ماهنامه

امنیت فناوری اطلاعات

شبکه گستر

امنیت شما | وظیفه ما

تیر

۱۳۹۹

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 تیر ماه ۱۳۹۹ پرداخته شده است.

در این ماهنامه جزییات گزارشی ارائه شده که در آن شرکت مایکروسافت به تکنیک‌های اخیر مهاجمان در حمله به سرورهای Exchange پرداخته است. بر این اساس در حالی که یکی از روش‌های متداول مهاجمان در دستیابی به سرورهای Exchange بکارگیری ترفندهای مهندسی اجتماعی برای سرقت اطلاعات اصالت‌سنجی کاربران و در ادامه استفاده از آنها برای رخنه در سطح شبکه و در نهایت رسیدن به سرور Exchange است در کارزارهای اخیر، نفوذگران با بهره‌جویی (Exploit) از آسیب‌پذیری‌های از نوع "اجرای کد به‌صورت از راه دور" کنترل این سرورها در اختیار هکرها قرار می‌گیرد.

همچنین در این ماهنامه قابلیت‌های جدید آخرین نسخه از بدافزار معروف TrickBot مورد بررسی قرار گرفته است. از جمله این قابلیت‌ها می‌توان به استخراج وضوح صفحه نمایش (Screen Resolution) قربانی برای اطمینان از اجرا نشدن در بسترهای مجازی اشاره کرد.

باج‌افزار WastedLocker دیگر تهدیدی است که در این ماهنامه مورد تحلیل قرار گرفته است. WastedLocker نمونه‌ای نسبتاً جدید از باج‌افزارهای هدفمند است که به نظر می‌رسد توسط گروه Evil Corp توسعه داده شده است. این گروه منتسب به مهاجمان روسی، پیش‌تر نیز در انتشار اسب تروای بانکی Dridex و باج‌افزار BitPaymer نقش داشته است. برخی منابع، درآمد Evil Corp از دو بدافزار مذکور را ده‌ها میلیون دلار برآورد می‌کنند. دو نفر از گردانندگان این گروه در فهرست افراد تحت تعقیب وزارت دادگستری آمریکا قرار داشته و FBI در ازای هر گونه اطلاعاتی که منجر به دستگیری این متهمان شود پاداشی ۵ میلیون دلاری تعیین کرده است.

در تیر ۱۳۹۹، شرکت‌های ادوبی، گوگل، وی‌ام‌ور، سیسکو، پائلو آلتو نت‌ورکز، نت‌گیر، مایکروسافت، موزیلا، اوراکل و اپل، گروه سامبا و بنیاد آپاچی اقدام به انتشار اصلاحیه و توصیه‌نامه امنیتی برای برخی از محصولات خود کردند. جزییات این اصلاحیه‌ها و گزارش‌هایی دیگر در حوزه امنیت فناوری اطلاعات را 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 Black Kingdom

این باج‌افزار که با نام‌های GAmmAWare و DemonWare نیز شناخته می‌شود در ازای آنچه که گردانندگان آن بازگرداندن فایل‌ها به حالت اولیه می‌خوانند در مهلتی مشخص مبلغی تا ۱۰ هزار دلار را از قربانی اخاذی می‌کند. در سال میلادی جاری گردانندگان Black Kingdom به‌منظور توزیع این باج‌افزار اقدام به بهره‌جویی (Exploit) از آسیب‌پذیری CVE-2019-11510 در نرم‌افزار Pulse Secure VPN کردند.

باج‌افزار Avaddo

باج‌افزار Avaddon از اواسط سال ۲۰۲۰ در قالب "باج‌افزار به‌عنوان سرویس" (RaaS) در بازارهای زیرزمینی مهاجمان به فروش رسانده می‌شود. خریداران این سرویس ملزم به تبعیت از قوانینی همچون به اشتراک نگذاشتن نشانی پنل مدیریتی و هدف قرار ندادن کاربران در کشورهای مشترک‌المنافع هستند. این باج‌افزار از طریق کارزارهای هرزنامه‌ای که به آنها یک دانلودکننده JavaScript در قالب تصویر JPG پیوست شده توزیع می‌شود. در کارزار از تکنیک‌های مختلف نظیر بکارگیری پروسه معتبر PowerShell، بهره‌گیری از Background Intelligent Transfer Service - به اختصار BITS -، اسکریپت‌نویسی، رمزگذاری و استخدام Windows Management Instrumentation - به اختصار WMI - به‌منظور اجرای فایل مخرب و ماندگار کردن باج‌افزار استفاده شده است.

عملیات Australia

در این کارزار مهاجمان احتمالا وابسته به یک دولت، سازمان‌ها و شرکت‌های استرالیایی را به‌طور خاص هدف حملات پیچیده قرار دادند. در جریان این حملات به‌شدت از نمونه‌کدهای اثبات‌گر (PoC) بهره‌جوها، شل‌های وب و سایر ابزارهای کد باز (Open-source) استفاده شده است. روش اصلی رخنه اولیه به شبکه قربانی، بهره‌جویی از آسیب‌پذیری‌هایی همچون CVE-2019-18935 در Telerik UI، CVE-2019-19781 در Citrix و CVE-2019-0604 در SharePoint گزارش شده است.

عملیات Qbot

اسب تروای بانکی Qbot بیش از یک دهه است که سازمان‌ها و کاربران را در نقاط مختلف جهان هدف قرار می‌دهد. این بدافزار که با نام‌های مختلفی همچون Qakbot، Akbot و Pinkslipbot شناخته می‌شود همچنان بر روی سرقت اطلاعات حساسی نظیر داده‌های مرورگر، داده‌های مالی و نام‌های کاربری و رمز عبور تمرکز دارد. در سال ۲۰۲۰ نسخه جدید این بدافزار از تکنیک‌های جدیدی شامل تزریق کد مخرب به explorer.exe و ساخت کلید Run در محضرخانه (Registry) برای ماندگاری پس از راه‌اندازی مجدد بهره می‌گیرد. در آخرین نسخه تمرکز مهاجمان بر روی مؤسسات مالی در آمریکا، کانادا و هلند بوده است.

عملیات Vendetta RoboSki

گروه Vendetta که از اوایل سال ۲۰۲۰ ظهور کرد در کارزار RoboSki

عملیات Hidden Story

گروه InvisiMole نهادهای نظامی و دفاعی، سیاسی و دولتی

اقدام به سرقت اطلاعات حساس سازمان‌ها از طریق ایمیل‌های هدفمند فیشینگ کرده است. در این کارزار از نامه‌های جعلی در ظاهر مرتبط با سازمان‌های نامدار برای متقاعد کردن قربانیان به باز کردن پیوست‌های مخرب استفاده شده است. سازمان‌ها در نقاط مختلف شامل آمریکای شمالی، اروپای شرقی، اروپای غربی، جنوب شرق آسیا و آفریقای شمالی هدف این کارزار قرار گرفته‌اند. پس از باز شدن پیوست، کد مخرب در حافظه اجرا شده و از سد ابزارهای موسوم به Sandbox و محصولات ضدویروس عبور کرده و در ادامه اقدام به دانلود فایل‌های اضافی بر روی سیستم آلوده می‌کند.

آسیب‌پذیری CVE-2020-9633

CVE-2020-9633 که نسخه ۳۲٫۰٫۰٫۳۷۱ و نسخ قبل از آن در نرم‌افزار Adobe Flash Player از آن تأثیر می‌پذیرند مهاجم را قادر به اجرای کد بر روی دستگاه قربانی می‌کند.

آسیب‌پذیری CVE-2020-1021

CVE-2020-1021، ضعفی از نوع "ترفیع امتیازی" (Elevation of Privilege) در سیستم عامل Windows است که از نحوه مدیریت نادرست فایل‌ها توسط بخش Windows Error Reporting ناشی می‌شود.

در اروپای شرقی با مجموعه ابزارهایی به روز شده مورد حمله قرار دادند. بدافزار مورد استفاده در این حملات از تکنیک‌های مختلفی شامل سوءاستفاده از برنامه‌های معتبر و بهره‌جویی از فایل‌های اجرایی آسیب‌پذیر شامل EternalBlue و BlueKeep برای توزیع در سطح شبکه استفاده کرده است. این گروه همچنین از قابلیت Data Protection API در سیستم عامل Windows برای رمزگذاری و DNS Tunneling برای برقراری ارتباط با سرورهای فرماندهی (C۲) استفاده می‌کند.

آسیب‌پذیری CVE-2020-1281

CVE-2020-1281، ضعفی از نوع "اجرای کد به‌صورت از راه دور" (Remote Code Execution) است که از نحوه اعتبارسنجی نادرست بخش OLE در سیستم عامل Windows ناشی می‌شود.

