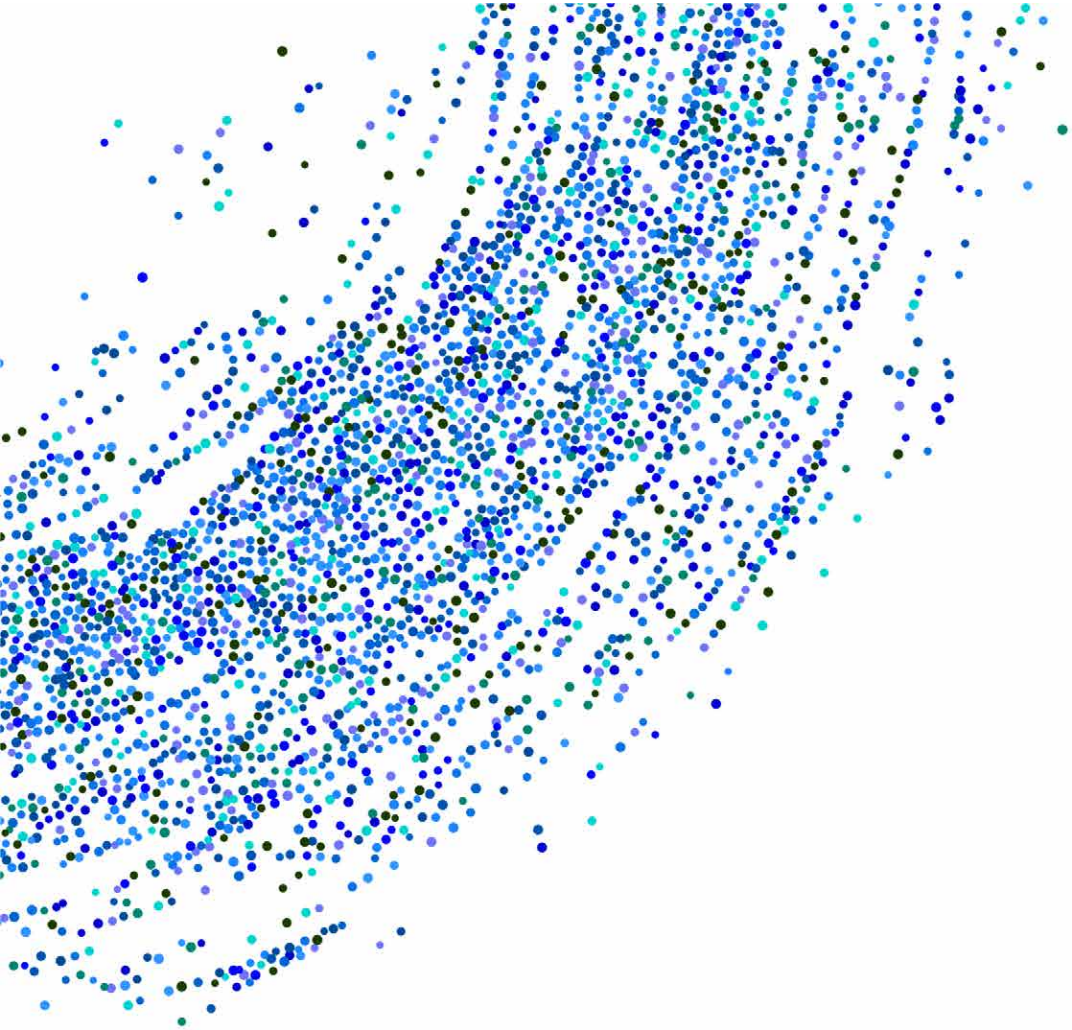
شبکه گستر

امنیت شما | وظیفه ما

ماهنامه
امنیت فناوری اطلاعات

شرکت مهندسی شبکه گستر | سال دوازدهم | بهمن ۱۴۰۱

فهرست مطالب



چکیده مدیریتی

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

در ماهی که گذشت شرکت بیت‌دیفندر، جزییات کارزاری را منتشر کرد که در جریان آن، مهاجمان از طریق نسخه‌ای مخرب از یک برنامه VPN اقدام به آلوده‌سازی دستگاه کاربران به جاسوس‌افزار EyeSpy می‌کنند. به گفته بیت‌دیفندر، ایران، بیشترین سهم از قربانیان این کارزار اخیر EyeSpy را داشته است. جزییات بیشتر در خصوص این جاسوس‌افزار را در این ماهنامه بخوانید.

در این ماهنامه، چکیده‌ای از گزارش فصلی ترلیکس (Trellix) که در آن به بررسی تهدیدات سایبری در سه‌ماهه سوم ۲۰۲۲ پرداخته شده ارائه شده است. دو شرکت مک‌آفی اینترپرایز (McAfee Enterprise) و فایرآی (FireEye) به‌عنوان دو قدرت امنیت فناوری اطلاعات در اواخر سال گذشته تحت برند ترلیکس با یکدیگر ادغام شدند. این اولین گزارش فصلی ترلیکس است که توسط مرکز تحقیقات پیشرفته این شرکت (Trellix Advanced Research Center) ارائه می‌شود.

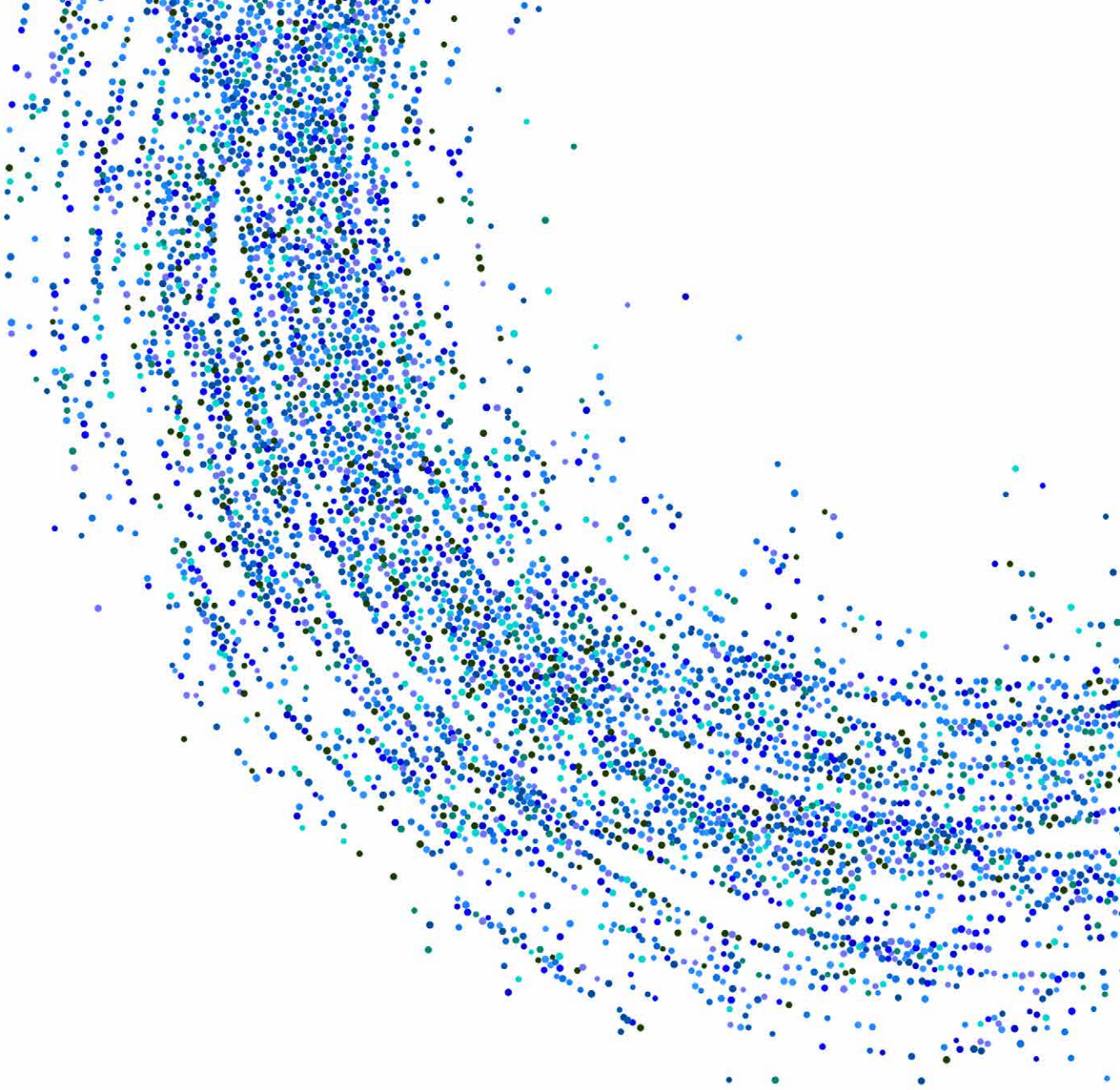
دی ۱۴۰۱ آخرین ماهی بود که شرکت مایکروسافت اقدام به عرضه اصلاحیه امنیتی برای Windows 7 کرد و من‌بعد، این سیستم عامل، به‌روزرسانی‌ها و اصلاحیه‌های امنیتی را برای وصله آسیب‌پذیری‌ها دریافت نخواهد کرد. علاوه بر این، Windows 8.1 نیز که برای اولین بار ۹ سال پیش ارائه شد، از ۲۰ دی ۱۴۰۱ دیگر توسط مایکروسافت پشتیبانی نمی‌شود. جزییات بیشتر را در این ماهنامه بخوانید.

در پی تصمیم شرکت مایکروسافت در خصوص مسدودسازی ماکروها در فایل‌هایی که از اینترنت دریافت می‌شوند، اکنون مدتی است که مهاجمان از روش‌های جایگزین نظیر افزونه‌های مخرب Excel برای انتشار بدافزارهای خود استفاده می‌کنند. بر اساس گزارشی که شرکت سیسکو آن را منتشر کرده، مهاجمان به طور فزاینده‌ای از افزونه‌های (Add-in) نرم‌افزار Excel در قالب فایل‌های XLL به عنوان بردار نفوذ اولیه جهت آلوده‌سازی سیستم‌های کاربران و رخنه به سازمان‌ها استفاده می‌کنند. پیش‌تر نیز شرکت پالو آلتو نتورکس از بهره‌جویی از فایل‌های XLL جهت توزیع بدافزارهای Agent Tesla و Dridex خبر داده بود که همگی بیانگر استقبال فزاینده مهاجمان از این تکنیک جدید است. خلاصه‌ای از گزارش سیسکو را در این ماهنامه بخوانید.

در دی ماه، شرکت بیت‌دیفندر گزارشی را منتشر کرد که بر طبق آن، ایران، بعد از آمریکا و برزیل، در جایگاه سوم کشورهای با بیشترین تعداد شناسایی باج‌افزار قرار گرفته است. دو باج‌افزار WannaCry و GandCrab نیز همان طور که در این ماهنامه خواهید خواند بیشترین انتشار را در مقایسه با سایر باج‌افزارها داشته‌اند.

طبق معمول هر ماه، در دی ۱۴۰۱ نیز شرکت‌های مختلف فناوری اطلاعات اقدام به انتشار اصلاحیه و توصیه‌نامه امنیتی برای برخی از محصولات خود کردند. جزییات اصلاحیه‌های عرضه‌شده از سوی شرکت‌های مایکروسافت، سیسکو، ترلیکس، فورتی‌نت، بیت‌دیفندر، گوگل، ادوبی، جونیپر نت‌ورکز، بنیاد موزیلا و جامعه دروپال را می‌توانید در این ماهنامه بخوانید. همچنین به توصیه‌نامه منتشر شده توسط شرکت فورتی‌نت که نسبت به بهره‌جویی فعال مهاجمان از ضعفی در FortiOS SSL-VPN هشدار داده، اشاره خواهیم کرد. این ضعف امنیتی مهاجمان احراز هویت نشده را قادر می‌سازد تا کد مخرب و دلخواه را به طور بالقوه و از راه دور در تجهیزات آسیب‌پذیر اجرا کنند.

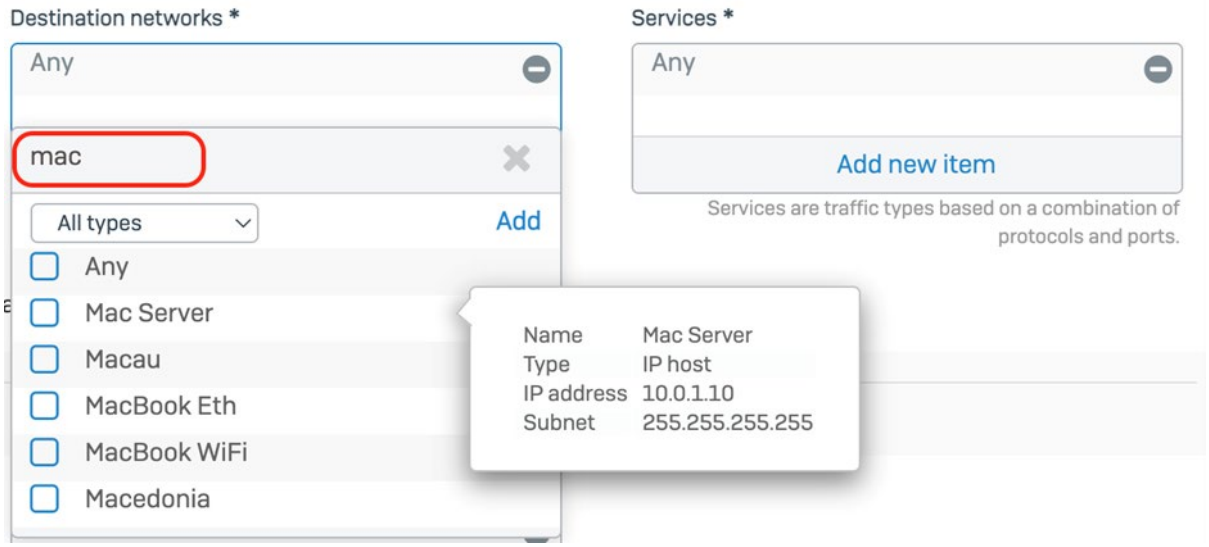
شرکت مهندسی شبکه گستر، ارائه‌دهنده محصولات و خدمات در زمینه امنیت شبکه از زمان تأسیس در سال ۱۳۷۰، همواره به امر آگاه‌سازی در زمینه امنیت فناوری اطلاعات به عنوان یکی از اصلی‌ترین راهکارهای مقابله با تهدیدات سایبری توجه خاص داشته است. امید است مطالب ماهنامه امنیت فناوری اطلاعات شرکت مهندسی شبکه گستر که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



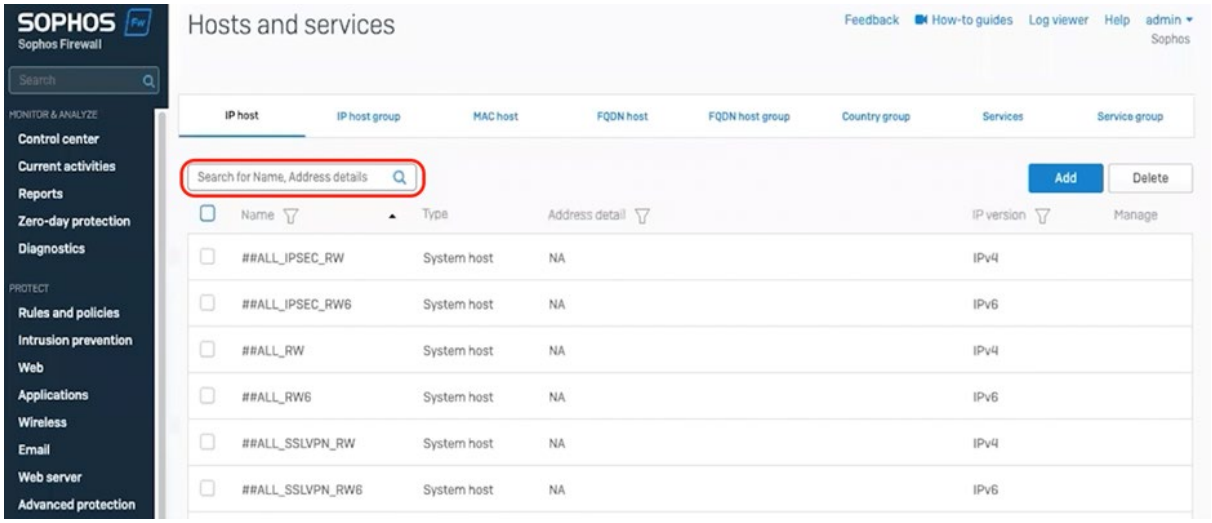
رویدادها و وقایع امنیتی

قابلیت جدید جستجو
در Sophos Firewall v19.5

همان‌طور که پیش‌تر نیز در این خبر اشاره شد در نسخه v19.5، امکانات جدیدی به قابلیت جستجو در Sophos Firewall افزوده شده است. از جمله آنها، امکان جستجوی هر نوع تنظیم یا پیکربندی در سیستم است. ضمن آن که در نسخه مذکور امکان جستجوی آبجکت‌های شبکه در حین ساخت قواعد فایروال، بهبود چشم‌گیری یافته است.



در Sophos Firewall v19.5 شما قادر خواهید بود تا هر آبجکتی را در فهرست هاست‌ها و سرویس‌ها بر اساس نام یا مقدار در نوار جستجوی بالای صفحه جستجو کنید.



