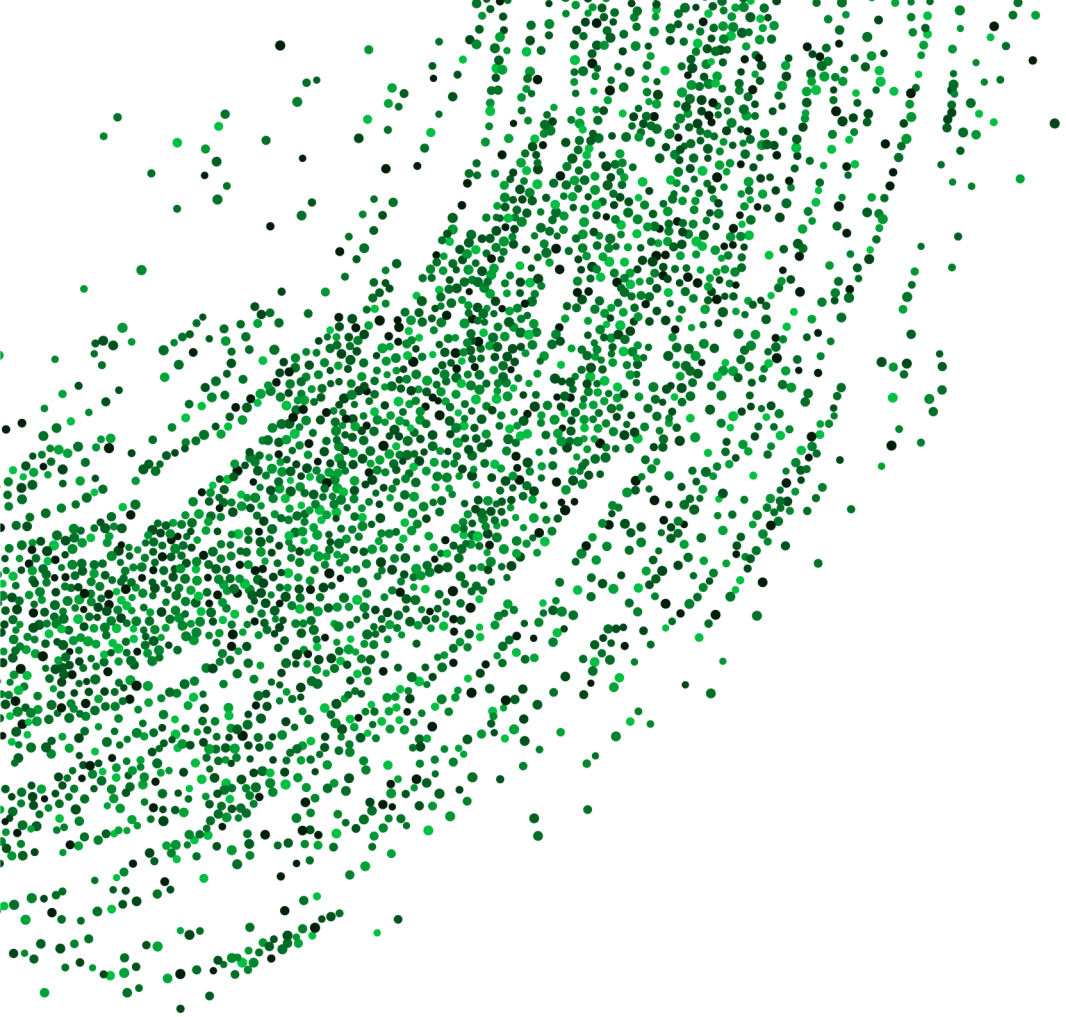
شبکه گستر

امنیت شما | وظیفه ما

ماهنامه
امنیت فناوری اطلاعات

شرکت مهندسی شبکه گستر | سال دوازدهم | اردیبهشت ۱۴۰۱

فهرست مطالب



چکیده مدیریتی

در این شماره از ماهنامه امنیت فناوری اطلاعات شرکت مهندسی شبکه گستر به بررسی مهمترین رخدادها و رویدادهای مرتبط با امنیت فناوری اطلاعات در اولین ماه از سال ۱۴۰۱ پرداخته شده است.

در این شماره به گزارش‌های جدیدی که چند شرکت امنیت سایبری درباره بدافزارهای FFDroider، Lightning Stealer، BazarBackdoor و Mirai منتشر کرده‌اند، خواهیم پرداخت و ویژگی‌های هر یک را که باعث جلب توجه محققان شده‌اند، تشریح خواهیم کرد.

یک جاسوس‌افزار اندرویدی جدید را معرفی خواهیم کرد که به عنوان یک سرویس «Process Manager» ظاهر می‌شود و به‌طور مخفیانه اطلاعات حساس ذخیره‌شده در دستگاه‌های آلوده را سرقت می‌کند.

همچنین گروه امنیتی سیمانتک نیز در گزارشی، مهاجمان چینی Cicada را که اکنون به اهداف متنوع‌تری نظیر سازمان‌های دولتی، حقوقی، مذهبی و مردم‌نهاد در کشورهای مختلف جهان علاقه‌مند شده‌اند، بررسی کرده است. فعالیت‌های مخرب این مهاجمان بر روی دستگاه قربانیان و سابقه فعالیت این گروه در گذشته، نشان می‌دهد که جاسوسی، انگیزه و هدف اصلی آنها می‌باشد.

بر اساس گزارش سایت خبری بلومبرگ که چکیده‌ای از آن نیز در این ماهنامه ارائه شده، کمیسیون ارتباطات فدرال ایالات متحده، شرکت امنیت سایبری روسی کسپرسکی را به فهرست نهادهایی که "خطر غیرقابل قبولی برای امنیت ملی ایالات متحده" دارند، اضافه کرده است. این اولین بار است که یک شرکت روسی به این لیست اضافه می‌شود و به نظر می‌رسد این اتفاق از عواقب جنگ روسیه و اوکراین است.

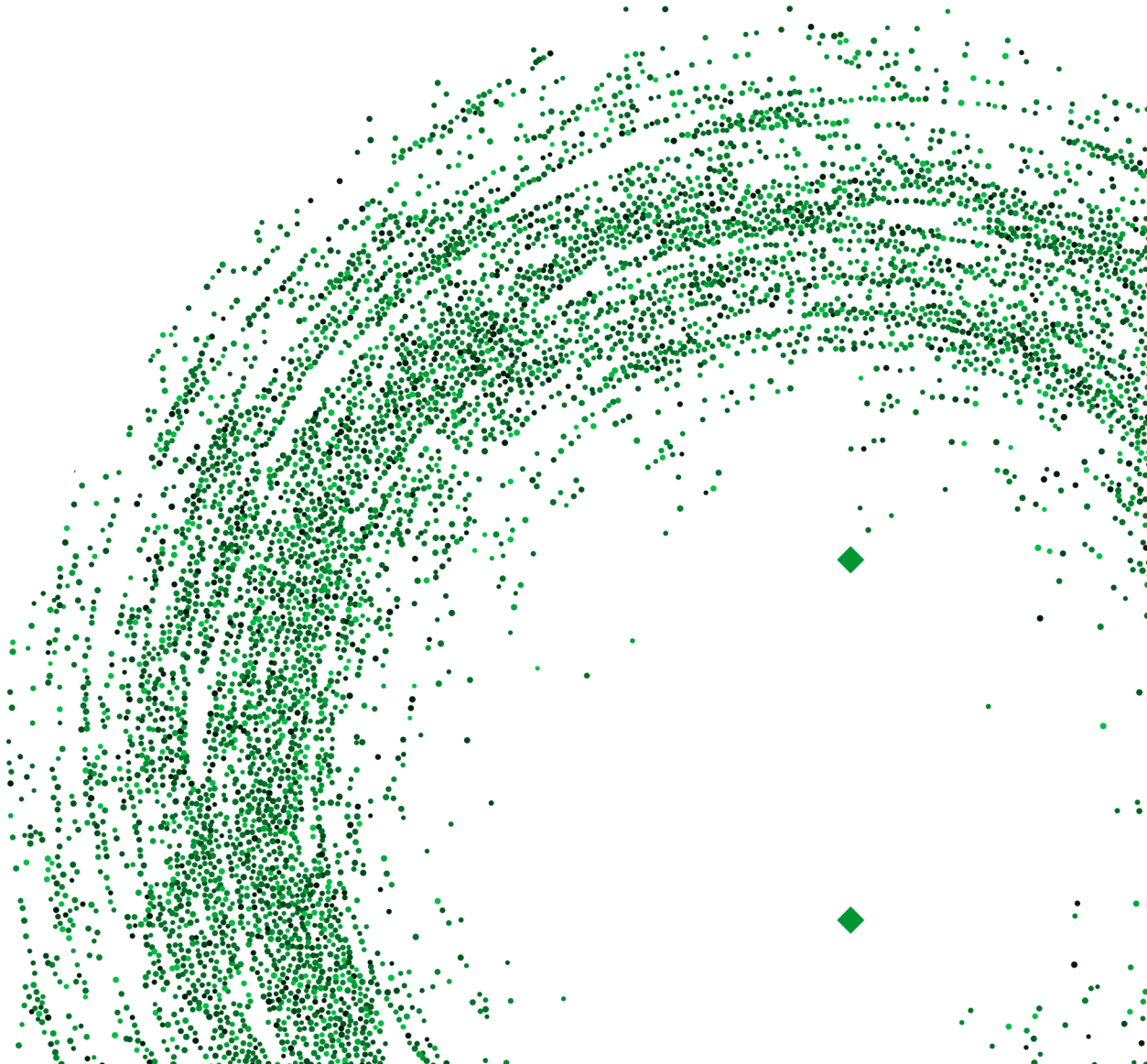
به تحلیل آمار حملات باج‌افزاری ثبت شده در زمستان سال گذشته که توسط شرکت دیجیتال شدوز انجام شده، خواهیم پرداخت. نتایج این تحلیل نشان می‌دهد که در طول این دوره سه ماهه، بیش از نیمی از حملات به تنهایی توسط دو باج‌افزار LockBit 2.0 و Conti انجام شده است.

در حوزه اتوماسیون صنعتی، به جزئیات دو آسیب‌پذیری امنیتی جدید در کنترل‌گر منطقی قابل برنامه‌ریزی (Programmable Logic Controllers به اختصار PLC) متعلق به شرکت راکول آتومیشن، اشاره خواهیم کرد که می‌تواند جهت تزریق کد مخرب به سیستم‌های آسیب‌پذیر و تغییر مخفیانه فرآیندهای خودکارسازی مورد سوءاستفاده قرار گیرد.

طبق معمول هر ماه، شرکت‌های مختلف فناوری اطلاعات اقدام به انتشار اصلاحیه و توصیه‌نامه امنیتی برای برخی از محصولات خود کردند. جزییات اصلاحیه‌های فروردین ماه شرکت‌های مایکروسافت، سیسکو، مک‌آفی‌اینترپرایز، بیت‌دیفندر، کسپرسکی، ای‌سِت، اف-سکیور، ترند میکرو، وی‌ام‌ور، ادوبی، گوگل، اپل، موزیلا، سوفوس، اوراکل، دروپال، آپاچی، سیتریکس و جونیپر نت‌ورکز را می‌توانید در این ماهنامه بخوانید.

شرکت مهندسی شبکه گستر، ارائه‌دهنده محصولات و خدمات در زمینه امنیت شبکه از زمان تأسیس در سال ۱۳۷۰، همواره به امر آگاه‌سازی در زمینه امنیت فناوری اطلاعات به عنوان یکی از اصلی‌ترین راهکارهای مقابله با تهدیدات سایبری توجه خاص داشته است. امید است مطالب ماهنامه امنیت فناوری اطلاعات شرکت مهندسی شبکه گستر که حاصل تلاش کارشناسان این شرکت است قدمی در جهت ارتقای دانش کاربران این حوزه باشد.

هشدارهای امنیتی



کشف یک جاسوس‌افزار
جدید اندرویدی

یک برنامه جاسوس‌افزار اندرویدی جدیدی شناسایی شده که به‌عنوان یک سرویس «Process Manager» ظاهر می‌شود و به‌طور مخفیانه اطلاعات حساس ذخیره‌شده در دستگاه‌های آلوده را سرقت می‌کند.

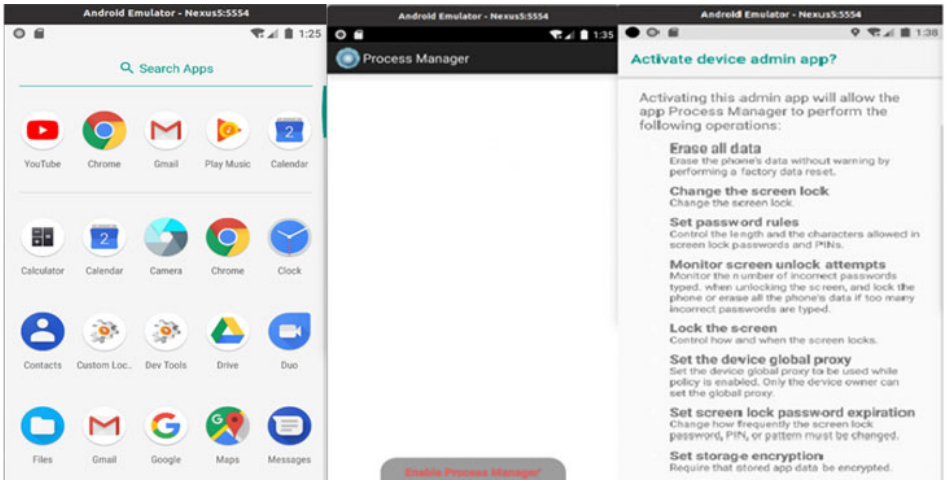
نام فایل نصب این برنامه "com.remote.app" است و در زمان اجرا با سرور کنترل و فرمان‌دهی ۸۲.۱۴۶.۳۵[.]۲۴۰ (Command-and-Control - به اختصار C2) که قبلاً توسط گروه نفوذگران روسی Turla بکار گرفته می‌شد، ارتباط برقرار می‌کند.

پویش این برنامه مخرب در سایت Virus Total در نشانی زیر قابل مشاهده می‌باشد.

https://www.virustotal.com/gui/file/e0eacd72afe39de3b327a164f9c69a78c9c0f672d3ad-202271772d816db4fad8

هنگام اجرای برنامه، هشداری در خصوص مجوزهای اعطاء شده به برنامه ظاهر می‌شود. این مجوزها عبارتند از باز کردن قفل صفحه نمایش، قفل کردن صفحه نمایش، تنظیم پروکسی دستگاه، تنظیم تاریخ انقضای رمز قفل صفحه، رمزگذاری منابع ذخیره‌سازی دستگاه و غیرفعال کردن دوربین‌ها.

