مرداد

۱۳۹۹

ماهنامه

امنیت فناوری اطلاعات

شبکه گستر

امنیت شما | وظیفه ما

newsroom.shabakeh.net

@SGnewsroom

فهرست مطالب

چکیده مدیریتی ۳

آمار جهانی از نگاه مک آفی ۵

هشدارهای امنیتی ۱۶

آسیب‌پذیری‌ها و اصلاحیه‌های امنیتی ۳۹

افتای ریاست جمهوری با همکاری شبکه گستر ۴۴

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 مرداد ماه ۱۳۹۹ پرداخته شده است.

همان‌طور که در این ماهنامه خواهید خواند یک هکر با تغییر کدهای ناقل Emotet در سایت‌های هک شده، گردانندگان این بدافزار پیشرفته را دچار سردرگمی کرد. در جریان عملیات این هکر، تصاویر متحرک GIF جایگزین کدهای مخرب ناقل بدافزار می‌شدند.

در این ماهنامه به بررسی روش کار یک گروه منتسب به مهاجمان روسی که اجرای کارزارهای موفق بر ضد بانک‌ها و مؤسسات مالی و سرقت میلیون‌ها دلار از آنها را در کارنامه دارد پرداخته شده است. کارزارهای اجرا شده توسط این گروه که به Silence معروف است را می‌توان از جمله مخرب‌ترین تهدیدات موسوم به پیشرفته و مستمر (APT) در سال‌های اخیر دانست. این مهاجمان با در اختیار گرفتن کنترل دستگاه‌های خودپرداز، اقدام به سرقت پول از آنها می‌کنند. در اکثر این کارزارها، گردانندگان Silence با بکارگیری ترفندهای مهندسی اجتماعی و ارسال ایمیل‌های فیشینگ اختصاصی و هدفمند، کارکنان بانک را هدف قرار می‌دهند.

در مرداد ماه، گردانندگان باج‌افزار Nefilim فایل‌هایی را منتشر کردند که در جریان حمله اخیر به یکی از اهداف خود اقدام به سرقت آنها کرده بودند. متأسفانه در ماه‌های اخیر نمونه‌های متعددی از نشت اطلاعات در پی اجرای حملات باج‌افزاری گزارش شده است. جزییات بیشتر در مورد این رخدادها را در این ماهنامه بخوانید.

در این ماهنامه به گزارشی از شرکت امنیتی مک‌آفی پرداخته شده که بر اساس آن گردانندگان باج‌افزار NetWalker از ماه مارس سال میلادی جاری موفق به دریافت حداقل ۲۵ میلیون دلار از قربانیان خود شده‌اند. Dharam نیز دیگر باج‌افزاری است که در این ماهنامه روش کار مهاجمان آن مورد بررسی و کالبدشکافی قرار گرفته است.

و در آخر اینکه در مرداد ۱۳۹۹، شرکت‌های سیتریکس، ادوبی، مایکروسافت، سیسکو، گوگل و موزیلا برای برخی محصولات خود اصلاحیه و توصیه‌نامه امنیتی منتشر کردند که مشروح 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 Phobos

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

باج‌افزار Snatch

گردانندگان باج‌افزار Snatch با اجرای حملات موسوم به سعی‌وخطا (Brute Force) و هک حساب‌های با دسترسی Administrator اقدام به رخنه به سرورهای با پودمان RDP باز می‌کنند. به‌محض دستیابی به یکی از سرورهای Domain Controller، با راه‌اندازی یک Shell معکوس، باج‌افزار حضور خود را تثبیت کرده و بستر را برای رمزگذاری فایل‌های دستگاه‌های متصل به دامنه فراهم می‌کند. علاوه بر آن برای عبور از سد محصولات امنیتی نصب شده بر روی دستگاه، باج‌افزار بعد از راه‌اندازی مجدد (Restart) سیستم در حالت Safe Mode، فرایند رمزگذاری را آغاز می کند.

باج‌افزار EvilQuest

خانواده جدیدی از باج‌افزارها است که کاربران دستگاه‌های مکینتاش را از طریق نرم‌افزارهای جعلی در ظاهر کاربردی و معتبر که بر روی سایت‌های Torrent میزبانی شده‌اند هدف قرار می‌دهد. این نرم‌افزار مخرب که با نام ThiefQuest نیز شناخته می‌شود با استفاده از یک Keylogger اطلاعات اصالت‌سنجی، داده‌های کیف‌های ارز رمز و سایر اطلاعات حساس را سرقت می‌کند. همچنین با نصب یک درب‌پشتی (Backdoor)، خود را بر روی دستگاه قربانی ماندگار می‌کند. در اطلاعیه باج‌گیری (Ransom Note) آن صرفاً نشانی های بیت کوین درج شده و راهی برای برقراری ارتباط با مهاجمان در آن در نظر گرفته نشده است.

کارزار GoldenSpy Chapter Two

در اواسط سال ۲۰۲۰ شرکت‌های چینی هدف بدافزار GoldenSpy که در یک نرم‌افزار معتبر پرداخت مالیات مخفی شده بود قرار گرفتند. چند هفته بعد، حذف‌کننده‌ای (Uninstaller) بر روی سرور فرماندهی (C۲) مهاجمان قرار گرفت که به‌صورت خودکار توسط نرم‌افزار دریافت و اقدام به حذف GoldenSpy و اثرات آن از روی دستگاه قربانی می‌کرد. مدتی بعدتر نسخه دومی از این حذف‌کننده نیز منتشر شد که البته با کدگذاری توسط Base64 مبهم‌سازی (Obfuscation) شده بود.

کارزار Favicon EXIF Data

در کارزاری کلاهبرداری مهاجمان با قرار دادن کد مخرب در فراداده‌های Exchangeable Image File Format - به

کارزار Tetrade

در کارزار Tetrade با بکارگیری چهار خانواده بدافزار بانکی با نام‌های Melcoz، Javali، Guildma و Grandoreiro

اختصار EXIF - و مخفی کردن آنها در سایت‌ها اقدام به سرقت اطلاعاتی همچون داده های مربوط به کارت های اعتباری از طریق فیلدهای ورودی سایت‌های آلوده کردند. اطلاعات سرقت شده با الگوریتم Base64 رمز شده و در قالب فایل تصویری به سرورهای فرماندهی ارسال می‌شدند. به نظر می رسد که گرداننده این کارزار گروه Magecart بوده که حمله به سازمان‌های مطرح را در کارنامه دارد.

کارزار Vaccine Development

گروه APT29 که با نام Cozy Bear نیز شناخته می‌شود دامنه‌ای گسترده از صنایع در کانادا، انگلیس و آمریکا هدف قرار داد. مهاجمان کارزار بر روی نهادهای دخیل در ساخت واکسن تمرکز داشته‌اند. این جاسوسان سایبری با استفاده از بدافزارهایی همچون WellMail، WellMess و SoreFang اقدام به سرقت داده‌های حساس کرده، نرم‌افزارهای مخرب را نصب نموده، فرامین Shell را فراخوانی کرده و اسکریپت‌ها را اجرا می‌کنند. گروه APT29 با ارسال ایمیل‌های فیشینگ هدفمند و بهره‌جویی از آسیب‌پذیری‌های سرورهای قابل دسترس بر روی اینترنت رخنه اولیه را انجام می‌داده است.

آسیب‌پذیری CVE-2020-6287

نسخ 7.30، 7.31، 7.40 و 7.50 محصول SAP NetWeaver AS JAVA از آسیب‌پذیری CVE-2020-6287 که ناشی از عدم اصالت‌سنجی مهاجم در جریان دست‌درازی به تنظیمات حیاتی در این محصول است تأثیر می‌پذیرند. مهاجم با دسترسی فراهم شده در نتیجه آسیب‌پذیری مذکور قادر به ایجاد کاربر با سطح دسترسی Administrator خواهد بود.

کاربران در نقاط مختلف جهان هدف قرار گرفتند. این کارزار منتسب به مهاجمان مقیم در برزیل بوده و از اواخر ۲۰۱۵ فعال بوده است. بدافزارهای مذکور مجهز به تکنیک‌های عبور از سد سازوکارهای دفاعی شامل ضدتحلیل، ضدبسترهای مجازی‌سازی، مبهم‌سازی، DLL Side Loading و بهره‌گیری از Background Intelligent Transfer Service - به اختصار BITS - است. بدافزار از طریق ایمیل‌های فیشینگ حاوی لینک یا پیوست مخرب توزیع می‌شود. در مواردی نیز سایت‌های هک شده یا سایت‌های در اختیار مهاجمان میزبان بدافزارها بوده‌اند.

آسیب‌پذیری CVE-2020-1350

CVE-2020-1350، ضعفی از نوع اجرای کد به‌صورت از راه دور (Remote Code Execution) است که از نحوه مدیریت نادرست درخواست‌های DNS در سیستم عامل Windows ناشی می‌شود.

آسیب‌پذیری CVE-2020-5902

CVE-2020-5902، ضعفی در تجهیزات ساخت شرکت اف5 است که مهاجم را قادر به اجرای کد به‌صورت از راه دور بر روی دستگاه آسیب‌پذیر می‌کند.

