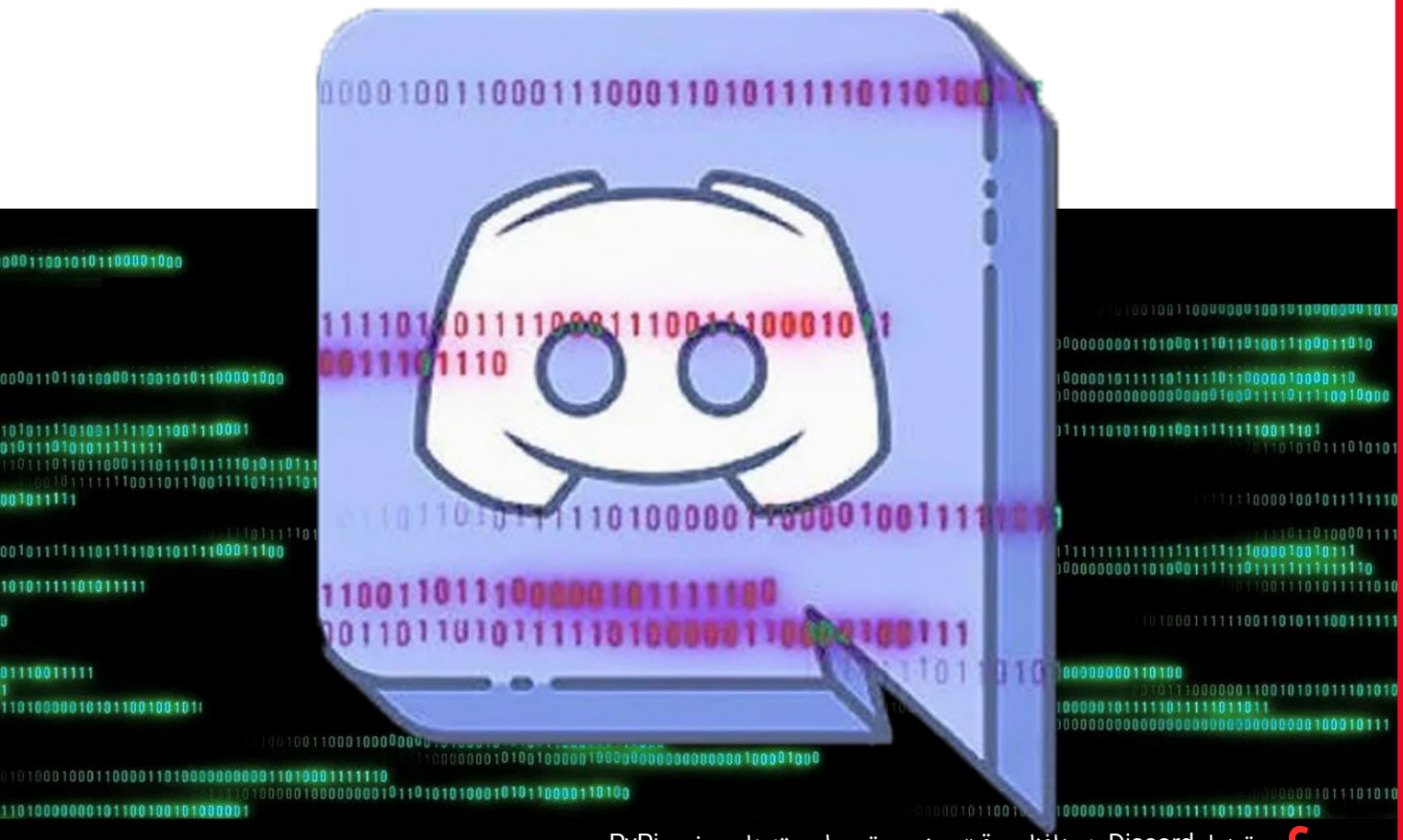
بدافزارهای بیشتر در PyPI

کسپرسکی گزارشی را منتشر کرد که در آن دو بسته دیگر PyPi را ارائه کرد که حاوی بدافزار سرقت اطلاعات هستند و همچنین کلاینت Discord را نیز تغییر می‌دهند.

دزدان در این بسته‌ها بر جمع‌آوری اعتبارنامه حساب‌ها از کیف پول‌های رمزنگاری، Steam و Minecraft تمرکز می‌کنند، در حالی که یک اسکریپت تزریقی ورودی‌هایی مانند آدرس‌های ایمیل، رمزهای عبور و اطلاعات صورت‌حساب را کنترل می‌کند.

پس از این مرحله، سارق پوشه‌های دانلود، اسناد و دسکتاپ میزبان را اسکن می‌کند تا لیست‌های بازیابی 2FA، فایل‌های متنی رمز عبور، توکن‌های Discord، اطلاعات حساب Paypal و موارد دیگر را پیدا کند.

دو مخرب کشف شده توسط کسپرسکی «pyquest» و «ultrarequests» هستند که پروژه‌هایی را با میلیون‌ها بار دانلود تقلید می‌کنند و حتی کد آنها را شبیه‌سازی می‌کنند.



تبدیل Discord به بدافزار سرقت رمز عبور توسط بسته‌های مخرب PyPi

استفاده هکرها از جعبه ابزار Sliver به جای Cobalt Strike

عوامل تهدید، مجموعه تست نفوذ Cobalt Strike را به نفع فریمورک‌های مشابهی که کمتر شناخته شده‌اند، کنار می گذارند. پس از Brute Ratel، کیت منبع باز و چند پلتفرمی به نام Sliver در حال تبدیل شدن به یک جایگزین جذاب است.

با این حال، فعالیت های مخرب با استفاده از Sliver را می‌توان با استفاده از پرس و جوهای شکار[1] استخراج شده از تجزیه و تحلیل جعبه ابزار، نحوه کار و اجزای آن شناسایی کرد.

کنار گذاشتن Cobalt Strike

در طول سال‌های گذشته، Cobalt Strike به عنوان یک ابزار حمله برای عوامل مختلف تهدید، از جمله عملیات باج‌افزار، محبوبیت زیادی پیدا کرده است.

از آنجایی که مدافعان یاد گرفته‌اند حملات را با تکیه بر این جعبه ابزار شناسایی و متوقف کنند، هکرها گزینه‌های دیگری را امتحان می‌کنند که می‌تواند از تشخیص و پاسخ نقطه پایانی[2] و راه‌حل‌های آنتی ویروس فرار کند.

عوامل تهدید بعد از مواجهه شدن با دفاع قوی‌تر در برابر Cobalt Strike، جایگزین‌هایی پیدا کرده‌اند. Palo Alto Networks مشاهده کرد که آنها به Brute Ratel، یک ابزار شبیه سازی حمله خصمانه که برای فرار از محصولات امنیتی طراحی شده است، روی آورده‌اند.