آسیب‌پذیری CVE-2020-1441

CVE-2020-1441، ضعفی از نوع "ترفیع امتیازی" که از نحوه مدیریت اشیاء (Object) در حافظه توسط بخش Windows Spatial Data Service در سیستم عامل Windows ناشی می‌شود. سوءاستفاده از این آسیب‌پذیری مهاجم با سطح دسترسی محلی (Local) را قادر به اجرای برنامه 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، ASN1،Sage، CryptoShield، Nemty، CrypMIC، Mobef، Paradise، Dxh26wam، GandCrab Revenge، CryptoMix، BartCrypt، Spora، Erebus، Mole، Cry، Fess-mant، 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 سرفروماندهی 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 Win-dows 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
Mikroceen	Mikroceen یک اسب تروای دسترسی از راه دور است که از اواخر سال 2017 سازمان‌ها را مورد حمله قرار داده است. گفته می شود که مهاجمان پشت پرده این وابسته به یک دولت هستند. سازمان‌های دولتی و شرکت‌های فعال در حوزه مخابرات و گاز در آسیای مرکزی اصلی‌ترین قربانیان این کارزار بوده‌اند.
Himera & AbSent-Loader	گردانندگان ناشناس این کارزار با بهره‌گیری از ترس عمومی از همه‌گیری بیماری کرونا کاربران را متقاعد به اجرا کردن فایل Word مخرب پیوست شده به هرزنامه‌های مورد استفاده در فیشینگ‌های هدفمند خود می‌کنند. به‌محض باز شدن پیوست توسط قربانی در جریان حمله ای چندمرحله‌ای فایل‌های مخرب دیگر دریافت شده و از طریق آنها راهکارهای دفاعی بی‌اثر شده و فرامین زمانبندی‌شده (Scheduled Task) برای ماندگاری بدافزار ایجاد می‌شود.
Kazuar	گروه Turla با به‌روزرسانی Kazuar و با بهره‌گیری از یک مبهم‌ساز (Obfuscator) مبتنی بر .Net تحلیل این درب‌پشتی (Backdoor) را بیش از قبل دشوار کرده است. مهاجمان با استفاده از عنوان معروف سایت Sysinternals این طور القا می‌کنند که درب‌پشتی یکی از ابزارهای ارائه شده در این سایت است. بر اساس آمار مک‌آفی برخی نمونه‌های این درب‌پشتی از جولای 2019 تا 2020 فعال بوده‌اند. اما تعداد کم موارد شناسایی شده، هدفمند بودن حملات آن را نشان می‌دهد.
FlowCloud	گروه TA410 با هدف قرار دادن برخی شرکت‌ها در آمریکا با نرم‌افزار مخرب FlowCloud اقدام به استخراج اطلاعات حساس شامل کلیدهای فشرده‌شده، تصاویر فعالیت کاربر و فایل‌های با اهمیت و ارسال آنها سرورهای فرماندهی خود کردند. مهاجمان از چندین دامنه و سرویس‌هایی همچون Drop-box برای میزبانی نرم‌افزار مخرب و ارسال داده‌های سرقت شده استفاده کردند. آلودگی اولیه شامل ارسال ایمیل‌های فیشینگ هدفمند یا پیوست فایل exe یا doc در ظاهر اسناد متعلق به شرکت‌های معتبر است.
Australia	در این کارزار مهاجمان احتمالا وابسته به یک دولت، سازمان‌ها و شرکت‌های استرالیایی را به‌طور خاص هدف حملات پیچیده قرار دادند. در جریان این حملات به‌شدت از نمونه‌کدهای اثبات‌گر (PoC) بهره‌جوها، شل‌های وب و سایر ابزارهای کد باز (Open-source) استفاده شده است. روش اصلی رخنه اولیه به شبکه قربانی، بهره‌جویی از آسیب‌پذیری‌هایی همچون CVE-2019-18935 در Telerik UI CVE-2019-19781 در Citrix و CVE-2019-0604 در SharePoint گزارش شده است.
Qbot	اسب تروای بانکی Qbot بیش از یک دهه است که سازمان‌ها و کاربران را در نقاط مختلف جهان هدف قرار می‌دهد. این بدافزار که با نام‌های مختلفی همچون Qakbot، Akbot و Pinkslipbot شناخته می‌شود همچنان بر روی سرقت اطلاعات حساسی نظیر داده‌های مرورگر، داده‌های مالی و نام‌های کاربری و رمز عبور تمرکز دارد. در سال 2020 نسخه جدید این بدافزار از تکنیک‌های جدیدی شامل تزریق کد مخرب به explorer.exe و ساخت کلید Run در محضرخانه (Registry) برای ماندگاری پس از راه‌اندازی مجدد بهره می‌گیرد. در آخرین نسخه تمرکز مهاجمان بر روی مؤسسات مالی در آمریکا، کانادا و هلند بوده است.

بسته بهره‌جو	توضیحات
Netwire	Netwire یک ابزار دسترسی از راه دور است که بر روی سرقت رمزهای عبور و ضبط کلیدهای فشرده شده توسط کاربر تمرکز دارد. در ژوئن 2020 گزارش شد که این بدافزار کاربران ایتالیایی زبان را هدف قرار داده است. نسخه مورد استفاده در آن کارزار در زنجیره حمله تکامل داده شده بود. بدافزار در قالب پیوست مخرب ایمیلی که ماکروی XML در آن تزریق شده توزیع می‌شد.
Dark Basin	در جریان کارزار Dark Basin شرکت‌های فعال در حوزه‌هایی خاص در چندین کشور مورد هدف قرار گرفتند. از جمله این حوزه‌ها می‌توان به گروه‌های وکلاتی، روزنامه‌نگاری، نهادهای رسمی دولتی، مالی، غیرانتفاعی، مدافع حقوق بشر، انرژی و شرکت‌های دارویی اشاره کرد. رخنه اولیه از طریق ایمیل‌های فیشینگ هدفمند حاوی نشانی‌های URL کوتاه‌شده‌ای که با کلیک بر روی آنها کاربر به سایت‌های جعلی در ظاهر Google Facebook، Yahoo Mail، Mail و مواردی از این دست هدایت شده و در آنجا اطلاعات اصالت‌سنجی کاربران ناآگاه سرقت می‌شد.
RoboSki	گروه Vendetta که از اوایل سال 2020 ظهور کرد در کارزار RoboSki اقدام به سرقت اطلاعات حساس سازمان‌ها از طریق ایمیل‌های هدفمند فیشینگ کرده است. در این کارزار از نامه‌های جعلی در ظاهر مرتبط با سازمان‌های نامدار برای متقاعد کردن قربانیان به باز کردن پیوست‌های مخرب استفاده شده است. سازمان‌ها در نقاط مختلف شامل آمریکای شمالی، اروپای شرقی، اروپای غربی، جنوب شرق آسیا و آفریقای شمالی هدف این کارزار قرار گرفته‌اند. پس از باز شدن پیوست، کد مخرب در حافظه اجرا شده و از سد ابزارهای موسوم به Sandbox و محصولات ضدویروس عبور کرده و در ادامه اقدام به دانلود فایل‌های اضافی بر روی سیستم آلوده می‌کند.
Hidden Story	گروه InvisiMole نهادهای نظامی و دفاعی، سیاسی و دولتی در اروپای شرقی با مجموعه ابزارهایی به روز شده مورد حمله قرار دادند. بدافزار مورد استفاده در این حملات از تکنیک‌های مختلفی شامل سوءاستفاده از برنامه‌های معتبر و بهره‌جویی از فایل‌های اجرایی آسیب‌پذیر شامل EternalBlue و BlueKeep برای توزیع در سطح شبکه استفاده کرده است. این گروه همچنین از قابلیت Data Pro-tection API در سیستم عامل Windows برای رمزگذاری و DNS Tunneling برای برقراری ارتباط با سرورهای فرماندهی (C2) استفاده می‌کند.

۱۰ باج‌افزار با بیشترین انتشار

بسته بهره‌جو	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.
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.
Ragnar Locker	مهاجمان Ragnar Locker در جریان اجرای عملیات شناسایی، اطلاعات حساس را سرقت کرده و قربانی را تهدید می کنند که در صورت عدم پرداخت باج که معمولاً مبالغ هنگفت صدها هزار دلاری است اقدام به انتشار عمومی داده ها خواهند کرد.
Mailto	این باج‌افزار که با نام Netwalker نیز شناخته می‌شود شبکه‌های سازمانی را مورد هدف قرار می‌دهد. نخستین نسخه آن در آگوست 2019 شناسایی شد و طی یک سال اخیر نسخ جدیدی از آن منتشر شده است. Mailto فایل‌ها را با Salsa20 رمزگذاری کرده و پسوندی تصادفی را به آنها الصاق می‌کند. این باج‌افزار از تکنیک جدیدی با عنوان Reflective DLL Loading برای تزریق DLL از طریق حافظه استفاده می‌کند.
Nefilim	این باج‌افزار پس از رمزگذاری فایل‌های قربانی با الگوریتم AES-128 اقدام به الصاق پسوند ".NEFILIM" به آنها می‌کند. در کدهای مورد استفاده Nefilim شباهت‌هایی با باج‌افزار Nemty به چشم می‌خورد. اما بر خلاف آن از سیستم پرداخت در بستر شبکه ناشناس TOR استفاده نکرده و از ایمیل برای تبادل اطلاعات در خصوص پرداخت باج استفاده می کند. مهاجمان این باج افزار تهدید می‌کنند که در صورت پرداخت نشدن باج ظرف 7 روز اطلاعات قربانی را به صورت به اشتراک خواهند گذاشت.
Lockbit	این باج‌افزار که در قالب "باج‌افزار به‌عنوان سرویس" عرضه می‌شود در سپتامبر 2019 پس از آنکه گردانندگان آن ظرف چند ساعت شبکه‌ای سازمانی را هک و فایل‌های تمامی سیستم‌ها را رمزگذاری کردند به معروفیت رسید. در جریان آن حمله مهاجمان با سعی‌وخطا (Brute-force) بر ضد یک سرویس‌دهنده VPN تحت وب آسیب‌پذیر موفق به رخنه به شبکه قربانی شدند. همچنین از SMB برای اجرای عملیات شناسایی و در ادامه بهره‌گیری از Microsoft Remote Access Server برای دسترسی از راه دور به سیستم‌ها استفاده کردند. Lockbit تلاش می‌کند که چندین سرویس شامل سرویس‌های متعلق به محصولات ضدویروس را متوقف کند.

