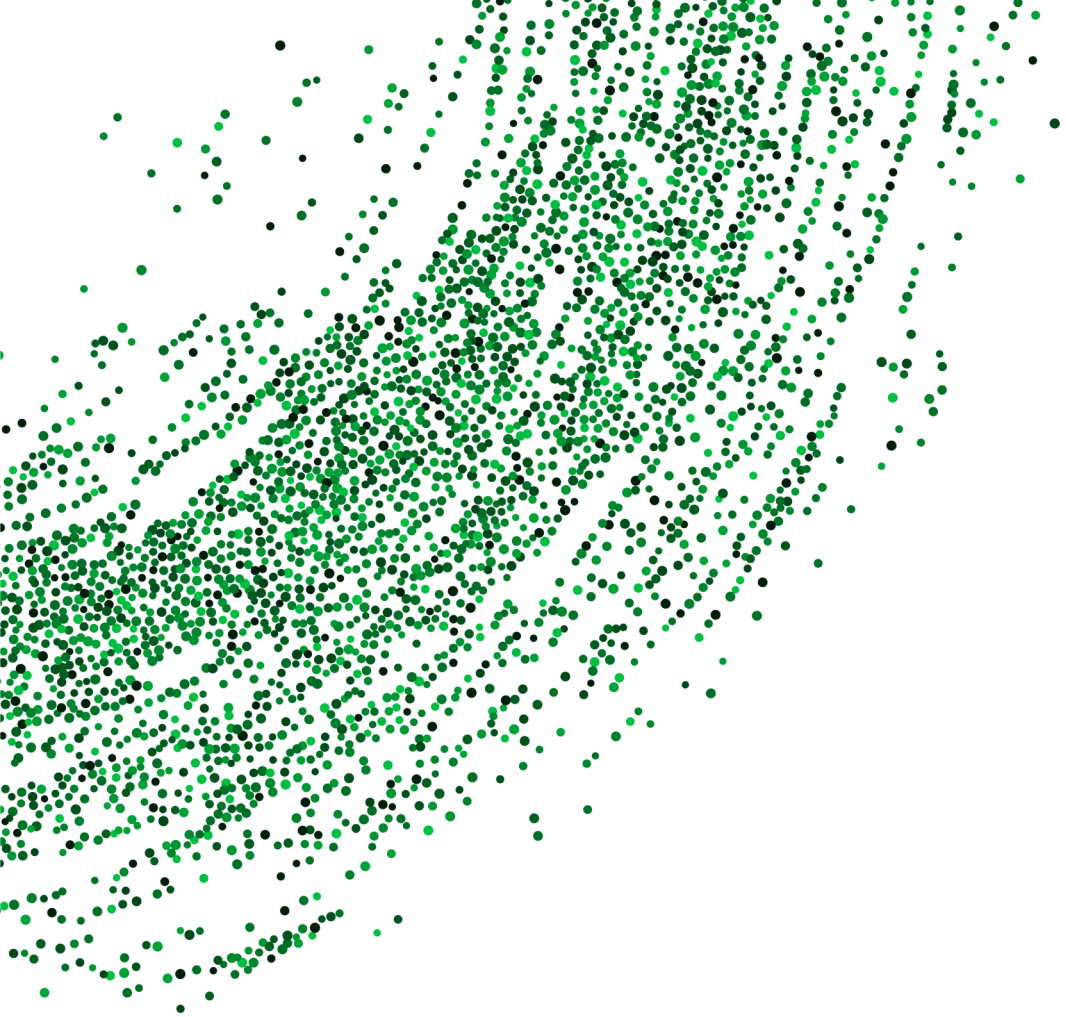
شبکه گستر

امنیت شما | وظیفه ما

ماهنامه
امنیت فناوری اطلاعات

شرکت مهندسی شبکه گستر | سال دوازدهم | فروردین 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 آخرین ماه از سال ۱۴۰۰ پرداخته شده است.

یافته‌های شرکت امنیتی بیت‌دیفندر نشان می‌دهد که باج‌افزار WannaCry که از سال ۲۰۱۷ قربانی می‌گیرد، همچنان تهدیدی جدی و فعال باقی مانده است و از میان ۱۰.۵ میلیون بدافزار شناسایی شده، ۴۳ درصد آن مربوط به باج‌افزار WannaCry می‌باشد که به مراتب بیشتر از هر باج‌افزار دیگری بوده است. محققان امنیتی شرکت امنیت سایبری سیمانتک نیز بدافزار پیچیده و پیشرفته Daxin را که شبکه‌های دولتی مقاوم‌سازی شده را برای جاسوسی سایبری مورد هدف قرار می‌دهد، بررسی کرده‌اند. برگردان مشروح این دو گزارش در این ماهنامه قابل مطالعه است.

در ماه گذشته یک آسیب‌پذیری با شناسه CVE-2022-0633 و دارای درجه اهمیت از نوع "بالا" در افزونه UpdraftPlus کشف شد. بنیاد وردپرس در اقدامی نادر، تمام سایت‌های مبتنی بر WordPress را به طور مستقیم و به اجبار بروز نمود تا ضعف امنیتی فوق را برطرف کند. آسیب‌پذیری مذکور به مشترکین سایت، کاربران با سطح دسترسی پایین و سایر کاربران غیرمجاز اجازه می‌دهد تا زمانی که در سایت آسیب‌پذیر حساب کاربری دارند، آخرین نسخه پشتیبان از پایگاه داده خصوصی سایت را که اغلب شامل اطلاعات حساس مشتریان یا تنظیمات امنیتی سایت می‌باشد، دریافت کنند. این ضعف امنیتی به تفصیل در این ماهنامه مورد بررسی قرار گرفته است.

دیگر موضوعی که در این ماهنامه به آن پرداخته شده است، نفوذ مهاجمان به حساب‌های کاربری Microsoft Teams و انتشار فایل‌های اجرایی مخرب در مکالمات گروهی، بین اعضاء گروه می‌باشد. بستر ارتباطی Microsoft Teams امکان مکالمه، کنفرانس تصویری و ذخیره فایل را به ویژه در محیط‌های کسب و کار فراهم می‌آورد. بیش از ۲۷۰ میلیون کاربر هر ماه از Microsoft Teams استفاده می‌کنند و به آن اعتماد دارند، علیرغم اینکه هیچ راهکاری برای محافظت در برابر فایل‌های مخرب در آن وجود ندارد.

در اسفند ماه، شرکت امنیتی سوفوس، نسخه جدید SG UTM 9.709 را طبق روال همیشگی در چند مرحله ارائه نمود که جزئیات دقیق بروزرسانی و فهرست اشکالات برطرف شده در این ماهنامه به تفصیل مورد بررسی قرار گرفته است.

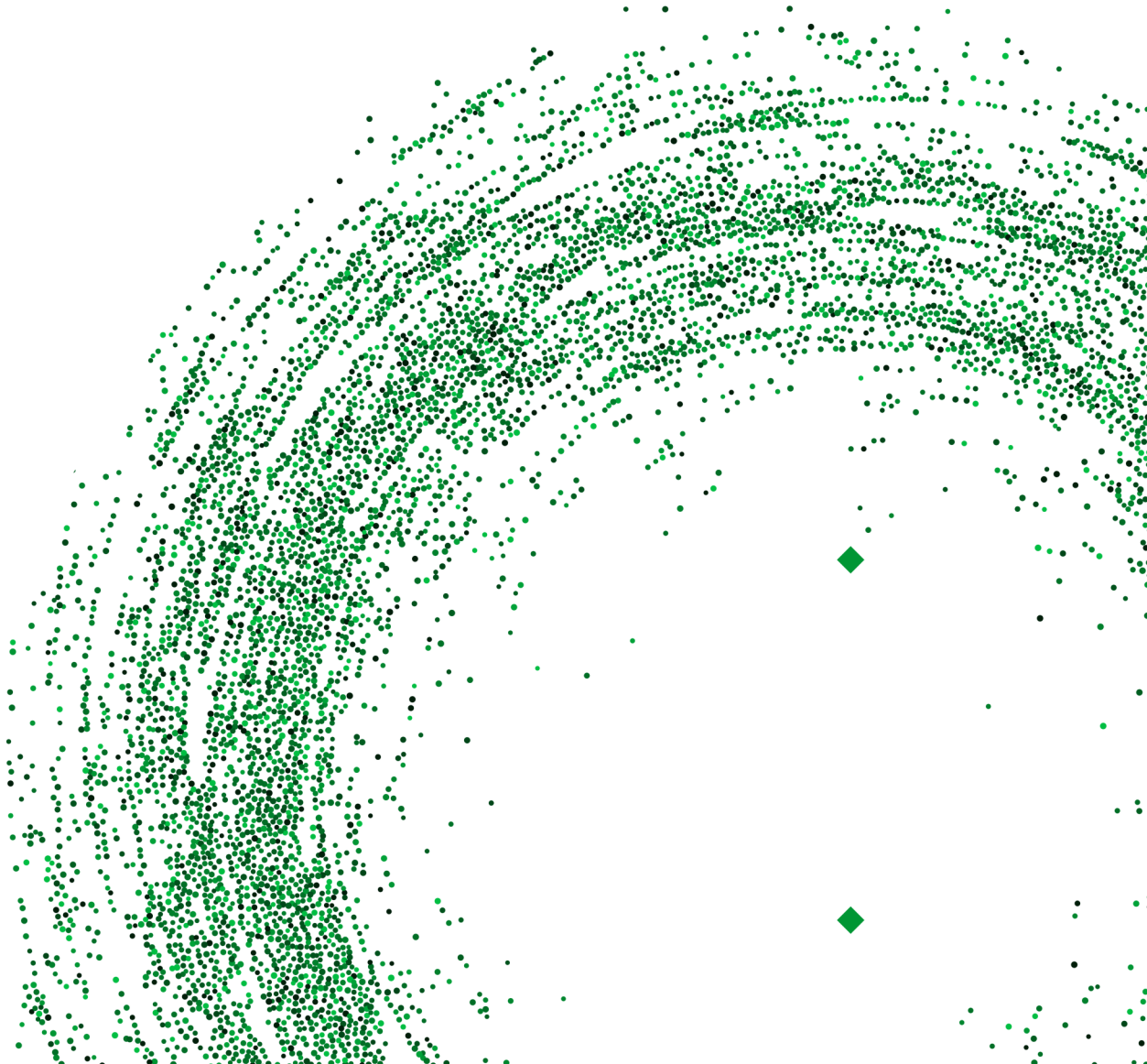
همزمان با شروع جنگ روسیه و اوکراین در اسفند ماه ۱۴۰۰، شرکت تلگرام اذعان نمود که در جریان این جنگ، با اعمال محدودیت کامل یا نسبی برای کانال‌های خاص، از سوءاستفاده مهاجمان سایبری از این پیام‌رسان جهت "تعمیق درگیری میان روسیه و اکراین" جلوگیری می‌کند. شرکت مایکروسافت نیز در گزارشی اعلام نمود که چند ساعت قبل از حمله روسیه به اوکراین، شبکه‌های اوکراینی با بدافزار FoxBlade مورد هدف حملات سایبری تهاجمی و مخرب قرار گرفتند. مشروح گزارش این دو شرکت در این ماهنامه قابل مطالعه است.

در آخرین ماه سال ۱۴۰۰، شرکت‌های مایکروسافت، سیسکو، مک‌آفی‌اینترپرایز، بیت‌دیفندر، ایسِت، اف-سکیور، برودکام، ترند میکرو، وی‌ام‌ور، ادوبی، گوگل، اپل، موزیلا، سوفوس، اس‌ای‌پی، دروپال و اپن-اس‌اس‌ال اقدام به عرضه بروزرسانی و توصیه‌نامه امنیتی برای برخی محصولات خود کردند. جزییات این بروزرسانی‌ها و گزارش‌های متنوع دیگر را در این ماهنامه بخوانید.

همچنین در اسفند ماه، اولین گزارش فصلی Advanced Threat Research تحت نام شرکت جدید Trellix منتشر شد. شرکت Trellix از ادغام دو شرکت بزرگ امنیتی McAfee و FireEye تشکیل شده است. این گزارش مروری بر روند تهدیدات سایبری در یکسال گذشته میلادی و به ویژه ماههای پایانی سال ۲۰۲۱ داشته و در پایان نیز انواع تهدیدات سایبری را بر اساس نوع بدافزار، منطقه فعالیت، نوع قربانیان و روشهای بکار گرفته شده، دسته‌بندی و میزان فراوانی هر یک با نمودارهای رنگین ارائه کرده است.

