مهر

۱۳۹۹

ماهنامه

امنیت فناوری اطلاعات

شبکه گستر

امنیت شما | وظیفه ما

newsroom.shabakeh.net

@SGnewsroom

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 مهر ۱۳۹۹ پرداخته شده است.

بر اساس گزارش‌های واصله به شرکت مهندسی شبکه گستر، در هفته‌های اخیر برخی مؤسسات هدف حملاتی قرار گرفته‌اند که در جریان آنها مهاجمان با سوءاستفاده از آسیب‌پذیری CVE-2020-1472 - معروف به Zerologon - اقدام به توزیع باج‌افزارهای با عملکرد Wiper در شبکه اهداف خود می‌کنند. جزییات Zerologon و راه‌های مقابله با آن را در این ماهنامه بخوانید.

باج‌افزارها همچنان از جمله تهدیداتی هستند که فعالیت آنها در صدر اخبار امنیت فناوری اطلاعات قرار دارد. از جمله این اخبار می‌توان به واریز ۹۹ بیت‌کوین معادل حدود ۱ میلیون دلار به کیف ارز رمز یک تالار گفتگوی اینترنتی (Forum) هکرهای روسی‌زبان توسط گردانندگان باج‌افزار REvil که با نام Sodinokibi نیز شناخته می‌شود اشاره کرد. این تالار گفتگوی اینترنتی اعضا را قادر به واریز بیت‌کوین به کیف ارز رمز که در کنترل سایت است می‌کند تا از این طریق به‌عنوان واسطی برای خرید و فروش خدمات و اقلام غیرقانونی توسط اعضا عمل کند. گردانندگان REvil نیز برای نشان دادن جدیتشان در کسب‌وکار و همچنین پشتوانه مالی خود، این مبلغ هنگفت را در کیف ارز رمز مذکور واریز کردند.

یا در نمونه‌ای دیگر که در این ماهنامه به آن پرداخته شده، گردانندگان اسب‌تروای مشهور TrickBot در حال بهره‌گیری از مجموعه بدافزاری جدیدی با عنوان BazarLoader/BazarBackdoor در حمله به اهداف خاص و بااهمیت خود هستند. در جریان این حملات در نهایت سیستم‌های سازمان به باج‌افزار مخرب Ryuk آلوده می‌شوند.

اما خبر خوش در حوزه باج افزارها هم این که محققان موفق به ساخت ابزاری شده‌اند که قربانیان ThunderX را قادر به رمزگشایی رایگان فایل‌های رمز شده توسط این باج‌افزار می‌کند. جزییات این اخبار در این ماهنامه قابل مطالعه است.

همان طور که در این ماهنامه به تفصیل به آن پرداخته شده مهاجمان با تزریق کد مخرب به سرویس معتبر Windows Error Reporting - به اختصار WER - اقدام به اجرای حملات موسوم به "بدون فایل" (Fileless) کرده‌اند. این نخستین بار نیست که تاکتیک بهره‌جویی (Exploit) از سرویس WER مورد استفاده مهاجمان قرار می‌گیرد و پیش‌تر نیز در باج‌افزار Cerber و بدافزار NetWire RAT گزارش شده بود.

همچنین در مهر ماه، محققان جزییات روت‌کیتی مبتنی بر Unified Extensible Firmware Interface - به اختصار UEFI - را منتشر کردند که در جریان بررسی حملات اجرا شده در سال میلادی گذشته بر ضد دو سازمان موفق به کشف آن شده‌اند. این نوع بدافزارها با رخنه در ماژول حافظه Serial Peripheral Interface - به اختصار SPI - نه تنها در صورت تغییر سیستم عامل ماندگار می‌ماند که حتی جایگزینی دیسک سخت نیز تأثیری در حضور این بدافزار نخواهد داشت. مشروح گزارش این محققان در این ماهنامه ارائه شده است.
در مهر ۱۳۹۹، شرکت‌های موزیلا، سیسکو، اپل، گوگل، اس‌آپ، مایکروسافت، ادوبی، مک‌آفی، جونیپر نت‌ورکز، وی‌اِم‌وِر، اوراکل و بیت‌دیفندر و بنیاد نرم‌افزاری آپاچی برای برخی محصولات خود اصلاحیه و توصیه‌نامه امنیتی منتشر کردند که جزییات آنها 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 به‌عنوان یکی از اصلی‌ترین راهکارهای مقابله با تهدیدات سایبری توجه خاص داشته است. امید است مطالب ماهنامه امنیت فناوری اطلاعات شرکت مهندسی شبکه گستر که حاصل تحقیق و پژوهش کارشناسان این شرکت است راهنمایی برای ارتقای دانش کاربران این حوزه باشد.

آمار جهانی از نگاه مک‌آفی

McAfee™
Together is power.

۱۰ تهدید اصلی

باج‌افزار Phobos

این باج‌افزار اقدام به رمزگذاری فایل‌ها با استفاده از الگوریتم AES می‌کند. نخستین نسخه از Phobos در اواخر سال ۲۰۱۷ شناسایی شد و روند عرضه نسخ جدید آن تا اوایل سال ۲۰۱۹ ادامه داشت. روش برقراری ارتباط با مهاجمان در این باج‌افزار ایمیل است.

باج‌افزار ProLock

خانواده باج‌افزاری ProLock که از اوایل سال میلادی جاری ظهور به طور مستمر در حال تکامل خود است. روش رخنه گردانندگان آن به شبکه سازمان ها اجرای حملات "سعی‌وخطا" (Brute-force) بر ضد سرورهای RDP است. در مواردی نیز آلودگی دستگاه به اسب تروای QakBot منجر به اجرای این باج‌افزار می‌شود. QakBot از طریق کارزارهای فیشینگ با پیوست‌ها یا لینک‌های مخرب منتشر می شود. در کارزار ProLock کد مخرب از یک فایل CSV، BMP یا JPG توسط پروسه معتبر PowerShell استخراج شده و در حافظه اجرا می‌شود. در اطلاعیه باج‌گیری ProLock قربانی تهدید می‌شود که در صورت عدم پرداخت باج فایل‌های سرقت در شبکه‌های اجتماعی و رسانه‌های عمومی افشا خواهد شد.

باج‌افزار Lockbit

باج‌افزارLockBit که ظهور آن به اوایل سال ۲۰۲۰ باز می‌گردد در قالب یک سرویس جدید موسوم به "باج‌افزار به‌عنوان سرویس" (Ransomware-as-a-Service - به اختصار RaaS) به سایر تبهکاران سایبری اجاره داده می‌شود. قابلیتی در LockBit مهاجمان را قادر می‌سازد تا پس از رخنه به شبکه سازمان این باج‌افزار را در مدتی بسیار کوتاه بر روی صدها دستگاه توزیع و فایل‌های آنها را رمزگذاری کنند. گردانندگان این باج افزار در جریان حملات خود اقدام به سرقت اطلاعات سازمانی قربانی کرده و به ادعای مهاجمان عدم پرداخت باج در موعد مقرر منجر به افشای عمومی اطلاعات خواهد شد.

باج‌افزار Thanos

باج‌افزار Thanos در فوریه ۲۰۲۰ در تالارهای اینترنتی زیرزمینی تبهکاران به عنوان یک باج‌افزار سفارشی تبلیغ می‌شد. عرضه آن در بازار نشانه‌ای از مورد استفاده قرار گرفتن آن توسط مهاجمان مختلف است. بکارگیری این باج‌افزار در چندین حمله سایبری با حمایت دولتی به سازمان‌هایی در خاورمیانه و شمال آفریقا گزارش شده است.

بهره‌جویی از آسیب‌پذیری‌های VPN

گروهی از مهاجمان در حال سوءاستفاده از آسیب پذیری های

حمله به شبکه‌ها

گروهی از مهاجمان با استفاده از ابزارهای تجاری و کدباز شامل

شناخته شده در Pulse Secure VPN، Citrix NetScaler و F5 برای رخنه به شبکه های هستند. مهاجمان با ماندگار کردن خود اقدام به سرقت اطلاعات با استفاده از نگارش هایی ویرایش شده از ابزارهای کد باز می کنند.

شبکه‌ها Mimikatz ،China Chopper ،Cobalt Strike را مورد هدف قرار می‌دهند. نفوذ اولیه این مهاجمان نیز از طریق بهره‌جویی از آسیب‌پذیری‌های شناخته شده در F5 Big-IP، تجهیزات Citrix VPN و سرورهای Pulse VPN صورت می‌پذیرد. همچنین این مهاجمان با ارسال ایمیل‌های فیشینگ هدفمند (Spear phishing) کاربر را تشویق به کلیک بر روی لینک‌های مخرب درج شده در ایمیل می‌کنند. در جریان حملات این گروه اطلاعات حساسی نظیر ایمیل‌ها از سرورهای Exchange را جمع‌آوری شده و از طریق پراکسی به سرورهای فرماندهی ارسال می‌شود.

PyVil؛ ابزار جاسوسی جدید Evilnum

گروه Evilnum بدافزار جدیدی را توسعه داده که مهاجمان آن را قادر به سرقت نشانی‌های ایمیل، رمزهای عبور و اطلاعات حساس متعدد سازمانی می‌کند. حملات این گروه هدفمند و تمرکز اصلی آنها شرکت‌های فعال در حوزه فن‌آوری مالی (FinTech) بوده است. این بدافزار جدید که به PyVil معروف شده علاوه بر استخراج مشخصات دستگاه آلوده نظیر نسخه Windows و محصول ضدویروس نصب شده بر روی آن، قادر است که با ضبط کلیدهای فشرده شده توسط کاربر (Keylogging) و تصویربرداری از فعالیت‌های او انواع اطلاعات سازمانی را سرقت کند. ضمن اینکه امکان اجرای بدافزارهای مورد نظر مهاجمان را نیز بر روی دستگاه قربانی فراهم می‌کند. در اکثر حملات Evilnum، رخنه اولیه به سازمان، از طریق ایمیل‌های فیشینگ هدفمند صورت می‌پذیرد. پیوست این ایمیل ها فایلی با پسوند ZIP است.

آسیب‌پذیری CVE-2020-0688

ضعفی از نوع "اجرای کد به‌صورت از راه دور" (Remote Code Execution) است که از نحوه مدیریت اشیاء (Object) در حافظه توسط Microsoft Exchange ناشی می‌شود.

آسیب‌پذیری CVE-2020-16875

ضعفی در Microsoft Exchange است که بهره‌جویی از آن مهاجم را قادر به اجرای کد به‌صورت از راه دور با سطح دسترسی کاربر System می‌کند.

آسیب‌پذیری CVE-2020-1472

ضعفی با درجه حساسیت "حیاتی" است که پودمان Netlogon Remote Protocol از آن تأثیر می‌پذیرد. آسیب‌پذیری مذکور که ضعفی از نوع "ترفیع امتیازی" (Elevation of Privilege) تلقی می‌شود مهاجم را قادر به توزیع فایل مخرب بر روی یکی از دستگاه‌های شبکه می‌کند.

۱۰ بسته بهره‌جو با بیشترین استفاده

بسته بهره‌جو	توضیحات
Neutrino	Neutrino و هم‌قطار اسبقش (Neutrino-v) از بسته‌های بهره‌جوی (Exploit Kit) معروفی هستند که از اواسط سال ۲۰۱۶ ظهور کردند. از این بسته بهره‌جو عمدتاً در سایت‌های هک شده و کارزارهای تبلیغ‌افزار (Malvertising) برای آلوده‌سازی کاربران به بدافزارهای مختلف استفاده می‌شود. این بسته بهره‌جو از آسیب‌پذیری‌های CVE-2016-4117، CVE-2015-3113، CVE-2013-2551، CVE-2016-3298، CVE-2015-2419، CVE-2015-0311، CVE-2016-1019، CVE-2015-7645، CVE-2015-0313، CVE-2014-6332، CVE-2015-5119، CVE-2017-0022، CVE-2013-0074، CVE-2013-7331، CVE-2015-5122، CVE-2016-7200، CVE-2015-8651، CVE-2014-0515، CVE-2015-0359، CVE-2013-2423، CVE-2016-0189، CVE-2015-3090 و CVE-2016-7201 سوءاستفاده می‌کند. از جمله باج‌افزارهایی که از Neutrino در فرایند انتشار خود بهره گرفته‌اند می‌توان به PizzaCrypts، CryptFIle2، Cerber، CrypMIC، Locky، CryptoWall، TeslaCrypt، Zepto، CryptXXX و BandarChor اشاره کرد. همچنین از این بسته بهره‌جو در کارزارهای سایبری ShadowGate، Afraidgate و ProMediads استفاده شده است.
Magnitude	این بسته بهره‌جو که با نام Popads نیز شناخته می‌شود در جریان کارزارهای تبلیغ‌افزار برای آلوده‌سازی سیستم مراجعه‌کنندگان به سایت در کنترل مهاجمان مورد استفاده قرار می‌گیرد. Magnitude از آسیب‌پذیری‌های CVE-2016-4117، CVE-2018-4878، CVE-2015-0311، CVE-2012-0507، CVE-2015-7645، CVE-2015-5119، CVE-2013-2463، CVE-2015-8651، CVE-2015-0359، CVE-2015-3090، CVE-2018-8174، CVE-2015-3113، CVE-2013-2551، CVE-2015-1701، CVE-2015-2419، CVE-2016-1019، CVE-2015-2426، CVE-2015-3105 ، CVE-2013-0634، CVE-2015-3133، CVE-2015-1671، CVE-2014-8439، CVE-2013-2471، CVE-2015-5122 و CVE-2016-0189 سوءاستفاده می‌کند. از جمله باج‌افزارهایی که Magnitude را مورد استفاده قرار داده‌اند می‌توان به Cerber، Magniber، CryptoWall، Locky و GandCrab اشاره کرد.
RIG	این بسته بهره‌جو از طریق تبلیغات مخربی که توسط مهاجمان در سایت‌های معتبر تزریق شده‌اند سیستم کاربران را مورد دست‌درازی قرار می‌دهد. در نسخه موسوم به VIP آن با عنوان RIG-v که در سال 2016 ظهور کرد از الگوهای جدید URL استفاده می‌شود. RIG از آسیب‌پذیری‌های CVE-2016-4117، CVE-2016-0034، CVE-2016-3298، CVE-2018-4878، CVE-2013-3896، CVE-2015-0311، CVE-2012-0507، CVE-2015-7645، CVE-2015-5119 و CVE-2014-0322، CVE-2013-0074، CVE-2016-7200، CVE-2012-1723، CVE-2015-8651، CVE-2013-2423، CVE-2015-0359، CVE-2013-2465، CVE-2015-3090، CVE-2016-7201، CVE-2018-8174، CVE-2015-3113، CVE-2013-2551،