گزارشی از مایکروسافت اشاره می‌کند که هکرها، از گروه‌های تحت حمایت دولت گرفته تا باندهای جرایم سایبری، در حملات بیشتر و بیشتر از ابزار تست امنیتی Sliver مبتنی بر Go[3] استفاده می‌کنند.

یک گروه که Sliver را به کار گرفتند توسط مایکروسافت به عنوان DEV-0237 ردیابی می‌شوند. این باند که با نام FIN12 نیز شناخته می‌شود، با اپراتورهای باج‌افزار مختلفی مرتبط شده است.

در گذشته این باند کدهای باج‌افزار را از اپراتورهای باج افزار مختلف[4] از طریق بدافزارهای مختلف، از جمله BazarLoader و TrickBot توزیع کرده است.

1-hunting queries
2-EDR - Endpoint Detection and Response
۳- ساخته محققان شرکت امنیت سایبری BishopFox
4-Ryuk، Conti، Hive، BlackCat

بر اساس گزارشی از ستاد ارتباطات دولت بریتانیا[1]، عوامل تحت حمایت دولتی روسیه، به ویژه APT29[2] نیز از Sliver برای حفظ دسترسی به محیط‌های در معرض خطر استفاده کرده‌اند.

مایکروسافت اشاره می کند که Sliver در حملات اخیر با استفاده از بارگذار بدافزار[3] Bumblebee به کار گرفته شده است که این بدافزار با گروه مجرمانه Conti به عنوان جایگزینی برای BazarLoader مرتبط است.

شکار فعالیت های مبتنی بر Sliver

با وجود اینکه این یک تهدید جدید است، روش‌هایی برای شناسایی فعالیت‌های مخرب ناشی از فریمورک Sliver و همچنین تهدیدات مخفی‌تر وجود دارد.

مایکروسافت مجموعه‌ای از تاکتیک‌ها، تکنیک‌ها و رویه‌ها (TTP) را ارائه می‌کند که مدافعان می‌توانند برای شناسایی Sliver و سایر فریمورک‌های نوظهور C2 استفاده کنند.

از آنجایی که شبکه کنترل و فرمانSliver از چندین پروتکل (DNS، HTTP/TLS، MTLS، TCP) پشتیبانی می‌کند و اتصالات ایمپلنت/اپراتور را می‌پذیرد، و می‌تواند خود را یک وب سرور قانونی جا بزند، شکارچیان تهدید می‌توانند شنوندگانی (listeners) را برای شناسایی ناهنجاری‌ها در شبکه برای زیرساختSliver تنظیم کنند.

مایکروسافت می‌گوید: «برخی از آثار به جا مانده رایج از بدافزارترکیبات منحصر به فرد هدر HTTP و هش‌های JARM هستند، که دومی تکنیک های انگشت نگاری فعال برای سرورهای TLS [روش شناسی برای Sliver و Bumblebee از RiskIQ] هستند»

مایکروسافت همچنین اطلاعاتی را در مورد نحوه شناسایی بارهای Sliver[4] که با استفاده از پایگاه کد رسمی و غیر سفارشی برای فریمورک C2 ایجاد شده است، به اشتراک گذاشت.

برای کدهای بدافزار Sliver، مایکروسافت توصیه می‌کند پیکربندی‌ها را زمانی که در حافظه بارگذاری می‌شوند استخراج کنید، زیرا فریمورک باید آن‌ها را ابهام‌زدایی و رمزگشایی کند تا بتوان از آنها استفاده کرد.

اسکن حافظه می تواند محققان را قادر به استخراج جزئیاتی مانند داده های پیکربندی کند.

شکارچیان تهدید همچنین می‌توانند به دنبال دستورات مورد استفاده برای تزریق فرآیند بگردند، که کد Sliver پیش‌فرض بدون انحراف از پیاده‌سازی‌های رایج به آن‌ها دست می‌یابد.

مایکروسافت خاطرنشان می‌کند که این جعبه ابزار همچنین برای تزریق دستور به افزونه‌ها و نام‌های مستعار[5]، برنامه‌های NET و دیگر ابزارهای شخص ثالث متکی است.

این فریمورک همچنین از PsExec برای اجرای دستوراتی استفاده می کند که امکان حرکت جانبی را فراهم می کند.

مایکروسافت برای تسهیل شناسایی فعالیت‌های Sliver در محیط خود برای شرکت‌های محافظت شده توسط Defender، مجموعه ای از پرس و جوهای شکار را ایجاد کرده است که می توانند در پورتال Microsoft 365 Defender اجرا شوند.

مایکروسافت تأکید می کند که مجموعه قوانین تشخیص ارائه شده و راهنمای شکار برای پایگاه کد Sliver است که در حال حاضر به صورت عمومی در دسترس است. پرس‌وجوهای مایکروسافت ممکن است انواع سفارشی شده Silver را به خوبی شناسایی نکند.

1-GCHQ

۲- با نام مستعار Cozy Bear، The Dukes، Grizzly Steppe

3-Coldtrain

٤-کد پوسته، فایل های اجرایی، کتابخانه ها/DLL های مشترک و خدمات

5-Beacon Object Files (BFOs)

مجرمان سایبری، بازی‌های محبوب کودکان را هدف بدافزارها قرار می دهند

تحقیقات کسپرسکی نشان می‌دهد که بازیهای Minecraft و Roblox بیشترین فایل‌های مخرب را همراه خود دارند. امروزه با وجود ۳ میلیارد بازیکن بازیهای ویدئویی در سراسر جهان، صنعت بازی تبدیل به هدفی رو به رشد برای مجرمان سایبری شده است. به ویژه بازی ماینکرفت که از محبوبترینهای این صنعت است.

این شرکت امنیتی با استفاده از آمار جمع‌آوری‌شده توسط شبکه امنیتی کسپرسکی[1]، که داده‌های تهدید ناشناس را که مشتریان به صورت داوطلبانه به اشتراک گذاشتند پردازش می‌کند، گسترده‌ترین گونه‌های بدافزار مرتبط با بزرگترین بازی‌های رایانه‌های شخصی و موبایل را بررسی کرد.

کسپرسکی گفت: ما از عناوین بازی‌ها به‌عنوان کلمات کلیدی استفاده کردیم و آن‌ها را در برابر تله‌متری KSN خود اجرا کردیم تا میزان شیوع فایل‌های مخرب و نرم‌افزارهای ناخواسته مرتبط با این بازی‌ها و همچنین تعداد کاربرانی که توسط این فایل‌ها مورد حمله قرار می‌گیرند را تعیین کنیم. همچنین، برنامه‌های تقلب جعلی را برای چندین بازی محبوب، و ارزکاوهایی که بر عملکرد رایانه گیمرها تأثیر می‌گذارند را ردیابی کردیم.

