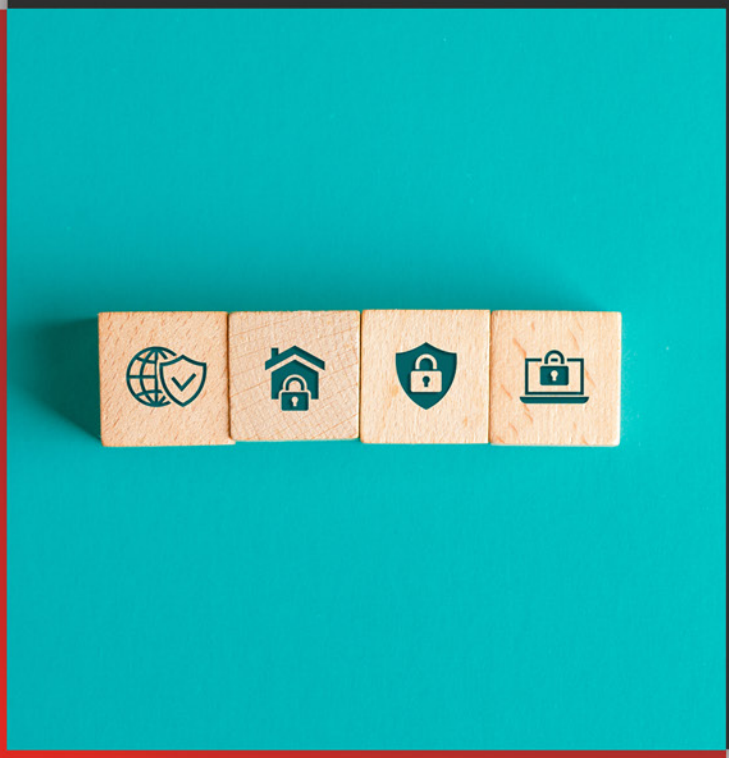
شهریور
۱۳۹۹

ماهنامه

امنیت فناوری اطلاعات



شبکه گستر

امنیت شما | وظیفه ما

newsroom.shabakeh.net

@SGnewsroom

فهرست مطالب

چکیده مدیریتی ۳

آمار جهانی از نگاه مک آفی ۵

هشدارهای امنیتی ۱۶

آسیب‌پذیری‌ها و اصلاحیه‌های امنیتی ۴۳

گزارش‌ها ۵۸

افتای ریاست جمهوری با همکاری شبکه گستر ۶۱

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 شهریور ۱۳۹۹ پرداخته شده است.

همان‌طور که در این ماهنامه خواهید خواند نمونه‌های اخیر بدافزار مخرب Lemon_Duck مجهز به قابلیت‌های پیشرفته‌ای جهت آلوده‌سازی دستگاه‌های با سیستم عامل Linux شده‌اند. همچنین نقاط آسیب‌پذیر جدیدی به فهرست ضعف‌های امنیتی مورد سوءاستفاده این بدافزار افزوده شده است. در یک سال گذشته شرکت مهندسی شبکه گستر گزارش‌های متعددی از حمله این بدافزار به سازمان‌های ایرانی دریافت کرده است.

در یک سال اخیر تعداد حملات هدفمند باج‌افزاری به سازمان‌های بزرگ در کشورهای مختلف از جمله ایران افزایشی چشمگیر داشته است. این مهاجمان اهداف خود را به‌صورت خاص انتخاب کرده و پس از سرقت فایل‌ها و داده‌های بااهمیت اقدام به رمزگذاری و از دسترس خارج کردن فایل‌ها می‌کنند. در ادامه، قربانی تهدید می‌شود که در صورت عدم پرداخت مبلغ اخاذی‌شده، اطلاعات سرقت شده به صورت عمومی منتشر و افشا خواهد شد. از جمله باج‌افزارهای مورد استفاده در این‌گونه حملات می‌توان به Conti و Netwalker اشاره کرد که در این ماهنامه به‌طور مفصل مورد بررسی قرار گرفته‌اند.

PyVil بدافزار دیگری است که در این ماهنامه به بررسی آن پرداخته شده است. PyVil 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 ماهی که گذشت مهاجمان از روش‌های خلاقانه جدید و البته مخرب برای عبور از سد محصولات امنیتی بهره گرفتند. برای مثال می‌توان به استفاده از نوع خاصی از فایل‌های Excel و یا راه‌اندازی یک ماشین مجازی بر روی دستگاه قربانی اشاره کرد که عملکرد آنها در این ماهنامه مورد بررسی قرار گرفته است.

همچنین در شهریور ۱۳۹۹، شرکت‌های گوگل، موزیلا، سیسکو، مایکروسافت، ادوبی، مک‌آفی و بیت‌دیفندر و بنیاد دروپل برای برخی محصولات خود اصلاحیه و توصیه‌نامه امنیتی منتشر کردند که جزییات آنها در این ماهنامه ارائه شده است.

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 F۵ 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، ASN1،Sage، 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 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 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

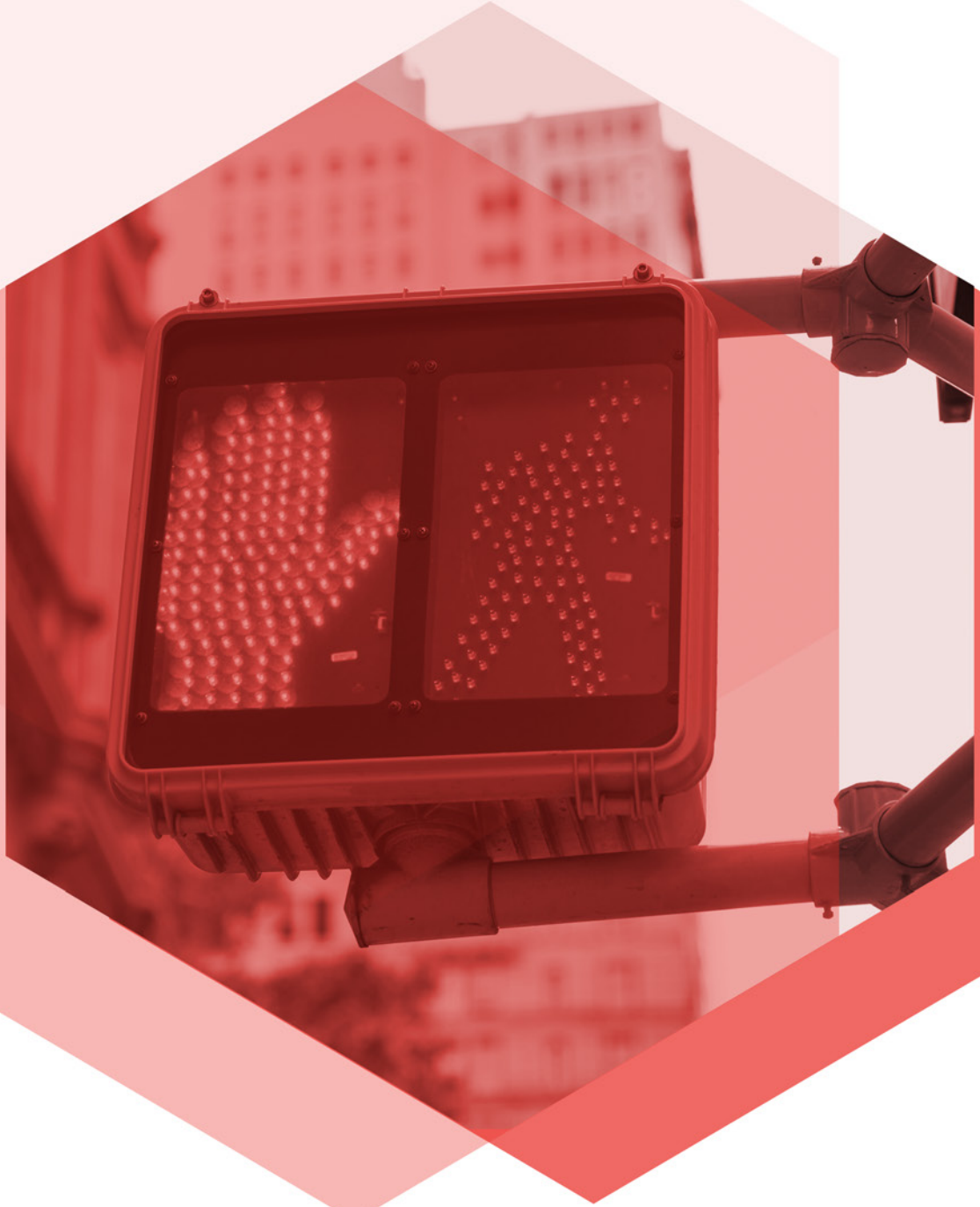
باج‌افزار	توضیحات
Dharma	Dharma که گونه ای از باج افزار CrySiS پسوندهای مختلفی را به فایل های رمزگذاری شده الصاق می کند. این باج افزار از سال ۲۰۱۶ فعال بوده و گردانندگان آن به طور مستمر اقدام به عرضه نسخ جدیدی از آن می کنند.
Phobos	این باج‌افزار پس از رمزگذاری فایل‌ها توسط الگوریتم AES اقدام به افزودن 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



Lemon_Duck؛
مجهزتر از قبل

نمونه‌های اخیر بدافزار مخرب Lemon_Duck مجهز به قابلیت‌های پیشرفته‌ای جهت آلوده‌سازی دستگاه‌های با سیستم عامل Linux و هک سرویس‌دهندگان Redis و Hadoop شده‌اند. همچنین نقاط آسیب‌پذیر جدیدی نیز به فهرست ضعف‌های امنیتی مورد سوءاستفاده این بدافزار برای تسخیر سیستم‌های Windows افزوده شده است.

در یک سال گذشته شرکت مهندسی شبکه گستر گزارش‌های متعددی از حمله این بدافزار به سازمان‌های ایرانی دریافت کرده است.

Lemon_Duck در دسته بدافزارهای موسوم به رمز ربا (Cryptojacking) قرار می‌گیرد.

در ارز رمزها (Cryptocurrency)، فرایندی با عنوان استخراج (Mining) وجود دارد که یکی از اصلی‌ترین وظایف آن تأیید اطلاعات تبادل شده در شبکه این واحدهای پولی است. فرایند استخراج مستلزم فراهم بودن توان پردازشی بسیار بالاست. در نتیجه شبکه ارز رمز نیز در قبال تلاشی که برای این پردازش‌ها انجام می‌شود به استخراج‌کنندگان پاداشی اختصاص می‌دهد. از همین رو، برخی افراد نیز با بکارگیری برنامه‌های استخراج‌کننده (Miner) تلاش می‌کنند تا در ازای استخراج ارز رمز، مشمول پاداش شبکه ارز رمز شوند. اما با توجه به نیاز به توان پردازش بالا، انجام استخراج می‌تواند یک سرمایه‌گذاری هزینه‌بر برای استخراج‌کننده باشد. به همین خاطر در حملات موسوم به رمز ربایی (Cryptojacking)، استخراج‌کننده بدخواه با آلوده کردن دستگاه دیگران به بدافزارهای ویژه استخراج، از توان پردازشی آنها به نفع خود بهره‌گیری می‌کند. در حقیقت در رمز ربایی، این مهاجمان هستند که همه منافع حاصل از استخراج را بدون هر گونه سرمایه‌گذاری کسب می‌کنند؛ در حالی که دستگاه قربانی انجام‌دهنده امور اصلی بوده است.

به‌محض آلوده شدن دستگاه به Lemon_Duck، یک استخراج‌کننده ارز رمز مونرو بر روی دستگاه اجرا می‌شود.

Lemon_Duck، فهرستی از نشانی‌های IP را به‌صورت تصادفی ایجاد کرده و پس از مورد هدف قرار دادن آنها، قابل دسترس بودن درگاه‌های زیر بر روی آنها را بررسی می‌کند:

- TCP/445 - درگاه پیش‌فرض SMB
- TCP/1433 - درگاه پیش‌فرض MS-SQL
- TCP/65529 - درگاهی که توسط Lemon_Duck بر روی دستگاه‌های آلوده شده به این بدافزار باز می‌شود.

به گزارش شرکت مهندسی شبکه گستر، در صورت باز بودن درگاه ۴۴۵، بدافزار از طریقPingCastle آسیب‌پذیر بودن دستگاه هدف به بهره‌جوی EternalBlue (ضعف امنیتی CVE-2017-0144) را مورد بررسی قرار می دهد. ماجرای EternalBlue به حدود ۳ سال قبل و انتشار اسناد محرمانه‌ای باز می‌گردد که در جریان آن فایل‌های سرقت شده از یک گروه نفوذگر حرفه‌ای با نام Equation که وابستگی اثبات شده‌ای به "سازمان امنیت ملی" دولت آمریکا (NSA) دارد توسط گروه Shadow Brokers بر روی اینترنت به اشتراک گذاشته شدند. در بین این فایل‌ها، بهره‌جوهایی به چشم می‌خوردند که از یک ضعف امنیتی روز-صفر در بخش سیستم عامل Windows که به EternalBlue موسوم شد سوءاستفاده می‌کردند. یک ماه پیش از درز این اطلاعات شرکت مایکروسافت اقدام به عرضه اصلاحیه‌ای با شناسه MS17-010 به‌منظور ترمیم آسیب‌پذیری مذکور نموده بود. باجافزارWannaCry از جمله بدافزارهایی بوده است که با بهره‌جویی از آسیب‌پذیری مذکور در مدتی کوتاه صدها هزار دستگاه را در سرتاسر جهان به خود آلوده کرد. با این حال تداوم بهره‌جویی مهاجمان از این آسیب‌پذیری نشانه‌ای از عدم توجه بسیاری از کاربران و راهبران شبکه نسبت به لزوم نصب اصلاحیه‌های امنیتی است.

چنانچه درگاه ۱۴۳۳ بر روی دستگاه هدف باز باشد بدافزار اقدام به اجرای حملات موسوم به سعی‌وخطا (Brute-force) جهت رخنه به سرویس‌دهنده MS-SQL نصب شده بر روی دستگاه می‌کند. برای این منظور Lemon_Duck با بکارگیری فهرستی از رمزهای عبور و همچنین مجموعه‌ای از درهم‌ساز (Hash) و NTLM تلاش می‌کند تا حساب کاربری sa در سرویس Microsoft SQL را هک کند. فهرست این رمزهای عبور به‌شرح زیر است:

"saadmin", "123456", "password", "PASSWORD", "123.com", "admin@123", "Aa123456", "qwer12345", "Huawei@123", "123@abc", "golden", "123!@#qwe", "1qaz@WSX", "Ab123", "1qaz!QAZ", "Admin123", "Administrator", "Abc123", "Admin@123", "999999", "Passw0rd", "123qwe!@#", "football", "welcome", "1", "12", "21", "123", "321", "1234", "12345", "123123", "123321", "111111", "654321", "666666", "121212", "000000", "222222", "888888", "1111", "555555", "1234567", "12345678", "123456789", "987654321", "admin", "abc123", "abcd1234", "abcd@1234", "abc@123", "p@ssword", "P@ssword", "p@ssw0rd", "P@ssw0rd", "P@SSWORD", "P@SSW0RD", "P@w0rd", "P@word", "iloveyou", "monkey", "login", "passw0rd", "master", "hello", "qazwsx", "password1", "qwerty", "baseball", "qwertyuiop", "superman", "۱qaz2wsx", "f-ckyou", "123qwe", "zxcvbn", "pass", "aaaaaa", "love", "administrator", "qwe1234A", "qwe1234a", "123123123", "1234567890", "88888888", "111111111", "112233", "a123456", "123456a", "5201314", "1q2w3e4r", "qwe123", "a123456789", "123456789a", "dragon", "sunshine", "princess", "!@#$%^&*", "charlie", "aa123456", "homelesspa", "1q2w3e4r5t", "sa", "sasa", "sa123", "sql2005", "sa2008", "abc", "abcdefg", "sapassword", "Aa12345678", "ABCabc123", "sqlpassword", "sql2008", "11223344", "admin888", "qwe1234", "A123456"

به‌محض موفقیت در هک حساب کاربری مذکور، بدافزار با استفاده از پروسه sqlserver.exe فرامین مخرب را بر ضد ماشین‌های دیگر اجرا می‌کند.

همچنین Lemon_Duck با بهره‌جویی از آسیب‌پذیری CVE-2017-8464 فایل‌های میانبر (LNK) و DLL مخرب را بر روی حافظه‌های جداشدنی (Removable Storage) متصل به دستگاه آلوده و در درایوهای اشتراکی موسوم به Map کپی می‌کند. باز کردن درایو منجر به اجرای فایل DLL مخرب و آلوده شدن دستگاه می‌شود. اصلاحیه CVE-2017-8464 از خرداد ۱۳۹۶ توسط شرکت مایکروسافت در دسترس قرار گرفته است.