بسته بهره‌جو	توضیحات
	CVE-2013-1493، CVE-2015-2419، CVE-2014-0497، CVE-2016-1019، CVE-2013-0322، CVE-2014-0569، CVE-2014-6332، CVE-2013-0634، CVE-2013-7331، CVE-2015-5122، CVE-2014-0515 و CVE-2016-0189 سوءاستفاده می‌کند. از جمله باج‌افزارهایی که استفاده از RIG را در کارنامه دارند می‌توان به CryptFIle2، Sage،ASN1، CryptoShield، Nemty، CrypMIC، Mobef، Paradise، Dxh26wam، GandCrab Revenge، CryptoMix، BartCrypt، Spora، Erebus، Mole، Cry، FessLeak، Matrix، Sodinokibi، Cerber، Philadelphia، Locky، CryptoWall، Alma Locker، Fake Globe، Princess Locker، BandarChor، YafunnLocker، ERIS، Goopic، Radamant، CryptoMix، GetCrypt، AnteFrigus و Buran اشاره کرد. همچنین از این بسته بهره‌جو در کارزارهای سایبری Pitty Tiger، FormBook، Afraidgate، DragonFly، ProMediads و Deep Panda استفاده شده است.
ThreadKit	مهاجمان با درج کد این بسته بهره‌جو در اسناد مبتنی بر Microsoft Office از مجموعه‌ای از آسیب‌پذیری‌های مایکروسافت سوءاستفاده می‌کنند. این بسته بهره‌جو در بازارهای زیرزمینی تبهکاران سایبری در Dark Web به فروش می‌رسد. از ThreadKit در چندین بدافزار نظیر FormBook، Loki Bot، Trickbot و Chthonic استفاده شده است. CVE-2017-8759، CVE-2017-8570، CVE-2017-0199، CVE-2018-4878، CVE-2017-11882، CVE-2018-0802 و CVE-2018-8174 در ThreadKit مورد بهره‌جویی قرار می‌گیرند.
Underminer	Underminer با رمزگذاری RSA، از کدهای بهره‌جو و ترافیک ارتباطی با سرفرماندهی خود محافظت می‌کند. این بسته بهره جو با سوءاستفاده از باگ‌هایی در مرورگر Internet Explorer و نرم افزار Flash Player کاربران را به انواع بدافزارها از جمله استخراج‌کنندگان ارز رمز و بوت‌کیت‌ها آلوده می‌کند. در Underminer از CVE-2015-5119، CVE-2018-4878، CVE-2018-15982، CVE-2016-0189 و CVE-2018-8174 بهره‌جویی می‌شود.
Fallout	این بسته بهره‌جو که در آگوست 2018 شناسایی شد از باگ‌هایی در نرم‌افزار Flash Player و سیستم عامل Windows سوءاستفاده می‌کند. CVE-2018-4878، CVE-2018-15982 و CVE-2018-8174 فهرست باگ‌های مذکور را تشکیل می‌دهند. موفقیت در بهره‌جویی، مهاجم را قادر به دریافت کدهای مخرب بیشتر بر روی دستگاه قربانی می‌کند. از Fallout در باج‌افزارهای Stop، GandCrab 5، Kraken Cryptor، GandCrab، Maze، Fake Globe، Minotaur، Matrix و Sodinokibi استفاده شده است.
Spelevo	Spelevo در اوایل سال 2019 شناسایی شد. در این بسته بهره‌جو از آسیب‌پذیری CVE-2018-15982 در نرم‌افزار Flash Player و CVE-2018-8174 در بخش VBScript Engine سیستم عامل Windows سوءاستفاده می‌شود. Spelevo در انتشار اسب تروای GootKit نقش داشته است. در فرایند آلوده‌سازی آن یک فرمان‌زمانبندی شده با هدف ماندگار کردن اسب تروا ساخته می‌شود. Maze نیز از جمله بدافزارهایی است که گردانندگان آن از Spelevo برای انتشار این بدافزار بهره گرفتند.

بسته بهره‌جو	توضیحات
Radio	این بسته بهره‌جو در اواسط سال 2019 کشف شد. Radio از آسیب‌پذیری CVE-2016-0189 در سیستم عامل Windows سوءاستفاده می‌کند. در انتشار Nemty از Radio بهره گرفته شده است.
Capesand	Capesand با هدف قرار دادن آسیب‌پذیری‌های CVE-2018-4878، CVE-2015-2419، CVE-2018-15982، CVE-2019-0752 و CVE-2018-8174 در نرم‌افزار Flash Player و سیستم عامل Windows مهاجم را قادر به دریافت و اجرای کد مخرب بر روی دستگاه قربانی می‌کند. بر خلاف سایر بسته‌های بهره‌جو، در Capesand کدهای بهره‌جو در کد منبع آن نبوده و باید با استفاده از یک رابط برنامه‌نویسی API از سرور فرماندهی گردانندگان آن فرخوانی شود.
Bottle	این بسته بهره‌جو که در اواخر سال 2019 کشف شد از آسیب‌پذیری CVE-2018-15982 در نرم‌افزار Flash Player و CVE-2018-8174 در بخش VBScript Engine سیستم عامل Windows سوءاستفاده می‌کند. در نمونه‌هایی از حملات اجرا شده با استفاده از این بسته بهره‌جو کاربران به صفحه حاوی کد مخرب هدایت و در آنجا دستگاه به بدافزار مورد نظر آلوده می‌شود.

۱۰ کارزار مطرح

کارزار	توضیحات
Evilnum	گردانندگان این کارزار حداقل از سال 2018 فعال بوده و عمدتاً شرکت‌های فعال در فن‌آوری‌های مرتبط با امور مالی را مورد هدف قرار می‌داده‌اند. اهداف این گروه همچنان ثابت باقی مانده اما ابزارها و روال‌های آنها طی این مدت تکامل پیدا کرده است. بدافزار مورد استفاده ترکیبی از کدهای اختصاصی مهاجمان و ابزارهای مخربی است که عمدتاً در وب تاریک به فروش می‌رسند.
ServHelper TA505	در این کارزار مهاجمان منتسب به گروه TA505 با بهره‌گیری از درب‌پشتی ServHelper یک استخراج‌کننده ارز رمز را بر روی دستگاه قربانی نصب می‌کنند. استخراج‌کننده مذکور با عنوان Loud-Miner در یک بستر مجازی (Virtual Environment) نصب شده و از سد محصولات ضدویروس عبور می‌کند. ServHelper از نصب شدن بر روی دستگاه‌های با حافظه فیزیکی کمتر از 5 گیگابایت خودداری می‌کند. نرم‌افزار مخرب از چندین تکنیک شامل PowerShell، مبهم‌سازی، تزریق DLL و cmd.exe برای اجرا، عبور از سد سیستم دفاعی و تثبیت خود بهره می‌گیرد.
GoldenSpy Chapter Two	در اواسط سال 2020 شرکت‌های چینی هدف بدافزار GoldenSpy که در یک نرم‌افزار پرداخت مالیات مخفی شده بود قرار گرفتند. چند هفته بعد، حذف‌کننده‌ای (Uninstaller) بر روی سرور فرماندهی مهاجمان قرار گرفت که به‌صورت خودکار توسط نرم‌افزار دریافت و اقدام به حذف GoldenSpy و اثرات آن از روی دستگاه قربانی می‌کرد. مدتی بعدتر نسخه دومی از این حذف‌کننده نیز منتشر شد که البته با کدگذاری توسط Base64 مبهم‌سازی شده بود.
Favicon EXIF Data	در کارزاری کلاهبرداری مهاجمان با قرار دادن کد مخرب در فراداده‌های Exchangeable Image File Format - به اختصار EXIF - و مخفی کردن آنها در سایت‌ها اقدام به سرقت اطلاعاتی همچون داده های مربوط به کارت های اعتباری از طریق فیلدهای ورودی سایت‌های آلوده کردند. اطلاعات سرقت شده با الگوریتم Base64 رمز شده و در قالب فایل تصویری به سرورهای فرماندهی ارسال می‌شدند. به نظر می رسد که گرداننده این کارزار گروه Magecart بوده که حمله به سازمان‌های مطرح را در کارنامه دارد.
XORDDoS / Kaiji	در جریان این کارزار کانتینرهای Docker هدف بدافزاری قرار گرفتند که قادر به اجرای حملات توزیع‌شده برای ازکاراندازی سرویس (Distributed Denial of Service - به اختصار DDoS) یا تبدیل سیستم آلوده به یک شبکه مخرب است. بدافزار جزییات مختلف سیستم نظیر فهرست پروسه‌های اجرا شده، اطلاعات CPU، پوشه‌ها و داده‌های شبکه‌ای را استخراج کرده و از چندین تکنیک از جمله اسکریپت‌نویسی، مبهم‌سازی و خط فرمان در جریان حمله بهره می‌گیرد.
Tetrade	در کارزار Tetrade با بکارگیری چهار خانواده بدافزار بانکی با نام‌های Melcoz، Javali، Guildma و Grandoreiro کاربران در نقاط مختف جهان هدف قرار گرفتند. این کارزار منتسب به مهاجمان مقیم در برزیل بوده و از اواخر 2015 فعال بوده است. بدافزارهای مذکور مجهز به تکنیک‌های عبور از سد سازوکارهای دفاعی شامل ضدتحلیل، ضدبسترهای مجازی‌سازی، مبهم‌سازی، DLL Side Loading و بهره‌گیری از Background Intelligent Transfer Service - به اختصار BITS - است. بدافزار از طریق ایمیل‌های فیشینگ حاوی لینک یا پیوست مخرب توزیع می‌شود. در مواردی نیز سایت‌های هک شده یا سایت‌های در اختیار مهاجمان میزبان بدافزارها بوده‌اند.

کارزار	توضیحات
Vaccine Development	گروه APT29 که با نام Cozy Bear نیز شناخته می‌شود دامنه‌ای گسترده از صنایع در کانادا، انگلیس و آمریکا هدف قرار داد. مهاجمان کارزار بر روی نهادهای دخیل در ساخت واکسن تمرکز داشته‌اند. این جاسوسان سایبری با استفاده از بدافزارهایی همچون WellMail، WellMess و SoreFang اقدام به سرقت داده‌های حساس کرده، نرم‌افزارهای مخرب را نصب نموده، فرامین Shell را فراخوانی کرده و اسکریپت‌ها را اجرا می‌کنند. گروه APT29 با ارسال ایمیل‌های فیشینگ هدفمند و بهره‌جویی از آسیب‌پذیری‌های سرورهای قابل دسترس بر روی اینترنت رخنه اولیه را انجام می‌داده است.
Shlayer	در این کارزار نسخه جدیدی از خانواده بدافزاری Shlayer مورد استفاده مهاجمان قرار گرفته است. Shlayer قادر به اجرا بر روی سیستم عامل macOS X است. این نسخه جدید از طریق نتایج موتورهای جستجوگر به سیستم قربانیان راه می‌یابد. به‌محض آنکه بر روی لینک مخرب کلیک می‌شود با چند تغییر مسیر، کاربر با یک پیغام جعلی به‌روزرسانی نرم‌افزار Adobe Flash Player روبرو می‌شود. در صورت به دام افتادن کاربر و دریافت و اجرای فایل دستگاه به تبلیغ‌افزار، جاسوس‌افزار و برخی دیگر از برنامه‌های مخرب آلوده می‌شود.
M00nD3V Logger	در بازارهای زیرزمینی تبهکاران سایبری یک برنامه مخرب سارق اطلاعات با عنوان M00nD3V Logger به فروش می‌رسید. این بدافزار با جستجوی دامنه گسترده‌ای از اطلاعات را بر روی ماشین قربانی شامل کلیدهای فشرده شده، داده‌های کلیپ‌بورد، تصاویر فعالیت کاربر، ویدئو و اطلاعات اصالت‌سنجی مرورگرهای وب شناسایی می‌کند. در ادامه اطلاعات استخراج شده و در بستر پودمان‌های SMTP و FTP به سرورهای فرماندهی ارسال می‌شود. بدافزار از طریق پیوست‌های مخرب یا سایت‌های هک شده به سیستم قربانی راه یافته و با بهره‌گیری از تکنیک‌هایی همچون مبهم‌سازی و اجرا از طریق Image File Execution Options از سد نرم‌افزارهای دفاعی عبور می‌کند.
Lazarus	چندین خانواده بدافزاری مرتبط با مهاجمان Lazarus دستگاه‌های با سیستم عامل Apple macOS را هدف قرار دادند. بدافزار در قالب برنامه‌های در ظاهر سودمند توزیع شده و پس از اجرا بر روی دستگاه قربانی اقدام به دریافت و نصب یک درب‌پشتی برای فراهم کردن امکان دسترسی مهاجمان و سرقت ارز رمز از روی دستگاه می‌کند. در برنامه‌نویسی این بدافزار از زبان‌های مختلفی نظیر C و Swift بهره گرفته شده است.