در بین سال های ۲۰۲۱ و ۲۰۲۲، کسپرسکی اعلام کرد که در مجموع ۳۸۴۲۲۴ کاربر با بدافزارهای مرتبط با بازی مواجه بودند و حدود ۹۱۹۸۴ فایل که به عنوان کپی از بازیهای محبوب ظاهر می شوند، در واقع میزبان برنامه های ناخواسته هستند.

1-KSN

به گفته کسپرسکی ماینکرفت محبوب‌ترین طعمه‌ای بود که در ۲۳۲۳۹ فایل مخرب استفاده شد و ۱۳۱۰۰۵ بازیکن را تحت تأثیر قرار داد. با این حال، تعداد فایل‌ها نسبت به سال قبل (۳۶۳۳۶ فایل) ۳۶ درصد کاهش داشت و کاربران نسبت به سال قبل (۱۸۴۸۸۷ کاربر) تقریباً ۳۰ درصد کمتر تحت تأثیر قرار گرفتند.

همچنین محبوب‌ترین بازی‌های بعدی که به‌عنوان فریب برای توزیع بدافزار استفاده می‌شوند ،Roblox Grand Theft Auto، Need for Speed، و Call of Duty هستند.علاوه بر این در حوزه موبایل ،Roblox، Minecraft PUBG، Grand Theft Auto و FIFA بزرگترین اهداف مهاجمان بودند.

در اکثر آلودگی‌هایی که کسپرسکی شاهد آن بود، از فریب دادن کاربران برای نصب دانلودرها استفاده شده بود.

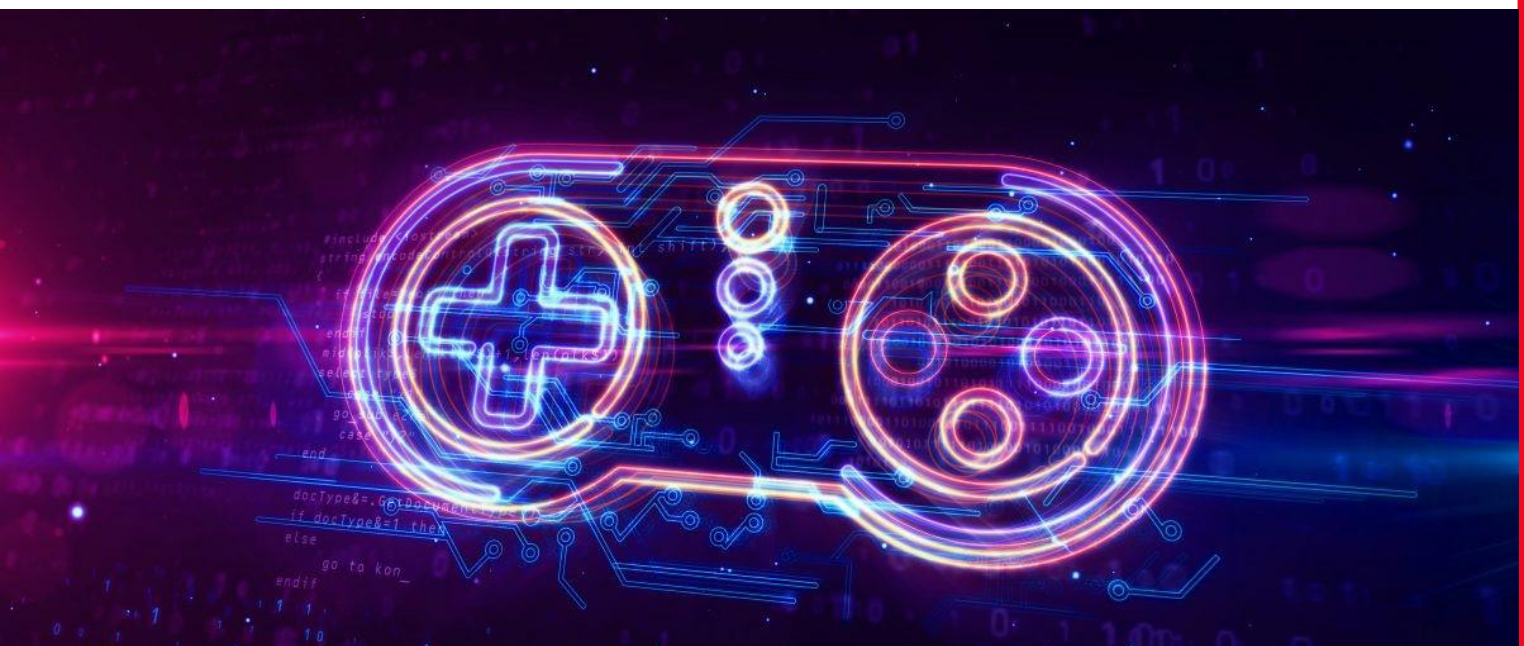
این شرکت خاطرنشان کرد: این نوع نرم افزارهای ناخواسته ممکن است به خودی خود خطرناک نباشد، اما می توان از آن برای بارگذاری تهدیدات دیگر بر روی دستگاه ها استفاده کرد.

از آنجایی که محتوای برخی از حساب‌ها ارزشمند تلقی می‌شوند، فیشرها وب‌سایت‌های جعلی را برای بازی‌هایی مانند GTA و Apex Legends راه‌اندازی کرده‌اند که ادعا می‌کنند ارز درون بازی را تولید می‌کنند، اما در واقع اطلاعات حساب مالکان را برای تصاحب و کشف اطلاعات حساس بهسرقت میبرند.

علاوه بر این مجرمان از بازی‌ها به عنوان فریب برای استفاده از منابع رایانه‌ای کاربران برای استخراج ارزهای دیجیتال استفاده کرده‌اند. توسط کسپرسکی مشخص شده است که سری Far Cry دارای ۵۱۰ فایل مخرب منحصر به فرد و ۱۰۵۰ کاربر آسیب‌دیده و پس از آن Minecraft با ۴۰۶ فایل و با ۹۳ کاربر آسیب‌دیده است. با این حال، این تولیدکننده محصولات امنیتی خاطرنشان کرد که کاربران تحت تأثیر در سال ۲۰۲۲ با شروع «زمستان کریپتو» به نصف کاهش یافتند.

