اردیبهشت

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 ۱۷

آسیب‌پذیری‌ها و اصلاحیه‌های امنیتی ۲۹

افتای ریاست جمهوری با همکاری شبکه گستر ۳۸

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 اردیبهشت ماه ۱۳۹۹ پرداخته شده است.

بر طبق آمار ارائه شده از سوی شرکت مک‌آفی، باج‌افزارهای Cuba، Odveta و VoidCrypt در صدر تهدیدات فعال قرار دارند. در اطلاعیه باج‌گیری Cuba اینطور اظهار می‌شود که اطلاعات قربانی قبل از رمزگذاری، سرقت شده و عدم پرداخت باج منجر به افشای آنها خواهد شد. انتشار داده‌ها در صورت عدم پرداخت، تهدیدی است که سال‌هاست گردانندگان باج‌افزار از آن حرف می‌زنند. در حالی که دسترسی مهاجم به فایل‌های قربانی به‌خصوص در حملات باج‌افزاری مبتنی بر RDP بر کسی پوشیده نیست، موانعی همچون زمانبر بودن انتقال اطلاعات در بستر اینترنت، همواره عامل جدی گرفته نشدن این چنین ادعاها و توخالی دانستن آنها توسط شرکت‌ها و متخصصان فعال در حوزه امنیت بوده است. حقیقت آن است که حملات باج‌افزاری هیچ گاه به‌عنوان حملاتی از نوع نشت اطلاعات در نظر گرفته نمی‌شده است. اما با واقعی شدن این ادعای قدیمی مهاجمان باج‌افزار زمان آن فرا رسیده که شرکت‌ها و به خصوص دست‌اندرکاران امنیت فناوری اطلاعات تجدید نظری در باورها و روال‌های خود داشته باشند. در بسیاری از موارد در میان فایل‌های رمزگذاری شده اطلاعات حساسی همچون اطلاعات کارکنان، مشتریان و شرکا که سازمان ملزم به حفاظت از آنهاست به چشم می‌خورد. با این رویکرد جدید باج‌گیران سایبری، منبعد قربانیان باج‌افزار، نه فقط دغدغه بازگرداندن اطلاعات رمزگذاری شده که نگرانی اعلام موضوع به مشتریان و شرکای تجاری خود را هم که الزام قانونی برخی کشورها در رخدادهای نشت اطلاعات است نیز خواهند داشت. در همین خصوص در این ماهنامه به اخاذی‌های ده‌ها میلیون دلاری گردانندگانREvil پرداخته شده است. گردانندگان REvil از جمله مهاجمانی هستند که اهداف خود را به‌صورت خاص انتخاب کرده و ضمن سرقت فایل‌ها و داده‌ها، در صورت پرداخت نشدن مبلغ اخاذی‌شده اقدام به افشای آنها می‌کنند. همچنین در این ماهنامه حملات اخیر باج‌افزارهای Snake و LockBit مورد بررسی قرار گرفته است.

در ماهی که گذشت شرکت مایکروسافت از اجرای کارزاری فیشنگ خبر داد که در آن با سوءاستفاده از بحران همه‌گیری ویروس کووید ۱۹، نرم‌افزار NetSupport Manager بر روی دستگاه قربانیان نصب می‌شود. در این کارزار از طریق ایمیل‌هایی که در ظاهر از سوی مرکز جانز هاپکینز در خصوص آمار مرگ ناشی از ویروس کووید ۱۹ ارسال شده‌اند کاربر تشویق به اجرای فایل Excel پیوست می‌شود.

در اردیبهشت ۱۳۹۹، شرکت‌های مایکروسافت، گوگل، جونیپر نت‌ورکز، وی‌اِم‌وِر، ادوبی، سیسکو و موزیلا، پروژه اوپن‌اس‌اس‌ال، گروه سامبا و بنیاد وردپرس اقدام به انتشار اصلاحیه و توصیه‌نامه امنیتی برای برخی از محصولات خود کردند که جزییات آنها در این ماهنامه قابل مطالعه 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 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.

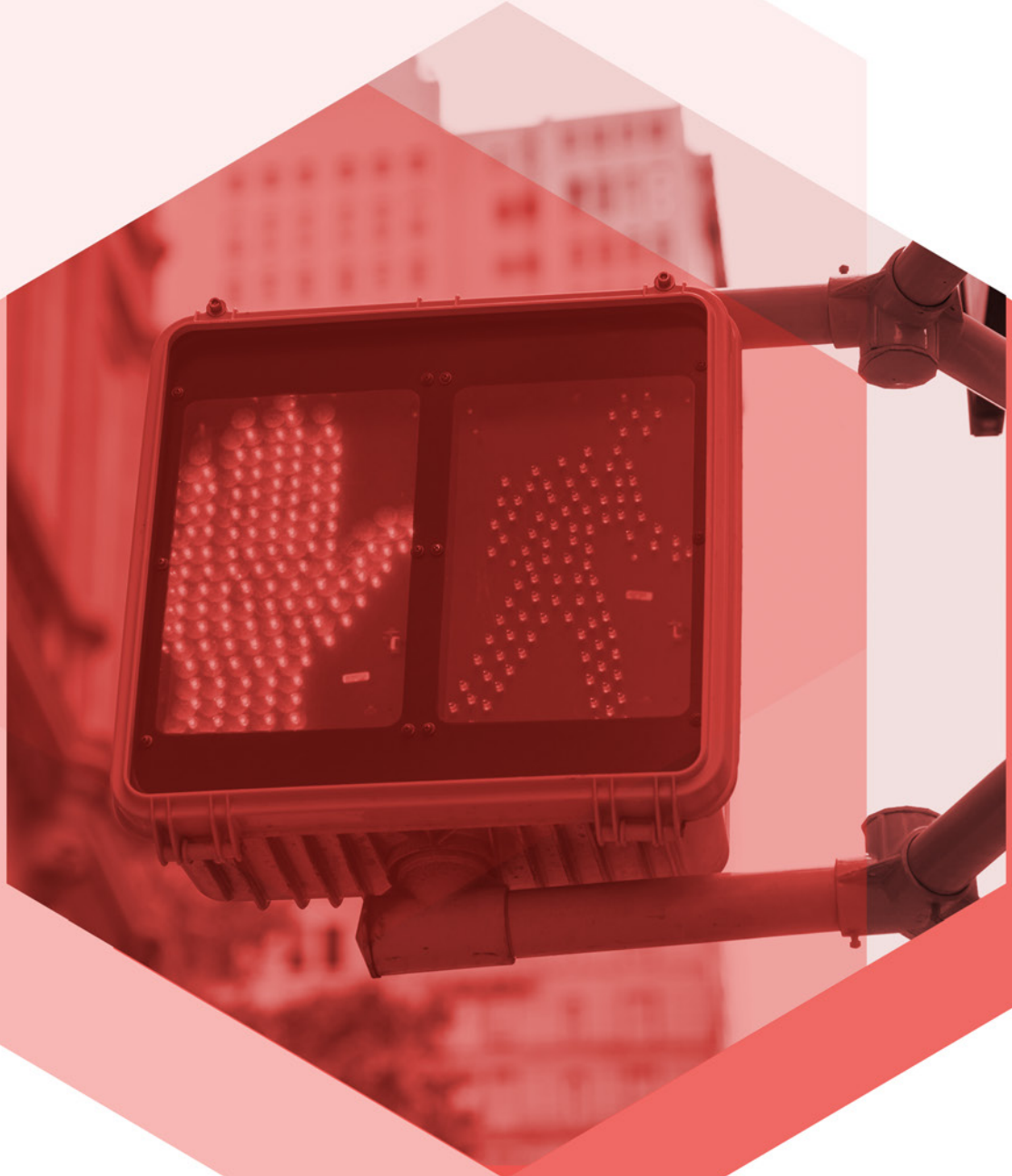
بسته بهره‌جو	توضیحات
IQY	گونه جدیدی از باج افزار Paradise که در قالب ایمیل های فیشینگ هدفمند با پیوست فایل IQY به سیستم قربانیان راه می یابد. در این حملات از فایل های IQY یا Internet Query برای فراخوانی پروسه معتبر PowerShell و اجرای کد مخرب استفاده می شود. این باج افزار از اجرا بر روی سیستم هایی که 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



LockBit؛ باج‌افزاری
با عملکرد انتشار خودکار در سطح شبکه

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.

LockBit که ظهور آن به سپتامبر ۲۰۱۹ 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.

به گزارش شرکت مهندسی شبکه گستر، در RaaS، صاحب باج‌افزار، فایل مخرب را به‌عنوان یک خدمت به متقاضی اجاره می‌دهد. متقاضی که ممکن است در برنامه‌نویسی تخصصی نداشته باشد تنها وظیفه انتشار باج‌افزار را بر عهده دارد. در نهایت بخشی از مبلغ اخاذی شده از قربانی به متقاضی و بخشی دیگر به نویسنده می‌رسد.

در LockBit معمولاً ۲۵ تا ۴۰ درصد از مبلغ اخاذی شده به گردانندگان باج‌افزار و باقی آن به توزیع‌کننده می‌رسد.

بر اساس گزارشی که شرکت امنیتی مک‌آفی آن را منتشر کرده در یکی از نمونه‌های جدید، مهاجمان توانسته‌اند که در مدتی کوتاه تقریباً ۲۵ سرور و ۲۲۵ ایستگاه کاری یک سازمان را به باج‌افزار LockBit آلوده کنند.