۱۰ باج‌افزار با بیشترین انتشار

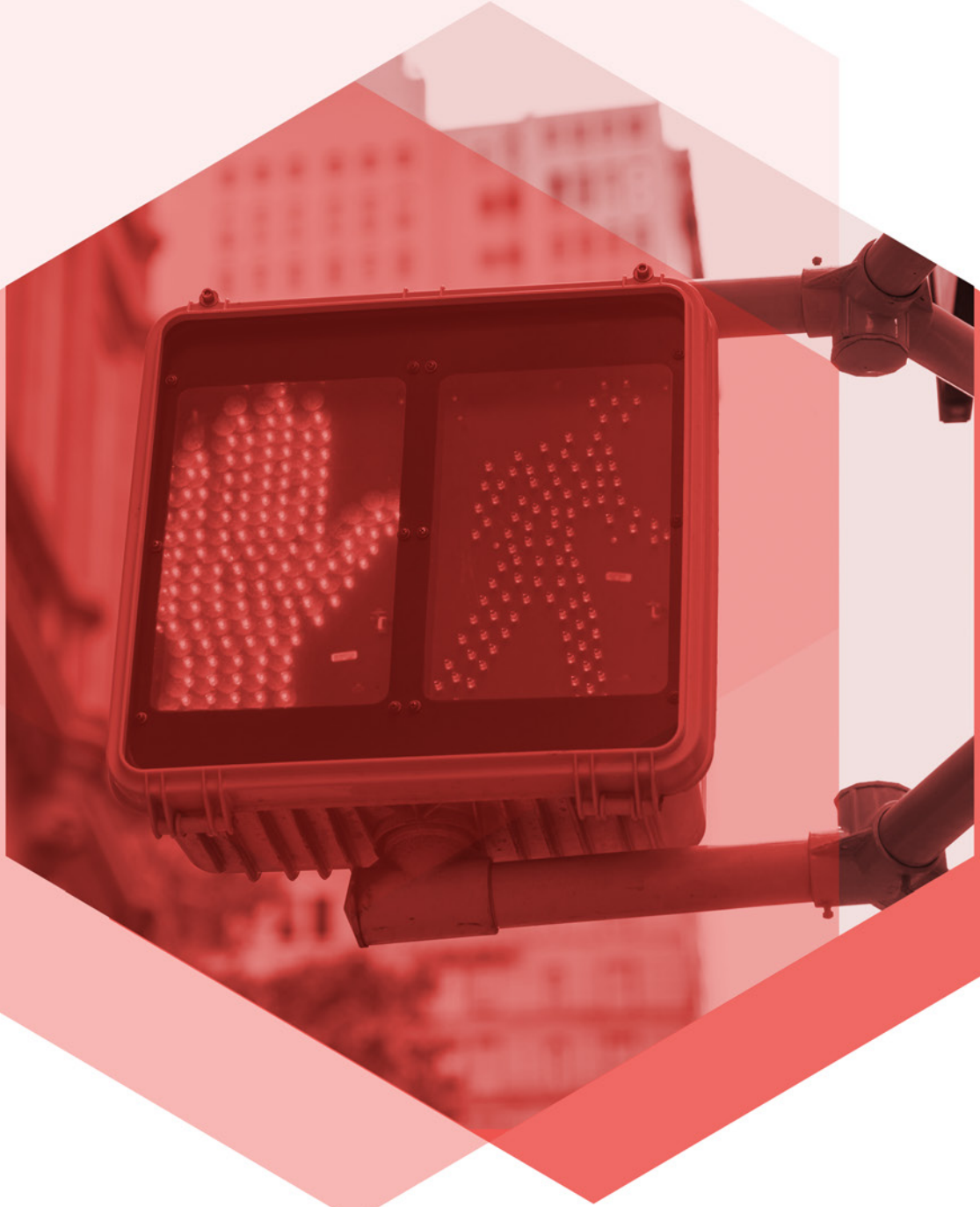
باج‌افزار	توضیحات
Dharma	Dharma که گونه ای از باج افزار CrySiS پسوندهای مختلفی را به فایل های رمزگذاری شده الصاق می کند. این باج افزار از سال ۲۰۱۶ فعال بوده و گردانندگان آن به طور مستمر اقدام به عرضه نسخ جدیدی از آن می کنند.
Phobos	این باج‌افزار پس از رمزگذاری فایل‌ها توسط الگوریتم AES اقدام به افزودن یکی از پسوندهای متنوع خود به آنها می‌کند. نخستین نسخه از Phobos در اواخر سال 2017 شناسایی شد و تا اوایل 2019 عرضه نسخه‌های جدید از آن ادامه داشت. روش برقراری ارتباط با گردانندگان باج‌افزار از طریق ایمیل‌های درج شده در اطلاعیه باج‌گیری است.
Sodinokibi	Sodinokibi که به فایل‌های رمزگذاری شده یک پسوند با نویسه‌های تصادفی الصاق می‌کند قربانی را تهدید می‌کند که در صورت عدم پرداخت به‌موقع باج، مبلغ آن دو برابر خواهد شد. این باج‌افزار از طریق ارائه‌دهندگان خدمات مدیریت شده (Managed Service Provider)، بهره‌جویی از آسیب‌پذیری‌های امنیتی، کارزارهای هرزنامه‌ای و بسته‌های بهره‌جو (Exploit kit) منتشر می‌شوند.
Maze	این باج افزار از الگوریتم های رمزگذاری RSA-2048 و ChaCha20 بهره می گیرد. Maze حمله به نهادهای دولتی و کارخانجات بزرگ را در کارنامه دارد. مهاجمان Maze قربانیان را تهدید می کنند که فایل ها را پیش از رمزگذاری سرقت کرده و در صورت عدم پرداخت باج اقدام به انتشار عمومی آنها خواهند کرد. برای مثال، در سال گذشته گردانندگان Maze در حمله‌ای باج‌افزاری به شرکت Allied Universal، باجی ۲.۳ میلیون دلاری را از آن شرکت طلب کردند. مدتی بعد و با تحقق نیافتن این خواسته مهاجمان، ۷۰۰ مگابایت از داده‌های Allied Universal در تالارهای گفتگوی نفوذگران منتشر و در دسترس قرار گرفته شد.
SunCrypt	SunCrypt که یکی از نشانی‌های IP بکار گرفته شده توسط آن مورد استفاده باج‌افزار Maze نیز قرار گرفته از اسکریپت‌های مخرب PowerShell که توسط مهاجمان مبهم‌سازی (Obfuscation) شده‌اند بهره می‌گیرد. در اطلاعیه باج‌گیری SunCrypt ادعا می‌شود که فایل‌های قربانی پیش از رمزگذاری سرقت شده‌اند و در صورت عدم پرداخت باج به‌صورت عمومی منتشر خواهد شد.
Mailto/Netwalker	NetWalker خانواده‌ای از باج‌افزارهاست که در آگوست ۲۰۱۹ ظهور کرد. اگر چه اولین نسخ آن تحت عنوان Mailto فعالیت می‌کردند اما خیلی زود، از اواخر ۲۰۱۹ به NetWalker تغییر نام پیدا کرد. بخش تحقیقات پیشرفته تهدیدات شرکت مک‌آفی با رصد نشانی‌های بیت‌کوین مرتبط با مهاجمان این باج‌افزار اعلام کرده که تنها در کمتر از شش ماه قربانیان بیش از ۲۵ میلیون دلار به مهاجمان پرداخت کرده‌اند.
ProLock	خانواده باج‌افزاری ProLock که از اوایل سال میلادی جاری ظهور به طور مستمر در حال تکامل خود است. روش رخنه گردانندگان آن به شبکه سازمان ها اجرای حملات "سعی‌وخطا" (Brute-force) بر ضد سرورهای RDP است. در مواردی نیز آلودگی دستگاه به اسب تروای QakBot منجر به اجرای این باج‌افزار می‌شود. QakBot از طریق کارزارهای فیشینگ با پیوست‌ها یا لینک‌های مخرب منتشر می شود. در کارزار ProLock کد مخرب از یک فایل CSV، BMP یا JPG توسط پروسه معتبر PowerShell استخراج شده و در حافظه اجرا می‌شود. در اطلاعیه باج‌گیری ProLock قربانی تهدید می‌شود که در صورت عدم پرداخت باج فایل‌های سرقت در شبکه‌های اجتماعی و رسانه‌های عمومی افشا خواهد شد.

باج‌افزار	توضیحات
Lockbit	باج‌افزارLockBit که ظهور آن به اوایل سال 2020 باز می‌گردد در قالب یک سرویس جدید موسوم به "باج‌افزار به‌عنوان سرویس" به سایر تبهکاران سایبری اجاره داده می‌شود. قابلیتی در LockBit مهاجمان را قادر می‌سازد تا پس از رخنه به شبکه سازمان این باج‌افزار را در مدتی بسیار کوتاه بر روی صدها دستگاه توزیع و فایل‌های آنها را رمزگذاری کنند. گردانندگان این باج افزار در جریان حملات خود اقدام به سرقت اطلاعات سازمانی قربانی کرده و به ادعای مهاجمان عدم پرداخت باج در موعد مقرر منجر به افشای عمومی اطلاعات خواهد شد.
Conti	خانواده جدیدی از باج‌افزارها است با بهره‌گیری از چندین تکنیک فایل‌های مورد نظر خود را شناسایی و نسبت به رمزگذاری آنها با سرعتی بالاتر از هم‌قطاران خود اقدام می‌کند. این باج‌افزار مجهز به تنظیمات خط‌فرمان برای پویش فایل‌های محلی و فایل‌های به اشتراک گذاشته در بستر SMB است. همچنین Conti از Windows Restart Manager برای آزاد کردن فایل‌های در اشغال برنامه‌های دیگر استفاده می‌کند. این باج‌افزار الگوریتم AES-256 برای رمزگذاری فایل‌ها بهره می‌گیرد.
Thanos	باج‌افزار Thanos در فوریه 2020 در تالارهای اینترنتی زیرزمینی تبهکاران به عنوان یک باج‌افزار سفارشی تبلیغ می‌شد. عرضه آن در بازار نشانه‌ای از مورد استفاده قرار گرفتن آن توسط مهاجمان مختلف است. بکارگیری این باج‌افزار در چندین حمله سایبری با حمایت دولتی به سازمان‌هایی در خاورمیانه و شمال آفریقا گزارش شده است.

۱۰ آسیب‌پذیری شاخص

آسیب‌پذیری	توضیحات
CVE-2020-9688	ضعفی در نسخه 2.0.0.518 نرم‌افزار Adobe Download Manager است که مهاجم را قادر به تزریق فرمان و در نهایت اجرای کد مخرب مورد نظر خود می‌کند.
CVE-2020-16875	ضعفی در Microsoft Exchange است که بهره‌جویی از آن مهاجم را قادر به اجرای کد به‌صورت از راه دور با سطح دسترسی کاربر System می‌کند.
CVE-2020-0922	یک آسیب‌پذیری از نوع "اجرای کد به‌صورت از راه دور" است که بخش COM در سیستم عامل Win-dows را تحت تأثیر قرار می‌دهد. هدایت کاربر به یک سایت حاوی JavaScript مخرب یک سناریوهای احتمالی سوءاستفاده از CVE-2020-0922 می‌تواند باشد. سطح حساسیت این آسیب پذیری بر طبق استاندارد ۸/۸، CVSS از ۱۰ اعلام شده است.
CVE-2020-0908	ضعفی از نوع "اجرای کد به‌صورت از راه دور" است که از نحوه مدیریت اشیاء توسط Windows Text Service Module ناشی می‌شود.
CVE-2020-1471	یک آسیب‌پذیری از نوع "ترفیع امتیازی" است که از بررسی ناصحیح اشیاء COM توسط CloudExpe-rienceHost ناشی می‌شود.
CVE-2020-0886	ضعفی از نوع "ترفیع امتیازی" است که Windows Storage Services از آن تأثیر می‌پذیرد.
CVE-2020-3566	این آسیب‌پذیری که پودمان Distance Vector Multicast Routing Protocol - به اختصار DVM-RP - در Cisco IOS XR از آن تأثیر می‌پذیرد مهاجم اصالت‌سنجی نشده را قادر می‌کند تا به‌صورت از راه دور موجب بروز اختلال در پروسه‌های اجرا شده بر روی دستگاه شود.
CVE-2020-1472	ضعفی با درجه حساسیت "حیاتی" است که پودمان Netlogon Remote Protocol از آن تأثیر می‌پذیرد. آسیب‌پذیری مذکور که ضعفی از نوع "ترفیع امتیازی" تلقی می‌شود مهاجم را قادر به توزیع فایل مخرب بر روی یکی از دستگاه‌های شبکه می‌کند.
CVE-2020-1210	بهره‌جویی از این آسیب‌پذیری که نرم‌افزار Microsoft SharePoint از آن تأثیر می‌پذیرد مهاجم را قادر به اجرای کد به‌صورت از راه دور می‌کند.
CVE-2020-6492	ضعفی در مرورگر Google Chrome است که مدیریت نادرست اشیاء در حافظه توسط WebGL ناشی می‌شود. سوءاستفاده از آن می‌تواند منجر به اجرای کد دلخواه مهاجم بر روی دستگاه شود.

