خبرنامه الکترونیکی ۶۳

مرکز تخصصی آپا دانشگاه سمنان

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

در این شماره می‌خوانید:

محافظت از سرورهای Microsoft IIS
در برابر حملات بدافزار

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

مرکز آپا دانشگاه سمنان

سرمایه‌گذاری روی دانش بیشترین بهره را دارد...

فهرست

خبر

آموزش

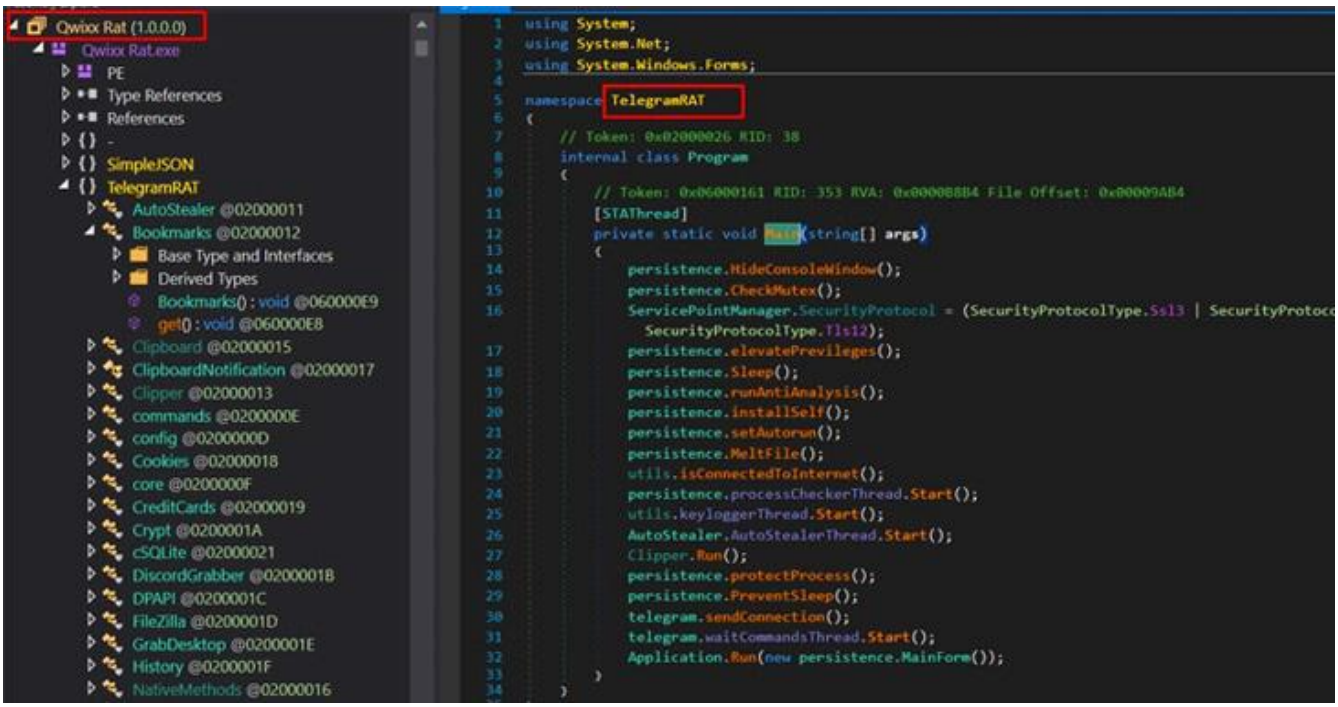
مرکز آپا دانشگاه سمنان

خبر

گزارش بدافزار QwixxRAT

این نرم‌افزار نقش یک "Remote Access Trojan" یا "RAT" را دارا می‌باشد که به وسیله عامل تهدید خودش از طریق پلتفرم‌های تلگرام و دیسکورد برای فروش عرضه می‌شود. بعد از نصب بر روی سیستم‌های ویندوز قربانی، این نرم‌افزار مخرب به صورت پنهانی اطلاعات حساس را جمع‌آوری می‌کند و سپس این اطلاعات را به ربات تلگرامی عامل تهدید ارسال می‌کند. این کار به عامل تهدید دسترسی غیرمجاز به اطلاعات حساس قربانی را فراهم می‌کند.