این قابلیت‌های جدید یافتن هر آن چه را که در جستجوی آن هستید بسیار آسان کرده و احتمال ساخت مجدد یک آبجکت موجود را کاهش می‌دهد.

لازم به ذکر است که Sophos Firewall v19.5 حاوی انبوهی از قابلیت‌های باارزش جدید است؛ فهرست کامل آنها در لینک زیر قابل مطالعه است:

https://community.sophos.com/sophos-xg-firewall/sfos-v19-5-early-access-program/m/files/9529/download

همچنین چکیده‌ای از امکانات افزوده شده در Sophos Firewall v19.5 در لینک زیر قابل دسترس است:

https://newsroom.shabakeh.net/26281/sophos-firewall-v19-5-is-now-available.html

امکان ارتقای از فرم‌ورهای با نسخه v18.5 و v19 به v19.5 EAP1 فراهم می‌باشد.

شماره تلفن ۴۲۰۵۲ در ساعات اداری و سامانه خدمات پس از فروش و پشتیبانی شرکت مهندسی شبکه گستر به نشانی my.shabakeh.net در طول شبانه روز در اختیار مشترکین گرامی است تا مشکلات و مسائل خود را مطرح کرده و پاسخ‌ها و راهنمایی‌های لازم را دریافت نمایند.

ابزار رمزگشای رایگان
برای باج‌افزار MegaCortex

محققان شرکت ضدویروس بیت‌دیفندر (Bitdefender) موفق به ساخت ابزاری شده‌اند که قربانیان MegaCortex را قادر به رمزگشایی رایگان فایل‌های رمز شده توسط این باج‌افزار می‌کند.

عرضه رمزگشای جدید حاصل مشارکت بیت‌دیفندر، پلیس اروپا (یوروپل)، پروژه No More Ransom و نهادهای قانونی زوریخ می‌باشد.

MegaCortex چیست؟

باج‌افزار MegaCortex برای اولین بار توسط محققان سوفوس (Sophos) در اردیبهشت سال ۱۳۹۸ شناسایی شد.

به گزارش شرکت مهندسی شبکه گستر، MegaCortex باج‌افزاری است که در جریان حملاتی هدفمند از طریق درب‌پشتی (Backdoor) ایجاد شده توسط بدافزارهایی همچون Emotet به دستگاه راه می‌یابد. MegaCortex پس از آلوده کردن نخستین دستگاه در شبکه سازمان، خود را از طریق بسته‌های بهره‌جو (Exploit Kit) یا با بهره‌گیری از بستر Active Directory بر روی سایر سیستم‌های درون شبکه توزیع می‌کند.

نسخه‌ای از باج‌افزار MegaCortex که در خرداد ۱۳۹۸ شناسایی شد، نشان داد که گردانندگان آن حملات هدفمندتری را انجام می‌دهند، باج‌خواهی را با توجه به مقیاس سازمان و قربانی تنظیم نموده و از زبان تهدیدآمیزی نیز استفاده می‌کنند.

در آبان ۱۳۹۸، مهاجمان MegaCortex از تاکتیک‌های اخاذی مضاعف استفاده کردند و قربانیان را تهدید نمودند که در صورت عدم پرداخت باج مطالبه شده، اطلاعات آنها را منتشر خواهند کرد. در پایان آن ماه، مرکز ملی امنیت سایبری هلند، MegaCortex را در میان فعال‌ترین باج‌افزارها در جرایم سایبری زیرزمینی قرار داد.

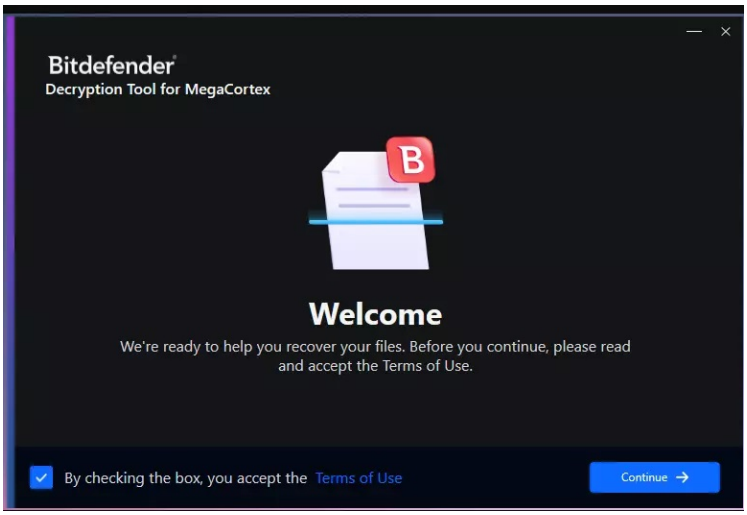
در طول سال ۲۰۲۰، فعالیت این باج‌افزار کاهش یافت و قربانیان زیادی تحت تأثیر آن قرار نگرفتند.

در مهر ۱۴۰۰، یوروپل از دستگیری ۱۲ فرد مسئول در ۱۸۰۰ حمله باج‌افزاری در ۷۱ کشور خبر داد که بسیاری از آنها از باج‌افزارهای MegaCortex و LockerGoga استفاده می‌کردند.

این دستگیری در نهایت منجر به انتشار رمزگشای باج‌افزار رایگان LockerGoga توسط بیت‌دیفندر شد.

داده‌های خود را رمزگشایی کنید

این ابزار رمزگشا یک فایل اجرایی مستقل است که نیازی به نصب ندارد و امکان یافتن خودکار فایل‌های رمزگذاری شده در سیستم را فراهم می‌کند؛ از این رو استفاده از آن بسیار ساده است.



همچنین این ابزار رمزگشا می‌تواند از فایل‌های رمزگذاری‌شده، نسخه پشتیبان تهیه کند تا در صورت ایجاد مشکل در پروسه رمزگشایی، فایل‌ها هنگام بازیابی خراب نشوند.

این ابزار برای قربانیانی که قبلاً سعی در رمزگشایی فایل‌های خود داشته‌اند، تنظیمات پیشرفته‌ای را ارائه داده که آنها را با فایل‌های جدید رمزگشایی شده، جایگزین می‌نماید.

ابزار رمزگشایی بیت‌دیفندر برای باج‌افزار MegaCortex از مسیر زیر قابل دسترس است:

https://www.bitdefender.com/blog/labs/bitdefender-partnership-with-law-enforcement-yields-megacortex-decryptor/

همچنین راهنمای استفاده از آن در نشانی زیر قابل دریافت است:

http://www.nomoreransom.org/uploads/UserManualMegaCortexDecryptor.pdf

بازنشستگی قطعی

Windows 7

شرکت مایکروسافت (Microsoft) در اطلاعیه‌ای اعلام نموده که از بعد از روز سه‌شنبه ۲۰ دی ۱۴۰۱، سیستم عامل Windows 7 دیگر به‌روزرسانی‌ها و اصلاحیه‌های امنیتی را برای وصله آسیب‌پذیری‌ها دریافت نخواهند کرد.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده، چکیده اطلاعیه مذکور ارائه شده است.

سالهاست که ویروس‌نویسان و نفوذگران به‌شدت به استفاده از نقاط ضعف سیستم‌های عامل - به ویژه سیستم عامل پرطرفدار Windows - روی آورده‌اند. وجود یک نقطه ضعف (Vulnerability) خطرناک در سیستم عامل می‌تواند سبب دور زدن قوی‌ترین نرم‌افزارهای ضدویروس یا دیواره‌های آتش شود!

شرکت مایکروسافت علاوه بر عرضه اصلاحیه فوری در مواقع اضطراری، در سه‌شنبه دوم هر ماه میلادی نیز اصلاحیه‌های امنیتی جدید خود را منتشر می‌کند. کمتر سه‌شنبه دوم ماه میلادی را می‌توان یافت، که مایکروسافت اصلاحیه‌ای «حیاتی» (Critical) برای سیستم‌عامل Windows عرضه نکرده باشد. بنابراین نفوذگران با اطلاع از جزئیات نقاط ضعف جدید کشف شده در سیستم‌های عامل پشتیبانی شده که توسط شرکت مایکروسافت منتشر می‌شوند می‌توانند با مهندسی معکوس این نقاط ضعف را در این سیستم‌های عامل از رده خارج نیز شناسایی نموده و از آنها سوءاستفاده کنند.

پایان عرضه به‌روزرسانی امنیتی برای Windows 7

مایکروسافت سیستم عامل Windows 7 را در ۳۰ مهر سال ۱۳۸۸ ارائه کرد. پشتیبانی (End of Support - به اختصار EOS) و پشتیبانی تمدید شده (Extended End of Support) از آن به ترتیب در ۲۳ دی ماه ۱۳۹۳ و در ۲۴ دی ماه ۱۳۹۸ به پایان رسید.

برنامه Extended Security Update - به اختصار ESU - آخرین دستاویز برای مشتریانی بود که پس از پایان پشتیبانی مایکروسافت در ۲۳ دی ۱۳۹۳، همچنان در حال اجرای این سیستم‌عامل قدیمی مایکروسافت بودند.

عدم پشتیبانی از Windows 8.1

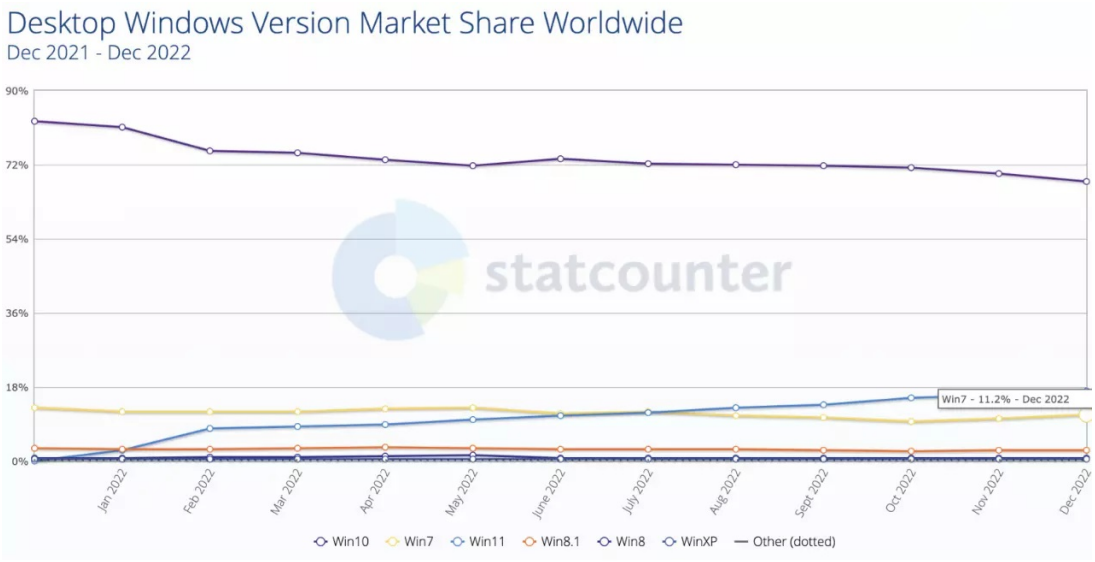
علاوه بر این، Windows 8.1 نیز که برای اولین بار نه سال پیش در آبان ۱۳۹۲ ارائه شده بود، از روز سه‌شنبه ۲۰ دی ۱۴۰۱ دیگر توسط مایکروسافت پشتیبانی نخواهند شد. جزئیات بیشتر در نشانی‌های زیر قابل مطالعه می‌باشند:

https://learn.microsoft.com/en-us/lifecycle/products/windows-7

https://support.microsoft.com/en-us/windows/windows-8-1-support-will-end-on-january-10-2023-3cfd4cde-f611-496a-8057-923fba401e93

https://learn.microsoft.com/en-us/lifecycle/products/windows-81

بر طبق آمار، در حال حاضر، Windows 7 سهمی بیش از ۱۱ درصد از دستگاه‌های با سیستم‌عامل Windows را در سراسر جهان به خود اختصاص داده است؛ این در حالی است که Windows 8.1 توسط ۲٫۵۹ درصد از مشتریان مایکروسافت مورد استفاده قرار می‌گیرد.



عدم پشتیبانی مرورگرهای وب از Windows 7 و Windows 8.1

Microsoft Edge 109 آخرین نسخه این مرورگر وب است که از Windows 7 و Windows 8/8.1 پشتیبانی می‌کند.

این نسخه از Microsoft Edge همچنین آخرین نسخه‌ای خواهد بود که از Windows Server 2008 R2، Windows Server 2012 و Windows Server 2012 R2 پشتیبانی می‌کند.

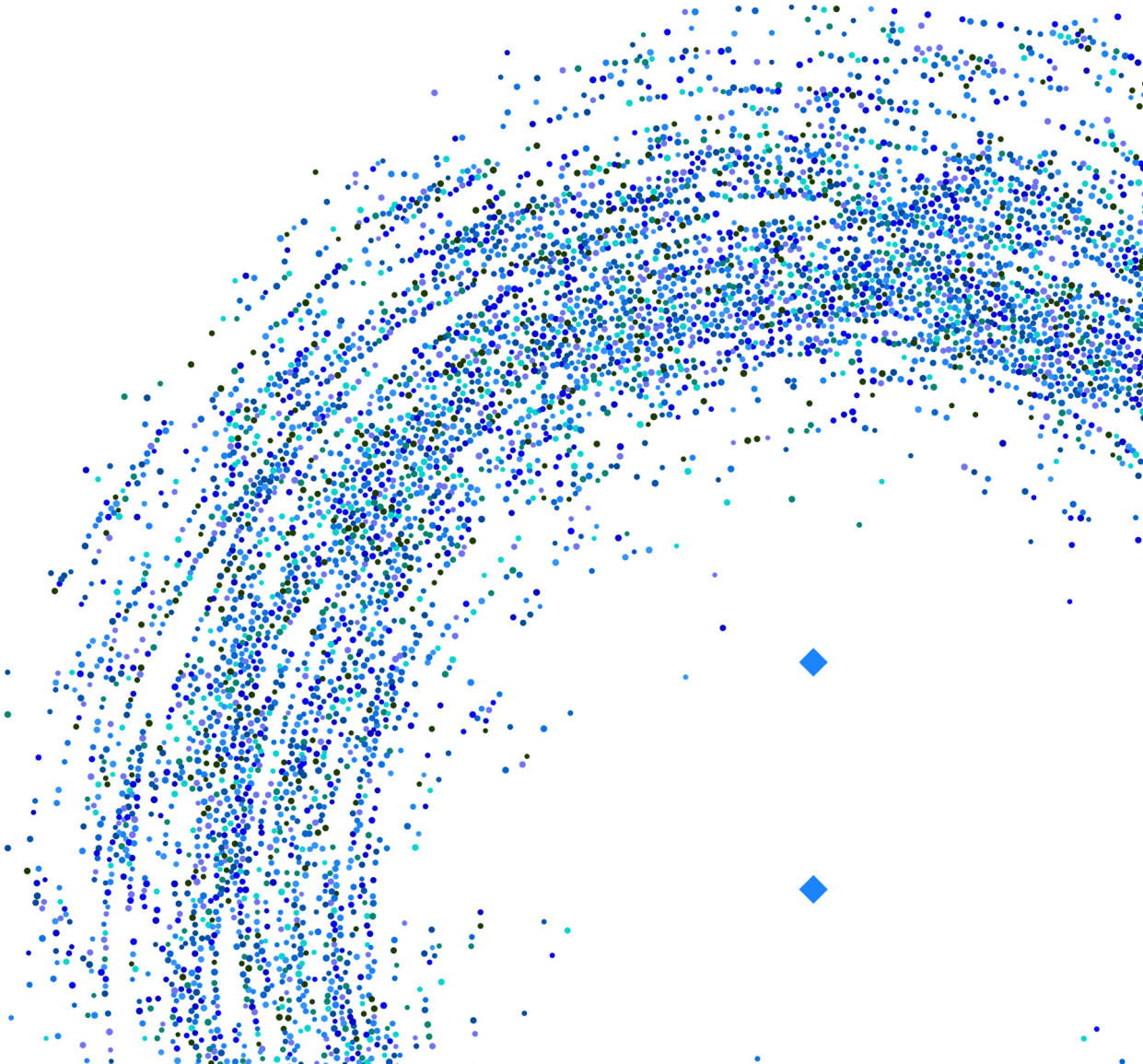
اطلاعیه مشابهی نیز توسط شرکت گوگل (Google) در ماه اکتبر منتشر شد که در آن اعلام نموده نسخه ۱۱۰ مرورگر وب Google Chrome نیز احتمالاً از ۱۲ بهمن ۱۴۰۱ پشتیبانی از Windows 7 و Windows 8.1 را متوقف خواهد کرد.

عدم پشتیبانی مرورگرهای وب به این معنا است که Microsoft Edge 109 و Google Chrome 110 به کار بر روی این سیستم‌عامل‌های قدیمی ادامه خواهند داد اما دیگر به‌روزرسانی‌ها و اصلاحیه‌های امنیتی را دریافت نخواهند کرد و کاربران خود را در معرض انواع تهدیدات امنیتی قرار می‌دهند.

Google Chrome اکنون بیش از ۶۴ درصد از مرورگرهای وب را به خود اختصاص داده است، پس از آن Safari با تقریبا ۱۸ درصد و Microsoft Edge با کمی بیش از ۴ درصد قرار دارند.