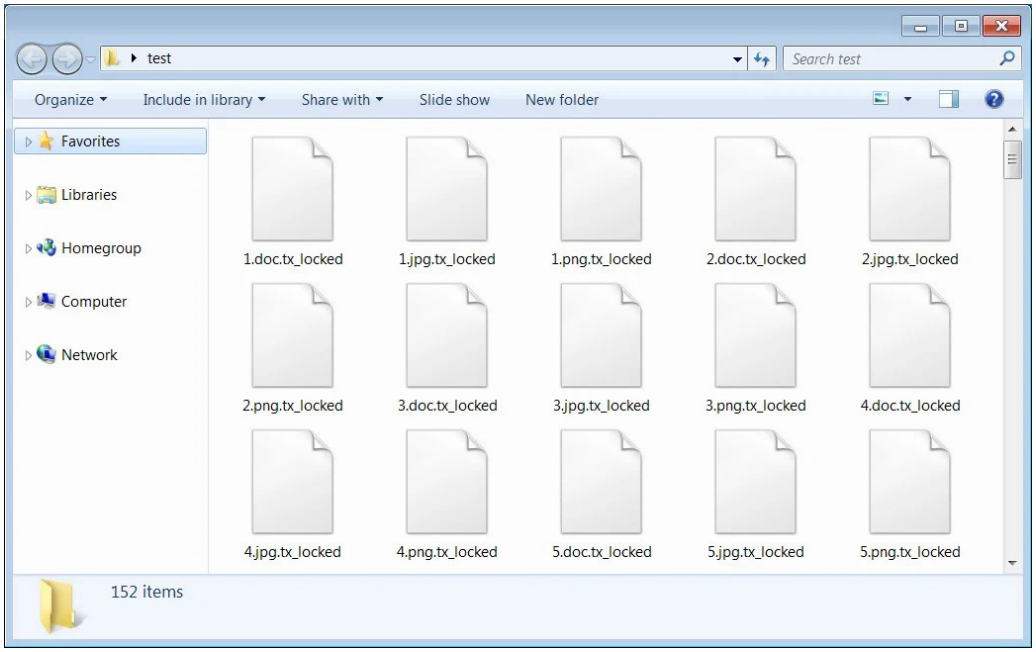
هشدارهای امنیتی



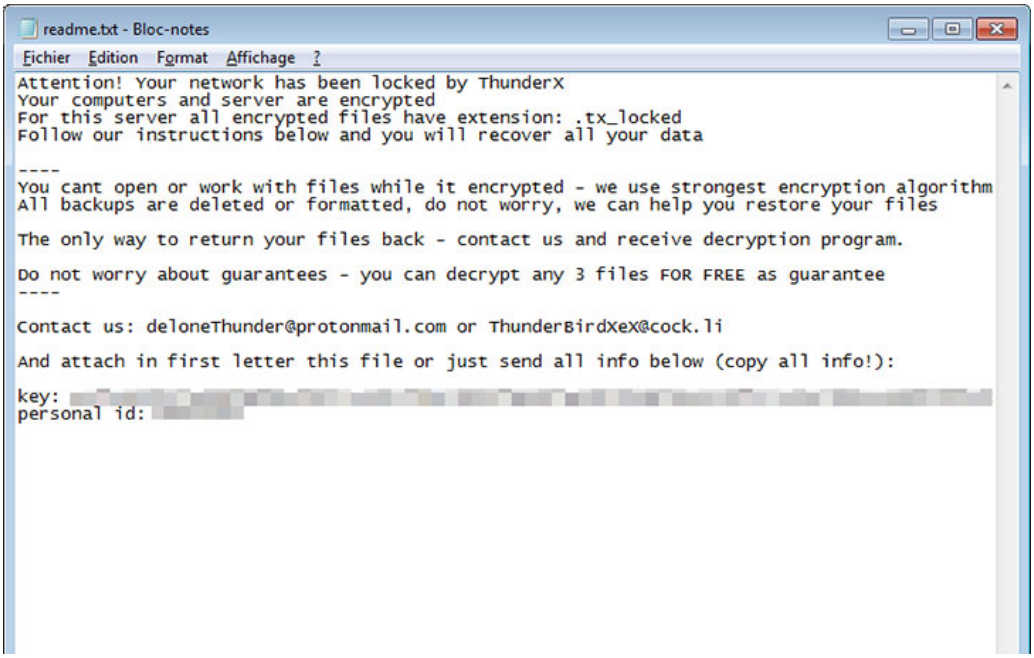
عرضه ابزار رمزگشایی
برای قربانیان باج‌افزار ThunderX

محققان موفق به ساخت ابزاری شده‌اند که قربانیان ThunderX را قادر به رمزگشایی رایگان فایل‌های رمز شده توسط این باج‌افزار می‌کند.

به گزارش شرکت مهندسی شبکه گستر، باج‌افزار نسبتاً جدیدی است که از حدود یک ماه قبل انتشار آن آغاز شده است. نسخه فعلی ThunderX به فایل‌های رمزگذاری شده پسوند tx_locked را الصاق می‌کند.



فایل اطلاعیه باج‌گیری (Ransom Note) این باج‌افزار readme.txt نام دارد که نمونه‌ای از آن در تصویر زیر قابل مشاهده است.



وجود چندین باگ در ThunderX محققان شرکت Tesorion را موفق به عرضه ابزاری کرده که قربانیان این باج‌افزار با استفاده از آن می‌توانند با معرفی یکی از فایل‌های رمز شده و فایل اطلاعیه باج‌گیری (readme.txt) به ابزار کلیه فایل‌ها را بدون نیاز به پرداخت باج به حالت اولیه بازگرداند.

ابزار مذکور از مسیر زیر قابل دریافت و استفاده است:

https://www.nomoreransom.org/en/decryption-tools.html#ThunderX

توضیح اینکه نمونه اشاره شده در این خبر با نام‌های زیر شناسایی می‌شود:

Bitdefender:

- Trojan.GenericKD.43798240

McAfee:

- GenericRXLZ-NA!897FA75679D2

Sophos:

- Mal/Generic-S

بازار گرمی گردانندگان باج‌افزار REvil

با واریز ۱ میلیون دلار

گردانندگان باج‌افزار REvil که با نام Sodinokibi نیز شناخته می‌شود ۹۹ بیت‌کوین، معادل حدود ۱ میلیون دلار را به کیف ارز رمز یک تالار گفتگوی اینترنتی (Forum) هکرهای روسی‌زبان واریز کردند.

به گزارش شرکت مهندسی شبکه گستر، چندین سال است که استفاده خدمات "باج‌افزار به‌عنوان سرویس" (Ransomware-as-a-Service - به اختصار RaaS) به‌شدت در میان مهاجمان سایبری رواج پیدا کرده است. در این خدمات نویسندگان باج‌افزار، نسخه‌ای از کد مخرب خود را به متقاضیان خدمت ارائه می‌دهند. متقاضی وظیفه انتشار باج‌افزار را بر عهده دارد که در صورت پرداخت شدن باج از سوی قربانی بخش عمده مبلغ (معمولا ۷۰ تا ۸۰ درصد) به او می‌رسد. باقی آن نیز (۲۰ تا ۳۰ درصد) سهم نویسندگان باج‌افزار یا در حقیقت ارائه‌دهندگان RaaS خواهد بود.

در REvil از متقاضی RaaS، توسط گردانندگان این باج‌افزار مصاحبه به‌عمل آمده و تنها در صورت اثبات داشتن تجربه و تخصص لازم با درخواست او موافقت می‌شود.

در چند روز اخیر این گردانندگان اقدام به انتشار آگهی در یک تالار معروف هکرهای روسی‌زبان جهت جذب هر چه بیشتر هکرهای باتجربه و ماهر به‌عنوان متقاضیان خدمات RaaS خود کرده‌اند. توانایی اجرای حملات موسوم به تست نفوذ و کار با تجهیزات ذخیره‌ساز متصل به شبکه (NAS)، نوار مغناطیسی ذخیره داده (Tape)، بسترهای Microsoft Solutions Framework - به اختصار MSF -، سرویس‌های Certificate Service - به اختصار CS -، ابزار Koadic و بستر مجازی‌سازی Hyper-V از جمله مهارت‌هایی است که در این آگهی به چشم می‌خورد.

این تالار گفتگوی اینترنتی اعضا را قادر به واریز بیت‌کوین به کیف پولی که در کنترل سایت است می‌کند تا از این طریق به‌عنوان واسطی برای خرید و فروش خدمات و اقلام غیرقانونی توسط اعضا عمل کند. گردانندگان REvil نیز برای نشان دادن جدیدتشان در کسب‌وکار و همچنین پشتوانه مالی خود، ۹۹ بیت‌کوین را در کیف ارز رمز مذکور واریز کردند.

Thus, we:
1. Expand the composition of the teams of acting advertisers with talented people;
2. We invite ready-made lineups to work with us;
All this is aimed at one thing - to increase the quality and quantity of waste material, which entails an increase in profits. But this does not mean that everyone will be accepted.

For your peace of mind and confidence, we have made a deposit of 1 million US dollars.

Last edited: Today at 15:29

REvil از جمله باج‌افزارهایی است که مهاجمان آن اهداف خود را به‌صورت خاص انتخاب کرده و ضمن سرقت فایل‌ها و داده‌ها، در صورت پرداخت نشدن مبلغ اخاذی‌شده اقدام به افشای آنها می‌کنند.

متاسفانه اجرای حملات باج‌افزاری هدفمند، به صنعتی چند میلیون دلاری تبدیل شده و اینگونه تبلیغات تبهکاران سایبری موجب افزایش هر چه بیشتر تعداد این حملات و مخرب و پیچیده‌تر شدن آنها می‌شود. لذا همچون همیشه بکارگیری روش‌های پیشگیرانه در مقابله با باج‌افزارها و مقاوم سازی پودمان RDP برای ایمن ماندن از گزند این بدافزارهای مخرب توصیه می‌شود.

سامانه‌ای برای بررسی هک شدن ایمیل توسط مهاجمان Emotet

شرکت ایتالیایی تی‌جی سافت (TG Soft) سامانه‌ای را راه‌اندازی کرده که امکان بررسی مورد سوءاستفاده قرار گرفتن ایمیل یا دامنه را در کارزارهای هرزنامه‌ای Emotet فراهم می‌کند.

به گزارش شرکت مهندسی شبکه گستر، روش اصلی انتشار بدافزار Emotet ایمیل‌های هرزنامه‌ای با پیوست فایل Word یا Excel مخرب است. در صورت باز شدن فایل پیوست و اجرای ماکروی مخرب تزریق شده در آن، Emotet بر روی دستگاه نصب می‌شود.

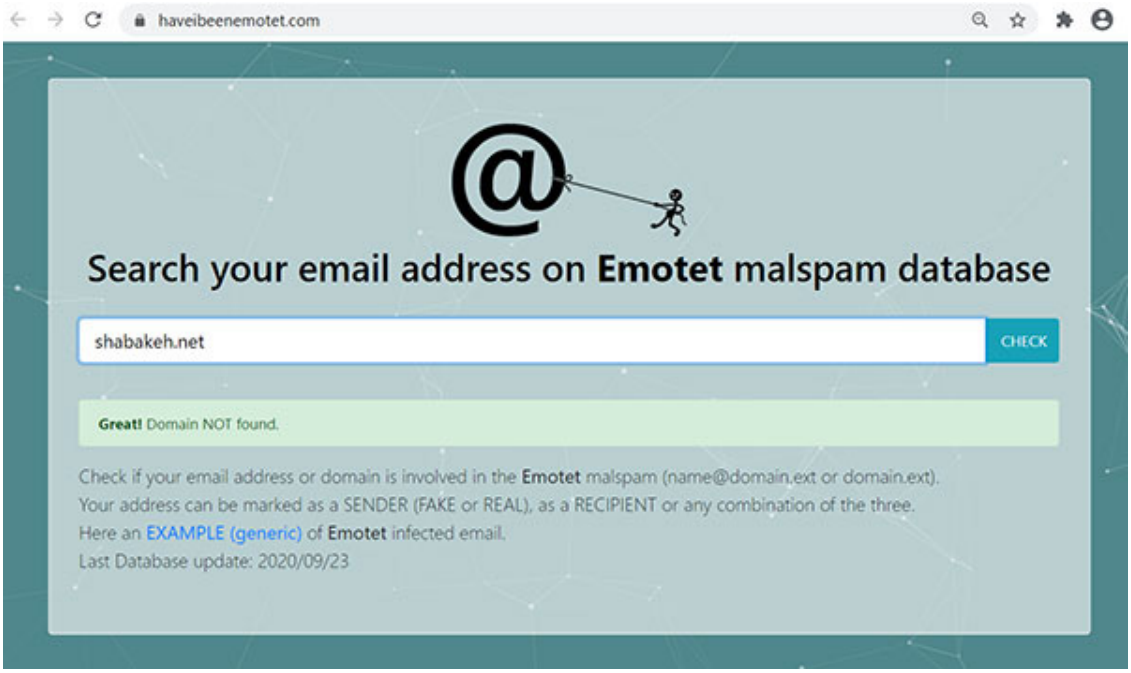
Emotet با استخراج اطلاعات ایمیل قربانی آن را به سرورهای فرماندهی (C۲) مهاجمان ارسال می‌کند. مهاجمان نیز در کارزارهای آتی این بدافزار از ایمیل سرقت شده برای معتبر جلوه دادن هرزنامه‌های ارسالی بهره می‌گیرند.

از مخرب‌ترین قابلیت‌های Emotet توانایی آن در دریافت و اجرای بدافزارهای دیگر نظیر TrickBot و QakBot است. ضمن این که Emotet در انتشار باج‌افزارهای Ryuk،Conto و ProLock نقش داشته است.