پس از فعالسازی برنامه، بدافزار نماد چرخ دنده شکل خود را از صفحه اصلی حذف نموده و در پس‌زمینه اجرا می‌شود و از مجوزهای گسترده خود جهت دسترسی به اطلاعات مخاطبین دستگاه و گزارش‌های تماس، ردیابی موقعیت مکانی آنها، ارسال و خواندن پیام‌ها، دسترسی به حافظه خارجی، گرفتن عکس و ضبط صدا سوءاستفاده می‌کند.



اطلاعات جمع‌آوری‌شده در قالب JSON ذخیره شده و متعاقباً به سرور کنترل و فرمان‌دهی منتقل می‌شود. با وجود استفاده همزمان از سرور C2، شواهد کافی برای نسبت دادن قطعی این جاسوس‌افزار به گروه Turla وجود ندارد.

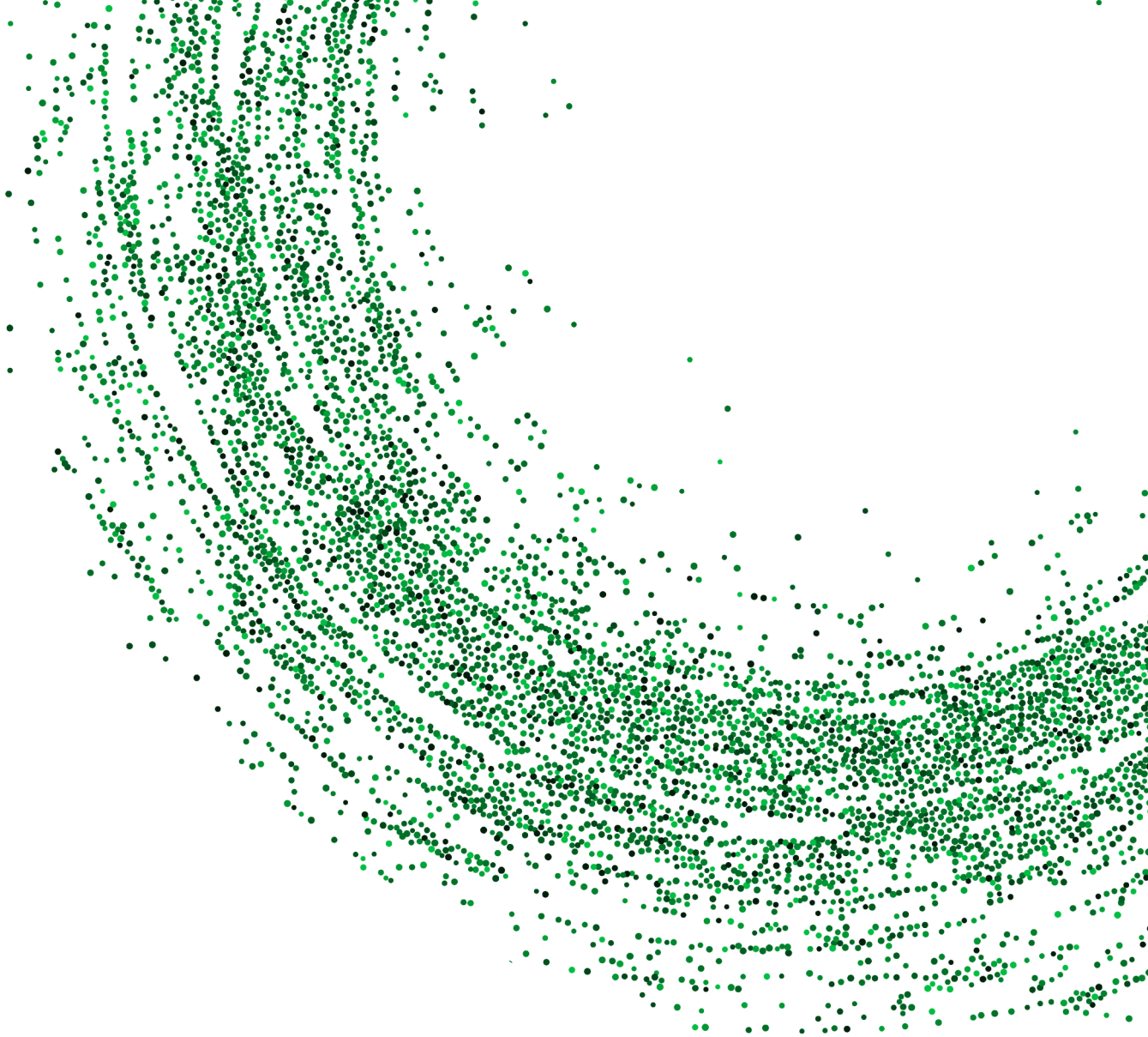
همچنین در این مرحله، روش توزیع اولیه جاسوس‌افزار و اهداف مورد نظر کارزار، شناسایی نشده است. ولی با این حال، جاسوس‌افزار مذکور سعی می‌کند یک برنامه واقعی و قانونی به نام Roz Dhan (به معنی ثروت روزانه) را که در Google Play موجود است، دریافت و نصب کند. برنامه Roz Dhan که بیش از ۱۰ میلیون بار نصب شده، به کاربران امکان می‌دهد بابت شرکت در نظرسنجی‌ها و تکمیل پرسشنامه‌ها جوایز نقدی دریافت کنند. این برنامه دارای یک گزینه پاداش بابت "معرفی کاربر جدید" (Referral) است که توسط جاسوس‌افزار مورد سوءاستفاده قرار می‌گیرد و مهاجم با نصب آن بر روی دستگاه‌های قربانی، درآمد کسب می‌کند.

مشروح گزارش در خصوص این جاسوس‌افزار در نشانی زیر قابل دریافت و مطالعه است:

https://lab52.io/blog/complete-dissection-of-an-apk-with-a-suspicious-c2-server/

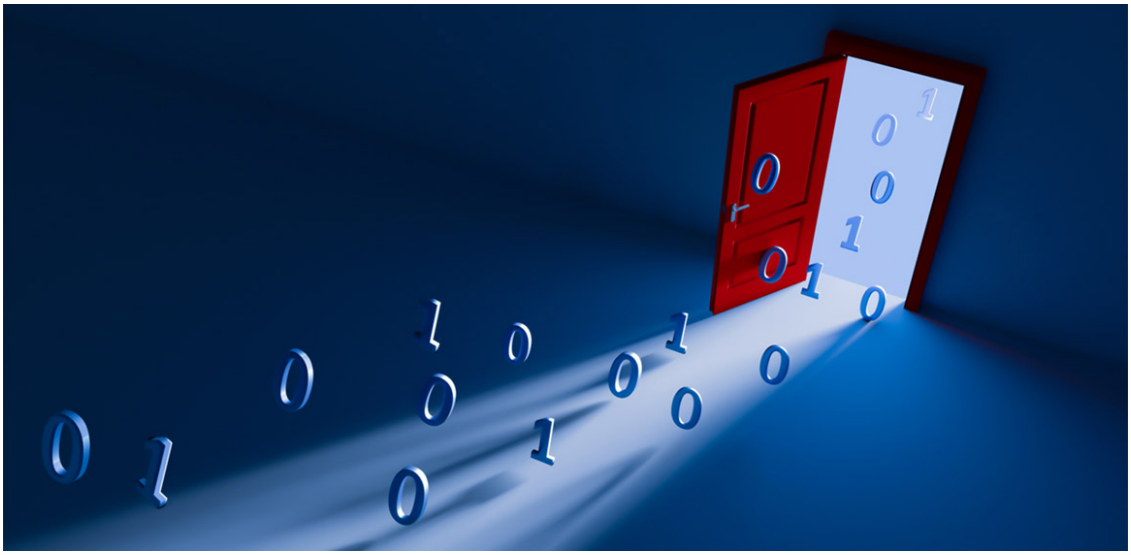
منبع:

https://thehackernews.com/2022/04/researchers-uncover-new-android-spyware.html



رویدادها و وقایع امنیتی

فرم تماس در سایت‌ها،
وسیله انتشار BazarBackdoor



بدافزار BazarBackdoor بجای استفاده از پیام‌های ایمیل فریب‌دهنده (Phishing) همیشگی، اکنون از فرم‌های تماس در سایت‌های سازمانی به‌عنوان ابزاری برای انتشار استفاده می‌کند تا از شناسایی شدن توسط محصولات امنیتی نیز در امان بماند.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده بدافزار مذکور مورد بررسی قرار گرفته است.

BazarBackdoor از نوع بدافزارهای "مخفی‌شونده" (stealth) است که دسترسی غیرمجاز (backdoor) به سیستم قربانی را فراهم می‌کند. این بدافزار در گذشته توسط گروه TrickBot ایجاد شده و در کارزارهای موسوم به "فریب سایبری" یا "فیشینگ" (Phishing) مورد استفاده قرار می‌گرفت. اکنون بدافزار BazarBackdoor توسط گردانندگان باج‌افزار Conti در حال توسعه است.

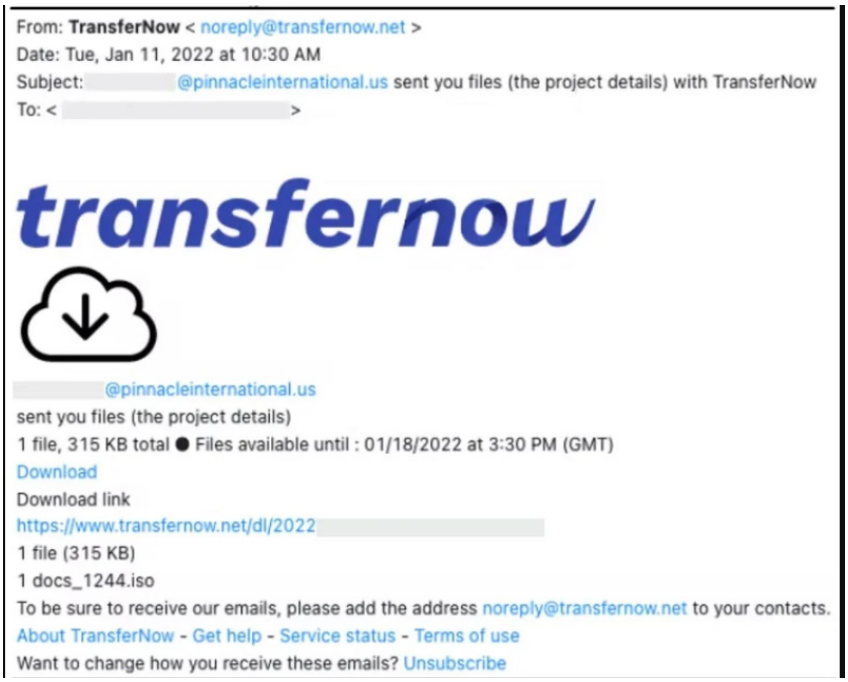
این بدافزار امکان دسترسی راه دور به یک دستگاه در شبکه قربانی را برای گردانندگان بدافزار فراهم می‌کند تا به عنوان یک سکوی پرتاب، آلودگی را به دستگاه‌های مجاور (Lateral Movement) در شبکه گسترش دهند.

بدافزار BazarBackdoor معمولاً از طریق پیام‌های ایمیل فیشینگ که حاوی پیوست مخرب هستند، انتشار می‌یابد. کاربر فریب خورده با اجرای فایل مخرب پیوست، باعث دریافت و اجرای بدافزار می‌شود. اما از آنجایی که امروزه محصولات امنیتی بهبود چشمگیری یافته‌اند و ایمیل‌ها را جهت شناسایی این بدافزارها بررسی می‌نمایند، منتشرکنندگان بدافزار به سراغ روش‌های جدیدی رفته‌اند.

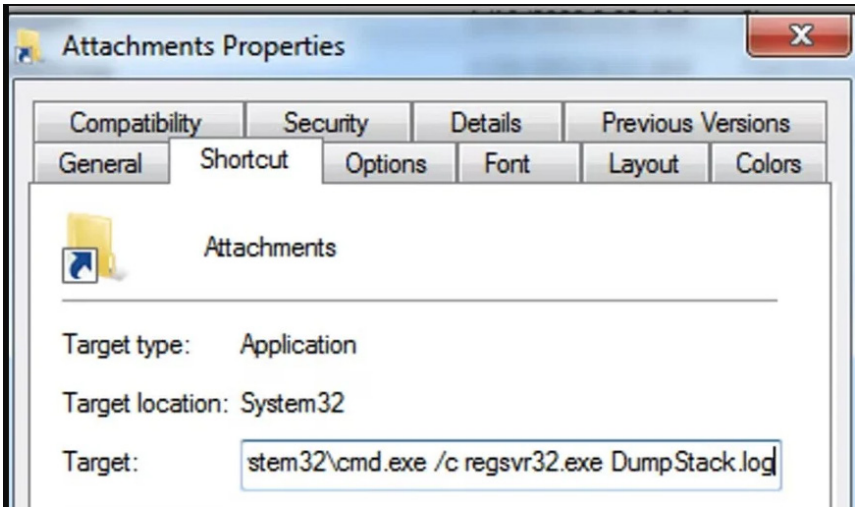
در کارزار جدیدی که از آذر ماه امسال شروع شده، کاربران سازمانی مورد هدف بدافزار BazarBackdoor قرار گرفته‌اند و بدافزار سعی در اجرای ابزار Cobalt Strike و یا فایل‌های مخرب خود دارد. Cobalt Strike یک ابزار تست نفوذ است که مورد سوءاستفاده مهاجمان و نفوذگران سایبری جهت توزیع کدهای بدافزاری خود در سطح شبکه نیز قرار می‌گیرد.

در این کارزار، به جای ارسال مستقیم ایمیل‌های فیشینگ به اهداف مورد نظر، BazarBackdoor از فرم‌های تماس سایت‌های سازمانی برای ایجاد ارتباط اولیه با کاربران سازمانی استفاده می‌کند.