در برخی نسخ این بدافزار، Lemon_Duck بر روی سیستم آلوده سطح دسترسی کاربر جاری را مورد بررسی قرار داده و چنانچه کاربر دارای دسترسی administrator باشد، ماژول PowerDump و ابزار Mimikatz را برای رونوشت برداشتن از درهم‌سازهای NTLM، نام کاربری، رمز عبور و اطلاعات دامنه (Domain) اجرا می‌کند. در ادامه، Lemon_Duck با مجوز این اطلاعات اصالت‌سنجی، فایل‌های مخرب را در کنار فایل Batch یا LNK مرتبط با آنها در پوشه ٪Startup٪ ماشین‌های قابل دسترس در بستر شبکه کپی کرده یا PowerShell را به‌صورت از راه دور با استفاده از WMI اجرا می‌کند. با استفاده از سازوکار فرامین زمانبندی‌شده (Scheduled Task) در Windows، نسخ جدید اسکریپت‌های مخرب بدافزار در بازه‌های زمانی حدوداً یک ساعته دریافت و اجرا می‌شوند. اسکریپت دانلود شده خود را با یک درهم‌سازی که در کد آن درج شده پیش از اجرا اعتبارسنجی می‌کند. در صورت موفق بودن، اسکریپت اقدام به دریافت کد مخرب دیگری که وظیفه آن استخراج ارز رمز مونرو بر روی دستگاه قربانی است می‌کند.

عناوین این فرامین به شرح زیر است:

- \Microsot\Windows\Bluetool
- \Microsot\Windows\Bluetooths
- Autocheck
- Autostart
- Escan
- Ddriver

نام و مسیر نمونه‌هایی از فایل‌های مخرب ایجاد شده توسط Lemon_Duck در زیر فهرست شده است:

- C:\windows\temp\tmp.vbs
- C:\windows\temp\p.bat
- C:\Windows\mkatz.ini
- C:\Windows\Temp\mkatz.ini
- C:\Windows\m.ps1
- C:\Windows\Temp\m.ps1
- C:\Windows\m2.ps1C:\Windows\Temp\m2.ps1
- C:\Windows\Temp\svhhost.exe
- C:\Windows\Temp\svvhost.exe
- C:\Windows\Temp\svchost.exe
- C:\Windows\Temp\ipc.txt
- C:\Windows\Temp\hash.txt
- C:\Windows\Temp\eb.txt
- C:\Windows\system32\svhost.exe
- C:\Windows\SysWOW64\svhost.exe
- C:\Windows\system32\drivers\svhost.exe
- C:\Windows\SysWOW64\drivers\svhost.exe

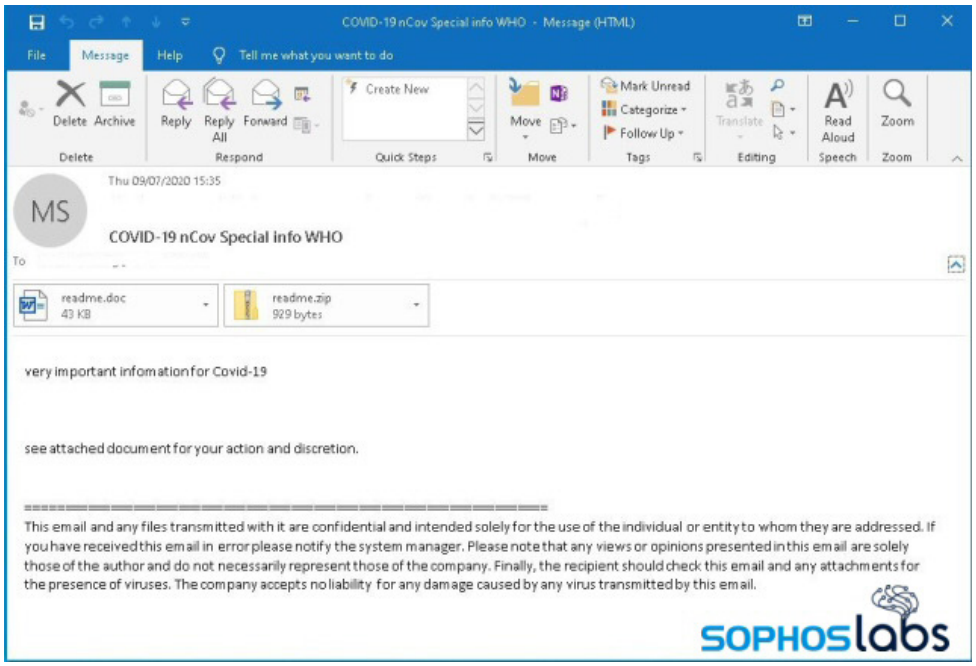
همچنین Lemon_Duck با پویش سرورهای قابل دسترس که درگاه پیش‌فرض Remote Desktop Protocol - به اختصار RDP - (TCP/3389) بر روی آنها باز است می‌کوشد تا با نام کاربری administrator و امتحان کردن فهرستی از رمزهای عبوری که در کد بدافزار تزریق شده از طریق ابزار کد باز FreeRDP بر روی این پودمان به دستگاه مقصد وارد شود. در صورت موفقیت در ورود، فرمان مخرب بر روی دستگاه اجرا می شود.

در مواردی پس از آلوده شدن دستگاه، بدافزار یک حساب کاربری جدید با نام k8h3d و رمز عبور k8d3j9SjfS7 ایجاد می‌شود. در مواقعی نیز رمز عبور sa توسط Lemon_Duck به sEqgIBKy تغییر می‌کند.

چنانچه ماشین با هر یک از روش‌های مورد اشاره در بالا آلوده شد، بدافزار تنظیمات دیواره آتش را تغییر داده و درگاه TCP/65529 را بر روی آن باز می‌کند. Lemon_Duck از آن به عنوان علامتی از آلوده بودن دستگاه استفاده می‌کند.

به‌تازگی نیز Lemon_Duck مجهز به ماژول پویش درگاه TCP/22 برای شناسایی سیستم‌های Linux قابل دسترس که از طریق درگاه مذکور امکان ثبت ورود (Login) از راه دور در بستر پودمان SSH به آنها وجود دارد شده است. پس از شناسایی دستگاه با درگاه TCP/22 باز، بدافزار اقدام به اجرای حملات سعی‌وخطا با نام کاربری root و رمزهای عبور اشاره شده در بالا می‌کند. در صورت موفقیت به رخنه به سیستم، یک Shell Code مخرب دریافت و اجرا می‌شود. بدافزار با ایجاد یک Cron Job از ماندگار ماندن خود بر روی دستگاه اطمینان حاصل می‌کند. در ادامه Lemon_Duck به جستجوی سایر دستگاه‌های Linux قابل دسترس پرداخته و تلاش می‌کند تا با اطلاعات اصالت‌سنجی ثبت شده در فایل ssh/known_hosts./ به آن سیستم‌ها نیز رخنه کند.

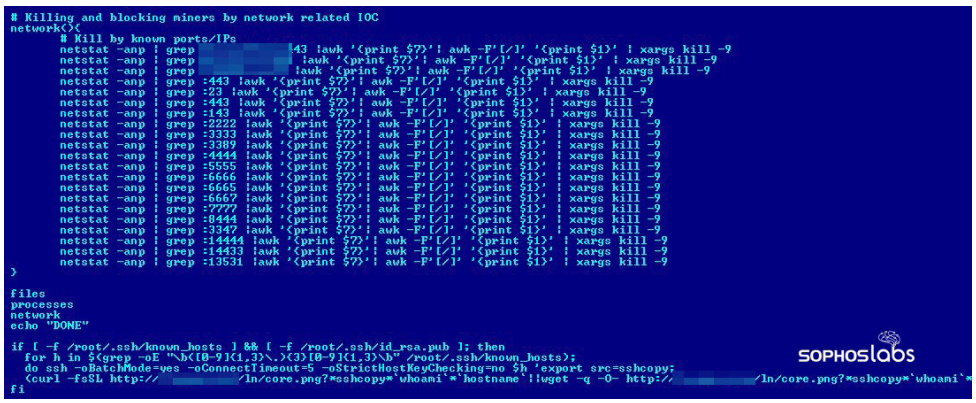
در ماه‌های اخیر مهاجمان Lemon_Duck با تکنیک‌های مهندسی اجتماعی و موضوعاتی مرتبط با کووید-۱۹، اقدام به ارسال هرزنامه‌هایی با پیوست فایل DOC کرده‌اند. با اجرای فایل توسط قربانی، بهره‌جوی آسیب‌پذیری CVE-2017-8570 اجرا شده و دستگاه به Lemon_Duck آلوده می‌شود. آسیب‌پذیری مذکور امکان اجرای کد به‌صورت از راه دور را فراهم می‌کند. مایکروسافت اصلاحیه CVE-2017-8570 را در تیر ۱۳۹۶ عرضه کرد و در صورت نصب بودن این اصلاحیه دستگاه در برابر این روش انتشار ایمن خواهد بود.



همچنین نسخ جدید Lemon_Duck مجهز به بهره‌جوی آسیب‌پذیری CVE-2020-0796 (معروف به SMBGhost) شده است. اگر چه به‌نظر می‌رسد که استفاده از این بهره‌جو در مرحله آزمایشی قرار داشته و در نمونه‌های مورد بررسی، از آسیب‌پذیری CVE-2020-0796 صرفاً برای استخراج اطلاعات در مورد دستگاه‌ها استفاده شده است. این در حالی است که بهره‌جویی از CVE-2020-0796 که ضعفی در پودمان SMBv3 تلقی می‌شود، می‌تواند سازمان را در معرض یک حمله مبتنی بر "کرم" (Worm) قرار داده و به‌سرعت شبکه را در اختیار مهاجمان قرار دهد. CVE-2020-0796 در اسفند ۱۳۹۸ توسط مایکروسافت ترمیم و اصلاح شد.

همچنین نویسندگان Lemon_Duck ماژول‌هایی را نیز برای هک سرویس‌دهندگان REmote DIctionary Server (معروف به Redis) و Hadoop در این بدافزار لحاظ کرده‌اند. برای شناسایی این سرویس‌دهندگان، درگاه‌های TCP/6379 (درگاه پیش‌فرض Redis) و TCP/8088 (درگاه پیش‌فرض Hadoop) پویش می‌شود.

Lemon_Duck برای در اختیار گرفتن کلیه منابع دستگاه، سایر استخراج‌کنندگان ارز رمز اقدام به متوقف کردن آنها می‌کند.



نویسندگان این بدافزار به طور مستمر در حال تکامل این بدافزار مخرب هستند. موارد زیر از جمله نکاتی است که با رعایت آنها می‌توان سازمان را از گزند این بدافزار مخرب ایمن نگاه داشت:

- 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
- محدود کردن سطح دسترسی کاربران
- مدیریت سخت‌گیرانه سطوح دسترسی اعمال شده بر روی پوشه‌های اشتراکی
- پرهیز از قابل دسترس کردن سرویس‌های حساسی نظیر MS-SQL و Domain Controller در بستر اینترنت یا مقاوم‌سازی آنها
- غیرفعال کردن پودمان RDP یا حداقل تغییر درگاه پیش‌فرض آن
- بکارگیری محصولات موسوم به Device Control و مسدودسازی حافظه‌های جداشدنی
- اطمینان از نصب بودن اصلاحیه‌های امنیتی بر روی تمامی دستگاه‌ها؛ در این مورد خاص، به ویژه اصلاحیه‌های CVE-2017-8570، CVE-2017-8464، CVE-2017-0144 و CVE-2020-0796
- ارتقای سیستم‌های عامل از رده خارج
- استفاده از ضدویروس قدرتمند و به‌روز با قابلیت نفوذیاب
- 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

نـشـانـه‌هـای آلـودگـی

دامنه، نشانی IP و نشانی URL:

- ackng[.]com
- ackng[.]com
- amynx[.]com
- jdjdcjq[.]top
- zer9g[.]com
- zz3r0[.]com
- ackng[.]com:444
- b69kq[.]com:443
- k3qh4[.]com:443
- 71.87.85
- hxxp://d.ackng.com/if_mail.bin?$params
- hxxp://d.ackng.com/kr.bin?$params
- hxxp://d.ackng.com/ln/xr.zip
- hxxp://d.ackng.com/m6.bin?$params
- hxxp://d.ackng.com/m6g.bin?$params
- hxxp://d.ackng.com/nvd.zip
- hxxp://d.ackng.com/ode.bin?$params
- hxxp://t.amynx.com/7p.php?0.8*ipc*%username%*%computername%*+[Environment]::OSVersion.version.Major
- hxxp://t.amynx.com/a.jsp?[attack_vector]_20200820&%username%+%computername%+UUID+random_no
- hxxp://t.amynx.com/eb.jsp?0.8*%username%*%computername%
- hxxp://t.amynx.com/ebo.jsp?0.8*%username%*%computername%

- hxxp://t.amynx.com/ipc.jsp?0.8
- hxxp://t.amynx.com/ipco.jsp?0.8
- hxxp://t.amynx.com/ln/a.asp?src_date_*whoami*hostname*guid
- hxxp://t.amynx.com/ln/core.png?0.8*ssh*whoami*hostname
- hxxp://t.amynx.com/ln/core.png?0.8*ssho*whoami*hostname
- hxxp://t.amynx.com/ln/core.png?rds
- hxxp://t.amynx.com/ln/core.png?rdso
- hxxp://t.amynx.com/ln/core.png?yarn
- hxxp://t.amynx.com/ln/core.png?yarno
- hxxp://t.amynx.com/ms.jsp?0.8*%computername%
- hxxp://t.amynx.com/mso.jsp?0.8*%computername%
- hxxp://t.amynx.com/rdp.jsp
- hxxp://t.amynx.com/rdpo.jsp
- hxxp://t.amynx.com/smgh.jsp?0.8*%computername%
- hxxp://t.amynx.com/smgho.jsp?0.8*%computername%
- hxxp://t.amynx.com/usb.jsp?0.8*%computername%
- hxxp://t.jdjdcjq.top/ln/a.asp?src_date_*whoami*hostname*guid

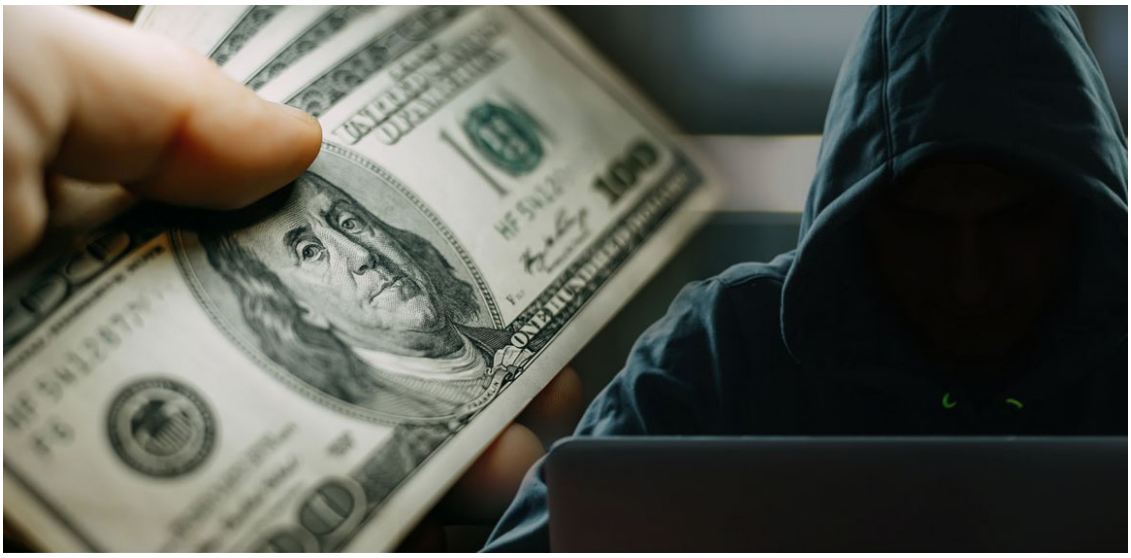
فایل:

- blackball
- zip
- zip
- C:\windows\temp\tmp.vbs
- C:\windows\temp\p.bat
- C:\Windows\mkatz.ini
- C:\Windows\Temp\mkatz.ini
- C:\Windows\m.ps1
- C:\Windows\Temp\m.ps1
- C:\Windows\m2.ps1C:\Windows\Temp\m2.ps1
- C:\Windows\Temp\svhhost.exe
- C:\Windows\Temp\svvhost.exe
- C:\Windows\Temp\svchost.exe
- C:\Windows\Temp\ipc.txt
- C:\Windows\Temp\hash.txt
- C:\Windows\Temp\eb.txt
- C:\Windows\system32\svhost.exe
- C:\Windows\SysWOW64\svhost.exe
- C:\Windows\system32\drivers\svhost.exe
- C:\Windows\SysWOW64\drivers\svhost.exe
- %temp%\godmali4.txt
- %temp%\kk4kk.log
- ./xr -o lplp.ackng.com:444 -opencl -donate-level=1 -nicehash -B -http-host=0.0.0.0 -http-port=65529

فرامین زمانبندی‌شده:

- \Microsot\Windows\Bluetool
- \Microsot\Windows\Bluetooths
- Autocheck
- Autostart
- Escan
- Ddriver

پیوستن Conti
به جمع باج‌افزارهای افشاگر



گردانندگان باج‌افزار Conti با هدف اعمال فشار هر چه بیشتر به قربانیان خود و وادار کردن آنها به پرداخت باج اقدام به راه‌اندازی سایتی حاوی اطلاعات سرقت‌شده کرده‌اند.