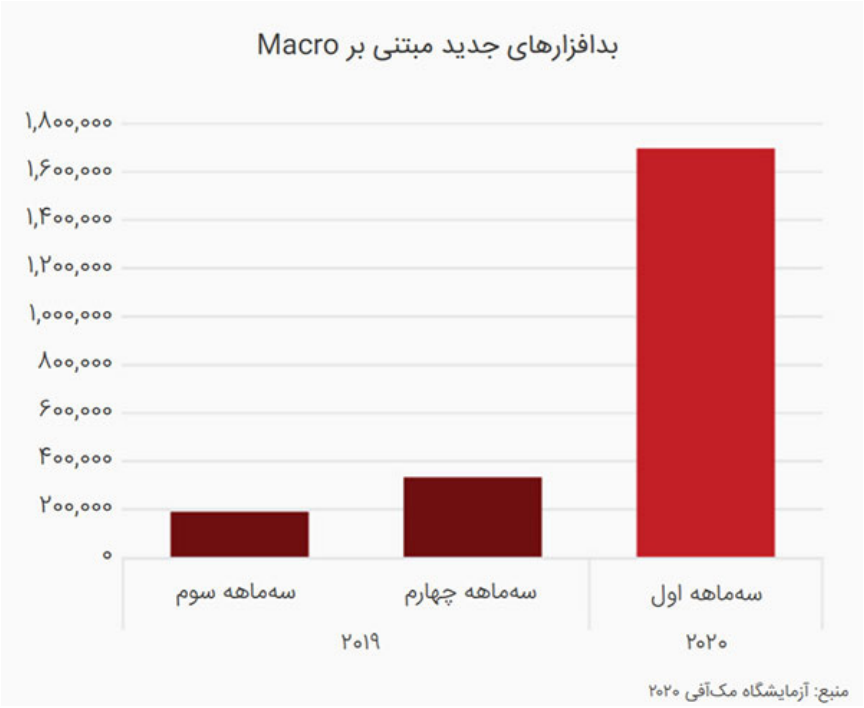
اکنون شرکت تی‌جی سافت با راه‌اندازی سامانه‌ای با عنوان Have I Been Emotet به نشانی www.haveibeenemotet.com کاربران و راهبران شبکه را قادر می‌کند که با وارد کردن دامنه (Domain) یا نشانی ایمیل، مورد بهره‌جویی قرار گرفتن آنها در کارزارهای هرزنامه‌ای Emotet در فاصله ۱۱ مرداد تا ۲ مهر سال جاری را مورد بررسی قرار دهند. طی این دوره تی‌جی سافت ۲.۱ میلیون نشانی ایمیل را از ۷۰۰ هزار ایمیل ارسالی استخراج کرده است.

نتایج جستجو در سامانه مذکور به سه دسته زیر تقسیم می‌شوند:

- REAL SENDER - که به معنای آن است که نشانی ایمیل، هک شده و از آن در انتشار هرزنامه‌های Emotet سوءاستفاده شده است.
- FAKE SENDER - که بدان معنا است که از نشانی ایمیل بررسی شده به‌صورت جعلی در هرزنامه‌های ارسالی Emotet بهره‌جویی شده است.
- RECIPIENT - که نشان‌دهنده هدف قرار گرفتن نشانی ایمیل در کارزارهای هرزنامه‌ای Emotet است.



از جمله مؤثرترین راهکارها در مقابله با تهدیدات هرزنامه‌ای مبتنی بر ماکروی مخرب پیکربندی صحیح قابلیت ماکرو (Macro) در مجموعه نرم‌افزاری Office مطابق با این راهنما است. بر طبق آخرین گزارش فصلی شرکت مک‌آفی تعداد نمونه‌های جدید از بدافزارهای مبتنی بر ماکرو در سه‌ماهه اول سال ۲۰۲۰ در مقایسه با سه‌ماهه چهارم ۲۰۱۹، حدود ۴۱۲ درصد افزایش داشته است.



سوءاستفاده از سرویس معتبر Windows
برای اجرای "بدون فایل" بدافزار

مهاجمان با تزریق کد مخرب به سرویس معتبر Windows Error Reporting - به اختصار WER - اقدام به اجرای حملات موسوم به "بدون فایل" (Fileless) کرده‌اند.

این نخستین بار نیست که تاکتیک بهره‌جویی (Exploit) از سرویس WER مورد استفاده مهاجمان قرار می‌گیرد و پیش‌تر نیز در باج‌افزار Cerber و بدافزار NetWire RAT گزارش شده بود.

در حمله اخیر که شرکت ملوربایتز آن را گزارش کرده مهاجمان با هک یک سایت از آن برای میزبانی کد مخرب بهره گرفته‌اند. در ادامه نیز ضمن بکارگیری چندین تکنیک ضدتحلیل از CactusTorch Framework به‌منظور اجرای حمله به‌صورت "بدون فایل" استفاده کرده‌اند.

به گزارش شرکت مهندسی شبکه گستر، ملوربایتز این حمله را اولین بار در ۲۷ شهریور در حین بررسی ایمیل‌های فیشینگ با پیوست یک فایل فشرده ZIP کشف کرد.

در فایل مذکور سندی به چشم می‌خورد که در آن یک ماکروی مخرب که نسخه‌ای سفارشی شده از ماژول CactusTorch است لحاظ شده بود.

به‌محض باز شدن سند و فعال شدن ماکرو، کد موسوم به Shellcode دریافت شده و در ادامه کدی مبتنی بر .NET مستقیما در حافظه Windows فراخوانی می‌شود.

پس از آن بدون کپی شدن هر گونه فایل بر روی دیسک سخت دستگاه قربانی، Shellcode در پروسه سرویس WER (فایل WerFault.exe) تزریق می‌شود.

در ابتدا رشته اجرایی (Thread) سرویس جدید با چندین سازوکار ضدتحلیل اطمینان حاصل می‌کند که بر روی یک ماشین مجازی، سندباکس و به‌طور کلی بسترهای مورد استفاده محققان و تحلیلگران بدافزار اجرا نشده باشد. در غیر این صورت اجرای خود را متوقف می‌کند.

بعد از آن، Shellcode نهایی در رشته اجرایی WER رمزگشایی و اجرا می‌شود که این خود موجب اجرا در یک رشته اجرایی جدید می‌گردد.

در نهایت، کد نهایی بدافزار نیز که در فایلی با نام favicon۳۲.ico بر روی asia-kotoba[.]net میزبانی شده دریافت و در یک پروسه جدید تزریق می‌شود.

با توجه به از دسترس خارج شدن URL مذکور، شرکت ملوربایتز موفق به دستیابی به کد نهایی نشده است.

دامنه‌ای که از آن برای میزبانی پیوست‌های ایمیل‌های فیشینگ استفاده شده (yourrighttocompensation[.]com) در شهر هوشی‌مین ویتنام ثبت شده است. به همین بخاطر اجرای حمله توسط گروه ویتنامی APT32 محتمل دانسته شده است. این گروه حمله مؤسسات تحقیقاتی، سازمان‌های حامی حقوق بشر و رسانه‌ها در کشورهای مختلف را در کارنامه دارد.

مشروح گزارش ملوربایتز در لینک زیر قابل مطالعه است:

https://blog.malwarebytes.com/malwarebytes-news/2020/10/kraken-attack-abuses-wer-service/

MosaicRegressor؛
روت‌کیتی دیگر، مبتنی بر UEFI

محققان کسپرسکی جزییات روت‌کیتی مبتنی بر Unified Extensible Firmware Interface - به اختصار UEFI - را منتشر کردند که در جریان بررسی حملات اجرا شده در سال میلادی گذشته بر ضد دو سازمان موفق به کشف آن شده‌اند.

این نوع بدافزارها با رخنه در ماژول حافظه Serial Peripheral Interface - به اختصار SPI - نه تنها در صورت تغییر سیستم عامل ماندگار می‌ماند که حتی جایگزینی دیسک سخت نیز تأثیری در حضور این بدافزار نخواهد داشت.

به گزارش شرکت مهندسی شبکه گستر، این بوت‌کیت UEFI که محققان کسپرسکی آن را MosaicRegressor نامگذاری کرده‌اند یک بستر مبتنی بر ماژول (Modular) و چندمرحله‌ای است که به گفته این شرکت توسط هکرهای چینی‌زبان در عملیات‌های جاسوسی و سرقت داده‌ها مورد استفاده قرار گرفته بوده است.

در MosaicRegressor مهاجمان با تزریق چندین ماژول مخرب اقدام به دستکاری ثابت‌افزار UEFI و بهره‌گیری از آن برای توزیع بدافزار بر روی دستگاه‌های مقصد می‌کردند.

MosaicRegressor مجهز به چند دریافت‌کننده (Downloader) و اجراکننده (Loader) واسطی است که امکان دریافت و اجرای کدهای مخرب بر روی دستگاه قربانی را برای مهاجمان فراهم می‌کنند. بستر چند ماژولی MosaicRegressor ضمن دشوار کردن تحلیل، مهاجمان را قادر به استفاده از امکانات مختلف بسته به شرایط بر روی ماشین‌های مقصد می‌کند.

محققان کسپرسکی نیز در بررسی‌های خود به تعداد محدودی از این کدها دست یافته‌اند. یکی از این کدها توسط نسخه‌ای از بوت‌کیت با نام BitsRegEx برای سرقت، آرشیو کردن و استخراج اطلاعات در پوشه موسوم به Recent Documents مورد استفاده قرار گرفته است. این روت‌کیت UEFI نسخه‌ای سفارشی از بوت‌کیت VectorEDK متعلق به شرکت ایتالیایی Hacking Team است که در سال ۱۳۹۴ افشا شده بود.

در فاصله سال‌های ۲۰۱۷ تا ۲۰۱۹، نمونه‌هایی از MosaicRegressor بر روی کامپیوترهای چندین سازمان غیرانتفاعی و نهاد دیپلماتیک در آفریقا، آسیا و اروپا فعال بوده.

محققان کسپرسکی معتقدند که همگی قربانیان به نحوی با جمهوری دموکراتیک خلق کره یا همان کره شمالی در ارتباط بوده‌اند.

کسپرسکی اعلام کرده که موفق به پیدا کردن روش اصلی آلودگی که منجر به رونویسی ثابت‌افزار UEFI می‌شده نگردیده است. یکی از احتمالات مطرح شده از سوی کسپرسکی دسترسی فیزیکی مهاجمان به ماشین‌های هدف و بالا آوردن آن از طریق یک حافظه USB Flash برای تزریق کد آلوده بوده است.

احتمال مطرح شده دیگر نصب از راه دور بوت‌کیت با بهره‌جویی (BIOS) از آسیب‌پذیری‌های BIOS است.

دو سال قبل نیز شرکت ای‌ست جزییات بوت‌کیت دیگری با نام LoJax را به‌صورت عمومی منتشر کرده بود. گروه روسی‌زبان APT28 بوت‌کیت LoJax را در کنار نرم‌افزار معتبر ضدسرقت LoJack در قالب ماژول‌های UEFI اصلاح شده به اهداف خود تزریق می‌کردند.

پیش از آن و در سال ۱۳۹۵ هم سایت افشاگر WikiLeaks اقدام به انتشار اسنادی سری کرد که در آنها ابزارهای مورد استفاده در عملیات‌های سایبری سازمان اطلاعات مرکزی آمریکا تشریح شده بودند. برخی از این اسناد نشان می‌داد که این سازمان با بهره‌جویی از آسیب‌پذیری‌هایی روز صفر، کد مخرب را مستقیماً به ثابت‌افزار دستگاه‌ها از جمله UEFI تزریق می‌کرده است. در پی درز اسناد مذکور در آن سال، شرکت مک‌آفی راهکاری را برای پویش UEFI دستگاه به‌منظور بررسی وجود کد مخرب بر روی آن منتشر کرد.

مشروح گزارش کسپرسکی در خصوص MosaicRegressor در لینک زیر قابل دریافت و مطالعه است:

https://securelist.com/mosaicregressor/98849/

نشانه‌های آلودگی (IoC) بوت‌کیت MosaicRegressor به شرح زیر است:

درهم‌ساز

F5B320F7E87CC6F9D02E28350BB87DE6
0C136186858FD36080A7066657DE81F5
91A473D3711C28C3C563284DFAFE926B
DD8D3718197A10097CD72A94ED223238
0EFB785C75C3030C438698C77F6E960E
12B5FED367DB92475B071B6D622E44CD
3B3BC0A2772641D2FC2E7CBC6DDA33EC
3B58E122D9E17121416B146DAAB4DB9D
70DEF87D180616406E010051ED773749
7908B9935479081A6E0F681CCEF2FDD9
AE66ED2276336668E793B167B6950040
B23E1FE87AE049F46180091D643C0201
CFB072D1B50425FF162F02846ED263F9
0D386EBBA1CCF1758A19FB0B25451AFE
233B300A58D5236C355AFD373DABC48B
449BE89F939F5F909734C0E74A0B9751
67CF741E627986E97293A8F38DE492A7
6E949601EBDD5D50707C0AF7D3F3C7A5
92F6C00DA977110200B5A3359F5E1462
A69205984849744C39CFB421D8E97B1F
D197648A3FB0D8FF6318DB922552E49E
B53880397D331C6FE3493A9EF81CD76E
AFC09DEB7B205EADAE4268F954444984
DC14EE862DDA3BCC0D2445FDCB3EE5AE
88750B4A3C5E80FD82CF0DD534903FC0
C63D3C25ABD49EE131004E6401AF856C
D273CD2B96E78DEF437D9C1E37155E00
72C514C0B96E3A31F6F1A85D8F28403C
9E182D30B070BB14A8922CFF4837B94D
61B4E0B1F14D93D7B176981964388291

3D2835C35BA789BD86620F98CBFBF08B
32ΛAD6468F6EDB80B3ABF97AC39A0721
7B213A6CE7AB30A62E84D81D455B4DEA
E2F4914E38BB632E975CFF14C39D8DCD
08ECD8068617C86D7E3A3E810B106DCE
1732357D3A0081A87D56EE1AE8B4D205
74DB88B890054259D2F16FF22C79144D
7C3C4C4E7273C10DBBAB628F6B2336D8
89527F932188BD73572E2974F4344D46
36B51D2C0D8F48A7DC834F4B9E477238
1C5377A54CBAA1B86279F63EE226B1DF
9F13636D5861066835ED5A79819AAC28
FA0A874926453E452E3B6CED045D2206