به عنوان نمونه در یک مورد مشاهده گردید که مهاجمان در قالب کارمندان یک شرکت ساختمانی کانادایی ظاهر شدند و درخواستی را برای استعلام قیمت محصول ارسال کردند. پس از اینکه کارمند مربوطه به ایمیل فیشینگ مهاجمان پاسخ داد، مهاجمان در پاسخ یک فایل ISO مخرب را که ظاهراً مربوط به مذاکرات خرید بود، ارسال نمودند. از آنجایی که ارسال مستقیم این فایل‌ها غیرممکن است و منجر به هشدار محصولات امنیتی می‌شود، همانطور که در تصویر زیر نشان داده شده مهاجمان از خدمات اشتراک‌گذاری فایل نظیر TransferNow و WeTransfer استفاده کرده بودند.



فایل پیوست و فشرده شده ISO حاوی یک فایل lnk. و یک فایل log. است. هدف از بسته‌بندی کدهای مخرب در فایل فشرده، ترغیب کاربر به استخراج دستی آنها پس از دانلود، دور زدن محصولات ضدویروس و شناسایی نشدن فایل‌های مخرب است. فایل lnk. حاوی فرمانی است که یک پنجره Terminal باز می‌کند و فایل log. را که در واقع فایل DLL بدافزار BazarBackdoor است را بارگذاری می‌کند.



هنگامی که بخش Backdoor بدافزار بارگیری می‌شود، به فرآیند svchost.exe تزریق شده و با سرور کنترل و فرمان‌دهی (Command and Control - به اختصار C2) ارتباط برقرار می‌کند تا فرامین را برای اجرا دریافت کند.

به دلیل آفلاین بودن بسیاری از نشانی‌های IP مربوط به سرورهای کنترل و فرمان‌دهی در زمان تحلیل حمله توسط محققان، آنها نتوانستند کد بدافزاری و مخرب مرحله دوم را بازیابی کنند، بنابراین هدف نهایی این کارزار همچنان ناشناخته باقی مانده است.

منبع:

https://www.bleepingcomputer.com/news/security/corporate-website-contact-forms-used-to-spread-bazarbackdoor-malware/

ممنوعیت استفاده از
محصولات کسپرسکی

بر اساس گزارش بلومبرگ، کمیسیون ارتباطات فدرال ایالات متحده (Federal Communications Commission - به اختصار FCC)، شرکت امنیت سایبری روسی کسپرسکی (Kaspersky Lab) را به فهرست نهادهایی که "خطر غیرقابل قبولی برای امنیت ملی ایالات متحده" دارند، اضافه کرده است.

این اولین بار است که یک شرکت روسی به این لیست اضافه می‌شود و به نظر می‌رسد این اتفاق از عواقب جنگ روسیه و اوکراین است.

کسب و کارها در ایالات متحده از استفاده از یارانه‌های دولتی ارائه شده از طریق FCC برای خرید محصولات یا بکارگیری خدمات از شرکت‌های موجود در فهرست فوق منع شده‌اند.

رئیس FCC در یک بیانیه مطبوعاتی اعلام نموده که افزودن کسپرسکی و همچنین آزمایشگاه‌های آن به فهرست نهادهای ممنوعه، به محافظت از شبکه‌های ایالات متحده در برابر تهدیدات ناشی از نهادهای تحت حمایت دولت روسیه که به دنبال جاسوسی و آسیب رساندن به منافع آمریکا هستند، کمک خواهد کرد.

شرکت کسپرسکی نیز در یک بیانیه مطبوعاتی دیگر در سایت خود به اقدام FCC پاسخ داده و گفته که این تصمیم "بر اساس دلایل سیاسی" با توجه به جنگ روسیه و اوکراین گرفته شده است و این شرکت "آماده همکاری با نهادهای دولتی ایالات متحده برای رسیدگی به مشکلات FCC و هر گونه نهاد نظارتی دیگر است".

در سال ۲۰۱۷ نیز ایالات متحده ادعا کرده بود که وزارت اطلاعات روسیه از نرم‌افزار ضدویروس کسپرسکی برای سرقت اسناد طبقه‌بندی شده سازمان امنیت ملی این کشور استفاده کرده است، ادعایی که توسط این شرکت روسی رد شد. در اواخر همان سال نیز دونالد ترامپ، رئیس جمهور سابق آمریکا، پس از متهم کردن این شرکت به داشتن ارتباط با دولت روسیه، فرمانی را امضا نمود که استفاده از محصولات کسپرسکی توسط سازمان‌ها و نهادهای فدرال را ممنوع کرده است.

منبع:

https://www.theverge.com/2022/3/26/22997532/fcc-kaspersky-list-national-security-threats-huawei-zte

رد پای نفوذگران Cicada
در عملیات گسترده جاسوسی

رد پای یک گروه نفوذگر چینی که تاکنون تنها بر روی افراد و سازمانهای ژاپنی تمرکز داشته در یک کارزار قدیمی جاسوسی که اکنون قربانیان جدیدی را هدف قرار داده است، شناسایی شده که نشان دهنده گسترش دامنه فعالیت این گروه است.

این حملات گسترده که گمان می‌رود در تابستان سال گذشته آغاز شده و تا اواخر سال نیز ادامه داشته، به گروهی به نام Cicada مرتبط است که در زمینه "تهدیدات مستمر و پیشرفته" (Advanced Persistent Threat - به اختصار APT) فعالیت می‌کند و با نام‌های Bronze Riverside، Potassium، Stone Panda، APT10 یا MenuPass Team نیز شناخته می‌شود.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده کارزار مذکور مورد بررسی قرار گرفته است.

گروه امنیتی سیمانتک، بخشی از شرکت برودکام (Broadcom Corporation) در گزارشی اعلام نمود که قربانیان کارزار Cicada، سازمان‌های دولتی، حقوقی، مذهبی و مردم‌نهاد در کشورهای مختلفی از سراسر جهان از جمله در اروپا، آسیا و آمریکای شمالی می‌باشند.

تمرکز عمده مهاجمان بر بخش‌های دولتی، سازمان‌های غیردولتی مردم‌نهاد و به خصوص آنهایی که در زمینه‌های مذهبی و آموزشی فعالیت می‌کنند، بوده است. اکثر سازمان‌های مورد هدف در ایالات متحده، کانادا، هنگ‌کنگ، ترکیه، سرزمین اشغالی فلسطین، هند، مونته‌نگرو، ایتالیا و یک مورد نیز در ژاپن مستقر بودند و مهاجم در برخی موارد به مدت ۹ ماه در شبکه‌های سازمانی برخی از این قربانیان فعال بوده است.

در بخش‌های مخابراتی، حقوقی و دارویی نیز قربانیانی وجود داشته اما به نظر می‌رسد سازمان‌های دولتی و غیرانتفاعی محور اصلی کارزار مذکور بوده‌اند.

یکسال قبل، در فروردین ۱۴۰۰، محققان شرکت کسپرسکی (Kaspersky, Lab.) یک عملیات جاسوسی اطلاعات را که نصب ابزارهای جمع‌آوری اطلاعات از تعدادی از بخش‌های صنعتی در ژاپن توسط این گروه در حال انجام بود، شناسایی کردند.

در اوایل بهمن ۱۴۰۰ نیز مهاجمان Cicada در یک حمله زنجیره تامین (Supply Chain) سازمان‌یافته با هدف سرقت اطلاعات حساس از سیستم‌های آسیب‌پذیر در بخش مالی تایوان دست داشتند.

محققان سیمانتک با مشاهده و بررسی مجموعه حملات جدید، پی بردند که دسترسی اولیه مهاجمان از طریق یک آسیب‌پذیری شناخته شده ولی ترمیم نشده در سرورهای Microsoft Exchange شروع می‌شود و با سوءاستفاده از این ضعف امنیتی، دسترسی غیرمجاز (Backdoor) انتخابی خود، از نوع SodaMaster را ایجاد می‌کنند.

محققان در ادامه عنوان نمودند که موفق نشدند در این حملات یک آسیب‌پذیری خاص را که مهاجمان از آن بهره‌جویی کرده‌اند، شناسایی کنند، به عنوان مثال نمی‌توان به طور قطعی گفت که آنها از ProxyShell یا ProxyLogon استفاده کرده‌اند.

SodaMaster یک تروجان (Trojan) دسترسی از راه دور و مبتنی بر Windows است که دارای قابلیت‌هایی جهت تسهیل فراخوانی کدهای مخرب و استخراج و تبادل اطلاعات با سرور کنترل و فرمان‌دهی (Command and Control - به اختصار C2) خود می‌باشد.

سایر ابزارهایی که در عملیات نفوذ از آنها استفاده می‌شود عبارتند از ابزار استخراج رمزهای عبور و اطلاعات اصالت‌سنجی به نام Mimikatz، یک پویشگر خط فرمان برای شناسایی سیستم‌های آسیب‌پذیر به نام NBTScan، ابزار WMIExec برای اجرای فرامین از راه دور و VLC Media Player برای اجرای یک بارگذاری کننده (Loader) سفارشی بر روی دستگاه آلوده.

با بررسی قربانیان حملات اخیر در بخش‌های مختلف، به نظر می‌رسد که مهاجمان این کارزار اکنون به اهداف متنوع‌تری علاقه‌مند شده‌اند. نوع سازمان‌هایی که مورد هدف قرار گرفته شده‌اند - سازمان‌های غیرانتفاعی و دولتی، از جمله سازمان‌هایی که در فعالیت‌های مذهبی و آموزشی مشارکت دارند - به احتمال زیاد به منظور جاسوسی مهاجمان Cicada مورد نظر قرار گرفته‌اند. همچنین فعالیت‌های مخربی که بر روی دستگاههای این قربانیان مشاهده شده و با در نظر گرفتن فعالیت‌های این گروه در گذشته، همه نشان می‌دهند که جاسوسی، انگیزه و هدف اصلی است.

منبع:

https://thehackernews.com/2022/04/researchers-trace-widespread-espionage.html

بهره‌جویی از آسیب‌پذیری Spring4Shell
برای توزیع بدافزار Mirai

در فروردین ۱۴۰۰، سه آسیب‌پذیری مهم در Java Spring Framework منتشر شد که یکی از آنها از نوع "اجرای کد از راه دور" (Remote Code Execution - به اختصار RCE) است و Spring4Shell یا SpringShell نامیده می‌شود.

Spring Framework یک بستر منبع باز جهت تولید برنامه‌های کاربردی مبتنی بر Java است و به دلیل اینکه برنامه‌نویسان را قادر به نوشتن و آزمایش سریع و آسان برنامه‌های تکه‌تکه (Modular Applications) می‌کند، پرطرفدار است. از آنجایی که ۶۰ درصد برنامه‌نویسان از Spring برای نوشتن برنامه‌های اصلی مبتنی بر Java استفاده می‌کنند، بسیاری از نرم‌افزارها به طور بالقوه تحت تأثیر این ضعف امنیتی قرار دارند.

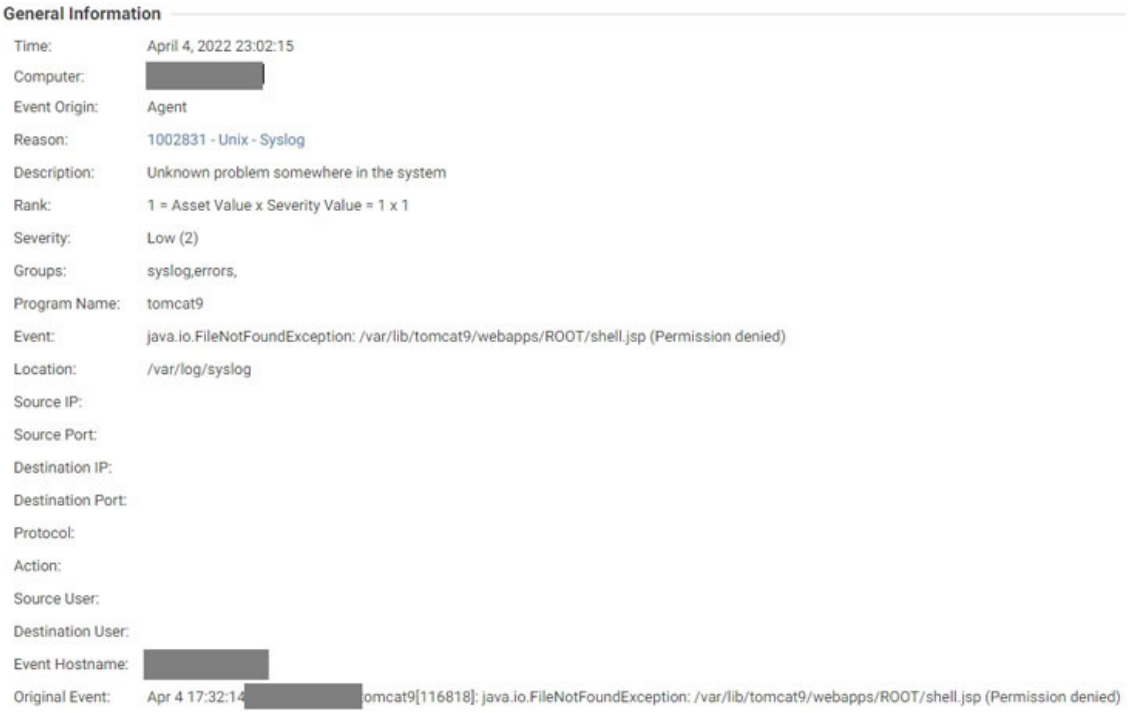
در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده آسیب‌پذیری مذکور مورد بررسی قرار گرفته است.

آسیب‌پذیری Spring4Shell دارای درجه اهمیت حیاتی (Critical) بوده و کتابخانه (Library) org.springframework:spring-bean از آن تاثیر می‌پذیرد. این ضعف امنیتی از تاریخ ۱۲ فروردین ۱۴۰۱ به طور فعال توسط مهاجمان جهت توزیع بدافزار Mirai، به ویژه در محدوده سنگاپور مورد سوءاستفاده قرار گرفته است.

این آسیب‌پذیری دارای شناسه CVE-2022-22965 بوده و درجه شدت آن ۹.۸ (بر طبق استاندارد CVSS) می‌باشد. مهاجم با سوءاستفاده از این ضعف امنیتی قادر به اجرای کد از راه دور بوده و می‌تواند کنترل کامل دستگاه آسیب‌پذیر را در دست بگیرد.

آژانس دولتی "امنیت سایبری و امنیت زیرساخت آمریکا" (Cybersecurity & Infrastructure Security Agency به اختصار CISA) نیز نسبت به Spring4Shell هشدار داده و اعلام نموده که این آسیب‌پذیری به طور فعال مورد سوءاستفاده قرار گرفته به صورتی که تنها در چند روز اول بیش از ۳۷ هزار مورد بهره‌جویی از آن ثبت شده است.