نکته قابل توجه اینکه برای آلوده‌سازی کلیه این سیستم‌ها و رمزگذاری فایل‌های آنها تنها سه ساعت صرف شده است.

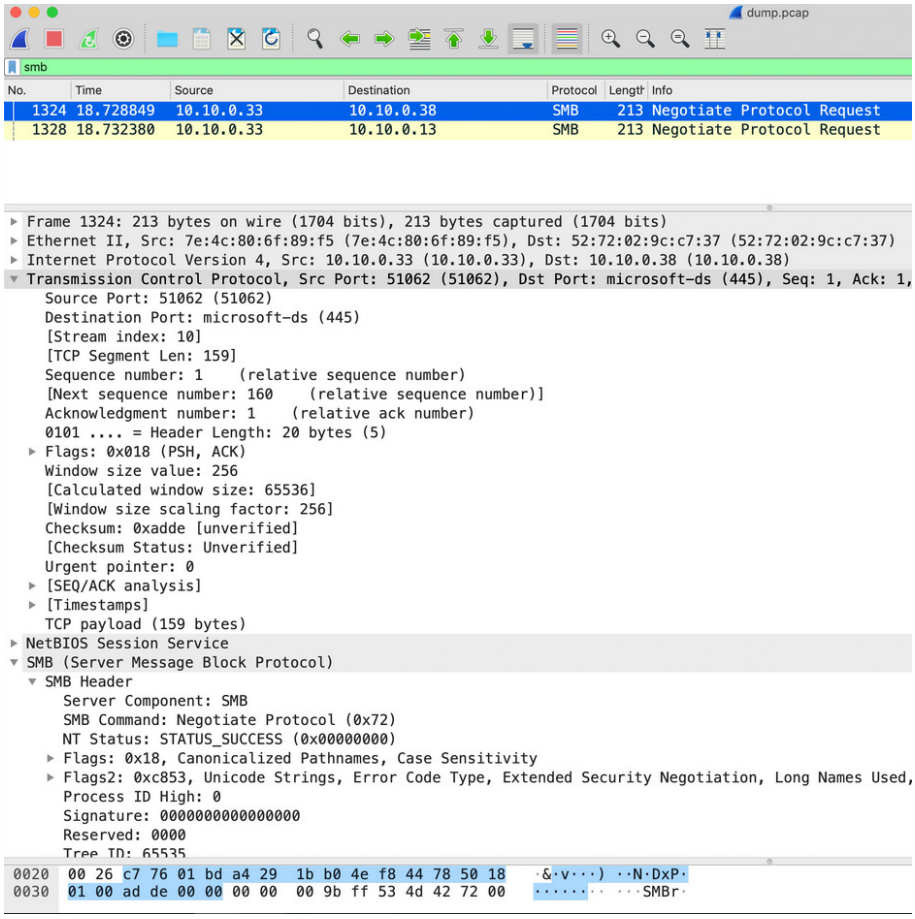
این مهاجمان برای رخنه به شبکه قربانی اقدام به اجرای حملات موسوم به "سعی‌وخطا" (Brute-force) بر ضد یک سرویس از رده خارج VPN کرده بودند.

بر خلاف اکثر حملات سایبری که در آنها هکرها پس از نفوذ به شبکه در پی کشف اطلاعات اصالت‌سنجی حداقل یک کاربر با سطح دسترسی Administrator می‌روند، در این حمله به دلیل دستیابی به اطلاعات مذکور در نتیجه اجرای حمله اولیه "سعی‌وخطا"، به‌محض ورود مهاجمان به شبکه، LockBit آماده توزیع انبوه بوده است.

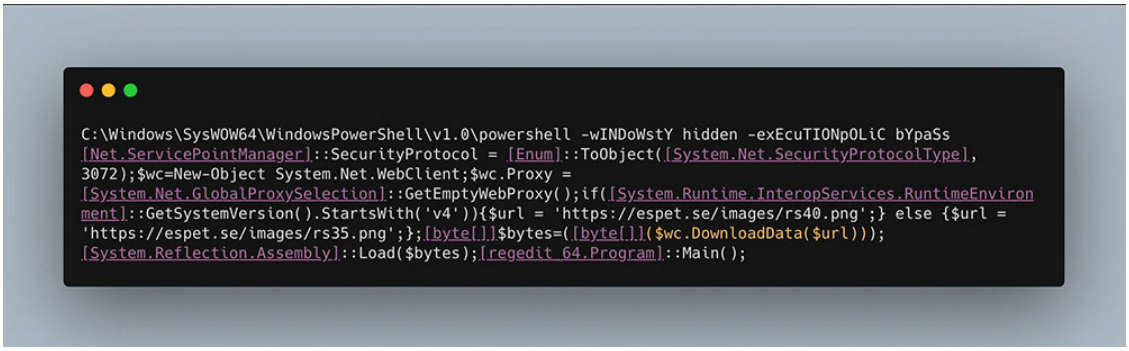
بر طبق این گزارش، مهاجمان پس از نفوذ به اولین سیستم سازمان در ساعت ۱ بامداد بلافاصله اقدام به اجرای LockBit که مجهز به حساب کاربری Administrator بود کرده و در ساعت حدود ساعت ۴ بامداد در حالی که اکثر سیستم‌ها به باج‌افزار آلوده شده بودند از شبکه خارج شدند.

تحلیل‌های مک‌آفی نشان می‌دهد که باج‌افزار LockBit دارای قابلیتی است که امکان انتشار خودکار خود بر روی سایر سیستم‌های شبکه را فراهم می‌کند.

LockBit زمانی که اجرا می‌شود علاوه بر رمزگذاری فایل‌های دستگاه، از طریق درخواست‌های ARP اقدام به شناسایی سایر دستگاه‌های شبکه کرده و در ادامه تلاش می‌کند تا در بستر پودمان SMB به آنها متصل شود.



با اتصال به کامپیوتر مقصد، یک فرمان PowerShell اجرا شده و باج‌افزار بر روی آن دستگاه نیز توسط یک اجراکننده مبتنی بر .NET فعال می‌شود.



در این صورت هر چه کامپیوترهای بیشتری در سطح شبکه آلوده می‌شوند فرایند توزیع باج‌افزار بر روی سایر سیستم‌های شبکه تسریع می‌شود.

در مقایسه با سایر حملاتی که در جریان آنها تعداد انبوهی از سیستم‌ها به باج‌افزار آلوده می‌شوند در این مورد بخصوص مهاجمان تنها برای مدت کوتاهی در سطح شبکه فعالیت داشتند. این در حالی است که در نمونه‌های معمول مهاجمان برای روزها و یا حتی هفته‌ها پیش از توزیع انبوه باج‌افزار و برای آماده‌سازی بستر در شبکه حضور دارند.

واقعیت آن است که حضور طولانی مدت مهاجم در شبکه احتمال اطلاع سازمان پیش از وقوع اتفاقات مخربی همچنین توزیع فراگیر باج‌افزار را نیز افزایش می‌دهد. حال آنکه با این عملکرد LockBit حتی مهاجمان غیرحرفه‌ای نیز می‌توانند در مدتی بسیار کوتاه سیستم‌های شبکه‌های بزرگ را به این باج‌افزار آلوده کنند.

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

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

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/tales-from-the-trenches-a-lockbit-ransomware-/story

حضور پررنگ‌تر
باج‌افزار Snake

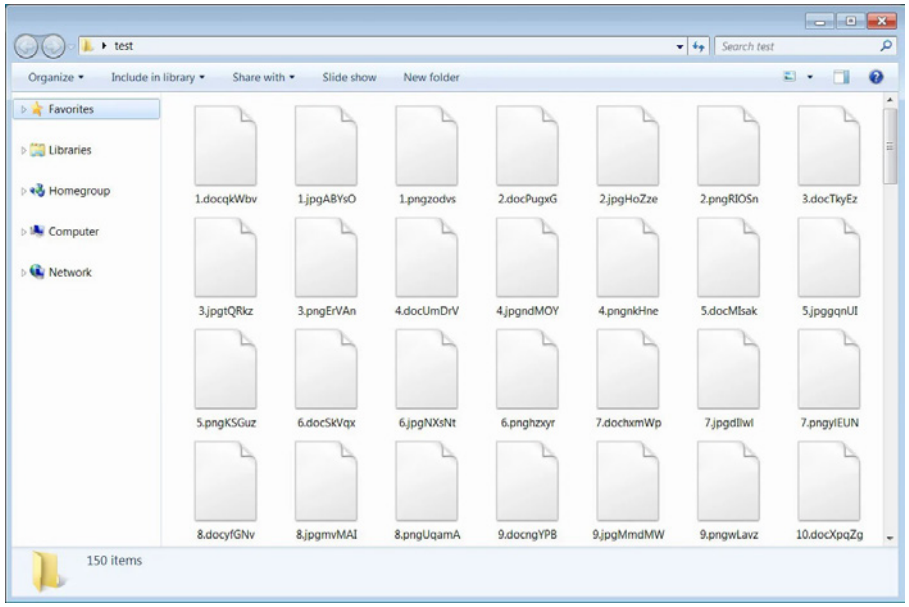
در روزهای اخیر، فعالیت Snake، در مقایسه با چند ماه گذشته به‌شدت افزایش یافته و سازمان‌ها در کشورهای مختلف هدف این باج‌افزار قرار گرفته‌اند.

Snake از جمله باج‌افزارهایی است که سازمان‌های بزرگ را به‌صورت کاملاً هدفمند مورد حمله قرار می‌دهد.