مسیرهای فایل

%APPDATA%\Microsoft\Credentials\MSI36C2.dat
%APPDATA%\Microsoft\Internet Explorer\%Computername%.dat
%APPDATA%\Microsoft\Internet Explorer\FileA.dll
%APPDATA%\Microsoft\Internet Explorer\FileB.dll
%APPDATA%\Microsoft\Internet Explorer\FileC.dll
%APPDATA%\Microsoft\Internet Explorer\FileD.dll
%APPDATA%\Microsoft\Internet Explorer\FileOutA.dat
%APPDATA%\Microsoft\Network\DFileA.dll
%APPDATA%\Microsoft\Network\DFileC.dll
%APPDATA%\Microsoft\Network\DFileD.dll
%APPDATA%\Microsoft\Network\subst.sep
%APPDATA%\Microsoft\WebA.dll
%APPDATA%\Microsoft\WebB.dll
%APPDATA%\Microsoft\WebC.dll
%APPDATA%\Microsoft\Windows\LnkClass.dat
%APPDATA%\Microsoft\Windows\SendTo\cryptui.sep
%APPDATA%\Microsoft\Windows\SendTo\load.dll %APPDATA%\Microsoft\Windows\load.rem
%APPDATA%\Microsoft\Windows\mapisp.dll
%APPDATA%\Microsoft\exitUI.rs
%APPDATA%\Microsoft\sppsvc.tbl
%APPDATA%\Microsoft\subst.tbl
%APPDATA%\newplgs.dll
%APPDATA%\rfvtgb.dll
%APPDATA%\sdfcvb.dll
%APPDATA%\msreg.dll
%APPDATA\Microsoft\dfsadu.dll
%COMMON_APPDATA%\Microsoft\Windows\user.rem
%TEMP%\BeFileA.dll
%TEMP%\BeFileC.dll

%TEMP%\RepairA.dll
%TEMP%\RepairB.dll
%TEMP%\RepairC.dll
%TEMP%\RepairD.dll
%TEMP%\wrtreg_32.dll
%TEMP%\wrtreg_64.dll
%appdata%\dwhost.exe
%appdata%\msreg.exe
%appdata%\return.exe
%appdata%\winword.exe

دامنه و نشانی‌های IP

menjitghyukl.myfirewall[.]org
۱۰۳.۱۹۵.۱۵۰[.]۱۰۶
۱۰۳.۲۲۹.۱[.]۲۶
۱۰۳.۲۴۳.۲۴[.]۱۷۱
۱۰۳.۲۴۳.۲۶[.]۲۱۱
۱۰۳.۳۰.۴۰[.]۱۱۶
۱۰۳.۳۰.۴۰[.]۳۹
۱۰۳.۳۹.۱۰۹[.]۲۳۹
۱۰۳.۳۹.۱۰۹[.]۲۵۲
۱۰۳.۳۹.۱۱۰[.]۱۹۳
۱۰۳.۵۶.۱۱۵[.]۶۹
۱۰۳.۸۲.۵۲[.]۱۸
۱۱۷.۱۸.۴[.]۶
۱۴۴.۴۸.۲۴۱[.]۱۶۷
۱۴۴.۴۸.۲۴۱[.]۳۲
۱۵۰.۱۲۹.۸۱[.]۲۱
۴۳.۲۵۲.۲۲۸[.]۱۷۹
۴۳.۲۵۲.۲۲۸[.]۲۵۲
۴۳.۲۵۲.۲۲۸[.]۷۵
۴۳.۲۵۲.۲۲۸[.]۸۴
۴۳.۲۵۲.۲۳۰[.]۱۸۰
۴۳.۲۵۲.۲۳۰[.]۱۷۳
۱۸۵.۲۱۶.۱۱۷[.]۹۱
۱۰۳.۲۱۵.۸۲[.]۱۶۱
۱۰۳.۹۶.۷۲[.]۱۴۸
۱۲۲.۱۰.۸۲[.]۳۰

BazarBackdoor،
سلاح جدید گردانندگان TrickBot

گردانندگان اسب‌تروای مشهور TrickBot در حال بهره‌گیری از مجموعه بدافزاری جدیدی با عنوان BazarLoader/BazarBackdoor در حمله به اهداف خاص و بااهمیت خود هستند. در جریان این حملات در نهایت سیستم‌های سازمان به باج‌افزار مخرب Ryuk آلوده می‌شوند.

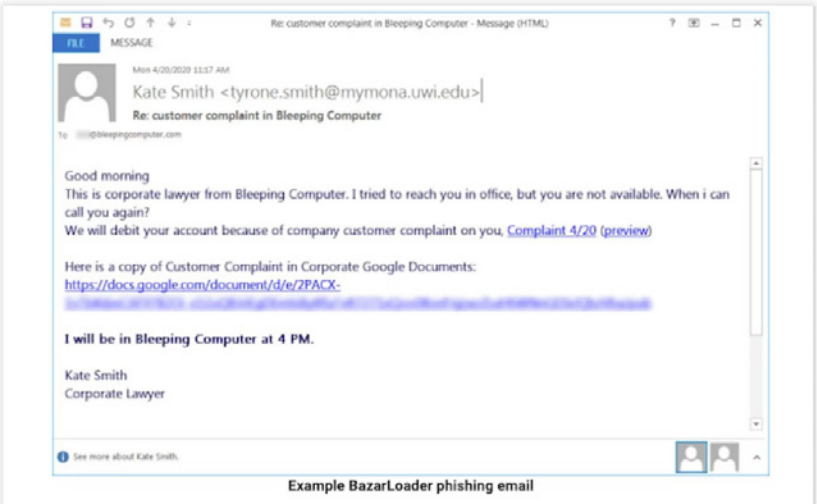
برای سال‌ها این افراد اقدام به آلوده‌سازی دستگاه‌ها و انجام امور مخربی نظیر سرقت رمزهای عبور و انواع اطلاعات حساس دیگر و توزیع آلودگی بر روی ماشین‌های دیگر با استفاده از ماژول‌های مختلف TrickBot می‌کردند.

بر اساس گزارشی که به‌تازگی ادونسد-اینتل آن را منتشر کرده گردانندگان TrickBot مدتی است که در برخی کارزارهای فیشینگ خود به استفاده از BazarLoader/BazarBackdoor روی آورده‌اند.

این مهاجمان بجای توزیع TrickBot که توسط بسیاری از راهکارها قابل شناسایی است از BazarLoader/BazarBackdoor به‌عنوان ابزاری برای آلوده‌سازی اهداف بااهمیت و باارزش خود استفاده می‌کنند.

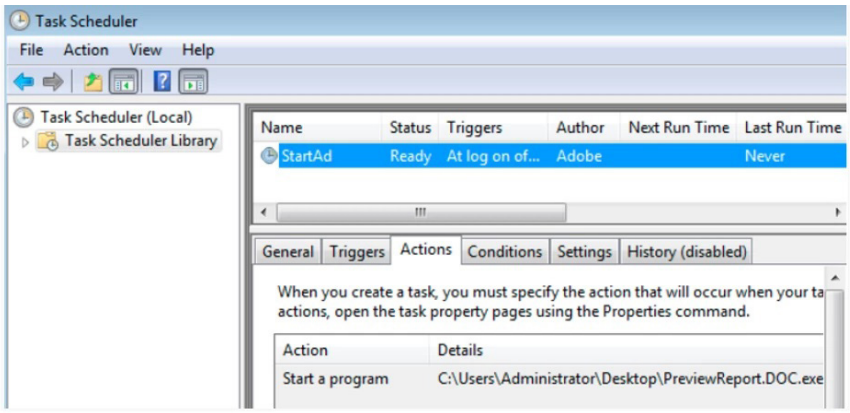
BazarBackdoor با حداقل قابلیت‌ها امکان گسترش آلودگی‌ها را برای مهاجمان فراهم می‌کند.

نمونه‌ای از ایمیل‌های ناقل BazarLoader در تصویر زیر قابل مشاهده است.



Example BazarLoader phishing email

با اجرای BazarLoader، در جریان فرایند موسوم به Process Hollowing، کد BazarBackdoor به پروسه‌های معتبر Windows نظیر cmd.exe، explorer.exe و svchost.exe تزریق می‌شود. یک فرمان زمانبندی‌شده (Scheduled Task) نیز برای اجرای خودکار BazarLoader در هر بار ثبت ورود (Login) کاربر به سیستم تعریف می‌شود.



در ادامه، BazarBackdoor اقدام به توزیع Cobalt Strike برای فراهم کردن دسترسی از راه دور مهاجمان به سیستم و انجام اقدامات مخربی همچون استفاده از BloodHound و Lasagne و در نتیجه دستیابی به اطلاعات اصالت‌سنجی دامنه سازمان می‌کند.

در نهایت این مهاجمان، باج‌افزار Ryuk را بر روی سیستم‌ها توزیع و از سازمان مبالغ هنگفتی را اخاذی می‌کنند.

به گزارش مهندسی شبکه گستر، BazarLoader/BazarBackdoor در حال تبدیل شدن به سلاحی مخرب و البته مؤثر در حملات هدفمند گردانندگان TrickBot است.

مشروح گزارش ادونسد-اینتل در لینک زیر قابل مطالعه است:

https://www.advanced-intel.com/post/front-door-into-bazarbackdoor-stealthy-cybercrime-weapon

توضیح اینکه کدهای مخرب اشاره شده در گزارش مذکور با نام‌های زیر قابل شناسایی است.

Bitdefender:

- GenericKD.44037412
- GenericKD.34741243
- GenericKD.44037996
- GenericKD.34733437
- GenericKD.34741225
- Gen:Variant.Razy.767614

McAfee:

- Artemis!AB1C5D9645E0
- Artemis!704DEA93EF12
- Artemis!C361742189A1
- Artemis!6DEF4F90609B
- Artemis!1E30713681E7
- Artemis!7AFB28BFB761

Sophos:

- Mal/BadCert-Gen
- Mal/Generic-S

هشدار مجدد

در خصوص آسیب‌پذیری Zerologon

بر اساس گزارش‌های واصله به شرکت مهندسی شبکه گستر، در هفته‌های اخیر برخی مؤسسات هدف حملاتی قرار گرفته‌اند که در جریان آنها مهاجمان با سوءاستفاده از آسیب‌پذیری CVE-2020-1472 - معروف به Zerologon - اقدام به توزیع باج‌افزارهای با عملکرد Wiper در شبکه اهداف خود می‌کنند.

همان‌طور که پیش‌تر در تاریخ ۵ مهر ماه در این خبر هشدار داده شد Zerologon ضعفی از نوع "ترفیع امتیازی" (Elevation of Privilege) است که پودمان Microsoft Netlogon Remote ProtoCol - که با عنوان MS-NRPC نیز شناخته می‌شود - از آن تأثیر می‌پذیرد.

Zerologon مهاجم را قادر می‌سازد تا بدون نیاز به اصالت‌سنجی شدن با اتصال در بستر پودمان MS-NRPC خود را به‌عنوان یک دستگاه عضو دامنه از جمله یک سرور Domain Controller - به اختصار DC - معرفی کرده و موفق به دستیابی به سطح دسترسی Domain Admin و در ادامه انجام مخرب مختلف در سطح دامنه شود.

به‌تازگی مرکز راهبردی افتای ریاست جمهوری با همکاری شرکت مهندسی شبکه گستر نیز اقدام به انتشار هشداری کرده که در آن به تفصیل به راه‌های مقابله با آسیب‌پذیری Zerologon پرداخته شده است؛ جزییات آن در لینک زیر قابل دریافت و مطالعه است.

https://www.afta.gov.ir/portal/home/?news/235046/237266/242016

لازم به ذکر است که در حملات گزارش شده به این شرکت، پس از هک و رخنه به شبکه سازمان و بهره‌جویی از آسیب‌پذیری Zerologon، در نهایت مهاجمان اقدام به نصب و اجرای باج‌افزارهای با عملکرد موسوم به Wiper بر روی دستگاه‌ها کرده و در عمل موجب مختل شدن کامل روند کار سیستم‌ها می‌شوند.

باید توجه داشت اگر چه در بسیاری موارد، کدهای مخرب به کار گرفته شده در حین حمله، توسط محصولات امنیتی قابل شناسایی هستند لیکن با توجه به سطح دسترسی کامل (Administrator) مهاجمان بر روی دستگاه‌های هدف، عملاً امکان تقلیل کنترل‌های امنیتی و نظارتی تعریف شده و دست‌درازی به محصولات نصب شده و در ادامه، نصب هر گونه بدافزار و ابزار مخرب دیگر برای آنها فراهم می‌شود. لذا مسدودسازی نقطه ورود و ترمیم حفره‌های امنیتی - در اینجا Zerologon - در کنار رعایت موارد زیر در ایمن ماندن از گزند این نوع حملات هدفمند از اهمیت بسزایی برخوردار است:

- استفاده از ضدویروس قدرتمند و به‌روز با قابلیت نفوذیاب و ضدبهره‌جو (Anti-exploit)
- استفاده از رمزهای عبور پیچیده، هک نشده و غیرتکراری برای حساب‌های کاربری محلی (Local) تحت دامنه (Domain) سیستم عامل و پایگاه‌های داده، به ویژه حساب‌های با سطح دسترسی Administrator/SysAdmin

- کاهش سطح دسترسی کاربران
- پرهیز از قابل دسترس کردن سرویس‌های حساسی نظیر MS-SQL و Domain Controller در بستر اینترنت
- غیرفعال کردن پودمان RDP یا حداقل تغییر درگاه پیش‌فرض آن
- اطمینان از نصب بودن اصلاحیه‌های امنیتی بر روی تمامی دستگاه‌ها
- ارتقای سیستم‌های عامل از رده خارج
- استفاده از دیواره آتش در درگاه شبکه
- فعال‌سازی سیاست‌های مقابله با بدافزارهای "بدون فایل" (Fileless) در محصولات امنیت نقاط پایانی بر اساس سیاست‌های پیشنهادی شرکت مهندسی شبکه گستر

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

آسیب‌پذیری‌ها و اصلاحیه‌های امنیتی

اصلاحیه‌های امنیتی مایکروسافت
برای ماه میلادی اکتبر

سه‌شنبه، ۲۲ مهر، شرکت مایکروسافت اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی اکتبر منتشر کرد. این اصلاحیه‌ها در مجموع، ۸۷ آسیب‌پذیری را در نرم‌افزارهای زیر ترمیم می‌کنند:

- .NET Framework
- Azure
- Group Policy
- Microsoft Dynamics
- Microsoft Exchange Server
- Microsoft Graphics Component
- Microsoft NTFS
- Microsoft Office
- Microsoft Office SharePoint
- Microsoft Windows
- Microsoft Windows Codecs Library
- PowerShellGet
- Visual Studio
- Windows COM
- Windows Error Reporting
- Windows Hyper-V
- Windows Installer
- Windows Kernel
- Windows Media Player
- Windows RDP
- Windows Secure Kernel Mode

به گزارش شرکت مهندسی شبکه گستر، درجه حساسیت ۱۴ مورد از آسیب‌پذیری‌های ترمیم شده "حیاتی" (Critical) و باقی آنها "مهم" (Important) گزارش شده است.