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 راهنمایی برای ارتقای دانش کاربران این حوزه باشد.

هشدارهای امنیتی



Microsoft Teams

بستر جدیدی برای توزیع بدافزار

محققان امنیتی هشدار می‌دهند که برخی مهاجمان با نفوذ به حساب‌های کاربری Microsoft Teams، وارد مکالمات گروهی شده تا بدین وسیله فایل‌های اجرایی مخرب را بین اعضاء گروه منتشر کنند.

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

بستر ارتباطی Microsoft Teams بخشی از مجموعه محصولات Microsoft 365 است که امکان مکالمه، کنفرانس تصویری و ذخیره فایل را به ویژه در محیط‌های کسب و کار فراهم می‌آورد. بیش از ۲۷۰ میلیون کاربر هر ماه از Microsoft Teams استفاده می‌کنند و به آن اعتماد دارند، علیرغم اینکه هیچ راهکاری برای محافظت در برابر فایل‌های مخرب در آن وجود ندارد.

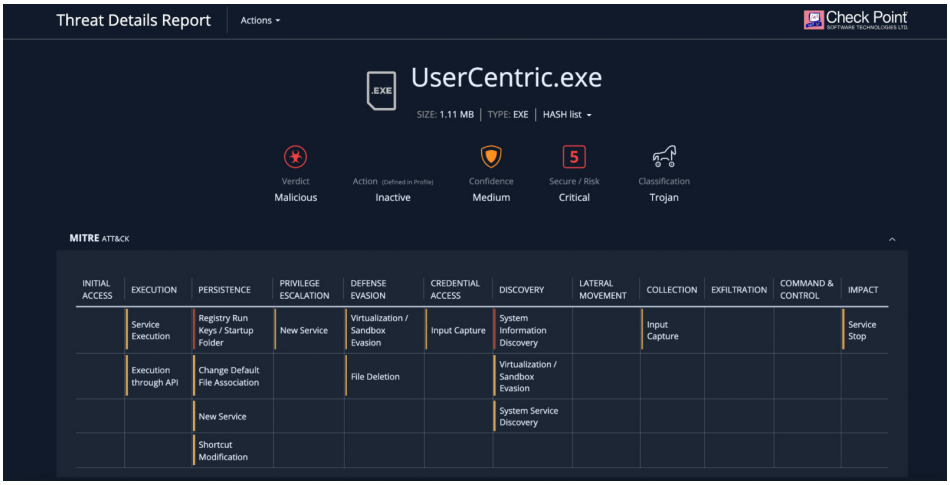
اخیراً محققان شرکت اوانان (Avanan, Inc.) که در زمینه امنیت ایمیل‌های ابری و بسترهای اشتراکی فعالیت می‌کنند، پی بردند که هکرها شروع به انتشار فایل‌های اجرایی مخرب در مکالمات بر روی بستر ارتباطی Microsoft Teams کرده‌اند.

این حملات از دی ماه امسال آغاز شده و این شرکت هزاران مورد از آنها را تاکنون شناسایی کرده است. بنا بر داده‌های موجود، بیشتر حملات به سازمان‌هایی در یک منطقه از ایالات متحده صورت گرفته است. طبق گزارش شرکت اوانان، مهاجمان یک فایل اجرایی به نام User Centric را در مکالمات منتشر می‌کنند تا کاربر را جهت اجرای آن فریب دهند. فایل مذکور پس از اجرا، داده‌هایی را در بخش Registry سیستم می‌نویسد و اقدام به نصب فایلهای از نوع DLL می‌کند و در سیستم Windows ماندگار می‌شود.

> “In this Teams attack, hackers have attached a malicious Trojan document to a chat thread. When clicked on, the file will eventually take over the user’s computer” - Avanan

روش بکارگرفته شده جهت دسترسی و نفوذ اولیه به حساب‌های کاربری Microsoft Teams همچنان برای محققان نامشخص است، اما احتمال می‌دهند که مهاجمان از طریق نفوذ به شبکه سازمان‌های همکار یا با استفاده از روش‌های ”فریب سایبری“ موسوم به ”فیشینگ“، اطلاعات اصالت‌سنجی ایمیل یا نرم افزار Microsoft 365 را سرقت نموده و به حساب کاربری افراد دسترسی پیدا کرده‌اند.

تحلیل بدافزار توزیع شده به این روش نشان می‌دهد که بدافزار می‌تواند از طریق فرامین Registry در Windows و یا با اضافه کردن فایل‌هایی در پوشه راه‌اندازی (Startup Folder)، در سیستم ماندگار شود و فعال بماند. همچنین بدافزار اطلاعات دقیقی در مورد سیستم‌عامل و سخت‌افزاری که روی آن اجرا می‌شود را به همراه وضعیت امنیتی دستگاه بر اساس نسخه سیستم‌عامل و وصله‌های نصب شده آن، جمع‌آوری می‌کند.



به گفته محققان شرکت اوانان، اگرچه روش بکار رفته در این حمله بسیار ساده است، اما برای مهاجمان بسیار موثر می‌باشد، زیرا بسیاری از کاربران به فایل‌های دریافتی از طریق Microsoft Teams اعتماد دارند. این شرکت ضمن تحلیل داده‌های بیمارستان‌هایی که از Microsoft Teams استفاده می‌کنند، دریافت که پزشکان نیز از این بستر برای اشتراک‌گذاری اطلاعات پزشکی بدون هیچ گونه محدودیتی استفاده می‌کنند.

افراد معمولاً به دلیل آموزش و آگاهی از حملات "فیشینگ" در ایمیل، نسبت به اطلاعات دریافتی از طریق ایمیل مشکوک و محتاط هستند اما در خصوص دریافت فایل‌های دریافت شده از طریق Teams هیچ دقتی ندارند. علاوه بر این، Teams قابلیت‌هایی نظیر دسترسی افراد مهمان و امکان همکاری با اشخاص خارج از سازمان را فراهم می‌کند که متاسفانه این دعوت‌ها معمولاً با حداقل نظارت و ملاحظات امنیتی انجام می‌شود.

محققان می گویند که این مسئله "به دلیل عدم وجود محافظت پیش فرض در Teams و پویش محدود لینک‌ها و فایل‌های مخرب در آن" و همچنین "عدم ارائه محافظت قوی برای Team توسط راهکارهای امنیتی ایمیل" تشدید می‌شود.

برای دفاع در برابر چنین حملاتی، موارد زیر به کاربران توصیه می‌شود:

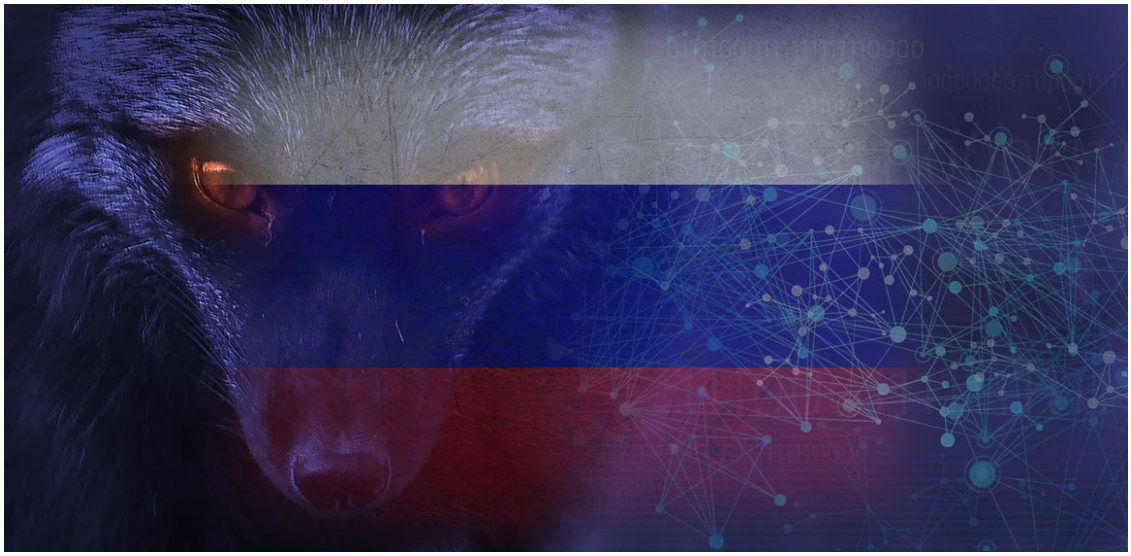
- بکارگیری راهکارهای امنیتی جهت دریافت تمامی فایل‌ها در جعبه شنی (Sandbox) و بررسی وجود محتوای مخرب در آنها.
- پیاده‌سازی و استفاده از محصولات امنیتی قوی و جامع جهت ایمن‌سازی تمامی بسترهای ارتباطی در محیط کسب و کار از جمله Microsoft Teams.
- تشویق کاربران به اطلاع‌رسانی و تماس با راهبران امنیتی سازمان در هنگام مشاهده یک فایل ناآشنا و غیرعادی.

منبع:

https://www.bleepingcomputer.com/news/security/hackers-slip-into-microsoft-teams-chats-to-distribute-malware/

بدافزار جدید FoxBlade

پیش قراول ارتش روسیه



شرکت مایکروسافت (Microsoft Corp.) در گزارشی اعلام نمود که چند ساعت قبل از حمله روسیه به اوکراین، شبکه‌های اوکراینی با بدافزار FoxBlade مورد هدف حملات سایبری تهاجمی و مخرب قرار گرفتند.

محققان مایکروسافت حملات مخربی را شناسایی کردند که در آن بدافزار FoxBlade، شبکه‌ها و زیرساخت‌های دیجیتال اوکراین را مورد هدف قرار داده است (پویش بدافزار مذکور در سایت Virus Total در نشانی زیر قابل مشاهده می‌باشد).

https://www.virustotal.com/gui/file/06086c1da4590dcc7f1e10a6be3431e1166286a9e7761f2de9de79d-7fda9c397

این بدافزار قبلاً توسط شرکت‌های امنیت سایبری سیمانتک (Symantec, Corp.) و ای‌ست (ESET, LLC.)، یک روز قبل از شروع درگیری بین روسیه و اوکراین مشاهده و گزارشی در خصوص آن منتشر شد. مشروح این گزارش که در آن از HermeticWiper برای نامگذاری بدافزار استفاده شده، به همراه علایم آلودگی (Indicators of Compromise - به اختصار IoC) در نشانی زیر قابل مطالعه می‌باشد.

https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/

مهاجمان در این حملات، اهداف دیجیتالی غیرنظامی اوکراین، از جمله بخش‌های مالی، کشاورزی، خدمات واکنش اضطراری، کمک‌های بشر دوستانه، سازمان‌ها و شرکت‌های بخش انرژی را مورد هدف قرار داده‌اند. مایکروسافت همچنین به دولت اوکراین در خصوص تلاش مهاجمان جهت سرقت داده‌ها از منابع دولتی نظیر اطلاعات مراقبت‌های بهداشتی، داده‌های بیمه، حمل‌ونقل و سایر اطلاعات شناسایی اشخاص هشدار داد و توصیه‌های فنی در خصوص روش‌های پیشگیری و محافظت در برابر این بدافزار را در نشانی‌های زیر ارائه نمود.

https://blogs.microsoft.com/on-the-issues/2022/02/28/ukraine-russia-digital-war-cyberattacks/

https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=DoS:Win32/FoxBlade.A!dha

در حال حاضر، نحوه نفوذ و آلودگی اولیه بدافزار FoxBlade مشخص نیست ولی این بدافزار بعد از آلودگی سیستم، امکان دریافت فایل‌های مخرب بیشتر را داشته تا سرعت انتشار آلودگی را افزایش دهد.

بدافزار FoxBlade عملیات مختلفی را بر روی سیستم‌های آلوده انجام می‌دهد. از جمله می‌تواند اقدام به تخریب و حذف اطلاعات نماید و یا از سیستم قربانی برای انجام حملات DDOS سوءاستفاده کند.

شرکت مایکروسافت سرویس ضدبدافزار Defender خود را ظرف سه ساعت پس از کشف FoxBlade بروزرسانی نمود تا فعالیت مخرب آن را مسدود سازد.