۱۰ بسته بهره‌جو با بیشترین استفاده

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

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

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

۱۰ کارزار مطرح

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

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

۱۰ باج‌افزار با بیشترین انتشار

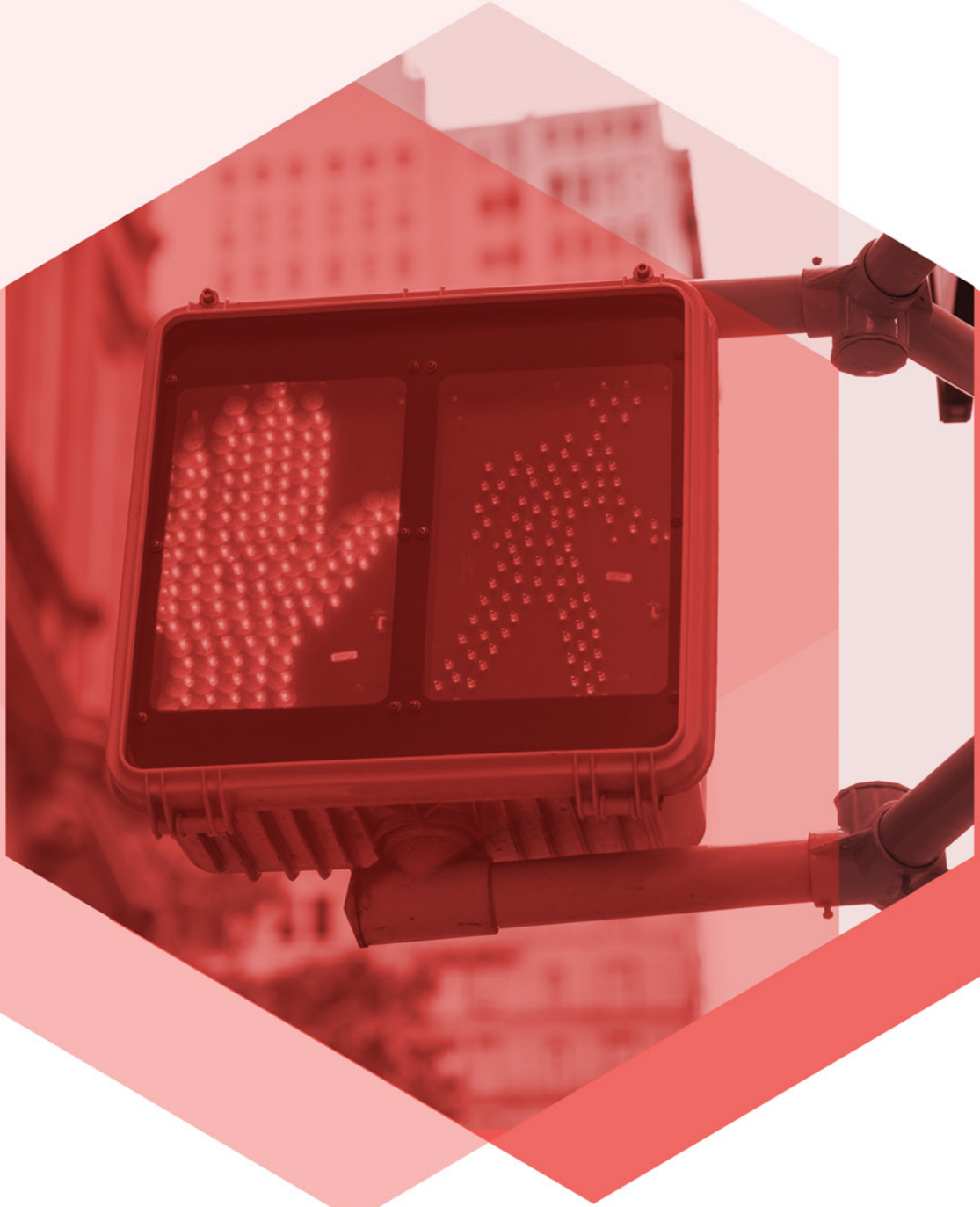
باج‌افزار	توضیحات
Dharma	Dharma که گونه ای از باج افزار CrySiS پسوندهای مختلفی را به فایل های رمزگذاری شده الصاق می کند. این باج افزار از سال ۲۰۱۶ فعال بوده و گردانندگان آن به طور مستمر اقدام به عرضه نسخ جدیدی از آن می کنند.
Phobos	این باج‌افزار پس از رمزگذاری فایل‌ها توسط الگوریتم AES اقدام به افزودن یکی از پسوندهای متنوع خود به آنها می‌کند. نخستین نسخه از Phobos در اواخر سال 2017 شناسایی شد و تا اوایل 2019 عرضه نسخه‌های جدید از آن ادامه داشت. روش برقراری ارتباط با گردانندگان باج‌افزار از طریق ایمیل‌های درج شده در اطلاعیه باج‌گیری است.
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.
Hakbit	این باج‌افزار که در اواخر سال 2019 شناسایی شد همچنان به حیات خود ادامه می‌دهد. Hakbit که با نام‌های Corona، Abarcy، Horse و Ravack نیز شناخته می‌شود فایل های قربانی را با الگوریتم AES رمزگذاری کرده و در ازای ارائه کلید رمزگشایی، از قربانی مبلغ 3 بیت‌کوین را اخاذی می‌کند. بدافزار چندین حوزه شامل صنایع دارویی، حقوقی، مالی، خرده‌فروشی، سلامت و درمان، فن‌آوری اطلاعات، تولید و بیمه را مورد هدف قرار داده است. یکی از روش‌های انتشار این بدافزار هرزنامه‌های با پیوست فایل Excel است.
Nefilim	این باج‌افزار پس از رمزگذاری فایل‌های قربانی با الگوریتم AES-128 اقدام به الصاق پسوند ".NEFILIM" به آنها می‌کند. در کدهای مورد استفاده Nefilim شباهت‌هایی با باج‌افزار Nemty به چشم می‌خورد. اما بر خلاف آن از سیستم پرداخت در بستر شبکه ناشناس TOR استفاده نکرده و از ایمیل برای تبادل اطلاعات در خصوص پرداخت باج استفاده می‌کند. مهاجمان Nefilim تهدید می‌کنند که در صورت پرداخت نشدن باج ظرف 7 روز اطلاعات قربانی را به‌صورت عمومی به اشتراک خواهند گذاشت.
Conti	خانواده جدیدی از باج‌افزارها است با بهره‌گیری از چندین تکنیک فایل‌های مورد نظر خود را شناسایی و نسبت به رمزگذاری آنها با سرعتی بالاتر از هم‌قطاران خود اقدام می‌کند. این باج‌افزار مجهز به تنظیمات خط‌فرمان برای پویش فایل‌های محلی و فایل‌های به اشتراک گذاشته در بستر SMB است. همچنین Conti از Windows Restart Manager برای آزاد کردن فایل‌های در اشغال برنامه‌های دیگر استفاده می‌کند. این باج‌افزار الگوریتم AES-256 برای رمزگذاری فایل‌ها بهره می‌گیرد.

باج‌افزار	توضیحات
EvilQuest	خانواده جدیدی از باج‌افزارها است که کاربران دستگاه‌های مکینتاش را از طریق نرم‌افزارهای جعلی در ظاهر کاربردی و معتبر که بر روی سایت‌های Torrent میزبانی شده‌اند هدف قرار می‌دهد. این نرم‌افزار مخرب که با نام ThiefQuest نیز شناخته می‌شود با استفاده از یک Keylogger اطلاعات اصالت‌سنجی، داده‌های کیف‌های ارز رمز و سایر اطلاعات حساس را سرقت می‌کند. همچنین با نصب یک درب‌پشتی، خود را بر روی دستگاه قربانی ماندگار می‌کند. در اطلاعیه باج‌گیری (Ransom Note) آن صرفاً نشانی های بیت کوین درج شده و راهی برای برقراری ارتباط با مهاجمان در آن در نظر گرفته نشده است.
WastedLocker	گروه معروف به Evil Corp eCrime که با نام Indrik Spider نیز شناخته می‌شود خانواده باج‌افزاری جدیدی با عنوان WastedLocker را عرضه کرده که برای رمزگذاری فایل‌های قربانی از الگوریتم‌های AES و RSA بهره می‌گیرد. این باج‌افزار رشته‌ای حاوی نام شرکت و کلمه wasted را به فایل‌های رمز شده الصاق می‌کند. همچنین به ازای هر فایل رمز شده یک فایل متنی را که در آن دو ایمیل برای برقراری ارتباط با مهاجمان درج شده ایجاد می‌کند. در مواردی مبلغ اخاذی شده به میلیون‌ها دلار می‌رسد. Evil Corp eCrime توزیع بدافزارهای بانکی و راه‌اندازی بات‌نت‌ها را نیز در کارنامه دارد.
Exorcist	این باج‌افزار پس از رمزگذاری با الگوریتم‌های AES و RSA به آنها پسوندی حاوی رشته‌ای از نویسه‌های تصادفی را الصاق می‌کند. گردانندگان Exorcist در فایل اطلاعیه باج‌گیری قربانیان را برای دریافت دستورالعمل پرداخت باج به سایت اختصاصی خود هدایت می‌کنند. این باج‌افزار هیچ قربانی در کشورهای عضو سابق اتحاد جماهیر شوروی نمی‌گیرد.

۱۰ آسیب‌پذیری شاخص

آسیب‌پذیری	توضیحات
CVE-2020-9688	ضعفی در نسخه 2.0.0.518 نرم‌افزار Adobe Download Manager است که مهاجم را قادر به تزریق فرمان و در نهایت اجرای کد مخرب مورد نظر خود می‌کند.
CVE-2020-1350	ضعفی از نوع اجرای کد به‌صورت از راه دور است که از نحوه مدیریت نادرست درخواست‌های DNS در سیستم عامل Windows ناشی می‌شود.
CVE-2020-6287	نسخ 7.30، 7.31، 7.40 و 7.50 محصول SAP NetWeaver AS JAVA از آسیب‌پذیری CVE-2020-6287 که ناشی از عدم اصالت‌سنجی مهاجم در جریان دست‌درازی به تنظیمات حیاتی در این محصول است تأثیر می‌پذیرند. مهاجم با دسترسی فراهم شده در نتیجه آسیب‌پذیری مذکور قادر به ایجاد کاربر با سطح دسترسی Administrator خواهد بود.
CVE-2020-5902	CVE-2020-5902، ضعفی در تجهیزات ساخت شرکت اف5 است که مهاجم را قادر به اجرای کد به‌صورت از راه دور بر روی دستگاه آسیب‌پذیر می‌کند.
CVE-2020-14724	ضعفی در محصول Oracle Solaris است که مهاجم با سطح دسترسی محدود را قادر به در اختیار گرفتن کنترل این محصول می‌کند.
CVE-2020-1147	ضعفی از نوع اجرای کد به‌صورت از راه دور است که محصولات .Microsoft، NET Framework SharePoint و Visual Studio در نتیجه عدم بررسی صحیح فایل ورودی XML از آن تأثیر می‌پذیرند.
CVE-2020-9682	ضعفی در نسخه 5.1 و نسخ قبل از آن Adobe Creative Cloud Desktop Application است که بهره‌جویی موفق از آن امکان اجرای فایل بر روی سیستم آسیب‌پذیر را فراهم می‌کند.
CVE-2020-14621	ضعفی در Java SE است که با بهره جویی آسان از آن مهاجم اصالت سنجی نشده با دسترسی محلی از طریق پودمان های مختلف را قادر به دست درازی به برخی داده های قابل دسترس برای این محصول می کنند.
CVE-2020-6510	ضعفی حیاتی در مرورگر Google Chrome است که مهاجم با دسترسی از راه دور را قادر به ایجاد اختلال در عملکرد دستگاه آسیب‌پذیر یا اجرای کد بر روی آن می‌کند.
CVE-2020-6512	ضعفی در مرورگر Google Chrome است که مهاجم با دسترسی از راه دور را قادر به ایجاد اختلال در عملکرد دستگاه آسیب‌پذیر یا اجرای کد بر روی آن می‌کند.

هشدارهای امنیتی



شوخی یک هکر
با گردانندگان بدافزار Emotet

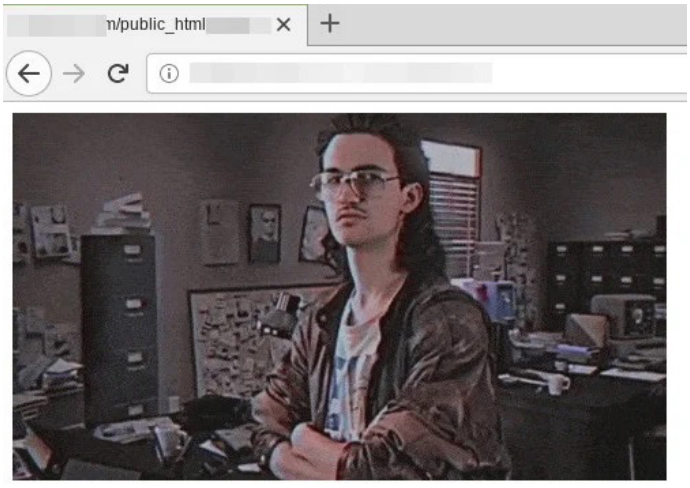
در روزهای اخیر، یک هکر با تغییر کدهای ناقل Emotet در سایت‌های هک شده، گردانندگان این بدافزار پیشرفته را دچار سردرگمی کرده است. در جریان عملیات این هکر، تصاویر متحرک GIF جایگزین کدهای مخرب ناقل بدافزار می‌شوند.

هدف از این اقدام هکر هر چه باشد در حال حاضر شبکه توزیع Emotet فلج شده و نویسندگان این بدافزار در تلاش هستند تا کنترل سایت‌های هک شده را مجدداً در اختیار بگیرند.