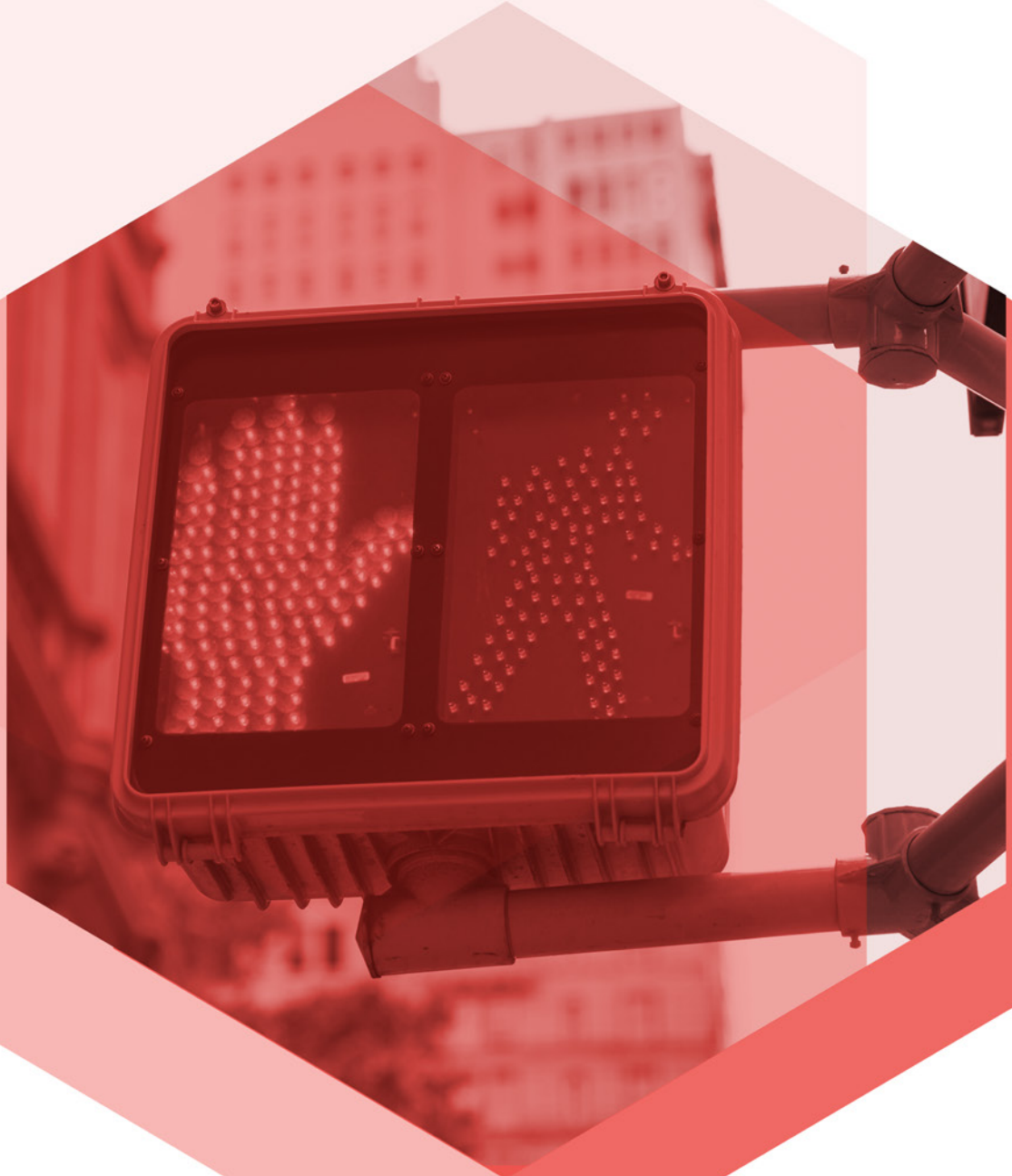
بسته بهره‌جو	توضیحات
Black Kingdom	این باج‌افزار که با نام‌های GAmmAWare و DemonWare نیز شناخته می‌شود در ازای آنچه که گردانندگان آن بازگرداندن فایل‌ها به حالت اولیه می‌خوانند در مهلتی مشخص مبلغی تا 10 هزار دلار را از قربانی اخاذی می‌کند. در سال میلادی جاری گردانندگان Black Kingdom به‌منظور توزیع این باج‌افزار اقدام به بهره‌جویی (Exploit) از آسیب‌پذیری CVE-2019-11510 در نرم‌افزار Pulse Secure VPN کردند.
Tycoon	خانواده جدیدی از باج‌افزارهاست که در اواخر سال 2019 شناسایی شد و تا اوسط سال میلادی جاری در حال تکامل بوده است. این باج‌افزار پسوندهای مختلفی همچون thanos، grinch و redrum را به فایل‌های رمز شده می‌چسباند. Tycoon برای رمزگذاری از الگوریتم‌های RSA و AES بهره می‌گیرد. روش برقراری ارتباط با باج‌گیران از طریق ایمیل بوده و در صورت عدم پرداخت باج ظرف 24 ساعت مبلغ آن دو برابر می‌شود. رخنه اولیه از طریق RDP است و Tycoon دستگاه‌های با هر یک از سیستم‌های عامل Windows و Linux را هدف قرار می‌دهد.
Avaddo	باج‌افزار Avaddon از اواسط سال 2020 در قالب "باج‌افزار به‌عنوان سرویس" (RaaS) در بازارهای زیرزمینی مهاجمان به فروش رسانده می‌شود. خریداران این سرویس ملزم به تبعیت از قوانینی همچون به اشتراک نگذاشتن نشانی پنل مدیریتی و هدف قرار ندادن کاربران در کشورهای مشترک‌المنافع هستند. این باج‌افزار از طریق کارزارهای هرزنامه‌ای که به آنها یک دانلودکننده JavaScript در قالب تصویر JPG پیوست شده توزیع می‌شود. در کارزار از تکنیک‌های مختلف نظیر بکارگیری پروسه معتبر PowerShell، بهره‌گیری از Background Intelligent Transfer Service - به اختصار BITS -، اسکریپت‌نویسی، رمزگذاری و استخدام Windows Management Instrumentation - به اختصار WMI - به‌منظور اجرای فایل مخرب و ماندگار کردن باج‌افزار استفاده شده است.

۱۰ آسیب‌پذیری شاخص

بسته بهره‌جو	توضیحات
CVE-2019-11510	ضعفی در Pulse Connect Secure است که نسخه 8.2 و نسخ قبل از 8.2R12.1، نسخه 8.3 و نسخ قبل از 8.3R7.1 و نسخه 9.0 و نسخ قبل از 9.0R3.4 این محصول امنیتی Pulse Secure از آن تأثیر می‌پذیرد. بهره‌جویی از این آسیب‌پذیری مهاجم از راه دور را قادر می‌کند تا با ارسال یک URI دستکاری شده فایل‌های بالقوه حساس را بخواند.
CVE-2020-9633	CVE-2020-9633 که نسخه 32.0.0.371 و نسخ قبل از آن در نرم‌افزار Adobe Flash Player از آن تأثیر می‌پذیرند مهاجم را قادر به اجرای کد بر روی دستگاه قربانی می‌کند.
CVE-2020-1281	CVE-2020-1281، ضعفی از نوع "اجرای کد به‌صورت از راه دور" (Remote Code Execution) است که از نحوه اعتبارسنجی نادرست بخش OLE در سیستم عامل Windows ناشی می‌شود.
CVE-2020-1021	CVE-2020-1021، ضعفی از نوع "ترفیع امتیازی" (Elevation of Privilege) در سیستم عامل Windows است که از نحوه مدیریت نادرست فایل‌ها توسط بخش Windows Error Reporting ناشی می‌شود.
CVE-2020-3342	ضعفی در بخش به‌روزرسانی محصول Cisco Webex Meetings Desktop App for Mac است که مهاجم اصالت‌سنجی نشده را قادر می‌کند تا به‌صورت از راه دور اقدام به اجرای کد کند. این آسیب‌پذیری از اعتبارسنجی نادرست رمزگذاری مورد استفاده در حفاظت از فایل‌ها که توسط برنامه به عنوان بخشی از به روزرسانی دریافت می‌شوند ناشی می‌شود. هدایت کاربر به یک سایت و در ادامه دریافت فایل‌هایی مشابه با آنچه که به طور معمول از سایت Webex دانلود می‌شود می‌تواند از جمله سناریوهای حمله باشد. در نتیجه اعتبارسنجی ناصحیح کد با سطح دسترسی کاربر جاری اجرا می‌شود.
CVE-2020-3361	ضعفی در Cisco Webex Meetings و Cisco Webex Meetings Server است که مهاجم اصالت‌سنجی‌نشده و از راه دور را قادر به دسترسی یافتن به سایت Webex می‌کند. این ضعف امنیتی از مدیریت نادرست توکن‌های اصالت‌سنجی با یک سایت آسیب‌پذیر Webex ناشی می‌شود. مهاجم با بهره‌جویی از CVE-2020-3361 از طریق ارسال درخواست‌های دستکاری شده به یک سایت آسیب‌پذیر Cisco Webex Meetings یا Cisco Webex Meetings Server قادر به دستیابی یافتن به سایت Webex با سطح دسترسی کاربر دیگر است.
CVE-2020-3263	ضعفی در Cisco Webex Meetings Desktop App که مهاجم اصالت‌سنجی‌نشده و از راه دور را قادر به اجرای برنامه بر روی سیستم می‌کند. آسیب‌پذیری مذکور از اعتبارسنجی ناصحیح نشانی‌های URL ورودی ناشی می‌شود. مهاجم می‌تواند با تشویق کاربر به دنبال کردن یک URL مخرب از این آسیب‌پذیری بهره‌جویی کرده و از طریق یک برنامه، برنامه‌های دیگری که بر روی سیستم است را اجرا کند. یا در صورتی که فایل‌های مخربی بر روی سیستم یا مسیر شبکه‌ای قابل دسترس جاسازی شده باشند منجر به اجرا شدن آنها شود.