آژانس دولتی "امنیت سایبری و امنیت زیرساخت آمریکا" (Cybersecurity & Infrastructure Security Agency - به اختصار CISA) و "پلیس فدرال آمریکا" (Federal Bureau of Investigation - به اختصار FBI) در نشانی زیر هشدار دادند که حملات تخریب داده‌ها که علیه کشور اوکراین صورت گرفته، ممکن است خواسته یا ناخواسته به کشورهای دیگر نیز سرایت کند و ضروری است سازمان‌های مختلف در باقی کشورها هوشیار بوده و سیستم‌های امنیتی خود را تقویت کنند.

https://www.cisa.gov/uscert/ncas/alerts/aa22-057a

منابع:

https://threatpost.com/microsoft-ukraine-foxblade-trojan-hours-before-russian-invasion/178702/

https://www.bleepingcomputer.com/news/security/microsoft-ukraine-hit-with-foxblade-malware-hours-before-invasion/

https://www.zdnet.com/article/microsoft-finds-foxblade-malware-on-ukrainian-systems-re-moving-rt-from-windows-app-store/?ftag=TRE-03-10aaa6b&bhid=%7B%24external_id%7D&mid=%7B%24MESSAGE_ID%7D&cid=%7B%24contact_id%7D&eh=%7B%24CF_emailHash%7D

Daxin

برای نفوذ به شبکه‌های بسته

به تازگی محققان امنیتی شرکت امنیت سایبری سیمانتک (Symantec, Corp.)، بدافزار پیچیده و پیشرفته Daxin را که شبکه‌های دولتی مقاوم‌سازی شده را برای جاسوسی سایبری مورد هدف قرار می‌دهد، بررسی کرده‌اند.

کارشناسان این شرکت از اواسط آبان امسال فعالیت این "تهدید پیشرفته و مستمر" (Advanced Persistent Threat - به اختصار APT) را شناسایی و رصد می‌کنند. به اذعان این شرکت، Daxin پیشرفته‌ترین بدافزاری است که تاکنون از گروه‌های چینی دیده شده و پیچیدگی‌های فنی بکار رفته در این بدافزار تابحال در بین بدافزارهای چینی سابقه نداشته است.

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

تنوع عملیات بدافزار Daxin شامل خواندن و نوشتن انواع فایلها، راه‌اندازی به اختیار و دخالت در عملیات عادی سیستم، قابلیت انتشار به سیستم‌های اطراف خود در شبکه، امکانات مخفی‌سازی و ... می‌شود.

آژانس دولتی "امنیت سایبری و امنیت زیرساخت آمریکا" (Cybersecurity & Infrastructure Security Agency - به اختصار CISA) نیز ضمن تایید فعالیت بدافزار Daxin، اعلام کرد که نسخ ابتدایی این بدافزار از سال ۲۰۱۳ میلادی که بخش عمده کد بدافزار طراحی و تهیه شده، مشاهده و رصد شده است. طبق اطلاعیه این آژانس، بدافزار Daxin از نوع بدافزارهای Rootkit است که دسترسی غیرمجاز (backdoor) به سیستم قربانی را فراهم می‌کند.

در اطلاعیه آژانس CISA آمده است که این بدافزار دارای امکانات تماس با مرکز کنترل و فرماندهی (Command and Control - به اختصار C2) است و این ارتباطات را به نحو پیچیده‌ای مخفی نگه می‌دارد. امکان تماس با مرکز کنترل و فرماندهی، گردانندگان Daxin را قادر می‌سازند تا به دستگاههایی که حتی به اینترنت متصل نیستند، دسترسی پیدا کنند.

در این اطلاعیه تاکید شده که ساختار بدافزار Daxin برای استفاده علیه اهداف مقاوم‌سازی شده، بهینه شده تا بدون ایجاد سوءظن، قادر به نفوذ به عمق شبکه قربانی باشد و بتواند اطلاعات مورد نظر را جمع آوری و سرقت کند.

نهایت هنرنمایی برای مخفی ماندن

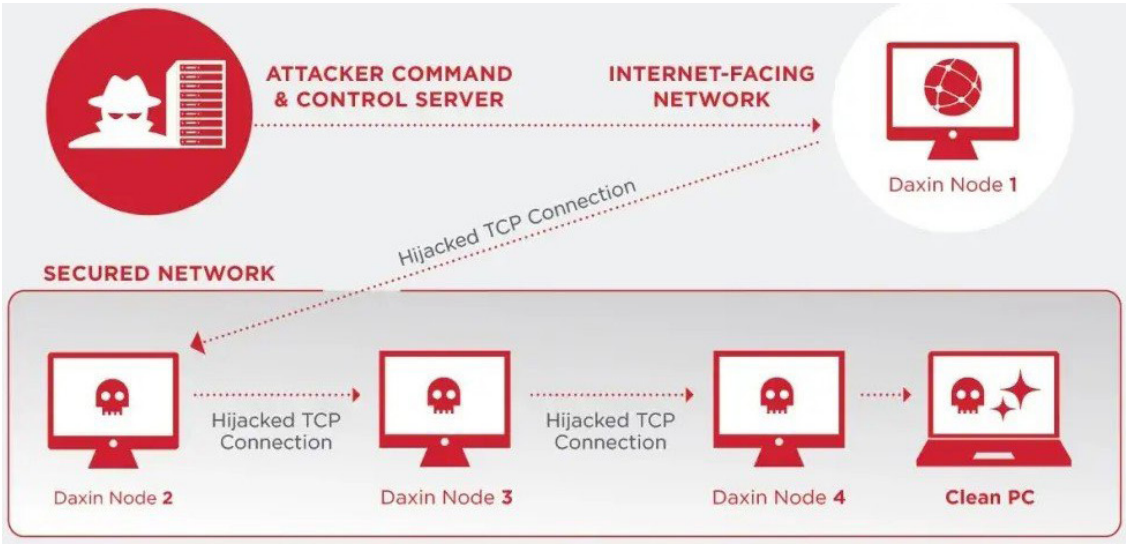
از لحاظ فنی، بدافزار Daxin در قالب یک Kernel Driver سیستم عامل Windows ظاهر می‌شود و عملیات ویژه‌ای برای مخفی نگه داشتن فعالیت‌های مخرب خود انجام می‌دهد.

قابلیت‌های Daxin نشان می‌دهد که تلاش زیادی بر روی طراحی راههای ارتباطی بدافزار صورت گرفته تا با ترافیک عادی شبکه همگن شده و به آسانی شناسایی نشود. بدین منظور، بدافزار هیچ سرویس شبکه جدیدی را فعال نمی‌کند و تنها از سرویس‌های فعال عادی در شبکه سوءاستفاده و بهره‌برداری می‌نماید.

این بدافزار به روش Network Tunneling با سرویس‌های عادی شبکه ارتباط برقرار می‌کند و حتی قادر به راه‌اندازی ارتباط زنجیره‌ای (daisy-chain) برای خود بین چند دستگاه متصل به هم است.

در شبکه‌ای از دستگاههای آلوده، بدافزار Daxin قابلیت Relay دارد و گردانندگان بدافزار می‌توانند با انتخاب هر مسیری در بین دستگاههای آلوده و ارسال یک فرمان، این دستگاهها را وادار به برقراری ارتباط مورد نظر کنند.

این بدافزار می‌تواند ارتباطات TCP/IP را تحت کنترل خود درآورد. بدافزار Daxin ترافیک ورودی TCP را برای داده‌های خاصی رصد می‌کند و هنگامی که این داده‌ها را تشخیص دهد، خود را بجای دریافت کننده واقعی ترافیک جایگزین کرده و کنترل این ارتباط را به دست می‌گیرد. سپس یک تبادل کلید رمزنگاری صورت گرفته و بدین ترتیب، یک کانال ارتباطی رمزگذاری شده و امن برقرار می‌گردد تا از این طریق بدافزار فرامین جدید را دریافت کرده و اطلاعات جمع‌آوری شده را ارسال نماید.



در اختیار گرفتن ارتباطات TCP، قابلیت مخفی‌سازی فوق العاده‌ای به بدافزار Daxin می‌دهد. همچنین امکان برقراری ارتباط در شبکه‌های سازمانی که سیاست‌های امنیتی سختگیرانه‌ای در تجهیزات فایروال تعریف نموده‌اند، را فراهم می‌کند. بعلاوه، در این حالت احتمال شناسایی شدن بدافزار توسط مراکز عملیات امنیت (SOC) که رفتارهای نامتعارف شبکه را همواره رصد می‌کنند، کاهش می‌یابد.

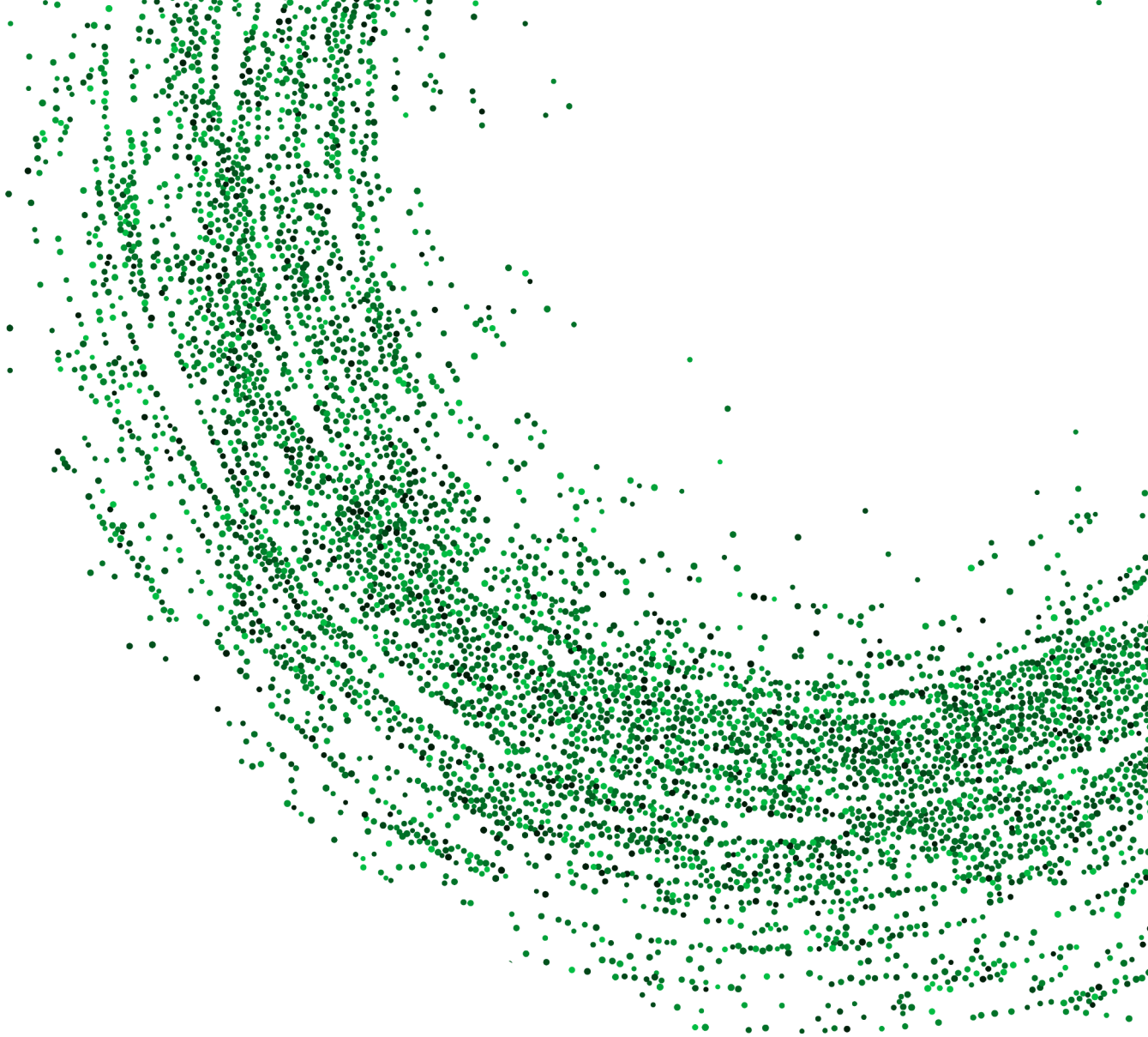
شرکت سیمانتک، به دلیل مشاهده بدافزار Daxin در کنار ابزارهای مخرب دیگر که توسط گروه‌های چینی مورد استفاده قرار می‌گیرند، فعالیت این بدافزار را نیز به این گروه‌ها نسبت داده است. همچنین تاکنون بیشتر قربانیان و اهداف مورد نظر Daxin، سازمانها و دولت‌هایی بوده‌اند که از لحاظ مختلف اقتصادی و سیاسی مورد توجه کشور چین هستند.