بسیاری از سازندگان دیگر پیش‌تر پشتیبانی از سیستم عامل Windows 7 را متوقف کرده بودند. از این رو ارتقاء یا تغییر سیستم‌های عامل از رده خارج به تمامی راهبران توصیه اکید می‌شود.

هشدارهای امنیتی



انتشار بدافزار

از طریق فایل‌های XLL

در پی تصمیم شرکت مایکروسافت (Microsoft) به مسدودسازی ماکرو در فایل‌هایی که از اینترنت دریافت می‌شوند، اکنون مدتی است که مهاجمان از روش‌های جایگزین نظیر افزونه‌های مخرب Excel برای انتشار بدافزارهای خود استفاده می‌کنند.

برخی محصولات شرکت مایکرسافت، از جمله مجموعه نرم‌افزارهای Office، قابلیتی با عنوان Visual Basic for Applications - به اختصار VBA - معروف به ماکرو (Macros) دارند. کاربرانی همچون حسابداران، مهندسان صنایع و مدیران سیستم می‌توانند از ماکروها در درون فایل‌هایی همچون Word و Excel استفاده کنند. ماکروها سبب سرعت بخشیدن به اموری می‌شوند که روالی تکرارشونده دارند.

بر اساس گزارشی که شرکت سیسکو (Cisco) آن را منتشر کرده، مهاجمان به طور فزاینده‌ای از افزونه‌های (Add-in) نرم‌افزار Excel در قالب فایل‌های XLL به عنوان بردار نفوذ اولیه جهت آلوده‌سازی سیستم‌های کاربران و رخنه به سازمان‌ها استفاده می‌کنند.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده برگردان چکیده گزارش مذکور ارائه شده است.

مدتهاست که توزیع فایل‌های نرم‌افزارهای مختلف Office از طریق ایمیل‌های فیشینگ نیزه‌ای (Spear-phishing) و سایر حملات مهندسی اجتماعی به طور گسترده توسط مهاجمان برای نفوذ به اهداف خود مورد استفاده قرار می‌گیرد.

این فایل‌ها معمولاً قربانی را تشویق می‌کنند تا قابلیت ماکرو را جهت مشاهده محتوای به ظاهر بی‌ضرر فعال کنند. حال آن که فعالسازی آن می‌تواند منجر به دریافت بدافزار از اینترنت و اجرای آن بر روی سیستم می‌شود. برای مقابله با این نوع از بهره‌جویی، مایکروسافت از مرداد ۱۴۰۱ قابلیت ماکرو را در فایل‌های Office پیوست‌شده به ایمیل مسدود نموده است.

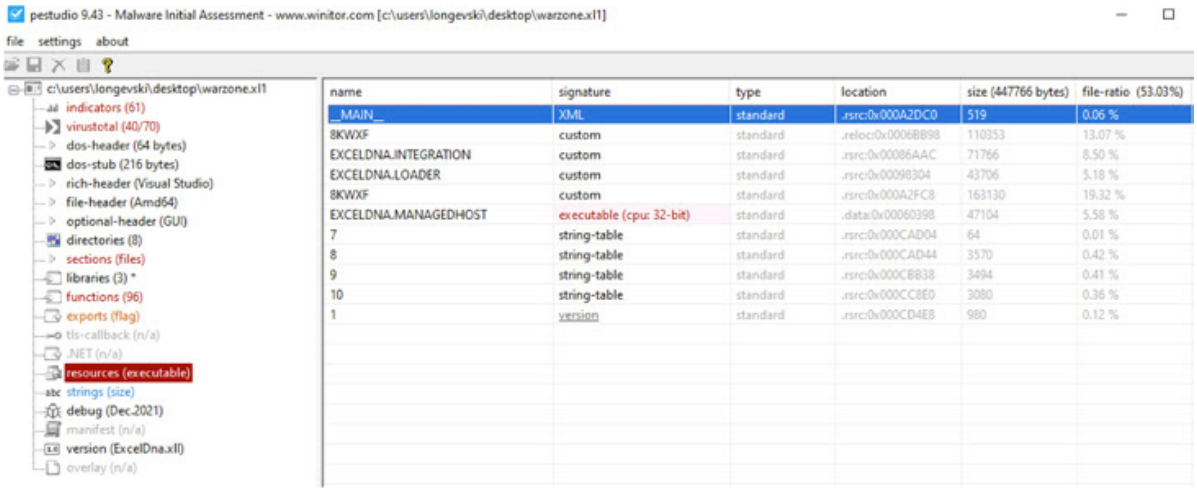
هر چند این مسدودسازی تنها در نسخه‌های جدید Access، Excel، PowerPoint، Visio و Word اعمال شده، اما با کاهش اثربخشی آن برای مهاجمان، این تبهکاران نیز در حال آزمودن تکنیک‌های جایگزین هستند.

یکی از این روش‌های جدید استفاده از فایل‌های XLL است که توسط مایکروسافت به عنوان یک نوع فایل Dynamic Link Library – به اختصار DLL – در نظر گرفته می‌شود و تنها توسط Excel باز می‌شود.

فایل‌های XLL قابل ارسال از طریق ایمیل بوده و با توجه به غیرمعمول بودن استفاده از آنها چه بسا به سادگی از سد محصولت ضدبدافزار نیز عبور کنند.

به نظر می‌رسد مهاجمان مورد اشاره شرکت سیسکو، از ترکیبی از افزونه‌های معتبر در کنار افزونه‌های اختصاصی که از طریق یک ابزار رایگان با نام Excel-DNA توسعه داده شده‌اند بهره می‌گیرند.

گفته می‌شود که اولین بهره‌جویی از فایل‌های XLL در سال ۱۳۹۶ رخ داده بوده است؛ در جریان آن حمله، مهاجمان APT10 (منتسب به هکرهای چینی که با نام مستعار Stone Panda نیز شناخته می‌شوند) از تکنیک Process Hollowing (تعویض فایل اجرایی و جایگزینی کد مخرب به جای آن) برای تزریق Payload از طریق «دسترسی غیرمجاز» (Backdoor) به حافظه استفاده کردند.



از آن زمان، گروه‌های دیگر نظیر TA410 (احتمالاً مرتبط با APT10)، DoNot Team، FIN7 و همچنین Agent Tesla، Arkei، Buer، Dridex، Ducktail، Ekipa RAT، FormBook، IcedID، Vidar Stealer و Warzone RAT در حال بکارگیری این روش در حملات خود می‌باشند.

پیش‌تر نیز شرکت پالو آلتو نتورکس (Palo Alto Networks) از بهره‌جویی از فایل‌های XLL جهت توزیع بدافزارهای Agent Tesla و Dridex خبر داده بود که همگی بیانگر استقبال فزاینده مهاجمان از این تکنیک جدید است.

هر چه تعداد کاربرانی که از نسخ جدید Office استفاده می‌کنند افزایش پیدا کند، احتمال بهره‌جویی مهاجمان از فایل‌های XLL به‌جای سوءاستفاده از قابلیت VBA افزایش می‌یابد.

ضمن آن که تبهکاران سایبری امروزه در حملات خود به دنبال بهره‌جویی از آسیب‌پذیری‌هایی که به تازگی کشف‌شده‌اند جهت راه‌اندازی کدهای مخرب در پروسه‌های نرم‌افزار Office نیز می‌باشند.

لازم به ذکر است که مسدوسازی ماکروها و ممانعت از اجرای آنها در فایل‌های دانلود شده از اینترنت توسط مایکروسافت در فایل‌های Publisher اعمال نمی‌شود و به تبهکاران سایبری امکان می‌دهد از این نرم‌افزار در کارزارهای فیشینگ خود سوءاستفاده کنند. برای مثال می‌توان به بدافزار Ekipa RAT اشاره کرد که گردانندگانش از طریق فایل‌های Publisher که ماکروی مخرب به آنها تزریق شده بود برای توزیع آن بهره بردند. لذا آموزش کاربران در پرهیز از فعالسازی قابلیت به خصوص در فایل‌های مشکوک همچنان نقشی مهم و مؤثر در مقابله با این تهدیدات دارد.

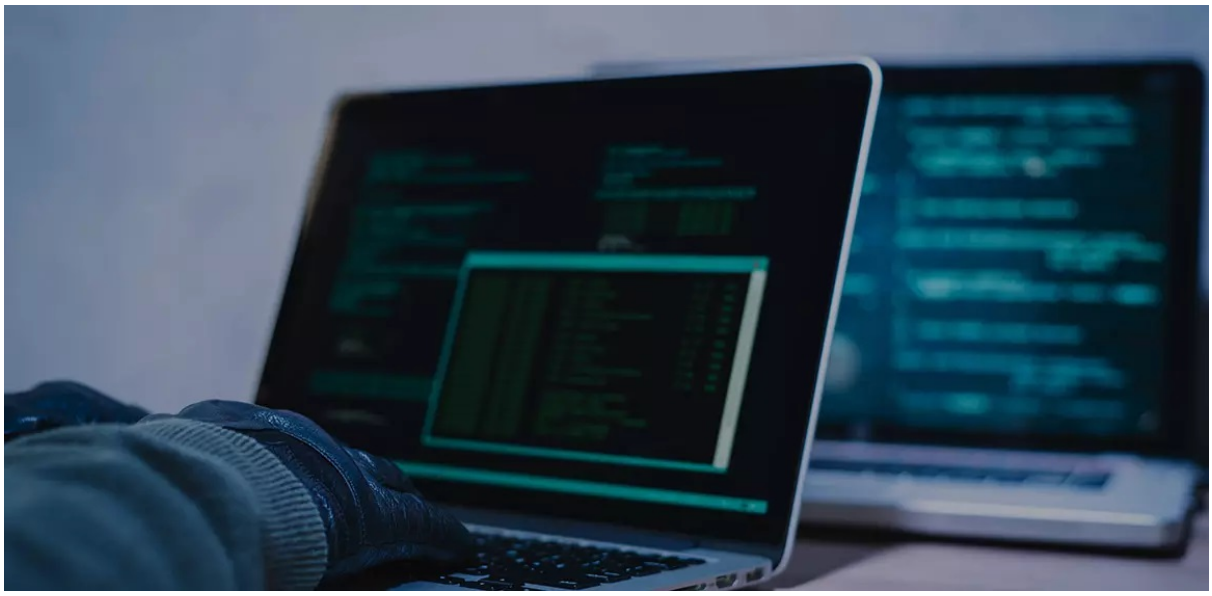
مشروح گزارش سیسکو و نشانه‌های آلودگی (IoC) تهدیدات مورد اشاره این شرکت در نشانی زیر قابل مطالعه می‌باشد:

https://blog.talosintelligence.com/xlling-in-excel-malicious-add-ins/

منبع

https://thehackernews.com/2022/12/apt-hackers-turn-to-malicious-excel-add.html

کاربران ایرانی،
اصلی‌ترین هدف کارزار اخیر EyeSpy



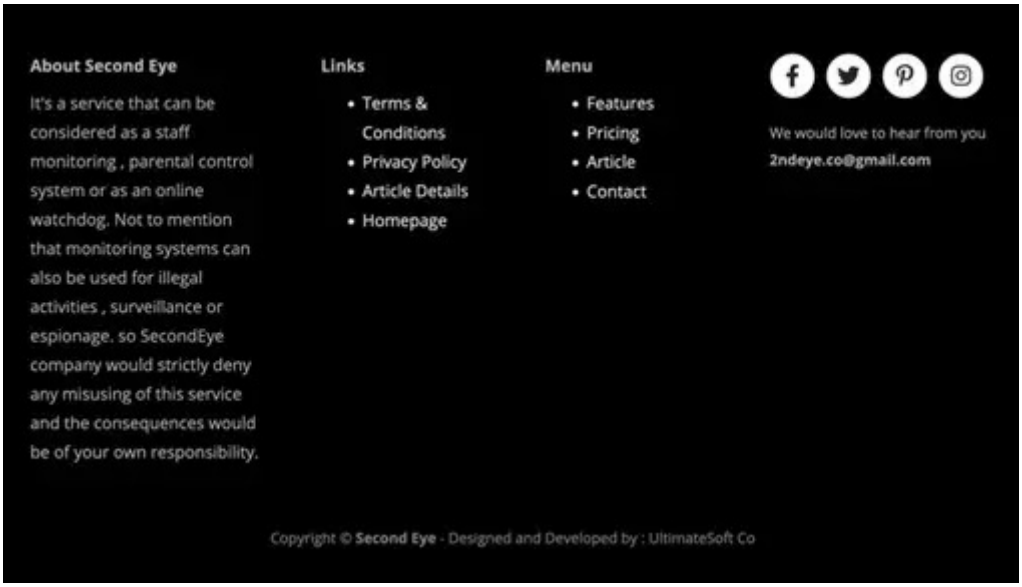
شرکت بیت‌دیفندر (Bitdefender)، جزییات کارزاری را منتشر کرده که در جریان آن، مهاجمان از طریق نسخه‌ای مخرب از یک برنامه VPN اقدام به آلوده‌سازی دستگاه کاربران به جاسوس‌افزار EyeSpy می‌کنند.

بر طبق گزارش بیت‌دیفندر، ایران، بیشترین سهم از قربانیان این کارزار اخیر EyeSpy را داشته است.

در کارزار مذکور، EyeSpy از طریق نسخه مخرب یک برنامه VPN با نام 20speed به دستگاه کاربران راه می‌یابد.

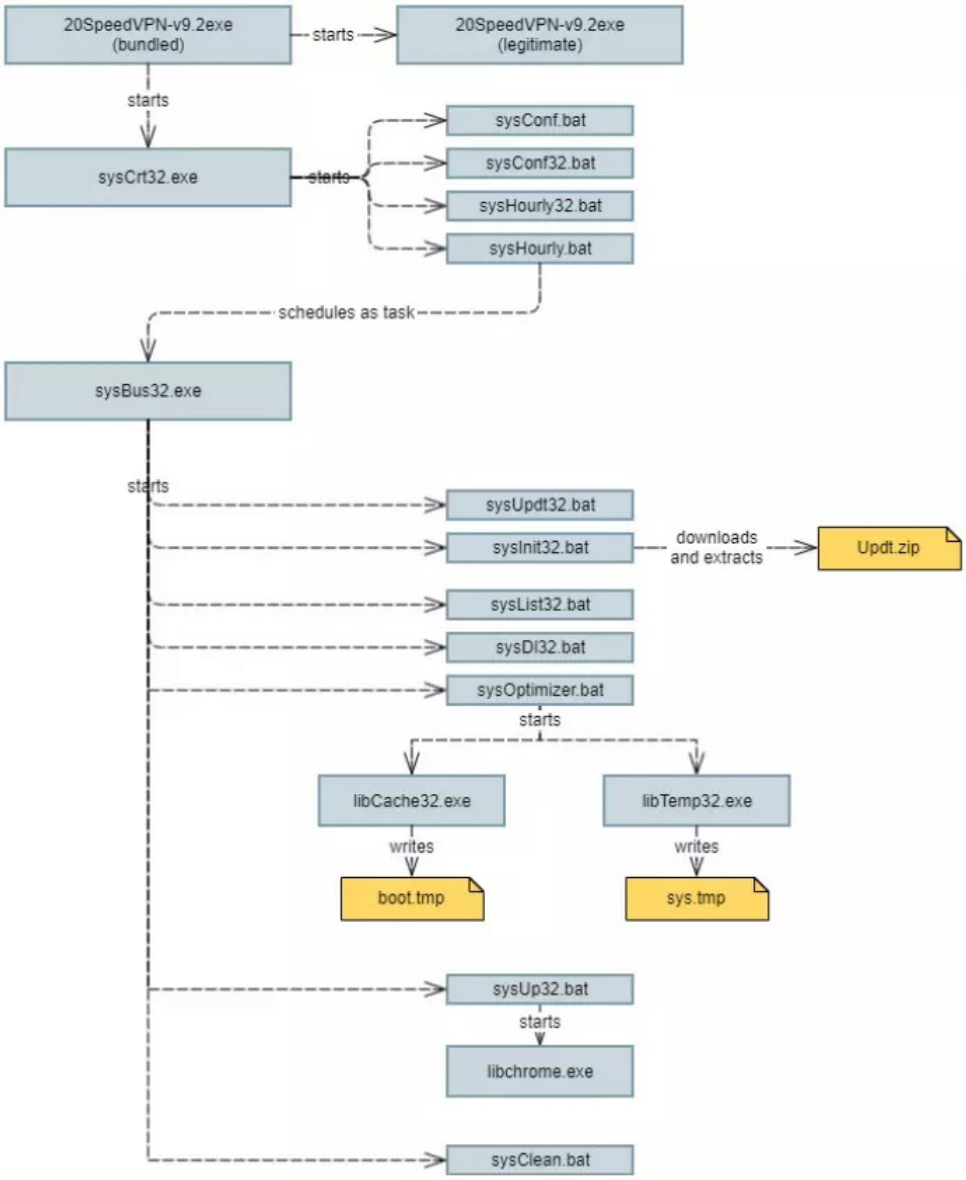
این نسخه مخرب از برخی قابلیت‌ها و اجزای SecondEye که یک برنامه نظارتی تجاری است برای جاسوسی از قربانی استفاده می‌کند.

توسعه‌دهندگان ایرانی SecondEye، این نرم‌افزار را ابزار نظارت بر کارکنان (Staff Monitoring)، سیستم کنترل والدین (Parental Control System) و به طور کلی یک نگهبان آنلاین (Online Watchdog) معرفی می‌کنند. در عین حال تأکید کرده‌اند سیستم‌های نظارتی می‌توانند برای فعالیت‌های غیرقانونی یا جاسوسی نیز مورد استفاده قرار بگیرند.