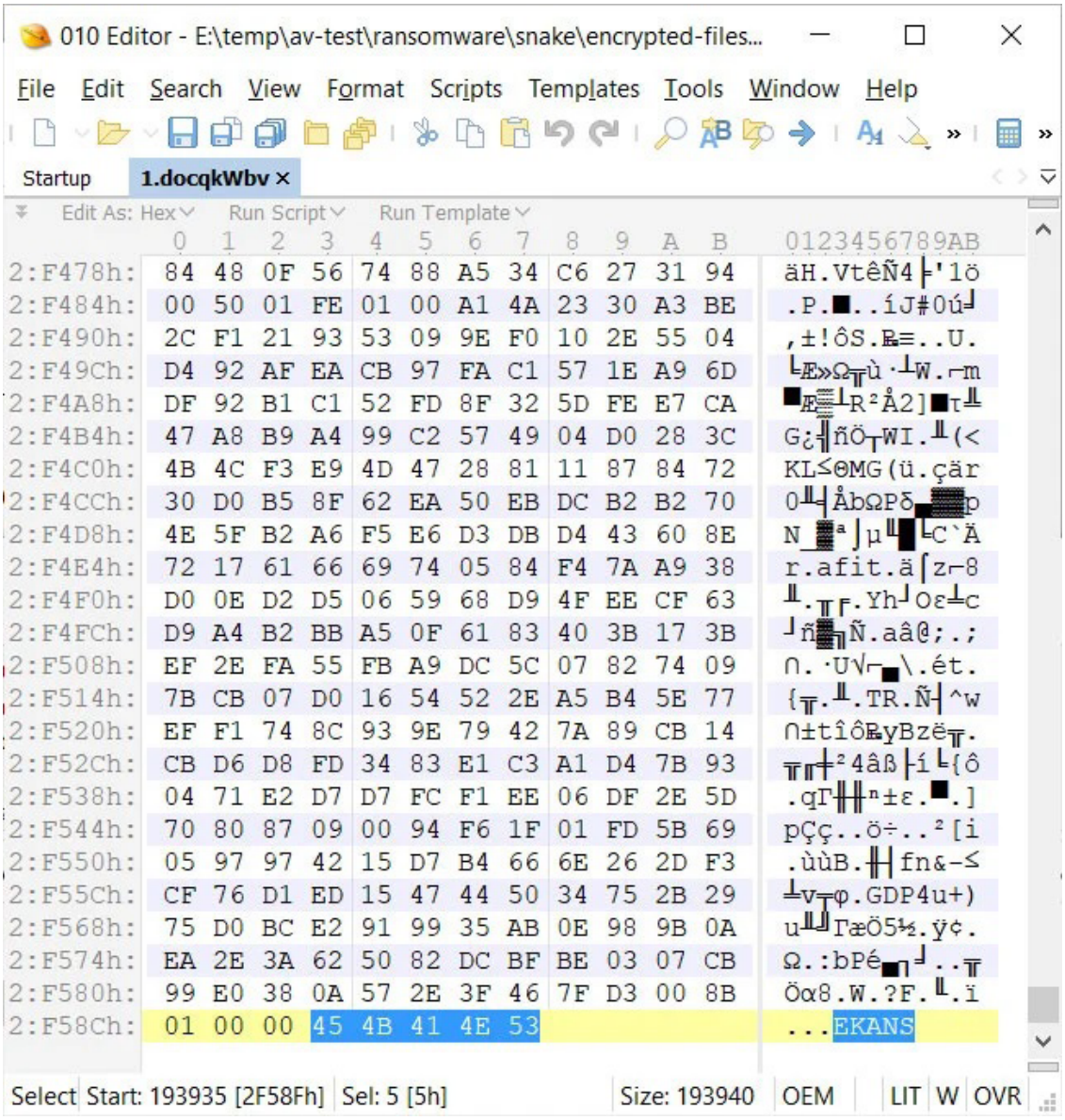
شرکت فرزنیوس، از بزرگ‌ترین تأمین‌کنندگان تجهیزات پزشکی و ارائه‌دهنده خدمات بیمارستانی در اروپا یکی از جدیدترین قربانیان این باج‌افزار است. فرزنیوس اعلام کرده که در پی این رخداد باج‌افزاری فعالیت برخی بخش‌های این شرکت محدود شده اما امور مربوط به مراقبت از بیماران در جریان است.

به گزارش شرکت مهندسی شبکه گستر، Snake که اولین بار در ماه ژانویه سال میلادی جاری شناسایی شد طی چند ماه قبل فعالیت نسبتاً محدودی داشت. اما از اواسط هفته گذشته دامنه حملات آن به‌طور بسیار چشمگیری افزایش یافته است.

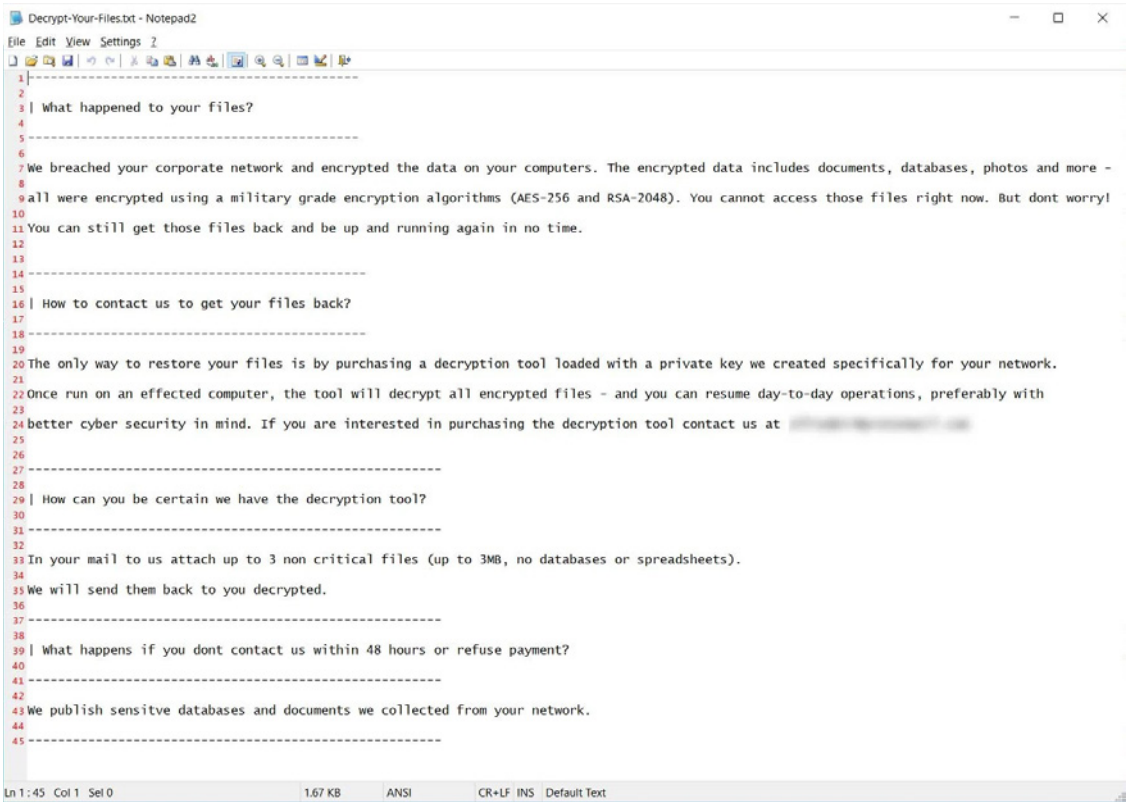
Snake پس از رمزگذاری فایل، پسوند docqkWbv را به آن الصاق می‌کند.



کلمه EKANS نیز به انتهای کد فایل افزوده می‌شود.



بتازگی گردانندگان Snake مدعی شده‌اند که فایل‌های قربانی را پیش از رمزگذاری سرقت می‌کنند. در اطلاعیه باج‌گیری (Ransom Note) نمونه‌های اخیر این باج‌افزار تهدید می‌شود که در صورتی که قربانی ظرف ۴۸ ساعت اقدام به پرداخت باج نکند بانک‌های داده‌ها و اسناد سرقت شده افشا می‌شوند.



سرقت اطلاعات و تهدید به انتشار عمومی آنها در صورت عدم پرداخت مبلغ اخاذی شده در حال تبدیل شدن به یک الگو در میان مهاجمان سایبری است. اگر چه هنوز نمی‌توان با اطمینان گفت که این ادعای گردانندگان Snake تهدیدی واقعی است یا صرفاً بلوفی برای متقاعد کردن قربانی به پرداخت باج است. معمولاً در اینگونه موارد برای اثبات ادعا، مهاجمان اقدام به انتشار بخشی از اطلاعات می‌کنند که در مورد Snake هنوز خبری در خصوص آن گزارش نشده است.