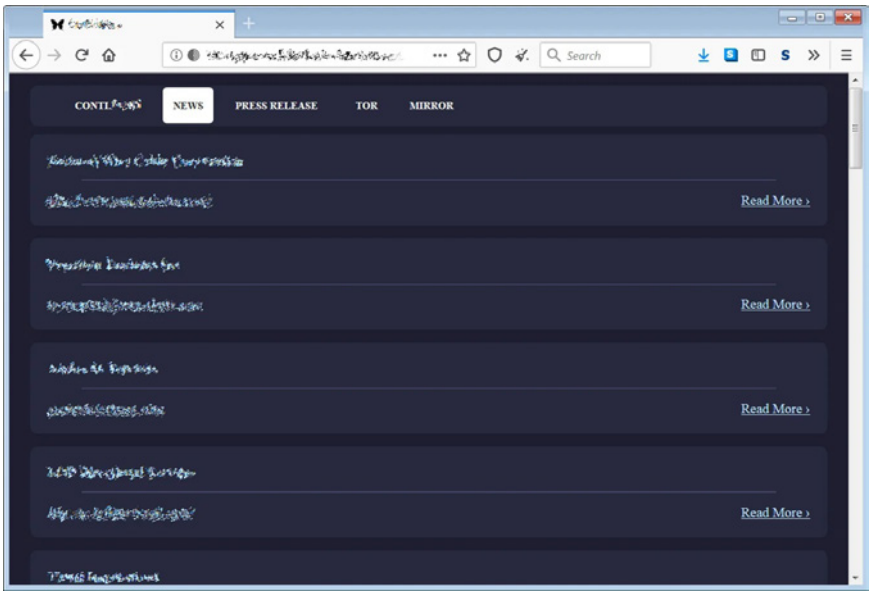
در حالی که تا همین چندی پیش، پس از آلوده شدن دستگاه‌های شبکه به اسب تروای TrickBot در نهایت باج‌افزار Ryuk بر روی آنها توزیع می‌شد از حدود یک ماه قبل انتشار Ryuk از طریق TrickBot متوقف شده و در عوض آن باج‌افزار Conti بر روی دستگاه آلوده نصب می‌شود. به همین خاطر برخی، Conti را جایگزین یا نسخه‌ای جدید از باج‌افزار مخرب Ryuk می‌دانند.

Conti باج‌افزار نسبتاً جدیدی است که در قالب خدمات "باج‌افزار به‌عنوان سرویس" (Ransomware-as-a-Service - به اختصار RaaS) به هکرهای باتجربه و حرفه‌ای در اجرای حملات موسوم به Human-operated اجاره داده می‌شود.

در جریان اکثر حملات Human-operated مهاجمان پس از رخنه به شبکه سازمان پیش از اجرای رمزگذاری، اقدام به سرقت داده‌ها می‌کنند.

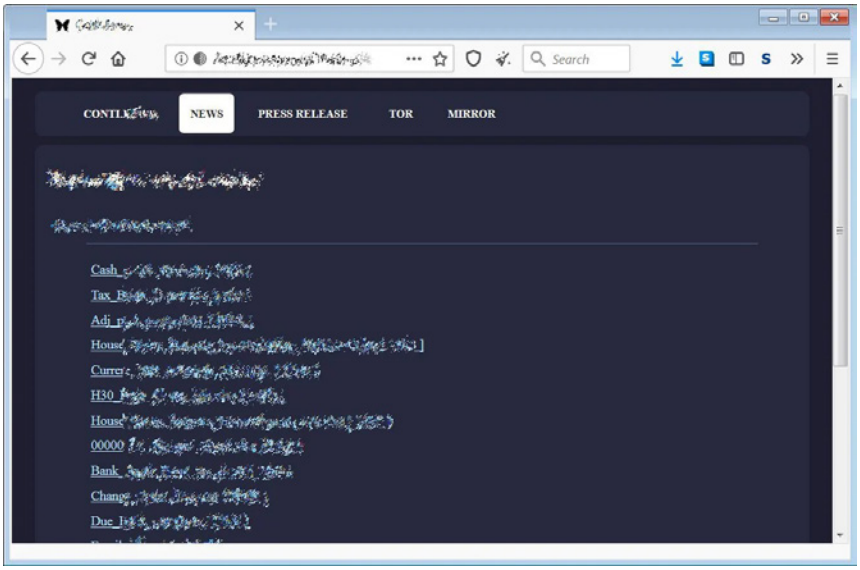
مهاجمان در ادامه با تهدید انتشار این داده‌های سرقت شده در سایت "نشت اطلاعات" (Data Leak Site)، قربانی را ناچار به پرداخت باج که معمولاً مبالغ هنگفتی است می‌کنند.

اگر چه Conti تقریباً از اوایل تابستان فعال بوده اما سایت نشت اطلاعات آن با عنوان Conti.News تنها چند روز است که راه‌اندازی شده است.

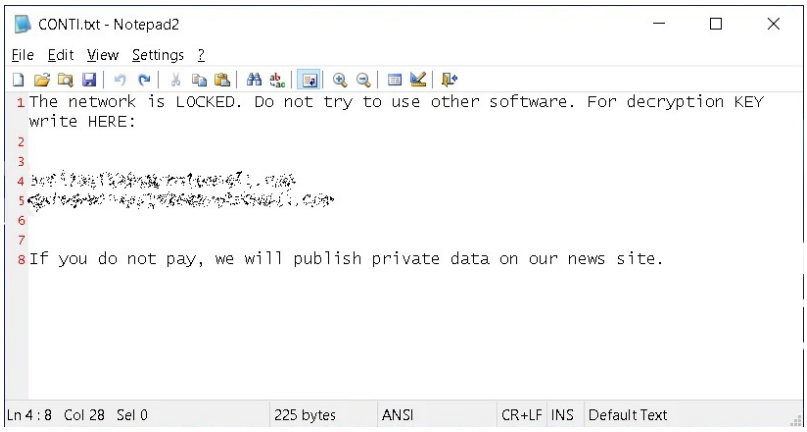


در حال حاضر در سایت مذکور نام حدود ۳۰ قربانی که در بین آنها اسامی چند شرکت سرشناس به چشم می‌خورد فهرست شده است.

برای هر کدام از قربانیان صفحه‌ای اختصاصی ایجاد شده که در آن بخشی از داده‌های سرقت شده در دسترس قرار گرفته است.



همچنین گردانندگان Conti تغییراتی را در اطلاعیه‌های باج‌گیری خود لحاظ کرده‌اند؛ به‌نحوی که در نمونه‌های جدید آنها به این موضوع اشاره شده که در صورت عدم پرداخت باج اطلاعات خصوصی قربانی منتشر خواهد شد.



از جمله باج‌افزارهای دیگری که علاوه بر رمزگذاری، داده‌های قربانی را سرقت می‌کنند می‌توان به Ako، Avaddon، Clop، CryLock، DoppelPaymer، Maze، MountLocker، Nemty، Nephilim، Netwalker، Pysa/Mespinoza، Ragnar، Locker، Revil، Sekhmet، Snatch و Snake اشاره کرد.

توضیح این‌که نمونه مورد بررسی در این خبر با نام‌های زیر قابل شناسایی است:

Bitdefender:

- DeepScan:Generic.Ransom.Ryuk2.912230DA

McAfee:

- Ransom-Conti!B7B5E1253710

Sophos:

- Troj/Ryuk-AM

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.

Evilnum که کارزارهای آن را می‌توان آن پیشرفته و مستمر (APT) دانست از سال ۲۰۱۸ فعال بوده است. حملات این گروه هدفمند و تمرکز اصلی آنها شرکت‌های فعال در حوزه فن‌آوری مالی (FinTech) بوده است. یکی از دلایل موفقیت این گروه تغییر مستمر ابزارها و تاکتیک‌های آنها است.

به گزارش شرکت مهندسی شبکه گستر، در توسعه ابزارهای مورد استفاده Evilnum از زبان‌های برنامه‌نویسی JavaScript و C# بهره گرفته شده است. اما شرکت سایبرایزن در گزارشی به بررسی بدافزار جدیدی از این گروه پرداخته که با زبان Python برنامه‌نویسی شده است.

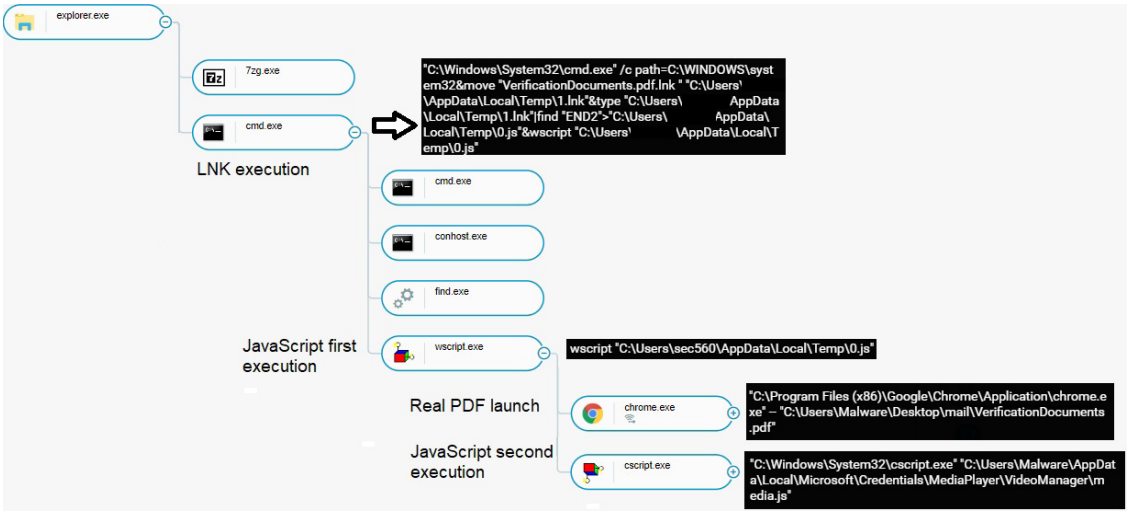
بدافزار مذکور که سایبرایزن از آن با عنوان PyVil یاد کرده نوعی اسب تروای دسترسی از راه دور (Remote Access Trojan - به اختصار RAT) محسوب می‌شود.

PyVil 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 (Spear Phishing) صورت می‌پذیرد. پیوست این ایمیل ها فایلی با پسوند ZIP است. فایل ZIP نیز خود یک فایل LNK در ظاهر با پسوند PDF است.

Name	Date modified	Type	Size
PersonalKYC.pdf	20/07/2020 10:07	Shortcut	686 KB

اجرای فایل LNK توسط قربانی موجب فراخوانی فایل‌های مخرب مورد نظر مهاجمان با بهره گیری از تکنیک های موسوم به "بدون فایل" (Fileless) بر روی دستگاه می‌شود.



برخی فایل‌های مخرب مورد استفاده در جریان این کارزار به نوعی نسخ قدیمی نرم‌افزارهای معتبری همچون Java Web Start Launcher هستند که کدهای مورد نظر مهاجمان در آنها تزریق شده است. برای مثال تصویر زیر مشخصات فایل دستکاری شده را نشان می‌دهد:

ddpp.exe File name	c:\users\[redacted]\appdata\local\microsoft\cre... Path	c:\users\[redacted]\appdata\local\microsoft\cre... Canonized Path
javaws.exe Original file name	Java(TM) Web Start Launcher Internal name	c: Mount Point
August 4, 2020 at 11:48:47 AM GMT+3 Creation time	August 4, 2020 at 11:48:47 AM GMT+3 Modification time	07717219943e911ac4cfb8e485a99cfb MD5 signature
2f66d8de16bb6959fd4e0eb6d6616ec4a5f6bd... SHA1 Signature	Not specific Product type	Oracle Corporation Company name
Java(TM) Platform SE 8 U131 Product name	11.131.2.11 File version	8.0.1310.11 Product version
false File is Signed	false Signature Verified	False Signed by Microsoft
Windows Executable Extension type	262144 Size	Copyright © 2017 Legal copyright

تصویر زیر نیز مشخصات فایل معتبر را نمایش می‌دهد:

javaws.exe File name	c:\users\[redacted]\desktop\javaws.exe Path	c:\users\[redacted]\desktop\javaws.exe Canonized Path
javaws.exe Original file name	Java(TM) Web Start Launcher Internal name	c: Mount Point
August 10, 2020 at 5:18:23 PM GMT+3 Creation time	August 10, 2020 at 5:18:24 PM GMT+3 Modification time	1b608a3165adcaa835f4bf1dc1647588 MD5 signature
c120d348b2767ba4cb78d5fc070a1655f3de6d... SHA1 Signature	Not specific Product type	Oracle Corporation Company name
Java(TM) Platform SE 8 U131 Product name	11.131.2.11 File version	8.0.1310.11 Product version
Oracle America, Inc. Internal/External Signer	true File is Signed	true Signature Verified
False Signed by Microsoft	Windows Executable Extension type	268864 Size

همان‌طور که پیداست تفاوت در امضا نشدن فایل مخرب توسط شرکت سازنده (Oracle) است.

علاوه بر استفاده از ضدویروس قدرتمند و به‌روز و ابزارهای موسوم به ضدهرزنامه، آموزش کاربران در پرهیز از باز کردن فایل‌های ناآشنا و مشکوک نقشی اساسی در ایمن نگاه داشتن سازمان از گزند این نوع تهدیدات مخرب دارد.

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

https://www.cybereason.com/blog/no-rest-for-the-wicked-evilnum-unleashes-pyvil-rat

دامنه‌ها:

- voipasst[.]com
- voipreq12[.]com
- telecomwl[.]com
- crm-domain[.]net
- leads-management[.]net
- fxmt4x[.]com
- xlmfx[.]com
- telefx[.]net
- voipssupport[.]com
- trquotesys[.]com
- extrasectr[.]com
- veritechx[.]com
- quotingtrx[.]com
- vvxtech[.]net
- corpxtech[.]com

نشانی‌های IP:

- ۱۹۳.۵۶.۲۸[.]۲۰۱
- ۱۸۵.۲۳۶.۲۳۰[.]۲۵
- ۵.۲۰۶.۲۲۷[.]۸۱
- ۱۷۶.۱۰۷.۱۸۸[.]۱۷۵

درهم‌ساز:

- db5d09edc2e9676a41f26f5f4310df9d13abdae8011b1d37af7139008362d5f1
- ۳b7cd07e87902deae4b482e987dea9e25a93a55ec783884e8b466dc55c346bce
- c7cf5c62ecfade27338acb2cc91a06c2615dbb97711f2558a9379ee8a5306720
- f5f79e2169db3bbe7b7ae3ff4a0f40659d11051e69ee784f5469659a708e829e
- cff5ed4de201256678c7c068c1dbda5c47f4b322b618981693b1fd07a0ea7e68
- ۸۳c375dcdadb8467955f5e124cf4e8d6eac78c51c03fb7393dc810a243ba1a90
- ۴ce0954ca7173bd696afe8f44bf48027b3d4d630c0cce414b95d6715e662b5fb
- 0d7dc074be83f1096f39ba95bfc4e1a17c411dbed0e5eeeb48e88a12d79b541c
- ۴e396586fd6dfcc24686aae73ba5c336939ee7a7aa9ffb76a1f78867926c6e4b
- ۵aa1109d057e830d6f3faf4b6ff6f69075d158dadb5f46794b3e07685922d09d
- ۲۵c119a7ee5b53212b5992992907a7772610b491ce2992c860dc206d0f3f844d
- e678ec3dbccfbd5cf0f303d2841e726ac7628044de5297bf9ebe791d66270a2f
- a81f152a31c03b45dbcf29439050bbe080b1f6308b032aebc0205886d1f41e5d

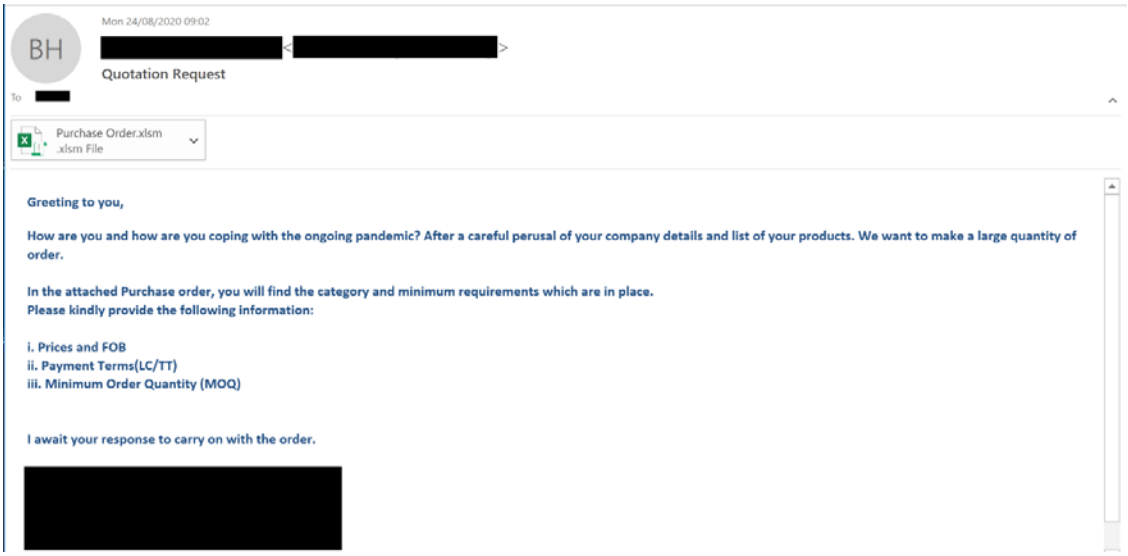
- ۶۱۳۶۳۰۹a207b89ccd423f8c087a9cdd633d8f5e78b8ebd576b7750b49274c532
- 0c920e7dfdd0028d9d15344c2e9c64ae57c2c9417dc7b22b865fdfe0cc0b8b1f
- ۷۹e21ff9142821b2e3d6e3dc8d812e86da231dbbd1217415b4add748a4c1ce3c
- c4b90fdec0848ad68abe18a42889ec0e5e45b7678afbf0353fedf53915b76275
- ۷۹e21ff9142821b2e3d6e3dc8d812e86da231dbbd1217415b4add748a4c1ce3c
- ۴۵۷۴۲۳۹efb728913fd379cc914039b1d7fa8c3ac8d6e3503d6f5bc73de504c96
- ۷۹b032dbb8ade21b97be5dcaa63c974b6cdbb3c6f32b4abf2872288ae43ea4a6
- ۱a3f39dc604dbca691aefeaf1d5a372fbca3650003d4145671525a2960e1239e
- bdc20527d5afc4f13fa45c9182c8f58eb88cb4edc76aa38be83d95fd3365ce0a
- ۰۴۸۳۸۸c04738763c0ec57124e3a88fc82a545639636fb5ed6cd397881dd6ced9
- ۱۱d9a87b144c0eaf71e8dea1b08117d464ed7f24a6e716e935e0c7f3a7e03edc
- 0b95c8c70d2dad47baef15d0299cd7e273e8a59ae0420921632b21789a80aef0

انتشار بدافزار
از طریق نوعی خاص از فایل‌های Excel

مهاجمان در روشی خلاقانه و البته مخرب در حال آلوده‌سازی سیستم‌ها به بدافزار از طریق نوع خاصی از فایل‌های Excel هستند. بهره‌گیری از این روش موجب پایین آمدن شانس شناسایی بدافزار و تسهیل عبور آن از سد محصولات امنیتی می‌گردد.