به گزارش شرکت مهندسی شبکه گستر، روش اصلی انتشار Emotet سایت‌های تسخیر شده‌ای است که گردانندگان این بدافزار کد مخرب را به صفحات آنها تزریق کرده‌اند. قربانیان نیز از طریق هرزنامه‌هایی (Spam) با پیوست فایل Office که در آن ماکروی مخرب جاسازی شده به این سایت‌ها هدایت شده و در آنجا دستگاه به Emotet آلوده می‌شود. در برخی موارد نیز هرزنامه حاوی لینک‌هایی است که کلیک بر روی آنها منجر به دریافت کد مخرب از سایت‌های مذکور می‌شود.

بنابراین کد تزریق شده در این سایت‌ها نقشی اساسی در فرایند آلودگی داشته و جایگزینی آن به موارد بی‌خطری همچون این فایل‌های GIF عملاً شبکه توزیع بدافزار را از کار می‌اندازد.

دو نمونه از سایت‌هایی که در آنها تصویر مورد نظر هکر جایگزین کد مخرب شده در زیر قابل مشاهده است.



بدین‌ترتیب، کلیک بر روی لینک درون هرزنامه یا اجرای فایل پیوست آن، بجای آنکه منجر به آلودگی دستگاه به Emotet شود موجب دانلود تصویر مورد نظر هکر می‌شود.

در نتیجه این اقدامات به نظر می‌رسد که گردانندگان Emotet، توزیع هرزنامه‌های خود را متوقف کرده‌اند. موضوعی که سبب محبوبیت این هکر نزد برخی محققان شده و عده‌ای او را شوالیه سفید خطاب کرده‌اند!

گردانندگان Emotet از شل‌های وب (Web Shell) برای مدیریت کدهای مخرب خود در سایت‌های هک شده استفاده می‌کنند. احتمال می‌رود که هکر با کشف رمز عبور این شل‌ها موفق به تغییر کدها شده باشد.

Emotet، یک بدافزار پیشرفته بانکی است که ساختاری پیمانه‌ای (Modular) و عملکردی کرم‌گونه (Worm) دارد. Emotet را می‌توان بدافزاری چندشکلی (Polymorphic) دانست که ضدویروس‌های سنتی مبتنی بر امضا را در برابر خود ناتوان می‌کند. این بدافزار با رویکرد پیمانه‌ای و در قالب فایل‌های DLL به‌طور پیوسته قابلیت‌های خود را به‌روز می‌کند. علاوه بر آن، Emotet مجهز به تکنیک‌های ضدتحلیلی نظیر ضدماشین مجازی است. بستری که بسیاری از تحلیلگران ویروس از آنها برای کالبدشکافی بدافزارها استفاده می‌کنند.

اگر چه شبکه توزیع این بدافزار مخرب دچار اختلالاتی جدی شده اما انتظار می‌رود که به‌زودی فعالیت آن از سرگرفته 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 تهدیداتی همچون بدافزار بانکی Emotet دارد.

Silence؛
نفوذگرانی حریص اما صبور

کارزارهای اجرا شده توسط گروه Silence را می‌توان از جمله مخرب‌ترین تهدیدات موسوم به پیشرفته و مستمر (APT) در سال‌های اخیر دانست. این گروه منتسب به مهاجمان روسی، اجرای کارزارهای موفق بر ضد بانک‌ها و مؤسسات مالی و سرقت میلیون‌ها دلار از آنها را در کارنامه دارد.

اگر چه تمرکز اصلی Silence بر روی کشورهای عضو اتحاد جماهیر شوروی سابق است اما نمونه‌های مختلفی مبنی بر نفوذ این گروه به شبکه بانک‌ها در دیگر کشورهای جهان نیز گزارش شده است.

به گزارش شرکت مهندسی شبکه گستر، این مهاجمان با در اختیار گرفتن کنترل دستگاه‌های خودپرداز، اقدام به سرقت پول از آنها می‌کنند.

در اکثر این کارزارها، گردانندگان Silence با بکارگیری ترفندهای مهندسی اجتماعی و ارسال ایمیل‌های فیشینگ اختصاصی و هدفمند، کارکنان بانک را هدف قرار می‌دهند.

عنوان و متن معمولاً مفصل و طولانی این ایمیل‌ها و دامنه مورد استفاده در ارسال آنها همگی القا کننده معتبر بودن آنهاست. در ایمیل‌های ارسالی دامنه‌هایی به چشم می‌خورد که بانک‌های صاحب آنها از پودمان‌هایی همچون Sender Policy Framework - به اختصار SPF - و Domain-based Message Authentication, Reporting and Conformance - به اختصار DMARC - جهت حفاظتشان استفاده نکرده‌اند.

برای عبور از سد محصولات ضدهرزنامه بسیاری از این ایمیل‌ها مجهز به گواهینامه‌های موسوم به Self-signed هستند.

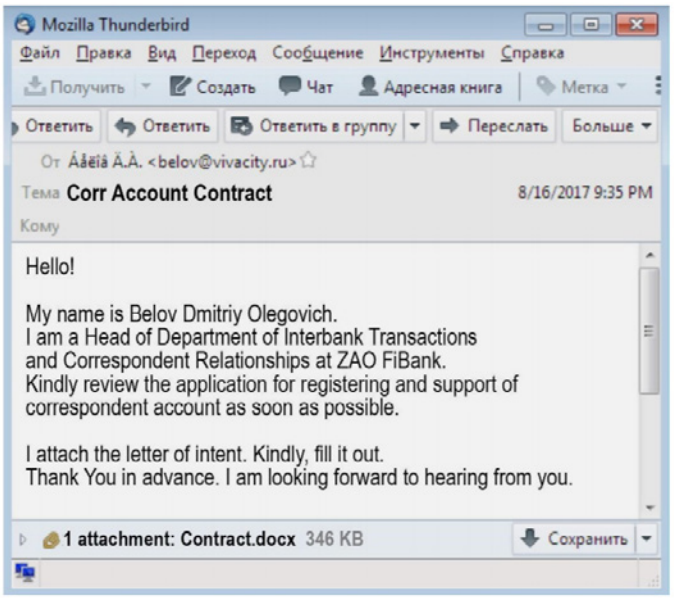
پیوست ایمیل‌های ارسالی، اسناد Word حاوی ماکروی مخرب یا مجهز به بهره‌جوی (Exploit) یک یا تعدادی از آسیب‌پذیری‌های زیر است:

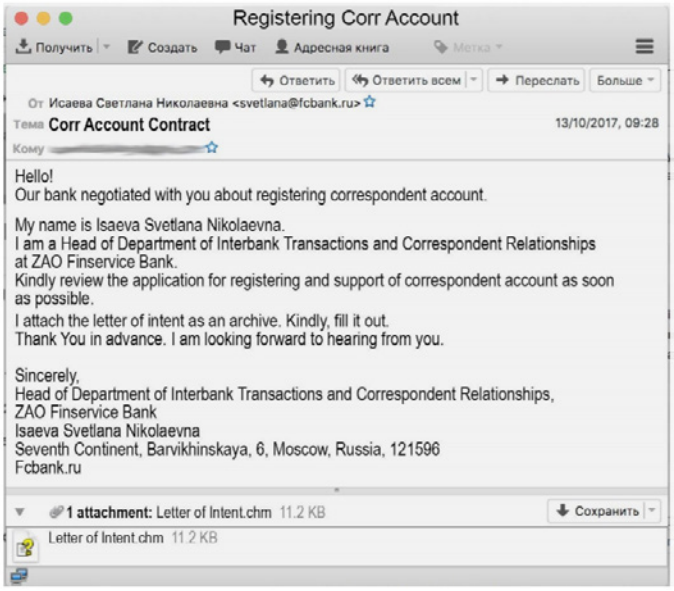
- CVE-2017-0199 - ضعفی در نرم‌افزارهای Office و WordPad که در فروردین سال ۹۶ توسط مایکروسافت ترمیم و اصلاح شد.
- CVE-2017-0262 - این اشکال مرتبط با آسیب‌پذیری Encapsulated PostScript در محصول Office است که در ۱۹ اردیبهشت ۹۶ ترمیم شد.
- CVE-2017-11882 - ضعفی در مجموعه نرم‌افزارهای Office که در ۲۳ آبان ۹۶، مایکروسافت آن را برطرف کرد.
- CVE-2018-0802 - ضعفی در بخش Equation Editor برنامه WordPad و مجموعه‌نرم‌افزاری Office است که در ۱۹ دی ۹۶ ترمیم و اصلاح شد.

- CVE-2018-8174 - این آسیب‌پذیری معروف به Double Kill مربوط به بخش مدیریت‌کننده اسکریپت‌های مبتنی بر Visual Basic در مرورگر Internet Explorer و مجموعه نرم‌افزاری Office است که در اردیبهشت ۹۷ توسط مایکروسافت ترمیم شد.

در مواردی نیز پیوست ایمیل‌ها، فایل‌های غیرمتداول CHM، اسکریپت‌های JS یا میانبرهای LNK بوده است.

نمونه هایی از این ایمیل ها در تصاویر زیر قابل مشاهده است:





در صورت به دام افتادن قربانی و اجرای فایل پیوست ایمیل، بدافزار Silence.Downloader (که با نام TrueBot نیز شناخته می‌شود) بر روی دستگاه نصب و در ادامه از طریق آن کد مخرب اصلی با عنوان Silence.Main از سرور فرماندهی (C2) دریافت و اجرا می‌شود. در مواردی این فرایند در قالب موسوم به Fileless بوده و Ivoke که یک دریافت‌کننده (Download) مبتنی بر PowerShell است بر روی دستگاه اجرا می‌شود.

با استقرار Silence.Main دستگاه به تسخیر مهاجمان در آمده و سپس با استفاده از ابزارهای زیر امکان برقراری ارتباط با سرور فرماندهی فراهم می‌شود:

- EDA - ابزاری مبتنی بر PowerShell است که با اجرای فرامین موسوم به Command Shell اقدام به ایجاد ترافیک در بستر پودمان DNS می‌کند. این ابزار بر پایه پروژه‌های Empire و dnscat2 توسعه داده شده است.
- ProxyBot - بدافزاری است که در قالب پراکسی ارتباط میان دستگاه و سرور فرماندهی را برقرار می‌سازد.

مهاجمان برای مدتی با صبورانه و به آرامی با تصویربرداری و ضبط ویدئو اقدام به استخراج اطلاعات و یادگیری روش کار در بانک قربانی می‌کنند. هدف، دستیابی به دستگاه‌های خودپرداز متصل به شبکه بانک و در اختیار گرفتن کنترل آنهاست.

پس از کشف هر دستگاه خودپرداز در شبکه، نفوذگران از بدافزار Atmosphere برای کنترل فرایند خروج پول از دستگاه بهره می‌گیرند.

این مهاجمان، مبالغ را از طرق مختلفی از دستگاه خودپرداز برداشت می‌کنند. از جمله، برداشت، توسط افراد اجیرشده که اصطلاحاً به آنها قاطر پول (Mule) گفته می‌شود. در یکی از این نمونه‌ها تصاویر دوربین‌های مدار بسته نشان می‌دهد که قاطر پول پیش از برداشت، اقدام به برقراری یک تماس تلفنی می‌کند. پس از هر تماس، فرمانی به دستگاه ارسال می‌گردد که موجب خروج پول از آن می‌شود. تصاویر زیر افرادی را نشان می‌دهند که در جریان حمله گروه Silence به بانک Dutch-Bangla در کشور بنگلادش نقش قاطر پول را ایفا کرده بودند.