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

نمونه‌های مورد بررسی در این خبر با نام‌های زیر قابل شناسایی هستند:

Bitdefender:

- Gen:Trojan.AV-Killer.ItW@aeiѺGqj

McAfee:

- Trojan-Ransom.b

Sophos:

- Troj/Ransom-FUJ

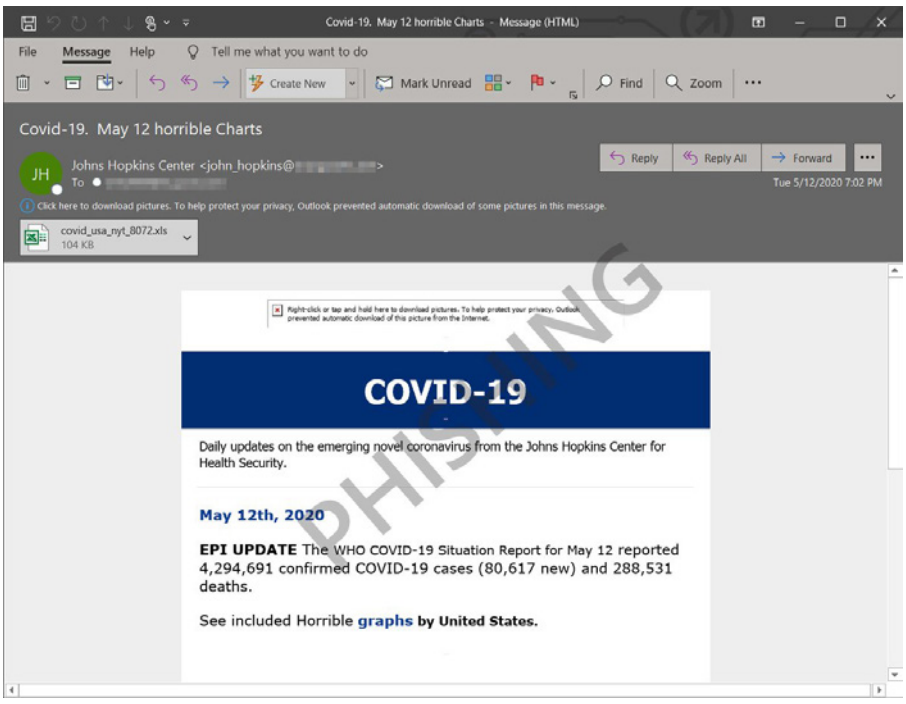
فیشینگ گسترده

برای انتشار ابزاری معتبر

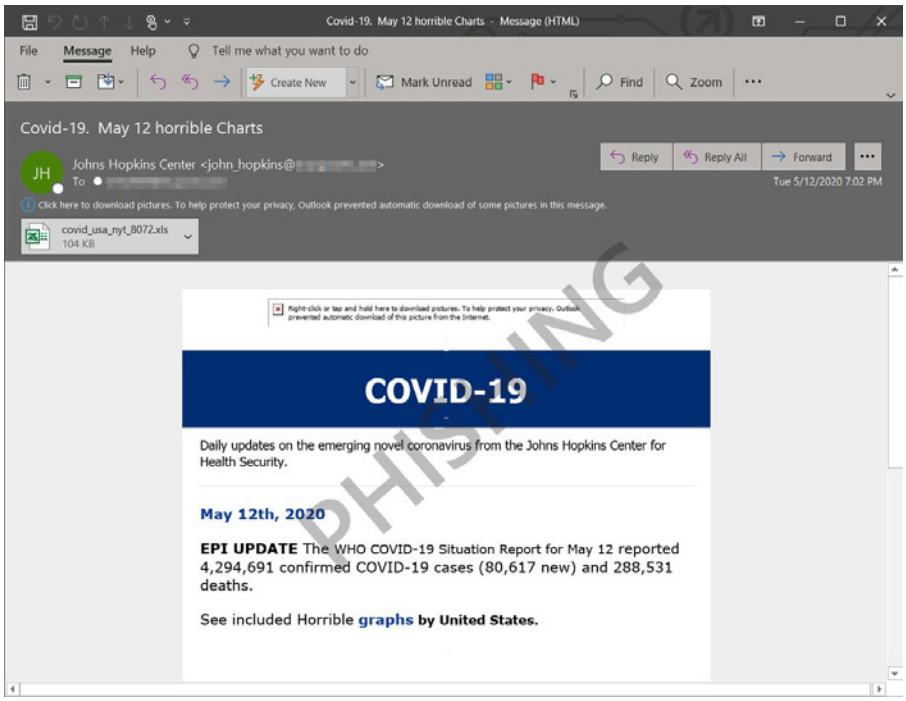
مایکروسافت از اجرای کارزاری فیشنگ خبر داده که در آن با سوءاستفاده از بحران همه‌گیری ویروس کووید ۱۹، نرم‌افزار NetSupport Manager بر روی دستگاه قربانیان نصب می‌شود.

NetSupport Manager یک ابزار معتبر دسترسی از راه دور است.

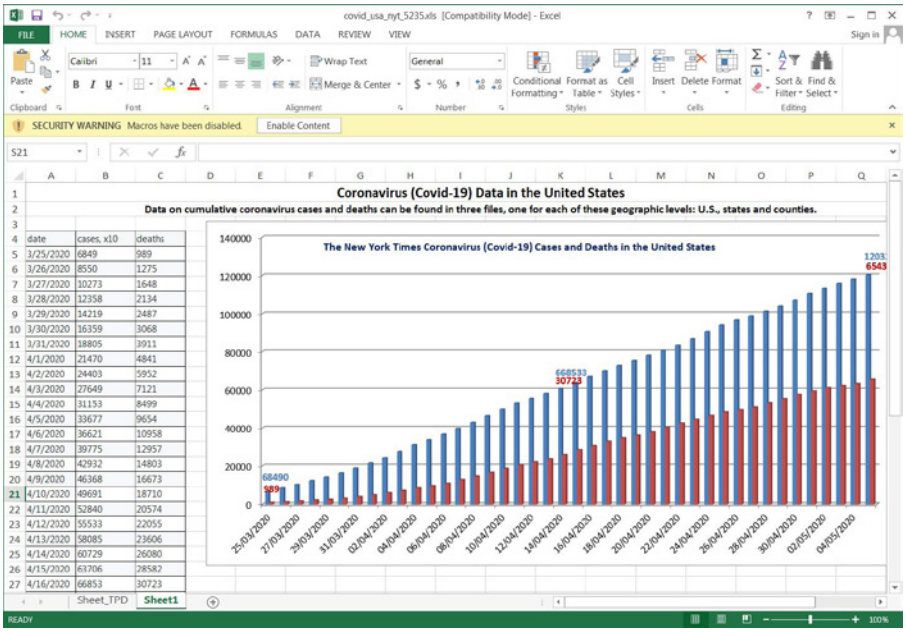
در این کارزار از طریق ایمیل‌هایی که در ظاهر از سوی مرکز جانز هاپکینز در خصوص آمار مرگ ناشی از ویروس کووید ۱۹ ارسال شده‌اند کاربر تشویق به اجرای فایل Excel پیوست می‌شود.



به گزارش شرکت مهندسی شبکه گستر، با اجرای پیوست که فایلی با نام covid_usa_nyt_8072.xls است کاربر با نموداری مشابه با تصویر زیر روبرو می‌شود.



به گزارش شرکت مهندسی شبکه گستر، با اجرای پیوست که فایلی با نام covid_usa_nyt_8072.xls است کاربر با نموداری مشابه با تصویر زیر روبرو می‌شود.

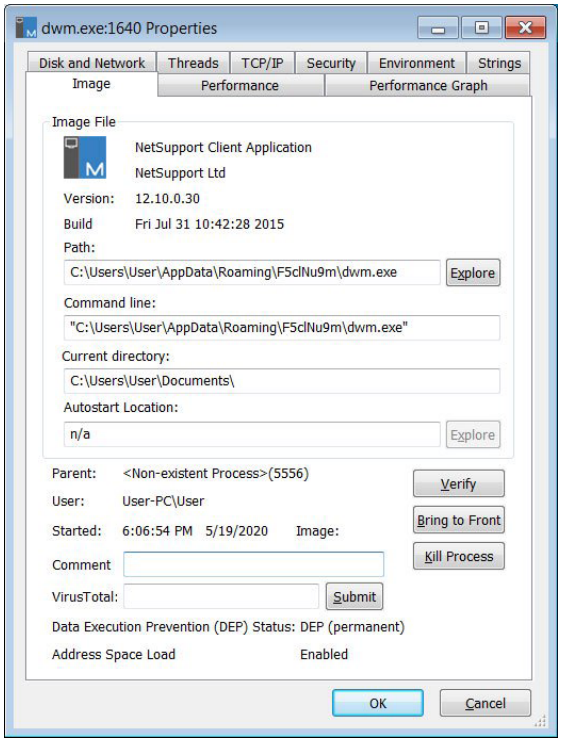


فایل مذکور حاوی ماکروهای مخربی است که در صورتی که کاربر بر روی دگمه Enable Content کلیک کند کدهای آنها اجرا شده و نرم‌افزار NetSupport Manager دریافت و بر روی دستگاه قربانی نصب می‌شود.

به گفته مایکروسافت صدها فایل منحصربه‌فرد Excel در این کارزار مورد استفاده قرار گرفته و همگی آنها به شدت مبهم‌سازی (Obfuscation) شده‌اند. با این حال در همه نمونه ها ماکروهای استفاده شده به یک نشانی URL یکسان متصل می‌شوند.

با نصب NetSupport Manager دسترسی کامل به دستگاه به‌صورت از راه دور برای مهاجمان فراهم می‌شود.

در این حمله خاص، NetSupport Manager با نام dwm.exe در پوشه‌ای با نام تصادفی در مسیر ٪AppData٪ ذخیره می‌شود.



این مهاجمان مدتی پس از اجرای ابزار مذکور، برنامه‌های مخرب مورد نظر خود را در قالب فایل‌های dll، ini و exe و اسکریپت‌های VBScript و PowerShell بر روی دستگاه قربانی اجرا می‌کنند.