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

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/daxin-backdoor-espionage

منبع:

https://threatpost.com/daxin-espionage-backdoor-chinese-malware/178706/



رویدادها و وقایع امنیتی

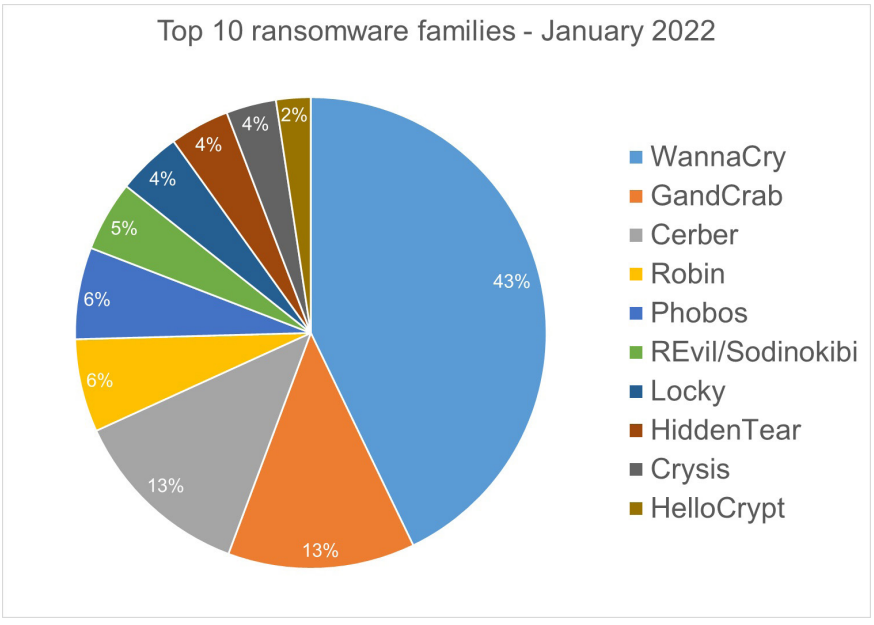
WannaCry؛

همچنان در صدر باج‌افزارهای فعال

نتایج بررسی و تحلیل‌ها حاکی از آن است که باج‌افزار WannaCry که از سال ۲۰۱۷ قربانی می‌گیرد، همچنان تهدیدی جدی و فعال باقی مانده است. در ماه گذشته، آمار شناسایی باج‌افزارهای خانواده WannaCry به مراتب بیشتر از هر باج‌افزار دیگری بوده 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.

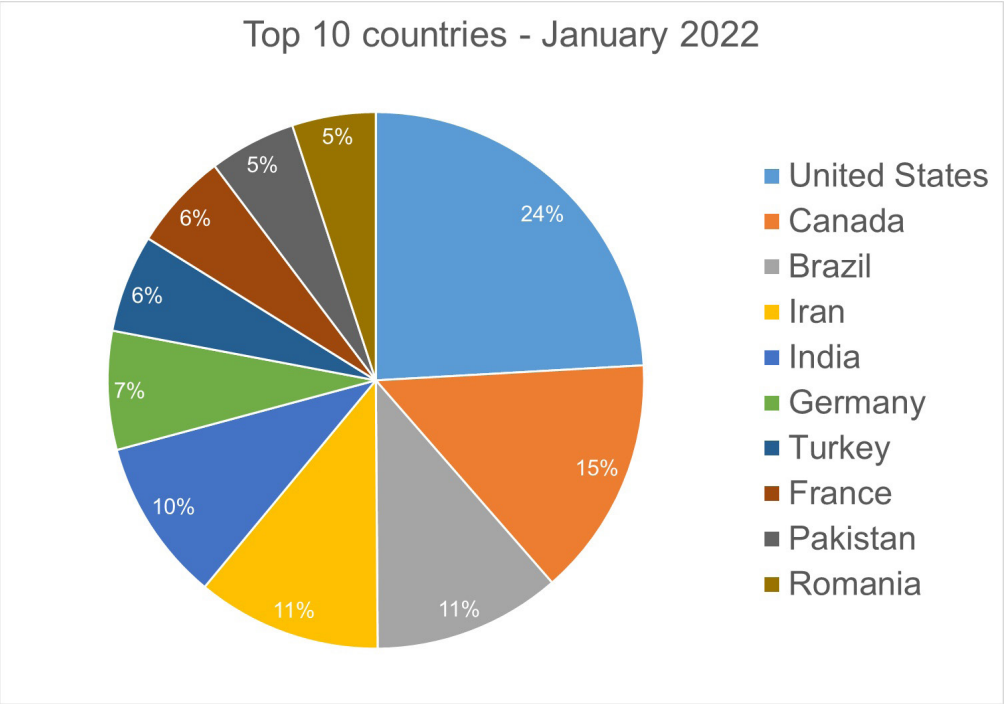
همانطور که در نمودار زیر نشان داده شده است، طبق گزارش جدید شرکت بیت دیفندر، از میان ۱۰.۵ میلیون بدافزار شناسایی شده از ۱۱ دی تا ۱۰ بهمن امسال، ۴۳ درصد آن مربوط به باج‌افزار WannaCry می‌باشد. بعد از آن، GandCrab با ۱۳ درصد در مقام دوم قرار دارد؛ علیرغم اینکه از سال ۲۰۱۹، این باج‌افزار خدمات خود را به عنوان یک باج‌افزار اجاره‌ای (Ransomware-as-a-Service - به اختصار RaaS) متوقف کرده است.



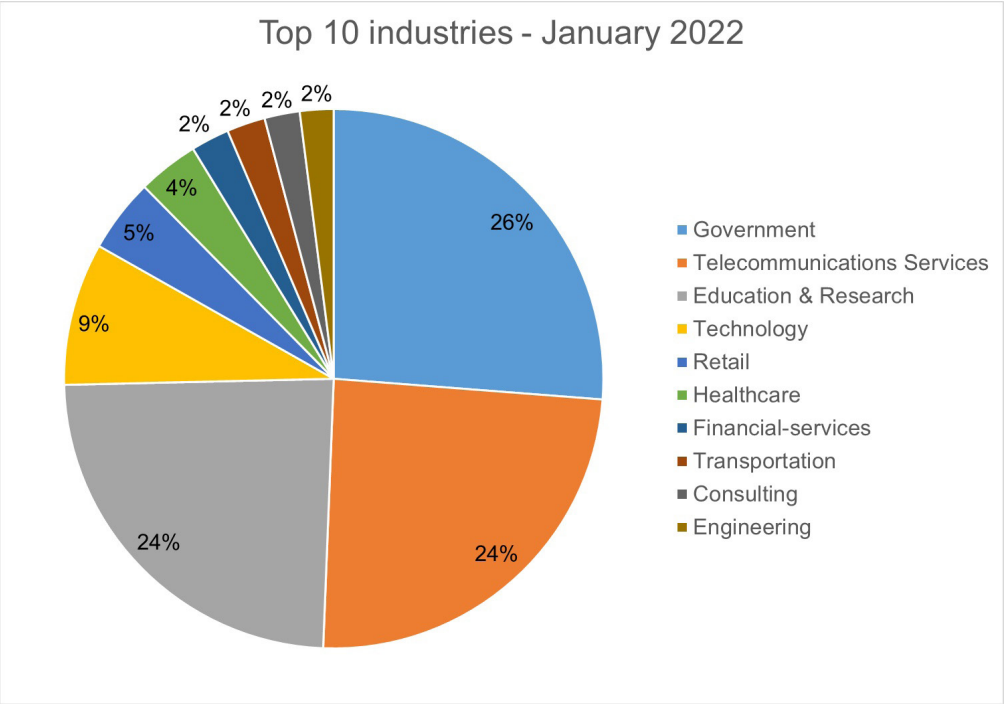
به نقل از شرکت بیت‌دیفندر، باج‌افزاری که در ظاهر فعالیت خود را متوقف کرده ولی همچنان در حال نفوذ و آلوده‌سازی سیستم‌ها می‌باشد، به این معنی است که کارزارهای خودکار آن هرگز متوقف نشده‌اند. البته شناسایی این باج‌افزارهای قدیمی می‌تواند دلایل دیگری هم داشته باشد. از جمله می‌توان به "خطای شناسایی" (False Positive) اشاره کرد. دلیل احتمالی دیگر می‌تواند "ابزارهای رهاشده" یا "abandoware" مانند سایت‌های مخربی که هنوز به طور خودکار نمونه‌های مخرب را منتشر می‌کنند، باشد. دلیل دیگر، باج‌افزارهای جدیدی هستند که از کد باج‌افزارهای قدیمی که احتمالاً از گروه‌های باج‌افزاری دیگر خریده‌اند، استفاده می‌کنند و در نتیجه تحت نام باج‌افزار اولیه و از رده خارج شده، تشخیص داده می شوند.

بیت‌دیفندر در ادامه عنوان نموده که حتی ممکن است یکی از گروه‌های باج‌افزاری رقیب، عملیات باج‌افزار را تحت کنترل خود درآورده و از قربانیان باج‌خواهی می‌کند. یا می‌توان آن را تقصیر گردانندگان باج‌افزار دانست که توقف کسب‌وکار خود را به دروغ اعلام می‌کنند و سپس با نام جدید ولی اغلب با استفاده از کد مشابه (یا بسیار مشابه) به فعالیت خود ادامه می‌دهند.

آمار منتشر شده در گزارش ژانویه شرکت بیت‌دیفندر، نشان می‌دهد که باج‌افزارها در ۱۴۹ کشور مختلف فعال هستند و قربانی می‌گیرند. اما ایالات متحده همچنان منطقه مورد علاقه باج‌افزارها است و ۲۴ درصد از موارد شناسایی شده را به خود اختصاص داده است. کانادا با ۱۵ درصد دومین کشور جهان از لحاظ میزان فعالیت باج‌افزارها است و کشورهای برزیل و ایران، هر یک با ۱۱ درصد در رتبه سوم قرار گرفته‌اند.



در این گزارش، حوزه و بخش‌هایی که بیشتر از بقیه مورد هدف و حمله قرار گرفته‌اند، به شکل زیر دسته‌بندی شده است. در صدر آن، مراکز دولتی با ۲۶ درصد قرار دارد، پس از آن بخش‌های مخابرات با ۲۴ درصد، آموزشی و تحقیقات با ۲۴ درصد و فناوری با ۹ درصد پس از آن قرار دارند.