محققان شرکت ترند میکرو (Trend Micro, Inc.)، در گزارشی اعلام نمودند که مهاجمان با بهره‌جویی از این ضعف امنیتی، بدافزار Mirai را در پوشه "tmp/" قرار داده و پس از بکارگیری فرمان "chmod" جهت تغییر مجوز، آن را اجرا می‌کنند.



General Information

Time:	April 4, 2022 23:02:15
Computer:	[redacted]
Event Origin:	Agent
Reason:	1002831 - Unix - Syslog
Description:	Unknown problem somewhere in the system
Rank:	1 = Asset Value x Severity Value = 1 x 1
Severity:	Low (2)
Groups:	syslog,errors,
Program Name:	tomcat9
Event:	java.io.FileNotFoundException: /var/lib/tomcat9/webapps/ROOT/shell.jsp (Permission denied)
Location:	/var/log/syslog
Source IP:	
Source Port:	
Destination IP:	
Destination Port:	
Protocol:	
Action:	
Source User:	
Destination User:	
Event Hostname:	[redacted]
Original Event:	Apr 4 17:32:14 [redacted] tomcat9[116818]: java.io.FileNotFoundException: /var/lib/tomcat9/webapps/ROOT/shell.jsp (Permission denied)

این اولین باری نیست که گردانندگان شبکه‌های مخرب Botnet به سرعت اقدام به اضافه کردن یک ضعف امنیتی جدید افشاء شده به مجموعه ابزارهای بهره‌جویی خود کرده‌اند. در آذر ۱۴۰۰ نیز موارد متعددی از سوءاستفاده شبکه‌های مخربی همچون Mirai و Kinsing از آسیب‌پذیری Log۴Shell جهت نفوذ به سرورهای حساس در اینترنت شناسایی شدند.

Mirai، در زبان ژاپنی به معنای "آینده" می‌باشد و نامی است که به یک بدافزار Linux داده شده است. این بدافزار دائماً دستگاه‌های موجود در شبکه خانه‌های هوشمند نظیر دوربین‌های IP و روترها (Routers) را که دارای پردازنده از نوع ARC هستند و نسخه ساده شده‌ای از سیستم عامل Linux را اجرا می‌کنند، هدف قرار داده و آنها را به شبکه‌ای از دستگاه‌های آلوده و تسخیر شده (Botnet) متصل می‌کند.

شبکه‌های Botnet متشکل از اینترنت اشیا، با بکارگیری مجموعه‌ای از سخت افزارهای به گروگان گرفته شده، می توانند حملات وسیع‌تری را نظیر حملات "فریب سایبری" (Phishing) در مقیاس بزرگ، استخراج دزدانه ارز دیجیتال، حملات توزیع‌شده از کاراندازی سرویس (Distributed Denial-of-Service - به اختصار DDos) انجام دهند.

به دنبال فاش شدن کد منبع (Source code) بدافزار Mirai در مهر سال ۱۳۹۵، انواع مختلفی از شبکه‌های مخرب نظیر Okiru، Masuta، Satori، و Reaper به وجود آمدند و آن را به تهدیدی دائمی و در حال جهش تبدیل کردند.

محققان شرکت اینتل ۴۷۱ (Intel۴۷۱, Inc.) نیز به تازگی با اشاره به انتشار کدهای منبع BotenaGo Botnet بر روی بستر برنامه‌نویسی GitHub در دی ماه ۱۴۰۰، عنوان نمودند کد منبع Mirai آنقدر تأثیرگذار بوده است که حتی برخی از بدافزارهای منشاء گرفته از آن، اکنون برای خود بطور مستقل نسخ جدید منتشر می‌کنند و با گروه‌های سایبری دیگری همکاری و مشارکت دارند.

در اوایل دی ۱۴۰۰ نیز شرکت امنیت سایبری کراودسترایک (CrowdStrike Holdings, Inc.) گزارش داد که بدافزارهایی که سیستم‌های Linux را مورد حمله قرار می‌دهند در سال ۲۰۲۱ نسبت به سال قبل از آن، ۳۵ درصد افزایش داشته است، به طوری که در سال ۲۰۲۱ مجموعه بدافزارهای Mirai، XOR DDoS و Mozi بیش از ۲۲ درصد از حملات هدفمند را علیه سیستم‌های Linux انجام داده‌اند.

این محققان بر این باورند که هدف اصلی این مجموعه از بدافزارها، آلوده‌سازی دستگاه‌های آسیب‌پذیر متصل به اینترنت، تحت کنترل در آوردن آنها در شبکه‌های مخرب و استفاده از آنها برای انجام حملات "توزیع شده از کاراندازی سرویس" (DDOS) می‌باشد.

در این راستا، توضیحات کامل در مورد آسیب‌پذیری Spring4Shell و بروزرسانی‌های عرضه شده در نشانی زیر قابل دسترس می‌باشد:

https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement

منابع:

https://thehackernews.com/2022/04/hackers-exploiting-spring4shell.html

https://www.dynatrace.com/news/blog/what-is-spring4shell-vulnerabilities-in-the-java-spring-framework/

بدافزارهای FFDroider و Lightning Stealer؛
سارقین جدید اطلاعات

محققان امنیت سایبری در مورد دو بدافزار سرقت‌کننده اطلاعات به نام‌های FFDroider و Lightning Stealer که قادر به استخراج و سرقت اطلاعات حساس و اجرای حملات بر روی دستگاه قربانیان می‌باشند، هشدار می‌دهند.

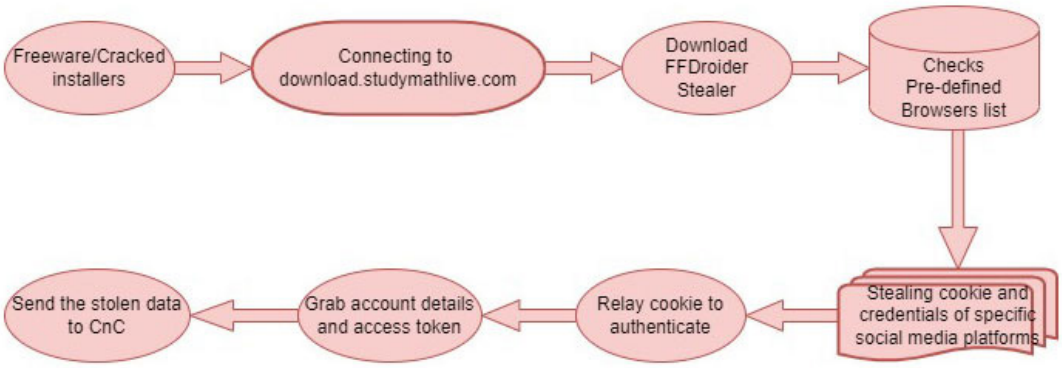
در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده بدافزارهای مذکور مورد بررسی قرار گرفته است.

محققان شرکت Zscaler ThreatLabz در گزارشی اعلام نمودند که بدافزار FFDroider که برای استخراج و ارسال اطلاعات کاربری و کوکی‌ها (cookies) به یک سرور کنترل و فرماندهی (Command & Control - به اختصار C2) طراحی شده، خود را بر روی دستگاه قربانی شبیه برنامه پیام‌رسان "Telegram" نشان می‌دهد.

سارقین اطلاعات، همانطور که از نام آنها پیداست، مجهز به ابزارهایی جهت جمع‌آوری اطلاعات حساس نظیر کلیدهای فشرده شده روی صفحه کلید (Keystroke)، تصاویر گرفته شده از صفحه نمایش (Screenshot)، فایل‌ها، رمزهای عبور ذخیره شده و کوکی‌های مرورگرهای وب، از سیستم‌های آسیب‌پذیر بوده و سپس اطلاعات سرقت شده را به یک دامنه تحت اختیار مهاجمان منتقل می‌کنند.

بدافزار FFDroider از طریق نسخه‌های کرک شده و نرم‌افزارهای رایگان با هدف اصلی سرقت کوکی‌ها و اطلاعات کاربری مرتبط با رسانه‌های اجتماعی محبوب و بسترهای تجارت الکترونیک منتشر می‌شود. این بدافزار با بکارگیری داده‌های سرقت شده و ورود به حساب‌های کاربری قربانیان، به سایر اطلاعات مربوط به حساب شخصی آنها دسترسی پیدا می‌کند.

این بدافزار عموماً مرورگرهایی نظیر Internet Explorer، Mozilla Firefox، Google Chrome و Microsoft Edge و سایت‌های eBay، Twitter Amazon، Instagram، Facebook و Etsy را مورد هدف قرار می‌دهد.



FFDroider Attack Cycle

به نقل از محققان، مهاجمان با استفاده از کوکی‌های سرقت شده، به حساب‌های کاربری شبکه‌های اجتماعی قربانیان وارد شده و از طریق روش‌های پرداخت ذخیره‌شده، به اطلاعات حساب آنها نظیر Facebook Ads-manager دست می‌یابند تا تبلیغات جعلی و مخرب ایجاد و اجرا نمایند. آنها در Instagram نیز، اطلاعات شخصی را با بکارگیری API استخراج می‌کنند.

همچنین بدافزار FFDroider دارای قابلیت ارتقاء خودکار خود به ماژول‌های جدید از طریق یک سرور بروزرسانی می‌باشد که به آن امکان می‌دهد مجموعه امکانات خود را در طول زمان و به مرور گسترش دهد و مهاجم را قادر می‌سازد از داده‌های سرقت شده برای دسترسی اولیه به اهداف موردنظر بهره‌برداری کند.

```
internal class MainEntrance
{
    // Token: 0x0600000F RID: 15 RVA: 0x000032AC File Offset: 0x000014AC
    private static void Main(string[] args)
    {
        List<ILogGecko> getLogGecko = Input.GetLogGecko;
        List<ILogChrome> getLogChrome = Input.GetLogChrome;
        List<List<IWallet>> getLogWallet = Input.GetLogWallet;
        IPcInfo getPcInfo = Input.GetPcInfo;
        List<IFile> getFiles = Files.GetFiles;
        List<ITelegram> getTelegram = Telegram.GetTelegram;
        List<IDiscord> getDiscord = Discord.GetDiscord;
        List<ISteam> getSteam = Steam.GetSteam;
        IScreen getScreenShot = PcInfo.GetScreenShot;
        Runner.Run(new ILog
        {
```

مشروح گزارش منتشر شده در خصوص بدافزار FFDroider، جزئیات حمله و نشانه‌های آلودگی آن در این نشانی قابل مطالعه است.

بدافزار Lightning Stealer نیز به روشی مشابه عمل می‌کند و می‌تواند داده‌های مربوط به بستر ارتباطی Discord، کیف‌های پول رمزارز، کوکی‌ها، رمزهای عبور، کارت‌های اعتباری و تاریخچه جستجو را از بیش از ۳۰ مرورگر مبتنی بر Firefox و مبتنی بر Chromium استخراج کرده و اطلاعات سرقت شده را با فرمت JSON به یک سرور ارسال کند.

محققان شرکت سی‌بل (Cyble Inc.) بر این باورند که سارقین اطلاعات، شگردهای جدیدی را به منظور شناسایی نشدن به کار می‌گیرند. گروه‌های باج‌افزاری از بدافزارهای سرقت کننده اطلاعات نظیر Lightening Stealer جهت دسترسی اولیه به شبکه و در نهایت استخراج داده‌های حساس استفاده می‌کنند.

به تازگی بدافزارهای سرقت کننده اطلاعات نظیر FFDroider و Lightning Stealer به طور فزاینده‌ای در کارزارهای مختلف به کار گرفته شده‌اند، به خصوص از اوایل فروردین ماه با توقف فعالیت Raccoon Stealer به دلیل جنگ روسیه و اوکراین.

Raccoon Stealer نیز یک بدافزار سرقت‌کننده اطلاعات است. گردانندگان این بدافزار در توییتی در تاریخ ۵ فروردین ۱۴۰۱ پس از ادعای مرگ یکی از مسئولین این بدافزار در حمله به اوکراین، اعلام نمودند که فعالیت خود را به حالت تعلیق درآورده‌اند.

در بهمن ۱۴۰۰ نیز محققان جزئیات بدافزاری جدید به نام Jester Stealer را افشاء نمودند که برای سرقت و انتقال انواع اطلاعات از دستگاه قربانیان طراحی شده است. از آن زمان تاکنون، حداقل سه بدافزار سرقت‌کننده اطلاعات مختلف، از جمله Mars Stealer، BlackGuard و META شناسایی شده‌اند.

منبع:

https://thehackernews.com/2022/04/researchers-warn-of-ffdroider-and.html

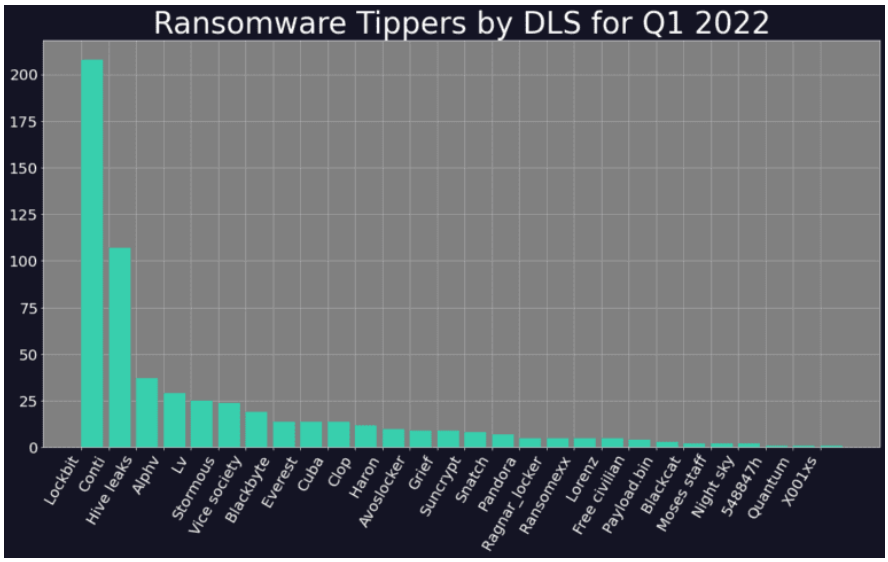
LockBit 2.0 و Conti؛
در صدر فعال‌ترین باج‌افزارها

گزارشات منتشر شده توسط محققان امنیت سایبری شرکت دیجیتال شدوز (Digital Shadows, Ltd.) حاکی از آن است که بیش از نیمی از حملات باج‌افزاری در زمستان سال ۱۴۰۰ تنها توسط دو باج‌افزار LockBit 2.0 و Conti انجام شده است.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده گزارش مذکور مورد بررسی قرار گرفته است.