مایکروسافت اعلام کرده که قربانیان این حملات باید سرقت شدن داده‌هایی همچون اطلاعات اصالت‌سنجی را نیز محتمل بدانند.

لذا پس از پاکسازی دستگاه‌های آلوده، باید رمزهای عبور تغییر یافته و سایر سیستم‌های شبکه نیز مورد بررسی قرار بگیرد.

علاوه بر استفاده از ضدویروس و ضدهرزنامه قدرتمند و به‌روز و همچنین پیکربندی صحیح تنظیمات ماکرو، 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.

اخاذی‌های ده‌ها میلیون دلاری

باج‌افزار REvil

گردانندگان باج‌افزار REvil مدعی هستند اطلاعاتی را در اختیار دارند که افشای آنها می‌تواند لطمه‌ای جدی به میزان استقبال رأی‌دهندگان از دونالد ترامپ در انتخابات بعدی ریاست جمهوری آمریکا وارد کند. همچنین این گروه قصد دارد تا داده‌های مربوط به مدونا را نیز در یک حراج به فروش بگذارد.

گردانندگان REvil از جمله مهاجمانی هستند که اهداف خود را به‌صورت خاص انتخاب کرده و ضمن سرقت فایل‌ها و داده‌ها، در صورت پرداخت نشدن مبلغ اخاذی‌شده اقدام به افشای آنها می‌کنند. ۲۱ فروردین روزنامه وال‌استریت جورنال گزارش کرد که شرکت تراولکس که شبکه آن آلوده به باج‌افزار REvil شده بود به‌منظور بازگرداندن سیستم‌ها به حالت اولیه اقدام به پرداخت باج ۲.۳ میلیون دلاری به این تبهکاران کرده است.

به گزارش شرکت مهندسی شبکه گستر، در یکی از جدیدترین موارد این مهاجمان با رخنه به شبکه شرکت حقوقی Grubman Shire Meiselas & Sacks - به اختصار GSMLaw - اقدام به سرقت اطلاعات ظاهراً بسیار باارزش قبل از رمزگذاری آنها کرده‌اند.

GSMLaw وکالت تعداد بسیار زیادی از افراد سرشناس را در کارنامه دارد.

این گروه در ابتدا مبلغ ۲۱ میلیون دلار را در ازای آنچه که این افراد آن را رمزگشایی فایل‌ها می‌خوانند از GSMLaw اخاذی کرد. در پی پرداخت نشدن باج ظرف ۱۰ روز، مهاجمان ضمن دو برابر کردن مبلغ، GSMLaw را تهدید به انتشار ۷۵۶ گیگابایت از داده‌های سرقت شده کردند.

با زیر بار نرفتن GSMLaw، مهاجمان REvil اقدام به انتشار ۲.۴ گیگابایت از اسناد مرتبط با لیدی گاگا (خواننده آمریکایی) کردند. در ادامه تهدید کردند که در صورت عدم پرداخت باج، اطلاعات دونالد ترامپ، رئیس جمهور آمریکا را که در جریان هک GSMLaw به دست این مهاجمان رسیده است منتشر خواهند کرد. اطلاعاتی که به گفته این گروه تأثیری منفی بر میزان محبوبیت ترامپ و انتخاب مجدد او در انتخابات آتی ریاست جمهوری آمریکا خواهد گذاشت.

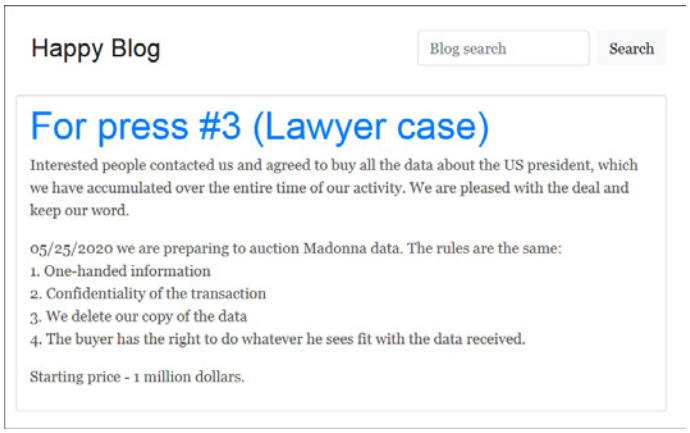
> The next person we'll be publishing is Donald Trump. There's an election race going on, and we found a ton of dirty laundry on time. Mr. Trump, if you want to stay president, poke a sharp stick at the guys, otherwise you may forget this ambition forever. And to you voters, we can let you know that after such a publication, you certainly don't want to see him as president. Well, let's leave out the details. The deadline is one week.
> Grubman, we will destroy your company to the ground if we don't see the money. Read the story of Travelex, it's very instructive. You repeating their scenario one to one.

با بی‌نتیجه ماندن تلاش مهاجمان در مستأصل کردن مدیران GSMLaw، بخشی از اطلاعات مرتبط با دونالد ترامپ، شامل ۱۶۰ ایمیل که به گفته این افراد در مقایسه با سایر اطلاعات بی‌ضرر محسوب می شود به اشتراک گذاشته شد.

بر طبق اعلام گردانندگان REvil اطلاعات اصلی در حراج‌های هفتگی به فروش گذاشته خواهد شد. این افراد قول داده‌اند که هیچ نسخه‌ای از داده‌ها را نزد خود نگاه نداشته و مدعی هستند که پس از پایان معامله این تنها خریدار است که رونوشت اطلاعات را در اختیار خواهد داشت.

> 1) We will auction customer data every week (by last name) on the information exchange.
> This data will be bought either by the stars themselves, or various media and blackmail them then, or simply kind people with good intentions. We do not care. The main thing is we will get the money.

در ادامه تهدید GSMLaw، گروه REvil خبر داده که قصد دارد تا با برگزاری یک مزایده، اطلاعات مربوط به مدونا، دیگر موکل این شرکت را با قیمت اولیه ۱ میلیون دلار به حراج بگذارد.



در عین حال GSMLaw حداقل تا زمان نگارش این خبر زیر بار پرداخت باج نرفته است.

مهاجمان باج‌افزار REvil گروهی با گرایش‌های به‌شدت مالی است.

باج‌افزار REvil با نام‌های Sodin و Sodinokibi نیز شناخته می‌شود. ۲۳ اردیبهشت ماه مرکز مدیریت راهبردی افتای ریاست جمهوری با همکاری شرکت مهندسی شبکه گستر در این گزارش به برخی قابلیت‌های جدید این باج‌افزار پرداخت.

انتشار داده‌های قربانی در صورت عدم پرداخت، تهدیدی است که سال‌هاست گردانندگان باج‌افزار از آن حرف می‌زنند. در حالی که دسترسی مهاجم به فایل‌های قربانی به‌خصوص در حملات باج‌افزاری مبتنی بر RDP بر کسی پوشیده نیست، موانعی همچون زمانبر بودن انتقال اطلاعات در بستر اینترنت، همواره عامل جدی گرفته نشدن این چنین ادعاها و توخالی دانستن آنها توسط شرکت‌ها و متخصصان فعال در حوزه امنیت بوده است.

اما به نظر می‌رسد که اقدامات اخیر مهاجمان باج‌افزارهایی همچون REvil همه چیز را تغییر داده است.

واقعیت آن است که حملات باج‌افزاری هیچ گاه به‌عنوان حملاتی از نوع نشت اطلاعات در نظر گرفته نمی‌شده است. اما با واقعی شدن این ادعای قدیمی مهاجمان باج‌افزار زمان آن فرا رسیده که شرکت‌ها و به خصوص دست‌اندرکاران امنیت فناوری اطلاعات تجدید نظری در باورها و روال‌های خود داشته باشد. در بسیاری از موارد در میان فایل‌های رمزگذاری شده اطلاعات حساسی همچون اطلاعات کارکنان، مشتریان و شرکا که سازمان ملزم به حفاظت از آنهاست به چشم می‌خورد. با این رویکرد جدید باج‌گیران سایبری، منبعد قربانیان باج‌افزار، نه فقط دغدغه بازگرداندن اطلاعات رمزگذاری شده که نگرانی اعلام موضوع به مشتریان و شرکای تجاری خود را هم که الزام قانونی برخی کشورها در رخدادهای نشت اطلاعات است نیز خواهند داشت.

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

آسیب‌پذیری‌ها و اصلاحیه‌های امنیتی

آسیب‌پذیری روز-صفر
در حدود ۳۰ ضدویروس معروف

تکنیک جدیدی در اجرای حملات سایبری کشف شده که سازوکار شناسایی بدافزار در محصولات چندین شرکت امنیتی را موردسوءاستفاده قرار می‌دهد.

گفته می‌شود ۲۸ محصول ضدویروس ساخت شرکت‌های معروفی همچون مک‌آفی، کسپرسکی، سیمانتک، ای‌ست، آویرا و بسیاری دیگر به باگ مورد سوءاستفاده توسط این تکنیک که اکنون جزییات آن نیز به‌صورت عمومی افشا شده آسیب‌پذیر هستند.

اگر چه بهره‌جویی (Exploit) از این باگ به‌صورت از راه دور (Remotely) قابل انجام نیست اما سوءاستفاده از آن می‌تواند بدافزار (یا مهاجم) را قادر به حذف فایل‌هایی کند که در حالت عادی فاقد مجوز انجام آن است.