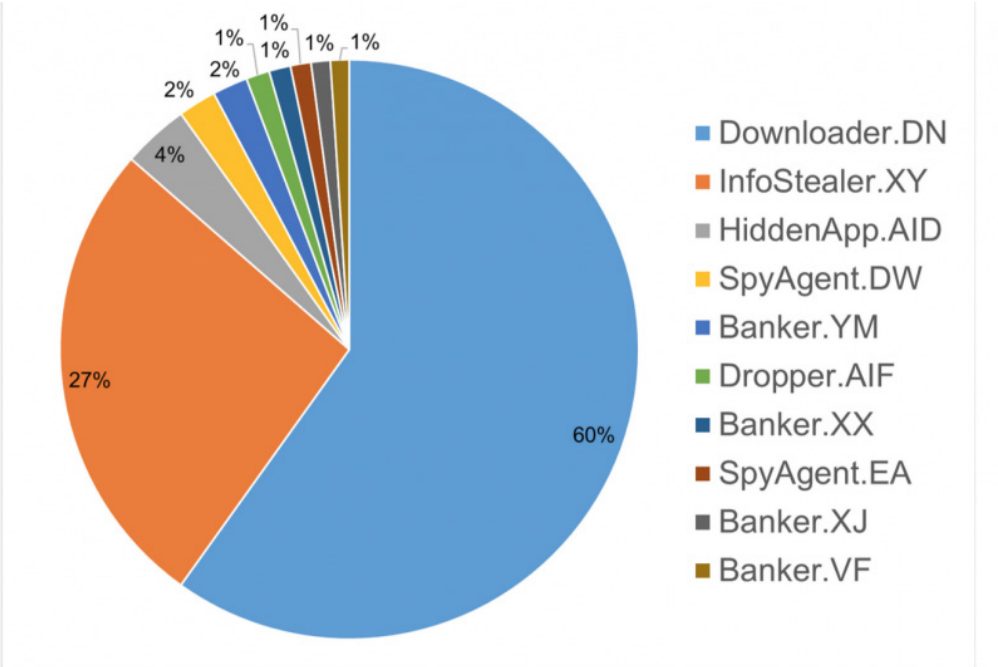
مهاجمان جدید

در ماه ژانویه، Bitdefender Labs دو کارزار بدافزاری جدید که مربوط به دو تروجان بانکداری همراه به نام‌های FluBot و TeaBot بودند را کشف کرد که در یک ماه گذشته اقدام به ارسال بیش از ۱۰۰ هزار پیام کوتاه مخرب جهت توزیع بدافزار نموده‌اند. عملکرد تروجان‌های بانکی ساده است؛ آنها اطلاعات بانکی، اطلاعات تماس، پیامک و سایر داده‌های خصوصی و محرمانه را از دستگاه‌های آلوده سرقت می‌کنند. بر اساس این گزارش، علاقه مهاجمان به بدافزارهای تلفن همراه منطقی است و امروزه دسترسی به معاملات ارزهای دیجیتال و عملیات بانکداری روی دستگاه‌ها و بسترهای تلفن همراه، به هدفی جذاب برای مجرمان سایبری تبدیل شده است.

شرکت کسپرسکی (Kaspersky, Lab.) نیز گزارش جداگانه‌ای را درخصوص بدافزارهای موبایل منتشر نموده و اعلام کرده که تعداد حملات به کاربران تلفن همراه در طول یکسال گذشته روندی کاهشی داشته است. با این حال، به نقل از کسپرسکی، اگرچه تعداد حملات کمتر شده، اما از نظر عملکرد، حملات بدافزاری پیچیده‌تر شده‌اند. در گزارش مذکور به چند نمونه از ترفندهای جدید تروجان‌های بانکی نیز اشاره شده است. در سال ۲۰۲۱، بدافزار Fakecalls که کاربران موبایل در کشور کره جنوبی را مورد هدف قرار می‌دهد، با افزودن پاسخ‌های از پیش ضبط‌شده اپراتور بانک در کد تروجان، ارتقاء پیدا کرده و سعی می‌کرد تا اطلاعات بانکی کاربران را در تماس تلفنی کاربر با بانک سرقت کند. همچنین، بدافزار Sova نیز که اقدام به سرقت کوکی‌ها (cookies) می‌کند، اکنون مهاجمان را قادر می‌سازد تا بدون داشتن اطلاعات اصالت‌سنجی، به ارتباط جاری (Session) و حساب بانکی همراه کاربر، دسترسی داشته باشند.

تروجان‌های اندرویدی

در یک ماه گذشته، فهرست بلند بالایی از تروجان‌های فعال در محیط Android مشاهده و شناسایی شده اند که همگی به دنبال کاربران گوشی‌های همراه با این سیستم عامل هستند. ۱۰ تروجان برتری که سیستم‌های Android را در یک ماه گذشته مورد هدف قرار داده‌اند و میزان فعالیت هر یک از آنها در زیر نمایش داده شده است.



محافظت ضعیف در فروشگاه‌های APP

محققان بیت‌دیفندر اعلام نموده‌اند که با توجه به این که تعداد برنامه‌های کاربردی در App Store مربوط به Apple نزدیک به پنج میلیون است و Google Play نیز نزدیک به سه میلیون برنامه دارد و روز به روز بر این آمار افزوده می‌شود، کنترل آنها به منظور کشف بدافزارها و ابزارهای تبلیغاتی مزاحم، بسیار دشوار می‌باشد زیرا برنامه‌های کاربردی معتبر نیز می‌توانند به دلیل آسیب‌پذیری امنیتی، ناسازگاری نرم‌افزاری یا نقض قوانین حقوقی به تهدیدی جدی تبدیل شوند.

با اینکه برنامه‌های مخرب پس از شناسایی و کشف به سرعت حذف می‌شوند ولی اغلب آنها صدها هزار بار قبل از حذف، توسط کاربران دانلود می‌شوند. یک نمونه از این برنامه‌های مخرب تلفن همراه، Joker است که سال گذشته در فروشگاه Google Play در یک برنامه تلفن همراه به نام Color Message ظاهر شد و بطور شگفت‌انگیزی قبل از اینکه حذف شود، بیش از نیم میلیون بار دانلود شد.

کنترل شدید برنامه‌های کاربردی و وضع مقررات توسط صاحبان فروشگاه‌های مذکور (App Store و Google Play)، حفاظت اولیه برای دستگاه‌های تلفن همراه بشمار می‌آید، اما این امر ناکافی بوده و توسط مقامات دولتی اروپا و ایالات متحده به چالش و سوال کشیده شده است تا بیشتر مورد بررسی و نظارت قرار گیرند.

منابع:

https://threatpost.com/wannacry-gandcrab-top-ransomware-scene/178589/

https://securelist.com/mobile-malware-evolution-2021/105876/

https://businessinsights.bitdefender.com/bitdefender-threat-debrief-february-2022

نقش Telegram
در جنگ روسیه و اکراین

محققان امنیتی اذعان نموده‌اند که در جریان جنگ روسیه و اکراین، مهاجمان سایبری و فعالان اجتماعی هکر (hacktivist) به طور فزاینده‌ای از پیام‌رسان تلگرام (Telegram) برای هماهنگ کردن فعالیت‌های خود، افشای اطلاعات و انتشار اطلاعات نادرست استفاده می‌کنند.

تعداد کاربران تلگرام در گروه‌های مرتبط با جنگ روزانه صد برابر می‌شود و در برخی گروه‌ها به ۲۰۰ هزار نفر در هر گروه رسیده است.

در بین این گروه‌ها، گروه‌های سایبری ضد دولت روسیه برجسته‌تر بوده و از جمله می‌توان به گروه Army IT اشاره کرد که تحت حمایت دولت اوکراین بوده و ۲۷۰ هزار عضو خود را به حملات توزیع شده "از کاراندازی سرویس" (Distributed Denial-of-Service - به اختصار DDoS) علیه نهادهای روسی ترغیب می‌کند.

فعالان اجتماعی نظیر Anna_ و Mark_ نیز که به صورت گروه‌های تلگرامی فعالیت می‌کنند از این پیام‌رسان برای هماهنگ کردن عملیات خود علیه اهداف روسی از طریق حملات توزیع شده "از کاراندازی سرویس" یا حملات پیامکی استفاده می‌نمایند.

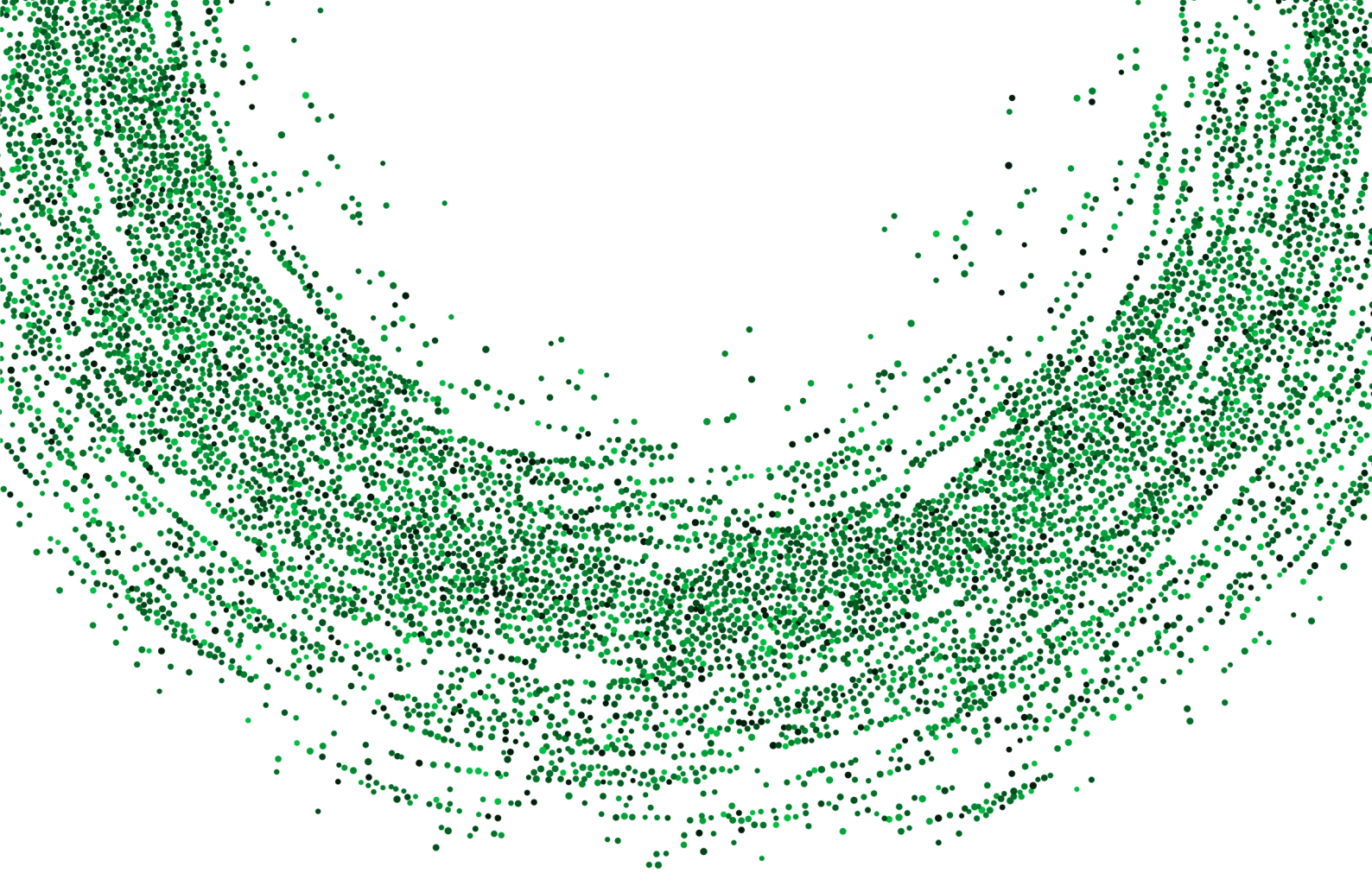
ممکن است تعداد این حملات بسیار بیشتر از آنچه به نظر می‌رسد، باشد و هدف بسیاری از این گروه‌های هکری بیشتر کسب اعتبار برای خود و شهرت برای اوکراین یا روسیه می‌باشد تا آسیب واقعی به کشور مقابل.

به نظر می‌رسد که مجرمان سایبری بیشتر به دنبال کسب امتیاز در این جنگ از طریق گروه‌های تلگرامی، با ده‌ها هزار کاربر، هستند که هدفشان جمع‌آوری کمک‌های مالی برای اوکراین است و از این طریق اقدام به پخش اخبار تایید نشده جهت دور زدن رسانه‌های واقعی می‌کنند.

در این راستا، شرکت تلگرام اعلام نموده که ممکن است با اعمال محدودیت کامل یا نسبی برای کانال‌های خاص، از سوءاستفاده مهاجمان سایبری از این پیام‌رسان جهت "تعمیق درگیری میان روسیه و اکراین" جلوگیری کند.

این پیام‌رسان که بیش از ۵۰۰ میلیون کاربر فعال دارد، در گذشته نیز برای فعالیت‌های بازار سیاه استفاده می‌شده است. در شهریور ۱۴۰۰ نیز در گروه‌هایی با ۳۰۰ هزار عضو، بیش از ۱۰ هزار شرکت اقدام به ارائه گواهی‌های تقلبی واکسن کووید-۱۹ به بیش از ۲۵ کشور با قیمتی بین ۸۵ تا ۲۰۰ دلار نمودند.