تحلیل حملات باج‌افزاری ثبت شده بین ۱۱ دی ۱۴۰۰ تا ۱۱ فروردین ۱۴۰۱، نشان می‌دهد که دو گروه باج‌افزاری LockBit 2.0 و Conti در طول این دوره سه ماهه، ۵۸ درصد از کل حملات را به خود اختصاص داده‌اند. از میان این دو، LockBit فعال‌تر بوده و ۳۸ درصد از حملات باج‌افزاری را انجام داده است. این مقدار تقریباً دو برابر تعداد حملات باج‌افزار Conti است، در همان دوره زمانی، ۲۰ درصد از حملات توسط گروه باج‌افزاری Conti صورت گرفته است.

هر دو این باج‌افزارها، اقدام به سرقت داده‌های قربانیان نموده و سپس آنها را تهدید می‌کنند که در صورت عدم پرداخت باج، اطلاعات حساس و حیاتی آنها را در سایت‌های افشاگر منتشر می‌کنند. بر اساس این گزارش، باج‌افزار LockBit بیشترین میزان انتشار داده‌ها را تاکنون داشته و در زمستان ۱۴۰۰، اطلاعات بیش از ۲۰۰ قربانی را منتشر کرده است. پس از این دو باج‌افزار، باج‌افزارهای دیگری نظیر Vice Society، Hive و Blackbyte در صدر حملات قرار داشته‌اند.



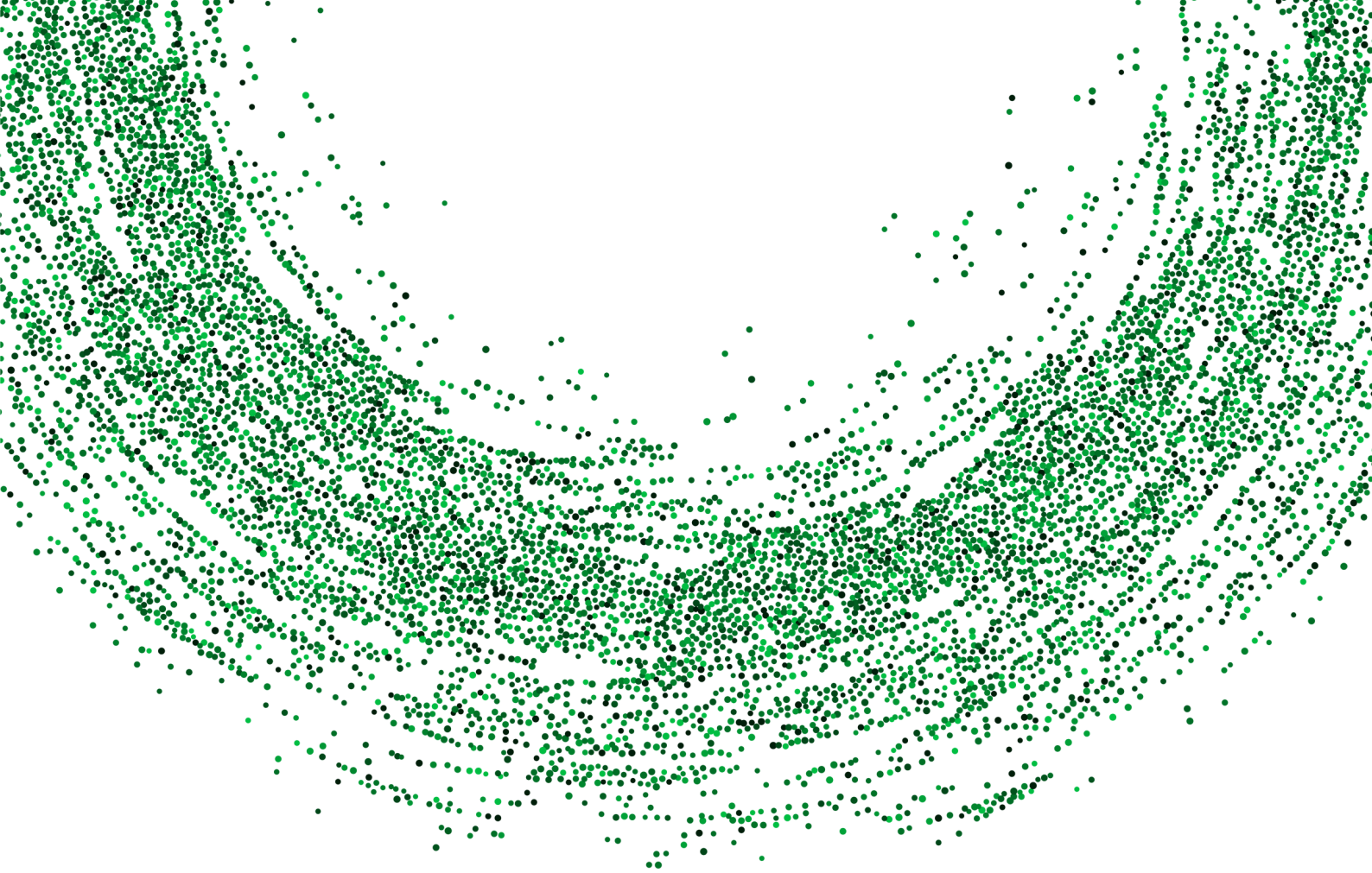
علیرغم افشای اسرار باج‌افزار Conti که اطلاعات زیادی در خصوص شگردها، ابزارها و دستورالعمل‌های دقیق آن ارائه نمود، همچنان این باج‌افزار تهدیدی بزرگ باقی مانده است. با این حال، افشای کدهای باج‌افزار Conti بر شهرت این گروه تاثیر منفی گذاشته و می‌تواند بر توانایی آن در جذب همکاران جدید تأثیر بگذارد و تأثیر بلندمدتی بر توانایی رشد آن داشته باشد.

همچنین به نظر می‌رسد که یکی از باج‌افزارهای بسیار فعال قبلی با نام Revil، فعالیت خود را متوقف کرده است. در حالی که برخی از گروه‌های باج‌افزاری ناپدید می‌شوند، باج‌افزارهای جدید دیگری نظیر Sugar، Pandora، Zeon، Night Sky، Stormous و x001xs از اواخر سال گذشته در حال ظهور می‌باشند. از آنجایی که گروه‌های باج‌افزاری جدید با نسبتی مشابه گروه‌های باج‌افزاری که در حال بسته‌شدن هستند، ایجاد می‌شوند، این احتمال وجود دارد که اعضای گروه‌های باج‌افزاری که تعطیل می‌شوند و دیگر فعال نیستند به سادگی عضو گروه‌های باج‌افزارهای نوظهور می‌شوند. به نقل از محققان، صرف‌نظر از عوامل خارجی و تغییر در هدف‌گیری، باج‌افزارها همچنان یکی از بزرگ‌ترین تهدیدات برای سازمان‌ها در سراسر جهان در سه ماهه آینده باقی خواهد ماند.

توصیه می‌شود که راهبران امنیتی سازمان‌ها به منظور جلوگیری از نفوذ باج‌افزارها و سوءاستفاده مجرمان سایبری از آسیب‌پذیری‌ها، وصله‌های امنیتی نرم‌افزارهای کاربردی و سیستم‌های عامل را در سریع‌ترین زمان ممکن اعمال کنند. سازمان‌ها همچنین باید احراز هویت چندعاملی را برای همه کاربران به کار گیرند و اگر مشکوک به هک شدن رمز عبور هستند، در اسرع وقت آن را تغییر دهند.

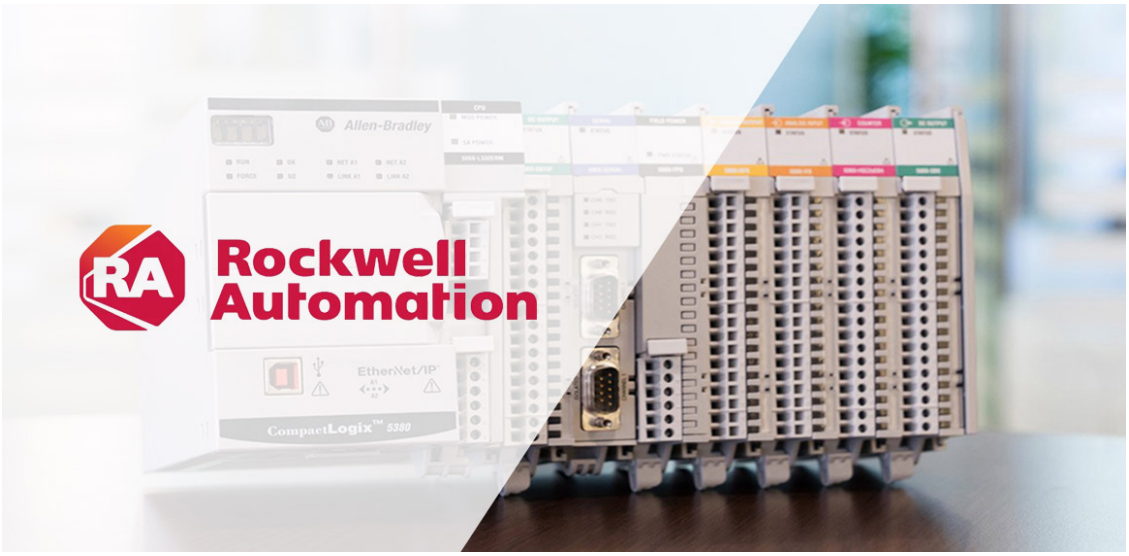
منبع:

https://www.zdnet.com/article/ransomware-these-two-gangs-are-behind-half-of-all-attacks/



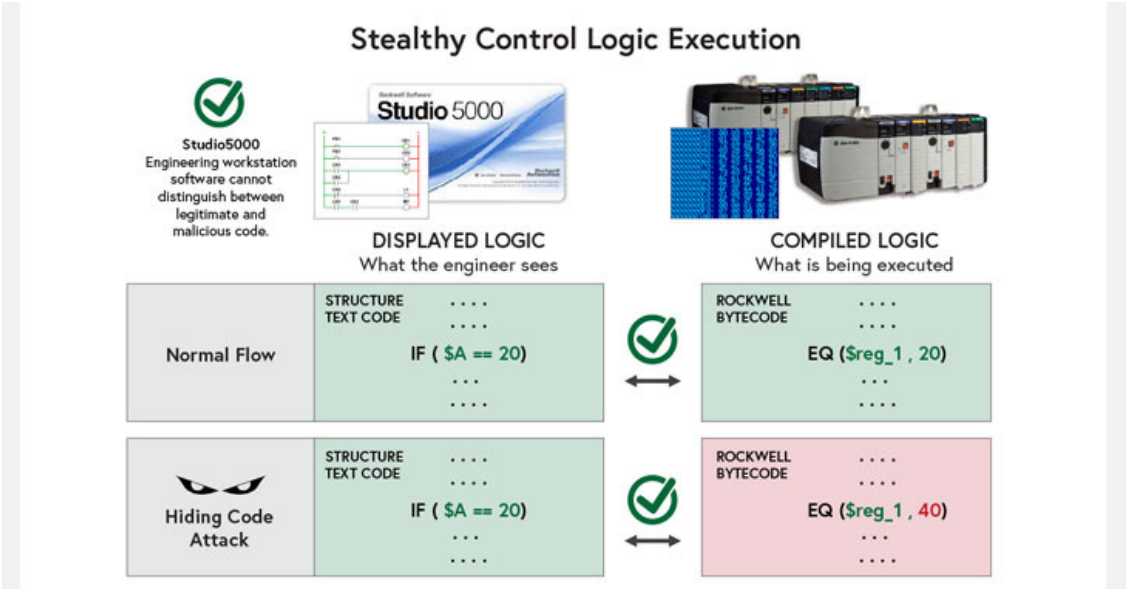
آسیب‌پذیری‌ها و اصلاحیه‌های امنیتی

افشای دو آسیب‌پذیری حیاتی
در محصولات Rockwell PLC



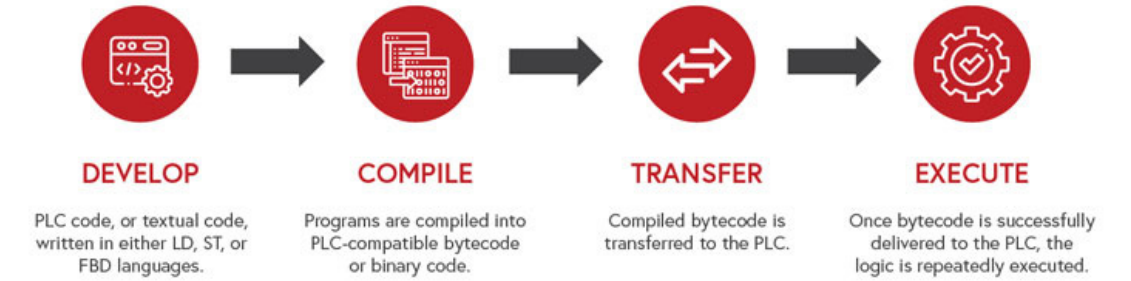
جزئیات دو آسیب‌پذیری امنیتی جدید در کنترل‌گر منطقی برنامه‌پذیر (Programmable Logic Controllers - به اختصار PLC) متعلق به شرکت راکول آتومیشن (Rockwell Automation, Inc.)، منتشر شده است که می‌تواند توسط مهاجم جهت تزریق کد مخرب به سیستم‌های آسیب‌پذیر و تغییر مخفیانه فرآیندهای خودکارسازی (Automation Processes) مورد سوءاستفاده قرار گیرد.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده ضعف‌های امنیتی مذکور مورد بررسی قرار گرفته است.



این ضعف‌های امنیتی، امکان ایجاد اختلال در فعالیت‌های صنعتی و آسیب فیزیکی به کارخانه‌ها را به شیوه‌ای مشابه حملات Stuxnet و Rogue7 دارند.