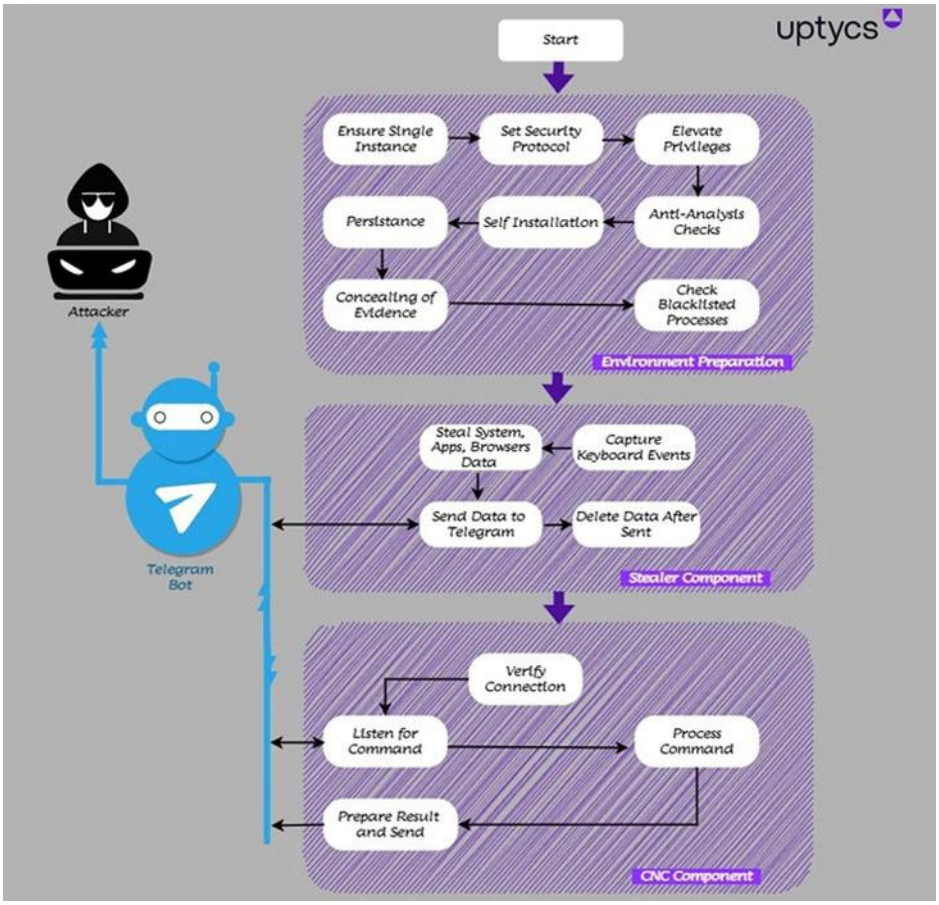
شرکت امنیت سایبری Uptycs که این نرم‌افزار مخرب را در اواخر ماه گذشته کشف کرده است، گفته است که این نرم‌افزار به دقت طراحی شده است تا تاریخچه مرورگر وب، نشان‌ها[1]، کوکی‌ها، اطلاعات کارت اعتباری، کلیدهای فشرده شده[2]، تصاویر صفحه نمایش، فایل‌های با پسوندهای خاص، و اطلاعات از برنامه‌هایی مانند Steam و Telegram را جمع‌آوری کند. این ابزار با قیمت ۱۵۰ روبل برای دسترسی هفتگی و ۵۰۰ روبل برای مجوز دائمی ارائه می‌شود و همچنین نسخه‌ی محدود و رایگانی نیز دارد.



QwixxRAT یک نرم‌افزار دودویی مبتنی بر زبان برنامه‌نویسی C# است که با ویژگی‌های مختلف ضدتجزیه و تحلیل ارائه می‌شود تا به صورت پنهانی عمل کرده و از تشخیص جلوگیری کند. این شامل یک تابع Sleep برای ایجاد تأخیر در فرآیند اجرا و همچنین چک‌های اجرا برای تشخیص اینکه آیا در یک محیط شناور یا مجازی عمل می‌کند، است.

توابع دیگر به آن اجازه می‌دهد که برای لیستی خاص از پردازه‌ها (مانند "netstat"، "processhacker"، "taskmgr"، "tcpview"، "netmon" و "wireshark") نظارت داشته باشد و در صورت شناسایی، فعالیت خود را تا زمانی که فرآیند خاتمه یابد متوقف کند.