کارزاری که این فایل‌های Excel در آن نقش ناقل بدافزار دارند از اواخر بهار امسال فعال بوده و سازمان‌ها را در کشورهای مختلف هدف قرار می‌دهد.

در این کارزار ایمیل‌هایی با موضوعات در ظاهر مرتبط با صورتحساب و سفارش خرید که این نوع فایل Excel به آنها پیوست شده به کاربر ارسال می‌شود.



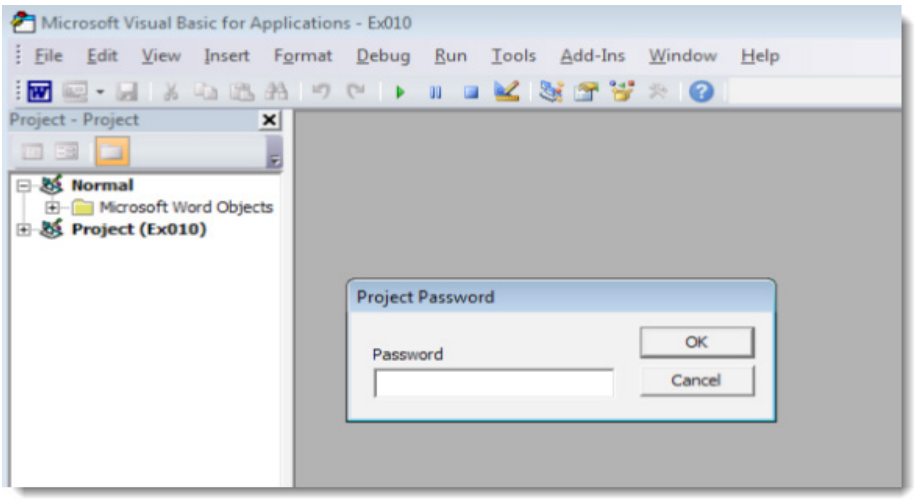
نکته قابل توجه اینکه فایل‌های مذکور نه در نرم‌افزار استاندارد Microsoft Office که توسط یک کتابخانه مبتنی بر .NET. با نام EPPlus ایجاد شده‌اند.

معمولاً برنامه‌نویسان از این کتابخانه جهت اضافه کردن قابلیت موسوم به "ارسال در قالب Excel"و (Export as Excel) یا "ذخیره در قالب صفحه گسترده" (Save as Spreadsheet) به نرم‌افزارهای خود بهره می‌گیرند. کتابخانه مذکور قادر به تولید صفحه گسترده

در قالب Office Open XML - به اختصار OOXML - بدون هر گونه فراداده (Metadata) است. همچنین EPPlus امکان افزودن ماکرو (Macro) را به صفحه گسترده فراهم می‌کند.

به گزارش شرکت مهندسی شبکه گستر، فایل Excel مورد استفاده در این کارزار حاوی یک اسکریپت مخرب ماکرو است. در صورت باز شدن فایل و کلیک کاربر بر روی دگمه Enable editing ماکروی مخرب اجرا شده و پس از دریافت بدافزار، آن را بر روی سیستم قربانی نصب می‌کند.

مهاجمان با استفاده از EPPlus نیز اقدام به تخصیص رمز عبور به ماکروی لحاظ شده در فایل کرده‌اند که در نتیجه آن امکان مشاهده کد مخرب از کاربر و محصولات امنیتی سلب شده است.



ضمن اینکه ساختار متفاوت فایل ایجاد شده توسط EPPlus موجب عبور آن از سد برخی محصولات ضدویروس و پویشگران ایمیل شده است.

در نمونه‌های مورد بررسی، بدافزارهای دریافت و اجرا شده توسط ماکرو، جاسوس‌افزارهایی همچون Azorult، AgentTesla، Formbook، Matiex و njRat بوده‌اند. این بدافزارها اطلاعات حساسی نظیر رمزهای عبور ذخیره شده از طریق مرورگرها و نرم‌افزارهای مدیریت ایمیل را استخراج و به گردانندگان خود ارسال می‌کنند.

بر طبق آمار شرکت امنیتی مک آفی تعداد ماکروهای مخرب جدید در سه‌ماهه اول سال میلادی جاری افزایشی ۴۱۲ درصدی در مقایسه با دوره قبلی داشته است.

علاوه بر استفاده از ضدویروس و ضدهرزنامه قدرتمند و به‌روز و همچنین پیکربندی صحیح تنظیمات ماکرو، آموزش کاربران در مواجهه با ایمیل‌های ناآشنا نقشی اساسی در ایمن‌سازی سازمان از گزند این نوع تهدیدات دارد.

فهرست نشانه‌های آلودگی (IoC) این کارزار به شرح زیر است:

درهم ساز:

- ۷d057dd5e8aa5e5562ce9598b6c606009ac7ec9a776edaf2d9ab2bcba347f00d
- ca4e091b93bd83468ae327ebff0926ae36ead03977a15ca73f7c2d9936d5144d
- ۳۴۱c88ec95fe4544b021ca347504064ae6d75c5e6e34d15f0823added11270e2
- ۳۳۱۰۵۲۵۵۵۶۸dc2908288601f702518c107d1262f127328218fdde70047b1a78b
- ۰۲f2ef392aadd8b486f022e3cd6bad2e6d0a2b6d39d2371b7d528e9ea6607a00
- 0d1524963d4d84b11c445d790e87c7ff2b53fef2f1c7d83abb0acf055bb1f88b
- ۱a74c0f00eaafc71570dbbbedb04005c9ffa726be5d25a9662b084fe6cf330a0

- ۳۹a9cbc67d57ccb8fd100ad0b5f2eb217c44feeb9d3f91c4be7e76338ad9a6d2
- ۳c51cd93b2321df2f3d939c1f0d045e6ed60fb33c4f445a4794e0987cd0de941
- ۵b2448e8b351214253d1a0f892efefc96cfcf4d2b51db2890d18f1af6d815287
- ۵c61dc124d13af2cd77828ed40807ddcd6790aa365b01c9cf9844a6bbf4188d0
- ۸f1ba82cad6bb1e9a27c6083fd8170d1067b1081439991b4147bedea991b4b1c
- ۹d3df770b6dcd5beb650a097a597bb70c49dde306517bbc731812bf18a806719
- a1445c88428ea52370d4379824bb1ebfac9c4a7ca172167b035097ee1a95485e
- acddabc78b0393a0b2822760a7e1d0d99eec3d7f2eaebdeb156369f36c9297c7
- b0e129540ee58ba0b23d465d0722e396a0500270a02b95b9bf632257c8d7f540
- c22ee6c1ffbbc94db718846d0d68da507573c24eb66ab1122a1d2a177fa42e2f
- df08c73129390db8bc51d52b403da41c92b946f2087a5bb3420b39c35aaf1e24
- f04dea1f1961781fd71d0bc778a50191e6133b38776aea562e0a8de0d4839fa6
- ۰۹۲۳f59b8b74bb67e46f62c6f2e6976be1d6b7b3ba1981eaa34673bfa2fa6d87
- 0b3f7a46c2376a4df9a7f15edc2f8fbaeb82b3bed52c675f92b0763d8de4ec50
- ۶c7295281dc0cee461d9d155c60271afed3dede70a297b65854fb9624c45b839
- ۸۲۲۴۵۰e5d4edad3d423f2a1fc96dea6ad0c6526d7b729b4854aec0b5ce7f9fd5
- ۸۸c3bb0f65a4507d724e5ff23a4587ac935a2394ffc0a65cd7770c4babb0996e
- a1c4da69ac7d81dbb6f4164eacc0da251b2da88a47e5f20c31507a4ca212357f
- aa41dc5b743292a550042e40eb1341edad8e6d181791f8f43dbefee0f3807929
- b533b8d4babe7ee8f42e24f90690c6444871c038234afedd45c0a8c942bb9df4
- c6b21d3260763f2056795d21d7a748f040f6fac6be5c1e450b905ec0bb46bbde
- f67b2b5288f9b0bb5fda819a46153daab4e338a96893d030056a221669515e9a
- ۸۲۶۹۵۷۳۴۱۶۵a830a7ec7f6030e27a9f3996df3a1c5a66ff3fefd41d2ef360b6f
- c40fa887be0159016f3afd43a3bdec6d11078e19974b60028b93def1c2f95726
- f51db63fe8be8e59e25e8363e5930309e9a9148925e583da18ea7e31bc9b0a96
- ۶۲۱۷۸۳dc841294e82a0912305f6638eb32572858fcaeb06a02753e36427bbb5b
- ۷e2917b1dd6daf2a235863d5fe40d292aa0372ad4880b5aa742855c76bd717b7
- ۰۰b2c7ee70bb3f29655e0c3b4eb07d76974702f39b9845220fa6e36a7be50c0f
- ۰۱acb46cbf549670eb502ad5840a816704bc433efeab7c82bf5a5f424c2dca58
- ۰۲fec2367e453d31e91cb9c34c937e58dbe8e5e5dff8b1400146c386f0737922
- ۰۳۰۷۶d67424903da167425c85349f2216951e011f6e0f10835e62e97e3ef9073
- ۰۳۹af9ca3b7fbc01c5b39b5cfec1a69ab44fc6e2dd4c71249f8aabec64f2ed9b
- ۰۵۸۱۴۲e8814bccee1ed81992a601e4f755b8e71525ed235d7b800e7ffd477d06
- ۰۶۳fbc6410f4542f4bbdd6f14182c5a411538d1ca884795ecbb82e29fc2b3d40
- ۰۶ca2c5ea52e63ab41491258e941086d8c6250aafb62e3fe93aa5d0858389af2
- ۰۸۵۹c26fd38d388dea87430e57c93c5fb4da7b978b2cbd746c4b20eb468d0008
- ۰۸۷۵d852719a6d039ce8697fa09f715a5bcb73f9197ed11a6542eb9f708bdab4
- ۰۹۲ea93921a5a98ea4a892f0da4556c14a1a483ec7ce13e07ac76a98d39ce1cf
- ۰۹۳۳c843ccb88cfbeaad94e253f30f8a8f80fa2250f54b625659541455c68de5
- ۰۹c9764646b5fd10290d561bf1841b123fc5599fdcca46760db4c8a883a67d83
- 0a7e2e56ddf654151b898a8c0a1c0b9d18a6c29a05fbb7f75df72fc7c4cea175
- 0e049cb0cb5da9b8050d4b407d6207b1d9d580a472869ffc9a52deaf5068e038
- 0e688b38f8824eb311afb1f26ea9176461147b48233aadc485dd405c49ab1b17
- 0fb26f19e30fbd8a79fb1a97c515e8dffe912fb53ed8b580f8d052d7fe3570df

- ۱۰۲۰۴۵f1813b3f00940f18e585631a0bf4aa39bb45bb90567a10f22520f23870
- ۱۰۴f8c1332e6b74722d70f9def8a9e1047a38fa880bbcd4e9bded6045305ee46
- ۱۴۷۷c8218db86c04b6ea602db18a74f6df749dd1d9c746bc409e8424157f32d3
- ۱۴۸a026124126abf74c390c69fbd0bcebce06b600c6a35630cdce29a85a765fc
- ۱۵df82f880bb2cdf16b953132f7dd0a80195bd266a98d32b7965391c0f6c08da
- ۱۶۱ade8ac6cb6107129a14fa6aceab06e873200ae13ea262bde1c2073c22301c
- ۱۶b52b81eecc5c79829b08e51a1cb71a4c6edf7447bd54cd7f783baddfbc5d34
- ۱۷۸fe3c3f021fd3abe778a9342d10d458b4b1a5d8da37736c9f8d5bf0b75f3fb
- ۱۸۱bd17ff9203ad7f097b76b10c61986835b2e154871f0bf1707531553cbafed
- ۱a343a1f550f061e16f49834bff55ad31a36aebd323fa7289f8d8ea395d88347
- ۱e2c6183522325bd2cc303e0acbfe83ddb8780ae2f083badee999891a0a9e988
- ۲۱d6825efd27302335a44a71f15d767ad5104fe18de541e8c1de8b7bec19a5b8
- ۲۲۷۲۰ce874580141941d61799801276b93aea14cd382f1ec3328f22921ea2520
- ۲۲b81e827a27007711a92a72e5b7b72ae1f4da6e8bd707c784751cdabfc0e763
- ۲۲ecb0e895a1aabb64acd7ebf3a73e5fa3fc93147cf4a9f3ac194d493df3dfea
- ۲۴d8103f7221bdddb23e2e2b901aa35238ab8369eda3c50eb3459cc1c7fec56b
- ۲۵۳۷e0dbc060ab93f55644bd49794c8e34d22a662b96e43a64a211d2583f15f3
- ۲۷fa7d56700d70b5702db1e7df92689d64733e9f3e568bdfb07bd712e4a76d4d
- ۲۸c713da2ea10f5e6817d951b2d03d857049e4e5963607b56ebd9cd496520a48
- ۲۹۵۱۴۶۷۸۳۷e74eb373a91f75ef2100a9e08c3d2fa4360cf7cfae5fa74fcf1cb9
- ۲a1c155eddcec617178343cb020df991fd665bdaf5fe5c16f2341eae4a08c665
- ۲ab0f6ae05223c9fc33bad509ebee4599da87f7ba810c639683477636db677c6
- ۲c2027c74d70fdfea03c69dd403a4ab7e3fa4202ef728e4d0e2c232bff15ea79
- ۲c85738faf54a7e87518c8b842cb632c1c2a8ceb80c209cbab3a9e552e05527d
- ۳۰eab4e461c76f40ddda3d89e2571b019afef3733b4004bb11a5a0c0a91059c0
- ۳۵۰۷ec1ea493fa77357bd6777f2fd8c1506b4694233bbfac5846c04f250f5d66
- ۳۶ffcf89799678a3546c40696e2df8de7f0e1fecd927eaf37df81e5612682c50
- ۳۸bcd9be700352e4a5006413f3a86f3b8c3536a0bc26fa435f819e4f2bba6626
- ۳a9b7eaa900fd48b31a145b322ac74f69c3bef74e3fa28642e3b6fea248ee390
- ۳cf60ebd0550470ef1af91bec89af8821c8d3f400d0ba4b030f0078811d61bcc
- ۳d2f4071f4039fc8d0fa05ecc9cbad6f350e028dbae28f059d6f40446e688a16
- ۴۱feaadc0d993dfa6539c34b7ea21b8d5e8dbc36548beadd7af0cf2f3eb2f94f
- ۴۲۵a292d93fc938bbf2f3f2b835f5408bf92c7851bfcbbe3746886edb6cceb4b
- ۴۲۶۶۵۸e14b0a77aa55344cedfa391f7de75b38fa9f3b0709bc0b83c9e6f50969
- ۴۵۴۸۸e4fc4494fc3e5f5a8d1769b743658738b9b2190a82884ca916575c1245f
- ۴۵۷ad9b165795858f87389383c77e4339c94cda66b99e798951ab8ba7d5ce0ef
- ۴۵cab564386a568a4569d66f6781c6d0b06a9561ae4ac362f0e76a8abfede7bb
- ۴ab13bf4b35e0ef28ae5525e3f344cf68967f9f764d0e34e91c6e28de3a74f19
- ۴b914ac20061af52b2e79e1ee99e8e63f59e270dc013e4a6556c8fac13a833bc
- ۴c5ded319ccb28f5fb737cf1dd1cf48c63390f14a10d6869b799a9cbc7e6e8db
- ۴defe854d09703a761b371239e75a1159c4037b24c4e8f830711c72b13aae75f
- ۴ebeccafe65679b83ee0d8cb5ff45a446a205ba65546c9121557dc49eb8ffb99
- ۴ec1304679ab30488b4b909a6c11f7faca9d5ee5e900733f2bf1b421d3c6b7c8
- ۴eecb58cb12874aa41c821a3db8fb733f5ef9ab62286f0848a8b6b63e254c746