منطق قابل برنامه‌ریزی و متغیرهای از پیش تعریف‌شده، این فرآیندهای خودکارسازی را هدایت کرده و تغییرات در هر کدام، باعث تغییر در عملکرد عادی تجهیزات PLC و فرآیندهایی که مدیریت می‌کند، می‌شود.



جزئیات دو آسیب‌پذیری به شرح زیر است:

- CVE-2022-1161: مهاجم می‌تواند با سوءاستفاده از این آسیب‌پذیری از راه دور، یک برنامه "textual" و قابل خواندن را در مکانی از حافظه جدا از محل برنامه اجرایی که قبلا به زبان ماشین تبدیل شده (معروف به Bytecode) بنویسد. ضعف امنیتی مذکور در سیستم‌عامل تجهیزات PLC بوده و دارای درجه شدت ۱۰ از ۱۰ بر طبق استاندارد CVSS می‌باشد و بر سیستم‌های کنترلی CompactLogix، ControlLogix و GuardLogix تاثیر می‌گذارد.
- CVE-2022-1159: این آسیب‌پذیری دارای درجه شدت ۷.۷ از ۱۰ است و مهاجم می‌تواند با دارا بودن سطح دسترسی بالا به یک ایستگاه کاری که برنامه Studio 5000 Logix Designer را اجرا می‌کند، فرآیند تبدیل برنامه به زبان ماشین (compilation) را متوقف نموده و بدون اطلاع کاربر فرامین مخرب را به برنامه کاربر اضافه کند.

مهاجم با بهره‌جویی موفقیت‌آمیز از این ضعف‌های امنیتی می‌تواند برنامه‌های کاربر را دستکاری کند و کدهای مخرب را دریافت و در کنترل‌کننده (Controller) قرار دهد و عملاً عملکرد عادی تجهیزات PLC را تغییر داده و فرامین مخرب را به دستگاه‌های فیزیکی که توسط سیستم صنعتی کنترل می‌شوند، ارسال کند.

سوءاستفاده از هر دو این آسیب‌پذیری‌ها نتیجه یکسانی خواهد داشت؛ کارشناس تصور می‌کند که برنامه سالم او بر روی سیستم PLC در حال اجرا است، در حالیکه یک برنامه کاملاً متفاوت و مخرب بر روی PLC اجرا می‌شود.

آژانس دولتی "امنیت سایبری و امنیت زیرساخت آمریکا" (Cybersecurity & infrastructure Security Agency - به اختصار CISA) توصیه می‌کند که به علت درجه شدت این آسیب‌پذیری‌ها، راهبران امنیتی در اسرع وقت با مراجعه به نشانی‌های زیر اقدامات لازم را برای سخت‌افزارها و نرم‌افزارهای آسیب‌پذیر انجام دهند.

https://www.cisa.gov/uscert/ncas/current-activity/2022/03/31/cisa-releases-security-advisories-rockwell-automation-products

https://www.cisa.gov/uscert/ics/advisories/icsa-22-090-05

https://www.cisa.gov/uscert/ics/advisories/icsa-22-090-07

منبع:

https://thehackernews.com/2022/04/critical-bugs-in-rockwell-plc-could.html

بروزرسانی‌ها و اصلاحیه‌های
فروردین ۱۴۰۱

در فروردین ۱۴۰۱ شرکت‌های زیر اقدام به عرضه بروزرسانی و توصیه‌نامه امنیتی برای برخی محصولات خود کردند.

مایکروسافت	ای‌سِت	گوگل	دروپال
سیسکو	اف-سکیور	اپل	آپاچی
مک‌آفی اینترپرایز	ترند میکرو	موزیلا	سیتریکس
بیت‌دیفندر	وی‌ام‌ور	سوفوس	جونیپر نت‌ورکز
کسپرسکی	ادوبی	اوراکل	

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده به برخی از بااهمیت‌ترین اصلاحیه‌های فروردین ماه پرداخته شده است.

مایکروسافت

سه‌شنبه ۲۳ فروردین ۱۴۰۱، شرکت مایکروسافت (Microsoft Corp.)، مجموعه اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی آوریل منتشر کرد. اصلاحیه‌های مذکور بیش از ۱۰۰ آسیب‌پذیری را در Windows و محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت ده مورد از آسیب‌پذیری‌های ترمیم شده این ماه "حیاتی" (Critical) و اکثر موارد دیگر "مهم" (Important) اعلام شده است.

این مجموعه اصلاحیه‌ها، انواع مختلفی از آسیب‌پذیری‌ها را در محصولات مایکروسافت ترمیم می‌کنند:

- "ترفیع اختیارات" (Elevation of Privilege)
- "اجرای کد از راه دور" (Remote Code Execution)
- "افشای اطلاعات" (Information Disclosure)
- "جعل" (Spoofing)
- "از کاراندازی سرویس" (Denial of Service - به اختصار DoS)

دو مورد از آسیب‌پذیری‌های ترمیم شده این ماه، از نوع "روز-صفر" (شناسه‌های CVE-2022-26904 و CVE-2022-24521) می‌باشند، یکی به صورت عمومی افشا شده و دیگری به طور گسترده در حملات مورد سوءاستفاده قرار گرفته است. مایکروسافت آن دسته از آسیب‌پذیری‌هایی را از نوع روز-صفر می‌داند که پیش‌تر اصلاحیه رسمی برای ترمیم آنها ارائه نشده، جزییات آنها به‌طور عمومی منتشر شده یا در مواقعی مورد سوءاستفاده مهاجمان قرار گرفته است.

آسیب‌پذیری‌های "روز-صفر" ترمیم شده در ماه آوریل ۲۰۲۲ عبارتند از:

- CVE-2022-26904: این آسیب‌پذیری دارای درجه شدت ۷ از ۱۰ (بر طبق استاندارد CVSS) بوده و از نوع "ترفیع اختیارات" می‌باشد و Service Windows User Profile از آن متاثر می‌شود.
- CVE-2022-24521: این ضعف امنیتی دارای درجه شدت ۷٫۸ از ۱۰ (بر طبق استاندارد CVSS) بوده و از نوع "ترفیع اختیارات" است و Windows Common Log File System Driver از آن تاثیر می‌پذیرد.

از آنجایی که اکنون مایکروسافت اصلاحیه‌هایی را برای این ضعف‌های امنیتی به صورت عمومی منتشر نموده، انتظار می‌رود که مهاجمان این آسیب‌پذیری‌ها را تحلیل نموده و نحوه بهره‌جویی از آنها را بیاموزند و احتمالاً به زودی به طور گسترده توسط مهاجمان مورد سوءاستفاده قرار خواهند گرفت. بنابراین، اکیداً توصیه می‌شود که راهبران امنیتی نسبت به اعمال بروزرسانی‌های امنیتی آوریل ۲۰۲۲ در اسرع وقت اقدام کنند.

در ادامه به بررسی جزئیات برخی آسیب‌پذیری های اصلاح شده این ماه و به ویژه به مواردی که ممکن است بیشتر مورد توجه مهاجمان قرار گیرند، می‌پردازیم.

شایان ذکر است که بنا بر اظهارات مایکروسافت، تا ۲۳ فروردین، هیچ یک از ضعف‌های امنیتی "حیاتی" ترمیم شده، به طور عمومی افشا یا مـورد سـوءاستفـاده قـرار نگرفتـه‌اند. امـا از میـان ایـن ده آسیب‌پذیری "حیـاتـی"، دو مـورد با شنـاسـه‌هـای CVE-2022-26809 و CVE-2022-24491 که درجه شدت هر دو ۹٫۸ (بر طبق استاندارد CVSS) است، باید مورد توجه قرار گیرند. این آسیب‌پذیری‌ها به ترتیب بر Remote Procedure Call Runtime و Windows Network File System تأثیر می‌گذارند و مهاجم می‌تواند با سوءاستفاده از آنها بصورت "از راه دور" کنترل سیستم آسیب‌پذیر را در دست بگیرد.

نیمی از آسیب‌پذیری‌های حیاتی این ماه یعنی پنج مورد بر پروتکل‌ها و قابلیت‌های شبکه، به‌ویژه RPC، SMB و NFS تأثیر می‌گذارند.

سه آسیب‌پذیری ترمیم شده این ماه بر Windows Remote Procedure Call Runtime - به اختصار RPC - تاثیر می‌گذارند که تنها یک مورد دارای درجه اهمیت "حیاتی" است (ضعف امنیتی با شناسه CVE-2022-26809). دو آسیب‌پذیری باقیمانده RPC دارای درجه اهمیت "مهم" می‌باشند (شناسه‌های CVE-2022-24528 و CVE-2022-24492).

در این ماه، شش آسیب‌پذیری از نوع "اجرای کد از راه دور" بر روی پروتکل Server Message Block - به اختصارSMB - تأثیر می‌گذارند که تنها دو مورد دارای درجه اهمیت "حیاتی" هستند (شناسه‌های CVE-2022-24500 و CVE-2022-24541) و چهار مورد دیگر "مهم" می‌باشند.

دو ضعف امنیتی "حیاتی" دیگر که NFS از آن تاثیر می‌پذیرد، دارای شناسه‌های CVE-2022-24491 و CVE-2022-24497 بوده و احتمال سوءاستفاده از آنها زیاد است. بخش آسیب‌پذیر بطور پیش‌فرض بر روی سیستم عامل Windows نصب و فعال نیست و این آسیب‌پذیری‌های حیاتی تنها می‌توانند سرورهای Windows را که پروتکل NFS بر روی آنها فعال شده‌اند، تحت تأثیر قرار دهند.

از میان ۹ مورد از آسیب‌پذیری‌های ترمیم شده این ماه که Windows Hyper-V را تحت تأثیر قرار می‌دهند (CVE-2022-26785، CVE-2022-26783، CVE-2022-24539، CVE-2022-24537، CVE-2022-24490، CVE-2022-23268، CVE-2022-23257، CVE-2022-22009 و CVE-2022-22008)، ضعف‌های امنیتی (CVE-2022-22008، CVE-2022-23257 و CVE-2022-24537) دارای درجه اهمیت "حیاتی" می‌باشند.

یکی از سه آسیب‌پذیری حیاتی این ماه در محیط Hyper-V، آسیب‌پذیری CVE-2022-23257 است که برای سوءاستفاده از آن مهاجم باید یک برنامه کاربردی دستکاری شده را روی Hype-V Guest راه‌اندازی و اجرا کند.

یکی دیگر از سه آسیب‌پذیری حیاتی این ماه در محیط Hyper-V، آسیب‌پذیری با شناسه CVE-2022-24537 است که جهت بهره‌جویی از این ضعف امنیتی، مهاجم باید کاربر را جهت اجرای اسکریپتی دستکاری شده، فریب دهد. با این که این آسیب‌پذیری از نظر درجه اهمیت "حیاتی" در نظر گرفته شده، ولی به نظر می‌رسد که برای بهره‌جویی از آن به شرایط و اقدامات بسیار خاصی نیاز است.

دیگر آسیب‌پذیری "حیاتی" رفع شده در این ماه، شناسه CVE-2022-23259 بوده و محصول Microsoft Dynamic 365 (on-premises) از آن تاثیر می‌پذیرد. این آسیب‌پذیری از نوع "اجرای کد از راه دور" می‌باشد. برای سوءاستفاده از آن، مهاجم باید یک کاربر احراز هویت شده و با تمهیداتی قادر به اجرای فرامین SQL مورد نظر باشد. بدین ترتیب مهاجم می‌تواند با ترفیع اختیارات، از این پس فرامین را به عنوان db_owner در پایگاه داده Dynamics 356 اجرا کند.

دو مورد از آسیب‌پذیری‌های این ماه بر LDAP تأثیر می‌گذارند (شناسه‌های CVE-2022-26919 و CVE-2022-26831)، که ضعف امنیتی CVE-2022-26919 دارای درجه اهمیت "حیاتی" می‌باشد. این آسیب‌پذیری از راه دور در شبکه، توسط یک کاربر احراز هویت شده، قابل بهره‌جویی است.

از سوی دیگر، مایکروسافت یادآوری می‌کند که بهره‌جویی از این ضعف امنیتی، "پیچیدگی بالایی" دارد و حمله تنها در صورتی امکان‌پذیر است که تنظیمات پیش‌فرض MaxReceiveBuffer تغییر کرده باشد. با این حال، از آنجایی که تعدادی آسیب‌پذیری غیرحیاتی نیز در اصلاحیه‌های این ماه وجود دارد که Active Directory را تحت تاثیر قرار می‌دهند، منطقی است که بروزرسانی این آسیب‌پذیری (CVE-2022-26919) در کنار آنها در اولویت قرار گیرد.

در این ماه دو آسیب‌پذیری از نوع "اجرای کد از راه دور" با درجه اهمیت "مهم" وجود دارد (شناسه‌های CVE-2022-26817 و CVE-2022-26814) که Active Directory را تحت تاثیر قرار می‌دهند. مهاجم در صورت موفقیت در بهره‌جویی از این ضعف‌های امنیتی می‌تواند اجرای کد را در سرویس Active Directory فعال کند. بنابراین، توانایی و موفقیت مهاجم در آلودگی Active Directory در یک سازمان و دسترسی یا ایجاد حساب‌های کاربری با سطح دسترسی ممتاز می‌تواند جهت توسعه و گسترش آلودگی به سیستم‌های مجاور در شبکه توسط مهاجم مورد استفاده قرار گیرد.

۱۸ مورد از آسیب‌پذیری‌های ترمیم شده این ماه بر DNS تأثیر می‌گذارند. همه آنها به جز یک مورد از نوع "اجرای کد از راه دور" می‌باشند؛ ضعف امنیتی با شناسه CVE-2022-26816 از نوع "افشای اطلاعات" و دارای درجه اهمیت "مهم" می‌باشد.

همچنین این ماه، ۱۵ آسیب‌پذیری در Print Spooler برطرف شده‌اند. همه آنها دارای درجه اهمیت "مهم" و از نوع "ترفیع اختیارات" می‌باشند. با این که هیچ‌کدام از آنها به‌طور عمومی افشا نشده و هیچ‌کدام تا تاریخ ۲۳ فروردین ۱۴۰۱، مورد سوءاستفاده قرار نگرفته‌اند و احتمال سوءاستفاده از همگی آنها "کم" می‌باشد، به علت تعداد بالای آنها، منطقی است که در اولویت بروزرسانی‌ها قرار داده شوند.