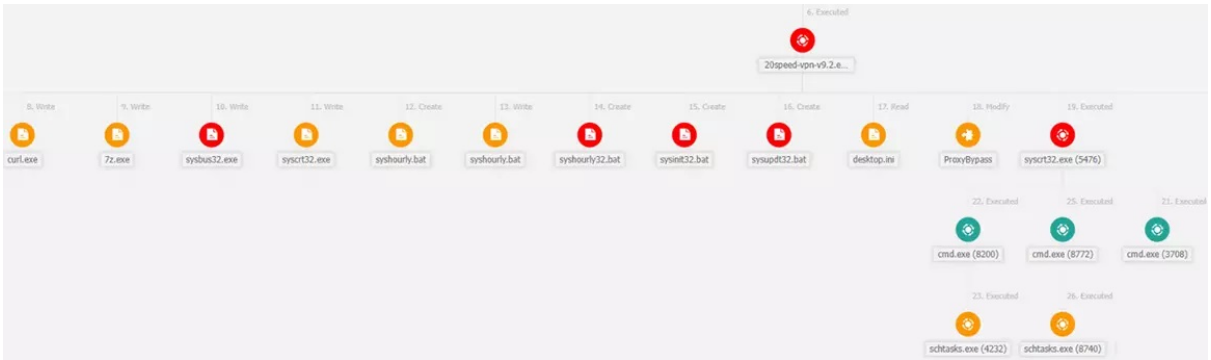


SecondEye دارای طیف گسترده‌ای از قابلیت‌های رصد فعالیت‌های کاربر است. از جمله این قابلیت‌ها می‌توان به ضبط صدا از طریق میکروفون دستگاه، تصویربرداری از طریق دوربین دستگاه و ثبت کلیدهای فشرده‌شده توسط کاربر اشاره کرد.

در کارزار EyeSpy، نفوذ به دستگاه از طریق اجرای نسخه مخرب 20speed توسط کاربر ناآگاه انجام می‌پذیرد. در ادامه اگر چه ارتباط VPN برقرار می‌گردد اما در پشت صحنه عملاً امکان جاسوسی از فعالیت‌های کاربر و اجرای انواع فرامین بالقوه مخرب برای مهاجمان فراهم می‌شود.

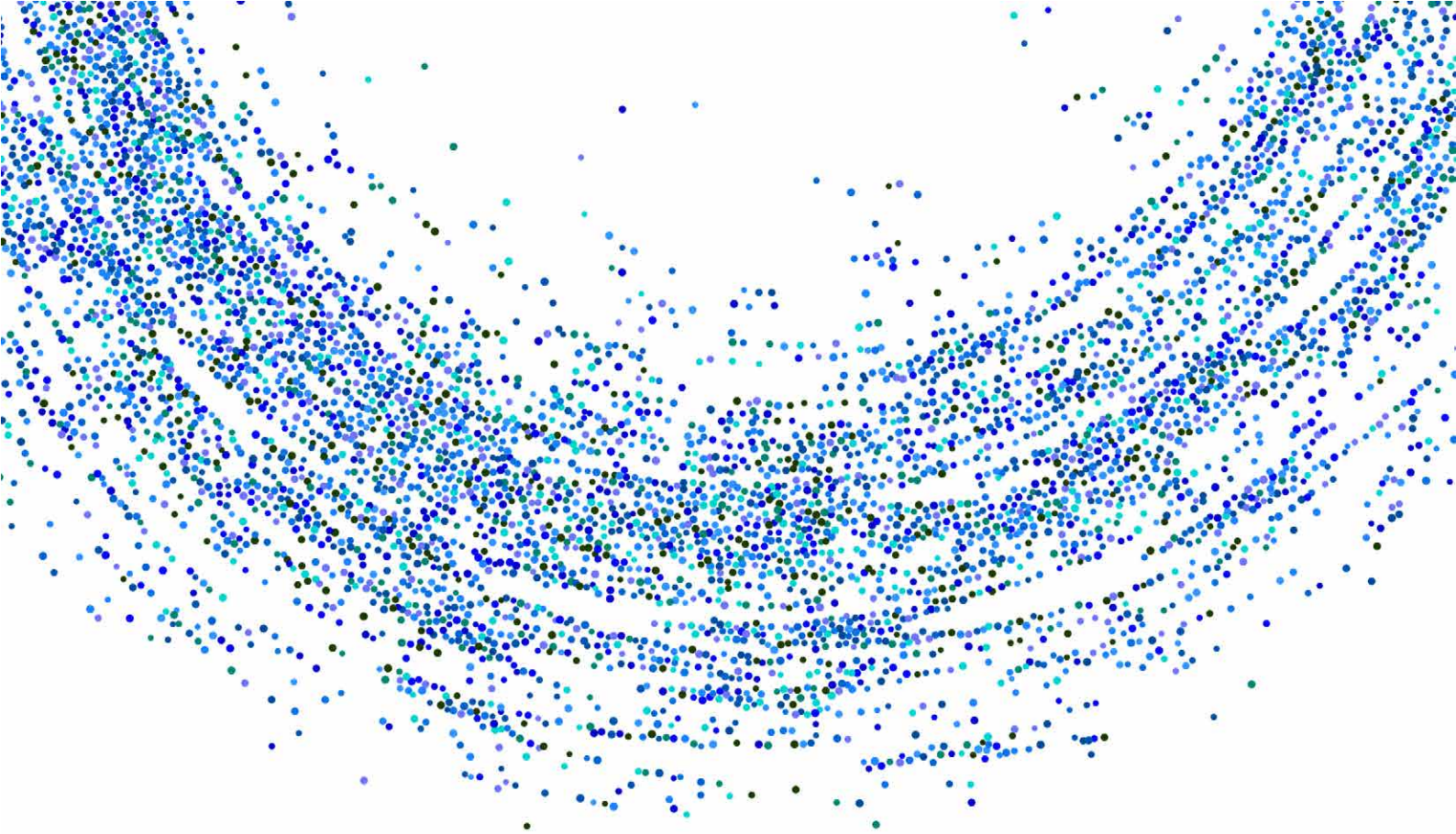


ضدویروس بیت‌دیفندر فایل‌های مخرب اصلی این کارزار را با نام‌های Application.20Speed.A و Trojan.SecondEye.A شناسایی می‌کند.



مشروح گزارش بیت‌دیفندر، همراه با فهرست کامل نشانه‌های آلودگی (IoC) در لینک زیر قابل دریافت و مطالعه است:

https://www.bitdefender.com/files/News/CaseStudies/study/427/Bitdefender-PR-Whitepaper-EyeSpyVPN-creat625-en-EN.pdf



آسیب‌پذیری‌ها و اصلاحیه‌های امنیتی

بهره‌جویی مهاجمان از
آسیب‌پذیری روز صفر فورتی‌نت

چندی پیش شرکت فورتی‌نت (Fortinet) با انتشار توصیه‌نامه‌ای نسبت به بهره‌جویی فعال مهاجمان از ضعفی در FortiOS SSL-VPN هشدار داد. اکنون وصله این آسیب‌پذیری که دارای شناسه CVE-2022-42475 می‌باشد، ارائه شده است.

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

این ضعف امنیتی مهاجمان احراز هویت نشده را قادر می‌سازد تا کد مخرب و دلخواه را به طور بالقوه و از راه دور در تجهیزات آسیب‌پذیر اجرا کنند.

در آن زمان شرکت فورتی‌نت در خصوص جزئیات بهره‌جویی از این آسیب‌پذیری در حملات، اطلاعاتی منتشر نکرده بود؛ در گزارشی که به تازگی این شرکت منتشر کرده، اینطور عنوان شده که مهاجمان از اکسپلویت‌های CVE-2022-42475 جهت هک FortiOS SSL-VPN و توزیع بدافزارها استفاده می‌کنند.

به نقل از محققان شرکت فورتی‌نت، پیچیدگی بالای بهره‌جویی از این اکسپلویت حکایت از تخصص بالای مهاجمان و هدفمند بودن حملات دارد.

مهاجمان با سوءاستفاده از این آسیب‌پذیری اقدام به نصب بدافزار نموده و به شدت بر حفظ ماندگاری در سیستم و فرار از راهکارهای تشخیصی تمرکز دارند تا بتوانند لاگ‌های گزارش را حذف کنند یا حتی در صورت لزوم، پروسه‌های مربوط به لاگ‌ها را از بین ببرند.

کدهای مخرب (Payload) مضاعف دانلود شده در دستگاه‌های آسیب‌پذیر ضمن نصب بدافزار، سیستم‌های پیشگیری از نفوذ (IPS) این دستگاه‌ها را - که جهت پیشگیری از نفوذ امنیتی طراحی شده و با رصد مداوم بر ترافیک شبکه سعی در شناسایی تهدیدات دارند- غیرفعال می‌نمایند.

همچنین این شرکت هشدار داده که در طی حمله، Payload مخرب از یک سایت راه دور دانلود شده اما این محققان موفق به بازیابی آن جهت تحلیل نشدند.

مشروح گزارش این شرکت به همراه نشانه‌های آلودگی (Indicators-of-Compromise - به اختصار IoC) آن در نشانی زیر قابل مطالعه می‌باشد:

https://www.fortinet.com/blog/psirt-blogs/analysis-of-fg-ir-22-398-fortios-heap-based-buffer-overflow-in-sslvpnd

فورتی‌نت به تمامی مشتریان توصیه می‌کند که در اسرع وقت ضمن اعمال وصله منتشر شده، FortiOS را به آخرین نسخه ارتقاء دهند تا از حملات در امان باشند.

منبع

https://www.bleepingcomputer.com/news/security/fortinet-govt-networks-targeted-with-now-patched-ssl-vpn-zero-day/

بروزرسانی‌ها و اصلاحیه‌های

دی ۱۴۰۱

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

مایکروسافت
سیسکو
ترلیکس
فورتی‌نت

بیت‌دیفندر
موزیلا
گوگل

ادوبی
دروپال
جونیپر نت‌ورکز

مایکـروسافت

۲۰ دی ۱۴۰۱، شرکت مایکروسافت (Microsoft)، مجموعه اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی ژانویه ۲۰۲۳ منتشر کرد. اصلاحیه‌های مذکور حدود ۱۰۰ آسیب‌پذیری را در Windows و محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت ۱۱ مورد از آسیب‌پذیری‌های ترمیم شده این ماه «حیاتی» (Critical) و اکثر موارد دیگر «مهم» (Important) اعلام شده است. این مجموعه اصلاحیه‌ها، انواع مختلفی از آسیب‌پذیری‌ها را در محصولات مایکروسافت ترمیم می‌کنند:

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

دو مورد از آسیب‌پذیری‌های ترمیم شده این ماه (شناسه‌های CVE-2023-21674 و CVE-2023-21549)، از نوع «روز-صفر» می‌باشند که یک مورد آن (CVE-2023-21674) به طور گسترده در حملات مورد سوءاستفاده قرار گرفته‌اند. 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.

در ادامه به بررسی جزییات ضعف‌های امنیتی روز صفر که در ماه میلادی ژانویه ۲۰۲۳ توسط شرکت مایکروسافت ترمیم شده‌اند، می‌پردازیم.

- CVE-2023-21549: این ضعف امنیتی که به طور عمومی افشاء شده، دارای درجه اهمیت «مهم» بوده و از نوع «ترفیع اختیارات» است. این ضعف امنیتی بر Windows SMB Witness Service تاثیر می‌گذارد. مهاجم جهت بهره‌جویی از این آسیب‌پذیری باید یک اسکریپت مخرب خاص را اجرا نموده که منجر به یک فراخوانی RPC در سرور RPC می‌شود؛ سوءاستفاده موفق از آن مهاجم را قادر به افزایش امتیازات بر روی سرور می‌نماید.
- CVE-2023-21674: این آسیب‌پذیری روز صفر دارای درجه اهمیت «مهم» بوده و از نوع «ترفیع اختیارات» است و Windows Advanced Local Procedure Call - به اختصار ALPC - از آن متاثر می‌شود. بهره‌جویی از این آسیب‌پذیری می‌تواند منجر به دور زدن Sandbox مرورگر شود؛ سوءاستفاده موفق از آن مهاجم را قادر به کسب امتیازات در سطح SYSTEM می‌نماید.

۱۱ مورد از آسیب‌پذیری‌های ترمیم شده این ماه دارای درجه اهمیت «حیاتی» می‌باشند که به نقل از مایکروسافت، احتمال سوءاستفاده از تمام آسیب‌پذیری‌های «حیاتی» این ماه کم می‌باشد به جز ضعف امنیتی CVE-2023-21743. در ادامه به بررسی جزییات این ضعف‌های امنیتی می‌پردازیم.

- CVE-2023-21743: این آسیب‌پذیری «حیاتی» از نوع «عبور از سد امکانات امنیتی» می‌باشد و Microsoft SharePoint Server را در شرایطی خاص تحت تاثیر قرار می‌دهد. این آسیب پذیری پیچیدگی کمی دارد و می تواند به راحتی توسط یک مهاجم فعال شود. در یک حمله مبتنی بر شبکه، یک کاربر احراز هویت نشده می تواند یک اتصال ناشناس به سرور SharePoint مورد نظر برقرار کند. عمل ارتقاء را می‌توان با اجرای SharePoint Products Configuration Wizard و فرمان Upgrade-SPFarm PowerShell cmdlet یا فرمان psconfig.exe -cmd upgrade -inplace b2b پس از اجرای به‌روزرسانی آغاز نمود.
- CVE-2023-21551، CVE-2023-21561 و CVE-2023-21730: این سه ضعف امنیتی بر Microsoft Cryptographic Services تاثیر می‌گذارند. این آسیب‌پذیری‌ها می‌توانند توسط یک مهاجم اصالت‌سنجی شده محلی مورد سوءاستفاده قرار گیرند که داده‌های دستکاری شده ویژه‌ای را به سرویس محلی CSRSS ارسال می‌کند. این به مهاجمان اجازه می‌دهد تا امتیازات خود را از بستر AppContainer به دسترسی در سطح SYSTEM ارتقاء دهند.
- CVE-2023-21556، CVE-2023-21555، CVE-2023-21543، CVE-203-21546 و CVE-2023-21679: این پنج آسیب‌پذیری «حیاتی» از نوع «اجرای کد از راه دور» می‌باشند و بر Windows Layer 2 Tunneling Protocol – به اختصار L2TP – تاثیر می‌گذارند. بهره‌جویی موفق یک مهاجم احراز هویت نشده را قادر می‌سازد تا کد مخرب را روی سرورهای RAS اجرا کند.
- CVE-2023-21548 و CVE-2023-21535: این دو ضعف امنیتی «حیاتی» به دلیل پیچیدگی‌شان، به «احتمال کمتر» مورد بهره‌جویی قرار خواهند گرفت. هر دو این آسیب‌پذیری‌ها، از نوع «اجرای کد از راه دور» می‌باشند و Windows Secure Socket Tunneling Protocol – به اختصار SSTP – از آنها متاثر می‌شود. از طرفی مهاجم تنها با برنده شدن در شرایط رقابتی (Race Condition) قادر به بهره‌جویی از آن می‌باشد؛ جهت بهره‌جویی مهاجم احراز هویت نشده می‌تواند اقدام به ارسال یک درخواست دستکاری شده ویژه به سرور آسیب‌پذیر نموده و فرامین غیرمجاز را از راه دور بر روی سیستم اجرا نماید.

در ادامه به بررسی جزییات دیگر آسیب‌پذیری‌های اصلاح شده این ماه و به ویژه به مواردی که ممکن است بیشتر مورد توجه مهاجمان قرار گیرند، می‌پردازیم.

- CVE-2023-21779: این ضعف امنیتی «مهم» که بهره‌جویی از آن به تعامل کاربر نیاز دارد، از نوع «اجرای کد از راه دور» است و Visual Studio Code از آن تاثیر می‌پذیرد. بهره‌جویی از این آسیب‌پذیری مستلزم آن است که مهاجم از راه دور و از طریق مهندسی اجتماعی، قربانی را متقاعد کند که یک فایل مخرب vscode خاص را از یک سایت دانلود و باز کند که منجر به یک حمله محلی در

سیستم آسیب‌پذیر می‌شود. از این رو توصیه می‌شود برنامه‌نویسان هرگز فایلی را که نمی‌دانند چیست یا از امن بودن آن اطمینان ندارند در Visual Studio Code باز نکنند.

- CVE-2023-21763 و CVE-2023-21764: این دو آسیب‌پذیری دارای درجه اهمیت «مهم» بوده و Microsoft Exchange Server را تحت تاثیر قرار می‌دهند و از نوع «ترفیع اختیارات» می‌باشند. این آسیب‌پذیری ناشی از عدم وصله صحیح یک باگ شناسایی شده قبلی به شماره شناسه CVE-2022-41123 می‌باشد. از طریق یک مسیر فایلی Hard-coded، یک مهاجم محلی ممکن است بتواند DLL خود را نصب نموده و کد مخرب را با امتیازات سطح SYSTEM اجرا کند. اکیداً توصیه می‌شود سازمان‌هایی که Exchange را استفاده می‌کنند، تمامی به‌روزرسانی‌های امنیتی Exchange را سریعاً جهت ترمیم این دو آسیب‌پذیری اجرا نمایند.