بسته بهره‌جو	توضیحات
CVE-2020-5740	اعتبارسنجی نادرست ورودی در Plex Media Server در سیستم عامل Windows است که مهاجم اصالت‌سنجی نشده با دسترسی محلی را قادر به اجرای کد Python با سطح دسترسی SYSTEM می‌کند.
CVE-2020-5741	ضعفی موسوم به Deserialization of Untrusted Data در Plex Media Server در سیستم عامل Windows است که مهاجم اصالت‌سنجی‌نشده با دسترسی محلی را قادر به اجرای کد Python می‌کند.
CVE-2020-1441	یک آسیب‌پذیری از نوع ترفیع امتیازی در سیستم عامل Windows است که از نحوه مدیریت اشیا در حافظه توسط Windows Spatial Data Service ناشی می‌شود. بهره‌جویی موفق مهاجم با دسترسی محلی را قادر به اجرای برنامه می‌کند.

هشدارهای امنیتی



افزایش سوءاستفاده مهاجمان
از آسیب‌پذیری‌های Exchange

مایکروسافت در گزارشی به تکنیک‌های اخیر مهاجمان در حمله به سرورهای Exchange پرداخته است.

مبنای اطلاعات ارائه شده در این گزارش تحلیل‌های صورت گرفته در خصوص کارزارهای اخیری است که در جریان آنها مهاجمان اقدام به توزیع کدهای موسوم به Web Shell بر روی سرورهای Exchange قابل دسترس بر روی اینترنت می‌کنند.

در مراحلی از این حملات چندین تکنیک بدون فایل (Fileless) مورد استفاده قرار گرفته تا شناسایی آنها توسط راهکارهای امنیتی را بیش از پیش دشوار کند.

به گزارش شرکت مهندسی شبکه گستر، در حالی که یکی از روش‌های متداول مهاجمان در دستیابی به سرورهای Exchange بکارگیری ترفندهای مهندسی اجتماعی و تکنیک‌های موسوم به دانلودهای سرراهی (Drive-by Download) برای سرقت اطلاعات اصالت‌سنجی کاربران سازمان و در ادامه استفاده از آنها برای رخنه در سطح شبکه و در نهایت رسیدن به سرور Exchange است در کارزارهای اخیر با بهره‌جویی (Exploit) از آسیب‌پذیری‌های از نوع "اجرای کد به‌صورت از راه دور" کنترل سرور در اختیار هکرها قرار می‌گیرد.

به گفته مایکروسافت در بسیاری موارد پس از آنکه مهاجمان کنترل سرور Exchange را در کنترل می‌گیرند اقدام به توزیع Web Shell در یکی از مسیرهای قابل دسترس در بستر وب سرور می‌کنند.

Web Shell ابزارهایی هستند که هکرها با توزیع آنها بر روی سرور هک شده جای پای خود را محکم کرده، فرامین و کدهای مورد نظر را به‌صورت از راه دور بر روی آن اجرا کرده، بدافزارهای جدید را دریافت نموده و دامنه نفوذ خود را در سطح شبکه گسترش می‌دهند.

از برنامه‌هایی که برای عرضه امکانات Ruby، Python، Perl، web shell و اسکریپت‌های شل Unix طراحی شده‌اند گرفته تا افزونه‌ها و تکه‌کدهای PHP یا ASP که در برنامه‌های وب تزریق شده‌اند همگی می‌توانند مهاجمان را قادر به آپلود Web Shell کنند.

در ماه آوریل نیز آژانس امنیت ملی آمریکا و اداره Signals Directorate استرالیا در بیانیه‌ای مشترک نسبت به افزایش حملات به سرورهای وب آسیب‌پذیر برای توزیع درب‌های پشتی مبتنی بر Web Shell هشدار دادند.

محققان مایکروسافت اعلام کرده‌اند که در حملات اخیر بر ضد سرورهای Exchange شاهد بهره‌جویی از آسیب‌پذیری‌های امنیتی و به‌طور خاص سوءاستفاده از ضعف امنیتی CVE-2020-0688 در این سرویس‌دهنده بوده‌اند. این در حالی است که اصلاحیه آسیب‌پذیری مذکور ماه‌ها است که در دسترس قرار گرفته است.

CVE-2020-0688 که بخش Exchange Control Panel - به اختصار ECP - از آن تأثیر می‌پذیرد از عدم توانایی Exchange در ایجاد کلیدهای رمزگذاری منحصربه‌فرد در زمان نصب ناشی می‌شود.

بهره‌جویی موفق از CVE-2020-0688 مهاجم را قادر به اجرای کد به‌صورت از راه دور با سطح دسترسی SYSTEM بر روی سرور آسیب‌پذیر می‌کند.

نتایج تحقیقی که در ماه آوریل انجام شد نشان می‌داد که ۸۲.۵ درصد از سرورهای Exchange نسبت به CVE-2020-0688 آسیب‌پذیر هستند.

سرویس‌دهندگان Exchange به دلیل نقش حساس آنها در سازمان‌ها و اهمیت داده‌های آنها از جمله سرورهایی هستند که محافظت ازشان باید همواره در اولویت قرار داشته باشد.

نصب کامل اصلاحیه‌های امنیتی، بهره‌گیری از راهکارهای ضدبدافزار، بازبینی مستمر گروه‌ها و نقش‌های حساس از لحاظ اعمال هر گونه تغییر مشکوک، در حداقل نگاه داشتن سطوح دسترسی و بررسی فوری فعالیت‌های مشکوک از جمله نکاتی است که رعایت آنها نقشی کلیدی در ایمن نگاه داشتن این سرورها از گزند تهدیدات سایبری دارد.

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

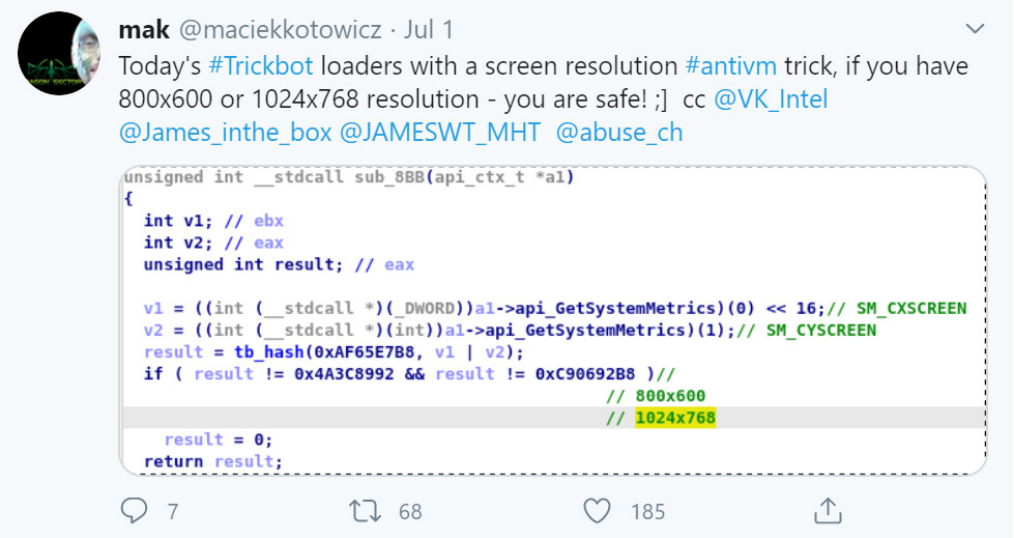
https://www.microsoft.com/security/blog/2020/06/24/defending-exchange-servers-under-attack/

بررسی وضوح صفحه نمایش،
قابلیت جدید TrickBot

نسخه جدید بدافزار معروف TrickBot برای اطمینان از اجرا نشدن در بسترهای مجازی اقدام به بررسی وضوح صفحه نمایش (Screen Resolution) قربانی می‌کند.

تحلیلگران بدافزار معمولاً با بهره‌گیری از ابزارهای مختلف، فایل‌های مشکوک را در بسترهای مجازی مورد بررسی قرار می‌دهند. به همین خاطر بدافزارهای پیشرفته مجهز به قابلیت موسوم به ضدماشین‌مجازی (Anti-VM) تلاش می‌کنند تا با روش‌هایی همچون جستجوی پروسه‌های خاص، سرویس‌های سیستم عامل، نام ماشین، نشانی MAC و مشخصه‌های CPU از اجرا شدن و افشای عملکرد خود در بستر مورد استفاده تحلیلگران بدافزار یا سیستم‌های معروف به سندباکس خودداری کنند.

اکنون محققان اعلام کرده‌اند که بررسی میزان وضوح صفحه نمایش دستگاه قربانی به‌عنوان یک روش جدید برای شناسایی بسترهای مجازی به فهرست قابلیت‌های TrickBot افزوده شده است. بدین‌ترتیب که در صورتی که وضوح ۶۰۰×۸۰۰ یا ۷۶۸×۱۰۲۴ باشد TrickBot اجرای خود را متوقف می‌کند.