افزایش استفاده از تلگرام در درگیری اوکراین و روسیه از چشم بنیانگذار پیام‌رسان Signal نیز دور نمانده است. وی آن را "یک دهه بازاریابی گمراه‌کننده" نامیده که اغلب مردم را با باور اینکه "تلگرام پیام‌رسانی رمزگذاری شده و امن است" فریب داده است. او در توئیت خود اعلام نموده که واقعیت برعکس است و تلگرام به طور پیش‌فرض یک پایگاه داده ابری ساده و آشکار از هر پیامی است که هر کاربر ارسال و دریافت کرده است. هر پیام، عکس، ویدئو، مشخصات تماس، اعضای گروه و فایل‌های ارسال و دریافت شده در ۱۰ سال گذشته، در اختیار هر کسی است که به آن پایگاه داده دسترسی دارد.



آسیب‌پذیری‌ها و اصلاحیه‌های امنیتی

بروزرسانی‌ها و اصلاحیه‌های

اسفند ۱۴۰۰

در اسفند ۱۴۰۰، شرکت‌های مایکروسافت، سیسکو، مک‌آفی‌اینترپرایز، بیت‌دیفندر، ایسِت، اف-سکیور، برودکام، ترند میکرو، وی‌ام‌ور، ادوبی، گوگل، اپل، موزیلا، سوفوس، اس‌ای‌پی، دروپال و اپن-اس‌اس‌ال اقدام به عرضه بروزرسانی 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 اسفند ماه پرداخته شده است.

مایکروسافت

در سه‌شنبه ۱۷ اسفند ۱۴۰۰، شرکت مایکروسافت (Microsoft Corp)، مجموعه اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی مارس منتشر کرد. اصلاحیه‌های مذکور بیش از ۷۰ آسیب‌پذیری را در Windows و محصولات مختلف این شرکت ترمیم می‌کنند. این مجموعه اصلاحیه‌ها، انواع مختلفی از آسیب‌پذیری‌ها را در محصولات 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)

با این حال، بنا بر اظهارات مایکروسافت، تاکنون هیچ یک از این ضعف‌های امنیتی به طور فعال مورد سوءاستفاده قرار نگرفته است.

درجه اهمیت سه مورد از آسیب‌پذیری‌های ترمیم شده این ماه "حیاتی" (Critical) و دیگر 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.

سه مورد از آسیب‌پذیری‌های ترمیم شده این ماه، از نوع "روز-صفر" (شناسه‌های CVE-2022-24459، CVE-2022-21990 و CVE-2022-24512) می‌باشند اما تاکنون هیچ یک از این آسیب‌پذیری‌ها بطور گسترده مورد سوءاستفاده قرار نگرفته‌اند.

مایکروسافت آن دسته از آسیب‌پذیری‌هایی را از نوع روز-صفر می‌داند که پیش‌تر اصلاحیه رسمی برای ترمیم آنها ارائه نشده، جزییات آنها به‌طور عمومی منتشر شده یا در مواقعی مورد سوءاستفاده مهاجمان قرار گرفته است. آسیب‌پذیری‌های "روز-صفر" ترمیم شده در ماه مارس ۲۰۲۲ عبارتند از:

- CVE-2022-21990: آسیب پذیری از نوع "اجرای کد از راه دور" بوده و بر روی Remote Client Desktop تاثیر می‌گذارد و دارای درجه شدت ۸.۸ از ۱۰ (بر طبق استاندارد CVSS) می‌باشد.
- CVE-2022-24459: ضعف امنیتی از نوع "ترفیع اختیارات" بوده و درجه شدت آن ۷.۸ از ۱۰ (بر طبق استاندارد CVSS) می‌باشد و Windows Fax و Scan Service از آن متاثر می‌شوند.
- CVE-2022-24512: آسیب پذیری از نوع "اجرای کد از راه دور" بوده با درجه شدت ۶.۳ از ۱۰ (بر طبق استاندارد CVSS) و .Net و Visual Studio از آن تاثیر می‌پذیرند.

با وجود اینکه که هیچ یک از این آسیب‌پذیری‌ها در حملات مورد سوءاستفاده قرار نگرفته است، مایکروسافت اعلام نموده که نمونه اثبات‌گر (Proof-of-Concept - به اختصار PoC) ضعف‌های امنیتی به شناسه CVE-2022-21990 و CVE-2022-24459 به صورت عمومی منتشر شده است. بنابراین احتمالاً به زودی توسط مهاجمان مورد سوءاستفاده قرار خواهند گرفت.

شایان ذکر است که تعداد وصله‌های با درجه اهمیت "حیاتی" برای ماه مارس ۲۰۲۲ نیز با توجه به تعداد ضعف‌های امنیتی برطرف شده در این ماه همانند ماه قبل به طرز عجیبی کم و تنها سه مورد است. در بروزرسانی و اصلاحیه‌های ماه فوریه ۲۰۲۲، مایکروسافت هیچ یک از آسیب‌پذیری‌های ترمیم شده را بصورت "حیاتی" رتبه‌بندی نکرده بود. فهرست ۳ ضعف امنیتی "حیاتی" ترمیم شده سومین ماه از سال میلادی ۲۰۲۲، که همگی می‌توانند منجر به اجرای کد از راه دور شوند، به شرح زیر است:

- CVE-2022-22006: ضعف امنیتی با درجه شدت ۷.۸ از ۱۰ (بر طبق استاندارد CVSS) که بر HEVC Video Extensions تاثیر می‌گذارد.
- CVE-2022-24501: آسیب‌پذیری که VP9 Video Extensions را متاثر می‌کند و دارای درجه شدت ۷.۸ از ۱۰ (بر طبق استاندارد CVSS) می‌باشد.
- CVE-2022-23277: این ضعف امنیتی دارای درجه شدت ۸.۸ از ۱۰ (بر طبق استاندارد CVSS) می‌باشد و مربوط به Microsoft Exchange Server است.

بهره‌جویی از هر دو ضعف امنیتی مربوط به VIDEO Extensions در HEVC و VP9، به مهندسی اجتماعی نیاز دارد. یک مهاجم با فریب قربانی جهت باز نمودن یک فایل مخرب و دستکاری شده می‌تواند منجر به خرابی سیستم شود. استانداردهای کدنویسی Video Extension جهت فشرده سازی ویدئو بوده و Windows قادر به اجرای آن است تا کاربران بتوانند ویدیوهای با کیفیت بالا را تماشا کنند. از آنجایی که این دو ضعف امنیتی نیاز به دخالت کاربر دارند احتمال سوءاستفاده از آنها کم می‌باشد.

آسیب‌پذیری CVE-2022-24501 که دارای درجه اهمیت "حیاتی" و از نوع "اجرای کد از راه دور" است بر VP9 Video Codec تأثیر می‌گذارد. در واقع این ماه دو ضعف امنیتی در VP9 Video Extension ترمیم شده که هر دو از نوع "اجرای کد از راه دور" است. آسیب‌پذیری دوم، شناسه CVE-2022-24451 و درجه اهمیت "مهم" دارد. هر دو این آسیب‌پذیری‌ها از طریق یک فایل ویدئویی مخرب قابل سوءاستفاده هستند و بروزرسانی هر دو آنها ضروری است.

نکته قابل توجه دیگر درباره آسیب‌پذیری‌های VP9 آن است که اصلاحیه‌های این دو ضعف امنیتی به همراه ۹ اصلاحیه دیگر که مربوط به قالب‌های مختلف گرافیکی و ویدئویی (HEIF, HEVC, raw) می‌شوند، بجای عرضه از طریق سامانه Windows Update، از طریق فروشگاه Microsoft Store ارائه می‌شوند. علاوه بر اینکه سیستم‌های آسیب‌پذیر بطور خودکار بروزرسانی خواهند شد، نحوه دسترسی به این اصلاحیه‌ها در اطلاعیه مایکروسافت هم توضیح داده شده است.

با این حال، آسیب‌پذیری CVE-2022-24501 در VP9 Video Extension از اهمیت بسیاری برخوردار است زیرا VP9 منبع باز و رایگان بوده و توسط مرورگرهای مدرن به جز Internet Explorer پشتیبانی می‌شود، بنابراین ضروری است که کاربران از بروزرسانی آن اطمینان حاصل کنند. ولی کاربران برای بکارگیری HEVC باید آن را خریداری کنند.

آسیب‌پذیری CVE-2022-23277 دارای درجه اهمیت "حیاتی" و از نوع "اجرای کد از راه دور" بوده و Microsoft Exchange Server از آن تاثیر می‌پذیرد. با این که مهاجم جهت بهره‌جویی از این ضعف امنیتی نیاز به احراز هویت دارد، این آسیب‌پذیری دارای پیچیدگی کم بوده و احتمال سوءاستفاده از آن "زیاد" است، بنابراین احتمالاً به زودی شاهد بهره‌جویی گسترده آن در سرورهای Exchange خواهیم بود. این ضعف امنیتی با سوءاستفاده از سرورهای آسیب‌پذیر Exchange می‌تواند به طور بالقوه در حین توسعه آلودگی در شبکه (Lateral Movement) ایمیل‌های تجاری را هک کرده و منجر به سرقت داده‌ها از ایمیل شود. لذا ضروری است با توجه به حملات اخیر به سرورهای Exchange و درجه اهمیت "حیاتی" و ماهیت آسیب‌پذیری آن، سازمان‌ها بروزرسانی آن را در اولویت قرار دهند.

بنا بر اظهارات محققان مایکروسافت، از میان آسیب‌پذیری‌های ترمیم شده ماه مارس ۲۰۲۲، ضعف‌های امنیتی زیر ممکن است بیشتر مورد توجه مهاجمان قرار گیرد.

آسیب‌پذیری با شناسه CVE-2022-24508 که از نوع "اجرای کد از راه دور" است و Windows SMBv3 Client/Server از آن متاثر می‌شود، می‌تواند در Windows 10 نسخه ۲۰۰۴ و نسخه‌های بالاتر مورد سوءاستفاده قرار گیرد.

از آنجایی که این ضعف امنیتی هم بر Client و هم Server تأثیر می‌گذارد، مهاجم می‌تواند از آن جهت توسعه آلودگی در شبکه استفاده کند. این ضعف امنیتی از آنجا ممکن است مورد توجه مهاجمان قرار بگیرد که در هنگام توسعه آلودگی در شبکه در Windows SMB نسخه ۳، قابل اجرا از راه دور است. با وجود اینکه بهره‌جویی موفقیت‌آمیز از آن به اطلاعات اصالت‌سنجی معتبر نیاز دارد، مایکروسافت توصیه هایی در خصوص محدود کردن ترافیک SMB در ارتباطات جانبی و خارجی ارائه می‌دهد. با این که این امر، گامی قوی در پیشگیری و دفاع از شبکه است، مسدود کردن چنین ارتباطاتی می‌تواند تأثیر نامطلوبی بر ابزارهای دیگری که از این اتصالات استفاده می‌کنند، داشته باشد.

با این که این ضعف امنیتی بجای "حیاتی" با درجه اهمیت "مهم" رتبه‌بندی شده است و تاکنون مورد سوءاستفاده قرار نگرفته و نمونه اثبات‌گر آن نیز منتشر نشده است، نحوه بهره‌جویی از آن، این آسیب‌پذیری را به یکی از گزینه‌های احتمالی مهاجمان برای حمله تبدیل کرده و بنابراین باید با اولویت بالایی ترمیم شود.

همچنین سه آسیب‌پذیری از نوع "ترفیع اختیارات" (CVE-2022-23286 در Windows Cloud Files Mini Filter Driver؛ CVE-2022-24507 در Windows Ancillary Function Driver for WinSock و CVE-2022-23299 در Windows PDEV) باید در اولویت بروزرسانی قرار داده شوند زیرا می‌توانند حلقه اتصال در حملات چند مرحله‌ای باشند و احتمال سوءاستفاده از آنها "زیاد" بوده و مورد علاقه مهاجم هستند.

و در نهایت، ضعف امنیتی با شناسه CVE-2022-21967 که در Xbox Live Authentication در سیستم‌عامل Windows وجود دارد و می‌تواند امکان "ترفیع اختیارات" را برای مهاجم فراهم کند. به دلیل منحصر به فرد بودن ممکن است مورد توجه مهاجمان قرار گیرد. به نظر می‌رسد این اولین وصله امنیتی است که به طور خاص Xbox را تحت تاثیر قرار می‌دهد. در سال ۲۰۱۵ توصیه‌نامه‌ای برای افشای سهوی لیسانس Xbox Live ارائه شد، اما به نظر می‌رسد این اولین بروزرسانی امنیتی خاص برای خود این دستگاه باشد.