تنها در حمله به یکی از بانک‌ها، مهاجمان موفق به سرقت ۳ میلیون دلار از آن شدند.

بررسی کد بدافزارها و ابزارهای مورد استفاده این گروه، از روسی‌زبان بودن گردانندگان Silence حکایت دارد.

متأسفانه این اخبار مانند فیلم‌های جیمزباندی تخیلی نیستند. این‌گونه حملات می‌تواند هشداری باشد به تمامی مؤسسات مالی و بانکی داخل کشور که علاوه بر بکارگیری نرم‌افزارها و تجهیزات امنیتی به‌روز، آموزش کارکنان را نیز مدنظر قرار دهند.

بدافزارهای مورد استفاده توسط Silence که در این گزارش به آنها پرداخته شده با نام‌های زیر قابل شناسایی هستند:

Bitdefender

- Application.Agent.HEE
- Backdoor.IRCBot.ADDS
- Exploit.MathType.Gen
- Gen:Heur.Jatommy.03110.aaW@baaaa
- Gen:Heur.Rocket.34
- Gen:Trojan.Heur.FU.buW@aq1hr4pi
- Gen:Trojan.Heur.JP.du0@aOfZpooi

- Gen:Variant.Fugrafa.1213
- Gen:Variant.Graftor.438258
- Gen:Variant.Jaik.20815
- Gen:Variant.MSILPerseus.182404
- Gen:Variant.MSILPerseus.189429
- Gen:Variant.Razy.500923
- Gen:Variant.Ursu.145423
- Gen:Variant.Ursu.233211
- Gen:Variant.Ursu.271418
- Gen:Variant.Zusy.251163
- Heur.BZC.YAX.Pantera.41.1899AC21
- JS:Trojan.JS.Downloader.ICY
- Trojan.Agent.CPPU
- Trojan.Agent.DOYJ
- Trojan.Autoruns.GenericKD.32465581
- Trojan.Autoruns.GenericKD.32526694
- Trojan.Autoruns.GenericKD.32583401
- Trojan.Downloader.Agent.ABXP
- Trojan.Generic.17914340
- Trojan.Generic.22540869
- Trojan.Generic.22908275
- Trojan.GenericKD.12126506
- Trojan.GenericKD.12133159
- Trojan.GenericKD.12141262
- Trojan.GenericKD.12198989
- Trojan.GenericKD.12480214
- Trojan.GenericKD.12606212
- Trojan.GenericKD.30454344
- Trojan.GenericKD.30465821
- Trojan.GenericKD.30606184
- Trojan.GenericKD.30606185
- Trojan.GenericKD.30620651
- Trojan.GenericKD.30621779
- Trojan.GenericKD.31289198
- Trojan.GenericKD.31549093
- Trojan.GenericKD.31723635
- Trojan.GenericKD.31760362
- Trojan.GenericKD.31851910
- Trojan.GenericKD.32037056
- Trojan.GenericKD.32081547
- Trojan.GenericKD.3418739
- Trojan.GenericKD.40398265
- Trojan.GenericKD.40712627

- Trojan.GenericKD.40764403
- Trojan.GenericKD.40893139
- Trojan.GenericKD.41082140
- Trojan.GenericKD.41176627
- Trojan.GenericKD.41493200
- Trojan.GenericKD.41618477
- Trojan.GenericKD.41624618
- Trojan.GenericKD.4895752
- Trojan.GenericKD.4898015
- Trojan.GenericKD.4900915
- Trojan.GenericKD.5360752
- Trojan.GenericKD.5385760
- Trojan.GenericKD.5622506
- Trojan.GenericKD.5622569
- Trojan.GenericKD.5810339
- Trojan.GenericKD.5810636
- Trojan.GenericKD.5811135
- Trojan.GenericKD.5812661
- Trojan.GenericKD.5841179
- Trojan.GenericKD.5854428
- Trojan.GenericKD.5854455
- Trojan.GenericKD.6028156
- Trojan.GenericKD.6175857
- Trojan.RansomKD.6254744
- W97M.Agent.GY

McAfee

- Agent-FGR!86EA1F46DF74
- Artemis!13CC98FCB654
- Artemis!43EDA1810677
- Artemis!7D3614DF9409
- Artemis!9596E59EA383
- Artemis!A3DE4A1E5B66
- Artemis!C4F18D40B17E
- BackDoor-FDYS!B2AD44093231
- Downloader-FBVT!47E733FD3EC2
- Exploit-CVE2015-2545
- Exploit-CVE2015-2545.l
- Exploit-CVE2015-2545.m
- Exploit-CVE2017-0199.cf
- Generic Trojan.fr
- Generic Trojan.gx
- Generic.bja

- Generic.blu
- Generic.fbe
- GenericR-LLK!121C7A3F139B
- GenericR-LLK!2FE01A04D6BE
- GenericR-LLK!88CB1BABB591
- GenericR-LLK!9B38AA473FDE
- GenericR-LLK!A6771CAFD711
- GenericRXCX-AT!9B037EAD562C
- GenericRXDI-MN!0074D8C3183E
- GenericRXDI-MN!440B21958AD0
- GenericRXDI-MN!9628D7CE2DD2
- GenericRXDI-MN!B7F971007488
- GenericRXDI-ZY!A1E210598820
- GenericRXDI-ZY!A58A830DCE46
- GenericRXEV-YM!CEFD39402D7F
- GenericRXEV-YM!D81AE5E0680D
- GenericRXFG-UY!B4313151019B
- GenericRXFG-UY!EF0FB10C602E
- GenericRXGT-CQ!81F3E843B26D
- GenericRXHE-TZ!C8D0CCD2E58C
- HTML/Downloader.aa
- HTML/Downloader.p
- HTML/Downloader.y
- JS/Agent.m
- JS/Downloader.gen.gx
- PHP/Downloader
- PS/Agent.c
- PS/Downloader!lnk.c
- RDN/GenDownloader.akk
- RDN/Generic Downloader.x
- RDN/Generic PWS.y
- RDN/Generic.ckt
- RDN/Generic.dns
- RDN/Generic.dx
- RDN/Generic.eyb
- RDN/Generic.ezg
- RDN/Generic.fpj
- RDN/Generic.frs
- Trojan-Downloader.k
- Trojan-FONO!3345DDE0C827
- Trojan-FONO!404D69C8B74D
- Trojan-FONO!B09B8BE361CD
- Trojan-FONO!C6C84DA4F271

- Trojan-FOOK!B43F65492F2F
- Trojan-FOOK!CFFFC5A0E5BD
- Trojan-FOOK!DD74FCFA1A98
- Trojan-FQCU!7D8AF1F6CF7D
- Trojan-FQOZ!3FF094C23E3E
- Trojan-FQOZ!50565C4B80F4
- Trojan-FQOZ!8191DAE4BDED
- Trojan-Silence
- Trojan-Silence!chm
- Trojan-Silence!lnk
- VBS/Agent.dm
- VBS/Downloader.fa
- W97M/Downloader.ps
- W97M/Silence

Sophos

- Install Monster (PUA)
- JS/Dwnldr-WAX
- Mal/DownLnk-D
- Mal/Generic-S
- Perl/Agent-BCMX
- PHP/Flood-JJ
- Troj/20152545-K
- Troj/Agent-AWNF
- Troj/Agent-AXIU
- Troj/Agent-AXPA
- Troj/Agent-AXPB
- Troj/Agent-AZSL
- Troj/Agent-BBVF
- Troj/Agent-BCLI
- Troj/Agent-BCLK
- Troj/Agent-BCLL
- Troj/Agent-BCLM
- Troj/Agent-BCLQ
- Troj/ATM-B
- Troj/ATMRip-B
- Troj/ChmDldr-M
- Troj/CHMDl-I
- Troj/CHMDl-J
- Troj/Delf-HEX
- Troj/Delf-HFB
- Troj/Delf-HFD
- Troj/Delf-HFE

- Troj/Dloadr-EDI
- Troj/DocDl-ISO
- Troj/DocDl-UJF
- Troj/DocDl-VLK
- Troj/DwnLdr-YRW
- Troj/DwnLdr-YRX
- Troj/DwnLdr-YSP
- Troj/HTMLDl-IS
- Troj/LnkDldr-AP
- Troj/MSIL-LSZ
- Troj/MSIL-MRY
- Troj/MSIL-MSK
- Troj/PS-Y
- Troj/RTFDldr-VY
- Troj/Truebot-A
- Troj/Truebot-B
- VBS/DwnLdr-YRQ

لازم به ذکر است که در این گونه کارزارهای هدفمند، مهاجمان، در هر حمله، معمولاً از بدافزارهای خاص، با امضایی متفاوت از نمونه‌های قبلی بهره می‌گیرند. لذا استفاده از راهکارهای پیشرفته‌ای همچون McAfee Threat Intelligence Exchange جهت شناسایی نمونه‌های جدید و ناشناخته می‌تواند نقشی اساسی در کشف زودهنگام این حملات هدفمند داشته باشد.

باز هم افشای اطلاعات
در پی حمله باج‌افزاری

گردانندگان باج‌افزار Nefilim در حال انتشار عمومی فایل‌هایی هستند که در جریان حمله اخیر به یکی از زیرمجموعه‌های شرکت معروف Dussmann Group اقدام به سرقت آنها کرده بودند.

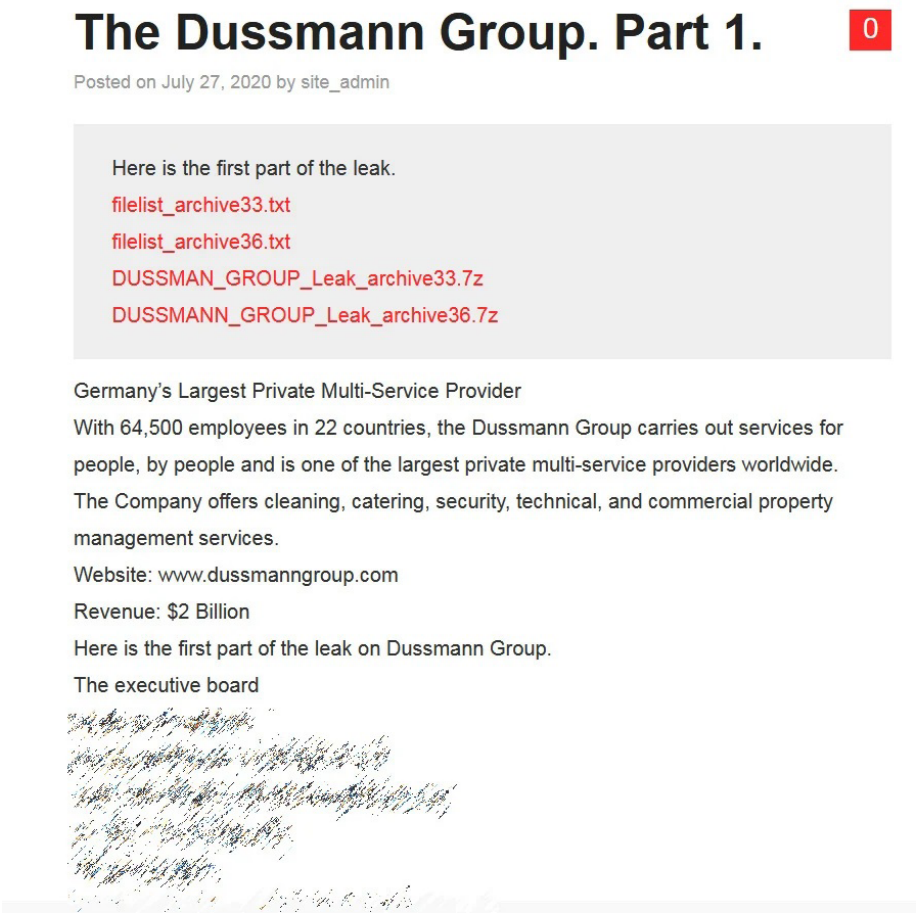
Dussmann Group یکی از بزرگ‌ترین شرکت‌های خصوصی آلمان است که با بیش از ۶۴ هزار کارمند در بیش از ۲۰ کشور جهان، در حوزه‌های مختلف مشغول به فعالیت است.