1- bookmarks
2- keystrokes



همچنین در QwixxRAT یک ابزار clipper نیز وجود دارد که به صورت پنهانی به اطلاعات حساسی که در کلیپ‌بورد دستگاه کپی شده است دسترسی می‌یابد. هدف از این کار انجام انتقالات غیرقانونی از کیف‌پول‌های رمزارزی می‌باشد.

دستیابی به کنترل و کنترل دستورات Command-and-control یا (C2) از طریق یک ربات تلگرام انجام می‌شود. از طریق این ربات تلگرام دستورات ارسال می‌شوند تا عملیات جمع‌آوری اطلاعات اضافی نظیر ضبط صدا و وب‌کم و حتی خاموش یا راه‌اندازی مجدد دستگاه آلوده انجام شود.

فاش شدن این اطلاعات در هفته‌های پس از آنکه شرکت سایبراینت[1] جزئیات دو نسخه دیگر از نرم‌افزارهای RAT به نام‌های RevolutionRAT و Venom Control RAT را اعلام کرد. این دو نسخه نیز در کانال‌های مختلف تلگرام با ویژگی‌های جمع‌آوری و انتقال داده و اتصال به مرکز کنترل و کنترل (C2) تبلیغ می‌شوند.

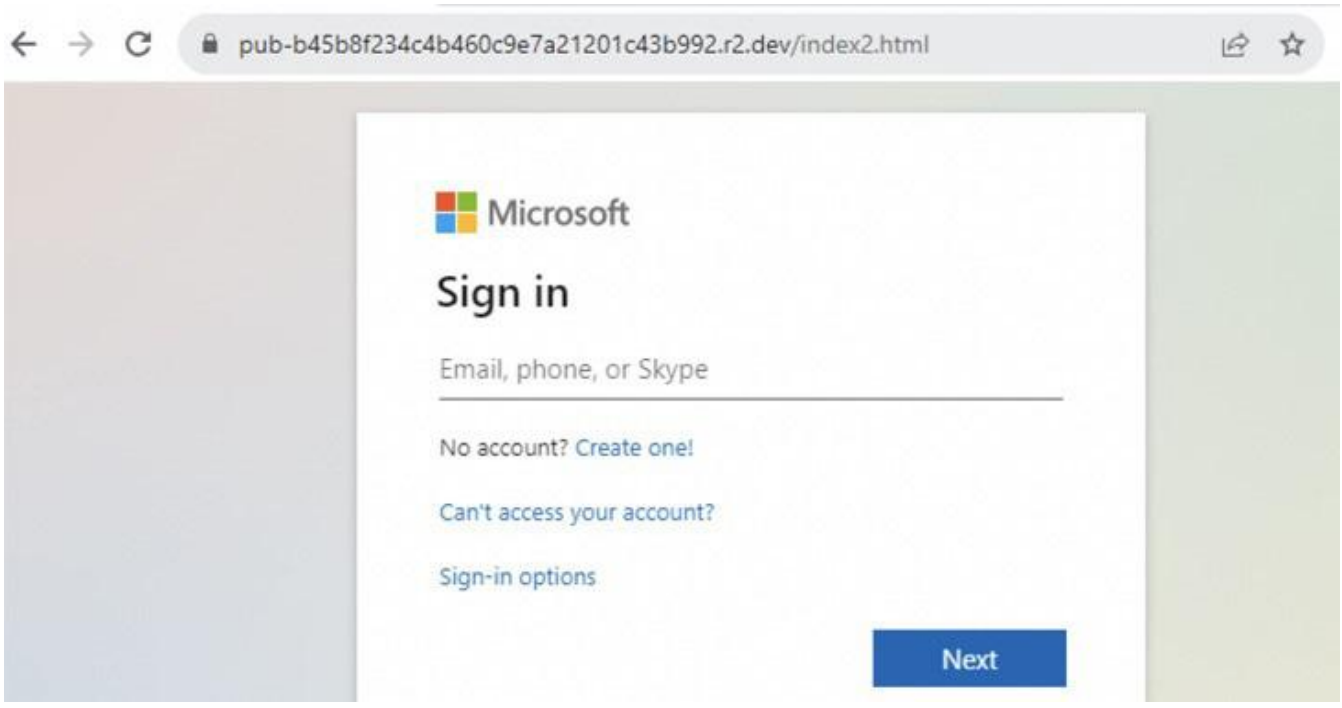
همچنین، این اطلاعات بعد از کشف یک کمپین جاری اعلام شده است که از سایت‌های تخریب شده به عنوان پلتفرم‌های در معرض خطر استفاده می‌کند تا با استفاده از کد جاوا اسکریپت مخرب یک به‌روزرسانی جعلی مرورگر Chrome ارائه دهد. هدف از این عملیات ترغیب قربانیان به نصب ابزار نرم‌افزاری مدیریت از راه دور با نام NetSupport Manager RAT است. استفاده از یک ترفند به‌روزرسانی مرورگر تقلبی با SocGholish یا FakeUpdates هم‌راستایی دارد، اما شواهد قطعی که ارتباط مستقیم بین دو نوع فعالیت را نشان دهد، هنوز محوطه‌ای از تحقیقات است.