بهره‌جویی موفق از آن مستلزم اجرای کد یا اسکریپتی بر روی سیستم قربانی است که وظیفه آن دست‌درازی به فایل‌های موسوم به Symbolic Link است. بدین‌ترتیب عملیاتی حذفی که توسط یک پروسه با سطح دسترسی بالا اجرا شده به‌نحوی تغییر داده می‌شود که بجای حذف فایل مورد نظر پروسه، فایل دلخواه مهاجم حذف می‌گردد.

در این میان محصولات زیر نیز از آسیب‌پذیری مذکور تأثیر می‌پذیرند:

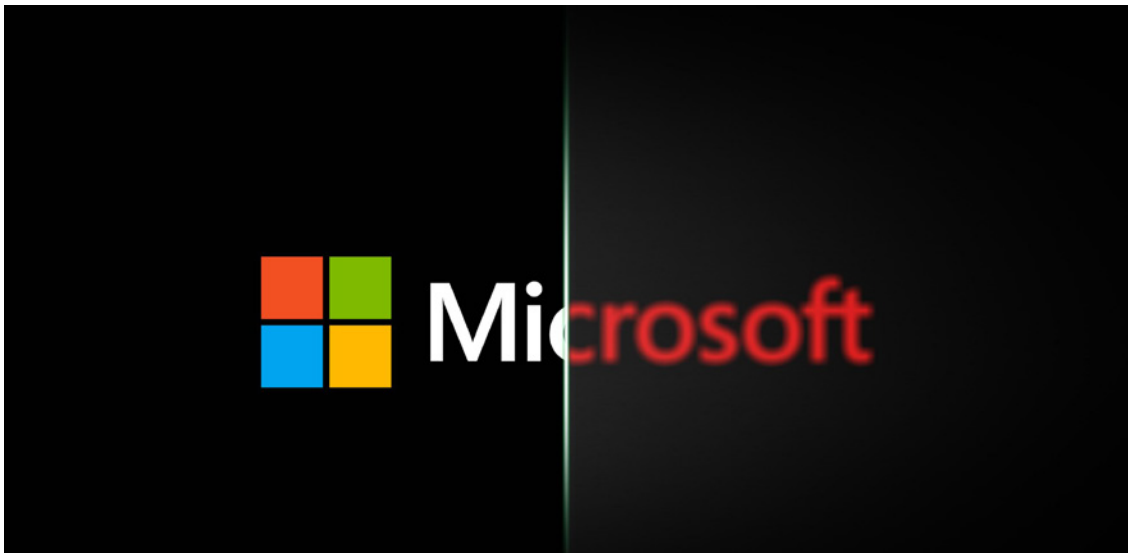
تمامی نسخ Endpoint Security (ENS) for Mac
نسخ 10.5.x، 10.6.x و 10.7.x نرم‌افزار ENS for Windows
تمامی نسخ VirusScan Enterprise (VSE) for Linux
تمامی نسخ VSE for Windows

خوشبختانه، مک‌آفی، ۵ اردیبهشت ماه این آسیب‌پذیری را در به‌روزرسانی‌های DAT 4053 (برای ENS for Windows) و DAT 9601 (برای ENS Mac، VSE for Windows و VSE for Linux) ترمیم و اصلاح کرد.

مقاله فنی مک‌آفی در خصوص آسیب‌پذیری مذکور در لینک زیر قابل دریافت و مطالعه است:

https://kc.mcafee.com/corporate/index?page=content&id=SB10316

اصلاحیه‌های امنیتی مایکروسافت
برای ماه میلادی می



به گزارش شرکت مهندسی شبکه گستر، سه‌شنبه، ۲۳ اردیبهشت، شرکت مایکروسافت اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی می منتشر کرد. این اصلاحیه‌ها در مجموع، ۱۲۲ آسیب‌پذیری را در سیستم عامل Windows و برخی دیگر از سرویس‌ها و نرم‌افزارهای مایکروسافت ترمیم می‌کنند. درجه حساسیت ۱۵ مورد از آسیب‌پذیری‌های ترمیم شده توسط اصلاحیه‌های مذکور "حیاتی" (Critical)، ۹۵ مورد "مهم" (Important)، ۶ مورد "متوسط" (Moderate) و ۶ مورد نیز "کم" (Low) اعلام شده است.

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

هیچ یک از آسیب‌پذیری‌های ترمیم شده توسط مجموعه اصلاحیه‌های این ماه، "روز-صفر" (Zero-day) اعلام نشده‌اند.

آسیب‌پذیری‌های "حیاتی"

از جمله آسیب‌پذیری‌های "حیاتی" ترمیم شده در این ماه می‌توان به موارد زیر اشاره کرد:

CVE-2020-1069، CVE-2020-1024، CVE-2020-1023 و CVE-2020-1102 که همگی ضعف‌هایی از نوع "اجرای کد به‌صورت از راه دور" (Remote Code Execution) در SharePoint هستند. بهره‌جویی از هر یک از ضعف‌های مذکور، مهاجم را قادر به اجرای کد بر روی دستگاه با نسخه آسیب‌پذیر SharePoint می‌کند. سوءاستفاده از CVE-2020-1069 مستلزم ارسال یک بسته دستکاری شده به سرور و باز شدن آن توسط کاربر است.

CVE-2020-1062 که یک آسیب‌پذیری "بروز اختلال در حافظه" (Memory Corruption) در مرورگر Internet Explorer بوده اعلام شده است. مهاجم می‌تواند با ایجاد یک صفحه اینترنتی حاوی بهره‌جو و هدایت کاربر به آن با استفاده از تکنیک‌های موسوم به "مهندسی اجتماعی" موجب "بروز اختلال در حافظه" شده و در ادامه اقدام به اجرای کد مورد نظر خود با سطح دسترسی کاربر جاری می‌کند.

سایر آسیب‌پذیری‌های "حیاتی" ترمیم شده در این ماه به‌شرح زیر است:

CVE-2020-1028	CVE-2020-1056	CVE-2020-1064
CVE-2020-1065	CVE-2020-1093	CVE-2020-1117
CVE-2020-1126	CVE-2020-1136	CVE-2020-1153
CVE-2020-1192		

آسیب‌پذیری‌های "مهم"

از میان آسیب‌پذیری‌های "مهم" این ماه، مورد زیر بیش سایرین جلب توجه می‌کند:

CVE-2020-1103 که ضعفی از نوع "نشت اطلاعات" در SharePoint است که مهاجم را قادر به اجرای حملات موسوم به Cross-site Search می‌کند. ورود همزمان کاربران به یک سرور و مشاهده یک صفحه وب دستکاری شده موجب بروز این آسیب‌پذیری می‌شود. مهاجم در ادامه می تواند با اجرای پرس‌وجوهای (Query) اقدام به جستجو و دسترسی یافتن به اطلاعات بالقوه حساس با سطح دسترسی کاربر جاری کرده و در ادمه حمله آنها را مورد استفاده قرار دهد.

سایر آسیب‌پذیری‌های "مهم" ترمیم شده در این ماه به‌شرح زیر است:

CVE-2020-0901	CVE-2020-0909	CVE-2020-0963
CVE-2020-1010	CVE-2020-1021	CVE-2020-1035
CVE-2020-1048	CVE-2020-1051	CVE-2020-1054
CVE-2020-1055	CVE-2020-1058	CVE-2020-1059
CVE-2020-1060	CVE-2020-1061	CVE-2020-1063
CVE-2020-1066	CVE-2020-1067	CVE-2020-1068
CVE-2020-1070	CVE-2020-1071	CVE-2020-1072
CVE-2020-1075	CVE-2020-1076	CVE-2020-1077
CVE-2020-1078	CVE-2020-1079	CVE-2020-1081

CVE-2020-1082	CVE-2020-1084	CVE-2020-1086
CVE-2020-1087	CVE-2020-1088	CVE-2020-1090
CVE-2020-1092	CVE-2020-1096	CVE-2020-1099
CVE-2020-1100	CVE-2020-1101	CVE-2020-1104
CVE-2020-1105	CVE-2020-1106	CVE-2020-1107
CVE-2020-1108	CVE-2020-1109	CVE-2020-1110
CVE-2020-1111	CVE-2020-1112	CVE-2020-1113
CVE-2020-1114	CVE-2020-1116	CVE-2020-1118
CVE-2020-1121	CVE-2020-1123	CVE-2020-1124
CVE-2020-1125	CVE-2020-1131	CVE-2020-1132
CVE-2020-1134	CVE-2020-1135	CVE-2020-1137
CVE-2020-1138	CVE-2020-1139	CVE-2020-1140
CVE-2020-1141	CVE-2020-1142	CVE-2020-1143
CVE-2020-1144	CVE-2020-1145	CVE-2020-1149
CVE-2020-1150	CVE-2020-1151	CVE-2020-1154
CVE-2020-1155	CVE-2020-1156	CVE-2020-1157
CVE-2020-1158	CVE-2020-1161	CVE-2020-1164
CVE-2020-1165	CVE-2020-1166	CVE-2020-1171
CVE-2020-1173	CVE-2020-1174	CVE-2020-1175
CVE-2020-1176	CVE-2020-1179	CVE-2020-1184

CVE-2020-1185 CVE-2020-1186 CVE-2020-1187

CVE-2020-1188 CVE-2020-1189 CVE-2020-1190

CVE-2020-1191

اصلاحیه‌های امنیتی ادوبی
برای ماه میلادی می

به گزارش شرکت مهندسی شبکه گستر، سه‌شنبه، ۲۳ اردیبهشت، شرکت ادوبی مجموعه اصلاحیه‌های امنیتی ماه میلادی می خود را منتشر کرد.