به گزارش شرکت مهندسی شبکه گستر، در حالت عادی به‌منظور افزایش امکانات ماشین مجازی نظیر وضوح تصویر بالاتر و کنترل بیشتر بر روی موشواره، لازم است که ابزاری موسوم به Guest Software بر روی ماشین نصب شود. اما از آنجا که نصب این ابزار سبب ایجاد کلیدهایی در محضرخانه (Registry) و اجرای پروسه‌هایی می‌شود که وجود آنها به سبب برخی تکنیک‌های ضدماشین‌مجازی بدافزارها موجب از کار افتادن بدافزار می‌شود محققان نیز از نصب آن خودداری می‌کنند. بنابراین وضوح صفحه بر روی اکثر ماشین‌های مجازی مورد استفاده تحلیلگران بدافزار ۶۰۰×۸۰۰ یا ۷۶۸×۱۰۲۴ است.

TrickBot که در ابتدا در نقش یک اسب تروای بانکی ظهور کرد دائماً در حال تکامل قابلیت‌های مخرب خود بوده است.

از جمله این قابلیت‌ها می‌توان به انتشار در سطح شبکه و سرقت اطلاعات اصالت‌سنجی ذخیره شده در مرورگرها، بانک‌های داده سرویس‌های Active Directory، کوکی‌ها، کلیدهای OpenSSH، اطلاعات اصالت‌سنجی RDP، رمز عبور VNC و اطلاعات اصالت‌سنجی PuTTY اشاره کرد.

عرضه ابزار رمزگشایی
برای باج‌افزار مرموز ThiefQuest

محققان موفق به ساخت ابزاری برای رمزگشایی رایگان فایل‌های رمز شده توسط باج‌افزار ThiefQuest شدند.

ThiefQuest که به تازگی مورد توجه منابع امنیتی قرار گرفته از جهاتی متفاوت از هم‌قطاران خود است.

به گزارش شرکت مهندسی شبکه گستر، ThiefQuest از محدود باج‌افزارهایی است که برای آلوده‌سازی دستگاه‌های با سیستم عامل macOS توسعه داده شده است.

دیگر نکته‌ای که ThiefQuest را از باج‌افزارهای متداول متمایز می‌کند توانایی آن در سرقت اطلاعات قربانی است. از جمله قابلیت‌های این باج‌افزار می‌توان به موارد زیر اشاره کرد:

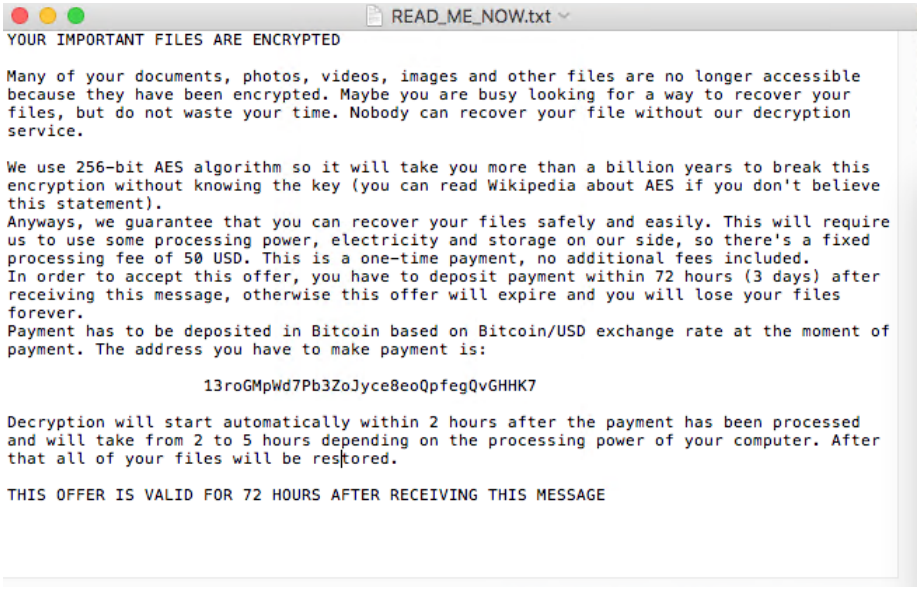
- ثبت کلیدهای فشرده شده توسط کاربر
- تزریق کد در حافظه
- تکنیک‌های ضدتحلیل
- نصب یک شل موسوم به معکوس با هدف اجرای از راه دور فرامین

ThiefQuest مجهز به یک اسکریپت مبتنی بر Python است که اقدام به جستجوی فایل‌های با قالب خاص در پوشه /Users کرده و پس از کدبندی (Encoding) با الگوریتم Base64 آنها را به سرورهای فرماندهی (C2) ارسال می‌کند. تصاویر، اسناد Word، گواهی‌نامه‌های SSL، گواهی‌نامه‌های امضای کد، کد منبع (Source Code)، پروژه‌ها، صفحات گسترده، بانک‌های داده و کیف‌های ارز رمز در فهرست فایل‌های مورد نظر این باج‌افزار قرار دارند.

همچنین ThiefQuest ویروسی واقعی بوده و قادر است تا با دست‌درازی به فایل‌های اجرایی معتبر و درج کد مخرب در آنها، آن فایل‌ها را نیز به ناقل خود تبدیل کند.

این باج‌افزار که در ابتدا توسط محققان EvilQuest نامگذاری شد بعدتر به دلیل وجود یک بازی ویدئویی با همین نام به ThiefQuest تغییر نام داده شد.

در اطلاعیه باج‌گیری ThiefQuest گفته می‌شود که قربانی ۷۲ ساعت برای پرداخت باج ۵۰ دلاری به منظور بازگرداندن فایل‌ها به حالت اولیه فرصت دارد.



بر خلاف سایر باج‌افزارها در اطلاعیه ThiefQuest هیچ راه تماسی با مهاجمان درج نشده است. ضمن اینکه نشانی کیف بیت‌کوین آن نیز برای تمامی قربانیان یکسان بوده و بنابراین به نظر نمی‌رسد که هدف مهاجمان آن حداقل در این نسخه اخاذی بوده باشد.

ThiefQuest برای رمزگذاری از یک روال اختصاصی رمزگذاری متقارن (Symmetric) بر مبنای الگوریتم آسیب‌پذیر RC۲ استفاده می‌کند.

تابع اصلی رمزگذاری نیز از کلیدی متقارن با طول ۱۲۸ بایت که به روشی ناامن کدبندی شده بهره می‌گیرد. همچنین به فایل رمزگذاری شده توسط این باج‌افزار بلوکی حاوی کلیدهای رمزگذاری/رمزگشایی و کلیدی که برای کد کردن آن استفاده شده افزوده می‌شود. به عبارت دیگر کلید در قالب متن ساده (Clear Text) نگهداری شده و با استخراج آن در فرایندی ساده امکان رمزگشایی فایل‌ها فراهم می‌گردد.

محققان SentinelOne نیز با بهره‌جویی از این باگ‌ها موفق به ساخت ابزار برای بازگرداندن فایل‌های رمزگذاری شده توسط ThiefQuest شده‌اند. ابزار مذکور در لینک زیر قابل دریافت است:

https://github.com/Sentinel-One/foss/tree/master/s1-evilquest-decryptor

برخی محققان معتقدند که عملکرد باج‌گیری ThiefQuest صرفاً ترفندی برای مخفی کردن ذات جاسوسی آن است. در اکثر مواقع پس از آلوده شدن دستگاه به باج‌افزار، کاربر اقدام به فرمت دستگاه و نصب مجدد سیستم عامل و در صورت وجود نسخه پشتیبان، بازگردانی آن می کند. به همین خاطر ممکن است که هیچگاه از سرقت شدن اطلاعات در زمان آلوده شدن سیستم به ThiefQuest مطلع نشود.

اما ایرادات متعددی به عملکرد و کدنویسی بخش باج‌افزاری ThiefQuest وارد است. این احتمال نیز مطرح است که این باج‌افزار در حالی که همچنان در مراحل توسعه خود بوده تصادفاً به دست محققان رسیده و ناخواسته مورد توجه قرار گرفته است. در این صورت دیر یا زود شاهد ظهور نسخه‌ای تکامل یافته از ThiefQuest خواهیم بود.

توضیح اینکه نمونه‌های مورد بررسی در این گزارش با نام‌های زیر توسط محصولات مک‌آفی قابل شناسایی است:

- Generic .lu
- OSX/Filecoder.a

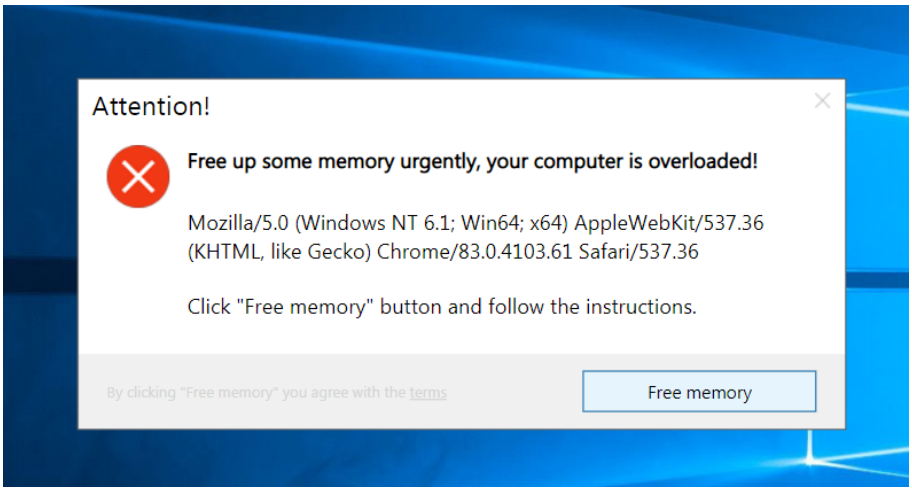
WastedLocker؛
باج‌افزار جدید هکرهای Evil Corp

مهاجمان در حال اجرای رشته حملاتی کاملاً هدفمند هستند که در جریان آنها با استفاده از باج‌افزار WastedLocker سرورها و ایستگاه‌های کاری دچار اختلال شده و از قربانی مبالغ هنگفتی - از ۵۰۰ هزار دلار تا بیش از ۱۰ میلیون دلار - اخاذی می‌شود.