Dussmann Group تایید کرده که به‌تازگی از یکی از زیرمجموعه‌های این شرکت عظیم با نام Dresdner K-hlanlagenbau GmbH - به اختصار DKA - هدف یک حمله باج‌افزاری قرار گرفته است.

در جریان حمله مذکور، گردانندگان Nefilim ادعا کردند که پیش از رمزگذاری فایل‌ها اقدام به سرقت آنها کرده بودند.

مهاجمان با تهدید به انتشار عمومی این فایل‌ها و اکنون افشای بخشی از آنها در تلاش هستند که مسئولان DKA را متقاعد به پرداخت مبلغ اخاذی شده کنند.

به گزارش شرکت مهندسی شبکه گستر، تا زمان انتشار این خبر مهاجمان ۱۴ گیگابایت از این فایل‌های سرقتی را با توضیحات زیر منتشر کرده‌اند.



The Dussmann Group. Part 1.

0

Posted on July 27, 2020 by site_admin

Here is the first part of the leak.
filelist_archive33.txt
filelist_archive36.txt
DUSSMAN_GROUP_Leak_archive33.7z
DUSSMANN_GROUP_Leak_archive36.7z

Germany's Largest Private Multi-Service Provider
With 64,500 employees in 22 countries, the Dussmann Group carries out services for people, by people and is one of the largest private multi-service providers worldwide. The Company offers cleaning, catering, security, technical, and commercial property management services.
Website: www.dussmanngroup.com
Revenue: $2 Billion
Here is the first part of the leak on Dussmann Group.
The executive board

مستندات Word، تصاویر، اسناد حسابداری و نقشه‌های AutoCAD از جمله این فایل‌های افشا شده هستند.

DKA نشت فایل‌های متعلق به این شرکت را تایید کرده است.

این شرکت اعلام کرده در جریان حمله مذکور دستگاه ۵۷۰ نفر از کارکنان آن هدف باج‌افزار قرار گرفت. همچنین گفته که در ارتباط نزدیک با نهادهای قانونی و متخصصان امنیتی است و کارکنان و مشتریانش را از این حمله سایبری مطلع کرده است.

گردانندگان Nefilim مدعی هستند ۲۰۰ گیگابایت از اطلاعات DKA را در اختیار دارند.

هنوز مشخص نیست که مهاجمان چگونه موفق به دستیابی به شبکه Nefilim شده بودند.

متأسفانه در ماه‌های اخیر نمونه‌های متعددی از نشت اطلاعات در پی اجرای حملات باج‌افزاری گزارش شده 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، 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.

درآمد ۲۵ میلیون دلاری مهاجمان NetWalker
در کمتر از ۶ ماه

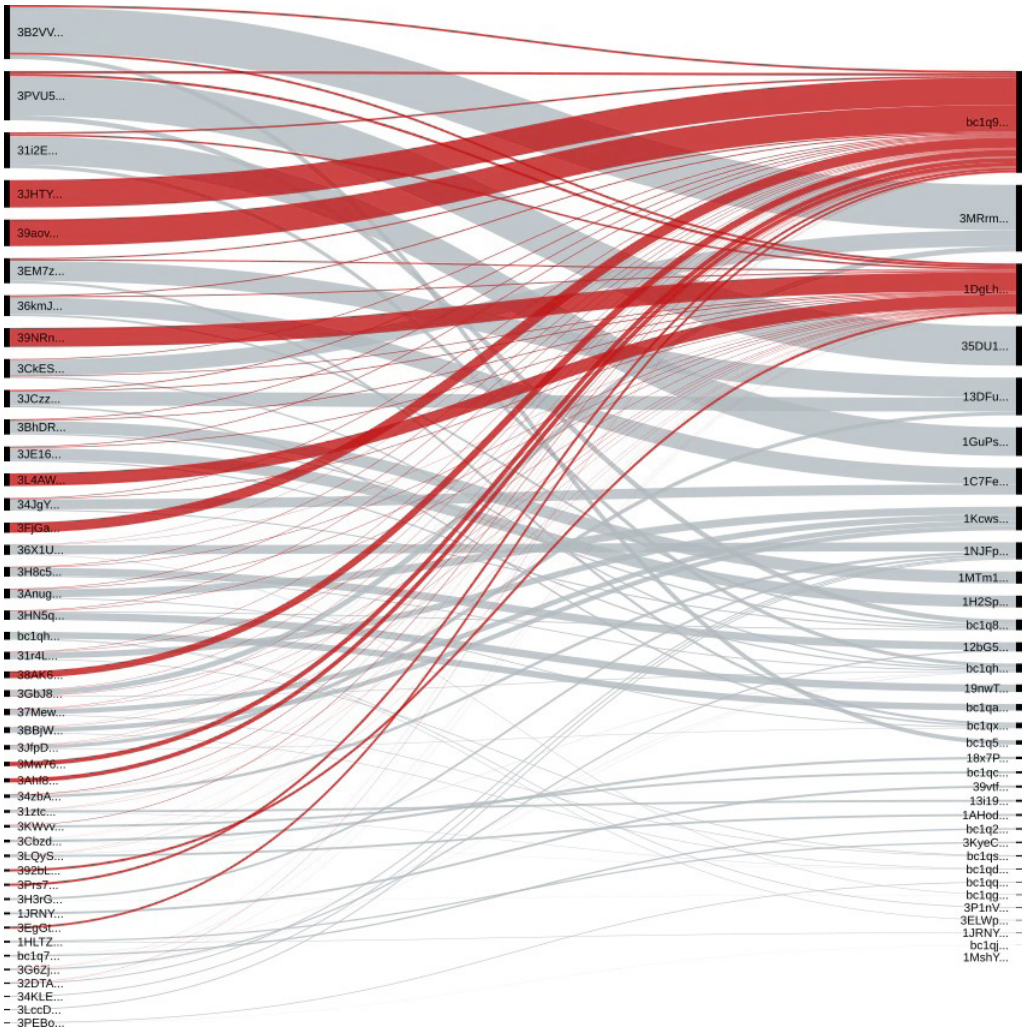
بر طبق گزارشی که شرکت امنیتی مک‌آفی آن را منتشر کرده گردانندگان باج‌افزار NetWalker از ماه مارس سال میلادی جاری موفق به دریافت حداقل ۲۵ میلیون دلار از قربانیان خود شده‌اند.

NetWalker خانواده‌ای از باج‌افزارهاست که در آگوست ۲۰۱۹ ظهور کرد. اگر چه اولین نسخ آن تحت عنوان Mailto فعالیت می‌کردند اما خیلی زود، از اواخر ۲۰۱۹ به NetWalker تغییر نام پیدا کرد.

تصویر زیر میزان شیوع این باج‌افزار را در نقاط مختلف جهان بر اساس آمار مک‌آفی نشان می‌دهد.

همانطور که در تصویر بالا نمایش داده شده ایران نیز در فهرست اهداف اصلی NetWalker قرار دارد.

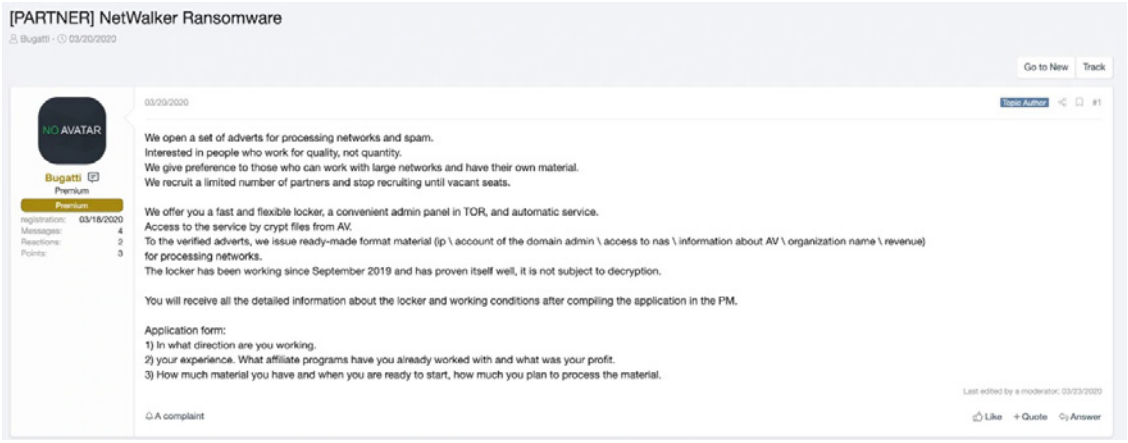
بخش تحقیقات پیشرفته تهدیدات شرکت مک‌آفی که به تازگی گزارش جامعی در خصوص عملیات‌های NetWalker منتشر کرده با رصد نشانی‌های بیت‌کوین مرتبط با مهاجمان این باج‌افزار اعلام کرده که تنها در کمتر از شش ماه گذشته قربانیان بیش از ۲۵ میلیون دلار به مهاجمان پرداخت کرده‌اند.



این تخمین یکی از مطرح‌ترین شرکت‌های امنیتی دنیا، NetWalker را در کنار باج‌افزارهای معروفی همچون Ryuk،و Dharma و Revil - که با نام Sodinokibi نیز شناخته می‌شود - قرار می‌دهد.

گردانندگان NetWalker امکان استفاده از آن را در قالب خدمات موسوم به "باج‌افزار به‌عنوان سرویس" (Ransomware-as-a-Service - به اختصار RaaS) برای سایر مهاجمان به ویژه هکرهای روسی‌زبان فراهم کرده‌اند.

همچنین به تازگی این افراد با تبلیغ در تالارهای گفتگو در تلاشند تا مهاجمان باتجربه و مجهز به منابع لازم برای رخنه به شبکه‌های بزرگ را جذب کرده و از آنها در اجرای حملات هدفمند کمک بگیرند.



ظاهراً نویسندگان NetWalker همچون برخی دیگر از هم‌قطاران حرفه‌ای خود به این نتیجه رسیده‌اند که تمرکز بر روی سازمان‌های بزرگ و اخاذی هنگفت از آنها سودمندتر از انتشار انبوه باج‌افزار و باج‌گیری مبالغ به مراتب کم از قربانیان عادی است.

از جمله روش‌های رخنه اولیه مهاجمان NetWalker به شبکه که در گزارش مک‌آفی به آن اشاره شده می‌توان به موارد زیر اشاره کرد:

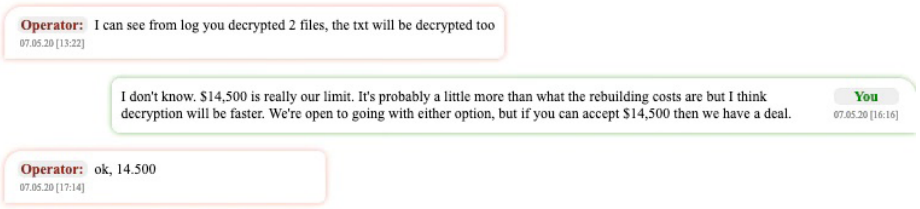
- بهره‌جویی (Exploit) از آسیب‌پذیری‌های امنیتی در سرویس‌هایی همچون Tomcat و WebLogic که در بستر اینترنت قابل دسترس هستند.
- اجرای حملات فیشینگ هدفمند (Spear Phishing) بر ضد حداقل یکی از کارکنان سازمان
- سوءاستفاده از پودمان Remote Desktop Protocol - به اختصار RDP

FBI نیز در هشداری از بهره‌جویی مهاجمان NetWalker از آسیب‌پذیری CVE-201911510 در سرورهای Pulse Secure VPN و CVE-2019-18935 در Telerik UI خبر داده است.