فهرست کامل آسیب‌پذیری‌های ترمیم شده توسط مجموعه‌اصلاحیه‌های آوریل ۲۰۲۲ مایکروسافت در گزارش زیر که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده قابل مطالعه است:

https://afta.gov.ir/fa-IR/Portal/4927/news/view/14608/2070/

سـیسـکو

شرکت سیسکو (Cisco Systems, Inc.) در فروردین ماه در چندین نوبت اقدام به عرضه بروزرسانی‌های امنیتی برای برخی از محصولات خود کرد. این بروزرسانی‌ها، ٤٦ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت دو مورد از آنها "حیاتی"، ۱۸ مورد از آنها از نوع "بالا" (High) و ۲۶ مورد از نوع "متوسط" (Medium) گزارش شده است. آسیب‌پذیری‌هایی همچون "از کارانداری سرویس"، "افشای اطلاعات"، "ترفیع اختیارات"، "تزریق کد از طریق سایت" (Cross-Site Scripting) و "خواندن و نوشتن فایل دلخواه" (Arbitrary File Read and Write) از جمله مهمترین اشکالات مرتفع شده توسط بروزرسانی‌های جدید هستند. مهاجم می‌تواند از بعضی از این آسیب‌پذیری‌ها برای کنترل سیستم آسیب‌پذیر سوءاستفاده کند. توضیحات کامل در مورد بروزرسانی‌های عرضه شده در لینک زیر قابل دسترس است:

https//:tools.cisco.com/security/center/publicationListing.x

مک‌آفی اینتـرپرایز

در فروردین ۱۴۰۱، شرکت مک‌آفی اینترپرایز (McAfee Enterprise) با انتشار توصیه‌نامه، از ترمیم ۶ آسیب‌پذیری با شناسه‌های CVE-2022-0842، CVE-2022-0857، CVE-2022-0858، CVE-2022-0859، CVE-2022-0861 و CVE-2022-0862 در بروزرسانی نسخه ۱۳ ابزار مدیریتی McAfee ePolicy Orchestrator خبر داد. این شرکت با عرضه نسخه 5.7.6 نرم‌افزار McAfee Agent، ضعف‌هایی با شناسه CVE-2022-1256، CVE-2022-1257 و CVE-2022-1258 را نیز در این محصول برطرف کرد. جزییات بیشتر در توصیه‌نامه‌های زیر قابل دریافت و مطالعه است:

https//:kc.mcafee.com/corporate/index?page=content&id=SB10382

https//:kc.mcafee.com/corporate/index?page=content&id=SB10379

همچنین در فروردین ماه شرکت مک‌آفی اینترپرایز اقدام به انتشار نسخ جدید زیر نمود:

- McAfee Agent 5.7.6
- Policy Auditor 6.5.3
- Drive Encryption 7.3.1
- MVISION Insights April 2022
- SIEM Enterprise Security Manager 11.5.6
- McAfee ePolicy Orchestrator Refresh 6 Update 13
- Data Loss Prevention Endpoint for Windows 11.6.500
- McAfee Application and Change Control for Linux 6.4.20

بیت‌دیفندر

شرکت بیت‌دیفندر (Bitdefender) در فروردین ماه، با انتشار بروزرسانی خودکار 3.4.0.276، آسیب‌پذیری CVE-2022-0677 را در محصول Endpoint Security Tools، ترمیم نمود. همچنین در ماهی که گذشت شرکت بیت‌دیفندر اقدام به انتشار نسخ جدید زیر کرد:

- GravityZone Control Center 6.28.1-1
- Security Server Multi-Platform 6.2.6.11403
- Bitdefender Endpoint Security for Mac 7.4.10.200022
- Bitdefender Endpoint Security Tools for Linux 7.0.3.1986
- Bitdefender Endpoint Security Tools for Windows 7.5.1.177

اطلاعات کامل در خصوص تغییرات و بهبودهای لحاظ شده در نسخ مذکور در لینک زیر قابل مطالعه است:

https://www.bitdefender.com/business/support/en/77212-48453-release-notes.html

کسپرسکی

شرکت کسپرسکی (AO Kaspersky Lab) با انتشار بروزرسانی خودکار، دو آسیب‌پذیری CVE-2022-27534 و CVE-2021-27223 را در محصولات زیر ترمیم کرد:

- Kaspersky Anti-Virus
- Kaspersky Total Security
- Kaspersky Security Cloud
- Kaspersky Internet Security
- Kaspersky Endpoint Security
- Kaspersky Small Office Security

توضیحات این شرکت در مورد آسیب‌پذیری‌های مذکور در لینک زیر قابل مطالعه است:

https://support.kaspersky.com/general/vulnerability.aspx?el=12430#310322_1

ای‌سِت

شرکت ضدویروس ای‌ست (ESET, LLC.) در فروردین ماه با بروزرسانی نسخ ضدویروس برای سیستم‌های عامل Linux، آسیب‌پذیری CVE-2022-0615 را ترمیم نمود. جزییات کامل در خصوص آسیب‌پذیری ترمیم شده در لینک زیر قابل دریافت و مطالعه است:

https//:support.eset.com/en/ca8230-use-after-free-vulnerability-fixed-in-eset-products-for-linux

اف-سکیور

شرکت ضدویروس اف-سکیور (F-secure, Corp.) با انتشار بروزرسانی ۲۲ مارس آسیب‌پذیری CVE-2021-44751 با درجه اهمیت متوسط را در محصول SAFE for Android برطرف نمود. اطلاعات کامل در خصوص آسیب‌پذیری مذکور در لینک زیر قابل دسترس است:

https//:www.f-secure.com/en/home/support/security-advisories/cve2021-44751-

ترند میکرو

شرکت ترند میکرو (Trend Micro, Inc.) با انتشار نسخه Antivirus for Mac 11.5.1038، آسیب‌پذیری CVE-2022-27883 از نوع "ارتقای سطح دسترسی" را ترمیم نمود. جزییات کامل در خصوص آسیب‌پذیری مذکور در لینک زیر قابل دریافت و مطالعه است:

https://helpcenter.trendmicro.com/en-us/article/tmka-10978

وی‌ام‌ور

در ماه گذشته، شرکت وی‌ام‌ور (VMware, Inc.) با انتشار توصیه‌نامه‌های امنیتی، نسبت به ترمیم ضعف‌های امنیتی با شناسه‌های CVE-2022-22951، CVE-2022-22952، CVE-2022-22966، CVE-2022-22962، CVE-2022-22964، CVE-2022-22958، CVE-2022-22959، CVE-2022-22960، CVE-2022-22957، CVE-2022-22956، CVE-2022-22955، CVE-2022-22954، CVE-2022-22965، CVE-2022-22948، CVE-2022-22961 و CVE-2022-22945 در محصولات زیر اقدام کرد:

- VMware Cloud Director
- VMware Horizon Client for Linux
- vRealize Suite Lifecycle Manager
- VMware Identity Manager (vIDM)
- VMware vRealize Automation (vRA)
- VMware vCenter Server (vCenter Server)
- VMware Workspace ONE Access (Access)
- VMware Carbon Black App Control (AppC)
- VMware Cloud Foundation (Cloud Foundation)
- VMware NSX Data Center for vSphere (NSX-V)
- VMware Tanzu Application Service for VMs (TAS)
- VMware Tanzu Operations Manager (Ops Manager)
- VMware Tanzu Kubernetes Grid Integrated Edition (TKGI)

سوءاستفاده از ضعف‌های امنیتی ترمیم شده توسط این بروزرسانی‌ها، مهاجم را قادر به در اختیار گرفتن کنترل سامانه آسیب‌پذیر و دستیابی به اطلاعات حساس می‌کند. جزییات بیشتر آن در لینک زیر قابل مطالعه است:

https//:www.vmware.com/security/advisories.html

ادوبی

شرکت ادوبی (Adobe, Inc.) مجموعه اصلاحیه‌های امنیتی ماه آوریل ۲۰۲۲ را برای چهار نرم‌افزار این شرکت منتشر کرده است. اصلاحیه‌های مذکور، ضعف‌های امنیتی را در محصولات زیر ترمیم کرده است:

- Adobe Commerce
- Adobe Acrobat and Reader
- Adobe After Effects
- Adobe Photoshop

بیشترین آسیب‌پذیری ترمیم شده این ماه ادوبی، مرتبط با Adobe Acrobat and Reader با ۶۲ مورد بوده است. ضعف‌های امنیتی برطرف شده در این نرم‌افزار دارای بالاترین درجه اهمیت یعنی "حیاتی" بوده و مرتبط با مشکلات آزادسازی فضای حافظه پس از استفاده از آن (Use-After-Free - به اختصار UAF) و نوشتن داده‌های Out-of-Bound به اختصار OOB می‌باشند. چنانچه مهاجم بتواند کاربر را متقاعد کند که یک فایل PDF دستکاری شده را باز کند، قادر خواهد بود کد مخرب خود را روی سیستم مورد نظر اجرا کند.

ادوبی در بروزرسانی ماه آوریل ۲۰۲۲، سیزده ضعف امنیتی که همگی دارای درجه اهمیت "حیاتی" و از نوع "اجرای کد" می‌باشند را در Photoshop ترمیم نموده است. در این محصول نیز مهاجم باید کاربر را جهت باز نمودن و اجرای یک فایل دستکاری شده فریب دهد.

همچنین این شرکت دو ضعف امنیتی با درجه اهمیت "حیاتی" را در محصول After Effects که می‌توانند امکان اجرای کد را برای مهاجم فراهم کنند، برطرف نموده است. هر دو آسیب‌پذیری مذکور از نوع "سرریز حافظه" (Buffer Overflow) می‌باشند.

در نهایت، اصلاحیه ارائه شده برای Adobe Commerce نیز تنها یک ضعف امنیتی با درجه اهمیت "حیاتی" و دارای درجه شدت ۹/۱ (بر طبق استاندارد CVSS) را رفع می‌کند. با وجود درجه شدت بالای اعلام شده برای این آسیب‌پذیری، مهاجم جهت بهره‌جویی از آن به سطح دسترسی بالا نیاز دارد.

اگر چه موردی مبنی بر سوءاستفاده از آسیب‌پذیری‌های ترمیم شده تا ۲۴ فروردین ۱۴۰۱ گزارش نشده، ادوبی به مشتریان خود توصیه می‌کند که در اسرع وقت اقدام به نصب بروزرسانی‌ها کنند. اطلاعات بیشتر در خصوص مجموعه اصلاحیه‌های ماه آوریل ۲۰۲۲ در لینک زیر قابل مطالعه است:

https://helpx.adobe.com/security/security-bulletin.html

گوگل

شرکت گوگل (Google, LLC) در فروردین ماه، در چندین نوبت اقدام به ترمیم آسیب‌پذیری‌های امنیتی مرورگر Chrome کرد. آخرین نسخه این مرورگر که در ۲۵ فروردین ماه انتشار یافت، نسخه ۱۰۰/۰/۴۸۹۶/۱۲۷ است. فهرست اشکالات مرتفع شده در لینک زیر قابل دریافت و مشاهده است:

https//:chromereleases.googleblog.com/2022/04/stable-channel-update-for-desktop.14_html

اپل

در فروردین ماه، شرکت اپل (Apple, Inc.) با انتشار بروزرسانی، ضعف‌های امنیتی متعددی را در چندین محصول خود از جمله iOS، iPadOS و macOS Monterey ترمیم و اصلاح کرد. سوءاستفاده از برخی از ضعف‌های مذکور، مهاجم را قادر به در اختیار گرفتن کنترل سامانه آسیب‌پذیر می‌کند. توصیه می‌شود با مراجعه به نشانی زیر، بروزرسانی‌های مربوطه هر چه سریع‌تر اعمال شود.

https//:support.apple.com/en-us/HT201222

مـوزیـلا

در ماه گذشته، شرکت موزیلا (Mozilla, Corp) با ارائه بروزرسانی، چند آسیب‌پذیری امنیتی را در مرورگر Firefox و نرم‌افزار مدیریت ایمیل Thunderbird برطرف کرد. اصلاحیه‌های مذکور، در مجموع ۱۳ آسیب‌پذیری را در محصولات مذکور ترمیم می‌کنند. درجه حساسیت سه مورد از آنها "بالا"، هفت مورد "متوسط" و سه مورد "پایین" گزارش شده است. سوءاستفاده از برخی از ضعف‌های مذکور، مهاجم را قادر به در اختیار گرفتن کنترل دستگاه آسیب‌پذیر می‌کند. توضیحات بیشتر در لینک زیر قابل مطالعه است:

https//:www.mozilla.org/en-US/security/advisories/

سـوفـوس

شرکت سوفوس (Sophos, Ltd.) در فروردین ماه نسخه جدید 9.710 از ثابت‌افزار SG UTM را منتشر کرده است. طبق روال همیشگی، نسخه جدید در چند مرحله عرضه خواهد شد.

در مرحله اول، بسته بروزرسانی از سرور سوفوس به نشانی زیر قابل دریافت است.

Up2date package 9.709 to 9.710:

https://download.astaro.com/UTM/v9/up2date/u2d-sys-9.709003-710001.tgz.gpg

- در مرحله دوم، شرکت سوفوس بسته بروزرسانی را از طریق سرورهای Up2Date خود به تدریج در چند مرحله، در دسترس قرار خواهد داد.
- در مرحله سوم، شرکت سوفوس بسته بروزرسانی را از طریق سرورهای Up2Date خود برای تمام مدل‌های باقیمانده، در دسترس قرار خواهد داد.

در این نسخه جدید، برنامه قدیمی SSLVPN Client دیگر در دسترس نخواهد بود و امکان دریافت آن از پورتال کاربران نیز حذف شده است. جایگزین آن، برنامه جدید و پیشرفته تر Sophos Connect می‌باشد. جهت کسب اطلاعات بیشتر به نشانی‌های زیر مراجعه شود.

https//:support.sophos.com/support/s/article/KB?000043484-language=en_US

https//:www.sophos.com/en-us/security-advisories/sophos-sa-20220303-sslvpn-local-dos

با توجه به اینکه عرضه و فروش برنامه IPSec VPN Client نیز در ۱۰ فروردین ۱۴۰۱ به پایان رسیده است، سوفوس صفحه User Portal را به منظور پشتیبانی از برنامه جدید Sophos Connect بروز کرده است.