Trellix اظهار می‌کند: سوءاستفاده از RATهای آماده در دسترس همچنان ادامه دارد چرا که این ابزارهای قدرتمندی هستند که قادر به تأمین نیازهای مخربان برای انجام حملات و دستیابی به اهدافشان می‌باشند. وی ادامه می‌دهد: اگرچه این RATها ممکن است به طور مداوم به‌روز نشوند، اما ابزارها و تکنیک‌ها برای ارسال این بارهای مخرب به قربانیان احتمالی به تدریج پیشرفت خواهند کرد.

1-Cyberint

سوء استفاده مجرمان سایبری از Cloudflare R2 برای میزبانی صفحات فیشینگ

استفاده تهدیدکنندگان از Cloudflare R2 برای میزبانی صفحات فیشینگ طی شش ماه گذشته شاهد افزایش 61 برابری بوده است. جان مایکل، محقق امنیتی Netskope، گفت: «اکثر کمپین‌های فیشینگ اعتبارنامه ورود مایکروسافت را هدف قرار می‌دهند، اگرچه برخی از صفحات هم هستند که Adobe، Dropbox و سایر برنامه‌های ابری را هدف قرار می‌دهند».



Cloudflare R2، مشابه Amazon Web Service S3، Google Cloud Storage و Azure Blob Storage، یک سرویس ذخیره‌سازی داده برای ابر است. این در حالی است که تعداد کل برنامه‌های ابری که دانلود بدافزار از آن‌ها آغاز می‌شود به 167 افزایش‌یافته است و مایکروسافت OneDrive، Squarespace، GitHub، Share-Point و Weebly در پنج رده بالاتر قرار دارند.