در درجه‌بندی شرکت مایکروسافت، نقاط ضعفی که سوءاستفاده از آنها بدون نیاز به دخالت و اقدام کاربر باشد، "حیاتی" تلقی شده و اصلاحیه‌هایی که این نوع نقاط ضعف را ترمیم می‌کنند، بالاترین درجه حساسیت یا "حیاتی" را دریافت می‌نمایند. نقاط ضعفی که سوءاستفاده موفق از آنها نیازمند فریب کاربر به انجام کاری باشد یا نیازمند دسترسی فیزیکی به دستگاه هدف باشد، توسط اصلاحیه‌هایی با درجه حساسیت "مهم" برطرف و ترمیم می‌گردند.

مطابق معمول در این ماه نیز، مایکروسافت در قالب یک توصیه‌نامه، اصلاحیه‌های نرم‌افزار Flash Player را که در نسخ جدیدتر مرورگرهای این شرکت گنجانده شده، ارائه کرده است.

از نکات قابل توجه در خصوص مجموعه اصلاحیه های این ماه مایکروسافت، ترمیم دو آسیب‌پذیری "حیاتی" است که مهاجم را قادر می‌کنند تا بدون نیاز به اصالت‌سنجی، به‌صورت از راه دور با ارسال بسته‌های مبتنی بر IPv6 موجب از کار افتان سیستم (CVE-2020-16899) یا اجرای کد مورد نظر خود بر روی سیستم هدف (CVE-2020-16898) شود.

CVE-2020-16951 و CVE-2020-16952 دو آسیب‌پذیری "حیاتی" ترمیم شده دیگر این ماه هستند که نرم‌افزار SharePoint از آنها تأثیر می‌پذیرد. سوءاستفاده از ضعف‌های مذکور مهاجم را قادر به اجرای کد به‌صورت از راه دور می‌کند.

CVE-2020-16947 نیز ضعفی از نوع "اجرای کد به‌صورت از راه دور" (Remote Code Execution) است که نرم‌افزار Outlook از آن تأثیر می‌پذیرد. مهاجم می‌تواند با ارسال یک ایمیل دستکاری شده فرامین خود را پس از باز شدن آن در نرم‌افزار Outlook یا حتی به‌محض ظاهر شدن آن در بخش موسوم به Preview Pane اجرا کند.

CVE-2020-16891 دیگر آسیب‌پذیری "حیاتی" ترمیم شده در این ماه است که راهکار مجازی‌سازی Hyper-V از آن متأثر می‌شود. بهره‌جویی از آن مهاجم یا بدافزار را از روی ماشین میهمان قادر به اجرای کد بر روی سیستم عامل دستگاه میزبان می‌کند.

CVE-2020-16911 هم ضعفی از نوع "اجرای کد به‌صورت از راه دور" در رابط گرافیکی GDI+ در سیستم عامل Windows است که به مهاجم امکان می‌دهد تا از طریق سایت حاوی بهره‌جو، فرامین مورد نظر خود را بر روی دستگاه آسیب‌پذیر مراجعه‌کننده به سایت اجرا کند.

CVE-2020-16915 به‌عنوان دیگر آسیب پذیری "حیاتی" این ماه، ضعفی از نوع "بروز اختلال در حافظه" (Memory Corruption) در Media Foundation است که در نهایت امکان اجرای از راه دور کد را فراهم می‌کند.

فهرست کامل آسیب‌پذیری‌های ترمیم شده توسط مجموعه اصلاحیه‌های ماه اکتبر مایکروسافت در اینجا قابل مطالعه است.

اصلاحیه‌های عرضه شده
در مهر ۱۳۹۹

در مهر ۱۳۹۹، شرکت‌های موزیلا، سیسکو، اپل، گوگل، اس‌آپ، مایکروسافت، ادوبی، مک‌آفی، جونیپر نت‌ورکز، وی‌ام‌وِر، اوراکل و بیت‌دیفندر و بنیاد نرم‌افزاری آپاچی برای برخی محصولات خود اصلاحیه و توصیه‌نامه امنیتی منتشر کردند.

در ماهی که گذشت شرکت موزیلا نیز با ارائه به‌روزرسانی، چندین آسیب‌پذیری را در مرورگر Firefox و نرم‌افزار Thunderbird برطرف کرد که توضیحات آنها در لینک های زیر قابل مطالعه است.

- https://www.mozilla.org/en-US/security/advisories/mfsa2020-42/
- https://www.mozilla.org/en-US/security/advisories/mfsa2020-45/
- https://www.mozilla.org/en-US/security/advisories/mfsa2020-47/

در مهر ۹۹، سیسکو در چندین نوبت اقدام به عرضه اصلاحیه‌های امنیتی برای دامنه گسترده ای از محصولات خود کرد. این به‌روزرسانی‌ها در مجموع، ۱۱۱ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت ۶۳ مورد از آنها "بالا" (High) گزارش شده است. آسیب‌پذیری به حملاتی همچون "اجرای کد به‌صورت از راه دور" (Remote Code Execution)، "از کاراندازی سرویس" (Denial of Service) و "تزریق فرمان" (Command Injection)، از جمله اشکالات مرتفع شده توسط به‌روزرسانی‌های جدید است. توضیحات کامل در مورد به‌روزرسانی‌های عرضه شده در لینک زیر قابل دسترس است.

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

در ۴ مهر ماه، شرکت اپل با انتشار به‌روزرسانی، ضعف‌هایی امنیتی را محصولات زیر ترمیم و اصلاح کرد.

- iCloud for Windows (https://support.apple.com/en-us/HT211846)
- macOS (https://support.apple.com/en-us/HT211849)

سوءاستفاده از برخی از ضعف‌های مذکور، مهاجم را قادر به در اختیار گرفتن کنترل سیستم آسیب‌پذیر می‌کند.

به گزارش شرکت مهندسی شبکه گستر، در ماهی که گذشت شرکت گوگل در دو نوبت با عرضه به‌روزرسانی اقدام به ترمیم آسیب‌پذیری‌های امنیتی مرورگر Chrome کرد. آخرین نسخه این مرورگر که در ۳۰ مهر انتشار یافت ۸۶.۰.۴۲۴۰.۱۱۱ است. فهرست اشکالات مرتفع شده در لینک‌های زیر قابل دریافت و مشاهده است.

- https://chromereleases.googleblog.com/2020/10/stable-channel-update-for-desktop.html
- https://chromereleases.googleblog.com/2020/10/stable-channel-update-for-desktop_20.html

اس‌آپ دیگر شرکتی بود که در مهر ماه ۹۹ با انتشار به روزرسانی امنیتی، چندین آسیب پذیری را در محصولات خود برطرف کرد. از جمله این آسیب پذیری ها می توان به CVE-2020-6364 اشاره کرد که سوءاستفاده از آن مهاجم را قادر به تزریق کد در سیستم عامل در محصولات SAP Solution Manager و SAP Focused Run می کند. جزییات بیشتر را در لینک زیر مطالعه کنید.

- https://onapsis.com/blog/sap-security-notes-October-2020

۲۲ مهر، شرکت مایکروسافت اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی اکتبر منتشر کرد. این اصلاحیه‌ها در مجموع، ۸۷ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می کنند. توضیحات کامل در خصوص اصلاحیه‌های ماه اکتبر مایکروسافت در لینک زیر قابل مطالعه است.

- https://newsroom.shabakeh.net/21799/microsoft-security-update-for-oct-2020.html

مایکروسافت در ۲۴ هم اقدام به انتشار دو اصلاحیه اضطراری برای بخش Codecs Library سیستم عامل Windows 10 - به شناسه CVE-2020-17022 - و نرم افزار Visual Studio - با شناسه CVE-2020-17023 - کرد که بهره جویی از هر کدام از آنها منجر به اجرای کد به صورت از راه دور خواهد شد. جزییات بیشتر را در لینک های زیر بخوانید.

- https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-17022
- https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-17023

ادوبی نیز در ۲۲ مهر ماه، یک آسیب پذیری "حیاتی" (Critical) با شناسه CVE-2020-9746 را در نرم افزار Flash Player ترمیم کرد. همان طور که در لینک زیر اشاره شده سوءاستفاده از آسیب پذیری مذکور امکان اجرای کد به صورت از راه دور را فراهم می کند.

- https://helpx.adobe.com/security/products/flash-player/apsb20-58.html

این شرکت در ۲۵ و ۳۰ مهر هم آسیب پذیری های کشف شده در محصولات زیر را پوشش داد.

- Magento: https://helpx.adobe.com/security/products/magento/apsb20-59.html
- Illustrator: https://helpx.adobe.com/security/products/illustrator/apsb20-53.html
- Dreamweaver: https://helpx.adobe.com/security/products/dreamweaver/apsb20-55.html
- Marketo: https://helpx.adobe.com/security/products/marketo/apsb20-60.html
- Animate: https://helpx.adobe.com/security/products/animate/apsb20-61.html
- After Effects: https://helpx.adobe.com/security/products/after_effects/apsb20-62.html
- Photoshop: https://helpx.adobe.com/security/products/photoshop/apsb20-63.html
- Premiere Pro: https://helpx.adobe.com/security/products/premiere_pro/apsb20-64.html
- Media Encoder: https://helpx.adobe.com/security/products/media-encoder/apsb20-65.html
- InDesign: https://helpx.adobe.com/security/products/indesign/apsb20-66.html
- Creative Cloud Desktop Application: https://helpx.adobe.com/security/products/creative-cloud/apsb20-68.html

در دومین سه شنبه ماه اکتبر، مصادف با ۲۲ مهر، مک‌آفی اقدام به انتشار نسخ زیر کرد.

- Application and Change Control for Windows 8.3.2: https://docs.mcafee.com/bundle/application-change-control-8.3.x-release-notes-windows
- Endpoint Upgrade Assistant 2.9: https://docs.mcafee.com/bundle/endpoint-upgrade-assistant-2.9.x-release-notes
- ePolicy Orchestrator 5.10.0 Update 9: https://docs.mcafee.com/bundle/epolicy-orchestrator-5.10.0-release-notes
- McAfee Active Response 2.4.4: https://docs.mcafee.com/bundle/active-response-2.4.x-release-notes

این نسخ شامل اعمال بهبود و رفع برخی باگ‌های شناسایی شده در نسخ قبلی محصولات مذکور است.

در این ماه، بنیاد نرم‌افزاری آپاچی، با انتشار به‌روزرسانی امنیتی، یک آسیب‌پذیری به شناسه CVE-2020-13943 نرم‌افزار Apache Tomcat ترمیم و اصلاح کرد. بهره‌جویی از این آسیب‌پذیری، مهاجم را قادر به دستیابی به اطلاعات بالقوه حساس می‌کند. اطلاعات بیشتر در لینک زیر قابل دریافت است.

- http://mail-archives.us.apache.org/mod_mbox/www-announce/202010.mbox/%3C2b767c6e-dcb9-5816-bd69-a3bc0771fef3%40apache.org%3E

جونیپر نت‌ورکز نیز ۲۴ مهر با ارائه به‌روزرسانی چندین ضعف امنیتی را محصولات مختلف این شرکت ترمیم کرد. سوءاستفاده از ضعف‌های مذکور مهاجم را قادر به در اختیار گرفتن کنترل دستگاه آسیب‌پذیر می‌کند. جزییات بیشتر در لینک زیر قابل مطالعه است.

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

وی‌اِم‌وِر دیگر شرکتی بود که در مهر ۱۳۹۹ اقدام به انتشار به‌روزرسانی کرد. محصولات زیر از ۶ آسیب‌پذیری ترمیم شده توسط این به‌روزرسانی‌ها تأثیر می‌پذیرند.

- VMware ESXi
- VMware Workstation Pro / Player (Workstation)
- VMware Fusion Pro / Fusion (Fusion)
- NSX-T
- VMware Cloud Foundation

سوءاستفاده از یکی ضعف‌های مذکور با شناسه CVE-2020-3992 که بر اساس استاندارد CVSS درجه حساسیت ۹.۸ از ۱۰ تخصیص داده شده مهاجم را قادر به در اختیار گرفتن کنترل دستگاه آسیب‌پذیر می‌کند. اطلاعات بیشتر در مورد به‌روزرسانی عرضه شده در لینک زیر قابل مطالعه است.