- CVE-2023-21674: این آسیب‌پذیری که Windows Advanced Local Procedure Call - به اختصار ALPC - از آن تاثیر می‌پذیرد، دارای درجه اهمیت «مهم» می‌باشد. بهره‌جویی از این ضعف امنیتی امکان «ترفیع اختیارات» را در سطح Kernel و SYSTEM برای مهاجم محلی فراهم می‌کند؛ از این رو مهاجم قادر خواهد بود تا Sandbox را در مرورگر دور بزند، این نوع از آسیب‌پذیری‌های اغلب در حملات بدافزاری یا باج‌افزاری مورد استفاده قرار می‌گیرند. این ضعف امنیتی توسط محققان آواست (Avast) به مایکروسافت گزارش شده و نشان‌دهنده خطر بالقوه چنین فعالیت‌های مخربی است.

از طرفی شرکت مایکروسافت احتمال بهره‌جویی از شش آسیب‌پذیری «مهم» زیر را «زیاد» اعلام نموده است؛ بهره‌جویی از تمامی این ضعف‌های امنیتی مهاجم را قادر به «افزایش اختیارات» می‌نماید.

- CVE-2023-21532: Windows GDI
- CVE-2023-21541: Windows Task Scheduler
- CVE-2023-21552: Windows GDI
- CVE-2023-21725: Windows Malicious Software Removal Tool
- CVE-2023-21726: Windows Credential Manager User Interface
- CVE-2023-21768: Windows Ancillary Function Driver for WinSock

همانطور که پیش‌تر در این خبر شرح داده شد، شرکت مایکروسافت در اطلاعیه‌ای اعلام نموده که از بعد از روز سه‌شنبه ۲۰ دی ۱۴۰۱، سیستم عامل Windows 7 دیگر به‌روزرسانی‌ها و اصلاحیه‌های امنیتی را برای وصله آسیب‌پذیری‌ها دریافت نخواهند کرد.

همچنین Windows 8.1 نیز که برای اولین بار نه سال پیش در آبان ۱۳۹۲ ارائه شده بود، از روز سه‌شنبه ۲۰ دی ۱۴۰۱ دیگر توسط مایکروسافت پشتیبانی نخواهند شد.

بسیاری از سازندگان دیگر نیز پیش از این پشتیبانی از سیستم عامل Windows 7 را متوقف کرده بودند. از این رو ارتقاء یا تغییر سیستم‌های عامل از رده خارج به تمامی راهبران توصیه اکید می‌شود.

فهرست کامل آسیب‌پذیری‌های ترمیم شده توسط مجموعه‌اصلاحیه‌های ژانویه ۲۰۲۳ مایکروسافت که با همکاری مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده در گزارش زیر قابل مطالعه است:

https://afta.gov.ir/fa-IR/Portal/4927/news/view/14608/2323

سیسکو

شرکت سیسکو (Cisco Systems) در دی ماه در چندین نوبت اقدام به عرضه بروزرسانی‌های امنیتی برای برخی از محصولات خود کرد. این بروزرسانی‌ها، ۲۳ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت ۲ مورد از آنها از نوع «حیاتی»، ۸ مورد از آنها از نوع «بالا» (High) و ۱۳ مورد از نوع «متوسط» (Medium) گزارش شده است. آسیب‌پذیری‌هایی همچون «از کاراندازی سرویس»، «اجرای کد از راه دور»، «نشت حافظه» (Memory Leak)، «افشای اطلاعات» و «تزریق کد از طریق سایت» (Cross site Scripting) از جمله مهمترین اشکالات مرتفع شده توسط بروزرسانی‌های جدید هستند. مهاجم می‌تواند از بعضی از این آسیب‌پذیری‌ها برای کنترل سیستم آسیب‌پذیر سوءاستفاده کند. اطلاعات بیشتر در نشانی زیر قابل دسترس می‌باشد:

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

ترلیکس

در ماهی که گذشت، ترلیکس (Trellix) از ترمیم دو آسیب‌پذیری به شناسه‌های CVE-2021-31833 و CVE-2023-0221 در نرم‌افزار Application and Change Control خبر داد. آسیب‌پذیری‌های مذکور در نسخه 8.3.4 و نسخه‌های بعد از آن برطرف شده‌اند. جزییات بیشتر در لینک زیر قابل دریافت و مطالعه است:

https://kcm.trellix.com/corporate/index?page=content&id=SB10370

فورتی‌نت

در ماهی که گذشت شرکت فورتی‌نت (Fortinet) با انتشار چندین توصیه‌نامه از ترمیم ۵ ضعف امنیتی در محصولات این شرکت خبر داد. درجه اهمیت دو مورد از آنها از نوع «بالا» و سه مورد از نوع «متوسط» گزارش شده است. جزییات بیشتر در خصوص ضعف‌های امنیتی مذکور در لینک زیر قابل مطالعه است:

https://www.fortiguard.com/psirt

بیت‌دیفندر

در دی ۱۴۰۱، شرکت بیت‌دیفندر (Bitdefender) نسخ جدید زیر را عرضه کرد:

GravityZone Control Center 6.30.2-2:
https://www.bitdefender.com/business/support/en/77212-78207-gravityzone-control-center.html

Endpoint Security Tools for Windows 7.8.1.244:
https://www.bitdefender.com/business/support/en/77212-77540-windows-agent.html

Endpoint Security for Mac 7.12.24.200022:
https://www.bitdefender.com/business/support/en/77212-78218-macos-agent.html

Security Server Multi-Platform 6.2.13.11842:
https://www.bitdefender.com/business/support/en/77212-78253-security-server-multi-platform.html

رفع باگ‌های امنیتی و اعمال برخی بهبودها، از جمله تغییرات اعمال شده در این نسخه‌ها گزارش شده است.

موزیلا

در دی ماه، بنیاد موزیلا (Mozilla) با ارائه بروزرسانی، چند آسیب‌پذیری امنیتی را در مرورگر Firefox برطرف کرد. این اصلاحیه‌ها، در مجموع ۱۲ آسیب‌پذیری را در محصولات مذکور ترمیم می‌کنند. درجه حساسیت پنج مورد از آنها «بالا»، چهار مورد «متوسط» و سه مورد «کم» 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/

گـوگـل

شرکت گوگل (Google) در دی ماه در یک نوبت اقدام به ترمیم آسیب‌پذیری‌های امنیتی مرورگر Chrome کرد. آخرین نسخه این مرورگر که در ۲۰ دی ماه انتشار یافت، نسخه 109.0.5414.74 برای Linux، نسخه 109.0.5414.87 برای Mac و نسخه 109.0.5414.74/.75 برای Windows است. فهرست اشکالات مرتفع شده در نشانی زیر قابل دریافت و مشاهده است:

https://chromereleases.googleblog.com/2023/01/stable-channel-update-for-desktop.html

ادوبـی

شرکت ادوبی (Adobe) مجموعه اصلاحیه‌های امنیتی ژانویه ۲۰۲۳ را منتشر کرد. اصلاحیه‌های مذکور، در مجموع ۲۹ آسیب‌پذیری را در ٤ محصول زیر ترمیم می‌کنند:

- Adobe Acrobat and Reader
- Adobe InDesign
- Adobe InCopy
- Adobe Dimension

تعداد آسیب‌پذیری ترمیم شده این ماه ادوبی برای Adobe Acrobat and Reader برابر با ۱۵ مورد بوده است. درجه اهمیت ۸ مورد از ضعف‌های امنیتی مذکور «حیاتی» و ۷ مورد «مهم» اعلام شده است. آسیب‌پذیری‌های «حیاتی» مذکور می‌توانند منجر به «اجرای کد» (Arbitrary code execution) شوند و مهاجم را قادر می‌سازند دستوراتی را در رایانه‌های آسیب‌پذیر اجرا کنند. در حالی که سوءاستفاده از ضعف‌های امنیتی «مهم» ترمیم شده در Adobe Acrobat and Reader می‌توانند منجر به «نشت حافظه»، «از کارانداختن سرویس» و «ترفیع اختیارات» شوند.

با نصب به‌روزرسانی ماه ژانویه ۲۰۲۳، نسخه نگارش‌های جاری نرم‌افزارهای Acrobat DC و Acrobat Reader DC به ۲۲/۰۰۳/۲۰۳۱۰، نگارش‌های ۲۰۲۰ به ۲۰/۰۰۵/۳۰۴۳۶ تغییر خواهد کرد.

اطلاعات بیشتر در خصوص مجموعه اصلاحیه‌های ماه ژانویه ۲۰۲۳ ادوبی در لینک زیر قابل مطالعه است:

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

دروپـال

۲۱ دی ۱۴۰۱، جامعه دروپال (Drupal Community) با عرضه بروزرسانی امنیتی، یک ضعف امنیتی با درجه اهمیت «نسبتاً حیاتی» (Moderately Critical) را در ماژول Private Taxonomy Terms نسخه Drupal 8.x. ترمیم نمود. سوءاستفاده از این آسیب‌پذیری، مهاجم را قادر به دور زدن مجوزها و ایجاد، تغییر یا حذف Private Taxonomy Terms خواهد نمود. با نصب این بروزرسانی، این ماژول در دروپال 8.x. به نسخه 8.x-2.6 تغییر خواهد کرد.

توضیحات کامل در خصوص این بروزرسانی و توصیه‌نامه منتشر شده، در نشانی زیر در دسترس می‌باشد:

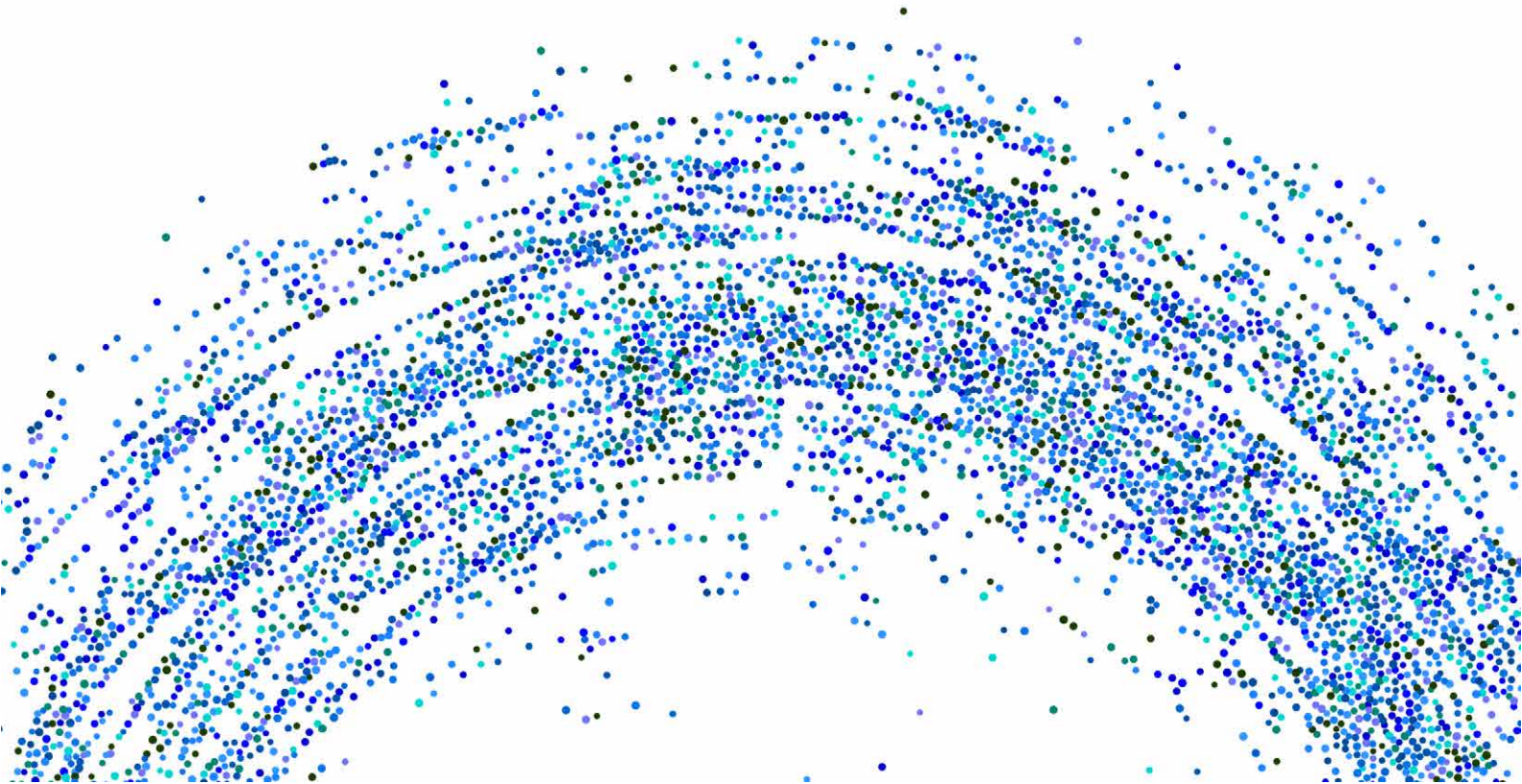
https://www.drupal.org/security

جونیپر نت‌ورکز

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

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

گزارش‌ها



حمله همزمان سه باج‌افزار
به یک قربانی

شرکت سوفوس (Sophos) در گزارشی جزئیات حمله سایبری به یک شرکت خودروسازی که در اردیبهشت۱۴۰۱، توسط سه باج‌افزار به طور جداگانه صورت گرفته را شرح داده است.

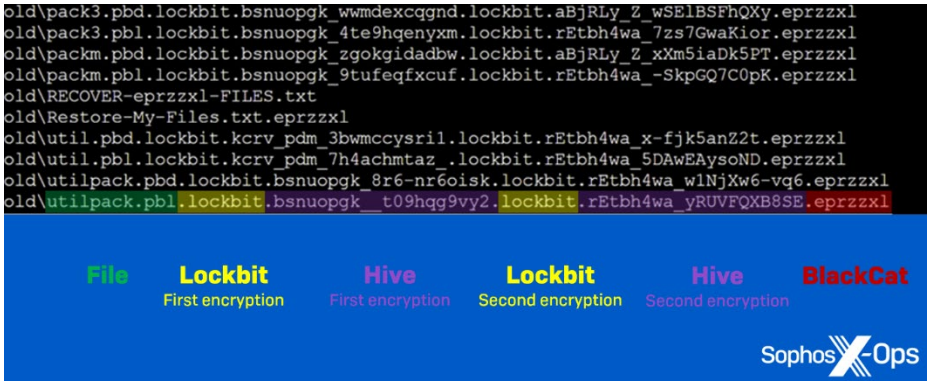
مهاجمان هر سه این باج‌افزارها، به طور مشابه از یک پیکربندی نادرست بهره‌جویی کردند - یکی از قواعد فایروال که پروتکل دسکتاپ از راه دور (Remote Desktop Protocol – به اختصار RDP) را در یک سرور مدیریت اجرا می‌کرد - اما هر یک از آنها از گونه‌ها و تاکتیک‌های باج‌افزاری متفاوتی استفاده کردند.

اولین باج‌افزار یعنی Lockbit داده‌ها را استخراج و به سرویس ذخیره‌سازی ابری Mega منتقل کرد، از Mimikatz برای سرقت رمز عبور استفاده نمود و باج‌افزار خود را با بکارگیری PsExec منتشر کرد.

مهاجمان باج‌افزار دوم که Hive نام داشت، از RDP برای گسترش آلودگی در شبکه استفاده کرده و تنها دو ساعت پس از حمله باج‌افزار Lockbit، کد مخرب خود را منتشر کردند.

هنگامی که قربانی داده‌ها را از نسخ پشتیبان بازیابی می‌کرد، مهاجمان ALPHV/BlackCat به شبکه دسترسی پیدا کرده و ابزار Atera Agent را که یک ابزار دسترسی از راه دور معتبر و متداول است جهت ماندگاری در سیستم نصب کردند و اقدام به استخراج داده‌ها نمودند. دو هفته پس از حملات Lockbit و Hive، مهاجمان باج‌افزار خود را توزیع کرده و لاگ‌های Windows را پاک کردند.

محققان سوفوس به این نکته پی بردند که همانطور که در شکل نشان داده شده، مهاجمان اقدام به رمزگذاری چندگانه چندین فایل نمودند به گونه‌ای که مشاهده شده برخی از این فایل‌ها، پنج بار رمزگذاری شده‌اند؛ هر کدام دو بار توسط Lockbit و Hive و یک بار توسط ALPHV/BlackCat.



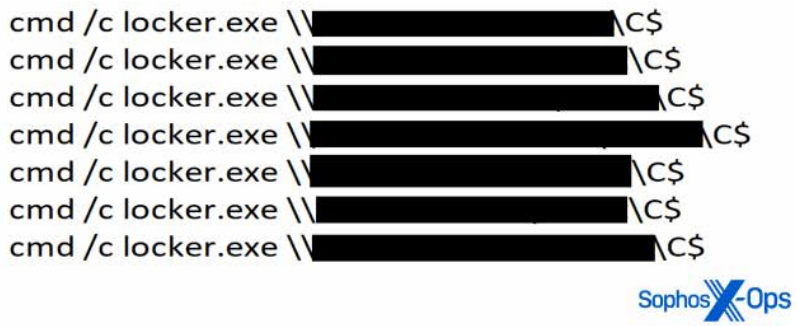
سوفوس پیش از این نیز چندین حمله باج‌افزاری دوگانه را مورد بررسی قرار داده و اخیراً نیز حملات چندگانه را به‌طور کلی‌تر بررسی نموده است زیرا به نظر می‌رسد که به طور فزاینده‌ای این گونه تهدیدات متداول شده است. اما این اولین رویدادی است که در آن سه دسته مهاجم و باج‌افزار به طور مستقل از یک نقطه جهت ورود و حمله به یک سازمان واحد استفاده می‌کنند.