با توجه به این‌که نمونه اثبات‌گر برخی از ضعف‌های امنیتی این ماه منتشر شده، باید انتظار داشت که مهاجمان این آسیب‌پذیری‌ها را تحلیل نموده و نحوه بهره‌جویی از آنها را بیاموزند، لذا توصیه می‌شود کاربران در اسرع وقت نسبت به بروزرسانی وصله‌ها اقدام نمایند.

فهرست کامل آسیب‌پذیری‌های ترمیم شده توسط مجموعه‌اصلاحیه‌های مارس 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/14608/2055

سیسکو

شرکت سیسکو (Cisco Systems, Inc.) در اسفند ماه در چندین نوبت اقدام به عرضه بروزرسانی‌های امنیتی برای برخی از محصولات خود کرد. این بروزرسانی‌ها، ۱۵ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت سه مورد از آنها "حیاتی"، هشت مورد از آنها از نوع "بالا" (High) و چهار مورد از نوع "متوسط" (Medium) گزارش شده است. آسیب‌پذیری‌هایی همچون "منع سرویس"، "تزریق فرمان" (Command Injection)، "خواندن و نوشتن فایل دلخواه" (Arbitrary File Read and Write)، "افشای اطلاعات" و "ترفیع اختیارات" 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 اینترپرایز

در اسفند ۱۴۰۰، شرکت مک‌آفی اینترپرایز (McAfee Enterprise) اقدام به انتشار نسخ جدید زیر کرد:

- Endpoint Security for Linux 10.7.9
- McAfee Application and Change Control 6.4.19 Linux
- MVISION Endpoint 2202
- MVISION Insights March 2022
- SIEM Enterprise Security Manager 11.5.5
- Web Gateway 11.1.1
- Web Gateway 10.2.7
- Web Gateway 9.2.18

بیت‌دیفندر

شرکت بیت‌دیفندر (Bitdefender) در اسفند ماه دو آسیب‌پذیری CVE-2021-4198 و CVE-2021-4199 را با بروزرسانی خودکار محصولات زیر، ترمیم نمود.

- Total Security versions prior to 26.0.3.29
- Internet Security versions prior to 26.0.3.29
- Antivirus Plus versions prior to 26.0.3.29
- Endpoint Security Tools for Windows versions prior to 7.4.3.146
- Endpoint Security Tools versions prior to 7.2.2.92
- VPN Standalone versions prior to 25.5.0.48

همچنین در ماهی که گذشت شرکت بیت‌دیفندر (Bitdefender) اقدام به انتشار نسخ جدید زیر کرد:

- GravityZone Control Center 6.27.1-5
- Bitdefender Endpoint Security Tools for Linux 7.0.3.1956
- Bitdefender Endpoint Security for Mac 7.4.10.200015
- Security Server Multi-Platform 6.2.6.11319
- Security Server (VMware NSX-T) 1.1.5.11317
- Security Server (VMware NSX-V) 6.2.5.11316

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

ایسِت

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

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

اف-سکیور

شرکت ضدویروس اف-سکیور (F-secure, Corp.) با انتشار بروزرسانی ۲۰۲۲-۰۲-۲۳_۰۱ آسیب‌پذیری CVE-2021-44747 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. اطلاعات کامل در این خصوص در لینک زیر قابل دسترس است:

https://www.f-secure.com/en/business/support-and-downloads/security-advisories/cve-2021-44747

همچنین آسیب‌پذیری CVE-2021-44750 در ابزار خطایابی Support Tool (fsdiag) که در محصولات گوناگون این شرکت وجود دارد، با ارایه اصلاحیه فوری ترمیم شده است. اطلاعات کامل در این خصوص در لینک زیر قابل دسترس است:

https://www.f-secure.com/en/business/support-and-downloads/security-advisories/cve-2021-44750

این شرکت با انتشار بروزرسانی ۱۸ فوریه آسیب‌پذیری‌های CVE-2021-44749 و CVE-2021-44748 با درجه اهمیت متوسط را در محصول SAFE for Android برطرف نمود. اطلاعات کامل در خصوص آسیب‌پذیری‌های مذکور در لینک زیر قابل دسترس است:

https://www.f-secure.com/en/business/support-and-downloads/security-advisories/cve-2021-44748

https://www.f-secure.com/en/business/support-and-downloads/security-advisories/cve-2021-44749

برودکام

شرکت برودکام (Broadcom, Inc.) با عرضه اصلاحیه‌ای با درجه اهمیت "بالا" یک آسیب‌پذیری از نوع ارتقای سطح دسترسی را در محصول Symantec Management Agent ترمیم کرده است. جزییات کامل در خصوص آسیب‌پذیری ترمیم شده در لینک زیر قابل دریافت و مطالعه است:

https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/20366

ترند میکرو

شرکت ترند میکرو (Trend Micro, Inc.) با عرضه اصلاحیه حیاتی در ۲۲ فوریه سه آسیب‌پذیری CVE-2022-25329 و CVE-2022-25330 و CVE-2022-25331 را ترمیم کرده است. همچنین این شرکت با انتشار نسخه Antivirus for Mac 11.0.2184 آسیب‌پذیری CVE-2022-24671 از نوع ارتقای سطح دسترسی را ترمیم نمود. جزییات کامل در خصوص آسیب‌پذیری‌های مذکور در لینک زیر قابل دریافت و مطالعه است:

https://success.trendmicro.com/dcx/s/solution/000290507?language=en_US

https://helpcenter.trendmicro.com/en-us/article/TMKA-10937

وی‌ام‌ور

در ماه گذشته، شرکت وی‌ام‌ور (VMware, Inc.) با انتشار توصیه‌نامه‌های امنیتی، نسبت به ترمیم ضعف‌های امنیتی با شناسه‌های CVE-2022-22943، CVE-2022-22944 و CVE-2022-22945 در محصولات زیر اقدام کرد:

- VMware Cloud Foundation (Cloud Foundation)
- VMware NSX Data Center for vSphere (NSX-V)
- VMware Workspace ONE Boxer
- VMware Tools for Windows

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.) در ۱۷ اسفند ماه مجموعه اصلاحیه‌های امنیتی ماه مارس ۲۰۲۲ را منتشر کرد. اصلاحیه‌های مذکور، در مجموع شش آسیب‌پذیری را در سه محصول زیر ترمیم می‌کنند:

- Adobe Illustrator
- Adobe Photoshop
- Adobe After Effects

درجه اهمیت پنج مورد از آسیب‌پذیری‌های ترمیم شده این ماه "حیاتی" و یک مورد دیگر "مهم" اعلام شده است.

بیشترین آسیب‌پذیری ترمیم شده این ماه ادوبی، مرتبط با Adobe After Effects با چهار مورد بوده است. هر چهار ضعف امنیتی برطرف شده در این نرم‌افزار دارای درجه اهمیت "حیاتی" بوده و از نوع "اجرای کد از راه دور" (Arbitrary Code Execution) می‌باشند.

ادوبی در بروزرسانی ماه مارس ۲۰۲۲، یک ضعف امنیتی با درجه اهمیت "حیاتی" از نوع "اجرای کد" که منجر به سرریز حافظه (Buffer Overflow) می‌شود را در Illustrator ترمیم نموده است.

در نهایت، وصله ارائه شده برای Photoshop نیز تنها یک ضعف امنیتی با درجه اهمیت "مهم" را که از نوع "نشت حافظه" (Memory Leak) می‌باشد، رفع می‌کند.

اگر چه موردی مبنی بر سوءاستفاده از آسیب‌پذیری‌های ترمیم شده تا ۱۷ اسفند گزارش نشده، ادوبی به مشتریان خود توصیه می‌کند که در اسرع وقت اقدام به نصب بروزرسانی‌ها کنند. اطلاعات بیشتر در خصوص مجموعه اصلاحیه‌های ماه مارس ۲۰۲۲ ادوبی در لینک زیر قابل مطالعه است:

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

گـوگـل

شرکت گوگل (Google, LLC) در اسفند ماه، در چندین نوبت اقدام به ترمیم آسیب‌پذیری‌های امنیتی مرورگرChrome کرد. آخرین نسخه این مرورگر که در ۲۴ اسفند ماه انتشار یافت، نسخه ۹۹.۰.۴۸۴۴.۷۴ است. فهرست اشکالات مرتفع شده در لینک زیر قابل دریافت و مشاهده است:

https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop_15.html

اپـــل

در اسفند ماه، شرکت اپل (Apple, Inc.) با انتشار بروزرسانی، ضعف‌های امنیتی متعددی را در چندین محصول خود از جمله iTunes، macOS Monterey، macOS Big Sur، Security Update Catalina، Safari، tvOS، watchOS، iPadOS، iOS، Logic Pro، Xcode و GarageBand 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 مرورگرهای Focus، Firefox، نرم‌افزار مدیریت ایمیل Thunderbird و Mozilla VPN برطرف کرد. اصلاحیه‌های مذکور، در مجموع ۱۱ آسیب‌پذیری را در محصولات مذکور ترمیم می‌کنند. درجه حساسیت دو مورد از آنها "حیاتی"، پنج مورد از آنها "بالا"، سه مورد "متوسط" و یک 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/

سـوفـوس

شرکت سوفوس (Sophos, Ltd.) در اسفند ماه نسخه SG UTM 9.709 را منتشر کرده است. طبق روال همیشگی، نسخه جدید در چند مرحله عرضه خواهد شد.

- در مرحله اول می‌توانید بسته بروزرسانی را از سرور سوفوس به نشانی زیر دانلود کنید. پس از ورود به نشانی زیر، به پوشه UTM / v9 / up2date بروید.

https://download.astaro.com/#UTM/

- Up2date package - ۹.۷۰۸ to 9.709:

https://download.astaro.com/UTM/v9/up2date/u2d-sys-9.708006-709003.tgz.gpg

- md5 sum is d11a09401290cb1c9b475dfc22e82bc0:

https://download.astaro.com/UTM/v9/up2date/u2d-sys-9.708006-709003.tgz.gpg.md5

- در مرحله دوم، شرکت سوفوس بسته بروزرسانی را از طریق سرورهای Up2Date خود برای بعضی مدل‌هایUTM، در دسترس قرار خواهد داد.
- در مرحله سوم، شرکت سوفوس بسته بروزرسانی را از طریق سرورهای Up2Date خود برای تمام مدل‌هایUTM، در دسترس قرار خواهد داد.

جزئیات نسخه جدید ۹.۷۰۹ و فهرست اشکالات ترمیم شده در نشانی‌های زیر قابل دریافت و مطالعه می‌باشد.

https://community.sophos.com/utm-firewall/b/blog/posts/utm-up2date-9-709-released

https://newsroom.shabakeh.net/23539/utm-up2date-9-709-released.html

اس‌ای‌پی

اس‌ای‌پی (SAP SE) نیز در ۱۷ اسفند ۱۴۰۰ با انتشار مجموعه‌اصلاحیه‌هایی، ۱۸ آسیب‌پذیری را در چندین محصول خود برطرف کرد. شدت شش مورد از این ضعف‌های امنیتی ۱۰ از ۱۰ و یک مورد ۹.۳ از ۱۰ (بر طبق استاندارد CVSS) گزارش شده است. توصیه می‌شود با مراجعه به نشانی زیر، بروزرسانی مربوطه هر چه سریع‌تر اعمال شود:

https://dam.sap.com/mac/app/e/pdf/preview/embed/ucQrx6G?ltr=a&rc=10

دروپـال

۲۵ اسفند ماه، جامعه دروپال (Drupal Community) با عرضه بروزرسانی‌های امنیتی، ضعف‌های امنیتی با شناسه‌های CVE-2022-24728 و CVE-2022-24729 را اصلاح کرد. سوءاستفاده از بعضی از این آسیب‌پذیری‌ها مهاجم را قادر به در اختیار گرفتن کنترل سامانه می‌کند. توضیحات کامل در این خصوص در نشانی زیر قابل دسترس است.