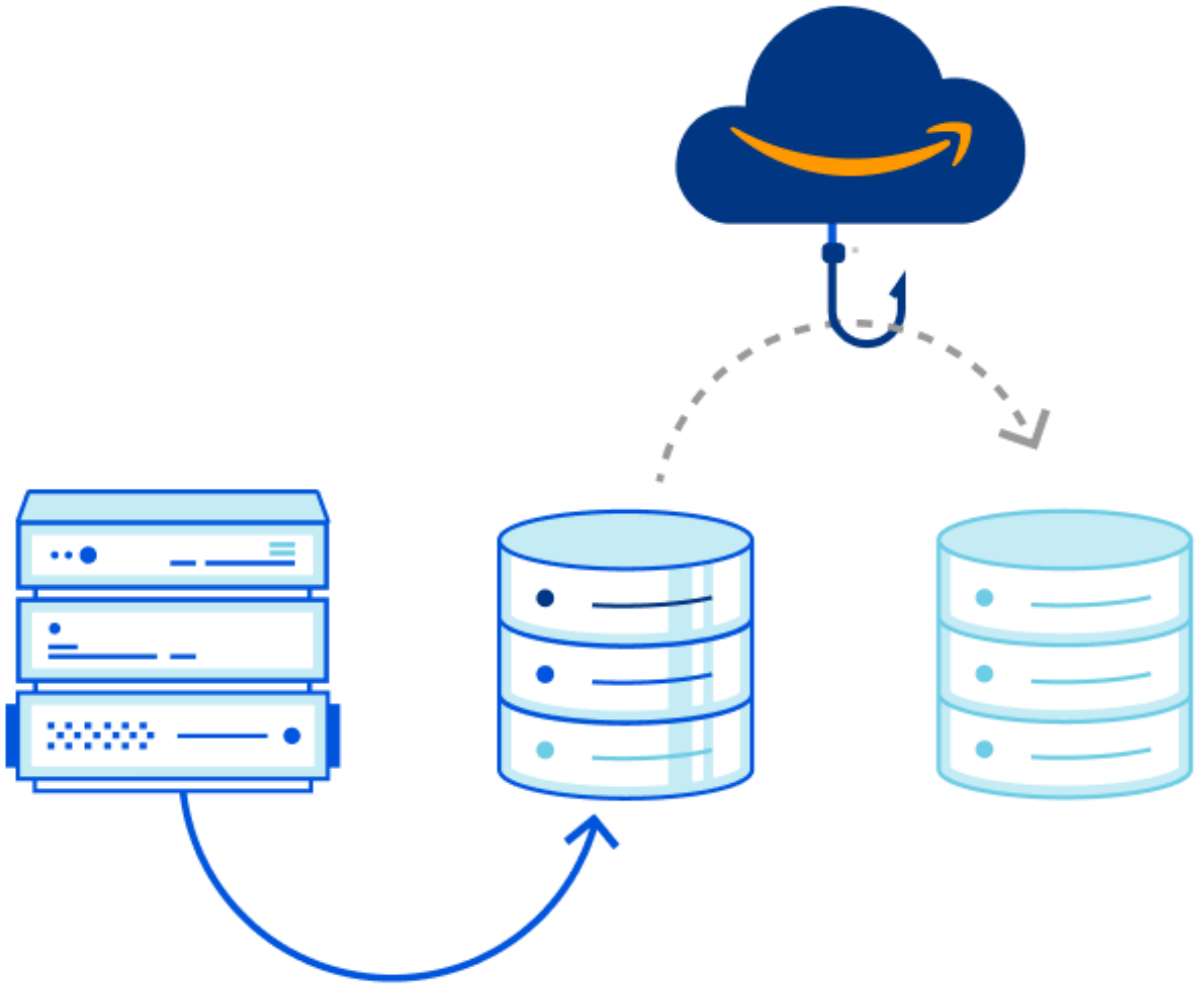
کمپین‌های فیشینگ شناسایی شده توسط Netskope نه تنها از Cloudflare R2 برای توزیع صفحات فیشینگ استاتیک سوءاستفاده می‌کنند، بلکه با استفاده از سرویس Turnstile این شرکت، (جایگزینی برای CAPTCHA)، چنین صفحاتی را در پشت موانع ضد ربات قرار می‌دهند تا از شناسایی فرار کنند.

با انجام این کار، از دسترسی اسکنرهای آنلاین مانند urlscan.io به سایت واقعی فیشینگ جلوگیری می‌کند، زیرا آزمایش CAPTCHA منجر به شکست می‌شود.

به‌عنوان یک لایه اضافی برای فرار از شناسایی، سایت های مخرب طوری طراحی شده‌اند که محتوا را تنها در صورت رعایت شرایط خاص بارگذاری کنند.

مایکل گفت: «این وب‌سایت مخرب نیاز دارد تا از طرف یک سایت مورد ارجاع قرار گیرد که در URL یک مهر زمانی برای نمایش صفحه فیشینگ واقعی داشته باشد. از سوی دیگر، سایت ارجاع دهنده نیاز دارد تا یک سایت فیشینگ را به عنوان پارامتر دریافت کند». در صورتی که هیچ پارامتر URL به سایت ارجاع دهنده ارسال نشود، بازدیدکنندگان به www.google[.]com هدایت می‌شوند.

این اتفاقات یک ماه پس از آن صورت می‌گیرد که این شرکت امنیت سایبری جزئیات یک کمپین فیشینگ را فاش کرد که مشخص شد صفحات ورود جعلی خود را در AWS Amplify برای سرقت اطلاعات بانکی کاربران و مایکروسافت 365 به همراه جزئیات پرداخت کارت از طریق Bot API تلگرام میزبانی می‌کرد.