به گزارش شرکت مهندسی شبکه گستر به نقل از شرکت مک‌آفی، این افراد در جریان گسترش آلودگی در سطح شبکه، از آسیب‌پذیری‌های CVE-2020-0796، CVE-2019-1458، CVE-2017-0213 و CVE-2015-1701 برای ترفیع سطح دسترسی (Elevation of Privilege) خود استفاده می‌کنند.

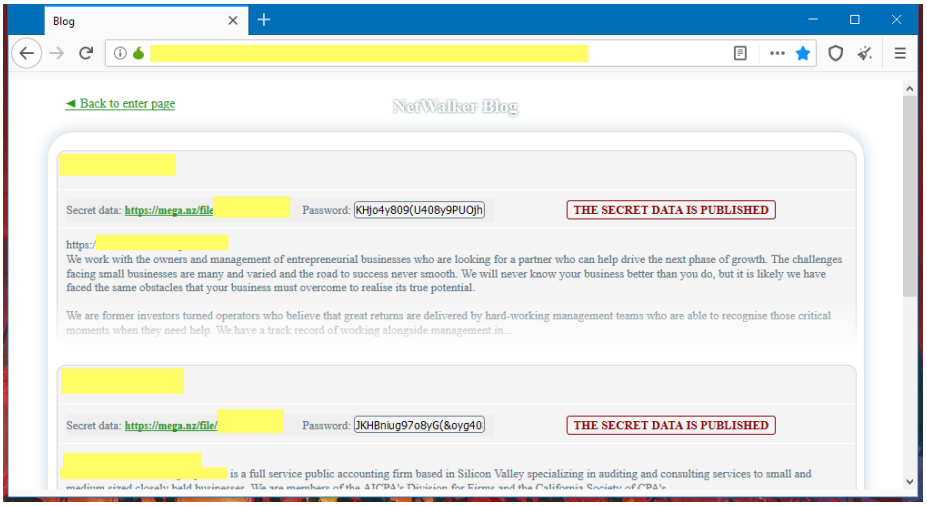
در حالی که تا قبل از ماه مارس سال میلادی جاری، روش برقراری ارتباط با مهاجمان، ایمیل‌های درج شده در فایل‌های موسوم به اطلاعیه باج‌گیری (Ransom Note) بود اکنون مدتی است قربانی برای اطلاع از روش پرداخت باج، به سایت اختصاصی NetWalker در شبکه ناشناس TOR هدایت می‌شود.

نمونه‌ای از مکاتبات صورت گرفته با گردانندگان این باج‌افزار در تصویر زیر قابل مشاهده است.

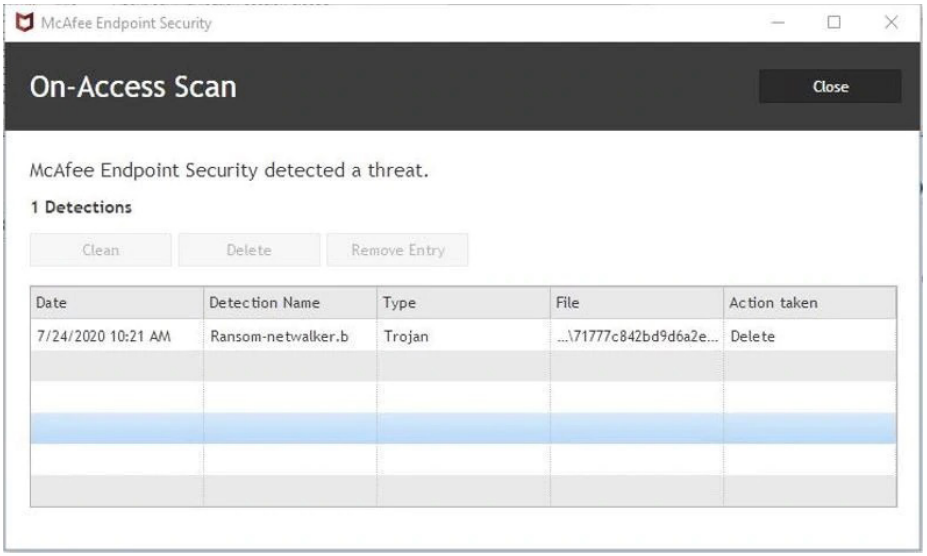


مانطور که پیداست مهاجمان حاضر به دادن تخفیف ۱۰ درصدی در صورت پرداخت باج ظرف ۷ روز شده‌اند.

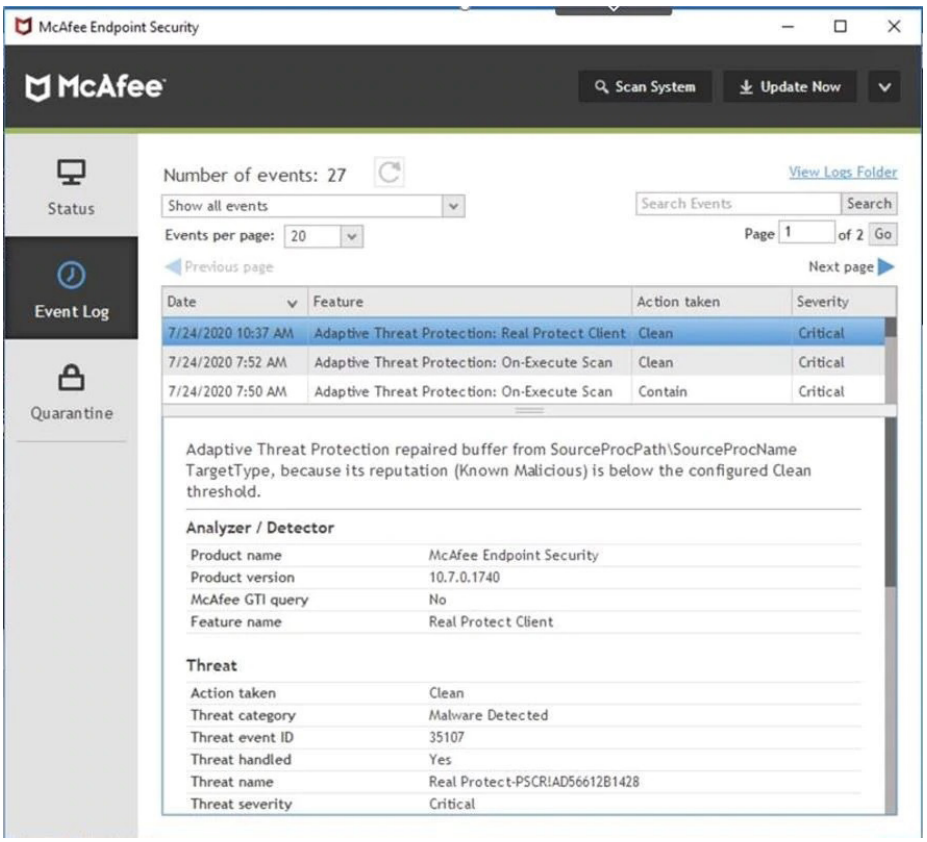
نکته نگران‌کننده اینکه مهاجمان نام و اطلاعات قربانیانی را که از پرداخت باج خودداری می‌کنند افشا می‌کنند. در حقیقت پس از دسترسی یافتن به سیستم‌ها ابتدا داده‌های حساس را سرقت کرده و سپس اقدام به رمزگذاری فایل‌ها می‌کنند. اگر سازمان در جریان مذاکره از پرداخت باج خودداری کند مهاجمان در سایت موسوم به Leak Portal خود نام آن را افشا کرده و شمارش معکوس برای نشت اطلاعات آغاز می‌شود. در صورت عدم پرداخت باج در مهلت مقرر اطلاعات سرقت شده از شبکه قربانی منتشر می‌شود.



فن‌آوری‌های نسخه 10.7 نرم‌افزار McAfee Endpoint Security قادر به شناسایی و مقابله با این باج‌افزار و فایل‌های مرتبط با آن هستند.



سازوکارهای یادگیری ماشین و حفاظت مبتنی بر رفتار McAfee Endpoint Security با شناسایی تکنیک‌ها و بهره‌جوهای جدید دامنه فعالیت این نوع تهدیدات را کاهش می‌دهند.



مک‌آفی NetWalker و فایل‌های مرتبط با آن را با نام‌های زیر شناسایی می‌کند:

- Artemis!0FF0D5085F7E
- Artemis!1527DAF8626C
- Artemis!2F96F8098A29
- Artemis!2F96F8098A29
- Artemis!50C6B1B805EC
- Artemis!BC96C744BD66
- Artemis!F5C877335920
- Generic .kk
- GenericRXKD-DA!01F703234047
- GenericRXKD-DA!0537D845BA09
- GenericRXKD-DA!0CBA10DF0C89
- GenericRXKD-DA!0E611C6FA27A
- GenericRXKD-DA!0FF5949ED496
- GenericRXKD-DA!18C32583A6FE
- GenericRXKD-DA!2B0384BE06D2
- GenericRXKD-DA!3F3CC36F4298
- GenericRXKD-DA!4E59FBA21C5E
- GenericRXKD-DA!59B00F607A75
- GenericRXKD-DA!5ABF6ED342FD

- GenericRXKD-DA!5CE75526A25C
- GenericRXKD-DA!5F55AC3DD189
- GenericRXKD-DA!608AC26EA80C
- GenericRXKD-DA!63EB7712D7C9
- GenericRXKD-DA!645C720FF0EB
- GenericRXKD-DA!6A64553DA499
- GenericRXKD-DA!729928E6FD6A
- GenericRXKD-DA!8102821249E1
- GenericRXKD-DA!9001DFA8D69D
- GenericRXKD-DA!9172586C2F87
- GenericRXKD-DA!ADDC865F6169
- GenericRXKD-DA!B4F8572D4500
- GenericRXKD-DA!B862EBC24355
- GenericRXKD-DA!BC75859695F6
- GenericRXKD-DA!BDC345B7BCEC
- GenericRXKD-DA!C0DDA75C6EAE
- GenericRXKD-DA!D09CFDA29F17
- GenericRXKD-DA!DBDD7A1F53AA
- GenericRXKD-DA!DD4F9213BA67
- GenericRXKD-DA!DE0B8566636D
- GenericRXKD-DA!F0CC568491CD
- GenericRXKD-DA!F957F19CD9D7
- GenericRXKD-DA!FCEDEA8111AB
- GenericRXKU-HO!187417F65AFB
- GenericRXKU-HO!1DB8C7DEA2F7
- GenericRXKU-HO!961942A472C2
- GenericRXKU-HO!997F0EC7FCFA
- GenericRXKU-HO!9FB87AC9C00E
- GenericRXKU-HO!DE61B852CADA
- GenericRXKU-HO!E33E060DA1A5
- PS/Agent.bu
- PS/Agent.bu
- PS/Agent.bx
- PS/Agent.bx
- PS/Netwalker.a
- PS/Netwalker.b
- PS/Netwalker.b
- PS/Netwalker.c
- PS/Netwalker.c
- PS/Netwalker.d
- Ransom-CWall!3D6203DF53FC
- Ransom-CWall!993B73D6490B
- Ransom-Mailto!D60D91C24570
- Ransom-NetW!1B6A2BFA39BC