- ۵۰۰۶۵ecd۹e۵۱۷۰۰bd۵b۱۱۲۴۷۷۱۶۳۱۷۳۵fee۶dc۶۱۳e۱de۶۰a۹۹۵۷e۴bf۸۲e۵۷a۶
- ۵۱۱۲۶cf۹b۵۴۳۷۳a۸۲e۸afe۳f۰۴۳a۶c۲c۴۴۴۴۲e۰۸۵۲f۸۸a۰f۸f۳۴a۰۰af۷e۶۵۹f۸
- ۵۱۶۲d۶۷fe۵۷۱a۸۰e۹b۱dc۷۶۸۳a۹۹bf۹۱d۰۹e۵۱۲۶۳۹a۰۹f۸۵۳caec۷۶a۹۸۶۱abe۶
- ۵۲۴۴۷۸b۵۶dc۳d۱۶bdb۱fd۰e۱۷۴a۵۳۴۰۸۱b۶cd۶a۰۷۶۴۰e۹faf۷۲۳efb۵d۱۶f۰۳۹۷
- ۵۲۸۳۲d۹۷۰۴۶۹۴bef۳۵f۷۷۸۵a۹۱۹a۸۳cb۹۸fc۱۱۰ac۴۳۰ed۲۷۶۱e۲۸d۸۵۱۸۹۸bc۰۹
- ۵۲c۳f۴d۹c۸۷ea۸۸a۳f۲۵۴۳۸۸dc۲b۷۰a۵۴۹bdd۲d۷۶e۲ccd۲af۵۰۱۰۴۵۴۴fd۰۹۵b
- ۵۳bc۲۴fddffe۸۷e۱۳f۱۴۱۴۲۸ab۸۶۰۵eea۳af۲df۲dce۲۶۸a۰۱۱b۳e۰e۱۲۱۳e۸ea۳
- ۵۴ce۷۸e۲۳۹۰f۳۷۸۸dc۷e۷c۲۳۲cf۶۰۴e۷d۹f۵۱۱۲۶۹۷۶۸۴۳۱۰۶۳۳۱۷۱۶b۰d۸۸dc۷۶
- ۵۶db۳۸f۰۰f۹۳ac۳۳۵۰da۶f۳af۳f۸d۵۸۴۸bfc۱۶c۸۱۲۱bd۵۹۸۶۹f۸c۴۴ae۰۸c۶۲dc
- ۵۷b۸۴e۷cff۶۲۳۰۸b۰۹d۰۱a۷۷۴efeb۹۶۲۹b۳۲۵۷۳a۴۷۸۴ba۰۵۱b۹۷۲e۳۱۱۲۸۷b۳۸۸
- ۵۸d۶ec۵c۸۰۳۴۳f۲d۸۶e۸۲edee۴۷cf۲۹۱۲۳۱۰beb۱fc۰f۱۲۸ce۷d۶۷۲۳dce۱c۹۳۳a
- ۵e۹df۵d۸۷۲cc۱f۰a۷ef۲f۹۳d۳۹۱۰۶a۲bb۴۵۱۴۶۵۰af۶a۴a۷f۶۱۷۲a۹۵ff۹a۳۸۵d۲۹
- ۵f۱۵۴۶c۲۸e۰۶۶۹۸۴۰۰fdb۰c۳۰۷bc۸۲e۴ab۷۴ecac۴۹۱۳cbd۱۰۶۶۴۸f۱۷a۸۱e۰۲ff
- ۵f۷dda۴۹dc۷۷d۴bc۲۸۲۷bd۵۰۵dc۵۳۰f۲۷۳۳۵۲a۸۹۹۸e۰۲۲۲fd۵۷۲۰۵۸e۸۴fa۲۰eb
- ۵fed۲۰۵۰ee۱۰cb۴۳cc۶۳۸۵۲۵۵۸۵۹۷d۶۴e۸fe۶۷c۳۰af۸۶۸۲b۹f۶۰ce۳۵۶e۲۴۹۰۱d
- ۶۱a۵۰۵۹۰۷fe۳d۸۸۸۵۶e۱be۸۴bf۲۵a۴۶۱۰۰۴۷۹۸۵۴af۵۲۴۷f۳۴۵۶۸۵۰۷۶۵۷۹۹c۴۹
- ۶۱eefc۶۹۷e۰۶ce۳be۰۰fc۵c۰e۳۸۱۲۱c۵۷f۸۸۱f۱۴d۸۵۹a۰۵c۹۰۸۲۳۰۴ad۷c۸۸۱f۸
- ۶۳۱۲ac۹۶۸ac۰۹۳۷۱۹۹۲fd۱۸۰e۸۶e۴c۵۵a۸۲۲۶۵۱c۱e۶۸۹۵۰۶۹۵۷۵۴۲۷۵b۴۷۲d۵۸۸
- ۶۴fb۲۴ad۰a۲۳۱۰f۶a۱۵۲۴cecf۳۶ef۹۴c۹abf۲ada۶a۳ff۱b۷e۴۵۷۰af۸d۱۹۹f۲ef
- ۶۷c۱۴۳۷cf۵۹daee۹۱a۳db۷۵eb۳۰f۷۶b۰ebf۷efedad۷۰۰e۸ecf۱۴۸۱e۷۶۱a۳۹۸۹۴
- ۶۸۲۹ad۷۱۱۳۶۷ebd۵۰c۶۱ac۴ae۳۳dc۱۳c۷bf۶۹۵۲bc۵d۷۲۰۴۱۱۳ce۰۹۷۶۵۴۷۰۲۷cf
- ۶۹fa۴b۳۱۵۶۰۸۰۴۰۹۰۰ae۴۶۳bc۸a۷۹۰۶۶۳۱۷۲۵۴aeb۹d۶۶ec۱۳۲e۲۳۶۲a۶۷۸۲۸۵۴
- ۶ca۵e۶c۹۲a۸۵۰be۷dda۹e۲e۸۹b۲۵۵۴e۶۴۹۰۱a۸۱۲ef۰۶۸e۷۲۶c۶۴fb۹cc۵۳e۵c۴۹
- ۶e۵fe۶۴daa۸۱dd۱۸۶ffc۹۹b۷df۶۹۸bd۳۸fa۹۵۴۳ecfebe۷cf۸۳۵۵۵۶۳۳۸۱c۴b۹۹۰
- ۶f۲۳df۵b۲۹f۶۵۷۲۳e۷b۹faf۵e۱۹۶fed۳۰۸e۷cd۲a۴a۴۴۶۳d۰dbefacf۴d۹۴f۵۳۸c۱
- ۶f۲e۵۰b۷fd۱۶۱۵۱۷c۳۲۶۰ef۶f۵ef۴bae۷۶۸۱۶ef۱۷۴۵۱۴۳۴۴c۸ecea۷۳adfa۱۳f۴
- ۷۰۰d۳aa۲aa۹e۱f۳۰d۶۲ea۸۷۹b۸c۵۶b۷۰۳adf۴۶۶۳b۹b۰۷۷۸b۶b۸۵d۴۳۹a۴a۸۷۰۲۰
- ۷۰f۵۱aa۷cd۷۰۵d۰۸۱dbd۴fcae۲۸۲de۵۱۶۳۶d۱ec۰۹c۹ef۰۹a۷dcd۴۹d۸۹ba۷۶۵d۶
- ۷۱۷c۵cb۱۴۰۶d۸e۰۴f۹۸۵۳۷۰۹c۶e۰d۳e۰۸c۲۷c۲۳۴۹e۳fd۶۳e۷۲۶۹۹۴۶b۱۴۲۴b۲c۳
- ۷۲۰e۶ca۸b۱۹a۲۴a۸۱df۲۴a۳۵۰a۱a۷۰eb۱۷b۷۱e۳۲bbf۶۷befbd۲۹۳۴۸۸۰c۱۵a۹۸b
- ۷۳f۵۷ca۶۱۳۸۷۸de۳ed۴۷۴۷edbb۶f۳aea۱۱۸e۰۶۳۴eb۳۸a۴cbfa۳f۳۸۵۱b۶۶۸f۷۵۲
- ۷۴c۲ce۲c۹۸۸e۴۰b۵b۴۷۶e۲d۸b۳۶cc۷۶۴e۱۷۹۲۹e۳۹۸۷a۸e۱۸be۹beecb۰۳۶۹۶۸۳۹
- ۷۵۲ac۲۸۷bf۲۴۳cb۹۶df۴efb۱۸bc۳f۱e۰bc۷۳۳۲۸۶ef۰۷c۲f۹c۲۵۰۵۵۴۵۱۳۳۲f۴۸۹
- ۷۸۶f۴۰۴a۰ad۹۴dd۴۳۸ffbec۸c۸b۶۴۵cdf۱۷۰۸b۵۱۷b۶bb۶d۸۸۳۳۸f۲d۰۶۲a۹۷۱f۰
- ۷cec۰۲۶۴a۸۸a۴۳۷۹ee۴۱d۲e۴bdc۵bd۳ca۹۹c۸b۰۲d۱۷۰۶c۱۳db۲۹۷۰۴۱e۵۲۱۶۱۹a
- ۷dee۱۷۳۹ef۳۷۶۷c۵۰eda۵a۲۵۷ef۲۹a۴ec۷e۹c۹ab۰۵a۳۸۲b۸c۸۵۸۱۹f۴۴baa۴d۹d
- ۷f۰۴۹۹۱a۰da۲۶ee۰۷d۶fe۴fa۹b۰e۰۶۴a۷d۹۳۷bc۲۳۸۹ad۶ee۶۰۱d۳۶۶۰c۰۵۴f۶۹c
- ۸۴۰c۶۷۶۴۳a۰۹c۱۶۴۱۵۴b۷۰۳f۶۰۸f۶۳۹۹۸۷۴۲۵۱۳۸۶a۰۲d۶۲c۰۴۴b۶eddd۲۸۹۵۷۱a
- ۸۴۱۳۶e۷۶۷۲۳۱۷۳۳۰۷۴c۸۷۶۴۰c۳e۵dfa۳۶۱adc۴fbbffd۰۲۷d۵۳۰۸bc۷۷۰۲۰۵۱۲d۸
- ۸۵۱ebeeV۴۹b۰۲d۶۵۵۰b۸d۶۲۴d۷e۸۴۳a۶۰۲۹۴۴۳۹۸۱e۸۱۷۷۶۸de۷۳۴۹d۶۷ceacff۶
- ۸۵۷۸d۳۲۸eb۴۱cbcbf۴۵۳b۴e۹۵۲۲۵aeeV۷۶f۱۷d۹e۵۱۰d۳۸۸۴۷۷۳f۲۲۵eb۷ba۰۰۶۲a
- ۸۶e۴۲۷e۸f۶۵۱۷۷۸۵۲۳df۵bd۸۷۱f۹d۵۴۰۴f۳۸۶۵۴c۰۹d۹۳d۹۵dcc۰۹۰۳e۸۵۵۴۰۵ef
- ۸۹۶۶cf۴۷۵۰۱۸b۶۰۶۵۱bf۲f۸۷۲ecc۲dc۹۷dcd۶۴ed۲۳a۲۶f۲۷e۸۷۹۳fc۴۹۲۶۰۹f۲a
- ۸۹b۹cfafb۰dfa۰a۵be۸b۲۵۹۲۸۲۶۵۹۸۵bdf۹۳۸d۰۲۲۹b۴۶۸۴۹۴۷f۱d۹۷۹۲ea۹e۴۷۷

- ۸a863b5f154e1ddba695453fdd0f5b83d9d555bae6cf377963c9009c9fa6c9be
- ۸b3ad8ccd1c9e2b7af2de1f3586a8bbcdf3c4a79e722aa6e309890a9fa0cd76c
- ۸c49532a4bcb4c79b7f87162ecc1d5581d88dfe2b729b76e153869d007f86dfe
- ۸d3996209ba2ecdf049096fbe494f5cb082441a864ddef20239954e8e8b8adb3
- ۸f0e1b1b0c1740ee119d83cbbf6deabe4ef4529d1820c852afd7210d98b9faf2
- ۸ff565a71accea4b92754bade1ae9b4b9f84ca0e5a5e4ff3e02fb08c72640ff3
- ۹۰b18263268b13d49a1f20cdae04c78864a8eb6acb038e6279d42b183a1d395d
- ۹۰b29f45ccd8a594a410c914c6f5300917baaa53b325330b8c5637f5fd3b8116
- ۹۰c466829477bba1e353c08ffc8554b45016ce3ab84c1f9dd44d04e1d7c8ab19
- ۹۲۶e59ef03f563a5275e84e75970c1713e6ee41e23ea3aa9d4abda5247221bac
- ۹۳a808a7823319a0643ac3cd43e409daec52d81f3d3a0070a6ef5a54f2bd786b
- ۹۴۶cdfa03a229cd83d0e927880e79049a707f534162e97d544027b51d550c388
- ۹۴abf64f20c01859317ff6eaffce2727ba25d4ade9b4c26002e3dc652aba3ef8
- ۹۵b8c1f748ebef3dcbad0fa3148d46d483d00620c3e56153e41fde8978daece9
- ۹۶۶d24f3e5616ad72402614d846d892fd5756ade55219ca6f3a5440259fc8594
- ۹a63be97d600c50abdddc22afd998e25ddac5030bcc4846b97cf7e1932eae7b8
- ۹b3f405188c61465d161759487dd24f7fdf8d35f53c9c4ce1a7de2991608d384
- ۹e39df4b339d4f021e3e781b7841d83888436aeda4bfda5a79038fb429eebde1
- ۹f533cfa9dc9cdd3c029924003ace654b277859f42266f442a2a547f335a3f2e
- a02258ba10419bc678e832f3224dc6340e22f567f7b8ba1d344a5e5213d129a1
- a076eaa41100a2ed81c3e420199a2cb7d5d9b6d70cd1c0f5c628169c33977f97
- a231b9e0cacf439e9d9e0522a3a7504fdd6a96d3d39e553ccc93b817db2e63ac
- a386bad94268c0fef10a3ede577bce3a16349d91b971da46845f84069a65ceec
- a4d0229132d6011ef40105a20c0005b0df402bcb08ddeb5771bf81ef6242c76e
- a6605413f5e39b2a8445a6639bed5f4663f59604bb15183d7c0065e3992348d7
- a742996c138614c9bbbc712e585000dd76e9fd3c56b02df030bfaad65fe6c0aa
- a840f0e1d1bfeb727b0d18cde3eb6995ae00f8bcf6d1e75aa2adbf40fca6008f
- a979468a630cd6363538edb3060e347367a00d5258ffe50d93c698764a48553d
- abd64beeee4c8f1d4777bd9ae186dce9228ac1f057e7e43d2b41052ff8661027
- ae58dbbdf285bf8bc6df4534b058bb0bdf857d3034c1a825dc38893464f28cdf
- af46cdc24841137fde934d17a1b059d8cf98d9bb480472f8abef75d4d7eca1f2
- b0c6b6931a14e29fbc24b04bda9caeb12139909899111ae8c80bbc190200c118
- b21a7ccc87b5e83878f537cb8cc1c75e098f454986cbe1f57b36e7ae74ad5e5f
- b29a4e94a19a7a488a37054b74c86aa6e43830bd10c675ddbe80274aead159cc
- b2b64ad1bd5028e67ede21914b3501f8c1e2f6172b12c0cfd516b41226e83d0c
- b3db0853d60e24942f88ede24d013d620dc0910d4fad364acb34c03969868e4e
- b54d4b871add23fd4ef21dee298f93898cd5e1b5601a772b997e165ab7624c0b
- b68057dffd25d389158dd3753873a8570d37c8eb5907e92b7e4f65aa362668a9
- b8ddc759605f6dc20f126f205e70600f2c033121bbbfb88943b150a975ffc431
- ba208e171bbb853b04e0e6bf86df6175aea437e07e828c6d8164a51d81c9c4b1
- bb0627e48f1f432fcac19ab38eb1b7702f450e977d6ee78773e18fd670cf50fc
- bb1972afed7256922af8f7471f5e9e35f48ae24e302c66c0b1621c7deb499b3e
- bfe10b027e5af48524a277948f87f3d86df3b97fb05007c6e2126ecd1ce47153
- bfec15094b359e8582cc9597e29b9ff7db464b53408a66e1b1b7114c8edd088d