اصلاحیه‌های مذکور، در مجموع، ۳۶ ضعف امنیتی را در محصولات زیر ترمیم می‌کنند:

- Adobe Acrobat / Reader
- Adobe DNG Software Development Kit

۲۴ مورد از آسیب‌پذیری‌های ترمیم شده توسط این اصلاحیه‌ها، مجموعه نرم‌افزارهای Acrobat / Reader را تحت تأثیر قرار می‌دهند. درجه حساسیت نیمی از آنها "حیاتی" (Critical) اعلام شده است. بسیاری از این ضعف‌های امنیتی در دسته آسیب‌پذیری به حملات اجرای کد قرار می‌گیرند. بدین‌ترتیب باز کردن یک PDF دستکاری شده در هر یک از نسخه‌های آسیب‌پذیر مجموعه نرم‌افزارهای Acrobat / Reader منجر به اجرای کد بالقوه مخرب تزریق شده در فایل خواهد شد. با نصب به‌روزرسانی ماه می، نسخه نگارش‌های جاری نرم‌افزارهای Acrobat DC و Acrobat Reader DC به 2020.009.20063 و نگارش‌های ۲۰۱۷ آنها به 2017.011.30171 تغییر خواهد کرد.

اطلاعات بیشتر در خصوص مجموعه اصلاحیه‌های ماه می ادوبی در لینک‌های زیر قابل مطالعه است:

- https://helpx.adobe.com/security/products/acrobat/apsb20-24.html
- https://helpx.adobe.com/security/products/dng-sdk/apsb20-26.html

اصلاحیه‌های عرضه شده
در اردیبهشت ۱۳۹۹

در اردیبهشت ۱۳۹۹، شرکت‌های مایکروسافت، گوگل، جونیپر نت‌ورکز، وی‌اِم‌وِر، ادوبی، سیسکو و موزیلا، پروژه اوپن‌اس‌اس‌ال، گروه سامبا و بنیاد وردپرس اقدام به انتشار اصلاحیه و توصیه‌نامه امنیتی برای برخی از محصولات خود کردند.

در ۳ اردیبهشت، شرکت مایکروسافت اقدام به عرضه به روزرسانی برای ترمیم چندین آسیب پذیری در محصولات Office 2016، Office 2019، Office 365 ProPlus و Paint 3D کرد. بهره جویی (Exploit) از آسیب پذیری های مذکور که از وجود ضعفی در کتابخانه Autodesk FBX ناشی می شوند مهاجم را قادر به اجرای کد به صورت از راه دور می کند. جزییات بیشتر در اینجا قابل دریافت است. این شرکت، در ۲۳ اردیبهشت نیز اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی می منتشر کرد که پیش‌تر در اینجا به تفصیل به آنها پرداخته شد.

در روزهای ابتدایی اردیبهشت، پروژه اوپن‌اس‌اس‌ال نسخه جدیدی از این کتابخانه کدباز منتشر کرد که در آن ضعفی با درجه حساسیت بالا، با شناسه CVE-2020-1967 ترمیم شده است. بهره‌جویی از آسیب‌پذیری مذکور، امکان اجرای حملات Denial-of-Service - به اختصار DoS - را فراهم می‌کند. اطلاعات بیشتر در اینجا قابل مطالعه است.

به گزارش شرکت مهندسی شبکه گستر، در اردیبهشت ماه، گوگل در چندین نوبت با عرضه به‌روزرسانی اقدام به ترمیم آسیب‌پذیری‌های امنیتی مرورگر Chrome کرد. آخرین نسخه این مرورگر که در ۳۰ اردیبهشت انتشار یافت 83.0.4103.61 است. فهرست اشکالات مرتفع شده در اینجا، اینجا، اینجا و اینجا قابل دریافت است.

جونیپر نت‌ورکز نیز در ۹ اردیبهشت با ارائه به‌روزرسانی یک ضعف امنیتی را در سیستم عامل مورد استفاده در تجهیزات ساخت این شرکت (Junos) ترمیم کرد. سوءاستفاده از ضعف مذکور مهاجم را قادر به در اختیار گرفتن کنترل دستگاه آسیب‌پذیر می‌کند. جزییات بیشتر در اینجا قابل مطالعه است.

در همین تاریخ گروه سامبا با عرضه به‌روزرسانی، دو ضعف امنیتی با شناسه‌های CVE-2020-10700 و CVE-2020-10704 را در نرم‌افزار کدباز Samba برطرف کرد. سوءاستفاده از یکی از این ضعف‌های ترمیم شده در اختیار گرفتن کنترل سیستم آسیب‌پذیر را فراهم می‌کند.

وی‌اِم‌وِر دیگر شرکتی بود که در اردیبهشت ۱۳۹۹ اقدام به انتشار به‌روزرسانی کرد. محصولات ESXi، vRealize Operations Manager و Cloud Director از آسیب‌پذیری های ترمیم شده توسط این به‌روزرسانی‌ها تأثیر می‌پذیرند. اطلاعات بیشتر در مورد به‌روزرسانی عرضه شده در اینجا، اینجا و اینجا قابل مطالعه است.

در ۱۰ اردیبهشت، شرکت ادوبی با عرضه نسخ جدید چندین ضعف امنیتی را در محصولات Bridge، Illustrator و Magento را عرضه کرد. ادوبی، در ۲۳ اردیبهشت نیز اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی می منتشر کرد که پیش‌تر در اینجا به تفصیل به آنها پرداخته شد. این شرکت در آخرین روز دومین ماه ۱۳۹۹، ضعف‌هایی را در Premiere Pro، Audition و Premiere Rush ترمیم و اصلاح کرد.

در اردیبهشت ۹۹، سیسکو در چندین نوبت اقدام به عرضه به‌روزرسانی‌های امنیتی کرد. این به‌روزرسانی‌ها در مجموع، ۴۹ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت ۱ مورد از این آسیب‌پذیری‌ها، "حیاتی" (Critical) و ۲۶ مورد از آنها "بالا" (High) گزارش شده است. آسیب‌پذیری به حملاتی همچون "اجرای کد به‌صورت از راه دور" (Remote Code Execution)، "از کاراندازی سرویس" (Denial of Service) و "تزریق فرمان" (Command Injection)، از جمله اشکالات مرتفع شده توسط به‌روزرسانی‌های جدید است. توضیحات کامل در مورد به‌روزرسانی‌های عرضه شده در اینجا قابل دسترس است.

۱۱ اردیبهشت، بنیاد وردپرس نسخه ۵.۴.۱ 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.

در اواسط اردیبهشت ۱۳۹۹، شرکت موزیلا، با ارائه به‌روزرسانی، چندین آسیب‌پذیری را در مرورگر Firefox برطرف کرد. درجه حساسیت ۳ مورد از آسیب‌پذیری‌های مذکور، "حیاتی" اعلام شده است. جزییات بیشتر در اینجا قابل دسترس است.

افتای ریاست جمهوری با همکاری شبکه گستر

شبکه گستر

شرکت مهندسی شبکه گستر

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

نسخه‌ای نمایشی از بهره‌جوی RCE آسیب‌پذیری SMBGhost

محققان اقدام به انتشار نسخه‌ای نمایشی از نمونه PoC آسیب‌پذیری SMBv۳ به حملات "اجرای کد به‌صورت از راه دور" کرده‌اند. رخدادی که اهمیت نصب فوری اصلاحیه این باگ امنیتی را بیش از قبل پررنگ می‌کند. ادامه مطلب را در اینجا بخوانید.

مجموعه‌تراشه‌های FPGA، آسیب‌پذیر به Starbleed

گروهی از محققان دانشگاهی باگ امنیتی جدیدی را کشف کرده‌اند که مجموعه تراشه‌های موسوم به FPGA ساخت شرکت Xilinx از آن تأثیر می‌پذیرند.ادامه مطلب را در اینجا بخوانید.

چهار آسیب‌پذیری روز-صفر در محصول امنیتی IBM

جزییات چهار آسیب‌پذیری روز-صفر در یک محصول امنیتی IBM، پس از آنکه این شرکت از ترمیم آنها سر باز زد به‌صورت عمومی منتشر شده است. ادامه مطلب را در اینجا بخوانید.

بات‌نت Hoaxcalls، مجهزتر از قبل

پژوهشگران هشدار داده‌اند که بات‌نت Hoaxcalls دامنه دستگاه‌های مورد هدف خود را گسترش داده است. این محققان از پیاده‌سازی قابلیت‌های جدیدی نیز برای اجرای حملات Distributed Denial of Service - به اختصار DDoS - در این بات‌نت خبر داده‌اند. Hoaxcalls بات‌نتی مبتنی بر تجهیزات موسوم به اینترنت اشیاء است. ادامه مطلب را در اینجا بخوانید.

اختلافات بر سر سه آسیب‌پذیری iOS

بر اساس بیانیه‌ای که اپل آن را ۵ اردیبهشت منتشر کرد این شرکت اعلام کرده که گزارش اخیری را که در آن ادعا شده هکرها در حال بهره‌جویی از سه آسیب‌پذیری روز-صفر در سیستم عامل iOS هستند به دقت بررسی کرده اما هنوز سندی دال بر صحیح بودن آن نیافته است. ادامه مطلب را در اینجا بخوانید.