WastedLocker را می‌توان نمونه‌ای نسبتاً جدید از باج‌افزارهای هدفمند دانست که به نظر می‌رسد توسط گروه Evil Corp توسعه داده شده است. این گروه منتسب به مهاجمان روسی، پیش‌تر نیز در انتشار اسب تروای بانکی Dridex و باج‌افزار BitPaymer نقش داشته است. برخی منابع، درآمد Evil Corp از دو بدافزار مذکور را ده‌ها میلیون دلار برآورد می‌کنند. دو نفر از گردانندگان این گروه در فهرست افراد تحت تعقیب وزارت دادگستری آمریکا قرار داشته و FBI در ازای هر گونه اطلاعاتی که منجر به دستگیری این متهمان شود پاداشی ۵ میلیون دلاری تعیین کرده است.

در این حملات از یک سازوکار مخرب مبتنی بر JavaScript، معروف به SocGholish بهره گرفته شده است. به‌محض دستیابی مهاجمان به شبکه قربانی از Cobalt Strike و چندین ابزار دیگر برای سرقت اطلاعات اصالت‌سنجی، ترفیع سطح دسترسی و توزیع باج‌افزار WastedLocker در سطح شبکه استفاده می‌شود.

این مهاجمان با هک حداقل ۱۵۰ سایت معتبر، به‌نحوی در کدهای آنها دست‌درازی کرده‌اند که در صورت باز شدن صفحه در مرورگر، کاربر به سایتی حاوی کد ناقل SocGholish هدایت شود. در آنجا با نمایش پیامی مشابه با آنچه که در تصویر زیر قابل مشاهده است کاربر تشویق به کلیک بر روی دگمه پنجره با پیغام جعلی می شود.



در صورت در دام افتادن کاربر ناآگاه، یک فایل ZIP بر روی دستگاه دریافت می‌شود. فایل ZIP مذکور حاوی کد JavaScript مخربی است که خود را به‌عنوان به‌روزرسانی مرورگر جا می‌زند. در ادامه از طریق wscript.exe فایل JavaScript دیگری فراخوانی و اجرا می‌شود. JavaScript در ابتدا مشخصه‌های دستگاه را با اجرای فرامین whoami، net user و net group استخراج کرده و در ادامه با استفاده از PowerShell اسکریپت‌های مخرب دیگری را دریافت می‌کند.

ادامه حمله، کاملاً خاص شبکه قربانی است که در ادامه به نمونه ای از آن پرداخته شده است.

مرحله دوم حمله شامل توزیع Cobalt Strike است. بدین‌منظور از PowerShell برای دریافت و اجرای یک فراخوانی‌کننده (Loader) که ناقل یک تزریق‌کننده (Injector) مبتنی بر .NET است استفاده می‌شود. به نظر می‌رسد که کدهای فراخوانی‌کننده و تزریق‌کننده بر پایه یک پروژه کد-باز با نام Donut که برای تزریق و اجرای کدهای مخرب در درون حافظه طراحی شده توسعه داده شده‌اند.

به گزارش شرکت مهندسی شبکه گستر، مهاجمان از کد تزریق شده تحت عنوان Cobalt Strike Beacon برای اجرای فرامین، تزریق به سایر پروسه‌ها و آپلود و دانلود فایل‌ها بهره می‌گیرند. همچنین از فرمان Get-NetComputer در ابزار PowerView با نامی تصادفی جهت شناسایی فهرست کامپیوترها در بانک داده Active Directory استفاده شده است. مهاجمان این اطلاعات را در یک فایل با پسوند tmp ذخیره می‌کنند.

Evil Corp به‌منظور ترفیع سطح دسترسی خود از تکنیکی که به‌صورت عمومی در دسترس بوده و در جریان آن از Software Licensing User Interface (پروسه slui.exe) که ابزاری معتبر برای فعالسازی Windows و به‌روزرسانی آن است استفاده می‌کند.

ضمن اینکه از Windows Management Instrumentation Command Line Utility (پروسه wmic.exe) برای اجرای فرامین بر روی دستگاه‌ها به‌صورت از راه دور به‌منظور اجرای اموری نظیر افزودن کاربر جدید یا اجرای اسکریپت‌های PowerShell بهره گرفته می‌شود. همچنین از ProcDump برای پاک کردن محتوای فایل‌های لاگ استفاده می‌شود.

مهاجمان با PsExec و mpcmdrun.exe که یک ابزار معتبر خط فرمان برای مدیریت Windows Defender است اقدام به غیرفعال کردن پویش فایل‌ها و پیوست‌های دریافت شده، حذف به‌روزرسانی‌ها و در برخی موارد غیرفعال کردن رصد بلادرنگ می‌کنند.

در ادامه با استفاده از PsExec، پروسه معتبر PowerShell اجرا گردیده و با فراخوانی کلاس win32_service سرویس‌ها بازیابی شده و با فرمان net stop سرویس‌های مورد نظر متوقف می‌شوند. پس از غیرفعال شدن Windows Defender و توقف سرویس‌ها از PsExec برای اجرای باج‌افزار WastedLocker بهره گرفته شده و در ادامه فرایند رمزگذاری داده‌ها و حذف آغاز می‌شود.

باج‌افزار با انتخاب تصادفی یکی از فایل‌های معتبر ذخیره شده در مسیر ٪SYSDIR٪، نسخه‌ای از آن را با نامی متفاوت در مسیر ٪APPDATA٪ ذخیره می‌کند. سپس ویژگی مخفی (Hidden) را به آن اعمال کرده و یک Alternate Data Stream را در قالب فایلی باعنوان bin: ایجاد می‌کند.

داده‌های ذخیره شده در Alternate Data Stream - به اختصار ADS - به‌سادگی توسط کاربر قابل شناسایی و روئیت نیستند.

در ادامه باج‌افزار در فایل (در ٪APPDATA٪) کپی شده و با پارامتر r- اجرا می‌شود.

به‌محض اجرای این ADS، فایل اصلی باج‌افزار در پوشه ٪SYSDIR٪ کپی شده و با ایجاد سرویسی برای این برنامه و در ادامه تنظیم خط فرمان آن با پارامتر s- پروسه‌های زیر اجرا می‌گردد:

- vssadmin.exe
- takeown.exe
- icacls.exe

WastedLocker برای حذف نسخه‌های موسوم به Shadow با بهره‌گیری از پروسه معتبر vssadmin.exe فرمان زیر را اجرا می‌کند:

- vssadmin.exe Delete Shadows /All /Quiet

از icacls.exe در قالب اجرای دستور زیر نیز برای ترفیع سطوح دسترسی سرویس باج‌افزار استفاده می‌شود:

- C:\Windows\system32\icacls.exe C:\Windows\system32\Id.exe /reset

همچنین Takeown.exe در قالب فرمان زیر اجرا می‌شود:

- C:\Windows\system32\takeown.exe /F C:\Windows\system32\Id.exe

برای رمزگذاری فایل‌ها، WastedLocker از الگوریتم‌های AES و RSA بهره می‌گیرد.

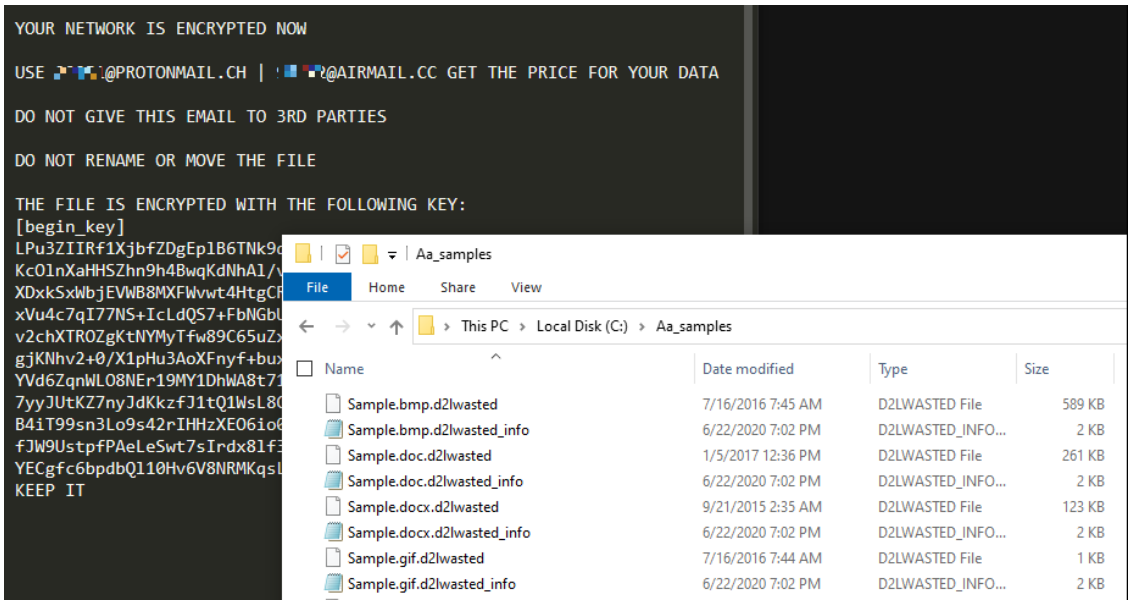
WastedLocker فایل‌های موجود درایوهای زیر را هدف قرار می‌دهد:

- جداشدنی (Removable)
- ثابت (Fixed)
- به اشتراک گذاشته شده (Shared)
- از راه دور (Remote)

هر کدام از فایل‌ها با کلید ۲۵۶ بیتی AES رمزگذاری می‌شوند. کلید مذکور خود نیز توسط کلید ۴۰۹۶ بیتی RSA رمزگذاری می‌شود.