مرکز آپا دانشگاه سمنان

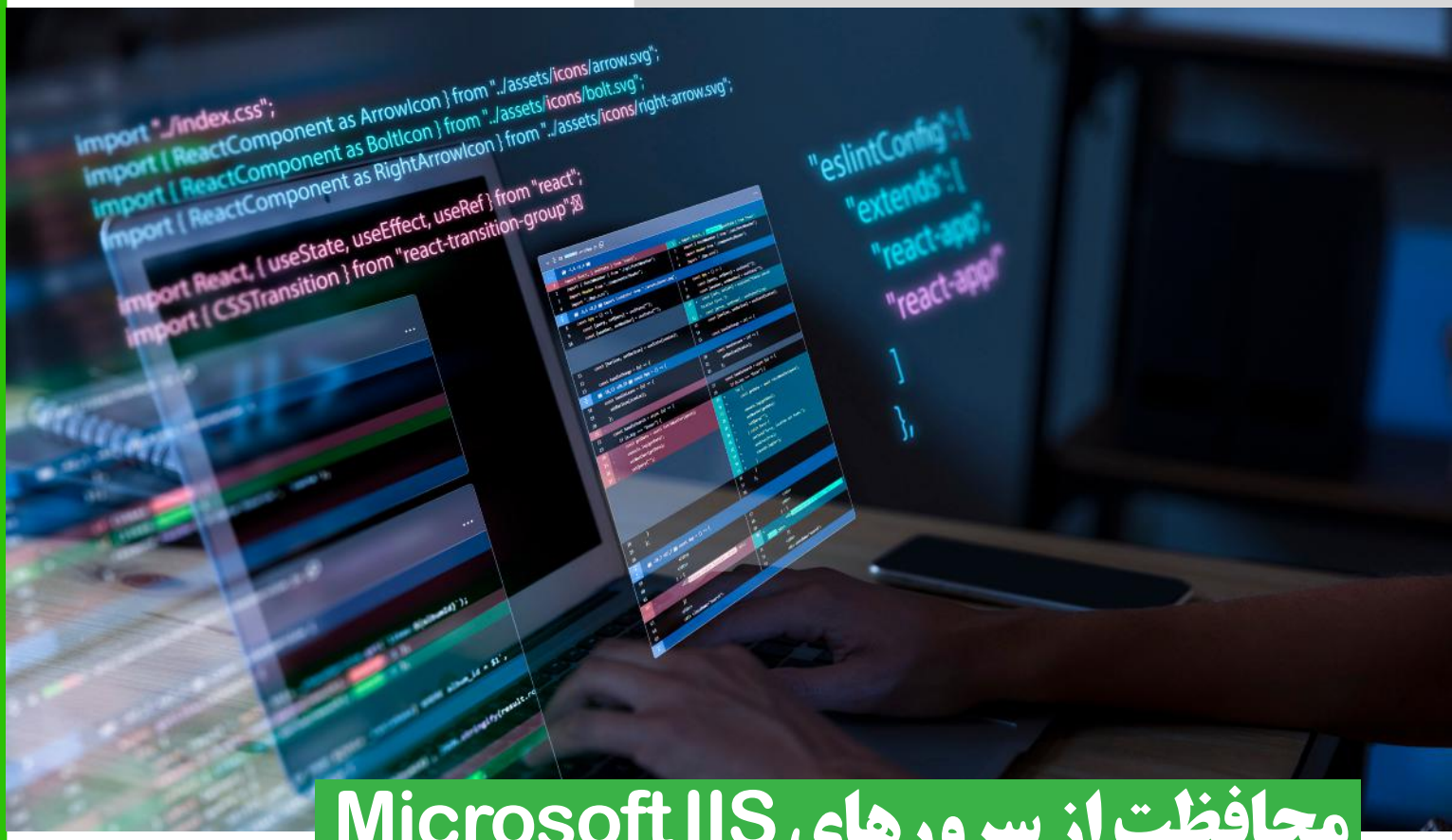
تو فضای مجازی

هر وقت چیزی زیادی خوب باشه،

حتما کلکی تو کاره...!