- c12ce1a73f6ab3029d1286de66751e079068e64bfc56f0652c8e19dd8c45e350
- c14bfab4289d53156e7f7f262935f4ba89d3657c1d0786d39b411c31e2ae8413
- c3c9751b7fc99801b395deb901fa0e9249e30ab310ca11528f6f82f502075286
- c3d0c76d8f14f098528be4d1bacdafd4ef566fd10599656363bd9e5dea082200
- c56ede1cae965b51ebeaaef254be5bf59a5bb2114f95b124e113062a0c9f60b3
- c704cee668058193d6349efff9555def1d296e21350a3a6e1e63acc996a4909a
- c8958307f5aede648da79b48385b054e30d7767af9da142721faccdb93448bef
- ca13825a684064276129a80caaffcc375c08bf46fb056ff2c94e8d4239dffbc8
- cab782e84c418a33549dc65a3d50b057deb17e2ae73eaf9c91be43802caf5dd5
- cb7d9e3fa6aa00fd18b44e1753b33cb1fcf80cdf6ecfc2164660d95843415aef
- cceb3af9ebb2d61c72ec1b5ef8b4715232b0e4224ce3b544a989438c4c23343c
- ce560011ab1f62ec4349301a19d55d4dcc7f8522a068f10e3813550197f5e9cf
- cf7587677945995e72470478cb36943e825bfe45fb82ea9da4a18b996cda6aa2
- cf9a25362438287900e28afd987befdcf651ea2e124f688d559273838f4b19a0
- d07a0bf242945c6fc13636e619071fafaeb03c2fea67c535c7ab0cbf68591cac
- d400ec69727a9c5ff6beea13ff08389c7910076c0f15669156d3732d03432ba7
- d93c3916280ae69d76d1ee3ea7327d7d966a1b369abdfa399e6aa902aa8cebf4
- d94e59fbbf9b5f93c469c0a903348ee95bc57f3b04991664ab568cdafa5fee6a
- dd07e4b225894da846f284566118ccc96a2aabca90c24337f36ddcc7066eeef4
- dd50de2a6100b7f33d8a53077298fa93ef09d86b75bcf088237941c4789369f2
- e02e2804d98658cc76ef89c09f52f66843e68cb94f7578f1ff856aa4999a3c19
- e06eb321cb8a38d8b9d29b9c1cc25af54254ac6dd57543f1cd0944a8e14a08b1
- e1dbe3338367397078a2e48770e98581226a9658c8812136725368a0c9ed53cd
- e36d67b672af1a1d41f77ad77abbf6d171e941bae26adcca1285a56936543647
- e3880ad4c222eaacdbe02f1e6b3c66d580d2f1335ad7ce2e342a45039eb30116
- e4bc0675158b375e0d118bc6a65c4b4caaaac2fb1202400a38ab3372ad851735
- e6ee6ba8fd749eb739ae17e401afb9c676d98ec9c60af7f897b5612bc6fdf393
- e7422c2c762926db79e45052c8257f1602c169bd306f30b3b82a1e3b169e5df9
- e75fcca16e431ee212b32548db05b6a8b2c9b208b47fcae3dfe0b3a385875f51
- e8002827a287f26cf1c8447e12a207360bf93079b40a5304da9dfa00c2809875
- e8afea66b28be927e5d534d3e6c2f375812404ba8ae9158cf41c66ad5f5cb33f
- ea17ffb8a502d013a4f54038cebdc1ec3fcc82404547a83f540e76fa4d380213
- ebd05c6e7ee7fb75d8121d7cefae8926ec1cca9d3114d0bd85772764f25836ea
- ec6c99b6c06de0e55a3f1168401218b5177a0ac06b9d32697afbee43a096ccea
- ecce5ff9b0aee22f086a1177fc0f96df5eedfad9860b8dfb7de7d67285125c68
- ed8d14180f477075f95847b47a019b02f0e179436db737052e3d8516cb48798c
- f0ab12c3aff583ac8993a72681013e2823f2199e739bf4b625f14e6fa0688fa4
- f234211a8277ad6929ab846aba05c925531fee15033faf7b6cf43631348622ff
- f245ca7356fcede97d484b5c96083e256f7c893dbd9b38d338d82ba60aaa4d27
- f3f7ddce5c5906d8f759ff7c3b376dbde07ab845400465ccf16f6c37ee1ed24e
- f4dcd21a2e0b2f4432b665157a1f934e5063be6bbf7ef5f92b365bbbeca92331
- f5d3aa74bda0272a4936902fe273189e17c1582affdec331318fa856804aebc3
- f62b4c2837258be0170fbcbfc844844f94e736aa559179228735d6e08fd895e6
- f669e327181307c2164d546634bbb1a8748029e27bed6f441f70210a9b575e25

- faadceee59468746b521773ea2038965ccb148e66c13011409c67bb4164bddfd
- fbe84a0b514ecbbfda0537e60cadadd0be4c00a49645bbbd3513613c762526cb
- ff4386a4ec4746d085fe2fa9cf974f39334fa3c64b27b2ab88468ea72c898fb2
- 0cceaafd17df02aaa546d427453894e81847cf2056a136bd3c0a7fd5320f379c
- b0c083472dee81acc9ce7dc31bd93bd358d15387dc797aef9ce4ff1f6dd8689c
- d1d9c177155e5a9a03880a50c6244acf64541e6dbd6ec89f716593401f91f226
- cfa367d911ebeaa1691499541cee04c559afdd29f361ae1ff34b0179dc95bdae
- 0ff9db2fae8bc12ec221cb1d48dc849e755d3060915e79b8faa5ad90435badbe
- ۲f9afe182833f0d8c78e054ad354368f20d76bffa339a01e69d749c843f4c0ae
- ۳۶۴۹۲e7e0d018546eeb857d763804fd0494b0fabfbdb66a031596f252ecf6fdf
- ۳b5dc0cfe5cc7f4ce51afade57e86fa2cf47f9b13f190307eb9c40fcb2b82157
- ۳f528af489e1ab1aa6a290cbc8752b3f2661fcf238ffe59b21ed89735c7647f1
- ۶۷۸c6d8585a6f5b73f1fb953852d72b18af35da4566248098ff1f13384977167
- bcfc34cba923f98aaef2289267664a3637c46b20d409a86e2eeefeb71f3cc4bb
- d333e67190f3eb0ce3ca187771324222964fa978d587fbff9f3f566f4b828f49
- ۱a000b08359d94eda05df64622b24c451ceffc772ad6473f3cce6fe95dc889c9
- ۲ba660e566a7bbaf32c1141d72009736e3772adcbb6d497ec56b32beaddc56a8
- ۳۰۷bf15bfb598feb5fa1fb506db3cc89219e4a2bff75f69dea3821bd86240446

عناوین ایمیل:

- Re: Quotation required/
- Quote volume and weight for preferred
- *****SPAM***** FW:Offer_10044885_[companyname]_2_09_2020.xlsx
- [SUSPECTED SPAM] Alternatives for Request
- Purchase Order Details
- Quotation Request

اخاذی ۴.۵ میلیون دلاری از شرکت Equinix

و چند درس برای سازمان‌های ایرانی

در یک سال اخیر تعداد حملات هدفمند باج‌افزاری به سازمان‌های بزرگ در کشورهای مختلف از جمله ایران افزایشی چشمگیر داشته است. این مهاجمان اهداف خود را به‌صورت خاص انتخاب کرده و پس از سرقت فایل‌ها و داده‌های بااهمیت اقدام به رمزگذاری و از دسترس خارج کردن فایل‌ها می‌کنند. در ادامه، قربانی تهدید می‌شود که در صورت عدم پرداخت مبلغ اخاذی‌شده، اطلاعات سرقت شده به صورت عمومی منتشر و افشا خواهد شد.

بسیاری از مهاجمان حرفه‌ای به این نتیجه رسیده‌اند که تمرکز بر روی سازمان‌های بزرگ و اخاذی هنگفت از آنها سودمندتر از انتشار انبوه باج‌افزار و باج‌گیری مبالغ به مراتب کم‌ارزش‌تر از قربانیان عادی است.

برای مثال، در پی حمله سایبری به شرکت چندملیتی Equinix و آلوده شدن سیستم‌های آن به باج‌افزار Netwalker مهاجمان از این غول مرکز داده مبلغ ۴۵۵ بیت‌کوین (معادل ۴.۵ میلیون دلار) در ازای عرضه ابزار رمزگشایی و عدم افشای اطلاعات سرقت شده، اخاذی کرده‌اند.

بر طبق گزارشی که پیش‌تر شرکت امنیتی مک‌آفی آن را منتشر کرده بود گردانندگان باج‌افزار NetWalker در کمتر از شش ماه موفق به دریافت حداقل ۲۵ میلیون دلار از قربانیان خود شده بودند.

بررسی‌ها نشان می‌دهد دسترسی مبتنی بر Remote Desktop Protocol - به اختصار RDP - به ۷۴ سرور متعلق به Equinix در بازارهای زیرزمینی تبهکاران سایبری به فروش می‌رسیده است. به همین خاطر رخنه اولیه به شبکه Equinix از طریق پودمان RDP بسیار محتمل دانسته می‌شود.

از جمله باج‌افزارهای دیگری که در جریان حملات هدفمند مهاجمان آن علاوه بر رمزگذاری، داده‌های قربانی را سرقت می‌کنند می‌توان به Ako، Avaddon، Clop، CryLock ،DoppelPaymer، Maze ،MountLocker ،Nemty ،Nephilim ،Pysa/Mespinoza، Ragnar Locker، Revil، Sekhmet، Snatch وSnake اشاره کرد.

متأسفانه در ماه‌های اخیر نمونه‌های متعددی از اجرای این گونه حملات به سازمان‌های ایرانی به شرکت مهندسی شبکه گستر گزارش شده است.

همچون کارزار اخیر NetWalker، در اکثر حملات هدفمند باج‌افزاری بر ضد سازمان‌های ایرانی، اتصال از راه دور مهاجمان به دستگاه‌های قابل دسترس در بستر اینترنت و با پودمان RDP باز و در ادامه اجرای حملات موسوم به سعی‌وخطا (Brute-force) اصلی‌ترین روش هک بوده است. در مواردی دسترسی RDP به یکی از سرورهای سازمان قربانی تنها برای چند ساعت باز بوده و همین مدت کم مهاجمان را قادر به هک موفق هک سرور کرده است. پس از موفقیت در رخنه به نخستین دستگاه شبکه، مهاجمان، با استفاده از اطلاعات

اصالت‌سنجی هک‌شده در مرحله قبل، اقدام به توزیع باج‌افزار بر روی دستگاه‌های قابل دسترس از روی دستگاه نخست می‌کنند. باید توجه داشت گرچه نمونه‌های باج‌افزاری مورد استفاده توسط مهاجمان در بسیاری از مواقع توسط محصولات ضدویروس مطرح قابل شناسایی است لیکن با توجه به سطح دسترسی بالا (Administrator) مهاجمان بر روی دستگاه مورد هدف، عملاً امکان تقلیل کنترل‌های امنیتی و نظارتی تعریف شده و دست‌درازی به محصولات نصب شده بر روی دستگاه و در ادامه، نصب هر گونه بدافزار و ابزار مخرب دیگر برای آنها فراهم می‌شود.

همچنین عدم توجه به نصب کامل اصلاحیه‌های امنیتی از جمله معضلاتی است که در بسیاری از سازمان‌های ایرانی هک شده به چشم می‌خورد. اطمینان از نصب بودن اصلاحیه‌های امنیتی به خصوص اصلاحیه‌های با درجه حساسیت "حیاتی" (Critical) بر روی تمامی سیستم‌ها نه یک توصیه که یک الزام و ضرورت امنیتی است.

متأسفانه تبعات اجرای موفق چنین حملاتی برای سازمان های قربانی بسیار پرهزینه و بعضاً جبران ناپذیر است.

موارد زیر از جمله نکاتی است که با رعایت آنها می‌توان سازمان را از گزند این بدافزار مخرب ایمن نگاه داشت:

- 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
- غیرفعال کردن پودمان RDP یا حداقل تغییر درگاه پیش‌فرض آن
- محدود کردن سطح دسترسی کاربران
- اطمینان از نصب بودن اصلاحیه‌های امنیتی بر روی تمامی دستگاه‌ها
- استفاده از ضدویروس قدرتمند و به‌روز با قابلیت نفوذیاب
- استفاده از دیواره آتش در درگاه شبکه

اجرای ماشین مجازی
برای مخفی کردن فایل‌های مخرب باج‌افزار

بر اساس گزارشی که شرکت امنیتی سوفوس آن را منتشر کرده، Maze، یکی از مخرب‌ترین باج‌افزارهای فعال این روزها با راه‌اندازی یک ماشین مجازی بر روی دستگاه قربانی فایل‌های خود را از دید محصولات امنیتی مخفی نگاه می‌دارد.

به گزارش شرکت مهندسی شبکه گستر، حملات مهاجمان Maze هدفمند بوده و در صورت موفقیت در نفوذ به شبکه قربانی، پیش از آغاز رمزگذاری، فایل‌های با اهمیت را شناسایی و نسبت به سرقت آنها اقدام می‌کنند. در ادامه ضمن اخاذی مبالغ هنگفت، قربانی را تهدید به انتشار عمومی اطلاعات سرقت شده می‌کنند. 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.

```
Attention!

----------------------------
| What happened?
----------------------------

We hacked your network and now all your files, documents, photos, databases, and other important
data are safely encrypted with reliable algorithms.
You cannot access the files right now. But do not worry. You can get it back! It is easy to
recover in a few steps.

We have also downloaded a lot of private data from your network, so in case of not contacting us
as soon as possible this data will be released.
If you do not contact us in a 3 days we will post information about your breach on our public
news website and after 7 days the whole downloaded info.

To see what happens to those who don't contact us, google:
* Southwire Maze Ransomware
* MDLab Maze Ransomware
* City of Pensacola Maze Ransomware

After the payment the data will be removed from our disks and decryptor will be given to you, so
you can restore all your files.
```

بر طبق گزارش سوفوس، این مهاجمان مدتی است که فایل‌های مخرب Maze را بجای اجرای مستقیم بر روی دستگاه از طریق یک ماشین مجازی نصب شده بر روی سیستم مدیریت و توزیع می‌کنند.

به‌عبارت دیگر ماشین مجازی، بستری حفاظت نشده را در اختیار مهاجمان قرار می‌دهد که امکان اجرای آزادانه فایل‌های باج‌افزار را بدون نگرانی از شناسایی و مسدود شدن توسط محصولات امنیتی فراهم می‌کند.

پیش‌تر در کارزارهای باج‌افزار Ragnar Locker نیز از این تاکتیک بهره گرفته شده بود.

مهاجمان Maze پس از رخنه به یکی از سیستم‌های شبکه، با توزیع یک فایل MSI (با نام pikujuwusewa.msi)، نسخه ۳.۰.۴ نرم‌افزار VirtualBox را بر روی دستگاه نصب و در ادامه یک ماشین مجازی با سیستم عامل Windows 7 را از طریق آن اجرا می‌کنند. حجم ماشین مذکور ۲.۶ گیگابایت گزارش شده است. این در حالی است که در Ragnar Locker از ماشینی با سیستم عامل Windows XP با حجم ۴۰۴ مگابایت استفاده می‌شود. اگر چه استفاده از سیستم عامل Windows 7 موجب افزایش حجم داده‌های دانلود شده توسط مهاجمان و در نتیجه بالاتر رفتن احتمال شناسایی حمله توسط راهبران امنیت سازمان می‌شود اما در عین حال قابلیت‌های بیشتری - در مقایسه با Windows XP - در اختیار مهاجمان قرار می‌دهد.

	Ragnar Locker	Maze
MSI installer	122 MB OracleVA.msi	733 MB pikujuwusewa.msi
Virtual Disk Image (VDI)	282 MB micro.vdi	1.90 GB micro.vdi
Ransomware binary in VDI	49 KB vrun.exe	494 KB payload

Maze از موفق‌ترین باج‌افزارهای اخیر موسوم به Human-operated است که گردانندگان به‌طور مستمر در حال تکامل آن هستند.

این باج‌افزار از الگوریتم‌های رمزگذاری RSA-2048 و ChaCha20 بهره می‌گیرد. Maze حمله به نهادهای دولتی و کارخانجات بزرگ را در کارنامه دارد.

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

https://news.sophos.com/en-us/2020/09/17/maze-attackers-adopt-ragnar-locker-virtual-machine-technique/

آسیب‌پذیری‌ها و اصلاحیه‌های امنیتی

بهره‌جویی گسترده مهاجمان
از آسیب‌پذیری روز-صفر WordPress

مهاجمان به‌طور گسترده در حال بهره‌جویی از یک آسیب‌پذیری حیاتی در افزونه File Manager سامانه WordPress هستند.

File Manager، افزونه‌ای (Plugin) برای مدیریت فایل‌های سایت‌های مبتنی بر WordPress است.

به گزارش شرکت مهندسی شبکه گستر، آسیب‌پذیری مذکور که بر اساس استاندارد CVSS به آن بالاترین شدت حساسیت (۱۰ از ۱۰) تخصیص داده شده، ضعفی از نوع "اجرای کد به‌صورت از راه دور" (Remote Code Execution) است که مهاجم اصالت‌سنجی نشده را قادر به تزریق و اجرای اسکریپت‌های مخرب در سایت‌های با افزونه آسیب‌پذیر File Manager می‌کند.

چند ساعت پس از اطلاع از وجود این آسیب‌پذیری در File Manager و بهره‌جویی مهاجمان از آن، نویسندگان این افزونه اقدام به ترمیم باگ و انتشار نسخه ۶.۹ کردند.

بر طبق اعلامیه Wordfence دیواره آتش این تیم امنیتی (Web Application Firewall) ظرف چند روز گذشته، ۴۵۰ هزار تلاش برای بهره‌جویی (Exploit) از این آسیب‌پذیری را مسدود کرده که از گسترده بودن دامنه این حملات حکایت دارد.