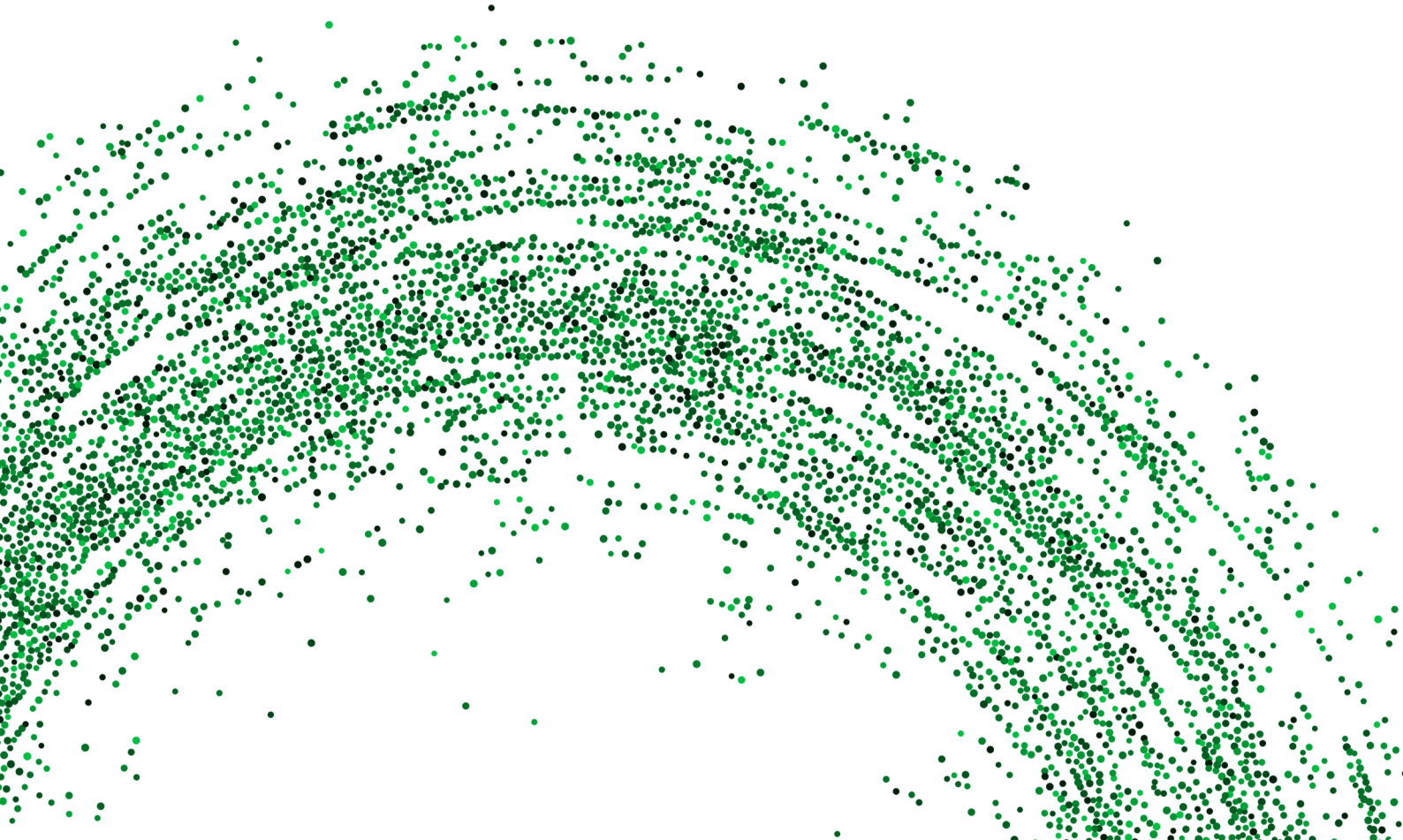
https://www.drupal.org/sa-core-2022-005

اپن-اس‌اس‌ال

۲۴ اسفند ماه، بنیاد اپن-اس‌اس‌ال (OpenSSL Foundation, Inc.) با عرضه بروزرسانی‌های امنیتی، ضعف‌های امنیتی متعددی را در نسخه‌های ۱.۰.۲، ۱.۱.۱ و ۳.۰ نرم‌افزار OpenSSL ترمیم نموده است. با نصب این بروزرسانی، نسخه نرم‌افزار OpenSSL نگارش ۱.۰.۲ به ۱.۰.۲zd، نگارش ۱.۱.۱ به ۱.۱.۱n و نگارش ۳.۰ به ۳.۰.۲ تغییر خواهند کرد. سوءاستفاده از بعضی از این آسیب‌پذیری‌ها مهاجم را قادر به "از کاراندازی سرویس" می‌کند. از این رو توصیه می‌شود که راهبران امنیتی در اولین فرصت نسبت به ارتقاء این نرم‌افزار اقدام کنند. توضیحات کامل در این خصوص در نشانی زیر قابل دسترس است.

https://www.openssl.org/news/secadv/20220315.txt

گزارش‌ها



گزارش فصلی مک‌آفی
منتشر شد

به شماره جدید گزارش Advanced Threat Research و به شرکت جدید Trellix خوش آمدید!

این اولین گزارش فصلی Advanced Threat Research است که تحت نام شرکت جدید Trellix منتشر می‌شود. شرکت Trellix از ادغام دو شرکت بزرگ امنیتی McAfee و FireEye تشکیل شده است.

اکنون که سال میلادی جدید ۲۰۲۲ را آغاز کرده ایم، مروری بر روند تهدیدات سایبری در یکسال گذشته و به ویژه ماههای پایانی سال ۲۰۲۱ خواهیم داشت.

در ماههای پایانی سال ۲۰۲۱، نقطه ضعف Log4j نه تنها عناوین اخبار را تحت الشعاع قرار داد، بلکه توان واکنش گروه‌های امنیتی را به چالش کشید. Log4j به عنوان حادترین ضعف امنیتی دهه‌های اخیر توصیف شده است. هر محصولی که کتابخانه Log4j را بکار گرفته بود، تحت تاثیر این ضعف امنیتی قرار داشت، از برنامه های کاربردی سازمانها تا خدمات ابری شرکتهای بزرگ بین المللی. گزارش مشروحی از این نقطه ضعف در این شماره ارائه شده است.

در اواخر سال ۲۰۲۱، برخی گروه‌های گرداننده باج افزار متلاشی شدند، دوباره فعال شدند، تغییر نام دادند و یا سرمایه جدید برای توسعه جذب کردند ولی در هر حال، همچنان یک تهدید رایج و مخرب علیه کاربران و سازمان‌های مختلف باقی مانده‌اند.

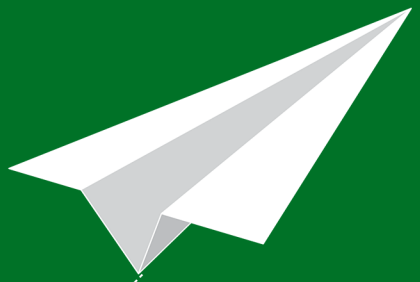
کارزارهای مرتبط با "تهدیدات مستمر و پیشرفته" (Advanced Persistent Threat - به اختصار APT) که در شش ماه گذشته فعال بوده و با روش‌ها و ابزارهای مختلف، هر کدام کشورها و کاربران خاصی را در جهان مورد هدف قرار داده‌اند، مورد بررسی و تحقیق قرار گرفته‌اند.

در این گزارش به روش مخرب "کسب روزی از زمین" (Living off the Land - به اختصار LotL) پرداخته شده و آمار مفیدی ارائه گردیده است. در روش LotL مجرمان سایبری از توابع و برنامه‌های عادی و سالم در سیستم قربانی برای انجام عملیات مخرب خود بر روی آن سیستم استفاده می‌کنند. این روش برای مخفی ماندن عملیات مخرب و شناسایی نشدن حملات بسیار موثر است.

همچنین در بخشی از این گزارش به نقاط ضعف کشف شده که از سوی تولیدکنندگان و سازندگان انواع محصولات اعلام و اصلاحیه‌هایی برای ترمیم آنها منتشر کرده‌اند، پرداخته شده ولی فارغ از درجه‌بندی رسمی (نظیر درجه CVSS و یا رتبه OWASP)، این نقاط ضعف فقط بر اساس تجربه و شناخت کارشناسان Trellix برای شما اولویت‌بندی و توضیح داده شده‌اند.

در پایان گزارش نیز انواع تهدیدات سایبری بر اساس نوع بدافزار، منطقه فعالیت، نوع قربانیان و روش‌های بکار گرفته شده، دسته‌بندی و میزان فراوانی هر یک با نمودارهای رنگین نمایش داده شده‌اند.

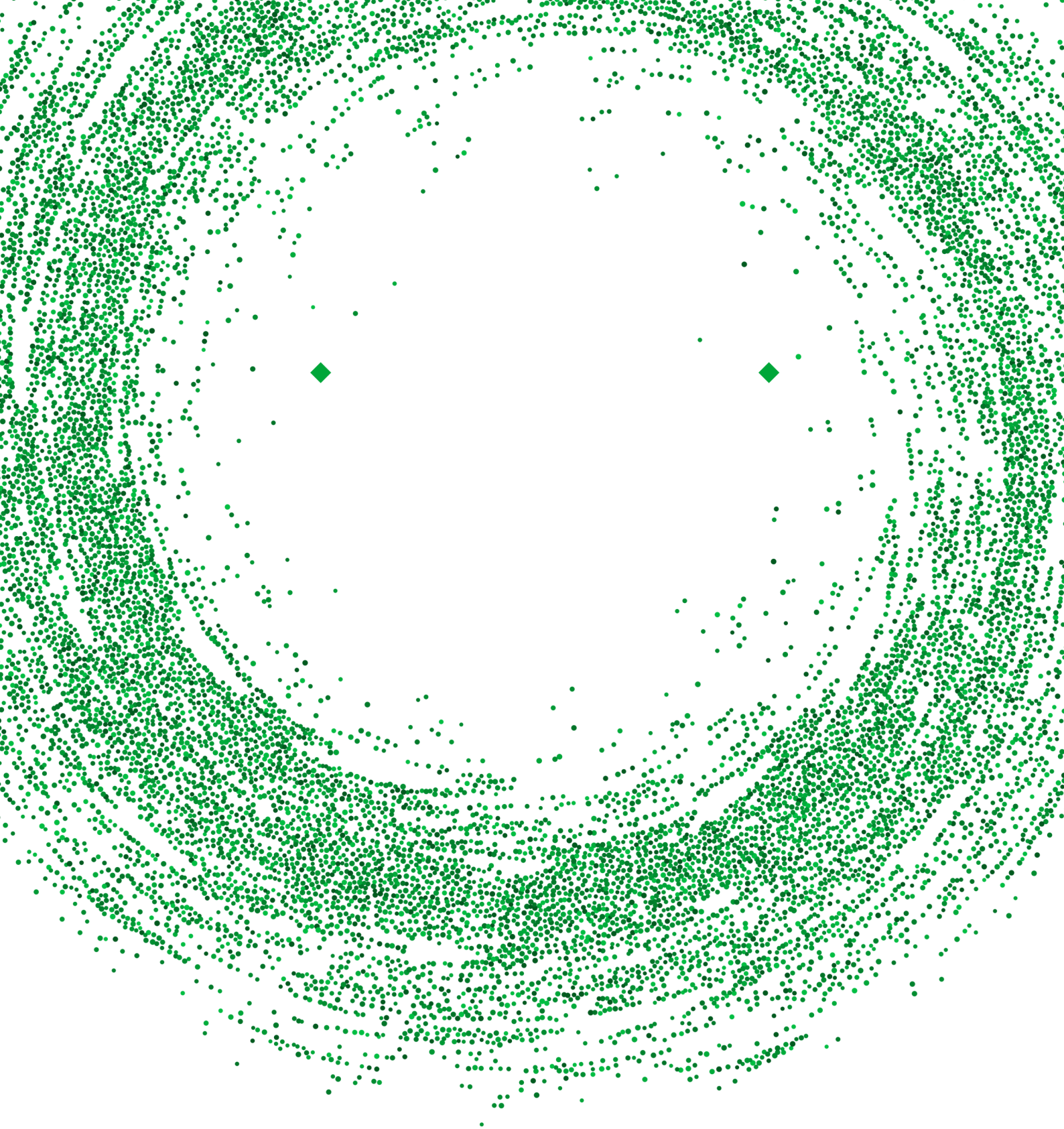
برای دریافت اولین گزارش ماهانه Advanced Threat Research شرکت جدید Trellix بر روی تصویر زیر کلیک کنید.



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