- Ransom-NetW!291E1CE9CD3E
- Ransom-NetW!2E2F5FE8ABA4
- Ransom-NetW!3A601EE68000
- Ransom-NetW!62C71449FBAA
- Ransom-NetW!7B77B436360A
- Ransom-NetW!8E310318B1B5
- Ransom-NetW!A0BC1AFED896
- Ransom-NetW!A9E395E478D0
- Ransom-NetW!AB8D59ABA3DC
- Ransom-NetW!BDE3EC20E9F8
- Ransom-NetW!BFF6F7B3A7DB
- Ransom-Netwalker
- RDN/Generic.dx
- RDN/Ransom

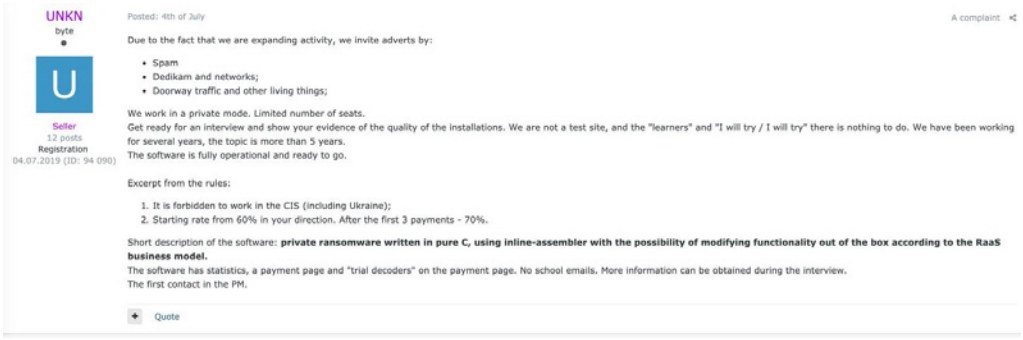
مشروح گزارش مک‌آفی در اینجا قابل دریافت و مطالعه است.

ابزار همه‌کاره Dharam
برای مشترکین این باج‌افزار

بر اساس گزارشی که شرکت امنیتی سوفوس آن را منتشر کرده، نویسندگان باج‌افزار Dharam به مشترکین خدمات موسوم به "باج‌افزار به عنوان سرویس" (Ransomware-as-a-Service - به اختصار RaaS) ابزاری را ارائه می‌کنند که آنها را قادر به اجرای تقریباً هر عملیات مخرب در شبکه قربانی می‌کند.

در RaaS، صاحب باج‌افزار، فایل مخرب را به‌عنوان یک خدمت به متقاضی اجاره می‌دهد. متقاضی که ممکن است تخصصی چندان بالایی نیز نداشته باشد تنها وظیفه انتشار باج‌افزار را برعهده دارد. معمولاً در این خدمات ۳۰ تا ۴۰ درصد مبلغ اخاذی‌شده به نویسنده باج‌افزار و باقی آن به مشترک که آلوده‌سازی دستگاه قربانی را عهده‌دار بوده می‌رسد.

به گزارش شرکت مهندسی شبکه گستر، بسیاری از نویسندگانی که سازمان‌ها را مورد هدف باج‌افزارهای خود قرار می‌دهند ارائه خدمات RaaS را محدود به هکرها و مهاجمان گزینش شده و مورد تایید می‌کنند. برای مثال در REvil از متقاضی RaaS، توسط گردانندگان این باج‌افزار مصاحبه به‌عمل آمده و تنها در صورت اثبات داشتن تجربه و تخصص لازم با درخواست او موافقت می‌شود (تصویر زیر).


UNKN
byte
Seller
12 posts
Registration
04.07.2019 (ID: 94 090)

Posted: 4th of July

A complaint

Due to the fact that we are expanding activity, we invite adverts by:

- Spam
- Dedikam and networks;
- Doorway traffic and other living things;

We work in a private mode. Limited number of seats.
Get ready for an interview and show your evidence of the quality of the installations. We are not a test site, and the "learners" and "I will try / I will try" there is nothing to do. We have been working for several years, the topic is more than 5 years.
The software is fully operational and ready to go.

Excerpt from the rules:

1. It is forbidden to work in the CIS (including Ukraine);
2. Starting rate from 60% in your direction. After the first 3 payments - 70%.

Short description of the software: **private ransomware written in pure C, using inline-assembler with the possibility of modifying functionality out of the box according to the RaaS business model.**
The software has statistics, a payment page and "trial decoders" on the payment page. No school emails. More information can be obtained during the interview.
The first contact in the PM.

Quote

اما نویسندگان Dharma در رویکردی متفاوت، نسبت به متقاضیان RaaS سخت‌گیر نیستند.

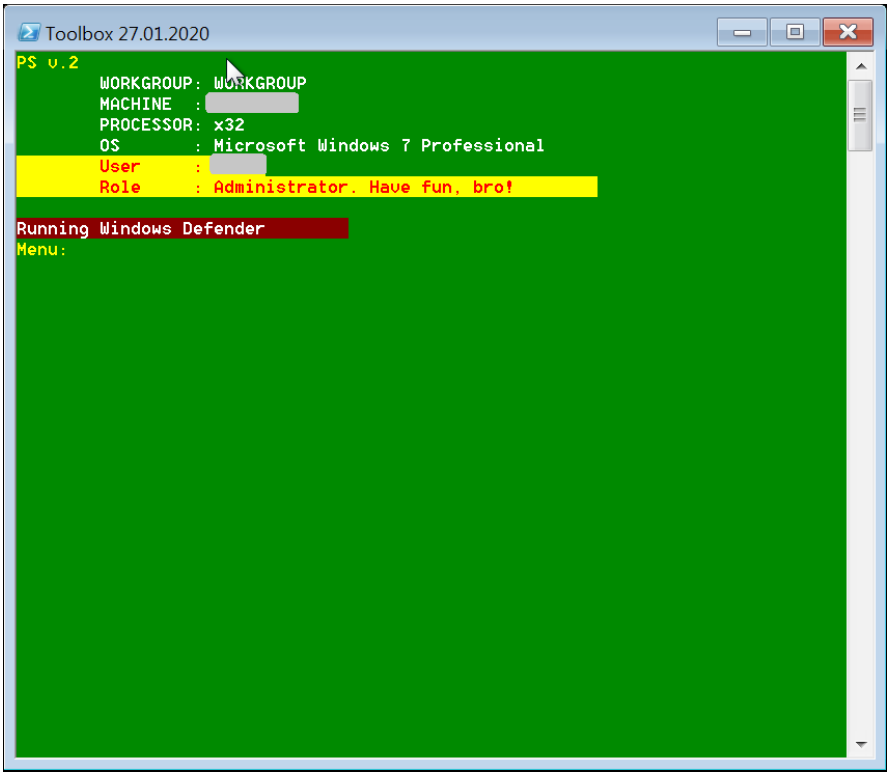
Dharma که با نام CrySis نیز شناخته می شود یکی از قدیمی‌ترین باج‌افزارهایی است که همچنان در حال فعالیت است.
در سال ۱۳۹۵، در یک اقدام عجیب کاربری با شناسه crss7777 کلیدهای رمزگشایی این باج‌افزار را در تالار گفتگوی CrySiS Support Topic سایت اینترنتی Bleeping Computer در قالب لینکی به یک فایل سرآیند زبان برنامه‌نویسی C به اشتراک گذاشت.

از آن زمان تاکنون Dharma حضوری نسبتاً فعال در صحنه باج‌افزارها داشته و سازمان‌های ایرانی نیز در مواردی هدف مهاجمان آن قرار گرفته‌اند.

بر خلاف بسیاری از باج‌افزارهای معروف امروزی که در جریان حمله به سازمان‌ها از قربانیان خود مبالغ هنگفت چندصدهزار دلاری را اخاذی می‌کنند میانگین باج در Dharma حدود ۹ هزار دلار است.

بر طبق تحقیق جدیدی که شرکت امنیتی سوفوس نتایج آن را منتشر کرده نویسندگان Dharma اکنون ابزاری آماده‌به‌کار در اختیار مشترکین خود قرار می‌دهند که حتی هکرهای بسیار کم‌تجربه را نیز قادر به رخنه به شبکه‌ها می‌کند.

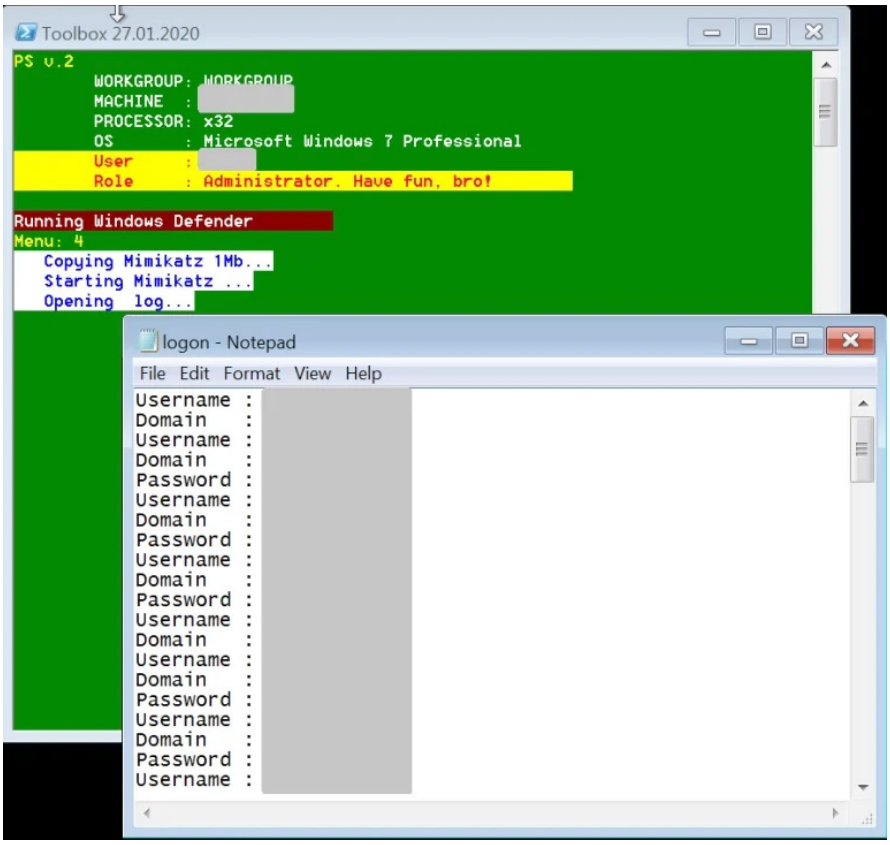
این ابزار با عنوان Toolbelt یک اسکریپت مبتنی بر PowerShell است که به‌محض اجرا امکان دریافت و اجرای ابزارهای متعدد را از یک پوشه اشتراکی موسوم به Mapped Remote Desktop به نشانی \\tsclient\e فراهم می‌کند.



در زمان اجرای ابزار، مهاجم می‌تواند تنها با وارد کردن یک عدد، یکی از ۶۲ عملیات مخرب را به دلخواه خود اجرا کند.