به‌نظر می‌رسد در مرحله شناسایی، مهاجمان تلاش می‌کنند که فایل‌هایی خالی را در سایت‌های بالقوه آسیب‌پذیر آپلود کنند؛ در صورت قابل آپلود بودن فایل (آسیب‌پذیر بودن سایت) در ادامه اسکریپت‌های مخرب مورد نظر خود را در سایت تزریق می‌کنند.

نکته جالب اینکه در صورت موفقیت در رخنه به سایت، مهاجمان با تخصیص رمز عبور به فایل‌های در معرض نفوذ، از مورد بهره‌جویی قرار گرفتن مجدد آنها توسط هم‌قطاران خود جلوگیری می‌کنند.

به کلیه مدیران و راهبران سایت‌ها توصیه می‌شود که در اسرع وقت نسبت به به‌روزرسانی افزونه File Manager اقدام کنند.

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

https://www.wordfence.com/blog/2020/09/700000-wordpress-users-affected-by-zero-day-vulnerability-in-file-manager-plugin/

نشانه‌های آلودگی (IoC)

وجود هر یک از فایل‌های زیر در مسیر wp-content/plugins/wp-file-manager/lib/files/:

- hardfork.php
- hardfind.php
- x.php

ارسال درخواست از نشانی های زیر:

- ۱۸۵.۲۲۲.۵۷.۱۸۳
- ۱۸۵.۸۱.۱۵۷.۱۳۲
- ۱۸۵.۸۱.۱۵۷.۱۱۲
- ۱۸۵.۲۲۲.۵۷.۹۳
- ۱۸۵.۸۱.۱۵۷.۱۷۷
- ۱۸۵.۸۱.۱۵۷.۱۳۳

اصلاحیه‌های امنیتی مایکروسافت
برای ماه میلادی سپتامبر

سه‌شنبه، ۱۸ شهریور، شرکت مایکروسافت اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی سپتامبر منتشر کرد. این اصلاحیه‌ها در مجموع، بیش از ۱۲۰ آسیب‌پذیری را در سیستم عامل Windows و محصولات زیر ترمیم می‌کنند:

- Microsoft Windows
- Microsoft Edge (EdgeHTML-based)
- Microsoft Edge (Chromium-based)
- Microsoft ChakraCore
- Internet Explorer
- SQL Server
- Microsoft JET Database Engine
- Microsoft Office and Microsoft Office Services and Web Apps
- Microsoft Dynamics
- Visual Studio
- Microsoft Exchange Server
- SQL Server
- ASP.NET
- Microsoft OneDrive
- Azure DevOps

به گزارش شرکت مهندسی شبکه گستر، درجه حساسیت ۲۳ 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.

هیچ یک از ضعف‌های امنیتی ترمیم شده توسط مجموعه اصلاحیه‌های ماه سپتامبر، روز-صفر (Zero-day) اعلام نشده‌اند.
از میان ۲۳ آسیب‌پذیری "حیاتی" این ماه، چند مورد زیر بیش از سایرین جلب توجه می‌کنند:

- CVE-2020-0922 که یک آسیب‌پذیری از نوع "اجرای کد به‌صورت از راه دور" (Remote Code Execution) است که بخش COM در سیستم عامل Windows 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 CVSS، ۸/۸ از ۱۰ اعلام شده است.
- CVE-2020-1508 و CVE-2020-1593 که هر دو آسیب‌پذیری‌هایی در Media Audio Decoder هستند و مهاجم را قادر به در اختیار گرفتن کنترل دستگاه می‌کنند.
- CVE-2020-1057 و CVE-2020-1172 که بخش ChakraCore Scripting Engine در مرورگرهای مایکروسافت از آنها تأثیر می‌پذیرد. بهره‌جویی از این دو آسیب‌پذیری مهاجم را قادر به اجرای کد با سطح دسترسی کاربر جاری می‌کند.

از میان آسیب‌پذیری‌های "مهم" ترمیم شده در این ماه نیز می‌توان به اصلاح چهار ضعف امنیتی با شناسه‌های CVE-2020-1193، CVE-2020-1218، CVE-2020-1332 و CVE-2020-1594 در مجموعه نرم‌افزاری Office اشاره کرد. ارسال ایمیل فیشینگ با پیوست مخرب می‌تواند از جمله سناریوهای محتمل مهاجمان برای بهره‌جویی از این آسیب‌پذیری‌ها باشد.
فهرست کامل آسیب‌پذیری‌های ترمیم شده توسط مجموعه اصلاحیه‌های ماه سپتامبر مایکروسافت در جدول زیر قابل مطالعه است:

محصول	CVE شناسه	ملاحظات	سطح حساسیت
Active Directory	CVE-2020-0761	آسیب‌پذیری به حملات "اجرای کد به‌صورت از راه دور"	مهم
Active Directory	CVE-2020-0856	آسیب‌پذیری به حملات "نشت اطلاعات" (Information Disclosure)	مهم
Active Directory	CVE-2020-0718	آسیب‌پذیری به حملات "اجرای کد به‌صورت از راه دور"	مهم
Active Directory	CVE-2020-0664	آسیب‌پذیری به حملات "نشت اطلاعات"	مهم
Active Directory Federation Services	CVE-2020-0837	آسیب‌پذیری به حملات "جعل" (Spoofing)	مهم
ASP.NET	CVE-2020-1045	آسیب‌پذیری به حملات "عبور از سد تنظیمات امنیتی" (Security Feature Bypass)	مهم
Common Log File System Driver	CVE-2020-1115	آسیب‌پذیری به حملات "ترفیع امتیازی" (Elevation of Privilege)	مهم

محصول	CVE شناسه	ملاحظات	سطح حساسیت
Internet Explorer	CVE-2020-1012	آسیب‌پذیری به حملات "ترفیع امتیازی"	مهم
Internet Explorer	CVE-2020-16884	آسیب‌پذیری به حملات "بروز اختلال در حافظه"	مهم
Internet Explorer	CVE-2020-1506	آسیب‌پذیری به حملات "ترفیع امتیازی"	مهم
Microsoft Browsers	CVE-2020-0878	آسیب‌پذیری به حملات "بروز اختلال در حافظه"	حیاتی
Microsoft Dynamics	CVE-2020-16857	آسیب‌پذیری به حملات "اجرای کد به‌صورت از راه دور"	حیاتی
Microsoft Dynamics	CVE-2020-16858	آسیب‌پذیری به حملات "تزریق اسکریپت از طریق سایت" (XSS)	مهم
Microsoft Dynamics	CVE-2020-16860	آسیب‌پذیری به حملات "اجرای کد به‌صورت از راه دور"	مهم
Microsoft Dynamics	CVE-2020-16859	آسیب‌پذیری به حملات "تزریق اسکریپت از طریق سایت"	مهم
Microsoft Dynamics	CVE-2020-16861	آسیب‌پذیری به حملات "تزریق اسکریپت از طریق سایت"	مهم
Microsoft Dynamics	CVE-2020-16872	آسیب‌پذیری به حملات "تزریق اسکریپت از طریق سایت"	مهم
Microsoft Dynamics	CVE-2020-16864	آسیب‌پذیری به حملات "تزریق اسکریپت از طریق سایت"	مهم
Microsoft Dynamics	CVE-2020-16878	آسیب‌پذیری به حملات "تزریق اسکریپت از طریق سایت"	مهم
Microsoft Dynamics	CVE-2020-16862	آسیب‌پذیری به حملات "اجرای کد به‌صورت از راه دور"	حیاتی
Microsoft Dynamics	CVE-2020-16871	آسیب‌پذیری به حملات "تزریق اسکریپت از طریق سایت"	مهم
Microsoft Exchange Server	CVE-2020-16875	آسیب‌پذیری به حملات "ترفیع امتیازی"	حیاتی
Microsoft Graphics Component	CVE-2020-0921	آسیب‌پذیری به حملات "نشت اطلاعات"	مهم
Microsoft Graphics Component	CVE-2020-0998	آسیب‌پذیری به حملات "نشت اطلاعات"	مهم
Microsoft Graphics Component	CVE-2020-1091	آسیب‌پذیری به حملات "ترفیع امتیازی"	مهم
Microsoft Graphics Component	CVE-2020-1152	آسیب‌پذیری به حملات "ترفیع امتیازی"	مهم

محصول	CVE شناسه	ملاحظات	سطح حساسیت
Microsoft Graphics Component	CVE-2020-1097	آسیب‌پذیری به حملات "نشت اطلاعات"	مهم
Microsoft Graphics Component	CVE-2020-1083	آسیب‌پذیری به حملات "نشت اطلاعات"	مهم
Microsoft Graphics Component	CVE-2020-1053	آسیب‌پذیری به حملات "ترفیع امتیازی"	مهم
Microsoft Graphics Component	CVE-2020-1308	آسیب‌پذیری به حملات "ترفیع امتیازی"	حیاتی
Microsoft Graphics Component	CVE-2020-1245	آسیب‌پذیری به حملات "ترفیع امتیازی"	حیاتی
Microsoft Graphics Component	CVE-2020-1285	آسیب‌پذیری به حملات "اجرای کد به‌صورت از راه دور"	حیاتی
Microsoft Graphics Component	CVE-2020-1256	آسیب‌پذیری به حملات "اجرای کد به‌صورت از راه دور"	مهم
Microsoft Graphics Component	CVE-2020-1250	آسیب‌پذیری به حملات "نشت اطلاعات"	مهم
Microsoft JET Database Engine	CVE-2020-1039	آسیب‌پذیری به حملات "اجرای کد به‌صورت از راه دور"	مهم
Microsoft JET Database Engine	CVE-2020-1074	آسیب‌پذیری به حملات "اجرای کد به‌صورت از راه دور"	مهم
Microsoft NTFS	CVE-2020-0838	آسیب‌پذیری به حملات "ترفیع امتیازی"	مهم
Microsoft Office	CVE-2020-1594	آسیب‌پذیری به حملات "اجرای کد به‌صورت از راه دور"	مهم
Microsoft Office	CVE-2020-1335	آسیب‌پذیری به حملات "اجرای کد به‌صورت از راه دور"	مهم
Microsoft Office	CVE-2020-16855	آسیب‌پذیری به حملات "نشت اطلاعات"	مهم
Microsoft Office	CVE-2020-1338	آسیب‌پذیری به حملات "اجرای کد به‌صورت از راه دور"	مهم
Microsoft Office	CVE-2020-1332	آسیب‌پذیری به حملات "اجرای کد به‌صورت از راه دور"	مهم
Microsoft Office	CVE-2020-1224	آسیب‌پذیری به حملات "نشت اطلاعات"	مهم
Microsoft Office	CVE-2020-1218	آسیب‌پذیری به حملات "اجرای کد به‌صورت از راه دور"	مهم
Microsoft Office	CVE-2020-1193	آسیب‌پذیری به حملات "اجرای کد به‌صورت از راه دور"	مهم

محصول	CVE شناسه	ملاحظات	سطح حساسیت
Microsoft Office SharePoint	CVE-2020-1345	آسیب‌پذیری به حملات "تزریق اسکریپت از طریق سایت"	مهم
Microsoft Office SharePoint	CVE-2020-1205	آسیب‌پذیری به حملات "جعل"	مهم
Microsoft Office SharePoint	CVE-2020-1210	آسیب‌پذیری به حملات "اجرای کد به‌صورت از راه دور"	حیاتی
Microsoft Office SharePoint	CVE-2020-1514	آسیب‌پذیری به حملات "تزریق اسکریپت از طریق سایت"	مهم
Microsoft Office SharePoint	CVE-2020-1595	آسیب‌پذیری به حملات "اجرای کد به‌صورت از راه دور"	حیاتی
Microsoft Office SharePoint	CVE-2020-1523	آسیب‌پذیری به حملات "دست‌درازی"	مهم
Microsoft Office SharePoint	CVE-2020-1440	آسیب‌پذیری به حملات "دست‌درازی"	مهم
Microsoft Office SharePoint	CVE-2020-1200	آسیب‌پذیری به حملات "اجرای کد به‌صورت از راه دور"	حیاتی
Microsoft Office SharePoint	CVE-2020-1482	آسیب‌پذیری به حملات "تزریق اسکریپت از طریق سایت"	مهم
Microsoft Office SharePoint	CVE-2020-1198	آسیب‌پذیری به حملات "تزریق اسکریپت از طریق سایت"	مهم
Microsoft Office SharePoint	CVE-2020-1227	آسیب‌پذیری به حملات "تزریق اسکریپت از طریق سایت"	مهم
Microsoft Office SharePoint	CVE-2020-1576	آسیب‌پذیری به حملات "اجرای کد به‌صورت از راه دور"	حیاتی
Microsoft Office SharePoint	CVE-2020-1452	آسیب‌پذیری به حملات "تزریق اسکریپت از طریق سایت"	حیاتی
Microsoft Office SharePoint	CVE-2020-1575	آسیب‌پذیری به حملات "تزریق اسکریپت از طریق سایت"	مهم
Microsoft Office SharePoint	CVE-2020-1453	آسیب‌پذیری به حملات "اجرای کد به‌صورت از راه دور"	حیاتی
Microsoft OneDrive	CVE-2020-16851	آسیب‌پذیری به حملات "اجرای کد به‌صورت از راه دور"	مهم
Microsoft OneDrive	CVE-2020-16852	آسیب‌پذیری به حملات "اجرای کد به‌صورت از راه دور"	مهم
Microsoft Scripting Engine	CVE-2020-1057	آسیب‌پذیری به حملات "بروز اختلال در حافظه"	حیاتی
Microsoft Scripting Engine	CVE-2020-1180	آسیب‌پذیری به حملات "بروز اختلال در حافظه"	مهم
Microsoft Scripting Engine	CVE-2020-1172	آسیب‌پذیری به حملات "بروز اختلال در حافظه"	حیاتی

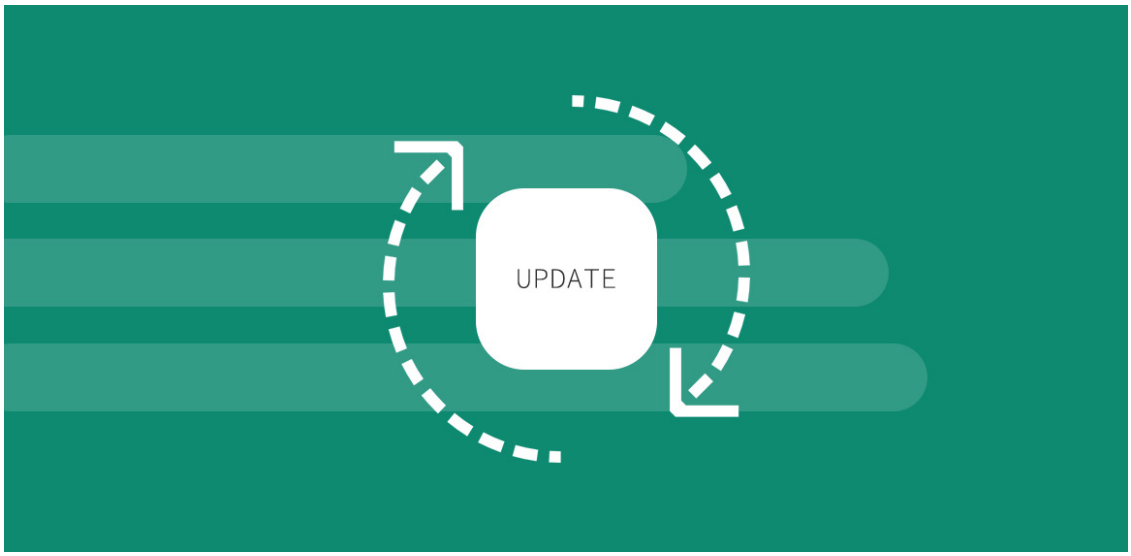
محصول	CVE شناسه	ملاحظات	سطح حساسیت
Microsoft Windows	CVE-2020-1596	آسیب‌پذیری به حملات "نشت اطلاعات"	مهم
Microsoft Windows	CVE-2020-1169	آسیب‌پذیری به حملات "ترفیع امتیازی"	مهم
Microsoft Windows	CVE-2020-1593	آسیب‌پذیری به حملات "اجرای کد به‌صورت از راه دور"	حیاتی
Microsoft Windows	CVE-2020-1159	آسیب‌پذیری به حملات "ترفیع امتیازی"	مهم
Microsoft Windows	CVE-2020-1598	آسیب‌پذیری به حملات "ترفیع امتیازی"	مهم
Microsoft Windows	CVE-2020-0790	آسیب‌پذیری به حملات "ترفیع امتیازی"	مهم
Microsoft Windows	CVE-2020-0922	آسیب‌پذیری به حملات "اجرای کد به‌صورت از راه دور"	حیاتی
Microsoft Windows	CVE-2020-0782	آسیب‌پذیری به حملات "ترفیع امتیازی"	مهم
Microsoft Windows	CVE-2020-0648	آسیب‌پذیری به حملات "ترفیع امتیازی"	مهم
Microsoft Windows	CVE-2020-0766	آسیب‌پذیری به حملات "ترفیع امتیازی"	مهم
Microsoft Windows	CVE-2020-1590	آسیب‌پذیری به حملات "ترفیع امتیازی"	مهم
Microsoft Windows	CVE-2020-1376	آسیب‌پذیری به حملات "ترفیع امتیازی"	مهم
Microsoft Windows	CVE-2020-1471	آسیب‌پذیری به حملات "ترفیع امتیازی"	مهم
Microsoft Windows	CVE-2020-16879	آسیب‌پذیری به حملات "ترفیع امتیازی"	مهم
Microsoft Windows	CVE-2020-1013	آسیب‌پذیری به حملات "ترفیع امتیازی"	مهم
Microsoft Windows	CVE-2020-1532	آسیب‌پذیری به حملات "ترفیع امتیازی"	مهم
Microsoft Windows	CVE-2020-1491	آسیب‌پذیری به حملات "ترفیع امتیازی"	مهم
Microsoft Windows	CVE-2020-1303	آسیب‌پذیری به حملات "ترفیع امتیازی"	مهم