کسپرسکی ابراز ناراحتی کرد که اغلب بازی‌هایی که هدف قرار می‌گیرند، بازی‌هایی هستند که در میان جوانانی که ممکن است از امنیت اطلاعات و رفتارهای مجرمانه سایبری آگاهی کافی نداشته باشند، محبوب هستند. با اینکه این شرکت توصیه‌های معمول برای استفاده از احراز هویت دو مرحله‌ای همراه با گذرواژه‌های قوی و منحصر به فرد را برای محافظت از حساب‌ها بیان کرد، اما بهتر است با فرزندان خود صحبت کنید و هشدارهای لازم را به آنها بدهید.

همچنین کسپرسکی همیشه بر روی تنظیم کردن برنامه‌ها بر روی کانال‌های مطمئن مانند ،Microsoft Store ،Steam Google Play، Apple App Store تاکید داشته است.



مجرمان سایبری، بازی های محبوب کودکان را هدف بدافزارها قرار می دهند

سرمایه گذاری روی
دانش بیشترین بهره را دارد.

مرکز آپا دانشگاه سمنان

آموزش

هک چراغ راهنمایی و رانندگی (بررسی امنیتی)

مقدمه

چراغ‌های راهنمایی و رانندگی در اوایل به صورت سخت‌افزار مستقلی طراحی شدند که هرکدام براساس زمان‌بندی ثابتی اجرا می‌شدند، ولی امروزه، پیشرفت علم آنها را به سیستم‌های پیچیده‌تر و شبکه‌ای تبدیل کرده است. اکنون این کنترل‌کننده‌های ترافیک، چندین برنامه زمان‌بندی را ذخیره می‌کنند، سنسورهای مختلفی در آنها به کار رفته است و با دیگر تقاطع‌ها توانایی برقراری ارتباط دارند تا بتوانند ترافیک را بهتر سازماندهی کنند.

مطالعات نشان می‌دهد یک سیستم هماهنگ چراغ راهنما، از نظر اتلاف زمان، اثرات زیست محیطی و امنیت عمومی مزایای بسیاری دارد، اما به دلیل پراکندگی جغرافیایی جاده‌ها و هزینه اتصالات فیزیکی بین آنها، هماهنگی به سختی انجام می‌شود. امروزه شبکه‌های بی‌سیم به کاهش این هزینه‌ها کمک کرده است و بسیاری از مناطق از سیستم‌های مدیریت ترافیک بی‌سیم هوشمند استفاده می‌کنند.

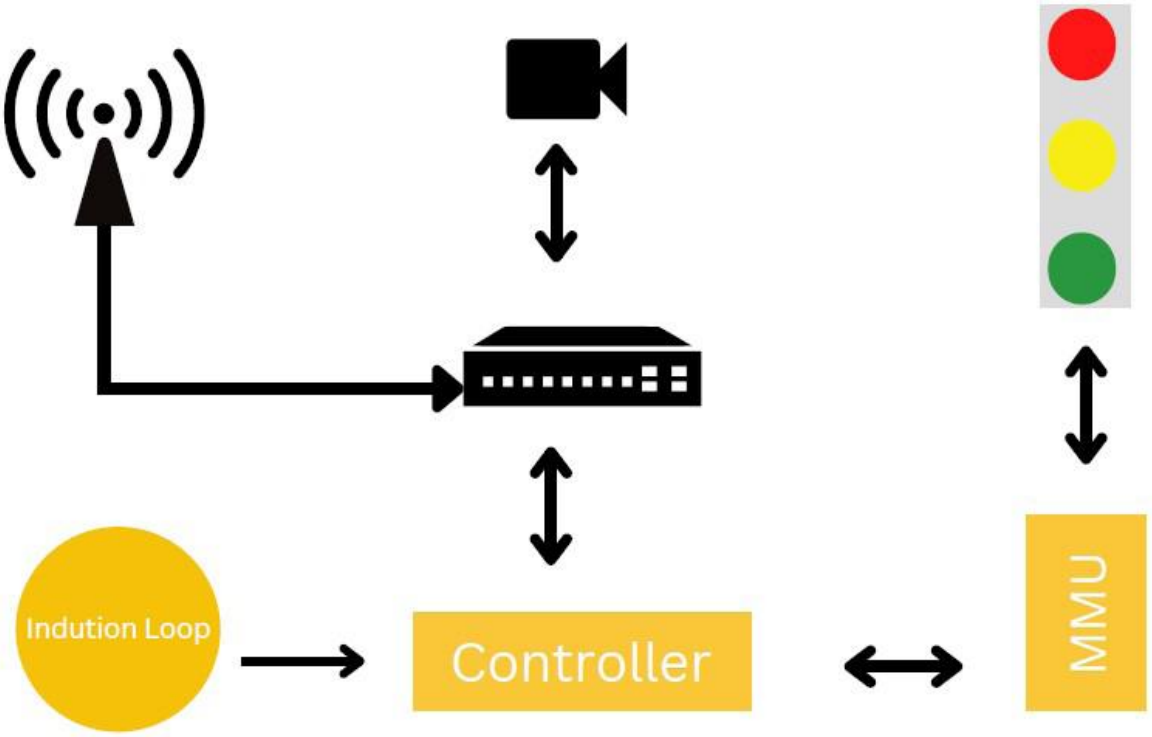
شبکه‌های بی‌سیم قابلیت‌های جدیدی از جمله نظارت در لحظه و هماهنگی بین تقاطع‌های مجاور فراهم می‌کند. با این حال، این پیشرفت‌ها با یکسری مشکلات جانبی ناخواسته همراه بوده است.

سیستم‌های سخت‌افزاری که قبلا فقط از نظر فیزیکی قابل دسترسی بودند، اکنون از راه دور قابل دسترسی هستند و با نرم‌افزار کنترل می‌شوند. همین امر دریچه جدیدی را برای مهاجمان باز می‌کند. برای آزمایش امکان‌سنجی حملات از راه دور در این سیستم‌ها، یک ارزیابی امنیتی بریا سیستم چراغ راهنمای بی‌سیم مستقر در ایالات متحده، انجام شده است.

در این آزمایش، چندین آسیب‌پذیری هم در شبکه بی‌سیم و هم در کنترل‌کننده چراغ راهنمایی کشف شد. با هماهنگی پلیس راه، چندین حمله با موفقیت انجام شد که یکی از آنها توانایی تغییر وضعیت چراغ‌های راهنمایی بود.