به ازای هر فایل رمزگذاری شده، باج‌افزار فایل دیگری حاوی اطلاعیه باج‌گیری (Ransom Note) را ایجاد می‌کند. پسوند فایل رمزشده عبارتی شامل نام سازمان مورد هدف با پیشوند wasted است.

تصویر زیر نمونه‌ای از فایل‌های رمزگذاری شده و فایل اطلاعیه باج‌گیری آن را نمایش می‌دهد.



پس از پایان رمزگذاری، WastedLocker اقدام به حذف سرویس‌ها و فایل‌های با نام تصادفی می‌کند.

باج‌افزار از رمزگذاری فایل‌های با هر یک از پسوندهای زیر خودداری می‌کند:

*\ntldr, *.386,*.adv, *.ani, *.bak,*.bat, *.bin, *.cab,*.cmd,*.com, *.cpl,*.cur, *.dat, *.diagcab, *.diagcfg,*.dll,*.drv, *.exe, *.hlp, *.hta, *.icl, *.icns,*.ics, *.idx,*.ini, *.key, *.lnk, *.mod,*.msc, *.msi,*.msp,*.msstyles,*.msu,*.nls, *.nomedia, *.ocx,*.ps1, *.rom, *.rtp, *.scr, *.sdi, *.shs, *.sys, *.theme, *.themepack,*.wim, *.wpx,*\boot-mgr,*\grldr.

همچنین فایل‌های ذخیره شده در هر یک از پوشه‌های زیر نیز از رمزگذاری شدن مستثنی شده‌اند:

*\$recycle.bin, *\appdata, *\bin, *\boot, *\caches, *\dev, *\etc, *\initdr, *\lib, *\programdata, *\run, *\sbin, *\sys, *\system volume information, *\users\all users, *\var, *\vmlinuz, *\webcache, *\windowsapps, c:\program files (x86), c:\program files, c:\programdata, c:\recovery, c:\users\ %USERNAME%\appdata\local\temp, c:\users\ %USERNAME%\appdata\roaming, c:\windows

اطلاعیه باج‌گیری WastedLocker که نمونه‌ای از آن در تصویر زیر قابل مشاهده است حاوی نشانی ایمیل مهاجمان و کلید عمومی RSA که برای رمزگذاری کلید AES مورد استفاده قرار گرفته است می‌باشد:

مبالغ اخاذی شده توسط این باج‌افزار از ۵۰۰ هزار دلار تا بیش از ۱۰ میلیون دلار گزارش شده است.

به گفته شرکت امنیتی مک‌آفی، سازوگار رمزگذاری این باج‌افزار نیازی به راه اندازی مجدد دستگاه ندارد.

WastedLocker با نام‌های زیر قابل شناسایی است:

McAfee:

- Ransom-Wasted

Bitdefender:

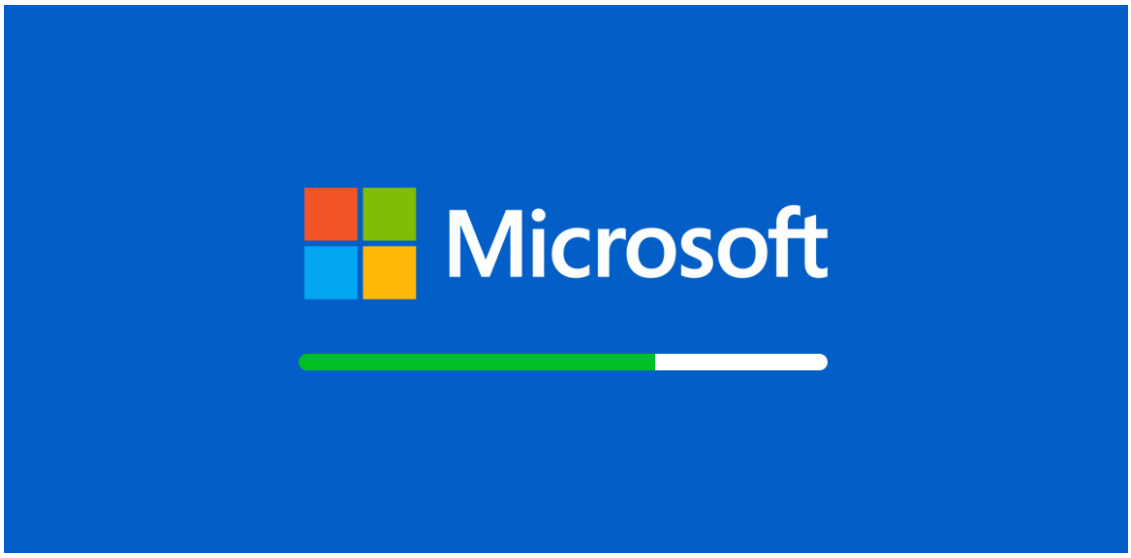
- Gen:NN.ZexaF.34136.bn1@aKevf5pi

Sophos:

- Mal/EncPk-APV

آسیب‌پذیری‌ها و اصلاحیه‌های امنیتی

اصلاحیه‌های امنیتی مایکروسافت
برای ماه میلادی جولای



به گزارش شرکت مهندسی شبکه گستر، سه‌شنبه، ۲۴ تیر، شرکت مایکروسافت اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی جولای منتشر کرد. این اصلاحیه‌ها در مجموع، ۱۲۳ آسیب‌پذیری را در سیستم عامل Windows و محصولات زیر ترمیم می‌کنند.

- Microsoft Edge (EdgeHTML-based)
- Microsoft Edge (Chromium-based) in IE Mode
- Microsoft ChakraCore
- Internet Explorer
- Microsoft Office and Microsoft Office Services and Web Apps
- Windows Defender
- Skype for Business
- Visual Studio
- Microsoft OneDrive
- Open Source Software
- .NET Framework
- Azure DevOps

درجه حساسیت ۱۸ مورد از آسیب‌پذیری‌های ترمیم شده توسط اصلاحیه‌های مذکور "حیاتی" (Critical) و ۱۰۵ مورد از آنها "مهم" (Important) اعلام شده است.

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

از نکات قابل توجه در خصوص مجموعه اصلاحیه‌های این ماه، ترمیم یک آسیب‌پذیری روز-صفر (Zero-day) با درجه شدت ۱۰ است که سرویس‌دهنده DNS در سیستم عامل Windows از آن تأثیر می‌پذیرد. بهره‌جویی از آسیب‌پذیری مذکور که به آن شناسه CVE-2020-1350 تخصیص داده شده مهاجم را قادر به اجرای کد به‌صورت از راه دور می‌کند. بکارگیری این آسیب‌پذیری جدی در

بدافزارهای از نوع کرم (Worm) محتمل به نظر می‌رسد. در صورت عدم امکان اعمال اصلاحیه، با استفاده از راهکار اشاره شده در لینک زیر می توان نسبت به مقاوم‌سازی موقت این آسیب‌پذیری اقدام کرد:

https://msrc-blog.microsoft.com/2020/07/14/july-2020-security-update-cve-2020-1350-vulnerability-in-windows-domain-name-system-dns-server/

همچنین سه آسیب‌پذیری "حیاتی" در مرورگر Edge و هسته اجرایی VBScript مهاجم را قادر به اجرای کد به‌صورت از راه دور می‌کند. هدایت کاربر به یک صفحه اینترنتی حاوی کد مخرب از جمله سناریوهای احتمالی در بهره‌جویی از این آسیب‌پذیری است. در صورت موفقیت مهاجم در سوءاستفاده از آسیب‌پذیری مذکور امکان اجرای کد به صورت از راه دور بر روی دستگاه قربانی با سطح دسترسی کاربر جاری فراهم می شود.

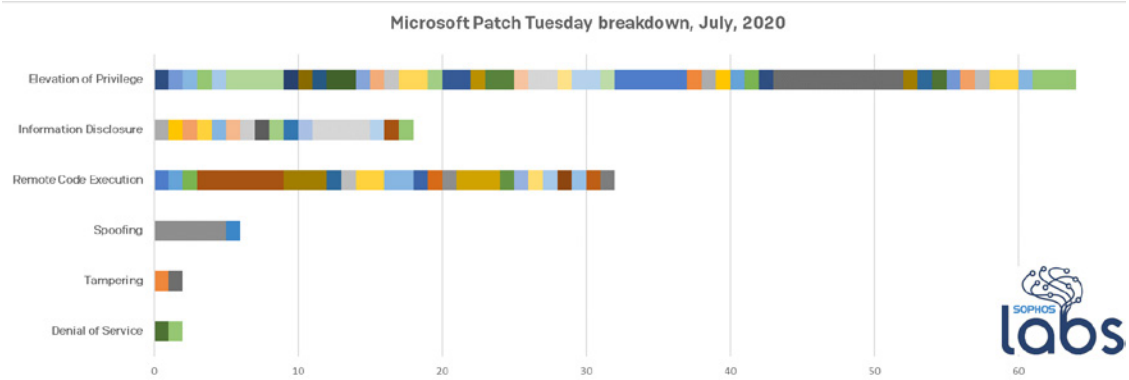
مهاجم با بهره‌جویی از آسیب‌پذیری‌های "حیاتی" زیر نیز می‌تواند تا از طریق روش‌هایی همچون تشویق کاربر به دریافت فایل‌های مخرب دستکاری شده در جریان حملات تحت وب یا فیشینگ اقدام به اجرای کد به‌صورت از راه دور بر روی سیستم قربانی کند.