جزئیات نسخه جدید ۹۷۱۰ و نحوه عملکرد آن در نشانی‌های زیر قابل مطالعه می‌باشد.

https//:community.sophos.com/utm-firewall/b/blog/posts/utm-up2date-9-710-released

https//:newsroom.shabakeh.net/23793/utm-up2date-9-710-released.html

این شرکت، دو آسیب‌پذیری با شناسه‌های CVE-2022-0386 و CVE-2022-0652 را نیز در فایروال‌های Sophos، سری SG ترمیم کرده است، لذا ضروری است فایروال‌ها به این نسخه جدید ارتقاء یابند. توضیحات بیشتر در خصوص این ضعف‌های امنیتی در نشانی زیر قابل دریافت است:

https//:newsroom.shabakeh.net/23750/sg-utm-cve.2022-0386-html

همچنین سوفوس در ماه گذشته یک آسیب‌پذیری به شناسه CVE-2022-1040 در بخش احراز هویت WebAdmin و UserPortal فایروال‌های Sophos سری XG، که امکان اجرای کد از دور (Remote Code Execution) را برای مهاجمان فراهم می‌کند، ترمیم نمود. جزئیات بیشتر درباره آسیب پذیری مذکور در لینک‌های زیر قابل دسترسی است:

https//:www.sophos.com/en-us/security-advisories/sophos-sa-20220325-sfos-rce

https//:newsroom.shabakeh.net/23742/xg-firewall-cve.2022-1040-html

این شرکت، نسخه جدیدی از ثابت‌افزار SFOS را نیز ارائه کرد که علاوه بر ترمیم ضعف‌های مهم امنیتی و عملکردی، برخی امکانات جدید درخواستی مشتریان و نمایندگان را نیز دارا می‌باشد. طبق معمول، این بروزرسانی نرم‌افزاری برای تمامی دستگاه‌های فایروال سوفوس با لیسانس معتبر، هیچ هزینه‌ای ندارد و باید در اسرع وقت برای همه دستگاه‌های فایروال تحت پشتیبانی، اعمال شود. جزئیات بیشتر در خصوص ویژگی‌های برجسته نسخه جدید SFOS v18.5 MR3 و نحوه بروزرسانی آن در نشانی‌های زیر قابل مطالعه می‌باشد.

https//:docs.sophos.com/releasenotes/index.html?productGroupID=nsg&productID=xg&versionID18.5=

https//:newsroom.shabakeh.net/23800/xg-update-18-5-3-release-notes.html

اوراکـل

۳۰ فروردین ۱۴۰۱، شرکت اوراکل (Oracle Corp) مطابق با برنامه زمانبندی شده سه‌ماهه خود، با انتشار مجموعه بروزرسانی‌های موسوم به Critical Patch Update اقدام به ترمیم ۵۲۰ آسیب‌پذیری امنیتی در ده‌ها محصول ساخت این شرکت کرد. سوءاستفاده از برخی از آسیب‌پذیری‌های مذکور مهاجم را قادر به اجرای کد به‌صورت از راه دور بدون نیاز به هر گونه اصالت‌سنجی می‌کند. جزییات کامل در خصوص آنها در لینک زیر قابل دریافت است:

https://www.oracle.com/security-alerts/cpuapr2022.html

دروپـال

اول فرودین ۱۴۰۱، جامعه دروپال (Drupal Community) با عرضه بروزرسانی‌های امنیتی، یک ضعف امنیتی با شناسه CVE-2022-24775 را در نسخه‌های ۹٫۲ و ۹٫۳ ترمیم نمود. سوءاستفاده از این آسیب‌پذیری، مهاجم را قادر به در اختیار گرفتن کنترل سامانه می‌کند.

همچنین در ۳۱ فروردین ماه، این شرکت با انتشار دو توصیه‌نامه امنیتی به شماره‌های SA-CORE-2022-008 و SA-CORE-2022-009، دو ضعفی امنیتی با درجه اهمیت نسبتاً حیاتی (Moderately critical) را در پروژه Drupal Core برطرف نمود.

توضیحات کامل در خصوص این بروزرسانی‌ها و توصیه‌نامه‌های منتشر شده، در آدرس‌های زیر در دسترس می باشد.

https://www.drupal.org/sa-core-2022-006

https://www.drupal.org/sa-core-2022-008

https://www.drupal.org/sa-core-2022-009

آپاچی

در فروردین ۱۴۰۱، بنیاد نرم‌افزاری آپاچی (Apache Software Foundation)، با انتشار توصیه‌نامه‌ای اقدام به ترمیم ضعفی به شناسه CVE-2021-31805 در Apache Struts نموده است. نسخه‌های ۲٫۰٫۰ تا ۲٫۵٫۲۹ از این آسیب‌پذیری تاثیر می‌پذیرند و سوءاستفاده از آن، مهاجم را قادر به اجرای کد از راه دور و کنترل سیستم آسیب‌پذیر می‌کند. توصیه می‌شود راهبران امنیتی ضمن مطالعه توصیه‌نامه مذکور در نشانی زیر، Struts را به نسخه ۲٫۵٫۳۰ ارتقاء دهند.

https//:cwiki.apache.org/confluence/display/WW/S2-062

سیتریکس

در اواسط فروردین ماه، شرکت سیتریکس (Citrix Systems, Inc.) نیز با عرضه بروزرسانی‌های امنیتی، هشت آسیب‌پذیری با شناسه‌های CVE-2022-26357، CVE-2022-27503، CVE-2022-27505، CVE-2022-27506، CVE-2021-44519، CVE-2021-44520، CVE-2022-26151 و CVE-2022-21827 را در Citrix Hypervisor، XenServer، Citrix Virtual Apps and Desktops، StoreFront، Citrix SD-WAN، XenMobile، Citrix ADC و Citrix Gateway ترمیم کرد. مهاجم می‌تواند از این ضعف‌های امنیتی برای کنترل سیستم آسیب‌پذیر سوءاستفاده کند. توصیه می‌شود راهبران امنیتی جزییات ضعف‌های امنیتی مذکور را در آدرس‌های زیر مرور کرده و بروزرسانی‌های لازم را اعمال کنند.

https://support.citrix.com/article/CTX390511

https://support.citrix.com/article/CTX377814

https://support.citrix.com/article/CTX370550

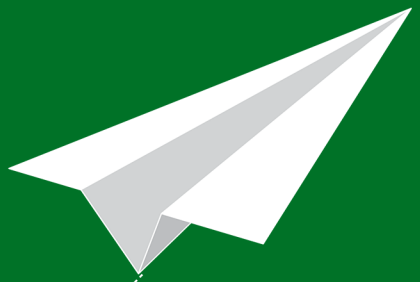
https://support.citrix.com/article/CTX370551

https://support.citrix.com/article/CTX341455

جونیپر نت‌ورکز

جونیپر نت‌ورکز (Juniper Networks, Inc.) هم در فروردین ماه با ارائه بروزرسانی چندین ضعف امنیتی را محصولات مختلف این شرکت ترمیم کرد. سوءاستفاده از ضعف‌های مذکور مهاجم را قادر به در اختیار گرفتن کنترل دستگاه آسیب‌پذیر می‌کند. جزییات بیشتر در لینک زیر قابل مطالعه است:

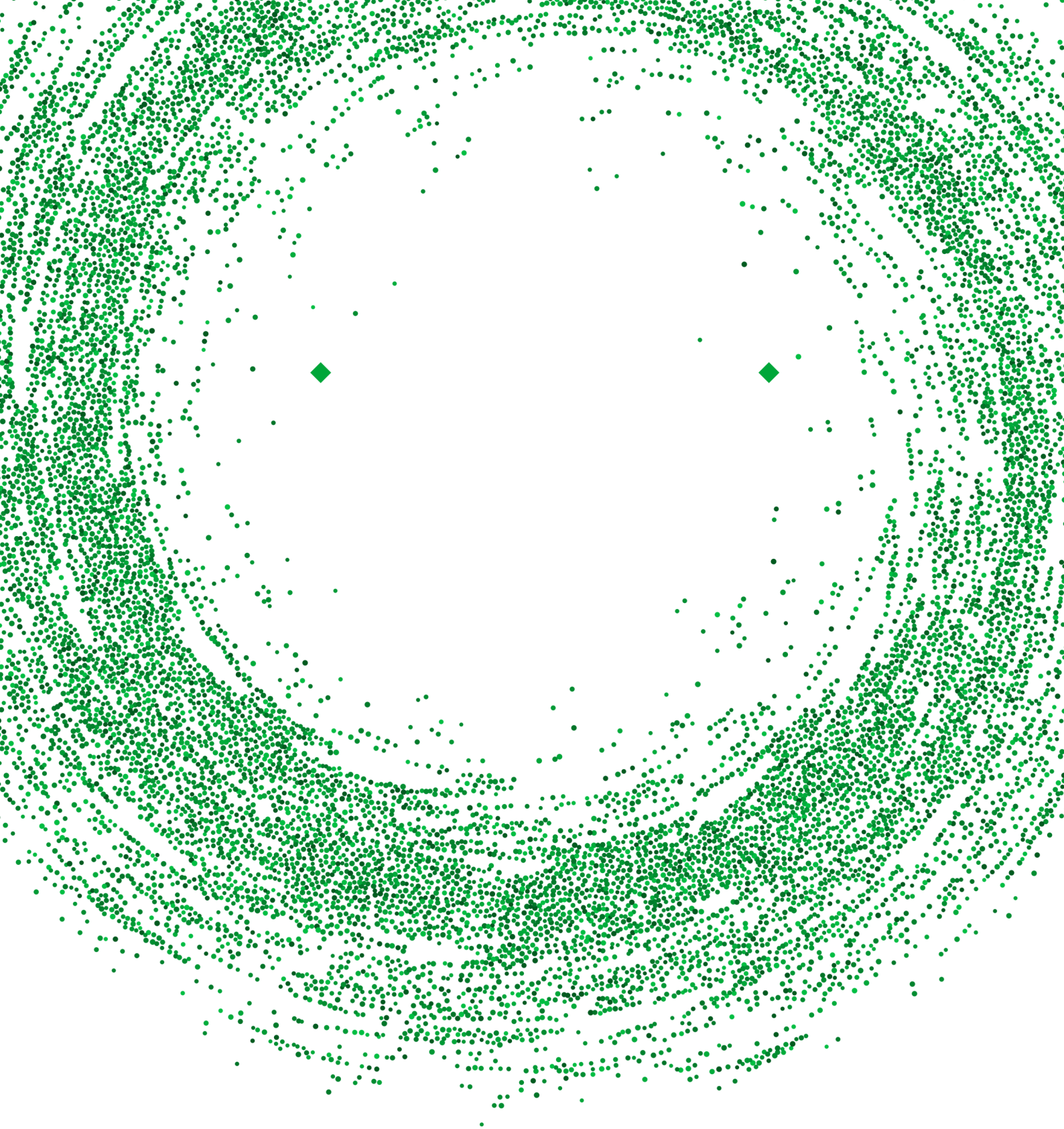
https://kb.juniper.net/InfoCenter/index?page=content&channel=SECURITY_ADVISORIES



آخـرین اخبـار امنیـت فنـاوری اطلاعات

@SGnewsroom

شرکت مهندسی شبکه گستر در سال ۱۳۷۰ تأسیس گردید و اولین شرکت ایرانی است که در زمینه نرم‌افزارهای ضدویروس فعالیت تخصصی و متمرکزی را آغاز کرده است. در ابتدا، همکاری مشترکی بین شرکت مهندسی شبکه گستر و شرکت انگلیسی S & S International (تولیدکننده ضدویروس مشهور Toolkit) آغاز گردید. در مدت کوتاهی، با فعالیت شبکه گستر به عنوان نماینده رسمی و انحصاری S & S International در ایران، به تدریج ضدویروس Dr Solomon's Toolkit به محبوب‌ترین ضدویروس در ایران تبدیل شد. پس از خرید شرکت S & S International توسط شرکت McAfee در سال ۱۳۷۷، شرکت شبکه گستر نیز مانند دیگر نمایندگان بین‌المللی فعالیت خود را بر روی نرم‌افزارهای ضدویروس McAfee ادامه داد. اکنون نیز شبکه گستر به عنوان فروشنده مجاز (Authorized Reseller) در منطقه خاورمیانه، به ارائه محصولات و خدمات در ایران اقدام می‌نماید. در سال ۱۳۸۴ شرکت مهندسی شبکه گستر موفق به کسب نمایندگی رسمی شرکت آلمانی Astaro، سازنده محصولات مدیریت یکپارچه تهدیدات (Unified Threat Management) گردید. به دنبال رشد چشمگیر و موفقیت جهانی محصولات امنیتی شرکت Astaro، در سال ۱۳۹۰ شرکت Sophos انگلیس، اقدام به خرید این شرکت آلمانی نمود. به دنبال این نقل و انتقال، شرکت مهندسی شبکه گستر با همکاری با شرکت Sophos، فعالیت خود را در این زمینه ادامه داده و اکنون محصولات Astaro سابق را تحت نام Sophos در ایران عرضه می‌نماید. از سال ۱۳۹۱ شرکت مهندسی شبکه گستر عرضه محصولات ضدویروس Bitdefender را به عنوان نماینده و توزیع‌کننده (Distributor) رسمی در ایران آغاز کرد. عرضه محصولات ضدویروس Bitdefender در کنار محصولات امنیتی McAfee، پاسخی به شرایط و نیازهای متفاوت کاربران و مدیران شبکه بوده است. ضدویروس چابک‌تر، مدیریت آسان‌تر و محصولی مقرون به صرفه‌تر، انتظارات برخی از کاربران و مدیران شبکه بود که با عرضه محصولات ضدویروس Bitdefender، شبکه گستر به نیازهای این بخش از بازار پاسخ داد. شرکت مهندسی شبکه گستر افتخار دارد که مجری برخی از بزرگترین پروژه‌های نصب و راه‌اندازی و طولانی مدت‌ترین قراردادهای نگهداری و پشتیبانی محصولات امنیت شبکه در کشور بوده است. این شرکت علاوه بر خدمات‌دهی به هزاران شرکت و سازمان که صدها هزار کاربر را در کشور شامل می‌شوند، دارای شبکه نمایندگی فروش و پشتیبانی در سراسر کشور نیز می‌باشد.



شرکت مهندسی شبکه گستر

تهران ۱۹۶۸۶، خیابان شهید دستگردی (ظفر)، شماره ۲۷۳

تلفن / دورنگار ۴۲۰۵۲ - ۰۲۱

رایانامه info@shabakeh.net

تارنمای شرکت www.shabakeh.net

خدمات پس از فروش و پشتیبانی my.shabakeh.net

مرکز آموزش events.shabakeh.net

اتاق خبر newsroom.shabakeh.net