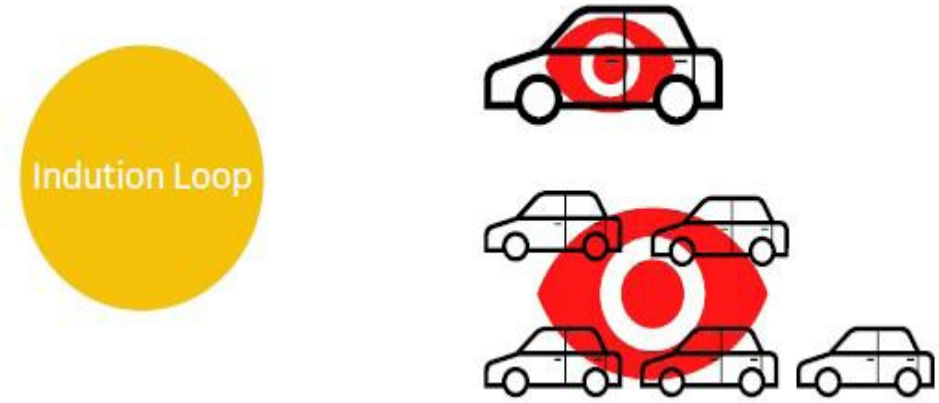
آسیب‌پذیری‌هایی که در زیرساخت‌ها کشف می‌شوند به معنای مشکل دستگاه یا انتخاب طراحی اشتباه نیست، بلکه نشان‌دهنده فقدان سیستماتیک آگاهی امنیتی است. از تجارت آموخته شده از این سیستم می‌توان توصیه‌هایی برای بخش‌های حمل و نقل طراحان سیستم‌های تعبیه شده ارائه داد.

تحلیل یک تقاطع ترافیکی



تقاطع ترافیک مدرن ترکیبی از سنسورها، کنترل‌کننده‌ها و دستگاه‌های شبکه‌ای مختلف است.

سنسورها

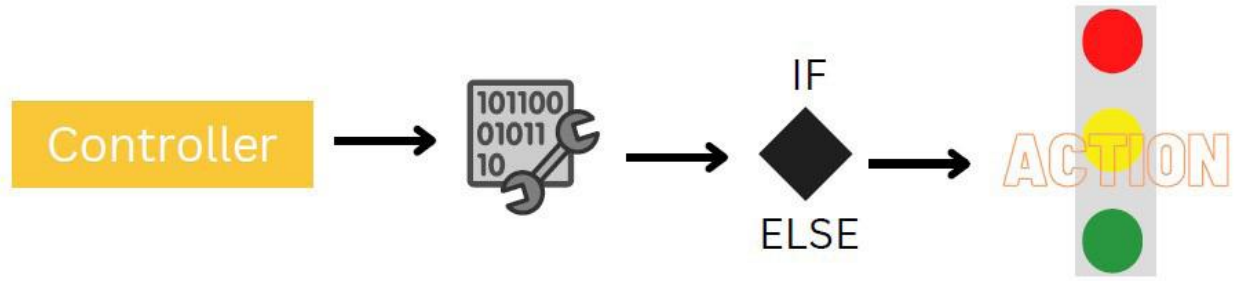


حلقه‌های القایی یا induction loops[1] اغلب برای شناسایی وسایل نقلیه استفاده می‌شود. این دستگاه‌ها در زیر زمین در جاده‌ها کار گذاشته می‌شوند و با اندازه‌گیری تغییر ظرفیت القاء مغناطیسی ناشی از بدنه فلزی خودرو، اتومبیل‌ها را تشخیص می‌دهند. تشخیص ویدئویی نیز اغلب برای تشخیص وسایل نقلیه در تقاطع‌ها استفاده می‌شود.

در ایالات متحده، ۷۹ درصد از تمام سیستم‌های تشخیص خودرو از حلقه‌های القایی یا تشخیص ویدئویی استفاده می‌کنند. سنسورهای مایکروویو، رادار و مافوق صوت کمتر رایج هستند، اما از آنها نیز استفاده می‌شود. معمولا دوربین‌های فیلمبرداری نیز برای بازرسی تقاطع از راه‌دور، نصب می‌شوند.

۱- همچنین به عنوان حلقه‌های داخل زمین شناخته می‌شود.

کنترل کننده‌ها

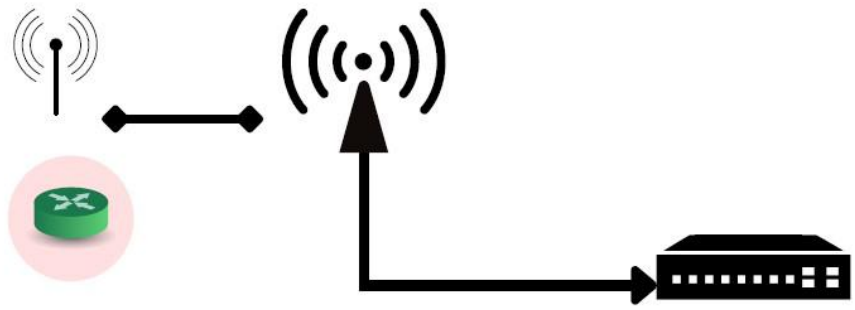


کنترل‌کننده‌های ترافیک ورودی‌های سنسور را می‌خوانند و حالت‌های چراغ را کنترل می‌کنند. کنترل‌کننده معمولا در یک کابینه فلزی در کنار جاده به همراه رله‌هایی برا فعال کردن چراغ‌های راهنمایی قرار می‌گیرد. سنسورها معمولاً مستقیماً به کنترل‌کننده متصل می‌شوند و به آن اجازه می‌دهند.

اطلاعات تشخیص وسیله نقلیه را با کنترل‌های زمان‌بندی از پیش برنامه‌ریزی شده ترکیب کند تا وضعیت فعلی چراغ‌های راهنمایی را تعیین کند.

تقاطع‌ها را می‌توان پیکربندی کرد تا در چندین حالت مختلف کار کنند. در ساده‌ترین حالت، حالت از پیش تعیین شده، چراغ‌ها بر روی زمان‌بندی از پیش تعیین شده کنترل می‌شوند. کنترل کننده‌های پیچیده‌تر در حالت نیمه فعال عمل می‌کنند که در آن خیابان فرعی براساس سنسورها فعال می‌شود و در غیر این صورت، در خیابان اصلی به طور مداوم تردد وجود دارد. در حالت کاملاً فعال، هر دو خیابان براساس ورودی سنسور سازماندهی می‌شوند. کنترل‌کننده‌ها می‌توانند هم به عنوان گره‌هایی ایزوله و هم به عنوان بخشی از یک سیستم به هم پیوسته عمل کنند.