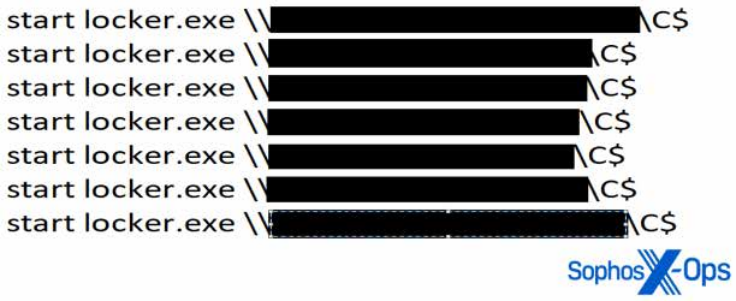
با این که حملات در اردیبهشت ۱۴۰۱ رخ داده، محققان مشاهده نمودند که یک مهاجم در دی ۱۴۰۰ یک پودمان RDP بر روی Domain Controller سازمان ایجاد کرده است؛ این فرد ممکن است مهاجم ایجاد کننده دسترسی اولیه (Initial Access Broker – به اختصار IAB) باشد؛ مهاجمی که سیستم‌های آسیب‌پذیر را شناسایی کرده و دسترسی به آنها را در سایت‌هایی در Dark Web به فروش می‌گذارد یا ممکن است یک عملیات جستجو و شناسایی اولیه جهت نفوذ باشد که توسط یکی از مهاجمان این سه باج‌افزار صورت گرفته است.

در هر صورت، در اواخر فروردین ۱۴۰۱، یکی از مهاجمان Lockbit از طریق سرور مدیریتی متصل به پودمان RDP به شبکه یک سازمان دسترسی پیدا کرد. سپس، مهاجم با نفوذ به سیستم‌های مجاور و متصل در شبکه به Domain Controller و سرورهای دیگر دست یافته و شروع به استخراج و انتقال داده‌ها به سرویس ذخیره‌سازی ابری Mega نمود و همچنین دو اسکریپت PowerShell زیر را اجرا کرد:

- sharefinder.ps1 برای جمع‌آوری اطلاعات در خصوص پوشه‌های اشتراکی شبکه
- invoke-mimikatz.ps1 جهت استخراج رمزهای عبور از Local Security Authority Subsystem – به اختصار LSASS

در ۱۱ اردیبهشت ۱۴۰۱، مهاجمان Lockbit دو اسکریپت دسته‌ای (1.bat و 2.bat) را از طریق PsExec جهت توزیع فایل‌های اجرایی مخرب LockBit_AF51C0A7004B80EA.exe و Locker.exe در سراسر شبکه بکار گرفتند.



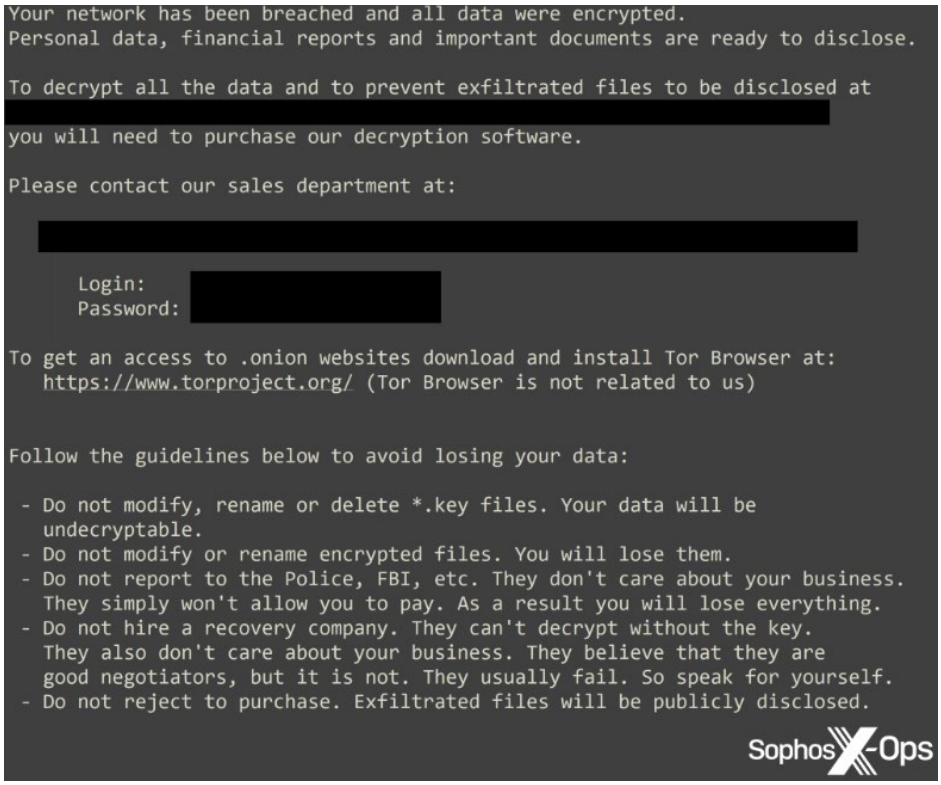


به محض اجرا، باج‌افزار فایل‌های موجود در ۱۹ سرور را رمزگذاری کرده و اطلاعیه‌های باج‌گیری (Ransom Note) با نام Restore-My-Files.txt را در سیستم قرار می‌دهد.

دو ساعت بعد، در حالی که مهاجمان Lockbit در حال رمزگذاری فایل‌ها بودند، یکی از گردانندگان باج‌افزار Hive از طریق همان پودمان RDP به شبکه نفوذ و دسترسی پیدا کرد و از RDP برای انتقال و دستیابی به سرورهای دیگر استفاده نمود.

باج‌افزار Hive از نرم‌افزار معتبر (PDQ Deploy) که قبلاً در شبکه نصب شده بود جهت توزیع باینری مخرب باج‌افزار windows_x32_encrypt.exe استفاده کرد. مجرمان به سوءاستفاده از فایل‌های اجرایی معتبر ادامه می‌دهند و از تکنیک «کسب روزی از زمین» (Living off the Land – به اختصار LotL) در جریان این حملات استفاده می‌کنند. 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 مؤثر است .

باج‌افزار Hive فایل‌های رمزگذاری‌شده را بر روی ۱۶ سرور قرار داده و اطلاعیه‌های باج‌گیری دیگری به نام HOW_TO_DECRYPT.txt را بر روی دستگاه‌های آلوده شده قرار داده است.

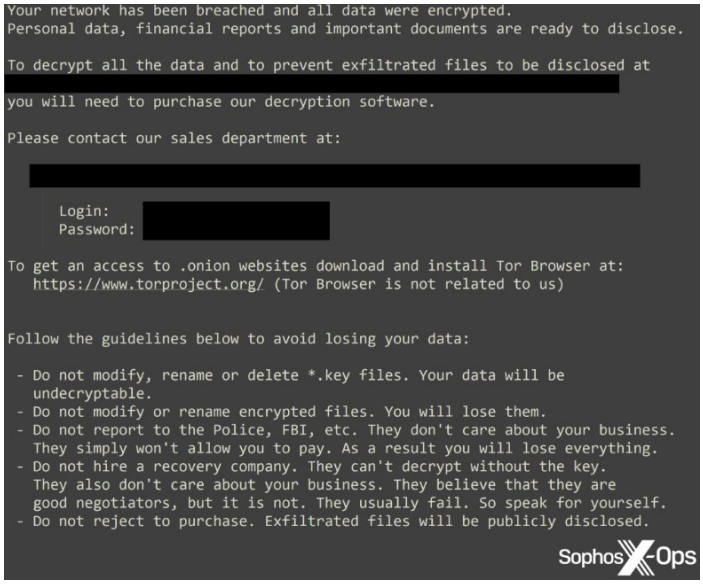


در این مرحله، تیم فناوری اطلاعات سازمان، اکثر سیستم‌های آلوده را تا ۱۰ اردیبهشت ۱۴۰۱ بازیابی کرد، یک روز قبل از اینکه مهاجمان Lockbit شروع به رمزگذاری فایل‌ها کنند. از منظر تحقیقاتی، این به معنای از بین رفتن برخی شواهد حیاتی بود. اما هنوز حملات تمام نشده بود.

تنها یک روز پس از بازیابی سیستم، مهاجمان ALPHV/BlackCat وارد عمل شدند و به واسطه بکارگیری پودمان RDP دقیقاً از همان سرور مدیریتی که توسط Lockbit و Hive مورد بهره‌جویی و حمله قرار گرفته به سازمان نفوذ و به Domain Controller، سرورهای فایل، سرورهای برنامه و سایر سرورها دست یافتند.

مهاجمان ALPHV/BlackCat داده‌ها را در طول یک هفته استخراج و به سرویس ذخیره‌سازی ابری Mega منتقل نمودند و با ایجاد یک دسترسی غیرمجاز (Back door) - یک ابزار دسترسی از راه دور معتبر به نام Atera Agent - ماندگاری خود را تثبیت کردند.

دو هفته پس از حملات Lockbit و Hive در ۲۵ اردیبهشت ۱۴۰۱، مهاجمان باج‌افزار ALPHV/BlackCat با استفاده از اطلاعات اصالت‌سنجی یک کاربر هک شده، فایل‌های اجرایی مخرب fXXX.exe و fXX.exe را بر روی شش سرور قرر داده و یک اطلاعیه باج‌گیری با عنوان RECOVER-eprzzxl-FILES.txt در هر پوشه بر جای گذاشتند.



تحلیل محققان SophosLabs، حاکی از آن است که این باینری‌های مخرب نه تنها فایل‌ها را رمزگذاری می‌کنند، بلکه Shadow Copy و لاگ‌های مربوط به رویدادهای رخ داده در Windows را نیز حذف می‌کنند؛ این امر روند آتی تحقیقات را پیچیده‌تر نمود زیرا مهاجمان ALPHV/BlackCat نه تنها گزارش لاگ‌های مربوط به حمله خود، بلکه موارد مربوط به حملات باج‌افزارهای Lockbit و Hive را نیز پاک کردند.

مشخص نیست که چرا باج‌افزارهای Lockbit و ALPHV/BlackCat هر کدام دو فایل اجرایی مخرب را مستقر کرده‌اند اما یکی از دلایل احتمالی آن تحمل‌پذیری خطا (Fault Tolerance) است؛ به این معنی که چنانچه یک فایل اجرایی شناسایی یا مسدود شود یا موفق به رمزگذاری فایل‌های سیستم نشود، دومی به عنوان پشتیبان عمل کند.

قابلیت‌های کلیدی باج‌افزار BlackCat

دو فایل اجرایی مخرب باج‌افزار BlackCat - fXXX.exe و fXX.exe - دارای قابلیت زیر هستند:

- فایل‌ها را رمزگذاری کرده و پسوند eprzzxl. را به آن اضافه می‌کند.
- شناسه‌های Universally Unique Ids - به اختصار UUIDs - را از دستگاه‌های آلوده شده استخراج می‌نماید:

```
wmic csproduct get UUID
```

- قابلیت Remote to Local و Remote to Remote را فعال نموده تا امکان دسترسی آسان به فایل‌ها و پوشه‌ها از مکان‌های راه دور فراهم شود:

```
fsutil behavior set SymlinkEvaluation R2L:1
fsutil behavior set SymlinkEvaluation R2R:1
```

- یک کلید Registry را با فرمان زیر تغییر داده تا امکان اجرای حداکثر تعداد درخواست‌های شبکه توسط پروسه‌های راه دور مجاز و قابل انجام باشد:

```
reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters /v MaxMpxCt
/d 65535 /t REG_DWORD /f
```

- نسخ Shadow Copy را حذف می‌نماید:

```
vssadmin.exe Delete Shadows /all /quiet
```

- با استفاده از فرمان زیر تعمیر و پاکسازی خودکار Windows را در دستگاه‌های آسیب‌پذیر غیرفعال می‌کند.

```
bcdedit /set {default} recoveryenabled No
```

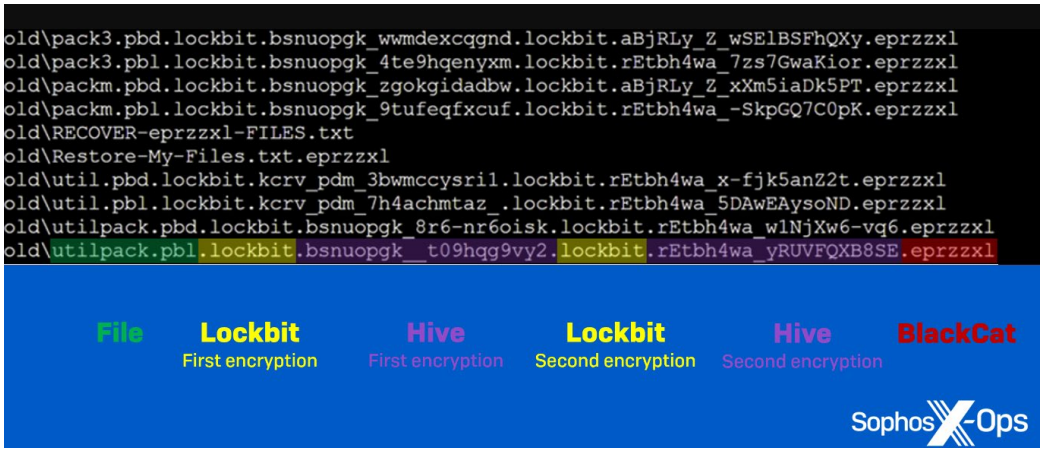
- لاگ مربوط به رویدادهای Windows را پاک می‌کند.

```
cmd.exe /c for /F \"tokens=*\" %1 in ('wevtutil.exe el') DO wevtutil.exe cl \"%1\"
```

پیامدهای بعدی

پس از نصب فایل‌های اجرایی مخرب، محققان سوفوس فایل‌هایی را شناسایی نمودند که توسط هر سه گروه باج‌افزاری رمزگذاری شده بودند؛ در واقع، همانطور که در تصویر نشان داده شده، برخی از فایل ها حتی پنج بار رمزگذاری شده بودند!

از آنجایی که حمله باج‌افزار Hive، ۲ ساعت پس از حمله باج‌افزار Lockbit شروع شد، باج‌افزار Lockbit همچنان در حال اجرا بود، بنابراین هر دو گروه به یافتن فایل‌ها ادامه دادند بدون اینکه بر روی فایل‌های رمزگذاری شده پسوندی قرار دهند.



با این حال، علی‌رغم اینکه هر سه گروه باج‌افزاری به بکارگیری تکنیک‌های «اخاذی مضاعف» (Double Extortion Technique) شناخته می‌شوند - در این تکنیک مهاجمان علاوه بر رمزگذاری فایل‌ها، تهدید می‌کنند که در صورت عدم پرداخت باج مطالبه شده، اقدام به انتشار داده‌های قربانی خواهند کرد - هیچ یک از اطلاعات سرقتی در این حملات منتشر نشد.

مواردی نظیر بازیابی سیستم، پاک کردن لاگ‌های BlackCat، فقدان لاگ‌های DHCP و تلفیق این سه حمله همگی موجب شدند که تحلیل حملات سه‌گانه برای محققان سوفوس دشوار شود.

علیرغم این چالش‌ها، تیم امنیتی سوفوس توانست شواهد به جا مانده را جمع‌آوری و تحلیل کند.

وقتی صحبت از دفاع به میان می‌آید، دو مورد همواره باید مورد توجه قرار گیرد: پیشگیری (بکارگیری از بهترین راهکارهای امنیتی برای به حداقل رساندن خطر حملات) و واکنش و پاسخ‌دهی (نحوه بازیابی سریع و ایمن در صورت وقوع حمله).

در بخش پیشگیری (Proactive)، در این مقاله بهترین راهکارها به طور کامل تشریح شده که در ادامه به مهمترین آنها می‌پردازیم:

1. به‌روزرسانی و اعمال وصله‌ها

همواره سیستم‌عامل Windows و سایر نرم‌افزارها را به‌روز نگه دارید (و هشدارها را جهت اطلاع‌رسانی در خصوص آسیب‌پذیری‌ها تنظیم کنید و منابع خبری را دنبال نمائید تا از اخبار جدید ضعف‌های امنیتی و باگ‌ها مطلع باشید).

همچنین بررسی کنید که آیا وصله‌های امنیتی به درستی نصب شده‌اند و برای سیستم‌های حیاتی نظیر سیستم‌های متصل به اینترنت یا Domain Controller اعمال شده‌اند یا خیر.

اعمال وصله‌ها در اسرع وقت، بهترین راهکار جهت جلوگیری از حملات در آینده است اما به این معنی نیست که قبلاً مورد حمله قرار نگرفته‌اید. توصیه می‌شود اطمینان حاصل نمائید که سازمان شما قبل از اجرای وصله‌ها مورد نفوذ قرار نگرفته باشد.