- https://www.vmware.com/security/advisories/VMSA-2020-0023.html

در مهر، اوراکل مطابق با برنامه زمانبندی شده سه‌ماهه خود، با انتشار مجموعه‌به‌روزرسانی‌های موسوم به Critical Patch Update اقدام به ترمیم ۴۰۲ آسیب‌پذیری امنیتی در ده‌ها محصول ساخت این شرکت کرد. بهره جویی از برخی از آسیب‌پذیری‌های مذکور مهاجم را قادر به اجرای کد به‌صورت از راه دور می‌کند که جزییات کامل در خصوص آنها در لینک زیر قابل دریافت است.

- https://www.oracle.com/security-alerts/cpuoct2020.html

در هفتمین ماه از سال ۱۳۹۹ شرکت بیت‌دیفندر اقدام به انتشار نسخ ۶.۶.۲۱.۳۰۴، ۶.۲.۲۱.۱۰۳ و ۴.۱۴.۹۳.۲۰۰۰۹۳ به ترتیب برای محصولات Endpoint Security Tools for Windows، Endpoint Security Tools for Linux و Endpoint Security for Mac کرد که در آنها اصلاحات امنیتی و بهبودهای عملکردی لحاظ شده است. جزییات بیشتر را در لینک‌های زیر بخوانید.

- https://www.bitdefender.com/support/bitdefender-endpoint-security-tools-version-6-6-21-304-release-notes-(windows)-2629.html
- https://www.bitdefender.com/support/bitdefender-endpoint-security-tools-version-6-2-21-103-release-notes-(linux)-2624.html
- https://www.bitdefender.com/support/endpoint-security-for-mac-version-4-14-93-200093-release-notes-2630.html

رویدادها و وقایع امنیتی

اطلاعیه مرکز ماهر

در خصوص حملات سایبری اخیر

مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای کشور (ماهر) در بیانیه‌ای نسبت به اخبار منتشره در خصوص اجرای حملات سایبری بر ضد چند سازمان دولتی واکنش نشان داده است.

متن این بیانیه به شرح زیر است:

پیرو برخی اخبار و شایعات منتشره اخیر لازم به ذکر است که

۱- رخداد حمله مهم سایبری صرفا مربوط به دو سازمان دولتی بوده که مراجع مسوول در حال رسیدگی به موضوع هستند و مرکز ماهر نیز به عنوان پشتیبان آماده کمکها و امدادهای احتمالی مورد نیاز است.

۲- بر اساس برخی تحلیلها و براوردهای فنی، هشدارهای پیشگیرانه برای مسوولین و کارشناسان دولتی در سطح ملی صادر شد که به هیچ وجه به معنای وجود حمله نبوده است.

۳- برخی دستگاههای دولتی بر اساس برداشت یا تحلیل خود پس از دریافت هشدارها اقدام به قطع موقت برخی خدمات و انجام تستهای فنی کردند که به دلیل احتیاط صورت گرفته است. اگر چه از نظر مرکز ماهر این اقدام ضرورتی نداشت.

۴- علیرغم شایعات مطرح شده در فضای مجازی و برخی رسانه ها، شواهدی از حمله گسترده به دستگاه های متعدد دولتی تا این لحظه مشاهده نشده است.

لازم به ذکر است که بخش مهمی از این فعالیت و فعالیتهای مشابه با همکاری تنگاتنگ مراکز آپا سطح کشور انجام می‌شود که قابل تقدیر و برای مرکز ماهر بسیار کلیدی است. لذا علیرغم وجود برخی تنگناهای بودجه ای که برای این مراکز ارزشمند بوجود آمده است حمایتها و همکاری های مرکز ماهر وزارت ارتباطات با مراکز آپا همچنان استمرار دارد و هرگونه قطع همکاری با مراکز فوق قویا تکذیب می‌شود. در انتها مرکز ماهر از هرگونه انتقاد و پیشنهاد کارشناسان جهت بهبود و ارتقاء عملکرد خود استقبال می‌کند.

گزارش‌ها


باج‌افزارهای جدید
۲،۵۰۰،۰۰۰
۲،۰۰۰،۰۰۰
۱،۵۰۰،۰۰۰
۱،۰۰۰،۰۰۰
۵۰۰،۰۰۰
سه‌ماهه دوم
سه‌ماهه سوم
سه‌ماهه چهارم
۲۰۱۷
سه‌ماهه اول
سه‌ماهه دوم
سه‌ماهه سوم
۲۰۱۸
سه‌ماهه چهارم
سه‌ماهه اول
۲۰۱۹

کسب نشان VBSpam+ توسط بیت‌دیفندر، برای بیست‌وچهارمین بار متوالی

شرکت بیت‌دیفندر که حفاظت از بیش از ۵۰۰ میلیون دستگاه در سرتاسر جهان را برعهده دارد برای بیست‌وچهارمین بار پیاپی موفق به کسب نشان VBSpam+ از مؤسسه ارزیابی Virus Bulletin گردید.

کسب این نشان در ۲۴ دوره متوالی، رکورد جدیدی در نتایج بررسی‌های این مؤسسه تلقی می‌شود. رکورد پیشین نیز به نام شرکت بیت‌دیفندر ثبت شده بود.

در آخرین آزمون این مؤسسه که در ماه سپتامبر سال میلادی جاری برگزار شد، راهکار Bitdefender Security for Mail Servers با شناسایی ۹۹.۸۸ درصد از هرزنامه‌ها بدون هر گونه "تشخیص نادرست" (False Positive) بالاترین امتیاز را در مقایسه با رقبای خود کسب کرد. در آزمون مذکور ۱۱ راهکار مطرح ضدهرزنامه شرکت داشتند.

در آزمون سپتامبر VBSpam، ضمن ارزیابی اثربخشی محصولات شرکت‌کننده در مقابله با هرزنامه‌ها، به‌طور ویژه بر روی میزان توانایی آنها در شناسایی ایمیل‌های با پیوست یا نشانی‌های URL که اجرا کردن یا کلیک بر روی آنها منجر به اجرای یک عملیات مخرب بر روی دستگاه قربانی می‌شود تمرکز شده بود.

بیت‌دیفندر از ابتدای راه‌اندازی VBSpam در سال ۲۰۰۹ در این آزمون شرکت داشته و در تمامی موارد موفق به دریافت نشان از این مؤسسه شده است.

بر اساس نظرسنجی انجام شده توسط بیت‌دیفندر حملات فیشینگ از پرچالش‌ترین تهدیدات در حوزه امنیت فناوری اطلاعات محسوب می‌شوند. به نحوی که ۲۵ درصد از شرکت‌کنندگان در نظرسنجی، فیشینگ را یکی از سه تهدید سایبری که در چندین سال گذشته با آن دست به گریبان بوده‌اند معرفی کرده‌اند. ضمن این که هرزنامه‌ها یکی از اصلی‌ترین راه‌های رخنه اولیه مهاجمان به شبکه سازمان در حملات هدفمند محسوب می‌شوند. فناوری‌های ضدهرزنامه بیت‌دیفندر همان‌طور که آزمون اخیر Virus Bulletin گواه آن است راهکاری مؤثر در ایمن نگاه داشتن سازمان از گزند این تهدیدات مخرب هستند.

شرکت بیت‌دیفندر در سال ۲۰۰۱ میلادی در کشور رومانی تأسیس شد و در زمانی اندک، به یکی از عرضه‌کنندگان مطرح نرم‌افزارهای ضدویروس تبدیل شد. شرکت بیت‌دیفندر سازنده یکی از سریع‌ترین و کارآمدترین نرم‌افزارهای ضدویروس در دنیا است.

محصولات بیت‌دیفندر دارنده ده‌ها نشان از مؤسسات ارزیابی مستقل هستند. همچنین محصولات بیت‌دیفندر به دفعات از سوی این مؤسسات معتبر به عنوان برترین ضدویروس سال معرفی شده‌اند.

افتای ریاست جمهوری با همکاری شبکه گستر

شبکه گستر

شرکت مهندسی شبکه گستر

در مهر ماه مرکز مدیریت راهبردی افتای ریاست جمهوری با همکاری شرکت مهندسی شبکه گستر اقدام به تهیه گزارش‌های زیر کرد.

تبدیل یک آگهی‌افزار به توزیع‌کننده بدافزارهای تمام‌عیار

محققان در کنفرانس امنیتی Virus Bulletin به بررسی خانواده‌ای از آگهی افزارها با نام Linkury پرداخته‌اند که اگر چه تا پیش از این عمدتا به توزیع برنامه‌های ناخواسته موسوم به Browser Hijacking معروف بوده اما در عمل از آن به‌عنوان ابزاری برای انتشار بدافزارهای تمام‌عیار بهره گرفته می‌شود. ادامه مطلب را در اینجا بخوانید.

اجرای حملات DDoS؛ اهرم فشار جدید مهاجمان باج‌افزار

در جریان حمله‌ای باج‌افزاری، مهاجمان از تاکتیکی جدید برای وادار کردن قربانی به پرداخت مبلغ اخاذی شده بهره گرفته‌اند. در این تاکتیک در صورت امتناع قربانی در مذاکره با گردانندگان باج‌افزار، سایت سازمان هدف حملات موسوم به DDoS قرار گرفته و حمله تا آمدن قربانی به پشت میز مذاکره تداوم پیدا می‌کند. ادامه مطلب را در اینجا بخوانید.

سرویس باج‌افزاری FONIX را دست‌کم نگیرید

سرویس باج‌افزاری FONIX اگر چه هنوز در ابتدای راه خود قرار دارد اما دارای ویژگی‌هایی متفاوت از هم‌قطاران خود است. از جمله نکات قابل توجه در خصوص FONIX بهره‌گیری آن از چهار الگوریتم رمزگذاری در حین دست‌درازی به هر فایل است. ادامه مطلب را در اینجا بخوانید.

مروری بر متداول‌ترین پیوست‌های ایمیل ناقل بدافزار

شناخت پیوست‌های مخربی که به‌طور گسترده توسط مهاجمان در ایمیل‌های فیشینگ ناقل بدافزار مورد استفاده قرار می‌گیرند نقشی مؤثر در ایمن ماندن از گزند این نوع تهدیدات دارد. ادامه مطلب را در اینجا بخوانید.

آخـرین اخبـار امنیـت فنـاوری اطلاعات

@SGnewsroom

شرکت مهندسی شبکه گستر در سال ۱۳۷۰ تأسیس گردید و اولین شرکت ایرانی است که در زمینه نرم‌افزارهای ضدویروس فعالیت تخصصی و متمرکزی را آغاز کرده است. در ابتدا، همکاری مشترکی بین شرکت مهندسی شبکه گستر و شرکت انگلیسی S & S International (تولیدکننده ضدویروس مشهور Toolkit) آغاز گردید. در مدت کوتاهی، با فعالیت شبکه گستر به عنوان نماینده رسمی و انحصاری S & S International در ایران، به تدریج ضدویروس Dr Solomon's Toolkit به محبوب‌ترین ضدویروس در ایران تبدیل شد. پس از خرید شرکت S & S International توسط شرکت McAfee در سال ۱۳۷۷، شرکت شبکه گستر نیز مانند دیگر نمایندگان بین‌المللی فعالیت خود را بر روی نرم‌افزارهای ضدویروس McAfee ادامه داد. اکنون نیز شبکه گستر به عنوان فروشنده مجاز (Authorized Reseller) در منطقه خاورمیانه، به ارائه محصولات و خدمات در ایران اقدام می‌نماید. در سال ۱۳۸۴ شرکت مهندسی شبکه گستر موفق به کسب نمایندگی رسمی شرکت آلمانی Astaro، سازنده محصولات مدیریت یکپارچه تهدیدات (Unified Threat Management) گردید. به دنبال رشد چشمگیر و موفقیت جهانی محصولات امنیتی شرکت Astaro، در سال ۱۳۹۰ شرکت Sophos انگلیس، اقدام به خرید این شرکت آلمانی نمود. به دنبال این نقل و انتقال، شرکت مهندسی شبکه گستر با همکاری با شرکت Sophos، فعالیت خود را در این زمینه ادامه داده و اکنون محصولات Astaro سابق را تحت نام Sophos در ایران عرضه می‌نماید. از سال ۱۳۹۱ شرکت مهندسی شبکه گستر عرضه محصولات ضدویروس Bitdefender را به عنوان نماینده و توزیع‌کننده (Distributor) رسمی در ایران آغاز کرد. عرضه محصولات ضدویروس Bitdefender در کنار محصولات امنیتی McAfee، پاسخی به شرایط و نیازهای متفاوت کاربران و مدیران شبکه بوده است. ضدویروس چابک‌تر، مدیریت آسان‌تر و محصولی مقرون به صرفه‌تر، انتظارات برخی از کاربران و مدیران شبکه بود که با عرضه محصولات ضدویروس Bitdefender، شبکه گستر به نیازهای این بخش از بازار پاسخ داد. شرکت مهندسی شبکه گستر افتخار دارد که مجری برخی از بزرگترین پروژه‌های نصب و راه‌اندازی و طولانی مدت‌ترین قراردادهای نگهداری و پشتیبانی محصولات امنیت شبکه در کشور بوده است. این شرکت علاوه بر خدمات‌دهی به هزاران شرکت و سازمان که صدها هزار کاربر را در کشور شامل می‌شوند، دارای شبکه نمایندگی فروش و پشتیبانی در سراسر کشور نیز می‌باشد.

شرکت مهندسی شبکه گستر

تهران ۱۹۶۸۶، خیابان شهید دستگردی (ظفر)، شماره ۲۷۳

تلفن / دورنگار	۴۲۰۵۲ - ۰۲۱
رایانامه	info@shabakeh.net
تارنمای شرکت	www.shabakeh.net
خدمات پس از فروش و پشتیبانی	my.shabakeh.net
مرکز آموزش	events.shabakeh.net
اتاق خبر	newsroom.shabakeh.net