شبکه

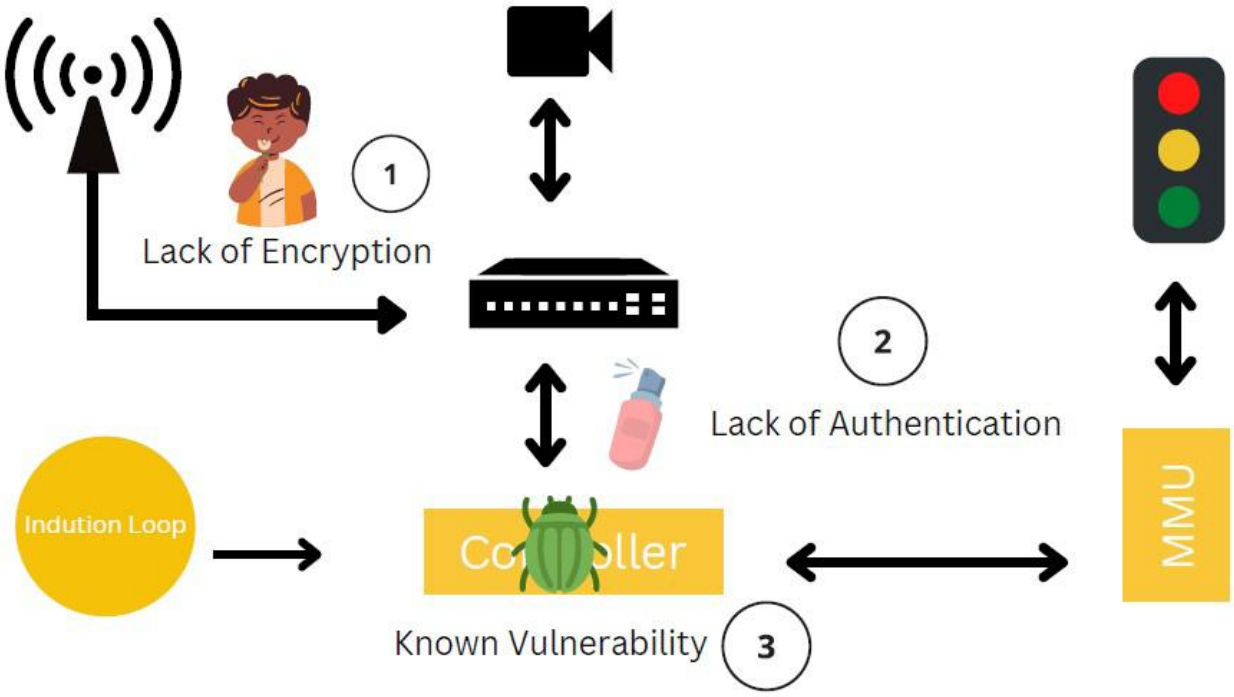


سیستمی که در اینجا بررسی شد، از رادیوهای تجاری موجود استفاده می‌کندکه روی باند ISM با فرکانس ۵٫۸ گیگاهرتز یا ۹۰۰ مگاهرتز کار می‌کنند. یک تقاطع به عنوان یک گره ریشه عمل می‌کند و به یک سرور مدیریت تحت کنترل پلیس جاده متصل می‌شود. تقاطع‌ها اغلب دارای دو رادیو هستند، یک رادیو slave برای ارسال به تقاطع بعدی به سمت ریشه و یک رادیوی master برای دریافت از یک یا چند گره فرزند فراتر از آن. همه دستگاه‌ها یک شبکه خصوصی واحد را تشکیل می‌دهند و به یک زیرشبکه IP تعلق دارند.

واحد مدیریت نقص فنی

واحدهای مدیریت نقص فنی[1] یا به اختصار MMU که به آنها واحدهای مدیریت ناسازگاری نیز گفته می‌شود، مکانیزم‌های امنیتی در سطح سخت‌افزار هستند. آنها به عنوان یک لیست سفید از حالت‌های چراغ راهنمایی عمل می‌کنند و خروجی‌های کنترل‌کننده‌های ترافیک را نظارت می‌کنند تا اطمینان حاصل کنند که هیچ حالت نامعتبری رخ نمی‌دهد. در این قسمت، پیکربندی‌های معتبر به جای نرم‌افزار، روی برد مدار ذخیره می‌شوند و پیکربندی‌های ایمن به صورت دقیق به هم متصل می‌شوند. اگر یک پیکربندی ناامن (مثلا چراغ سبزهای نادرست) شناسایی شود، MMU کنترل‌کننده را لغو می‌کند و چراغ‌ها را به اجبار به یک پیکربندی امن می‌برد.

نقاط آسیب‌پذیر



به طور خلاصه، سه نقطه ضعف عمده در استقرار زیرساخت‌های ترافیکی پلیس‌راه کشف شد:

۱. شبکه به دلیل عدم رمزگذاری، برای مهاجمان قابل دسترسی است.

۲. دستگاه‌های موجود در شبکه به دلیل استفاده از نام‌های کاربری و رمز عبور پیش‌فرض، فاقد احراز هویت مطمئن هستند.

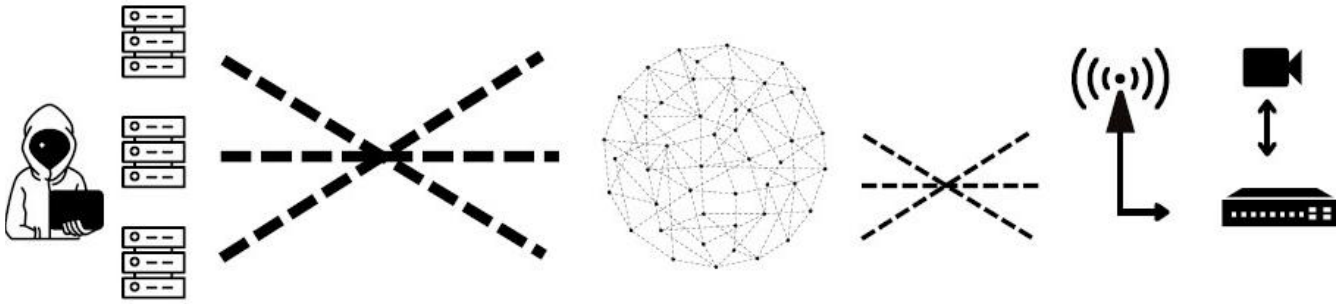
۳. کنترل‌کننده ترافیک، در برابر اکسپلویت‌های شناخته شده آسیب‌پذیر است.