مرکز آپا دانشگاه سمنان

آموزش



محافظت از سرورهای Microsoft IIS در برابر حملات بدافزار

Microsoft Internet Information Services[1] یک بسته نرم‌افزاری وب سرور است که برای ویندوز سرور طراحی‌شده است. سازمان‌ها معمولاً از سرورهای Microsoft IIS برای میزبانی وب‌سایت‌ها، فایل‌ها و سایر محتواها در وب استفاده می‌کنند. عوامل تهدید به‌طور فزاینده‌ای این منابع اینترنتی را به عنوان میوه‌های کم ارزش برای یافتن و بهره برداری از آسیب‌پذیری‌هایی که دسترسی به محیط‌های فناوری اطلاعات را تسهیل می‌کنند، هدف قرار می‌دهند.

اخیراً، مجموعه‌ای از فعالیت‌های گروه تهدید دائمی پیشرفته Lazarus[2] بر یافتن سرورهای آسیب‌پذیر مایکروسافت IIS و آلوده کردن آنها به بدافزار یا استفاده از آنها برای توزیع کدهای مخرب متمرکزشده است. این مقاله جزئیات حملات بدافزار را تشریح می‌کند و پیشنهادات عملی برای محافظت از سرورهای Microsoft IIS در برابر آنها ارائه می‌دهد.

مروری بر سرورهای Microsoft IIS

IIS برای اولین بار با ویندوز NT 3.51 به‌عنوان یک بسته اختیاری در سال 1995 معرفی شد. از آن زمان، چندین بار تکرار، بهبودها و ویژگی‌های اضافه‌شده برای همسویی با اینترنت در حال تکامل، از جمله پشتیبانی از درخواست‌های HTTP (HTTPS امن) اضافه شده است. Microsoft IIS علاوه بر اینکه یک وب سرور است و درخواست‌های HTTP و HTTPS را ارائه می‌کند، یک سرور FTP برای انتقال فایل و یک سرور SMTP برای خدمات ایمیل نیز دارد.

حمله Lazarus به سرورهای مایکروسافت IIS

Lazarus یک گروه جاسوسی سایبری و جرائم سایبری کره شمالی است که اخیراً مشاهده‌شده است که از آسیب‌پذیری‌های خاص مایکروسافت IIS سوءاستفاده می‌کند. این باند قبلاً برخی از بدنام‌ترین حملات

1-IIS
2-APT

سایبری تاریخ را انجام داده بود، ازجمله حادثه باج افزار WannaCry در سال 2017 و سرقت 100 میلیون دلار ارز مجازی در ژوئن 2022

دور اولیه فعالیت مخرب

تحقیقاتی که در ماه مه 2023 توسط شرکت امنیت سایبری کره جنوبی ASEC انجام شد، تأیید کرد که عوامل تهدیدکننده Lazarus فعالانه سرورهای آسیب‌پذیر مایکروسافت IIS را اسکن می‌کنند و از آنها سوءاستفاده می‌کنند. فعالیت اولیه حول تکنیک‌های بارگذاری جانبی DLL متمرکز بود که از سرورهای آسیب‌پذیر برای اجرای کد دلخواه سوءاستفاده می‌کرد. حملات بارگذاری جانبی DLL با بهره‌گیری از روشی که فرآیند وب سرور w3wp.exe، IIS، کتابخانه‌های پیوند پویا[1] را بارگیری می‌کند، کار می‌کنند.

1-DLL

حملات بیشتر با استفاده از سرورهای IIS برای توزیع بدافزار

دور دیگری از حملات بدافزار شامل سرورهای مایکروسافت IIS، امنیت مالی و نرم‌افزار بررسی یکپارچگی، INISAFE CrossWeb EX را هدف قراردادند. این برنامه که توسط Initech توسعه‌یافته است، از نسخه 3.3.2.41 یا قبل از آن در برابر تزریق کد آسیب‌پذیر است.

تحقیقات 47 شرکت را کشف کرد که توسط بدافزاری که از اجرای نسخه‌های آسیب‌پذیر فرآیند نرم‌افزار inisafecrosswebexsvc.exe، Initech سرچشمه می‌گرفت، کشف کرد. نسخه‌های آسیب‌پذیر CrossWeb EX یک DLL مخرب SCSKAppLink.dll را بارگیری می‌کنند. این DLL مخرب سپس بار مخرب دیگری را واکشی می‌کند و نکته جالب این است که URL مربوط به payload به یک سرور مایکروسافت IIS اشاره می‌کند.

منبع:

https://thehackernews.com/2023/09/protecting-your-microsoft-iis-servers.html?m=1

تلاش ما
حفظ امنیت
شماست...