انتشار کلیدهای رمزگشایی باج‌افزار Shade/Troldesh

گردانندگان باج‌افزار Shade - که با نام Troldesh نیز شناخته می‌شود - ضمن اعلام توقف فعالیت این باج‌افزار، به نشانه حسن‌نیت اقدام به عرضه بیش از ۷۵۰ هزار کلید رمزگشایی متعلق به قربانیان خود کرده‌اند. ادامه مطلب را در اینجا بخوانید.

اخاذی در پس هشدار FBI

باج‌افزار Lucy با آلوده‌سازی گوشی‌های هوشمند مبتنی بر Android و رمزگذاری داده‌های آنها اقدام به اخاذی از قربانیان می‌کند. این باج‌افزار در اواخر سال ۲۰۱۸ ظهور کرد و نویسندگان آن در نسخه جدید آن اقداماتی پیچیده‌تر از یک رمزگذاری معمول را انجام می‌دهند. ادامه مطلب را در اینجا بخوانید.

توصیه‌های Microsoft برای مقابله با باج‌افزارها

شرکت Microsoft هشدار داده که مهاجمان در کارزارهای سایبری در حال آلوده‌سازی مراکز فعال در حوزه سلامت و سرویس‌های حیاتی به باج‌افزارهای از نوع موسوم به Human-operated هستند. 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. ادامه مطلب را در اینجا بخوانید.

سال‌ها انتشار جاسوس‌افزار از طریق Play Store

مهاجمان در کارزاری با نام PhantomLance با به‌اشتراک‌گذاری برنامه‌های حاوی جاسوس‌افزار بر روی Play Store و انباره‌های جایگزین نظیر APKpure و APKCombo کاربران دستگاه‌های با سیستم عامل Android را هدف قرار می‌دهند. ادامه مطلب را در اینجا بخوانید.

تلاش مهاجمان برای بهره‌جویی از WebLogic

شرکت اوراکل در هشدار امنیتی اضطراری خود از مشتریان WebLogic خواسته تا نسبت به نصب فوری آخرین اصلاحیه‌های این محصول که در ۲۶ فروردین عرضه شدند اقدام کنند. اوراکل همچنین اعلام کرده که گزارش‌هایی را در خصوص تلاش مهاجمان برای بهره‌جویی از یکی از آسیب‌پذیری‌های WebLogic به شناسه CVE-2020-2883 دریافت کرده است. ادامه مطلب را در اینجا بخوانید.

ترمیم دو آسیب‌پذیری حیاتی در Salt

در پی کشف دو آسیب‌پذیری "حیاتی" در Salt، توسعه‌دهندگان این بستر مدیریتی در هشداری از کاربران خواسته‌اند که نسبت به به‌روزرسانی آن اقدام کنند. Salt پروژه ای کد باز است که معمولاً در مراکز داده و سرورهای ابری مورد استفاده قرار می‌گیرد. ادامه مطلب را در اینجا بخوانید.

افزایش حملات RDP در پی همه‌گیری جهانی کرونا

شرکت کسپرسکی اعلام کرده که از زمان شروع همه‌گیری جهانی کرونا، تعداد حملات موسوم به "سعی‌وخطا" بر ضد پودمان RDP به‌شدت افزایش یافته است. ادامه مطلب را در اینجا بخوانید.

صدها هزار سایت در خطر هک در نتیجه آسیب‌پذیری Ninja Forms

توسعه‌دهندگان Ninja Forms ضعفی امنیتی با درجه حساسیت بالا را در این افزونه ترمیم کردند. Ninja Forms یک افزونه WordPress با بیش از یک میلیون نصب است. ادامه مطلب را در اینجا بخوانید.

تروجانی بانکی با قابلیت عبور از سد 2FA

یک تروجان بانکی جدید با عنوان EventBot کاربران در ایالات متحده و چندین کشور اروپایی شامل انگلیس، آلمان، ایتالیا، اسپانیا، سوئیس و فرانسه را هدف قرار داده است. این تروجان کاربران بیش از ۲۰۰ برنامه مالی را هدف قرار می‌دهد. ادامه مطلب را در اینجا بخوانید.

افشای جزییات آسیب‌پذیری OpenSSL

پروژه OpenSSL نسخه جدیدی از این کتابخانه کدباز منتشر کرده که در آن ضعفی با درجه حساسیت بالا، با شناسه CVE-2020-1967 ترمیم شده است. ادامه مطلب را در اینجا بخوانید.

Kaiji، بات‌نت جدید اینترنت اشیاء

محققان امنیتی از شناسایی بدافزار جدیدی با عنوان Kaiji خبر داده‌اند که به‌طور خاص برای آلوده‌سازی سرورهای مبتنی بر Linux و دستگاه‌های موسوم به اینترنت اشیاء طراحی شده است. ادامه مطلب را در اینجا بخوانید.

ترمیم ۱۲ آسیب‌پذیری با درجه حساسیت بالا در محصولات امنیتی Cisco

سیسکو با عرضه به‌روزرسانی، ۱۲ آسیب‌پذیری با درجه حساسیت "بالا" را در محصولات ASA و FTD ترمیم کرد. ادامه مطلب را در اینجا بخوانید.

باج‌افزار Sodinokibi، تواناتر از قبل

تکامل باج‌افزار Sodinokibi - که با نام REvil نیز شناخته می‌شود - همچنان ادامه دارد؛ در جدیدترین مورد، گردانندگان آن اقدام به افزودن قابلیتی کرده‌اند که باج‌افزار را قادر به رمزگذاری، حتی در زمانی که فایل توسط پروسه‌ای دیگر، باز یا قفل شده است می‌کند. ادامه مطلب را در اینجا بخوانید.

برنامه‌های وب، هدف Blue Mockingbird

محققان از فعالیت یک کارزار استخراج ارز رمز مونرو با عنوان Blue Mockingbird خبر داده‌اند که در جریان گسترش آن از آسیب‌پذیری CVE-2019-18935 در برنامه‌های وب بهره‌جویی می‌شود. ادامه مطلب را در اینجا بخوانید.

کاربران نگران کرونا، هدف تروجان بانکی Zeus Sphinx

تروجان بانکی Zeus Sphinx در حالی با سوءاستفاده از نگرانی جهانی از بحران همه‌گیری کووید ۱۹ در حال انتشار است که به‌طور مستمر خود را به‌روزرسانی و مجهز به قابلیت‌های مخرب بیشتر می‌کند. ادامه مطلب را در اینجا بخوانید.

میلیون‌ها دستگاه، آسیب‌پذیر به ضعف‌های امنیتی تاندربولت

یک محقق هلندی، ۹ سناریو حمله را مطرح کرده که در آنها مهاجم با دسترسی فیزیکی به دستگاه قادر به سرقت داده‌ها از روی درایوها و حافظه‌های رمزگذاری شده است. حملات مذکور که از آنها با عنوان Thunderspy یاد شده بر روی تمامی کامپیوترهای مجهز به رابط‌های سخت‌افزاری تاندربولت ساخت ۲۰۱۱ و سال‌های بعد از آن قابل اجرا گزارش شده‌اند. ادامه مطلب را در اینجا بخوانید.

تحلیل چگونگی بهره‌جویی مهاجمان از آسیب‌پذیری WebLogic

تحلیل چگونگی بهره‌جویی مهاجمان از آسیب‌پذیری WebLogic. ادامه مطلب را در اینجا بخوانید.

پروژه مشترک Microsoft و Intel در تبدیل بدافزار به تصویر

شرکت‌های مایکروسافت و اینتل در یک پروژه تحقیقاتی مشترک در حال بررسی رویکردی جدید در شناسایی و طبقه‌بندی بدافزارها هستند. این پروژه با عنوان STAMINA متکی به تکنیک جدیدی است که در آن نمونه‌های بدافزاری به تصاویر سیاه و سفید تبدیل شده و در ادامه با پویش تصویر، شالوده و الگوهای ساختاری مرتبط با نمونه‌های بدافزاری در آنها شناسایی می‌شود. ادامه مطلب را در اینجا بخوانید.

QNodeService، تروجانی غیرمتعارف بر بستر Node.js

محققان از شناسایی تروجان جدیدی با عنوان QNodeService خبر داده‌اند که ظاهراً در قالب فیشینگ‌های با الگوی بیماری کووید ۱۹ منتشر می‌شود. ادامه مطلب را در اینجا بخوانید.

استفاده باج‌افزار ProLock از تروجان QakBot برای رخنه به شبکه قربانیان

اگر چه ProLock بدافزار نسبتاً جدیدی در صحنه باج‌افزارها محسوب می‌شود اما به دلیل هدف قرار دادن کسب‌وکارها و سازمان‌های دولتی و اخاذی مبالغ هنگفت از آنها به‌سرعت در حال معروف شدن است. ادامه مطلب را در اینجا بخوانید.

CoViper؛ یک Wiper فعلاً آزمایشی

محققان از شناسایی نمونه‌ای جدید از خانواده بدافزارهای موسوم به Wiper خبر داده‌اند که در جریان اخیر به نحوی از بحران همه‌گیری ویروس کووید ۱۹ بهره‌گیری می‌کند. ادامه مطلب را در اینجا بخوانید.

مروری بر آسیب‌پذیری فراگیر BIAS

محققان جزییات آسیب‌پذیری جدیدی در پودمان Bluetooth، معروف به BIAS را منتشر کردند. پودمانی که به‌طور گسترده در دستگاه‌های مدرن امروزی همچون گوشی‌های هوشمند، تبلت‌ها، لپ‌تاپ‌ها و دستگاه‌های اینترنت اشیاء مورد استفاده قرار می‌گیرد. 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