مهاجمان ممکن است دسترسی‌های غیرمجاز (که ممکن است شامل نصب نرم‌افزارهای معتبر و متداول باشد) را غیرفعال کنند یا آسیب‌پذیری‌های جدیدی را عمداً یا سهوا معرفی کنند، بنابراین این نکته‌ای کلیدی جهت واکنش و پاسخ به حملات احتمالی بعدی است.

2. مسدودسازی سرویس‌های قابل دسترس

شبکه سازمان خود را از بیرون پویش کنید و درگاه‌هایی را که معمولاً توسط VNC، RDP یا سایر ابزارهای دسترسی از راه دور استفاده می‌شود، شناسایی و مسدود نمائید. اگر سیستمی باید با بکارگیری ابزار مدیریت از راه دور قابل دسترس باشد، آن ابزار را از طریق VPN یا یک راهکار امنیتی موسوم به اعتماد صفر (Zero-trust) که از MFA برای ورود به سیستم خود استفاده می‌کند، در دسترس قرار دهید.

همچنین لازم به یادآوری است که حملات می‌توانند بیش از یک بار اتفاق بیفتند. اگر یک نقطه دسترسی باز بماند، سایر مهاجمان احتمالاً آن را شناسایی کرده و از آن بهره‌جویی می‌کنند.

3. تقسیم بندی شبکه و بکارگیری رویکرد اعتماد صفر

سرورهای مهم را از یکدیگر و از ایستگاه‌های کاری با قرار دادن آنها در VLAN مجزا جدا و تقسیم‌بندی کنید و به این ترتیب از یک مدل اعتماد صفر (Zero-trust) در شبکه استفاده کنید.

4. بکارگیری رمزهای عبور قوی و استفاده از احراز هویت چندعاملی

رمزهای عبور قوی به عنوان یکی از اولین خطوط دفاعی محسوب می‌شوند. تمامی رمزهای عبور باید منحصر به فرد و پیچیده باشند و هرگز مجدد مورد استفاده قرار نگیرند. چنانچه یک نرم‌افزار مدیریت رمز عبور را جهت ذخیره اطلاعات اصالت‌سنجی در اختیار کارکنان قرار دهید، انجام این کار آسان‌تر خواهد بود. با این وجود حتی رمزهای عبور قوی نیز ممکن است مورد سرقت قرار بگیرند و افشاء شوند.

استفاده از احراز هویت چند عاملی (Multifactor Authentication – به اختصار MFA) جهت ایمن‌سازی دسترسی به منابع مهم نظیر ایمیل، ابزارهای مدیریت از راه دور و دارایی‌های شبکه بهتر از عدم بکارگیری MFA است.

5. ایجاد فهرستی از تجهیزات و حساب‌های کاربری

دستگاه‌های محافظت‌نشده و وصله‌نشده در شبکه موجب افزایش تهدیدات می‌شوند و موقعیتی را ایجاد می‌کنند که در آن فعالیت‌های مخرب ممکن است مورد توجه قرار نگیرند.

داشتن فهرستی از موجودی فعلی سازمان یعنی تمام کامپیوترهای متصل به شبکه و دستگاه‌های IoT حیاتی است. بدین منظور می‌توانید از پویش‌های شبکه و بررسی فیزیکی جهت مکان‌یابی و فهرست‌بندی آنها استفاده کنید.

به منظور مسدودسازی مهاجمان در نقاط مختلف، از راهکارهای امنیتی چند لایه استفاده کنید. این محصولات امنیت را در تمام نقاط پایانی شبکه خود گسترش دهید.

در عین حال هنگامی که مهاجمان داخل یک شبکه باشند، بدون داشتن برنامه‌ای جامع جهت واکنش به رویدادها، کاهش و انجام اقدامات فوری، کار زیادی نمی‌توان برای «توقف آلوگی» انجام داد.

نشانه‌های آلودگی (Indicators of Compromise – به اختصار IoC) مربوط به باج‌افزارهای Lockbit، Hive و BlackCat در نشانی‌های زیر قابل دریافت می‌باشد:

https://github.com/sophoslabs/IoCs/blob/master/Ransomware_BlackCat%20-%20triple%20ransomware%20attack.csv

https://github.com/sophoslabs/IoCs/blob/master/Ransomware_Hive%20-%20triple%20ransomware%20attack.csv

https://github.com/sophoslabs/IoCs/blob/master/Ransomware_Lockbit%20-%20triple%20ransomware%20attack.csv

منبع

https://news.sophos.com/en-us/2022/08/10/lockbit-hive-and-blackcat-attack-automotive-supplier-in-triple-ransomware-attack/

بررسی تهدیدات سایبری
در گزارش فصلی ترلیکس

این اولین گزارش فصلی ترلیکس است که توسط مرکز تحقیقات پیشرفته این شرکت (Trellix Advanced Research Center) ارائه می‌شود.

راه‌اندازی مرکز تحقیقات پیشرفته ترلیکس در تابستان امسال نقطه عطف مهمی در مسیر حرکت شرکت نوظهور ترلیکس است. این مرکز، متشکل از صدها تحلیلگر و محقق امنیتی نخبه، عهده‌دار مسئولیت کمک به مشتریان در شناسایی جدیدترین تهدیدات امنیت سایبری و پاسخگویی مؤثر به آنها است.

در این گزارش به بررسی تهدیدات سایبری در سه‌ماهه سوم ۲۰۲۲ پرداخته شده است.

تهدیدات سایبری در بازه زمانی مذکور همچنان خبرساز بودند. همان طور که در این گزارش خواهید خواند در سه‌ماهه سوم شاهد تشدید رویدادهای سایبری، افزایش پیچیدگی فنی حملات و تأثیرات آنها بر روی حوزه‌های اقتصادی و ژئوپلیتیکی بودیم.

در سه‌ماهه سوم، باج‌افزار LockBit بیشترین انتشار را در مقایسه با هم‌قطاران خود داشته است. Cobalt Strike و Mimikatz نیز پراستفاده‌ترین ابزارهای مخرب در این دوره بوده‌اند.

بررسی‌های مرکز تحقیقات پیشرفته ترلیکس نشان می‌دهد که Mustang Panda، فعال‌ترین گروه APT در سه‌ماهه سوم ۲۰۲۲ بوده است. APT29 و APT36 از دیگر گروه‌های فعال در دوره مذکور بودند که در گزارش ترلیکس به ترتیب در جایگاه دوم و سوم قرار گرفته‌اند.

همچون دوره‌های قبلی در این گزارش نیز آماری از روش مخرب "کسب روزی از زمین" (Living off the Land - به اختصار LotL) پرداخته شده است. در روش LotL مهاجمان از برنامه‌های عادی و سالم در سیستم قربانی برای انجام عملیات مخرب خود بر روی آن دستگاه استفاده می‌کنند. بدیهی است که این روش برای مخفی ماندن عملیات مخرب و شناسایی نشدن حملات بسیار مؤثر است. بر طبق گزارش ترلیکس، دو پروسه معتبر CMD و PowerShell بیشترین سهم بهره‌جویی توسط مهاجمان را به خود اختصاص داده‌اند.

در بخشی دیگر از این گزارش نیز اصلی‌ترین تهدیدات مبتنی بر ایمیل در سه‌ماهه سوم ۲۰۲۲ مورد بررسی قرار گرفته است.

ادغام شرکت مک‌آفی اینترپرایز (McAfee Enterprise) و شرکت فایرآی (FireEye) به‌عنوان دو قدرت امنیت فناوری اطلاعات تحت برند ترلیکس که در اواخر سال گذشته رخ داد نویدبخش آینده‌ای روشن در مقابله با تهدیدات سایبری است. ضمن آن که اطلاعات انبوه شرکت جدید ترلیکس و دامنه گسترده محصولات و مشتریان آن در سرتاسر جهان چشم‌اندازی دقیق را از وضعیت تهدیدات سایبری فراهم می‌کند.

برای دریافت این گزارش بر روی تصویر زیر کلیک نمایید.

گزارش ماه دسامبر بیت‌دیفندر

در خصوص تهدیدات سایبری

شرکت بیت‌دیفندر (Bitdefender) گزارش ماه دسامبر خود را در خصوص تهدیدات سایبری منتشر کرد. در این گزارش ضمن مرور برخی تکنیک‌های مورد استفاده مهاجمان سایبری، خلاصه‌ای از آمار بدافزارهایی همچون باج‌افزارها نیز ارائه شده است.

در بخشی از این گزارش به بررسی جزییات یک آسیب‌پذیری در برخی راهکارهای موسوم به Endpoint Detection and Response - به اختصار EDR - پرداخته شده است.

این آسیب‌پذیری که به Aikido معروف شده، امکان معدوم‌سازی (Wipe) داده‌ها را از طریق EDR نصب‌شده بر روی دستگاه برای مهاجم فراهم می‌کند.

در کنفرانس Blackhat سال ۲۰۲۲ با ارائه نمونه اثبات‌گر (PoC) آسیب‌پذیری مذکور، نشان داده شد که چگونه دسترسی کاربر غیرمجاز می‌تواند بخش حسگر EDR را برای پاک کردن فایل‌های روی سیستم دستکاری کند.

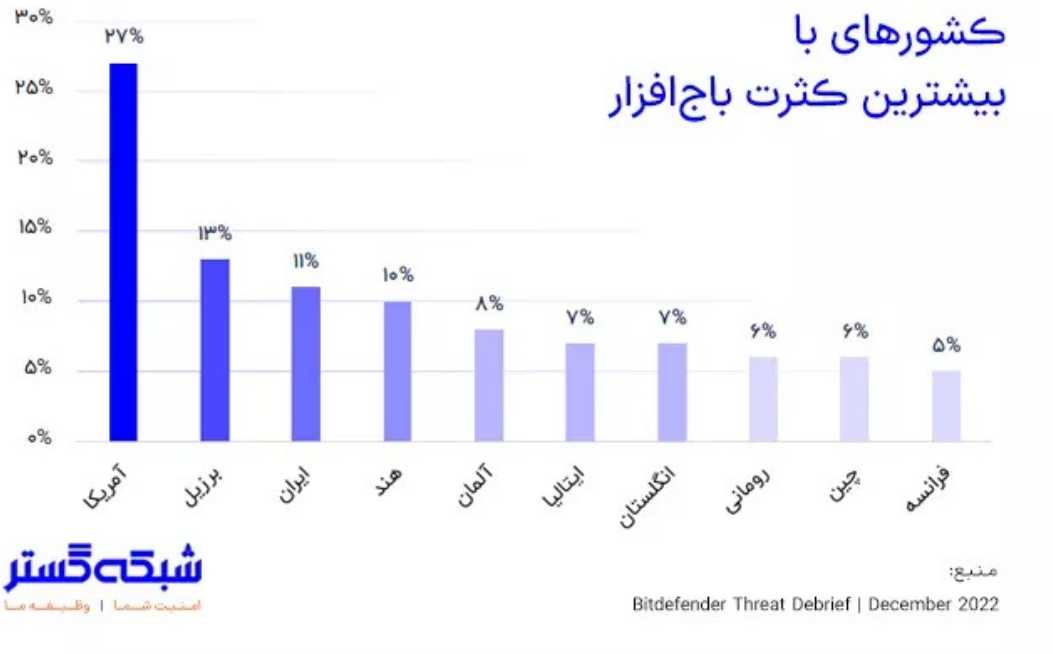
توضیح این که راهکارهای EDR توسعه داده شده توسط شرکت‌های بیت‌دیفندر و مک‌آفی (McAfee) به Aikido آسیب‌پذیر نیستند.

بر طبق گزارش ماه دسامبر بیت‌دیفندر، در بازه ۱۰ آبان تا ۹ آذر ۱۴۰۱، دو باج‌افزار WannaCry و GandCrab به ترتیب با ۵۲ و ۱۳ درصد، بیشترین انتشار را در مقایسه با سایر باج‌افزارها داشته‌اند.

به گزارش شرکت مهندسی شبکه گستر، باج‌افزار WannaCry در اردیبهشت ۱۳۹۶ در مدتی بسیار کوتاه با سوءاستفاده از یک آسیب‌پذیری شناخته شده صدها هزار دستگاه را در سطح جهان به خود آلوده کرد. با این توضیح که مایکروسافت، آسیب‌پذیری مذکور، معروف به EternalBlue را سه ماه پیش از گسترش این باج‌افزار توسط اصلاحیه MS17-010 برطرف کرده بود. به عبارت دیگر کوتاهی کاربران در نصب اصلاحیه مذکور منجر به آلودگی دستگاه‌ها به WannaCry شد.

علیرغم گذشت بیش از نیم‌دهه از شناسایی WannaCry و اطلاع‌رسانی‌های گسترده‌ای در خصوص لزوم نصب اصلاحیه MS17-010 به‌عنوان راهکاری برای مقابله با این باج‌افزار، WannaCry همچنان در کشورهای مختلف از جمله ایران قربانی می‌گیرد.

همچنین در گزارش بیت‌دیفندر، ایران، بعد از آمریکا و برزیل، در جایگاه سوم کشورهای با بیشترین تعداد شناسایی باج‌افزار قرار گرفته است.



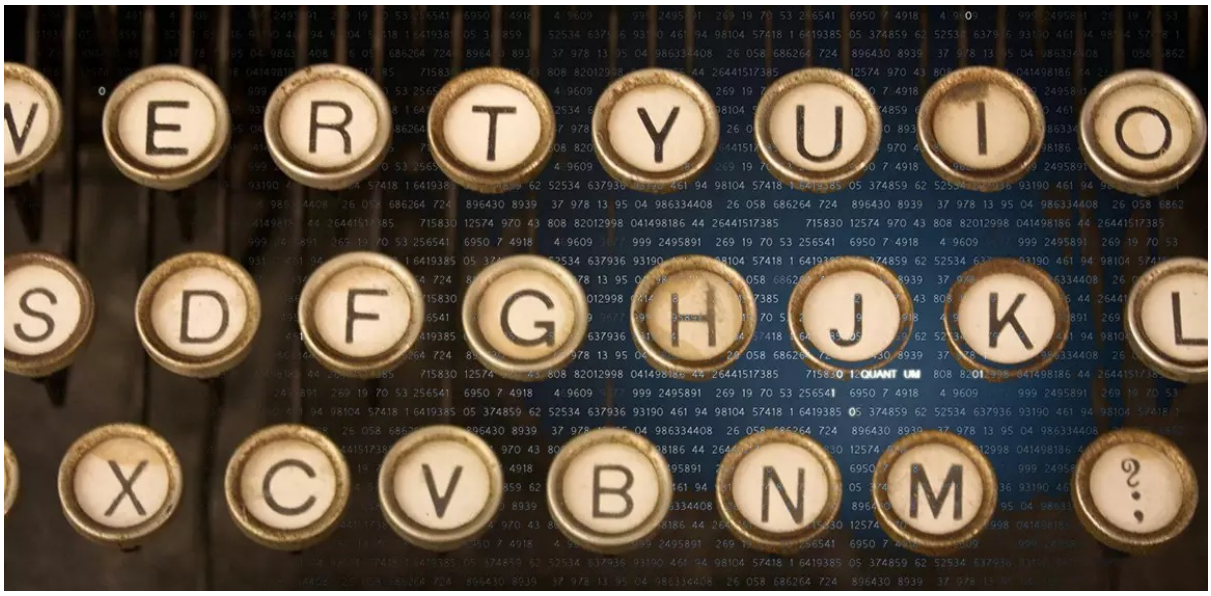
مؤثرترین راهکار در مقابله با تهدیدات مخرب باج‌افزاری، پیشگیری از ورود آنها به سازمان است. بر طبق گزارش بیت‌دیفندر مهاجمان اغلب از تکنیک موسوم به "فیشینگ نیزه‌ای" (Spear Phishing) به منظور نفوذ اولیه دستگاه قربانیان به باج‌افزار بهره می‌گیرند. آگاهی‌بخشی کارکنان نقشی کلیدی در خنثی‌سازی این تکنیک دارد.

مشروح گزارش بیت‌دیفندر با عنوان Bitdefender Threat Debrief در لینک زیر قابل دریافت و مطالعه است:

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

نگاهی به بدترین رمزهای عبور

سال ۲۰۲۲



آیا از رمزهای عبوری استفاده می‌کنید که بسیاری دیگر هچون شما از آن‌ها استفاده می‌کنند؟ اگر این‌طور است به شما هشدار می‌دهیم که احتمال هک شدن آن‌ها بسیار بالا است.

هک رمزهای عبور همچنان از اصلی‌ترین راه‌های نفوذ مهاجمان به حساب‌های آنلاین محسوب می‌شود.

شرکت NordPass فهرستی از رایج‌ترین رمزهای عبور را که کاربران در سال ۲۰۲۲ از آن‌ها استفاده می‌کردند منتشر کرده است. این فهرست که در اینجا قابل دسترس است حاوی ۲۰۰ رمز عبور متداول است.

فهرست مذکور حاصل از ارزیابی یک بانک داده ۳ ترابایتی توسط محققان امنیتی مستقل است.

از آنجا که هک رمزهای عبور یک خطر امنیتی بزرگ است، چنانچه رمز عبور شما در این فهرست قرار دارد، توصیه می‌کنیم پیش از آنکه خیلی دیر شود فوراً نسبت به تغییر آن در تمامی حساب‌های کاربری خود اقدام کنید.

بر طبق گزارشی که در تابستان امسال منتشر شد ۲۴ میلیارد نام کاربری و رمز عبور در بازارهای زیرزمینی تبهکاران سایبری در حال تبادل و خریدوفروش شدن است. آماری که در مقایسه با سال قبل از آن ۶۵ درصد افزایش داشته است.