1-Malfunction Management Unit

انواع حملات

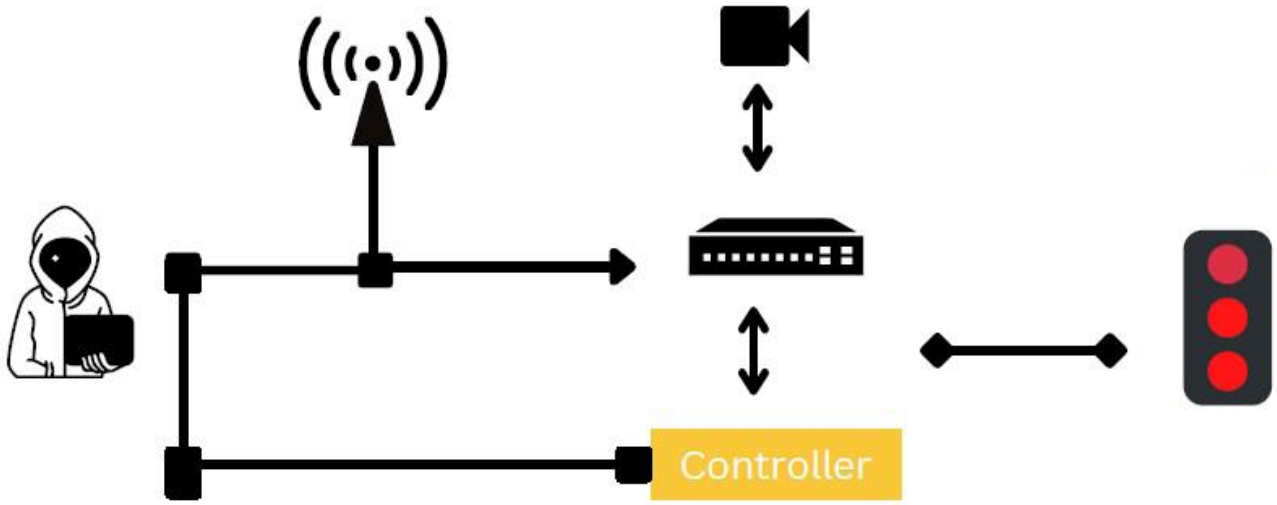
منع سرویس (DoS)

حمله منع سرویس در اینجا، به توقف عملکرد عادی چراغ راهنمایی اشاره دارد. بدیهی‌ترین راه برای ایجاد خرابی در سرویس، تنظیم همه چراغ‌ها روی قرمز است. این امر باعث ازدحام ترافیک و سردرگمی قابل توجهی برای رانندگان می‌شود. از طرف دیگر، مهاجم می‌تواندا تلاش برای پیکربندی ناامن، MMU را به تصرف خود درآورد. این امر باعث می‌شود که چراغ‌ها وارد یک حالت ایمن اما نامناسب شوند.



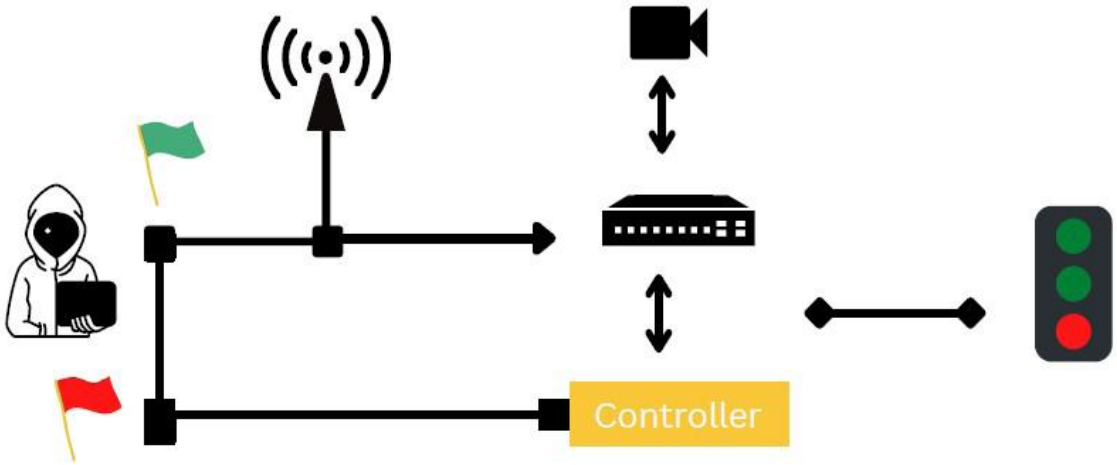
از آنجایی که این حالت می‌تواند از راه دور فعال شود، اما بدون دسترسی فیزیکی به کنترل‌کننده، قابلیت تنظیم مجدد وجود ندارد، در نتیجه مهاجم می‌تواند سریع‌تر از اینکه تکنسین‌ها برای تعمیر آنها اعزام شوند، چراغ‌های راهنمایی را غیرفعال کند. این حملات آشکار هستند و به سرعت توسط پلیس راه شناسایی شده و آنها باید اتصالات شبکه بین تقاطع‌ها را غیرفعال کنند.

ازدحام ترافیک



به طور ماهرانه‌تر، حملاتی می‌تواند علیه کل زیرساخت ترافیک یک شهر انجام شود که زمان‌بندی یک تقاطع را نسبت به تقاطع بعدی، دستکاری می‌کند. این اقدام باعث تراکم ترافیک قابل توجهی می‌شود اما نسبت به اقدامات آشکار، تشخیص آن بسیار کمتر است. این نوع حمله می‌تواند باعث ضرر مالی در جامعه شود. یک مطالعه در شهر بوستون انجام شد و محاسبه کرد که صرفاً پیکربندی مجدد زمان‌بندی ۶۰ تقاطع در یک منطقه از شهر می‌تواند سالانه ۱۲ میلیون دلار در ساعت شخصی، ایمنی، انتشار گازهای گلخانه‌ای و هزینه انرژی صرفه‌جویی کند.

کنترل چراغ راهنما



همچنین یک مهاجم می‌تواند چراغ‌ها را برحسب منافع شخصی کنترل کند، او می‌تواند چراغ‌ها را به رنگ سبز در مسیری رانندگی می‌کند تغییر دهد.
از آنجایی که این حملات از راه دور انجام می‌شوند، حتی می‌تواند این کار را به طور خودکار در حین رانندگی انجام دهد و پس از عبور او از تقاطع، چراغ‌ها دوباره به وضعیت عادی خود بازگردند.
در اقدامی مخرب‌تر، می‌توان چراغ‌ها را به صورت هماهنگ با حمله دیگری به قرمز تغییر داد تا باعث ازدحام ترافیک و کندی حرکت خودروهای اورژانس شود.

منبع: www.hadess.io

مرکز آپا دانشگاه سمنان

خبر کوتاه

دور زدن ویژگی امنیتی جدید اندروید ۱۳ توسط توسعه‌دهندگان بدافزار

1

semCERT
@semcert

دور زدن ویژگی امنیتی جدید #اندروید 13 توسط توسعه دهندگان #بدافزار

در نسخه‌های قبلی اندروید، بیشتر بدافزارهای تلفن همراه از طریق برنامه‌های dropper موجود در Play Store که به عنوان برنامه‌های قانونی ظاهر می‌شوند، به میلیون‌ها دستگاه راه پیدا می‌کردند.