پس از وارد کردن شماره، ابزار فایل‌های مورد نیاز را از پوشه اشتراکی دریافت کرده و آنها را اجرا می‌کند.

Toolbelt با بهره‌گیری از ابزارهایی همچون Mimikatz برای استخراج رمزهای عبور کاربران، NirSoft Remote Desktop PassView به‌منظور سرقت اطلاعات اصالت‌سنجی پودمان RDP، Hash Suite Tools Free جهت Dump کردن درهم‌سازها (Hash) و انواع ابزارهای دیگر برای شناسایی کامپیوترها مهاجم را قادر به رخنه به دستگاه‌های متصل به شبکه و نهایتاً توزیع باج‌افزار بر روی آنها می‌کند.



با عرضه این ابزار می‌توان انتظار داشت که افراد بیشتری به جمع مهاجمان Dharma پیوسته و دامنه آلودگی‌های آن افزایش چشمگیری پیدا کند.

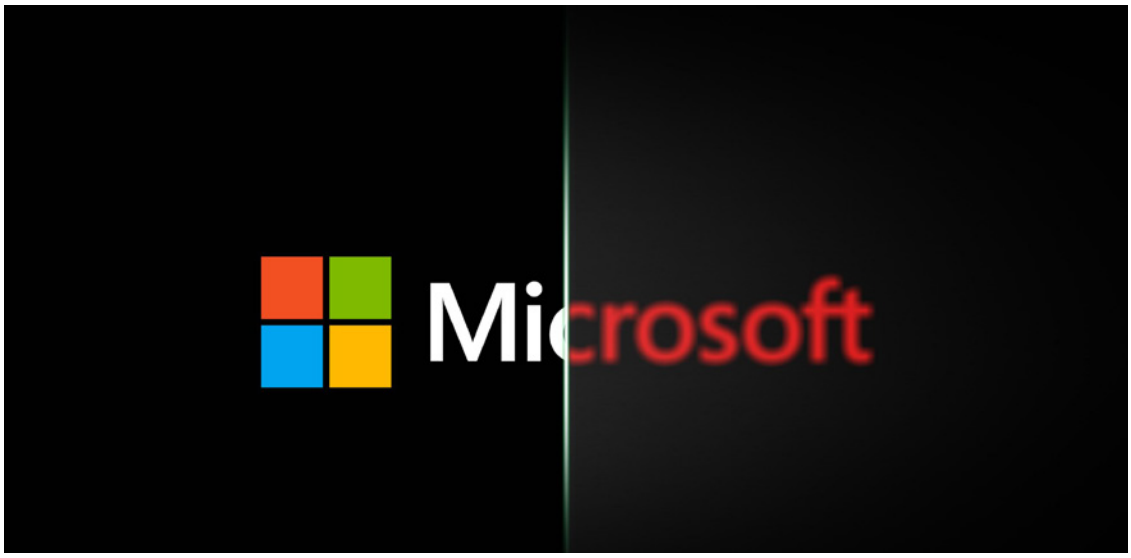
مشروح گزارش سوفوس در لینک زیر قابل دریافت و مطالعه است:

https://news.sophos.com/en-us/2020/08/12/color-by-numbers-inside-a-dharma-ransomware-as-a-service-attack/

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

اصلاحیه‌های امنیتی مایکروسافت
برای ماه میلادی آگوست



به گزارش شرکت مهندسی شبکه گستر، سه‌شنبه، ۲۱ مرداد، شرکت مایکروسافت اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی آگوست منتشر کرد. این اصلاحیه‌ها در مجموع، ۱۲۰ آسیب‌پذیری را در سیستم عامل Windows و دامنه گسترده‌ای از محصولات، سرویس‌ها و پودمان‌های این شرکت ترمیم می‌کنند.

درجه حساسیت ۱۷ مورد از آنها "حیاتی" (Critical) و ۱۰۳ مورد "مهم" (Important) اعلام شده است.

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

لازم به ذکر است که دو مورد از آسیب‌پذیری‌های ترمیم شده روز-صفر (Zero-day) بوده و به‌صورت فعال توسط مهاجمان در حال بهره‌جویی (Exploit) است. از این دو، جزییات یک مورد نیز به‌صورت عمومی افشا شده است.

CVE-2020-1380 به‌عنوان یکی از این آسیب‌پذیری‌های روز-صفر ضعفی از نوع بروز اختلال در حافظه (Memory Corruption) در بخش Scripting Engine مرورگر Internet Explorer 11 است که بهره‌جویی از آن مهاجم را قادر به اجرای کد به‌صورت از راه دور می‌کند. علاوه بر تزریق بهره‌جو در سایتی اینترنتی و هدایت کاربر به آن، مهاجم می‌تواند با جاسازی یک افزونه ActiveX با برچسب "ایمن برای اجرا شدن" (Safe for Initialization) در یک برنامه یا سند تحت Office و فریب کاربر در باز کردن آن اقدام به سوءاستفاده از این آسیب‌پذیری‌ها و اجرای کد دلخواه خود کند. به گفته مایکروسافت این آسیب‌پذیری به‌طور گسترده در حملات سایبری مورد بهره‌جویی قرار گرفته است.

بغیر از CVE-2020-1380، آسیب‌پذیری CVE-2020-1555 نیز که توسط مجموعه اصلاحیه‌های آگوست ترمیم شده بخش Scripting Engine در مرورگر Internet Explorer را تحت تأثیر قرار می‌دهد.

دومین آسیب پذیری روز-صفر این ماه با شناسه CVE-2020-1464 ضعفی از نوع جعل (Spoofing) در Windows است که مهاجم را قادر به جعل شرکت‌ها در زمان امضای دیجیتال کردن یک فایل اجرایی می‌کند.

همچنین Media Foundation بیشترین تعداد از آسیب‌پذیری‌های "حیاتی" ترمیم شده این ماه را به خود اختصاص داده است:

- CVE-2020-1379
- CVE-2020-1477
- CVE-2020-1492
- CVE-2020-1525
- CVE-2020-1554

با بهره‌جویی از باگ‌های مذکور مهاجم می‌تواند به‌نحوی در حافظه دست‌درازی کند که کد دلخواه او به‌صورت از راه دور بر روی دستگاه قربانی نصب شود. بهره‌جوی هر یک از این آسیب‌پذیری‌ها می‌تواند در یک سند یا صفحه وب تزریق شده و با اجرا شدن توسط کاربر ناآگاه فعال شود.

CVE-2020-1472 دیگر آسیب‌پذیری "حیاتی" این ماه است که پودمان Netlogon Remote Protocol از آن تأثیر می‌پذیرد. آسیب‌پذیری مذکور که ضعفی از نوع "ترفیع امتیازی" (Elevation of Privilege) تلقی می‌شود مهاجم را قادر به توزیع فایل مخرب بر روی یکی از دستگاه‌های شبکه می‌کند.

جزییات بیشتر در خصوص مجموعه اصلاحیه‌های آگوست ۲۰۲۰ مایکروسافت در اینجا قابل دریافت و مطالعه است.

اصلاحیه‌های عرضه شده
در مرداد ۱۳۹۹

در مرداد ۱۳۹۹، شرکت‌های سیتریکس، ادوبی، مایکروسافت، سیسکو، گوگل و موزیلا برای برخی محصولات خود اصلاحیه و توصیه‌نامه امنیتی منتشر کردند.

در ۲ مرداد شرکت سیتریکس اقدام به عرضه اصلاحیه برای برطرف کردن یک آسیب‌پذیری امنیتی در نرم‌افزار Workspace app for Windows کرد. در صورت فعال بودن پودمان SMB بر روی دستگاه میزبان Workspace، مهاجم قادر خواهد بود تا با بهره‌جویی (Exploit) از این آسیب‌پذیری کنترل دستگاه قربانی را به‌صورت از راه دور در اختیار بگیرد. جزییات بیشتر در مقاله فنی CTX277662 قابل مطالعه است. این شرکت در ۲۱ مرداد هم پنج آسیب‌پذیری با شناسه‌های CVE-2020-8208، CVE-2020-8209، CVE-2020-8210، CVE-2020-8211 و CVE-2020-8212 را در Citrix Endpoint Management - که با نام XenMobile نیز شناخته می‌شود - ترمیم کرد. درجه اهمیت دو مورد از آسیب‌پذیری مذکور، "حیاتی" (Critical) گزارش شده است. اطلاعات بیشتر در اینجا قابل دریافت است.

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

- Bridge (APSB20-44)
- Photoshop (APSB20-45)
- Prelude (APSB20-46)
- Reader Mobile (APSB20-50)
- Magento Commerce 2 (APSB20-47)
- Acrobat / Reader (APSB20-48)
- Lightroom (APSB20-51)

۲۵ مورد از آسیب‌پذیری‌های ترمیم شده توسط این به‌روزرسانی‌ها، مجموعه نرم‌افزارهای Acrobat / Reader را تحت تأثیر قرار می‌دهند. درجه حساسیت ۱۱ مورد از آنها "حیاتی" 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، نسخه نگارش‌های جاری نرم‌افزارهای Acrobat DC و Acrobat Reader DC به ۲۰۲۰.۰۱۲.۲۰۰۴۱ و نگارش‌های ۲۰۱۷ آنها به ۲۰۱۷.۰۱۱.۳۰۱۷۵ تغییر خواهد کرد.

۲۱ مرداد، شرکت مایکروسافت اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی آگوست منتشر کرد. این اصلاحیه‌ها در مجموع، ۱۲۰ آسیب‌پذیری را در سیستم عامل Windows و دامنه گسترده‌ای از محصولات، سرویس‌ها و پودمان‌های این شرکت ترمیم می‌کنند. درجه حساسیت ۱۷ مورد از آنها "حیاتی" و ۱۰۳ مورد "مهم" (Important) اعلام شده است. جزییات کامل اصلاحیه های عرضه شده در اینجا قابل مطالعه است.

سیسکو نیز در مرداد ماه در چندین نوبت با انتشار اصلاحیه، در مجموع ۶۱ آسیب‌پذیری امنیتی را در محصولات مختلف خود ترمیم کرد. درجه اهمیت ۵ مورد از این آسیب‌پذیری‌ها، "حیاتی" و ۱۶ مورد از آنها "بالا" 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.

به گزارش شرکت مهندسی شبکه گستر، در ماهی که گذشت شرکت گوگل در دو نوبت با عرضه به‌روزرسانی اقدام به ترمیم آسیب‌پذیری‌های امنیتی مرورگر Chrome کرد. آخرین نسخه این مرورگر که در ۲۹ مرداد انتشار یافت ۸۴.۰.۴۱۴۷.۱۳۵ است. فهرست اشکالات مرتفع شده در اینجا و اینجا قابل دریافت و مشاهده است.

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

افتای ریاست جمهوری با همکاری شبکه گستر

شبکه گستر

شرکت مهندسی شبکه گستر

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

ترمیم ۱۲۰ آسیب‌پذیری امنیتی توسط مجموعه اصلاحیه‌های ماه آگوست مایکروسافت

سه‌شنبه، ۲۱ مرداد، شرکت مایکروسافت اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی آگوست منتشر کرد. این اصلاحیه‌ها در مجموع، ۱۲۰ آسیب‌پذیری را در سیستم عامل Windows و دامنه گسترده‌ای از محصولات، سرویس‌ها و پودمان‌های این شرکت ترمیم می‌کنند. ادامه مطلب را در اینجا بخوانید.

آخـرین اخبـار امنیـت فنـاوری اطلاعات

@SGnewsroom

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

شرکت مهندسی شبکه گستر

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

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