مهاجمان از روش‌های مختلفی برای دستیابی به رمز عبور کاربران استفاده می‌کنند:

فیشینگ: یکی از قدیمی‌ترین ترفندهای موجود، کلاهبرداری از طریق ایمیل، پیامک یا تلفن است که از آن به فیشینگ (Phishing) یاد می‌شود؛ در این حمله مهاجمان تظاهر می‌کنند که از سوی یک نهاد معتبر و قانونی تماس گرفته‌اند. به طور معمول آنها شما را ترغیب می‌کنند که نام کاربری و سایر جزئیات خود را در وب‌سایتی که در کنترل آن‌هاست وارد کنید.

حملات سعی و خطا: هکرها با بکارگیری ابزارهای خودکار در حملات موسوم به سعی و خطا (Brute Force) تلاش می‌کنند با آزمون و خطا به حساب‌های کاربری نفوذ کنند. آنها اغلب رمزهای عبور رایج را وارد می‌کنند تا ببینند کدام یک از آنها با آن رمز عبور مطابقت دارند.

سناریوهای پر کردن اطلاعات اصالت‌سنجی: سناریوهای پر کردن اطلاعات اصالت‌سنجی (Credential Stuffing)، نوعی حمله سعی و خطا است که در آن هکرها از رمزهای عبوری که پیش‌تر سرقت یا افشا شده‌اند استفاده می‌کنند. مهاجمان، در این روش، معمولاً از طریق اسکریپت‌های خودکار قابل استفاده بودن این رمزهای عبور را بر روی وب‌سایت‌ها و سرویس‌های آنلاین بررسی و امتحان می‌کنند.

کی لاگرها: کی لاگرها/ سارقان اطلاعات (Keylogger/info-stealer) نوعی بدافزار هستند که کلیدهای فشرده شده توسط کاربر را ضبط و به مهاجم ارسال می‌کنند.

نگاه از پشت: نگاه از پشت یا سرقت رمز عبور با نگاه به دست کاربر (Shoulder Surfing)، نوعی از حملات مهندسی اجتماعی است که به کسب اطلاعات شخصی یا خصوصی از طریق مشاهده مستقیم اشاره دارد. کاربران هنگام ورود نام کاربری و رمز عبور یا هنگام دسترسی به داده‌های حساس باید همیشه مراقب محیط اطراف خود باشند.

هکرها می‌توانند پس از ورود به حساب کاربری دست به هر اقدامی که کاربر هک‌شده مجوز انجام آن را دارد بزنند. میزان تراکنش‌های جعلی مربوط به کارت‌های پرداخت در سال ۲۰۲۱ از ۳۲ میلیارد دلار فراتر رفت و پیش‌بینی می‌شود تا سال ۲۰۲۷ به ۳۸/۵ میلیارد دلار افزایش یابد.

۲۰ رمز عبور رایج در سال ۲۰۲۲

متأسفانه، بسیاری از کاربران اینترنت، حملات را برای تبهکاران سایبری آسان‌تر می‌کنند. در فهرست NordPass کلمه «password» با نزدیک به پنج میلیون تکرار پر استفاده‌ترین رمز عبور در سال ۲۰۲۲ بوده است. در رتبه دوم «۱۲۳۴۵۶» و پس از آن «۱۲۱۲۳۴۵۶۷۸۹» قرار دارد. در رتبه‌های چهارم و پنجم رمزهای عبور متداول «guest» و «qwerty» قرار داشتند.

Position	Password	Position	Password
1	password	11	1234567
2	123456	12	1234
3	12123456789	13	1234567890
4	guest	14	000000
5	qwerty	15	555555
6	12345678	16	666666
7	111111	17	123321
8	12345	18	654321
9	col123456	19	7777777
10	123123	20	123

علاوه بر متداول‌ترین رمزهای عبور نشان داده شده در جدول، محققان هر ساله الگوهای مشابهی را در رمزهای عبور مشاهده نموده‌اند. در ادامه به فهرستی از مواردی که در تمامی زمان‌ها مورد علاقه کاربران است، می‌پردازیم:

- **تیم‌های ورزشی**: به عنوان مثال، استفاده از نام تیم‌های فوتبال نظیر «Red Star Belgrade» که تعداد آن بیش از ۵۸/۵ میلیون بار بوده است.
- **برندهای مد**: برندهای مد و فشن مانند «tiffany» که تقریباً ۱۴/۸ میلیون بار استفاده شده است.
- **ناسزا**: بیش از ۲۱ میلیون بار از دشنام‌ها به عنوان رمزهای عبور استفاده کرده‌اند.
- **هنرمندان**: با بیش از ۳۳ میلیون مورد، U2 در صدر قرار گرفته است.
- **فیلم‌ها**: محبوب‌ترین آنها «Leon» با ۶/۴ میلیون رمز عبور می‌باشد.
- **خودروها**: بیش از هشت میلیون کاربر رمز عبور خود را «mini» گذاشتند.
- **بازی‌های ویدیویی**: محبوب‌ترین بازی در سال ۲۰۲۲، «arma» با بیش از ۶/۲ میلیون کاربر بوده است.
- **غذا**: تقریباً ۸/۶ میلیون بار از کلمه «fish» برای رمز عبور استفاده شده است.

حتی بدتر از آن این که چنانچه از این رمزهای عبور مجدداً استفاده کنیم، آن‌ها را در محیط‌های عمومی یادداشت کنیم یا با دیگران به اشتراک بگذاریم، نفوذ برای هکرها و کلاهبرداران احتمالی آسان‌تر خواهد شد. اگر در محل کار رمزهای عبور مشابه با رمزهای شخصی خود بکار بگیریم، حتی ممکن است کل سازمان را در معرض حمله سایبری قرار دهیم.

نحوه انتخاب رمزهای عبور امن

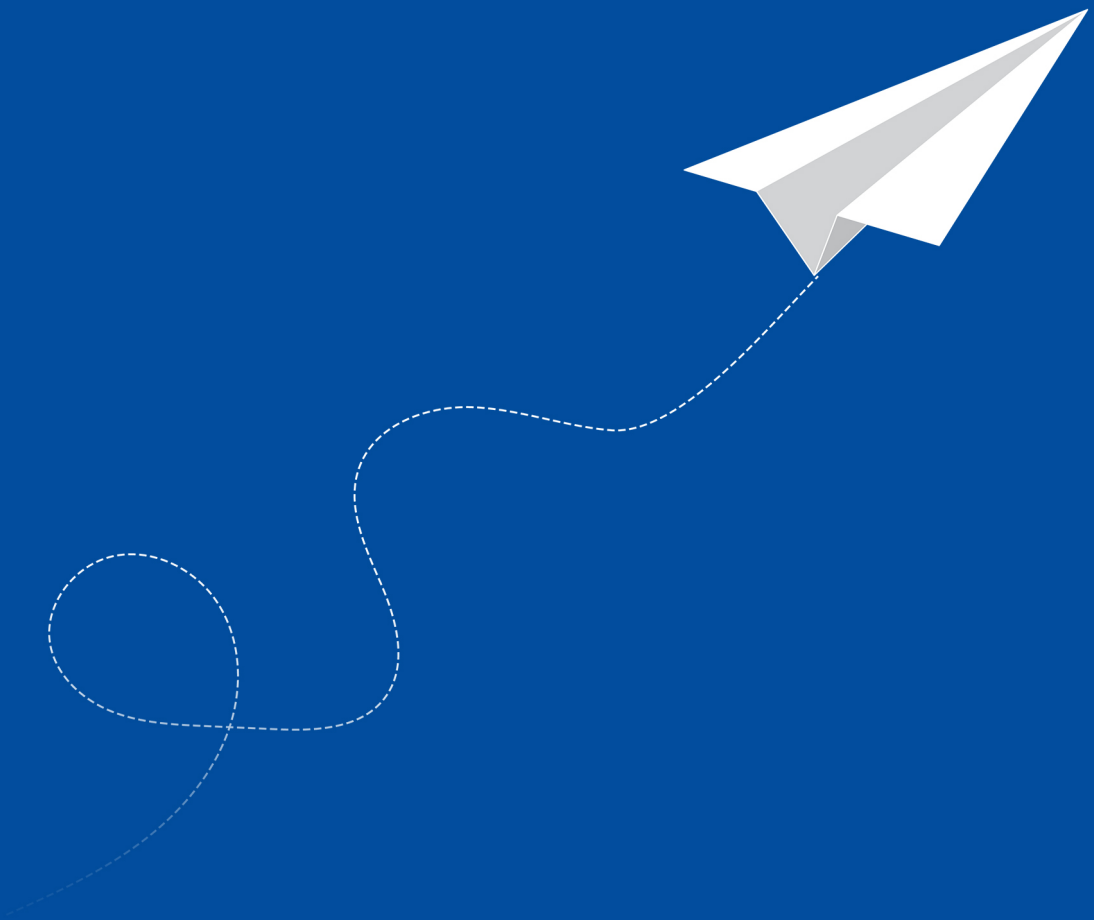
خوشبختانه، بکارگیری رمزهای عبور امن یکی از ساده‌ترین چیزهایی است که می‌توانیم در زندگی دیجیتالی خود از آن استفاده کنیم. توصیه می‌شود نکات زیر را جهت انتخاب رمزهای عبور و کمک به محافظت از اطلاعات شخصی و مالی خود در نظر بگیرید:

- همیشه از گذرواژه‌ها یا رمزهای عبور پیچیده و منحصربه‌فرد استفاده کنید؛ به این ترتیب، حدس زدن آن‌ها یا سناریوهای پر کردن اطلاعات اصالت‌سنجی برای هکرها سخت‌تر خواهد بود.
- هرگز از رمزهای عبور مجدداً استفاده نکنید و یا یک رمز عبور را برای چند حساب کاربری بکار نبرید. در صورت استفاده از یک رمز عبور برای چند حساب کاربری، در صورت کشف آن توسط مهاجمان، قادر خواهند بود به تمامی حساب‌های شما نفوذ کنند.
- رمزهای عبور خود را به اشتراک نگذارید زیرا دیگران ممکن است از آنها حتی سهواً سوءاستفاده کنند.
- قدرت و پیچیدگی رمزهای عبور خود را بررسی کنید و هر کدام را که خیلی ضعیف یا قدیمی است، به‌روز کنید.
- در صورت امکان، احراز هویت چندعاملی (Multifactor Authentication – به اختصار MFA) را برای حساب کاربری خود فعال کنید. اکثر حساب‌های کاربری گزینه‌ای برای انجام این کار دارند. با MFA، یک لایه امنیتی مضاعف به رمزهای عبور اضافه می‌شود. این لایه امنیتی ممکن است پویش چهره، اثر انگشت یا یک رمز عبور یکبار مصرف باشد.
- از طریق Wi-Fi عمومی وارد سیستم نشوید زیرا استراق سمع دیجیتالی در آن شبکه ممکن است منجر به سرقت یا افشای رمز عبور شما شود.
- از راهکارهای امنیتی و ضدویروس یک شرکت معتبر جهت محافظت در برابر سارقان اطلاعات، بدافزارها و همچنین در برابر حملات فیشینگ و به طور کلی تهدیدات سایبری استفاده کنید.

- مواظب تهدیدات موسوم به نگاه از پشت - سرقت رمز عبور با نگاه به دست کاربر - (Shoulder Surfing)، خصوصاً در محیط‌های بیرون باشید.
- بر روی لینک‌های مشکوک در ایمیل‌ها و متن‌های آن کلیک نکنید.
- فقط با استفاده از HTTPS وارد سایت‌ها شوید زیرا این سایت‌ها ایمن هستند و بنابراین محافظت بیشتری در برابر حملات سایبری ارائه می‌دهند.

منبع

https://www.welivesecurity.com/2023/01/02/most-common-passwords-what-do-if-yours-list/



اطلاعات فناوری امنیت اخبار آخرین

@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.

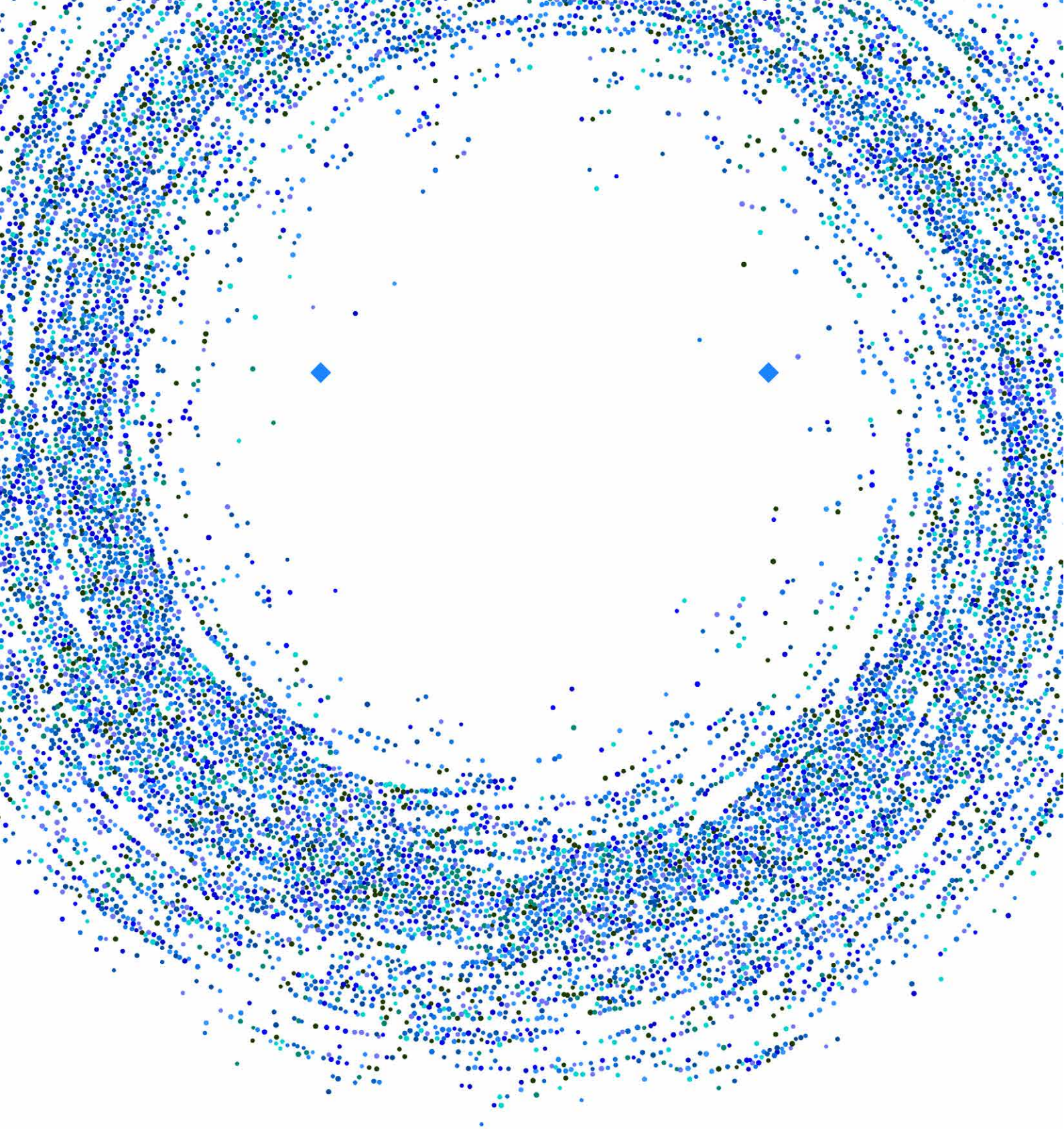
در ابتدا، همکاری مشترکی بین شرکت مهندسی شبکه گستر و شرکت انگلیسی S & S International سازنده ضدویروس مشهور (سازنده ضدویروس مشهور Toolkit) آغاز گردید. در مدت کوتاهی، با فعالیت شبکه گستر به‌عنوان نماینده رسمی و انحصاریS & S International، به‌تدریج ضدویروس Dr Solomon’s Toolkit به محبوب‌ترین ضدویروس در ایران 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 سازمانی ضدویروس McAfee ادامه داد. اخیراً بخش خدمات و محصولات سازمانی McAfee به همراه شرکت FireEye توسط گروه سرمایه‌گذاری STG خریداری و در هم ادغام شدند و اکنون این دو غول امنیت فناوری اطلاعات تحت نام Trellix در حال گذار و یکپارچه‌سازی محصولات دو شرکت تحت نام جدید هستند. در سال ۱۳۸٤ 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 نقل‌وانتقال، شرکت مهندسی شبکه گستر با همکاری شرکت Sophos، فعالیت خود را در این زمینه ادامه داد 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 به‌عنوان نماینده توزیع (Distributor) رسمی در ایران آغاز کرد. عرضه محصولات ضدویروس Bitdefender در کنار محصولات امنیتی McAfee سابق، 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.

سال ۱٤۰۰ برخی ملاحظات ملی و بین‌المللی و همچنین جایگاه ثابت شرکت Kaspersky در بین دیگر شرکت‌های ضدویروس رده اول جهان، آغازگر توجه شبکه گستر به این شرکت امنیتی بوده است. اکنون شرکت مهندسی شبکه گستر در قالب همکاری رسمی، محصولات و خدمات شرکت Kaspersky نیز را به کاربران ایرانی ارائه می‌نماید.

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 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