2

semCERT
@semcert

به این صورت که در طول نصب، برنامه‌های بدافزار از کاربران می‌خواهند به مجوزهای مخاطره‌آمیز دسترسی داشته باشند و سپس با سوءاستفاده از امتیازات سرویس دسترسی، کدهای مخرب را بارگذاری کنند.

3

semCERT
@semcert

در اندروید 13، #گوگل تلاش کرد بدافزار موبایلی را که می‌خواست مجوز قدرتمند اندروید را فعال کند، فلج کند. یکی از این مجوزها AccessibilityService است و این بدافزار پس از فعال کردن این مجوزها، کار مخفیانه و مخربی در پس‌زمینه انجام می‌دهد.

4

semCERT
@semcert

مهندسان امنیتی گوگل یک ویژگی «تنظیمات محدود» را معرفی کردند که برنامه‌های جانبی را از درخواست امتیازات سرویس دسترس‌پذیری مسدود می‌کند و عملکرد را به APKهای Google Play محدود می‌کند.

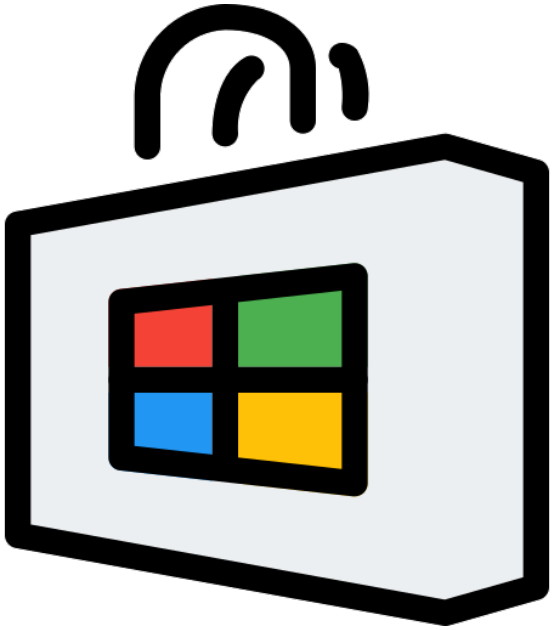
5

semCERT
@semcert

با این حال، محققان ThreatFabric توانستند یک کد اثبات مفهوم تولید کنند که به راحتی این ویژگی امنیتی جدید را دور زده و به خدمات دسترسی، دسترسی پیدا می‌کند.

✅ منبع: Bleeping computer

ربودن ADFS توسط گروه Cozy Bear



1

semCERT
@semcert

ربودن ADFS توسط گروه Cozy Bear

مایکروسافت بدافزار جدیدی را کشف کرده است که توسط گروه هکر روسی APT29 استفاده می‌شود. مهاجم با کمک این بدافزار میتواند به عنوان هر شخصی در یک شبکه احراز هویت شود.

2

semCERT
@semcert

به عنوان یک عامل جاسوسی سایبری تحت حمایت دولت، APT29 از قابلیت جدید برای پنهان کردن حضور خود در شبکه های اهداف خود، معمولاً دولت و سازمان های مهم در سراسر اروپا، ایالات متحده و آسیا استفاده می‌کند.

3

semCERT
@semcert

ابزار مخرب جدید کهMagicWebنام دارد، تکامل یافته«FoggyWeb»است که به هکرها اجازه می‌دهد تا به پایگاه داده پیکربندی سرورهای Active Directory Federation Services (ADFS) نفوذ کنند،گواهی‌های امضای توکن و رمزگشایی توکن را رمزگشایی کنند وکدهای اضافی را ازسرور فرمان و کنترل(C2)واکشی کنند.

4

semCERT
@semcert

ابزار MagicWeb یک DLL قانونی مورد استفاده توسط ADFS را با یک نسخه مخرب جایگزین می کند تا گواهی‌های احراز هویت کاربر را دستکاری کند و ادعاهای (claims) ارسال شده در توکن های تولید شده توسط سرور را تغییر دهد.

✅ منبع: bleeping computer

آسیب‌پذیری‌های روز صفر QNAP در حملات باج‌افزاری استفاده می‌شود!

1

semCERT
@semcert

آسیب‌پذیری‌های روز صفر QNAP در حملات باج‌افزاری استفاده می‌شود!

شرکت QNAP به مشتریان خود در مورد حملات باج افزار DeadBolt که از روز شنبه با بهره‌برداری از یک آسیب‌پذیری روز صفر در نرم‌افزار Photo Station آغاز شده است هشدار داده است.

2

semCERT
@semcert

این شرکت نقص امنیتی را با به‌روزرسانی اصلاح کرده است اما حملات ادامه دارد.

روز دوشنبه شرکت QNAP تهدید امنیتی DEADBOLT را شناسایی کرد که با بهره‌برداری از آسیب‌پذیری نرم‌افزار Photo Station به رمزگذاری دستگاه‌های NAS دارای اینترنت و بدون حفاظت می‌پردازد.

3

semCERT
@semcert

شرکت QNAP دوازده ساعت پس از اینکه باج افزار DeadBolt شروع به حمله کرد، به‌روزرسانی‌های امنیتی را منتشر کرد و از مشتریان NAS خواست فوراً Photo Station را به جدیدترین نسخه به‌روزرسانی کنند.

4

semCERT
@semcert

علاوه بر این QNAP به کاربران خود پیشنهاد می‌کند QuMagie را که یک ابزار مدیریت ذخیره‌سازی عکس امن‌تر می‌باشد جایگزین Photo Station کنند.

دستگاه‌های QNAP هدف مکرر گروه‌های باج‌افزار و دیگر مجرمان قرارگرفته‌اند که باعث شده این شرکت در ماه‌های اخیر هشدارهای متعددی را صادر کند.

5

semCERT
@semcert

باج‌افزار DeadBolt در ازای دریافت کلید رمزگشا، مبلغی بیش از هزار دلار را از کاربران آسیب‌دیده درخواست کرده است.
با این حال، سایر گروه‌های باج‌افزار NAS هم مبالغ قابل توجهی از قربانیان خود می‌خواهند.

6

semCERT
@semcert

به عنوان نمونه باج‌افزار Checkmate که در ماه جولای محصولات QNAP NAS را هدف قرار داد برای دریافت کلید از قربانیان خواست 15000 دلار بپردازند.
✅ منبع: Bleeping Computer

تلاش ما
حفظ امنیت
شماست...