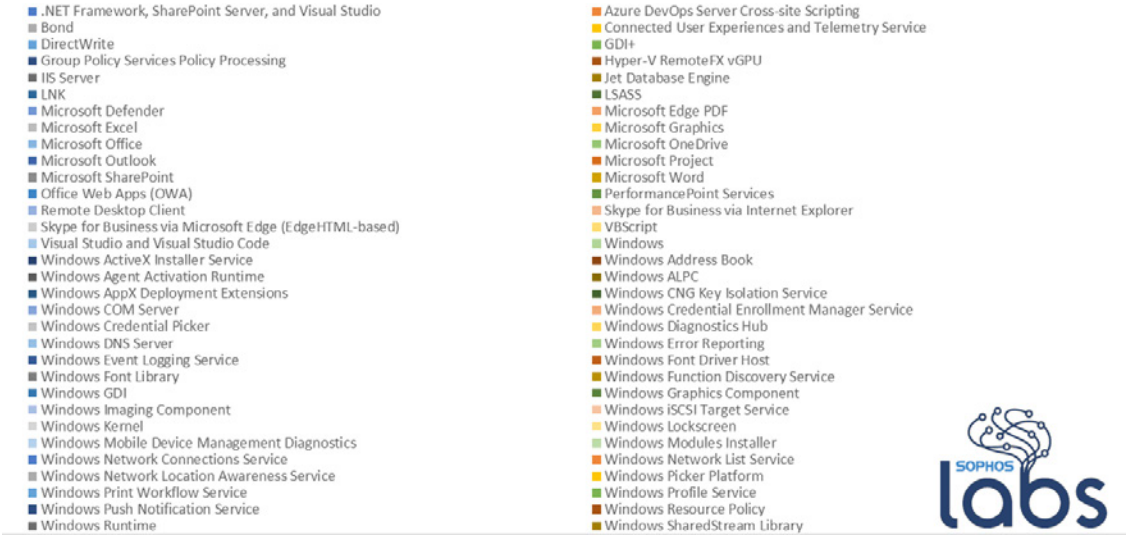
- CVE-2020-1349
- CVE-2020-1409
- CVE-2020-1410
- CVE-2020-1421

شش ضعف امنیتی زیر در محصول Hyper-V، دیگر آسیب‌پذیری‌های "حیاتی" این ماه هستند که مهاجم را قادر به اجرای کد بر روی سیستم عامل میزبان از طریق ماشین میهمان می‌کنند.

- CVE-2020-1032
- CVE-2020-1036
- CVE-2020-1040
- CVE-2020-1041
- CVE-2020-1042
- CVE-2020-1043

تصاویر زیر انواع آسیب پذیری های ترمیم شده در این ماه و محصولات تأثیرپذیر از آنها را نمایش می دهد.





جزییات بیشتر در خصوص مجموعه اصلاحیه جولای ۲۰۲۰ مایکروسافت در اینجا قابل دریافت و مطالعه است.

اصلاحیه‌های عرضه شده
در تیر ۱۳۹۹

در تیر ۱۳۹۹، شرکت‌های ادوبی، گوگل، وی‌ام‌ور، سیسکو، پائلو آلتو نت‌ورکز، نت‌گیر، مایکروسافت، موزیلا، اوراکل و اپل، گروه سامبا و بنیاد آپاچی اقدام به انتشار اصلاحیه و توصیه‌نامه امنیتی برای برخی از محصولات خود کردند.

در تیر ماه، شرکت ادوبی در سه نوبت اقدام به عرضه به‌روزرسانی برای برخی از محصولات خود کرد. از جمله این محصولات می‌توان به موارد زیر اشاره کرد:

- Magento (APSB20-41)
- Download Manager APSB20-49
- ColdFusion APSB20-43
- Genuine Service APSB20-42
- Media Encoder APSB20-36
- Creative Cloud Desktop Application APSB20-33
- Bridge APSB20-44
- Photoshop APSB20-45
- Prelude APSB20-46
- Reader Mobile APSB20-50

اجرای کد (Arbitrary Code Execution)، ترفیع امتیازی (Elevation of Privilege) و مرور پوشه‌ها (Directory Traversal) از جمله آسیب‌پذیری‌های ترمیم شده توسط این به‌روزرسانی‌ها هستند.

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 ۲۴ تیر انتشار یافت ۸۴.۰.۴۱۴۷.۸۹ است. فهرست اشکالات مرتفع شده در اینجا و اینجا قابل دریافت و مشاهده است.

وی‌اِم‌وِر دیگر شرکتی بود که در تیر ۱۳۹۹ اقدام به انتشار به‌روزرسانی کرد. محصولات ESXi، Workstation، Fusion، Cloud Foundation، Remote Console و Horizon Client از آسیب‌پذیری‌های ترمیم شده توسط این به‌روزرسانی‌ها تأثیر می‌پذیرند. اطلاعات بیشتر در مورد به‌روزرسانی عرضه شده در اینجا و اینجا قابل مطالعه است.

در تیر ۹۹، سیسکو در چندین نوبت اقدام به عرضه به‌روزرسانی‌های امنیتی کرد. این به‌روزرسانی‌ها در مجموع، ۴۴ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت ۵ مورد از این آسیب‌پذیری‌ها، "حیاتی" (Critical) و ۱۴ 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 اینجا قابل دسترس است.

۹ تیر ماه، شرکت پالو آلتو نت‌ورکز، ضعفی با شناسه CVE-2020-2021 را در سیستم عامل PAN-OS که در تجهیزات دیواره آتش این شرکت استفاده می شود ترمیم کرد. بهره جویی از آسیب پذیری مذکور، مهاجم را قادر به دسترسی یافتن به اطلاعات بالقوه حساس می کند. جزییات بیشتر در اینجا قابل مطالعه است.

در تیر ماه اعلام شد که برخی مدل‌ها از روترهای ساخت نت‌گیر دارای آسیب‌پذیری‌هایی هستند که مهاجم با دسترسی از راه دور را قادر به در اختیار گرفتن کنترل دستگاه می‌کنند. توصیه‌نامه نت‌گیر در اینجا قابل دریافت است.

۱۰ تیر ماه، شرکت مایکروسافت اقدام به ترمیم دو آسیب‌پذیری "حیاتی" با شناسه‌های CVE-2020-1425 و CVE-2020-1457 در سیستم های عامل Windows 10 و Windows Server کرد. آسیب‌پذیری‌های مذکور از نحوه مدیریت اشیا در حافظه توسط Windows Codecs Library ناشی می‌شود. مهاجم با بهره‌جویی از هر یک از آسیب‌پذیری‌های مذکور قادر به اجرای کد به‌صورت از راه دور بر روی دستگاه قربانی خواهد بود. همچنین این شرکت، سه‌شنبه، ۲۴ تیر، اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی جولای منتشر کرد. این اصلاحیه‌ها در مجموع، ۱۲۳ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می‌کنند که جزییات آنها در اینجا قابل دریافت است.

۱۳ تیر ماه گروه سامبا با عرضه به‌روزرسانی، چهار ضعف امنیتی با شناسه‌های CVE-2020-10730، CVE-2020-10745، CVE-2020-10760 و CVE-2020-14303 را در نرم‌افزار کدباز Samba برطرف کرد. سوءاستفاده از یکی از این ضعف‌های ترمیم شده در اختیار گرفتن کنترل سیستم آسیب‌پذیر را فراهم می‌کند.

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

در تیر، اوراکل مطابق با برنامه زمانبندی شده سه‌ماهه خود، با انتشار مجموعه‌به‌روزرسانی‌های موسوم به Critical Patch Update اقدام به ترمیم ۴۳۳ آسیب‌پذیری امنیتی در ده ها محصول ساخت این شرکت کرد. بهره جویی از برخی از آسیب پذیری های مذکور مهاجم را قادر به اجرای کد به صورت از راه دور می کنند. که جزییات کامل در خصوص آنها در اینجا قابل دریافت است.

در ۲۶ تیر ماه، شرکت اپل با انتشار به‌روزرسانی، ضعف‌هایی امنیتی را در سیستم های عامل iOS/iPadOS، macOS، tvOS و watchOS و مرورگر Safari ترمیم و اصلاح کرد. سوءاستفاده از برخی از ضعف‌های مذکور، مهاجم را قادر به در اختیار گرفتن کنترل سیستم می‌کند.

در این ماه، بنیاد نرم‌افزاری آپاچی، با انتشار به‌روزرسانی امنیتی، سه آسیب‌پذیری به شناسه های CVE-2019-10072، CVE-2020-13934 و CVE-2020-13935 را در نرم‌افزار Apache Tomcat ترمیم و اصلاح کرد. بهره‌جویی از این آسیب‌پذیری‌ها، مهاجم را قادر به ایجاد اختلال یا از کار انداختن کامل سرویس‌دهنده می‌کند.

افتای ریاست جمهوری با همکاری شبکه گستر

شبکه گستر

شرکت مهندسی شبکه گستر

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

ترمیم ۱۲۳ آسیب‌پذیری توسط مجموعه اصلاحیه‌های جولای مایکروسافت

سه‌شنبه، ۲۴ تیر، شرکت مایکروسافت اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی جولای منتشر کرد. این اصلاحیه‌ها در مجموع، ۱۲۳ آسیب‌پذیری را در سیستم عامل Windows و برخی دیگر از محصولات این شرکت ترمیم می‌کنند. 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