محصول	CVE شناسه	ملاحظات	سطح حساسیت
Microsoft Windows	CVE-2020-1252	آسیب‌پذیری به حملات "اجرای کد به‌صورت از راه دور"	حیاتی
Microsoft Windows	CVE-2020-1559	آسیب‌پذیری به حملات "ترفیع امتیازی"	مهم
Microsoft Windows	CVE-2020-1507	آسیب‌پذیری به حملات "ترفیع امتیازی"	مهم
Microsoft Windows	CVE-2020-1508	آسیب‌پذیری به حملات "اجرای کد به‌صورت از راه دور"	حیاتی
Microsoft Windows	CVE-2020-0914	آسیب‌پذیری به حملات "نشت اطلاعات"	مهم
Microsoft Windows	CVE-2020-0886	آسیب‌پذیری به حملات "ترفیع امتیازی"	مهم
Microsoft Windows	CVE-2020-0989	آسیب‌پذیری به حملات "نشت اطلاعات"	مهم
Microsoft Windows	CVE-2020-0875	آسیب‌پذیری به حملات "نشت اطلاعات"	مهم
Microsoft Windows	CVE-2020-0912	آسیب‌پذیری به حملات "ترفیع امتیازی"	مهم
Microsoft Windows	CVE-2020-1038	آسیب‌پذیری به حملات "از کاراندازی سرویس" (Denial of Service)	مهم
Microsoft Windows	CVE-2020-0908	آسیب‌پذیری به حملات "اجرای کد به‌صورت از راه دور"	حیاتی
Microsoft Windows	CVE-2020-1052	آسیب‌پذیری به حملات "ترفیع امتیازی"	مهم
Microsoft Windows	CVE-2020-0911	آسیب‌پذیری به حملات "ترفیع امتیازی"	مهم
Microsoft Windows	CVE-2020-0805	آسیب‌پذیری به حملات "عبور از سد تنظیمات امنیتی"	مهم
Microsoft Windows	CVE-2020-1119	آسیب‌پذیری به حملات "نشت اطلاعات"	مهم
Microsoft Windows	CVE-2020-1146	آسیب‌پذیری به حملات "ترفیع امتیازی"	مهم
Microsoft Windows	CVE-2020-0951	آسیب‌پذیری به حملات "عبور از سد تنظیمات امنیتی"	مهم
Microsoft Windows	CVE-2020-1122	آسیب‌پذیری به حملات "ترفیع امتیازی"	مهم
Microsoft Windows	CVE-2020-1098	آسیب‌پذیری به حملات "ترفیع امتیازی"	مهم

محصول	CVE شناسه	ملاحظات	سطح حساسیت
Microsoft Windows Codecs Library	CVE-2020-1319	آسیب‌پذیری به حملات "اجرای کد به‌صورت از راه دور"	حیاتی
Microsoft Windows Codecs Library	CVE-2020-0997	آسیب‌پذیری به حملات "اجرای کد به‌صورت از راه دور"	حیاتی
Microsoft Windows Codecs Library	CVE-2020-1129	آسیب‌پذیری به حملات "اجرای کد به‌صورت از راه دور"	حیاتی
Microsoft Windows DNS	CVE-2020-0839	آسیب‌پذیری به حملات "ترفیع امتیازی"	مهم
Microsoft Windows DNS	CVE-2020-1228	آسیب‌پذیری به حملات "از کاراندازی سرویس"	مهم
Microsoft Windows DNS	CVE-2020-0836	آسیب‌پذیری به حملات "از کاراندازی سرویس"	مهم
Open Source Software	CVE-2020-16873	آسیب‌پذیری به حملات "جعل"	مهم
SQL Server	CVE-2020-1044	آسیب‌پذیری به حملات "عبور از سد تنظیمات امنیتی"	متوسط
Visual Studio	CVE-2020-16874	آسیب‌پذیری به حملات "اجرای کد به‌صورت از راه دور"	حیاتی
Visual Studio	CVE-2020-16856	آسیب‌پذیری به حملات "اجرای کد به‌صورت از راه دور"	مهم
Visual Studio	CVE-2020-16881	آسیب‌پذیری به حملات "اجرای کد به‌صورت از راه دور"	مهم
Windows DHCP Server	CVE-2020-1031	آسیب‌پذیری به حملات "نشت اطلاعات"	مهم
Windows Diagnostic Hub	CVE-2020-1130	آسیب‌پذیری به حملات "ترفیع امتیازی"	مهم
Windows Diagnostic Hub	CVE-2020-1133	آسیب‌پذیری به حملات "ترفیع امتیازی"	مهم
Windows Hyper-V	CVE-2020-0904	آسیب‌پذیری به حملات "ترفیع امتیازی"	مهم
Windows Hyper-V	CVE-2020-0890	آسیب‌پذیری به حملات "از کاراندازی سرویس"	مهم
Windows Kernel	CVE-2020-0941	آسیب‌پذیری به حملات "نشت اطلاعات"	مهم
Windows Kernel	CVE-2020-0928	آسیب‌پذیری به حملات "نشت اطلاعات"	مهم
Windows Kernel	CVE-2020-16854	آسیب‌پذیری به حملات "نشت اطلاعات"	مهم

محصول	CVE شناسه	ملاحظات	سطح حساسیت
Windows Kernel	CVE-2020-1034	آسیب‌پذیری به حملات "ترفیع امتیازی"	مهم
Windows Kernel	CVE-2020-1033	آسیب‌پذیری به حملات "نشت اطلاعات"	مهم
Windows Kernel	CVE-2020-1589	آسیب‌پذیری به حملات "نشت اطلاعات"	مهم
Windows Kernel	CVE-2020-1592	آسیب‌پذیری به حملات "نشت اطلاعات"	حیاتی
Windows Print Spooler Components	CVE-2020-1030	آسیب‌پذیری به حملات "ترفیع امتیازی"	حیاتی
Windows Shell	CVE-2020-0870	آسیب‌پذیری به حملات "ترفیع امتیازی"	حیاتی

اصلاحیه‌های عرضه شده
در شهریور ۱۳۹۹



در شهریور ۱۳۹۹، شرکت‌های گوگل، موزیلا، سیسکو، مایکروسافت، ادوبی و مک‌آفی و بنیاد دروپل برای برخی محصولات خود اصلاحیه و توصیه‌نامه امنیتی منتشر کردند.

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 ۱۸ شهریور انتشار یافت ۸۵.۰.۴۱۸۳.۱۰۲ است. فهرست اشکالات مرتفع شده در لینک‌های زیر قابل دریافت و مشاهده است.

- https://chromereleases.googleblog.com/2020/08/stable-channel-update-for-desktop_25.html
- https://chromereleases.googleblog.com/2020/09/stable-channel-update-for-desktop.html

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/mfsa2020-36/
- https://www.mozilla.org/en-US/security/advisories/mfsa2020-40/
- https://www.mozilla.org/en-US/security/advisories/mfsa2020-41/

سیسکو هم در شهریور ماه در چندین نوبت با انتشار اصلاحیه، در مجموع ۳۳ آسیب‌پذیری امنیتی را در محصولات مختلف خود ترمیم کرد. درجه اهمیت ۱ مورد از این آسیب‌پذیری‌ها، "حیاتی" (Critical) و ۲۰ 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)، "ترفیع امتیازی" (Privilege Escalation) 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

۱۸ شهریور، شرکت مایکروسافت اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی سپتامبر منتشر کرد. این اصلاحیه‌ها در مجموع، بیش از ۱۲۰ آسیب‌پذیری را در سیستم‌عامل Windows و برخی محصولات دیگر این شرکت ترمیم می‌کنند. درجه حساسیت ۲۳ مورد از آسیب‌پذیری‌های ترمیم شده "حیاتی" و باقی آنها "مهم" (Important) گزارش شده است. جزییات کامل اصلاحیه‌های عرضه شده در لینک زیر قابل دریافت است.

- https://newsroom.shabakeh.net/21741

در شهریور ماه، شرکت ادوبی اقدام به عرضه به‌روزرسانی برای محصولات Experience Manager ،InDesign، Framemaker و Media Encoder کرد. بهره‌جویی از برخی از آسیب‌پذیری‌های ترمیم شده توسط به‌روزرسانی‌های مذکور مهاجم را قادر به در اختیار گرفتن دستگاه می‌کند. اطلاعات بیشتر در لینک‌های زیر قابل مطالعه است.

- https://helpx.adobe.com/security/products/indesign/apsb20-52.html
- https://helpx.adobe.com/security/products/framemaker/apsb20-54.html
- https://helpx.adobe.com/security/products/experience-manager/apsb20-56.html
- https://helpx.adobe.com/security/products/media-encoder/apsb20-57.html

در شهریور ماه، بنیاد دروپل در دو نوبت باگ‌هایی را در برخی از نسخه‌های Drupal اصلاح کرد که بهره‌جویی از برخی از آنها، موجب افشای داده‌های بالقوه حساس می‌شود. توضیحات کامل در این خصوص در لینک های زیر قابل دسترس است.

- https://www.drupal.org/sa-core-2020-007
- https://www.drupal.org/sa-core-2020-008
- https://www.drupal.org/sa-core-2020-009
- https://www.drupal.org/sa-core-2020-010
- https://www.drupal.org/sa-core-2020-011

در ۲۷ شهریور، شرکت اپل با انتشار به‌روزرسانی، ضعف‌هایی امنیتی را در سیستم‌های عامل tvOS، watchOS، iOS و iPadOS و نرم‌افزارهای Safari و Xcode کرد که در لینک‌های زیر به تغییرات لحاظ شده در آنها پرداخته شده است:

- https://support.apple.com/en-us/HT211843
- https://support.apple.com/en-us/HT211844
- https://support.apple.com/en-us/HT211850
- https://support.apple.com/en-us/HT211845
- https://support.apple.com/en-us/HT211848

در شهریور ماه شرکت مک‌آفی به‌روزرسانی ۲۰۲۰ September نرم‌افزار McAfee Endpoint Security - به اختصار McAfee ENS - را با درجه حساسیت "حیاتی" (Critical) منتشر کرد. علاوه بر بهینه‌سازی برخی قابلیت‌ها در به‌روزرسانی ۲۰۲۰ September موارد زیر نیز در McAfee ENS 10.7 لحاظ شده است:

- افزوده شدن قابلیت موسوم به Observe Mode به بخش Threat Prevention On-Access Scanner نرم‌افزار McAfee ENS که در بسترهای آزمایشگاهی کاربرد خواهد داشت.
- افزوده شدن تنظیمی که فعال‌سازی آن موجب مجاز تلقی شدن دریافت فایل‌های با درجه سبز (Green Rating) از نشانی‌های URL بررسی نشده (Unverified) خواهد شد.
- افزوده شدن قاعده‌ای در بخش Access Protection که فعال‌سازی آن از مورد دست‌درازی قرار گرفتن فایل‌های ذخیره شده در پوشه سوابق McAfee ENS بر روی دستگاه جلوگیری خواهد کرد.
- مجهز شدن بخش Credential Theft Protection به تنظیمات جدید؛ وظیفه Credential Theft Protection حفاظت از دستگاه از گزند حملات مبتنی بر LSASS است.
- سازگاری با نسخه 20H2 سیستم‌های عامل مایکروسافت که قرار است در ماه میلادی آینده عرضه شوند.

جزییات بیشتر در خصوص به‌روزرسانی مذکور در لینک زیر قابل دریافت است.

- https://docs.mcafee.com/bundle/endpoint-security-v10-7-x-sep-2020-update-release-notes/resource/prod-endpoint-security-v10-7-x-release-notes.pdf

همچنین مک‌آفی نسخه ۵.۶.۶ نرم‌افزار McAfee Agent را نیز عرضه کرده که در آن دو آسیب پذیری "ترفیع امتیازی"، یک ضعف امنیتی "دست‌درازی به ترتیب جستجوی(DLL Search Order Hijacking) "DLL و یک باگ "تزریق(DLL Injection) "DLL ترمیم و اصلاح شده است. در نسخه جدید از نگارش ۸.۳ سیستم عامل Red Hat Enterprise Linux نیز پشتیبانی می‌شود. اطلاعات بیشتر در لینک زیر قابل مطالعه است:

- https://kc.mcafee.com/corporate/index?page=content&id=KB51573

در ششمین ماه از سال ۱۳۹۹ شرکت بیت دیفندر اقدام به انتشار نسخ ۶.۶.۲۰.۲۹۴، ۶.۲.۲۱.۹۷ و ۴.۱۳.۸۶.۲۰۰۰۸۶ 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-6-6-20-294-release-notes-(windows)-2616.html
- https://www.bitdefender.com/support/bitdefender-endpoint-security-tools-version-6-2-21-97-release-notes-(linux)-2617.html
- https://www.bitdefender.com/support/endpoint-security-for-mac-version-4-13-86-200086-release-notes-2613.html

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

گزارش فصلی مک‌آفی
منتشر شد

گزارش فصلی مک‌آفی منتشر شد.

سال ۲۰۲۰ در حالی آغاز شد که بحران همه‌گیری ویروس کووید-۱۹ و ترس عمومی از آن، کاربران نگران و جویای کسب اطلاعات در خصوص این بیماری را به هدفی آسیب‌پذیر برای تبهکاران سایبری و گردانندگان حملات فیشینگ تبدیل کرد.

در این گزارش اختصاصی، شرکت امنیتی مک‌آفی با نگاهی عمیق به بررسی تهدیدات مرتبط با کووید-۱۹ پرداخته است.

سوءاستفاده مهاجمان سایبری از همه‌گیری کووید-۱۹ برای هدف قرار دادن کارکنانی که به دلیل شیوع این ویروس از منزل و خارج از محدوده امن سازمان به دورکاری می پردازند از همان ابتدا دور از انتظار نبود. فراهم کردن بستری امن در زمانی که سازمان‌ها به‌صورت اضطراری و فوری ناچار شدند تا بدون تجربه قبلی اقدام به دورکار کردن عده زیادی از کارکنان خود کنند چالشی جدی برای مراکز عملیات امنیتی (SOC) و مدیران ارشد فناوری (CTO) بود.

در این دوران فراهم شدن امکان مشارکت و تأمین سیستم‌هایی کارا مستلزم اعتماد به کارکنان برای رسیدگی به کارهایشان در بستر اینترنت است. از سویی دیگر نگرانی از تغییر روال‌ها، رسیدگی به نیازهای جدید خانواده در دوران قرنطینه، لزوم حفظ فاصله‌گذاری اجتماعی، وسایل بهداشتی و حفاظتی مورد نیاز، کمبودها و در عین حال افزایش نیازها، بیکاری روز افزون و حذف برخی مزایا بسیاری را در معرض فشارهای روانی و استرس قرار داده است. در این برهه از زمان، تبهکاران سایبری نیروهای انسانی دورکار، پریشان و آسیب‌پذیر را هدف و ابزاری عالی برای رسیدن به اهداف پلید خود دیدند.

مهاجمان با تکنیک‌های مهندسی اجتماعی و موضوعاتی مرتبط با کووید-۱۹، اقدام به ارسال هرزنامه‌های کلاهبرداری و راه‌اندازی سایت‌های با محتوای جعلی برای به دام انداختن کارکنان دورکار کردند. این افراد کوشیدند تا با سوءاستفاده از آسیب‌پذیری‌های ناشی از این همه‌گیری، کارکنان و به تبع آن سازمان را هدف انباره بدافزارهای خود قرار داده و به شبکه داخلی سازمان‌ها راه پیدا کنند.

از همان گزارش‌های اولیه در خصوص شیوع ویروس کرونا محققان مک‌آفی تاکتیک‌ها و تکنیک‌های مهاجمان سایبری را که از این بحران برای پیش‌برد اهداف پلید خود بهره می‌بردند مورد رصد قرار دادند.

در این گزارش ضمن کالبدشکافی برخی نمومونه‌ها از تلاش تبهکاران سایبری در سوءاستفاده از بحران کرونا، آمار تهدیدات سایبری در سه‌ماهه اول سال ۲۰۲۰ نیز مورد بررسی و تحلیل قرار گرفته است.


McAfee
گزارش و آمار فصلی از فعالیت
بدافزارها و تهدیدات سایبری
ویژه‌نامه کرونا
Top 10 Targeted Industry Sectors

افتای ریاست جمهوری با همکاری شبکه گستر

شبکه گستر

شرکت مهندسی شبکه گستر

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

ترمیم ۱۲۹ آسیب‌پذیری امنیتی توسط مجموعه اصلاحیه‌های ماه سپتامبر مایکروسافت

سه‌شنبه، ۱۸ شهریور، شرکت مایکروسافت اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی سپتامبر منتشر کرد. این اصلاحیه‌ها در مجموع، بیش از ۱۲۰ آسیب‌پذیری را در محصولات مختلف مایکروسافت 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