ماهنامه امنیت فناوری اطلاعات

مـرداد ۱۳۹۸

شبکه گستر

امنیت شما | وظیفه ما

فهرست مطالب

چکیده مدیریتی ۳

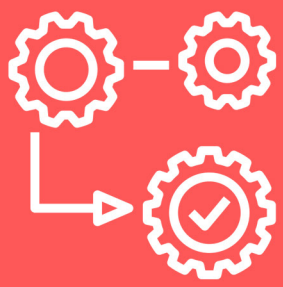
هشدارهای امنیتی ۵

رویدادهای امنیتی ۱۳

آسیب‌پذیری‌ها و اصلاحیه‌های امنیتی ۱۷

گزارش‌ها ۲۳

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 ۱۳۹۸ پرداخته شده است.

STOP و VJw0rm از جمله بدافزارهایی بودند که در مرداد امسال کاربران و مؤسسات ایرانی را هدف حملات گسترده خود قرار دادند.

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

روش انتشار VJw0rm نیز بهره‌گیری از حافظه‌های جداشدنی[۱] موسوم به USB Flash است. بدین نحوه که علاوه بر کپی دو نمونه از خود بر روی حافظه متصل به دستگاه آلوده‌شده، تمامی پوشه‌ها و فایل‌های موجود بر روی آن را مخفی نموده و به ازای هر یک از آنها یک میانبر[۲] ایجاد می‌کند. اتصال حافظه به دستگاهی پاک و در ادامه اجرای میانبر توسط کابر موجب آلوده شدن سیستم به بدافزار می‌شود.

در مرداد ماه، شرکت‌های مایکروسافت، ادوبی، گوگل، پالوآلتو نت‌ورکز، فورتینت، پالس سیکیور، سیسکو و وی‌ام‌وِر اقدام به انتشار اصلاحیه و توصیه‌نامه امنیتی برای برخی از محصولات خود کردند. در میان آسیب‌پذیری‌های ترمیم شده مایکروسافت در این ماه، دو مورد بیش از سایرین جلب توجه می‌کنند. این دو با شناسه‌های CVE-2019-1181 و CVE-2019-1182 ضعف‌هایی بسیار بحرانی در پودمان Remote Desktop Protocol – به اختصار RDP – هستند. به‌منظور بهره‌جویی از آنها تنها کافی است که یک درخواست دستکاری شده بر روی این پودمان به سیستم ارسال شود. با این کار، بدون هر گونه نیاز به دخالت کاربر، عملا درگاهی برای اجرای فعالیت‌های مخرب نظیر ایجاد حساب کاربری جدید با دسترسی کامل، نصب بدافزار و حتی مشاهده داده‌ها، تغییر و یا حذف آنها برای مهاجم باز می‌شود. آسیب‌پذیری RDP یادآور بهره‌جوی معروف BlueKeep است که با تبدیل بدافزارهایی همچون WannaCry به کرمی[۳] مخرب سبب آلوده شدن صدها میلیون دستگاه در کشورهای مختلف در مدتی بسیار کوتاه شد. مایکروسافت با تأکید فراوان از کاربران خواسته تا در اسرع وقت نسبت به نصب اصلاحیه‌های مربوطه اقدام کنند.

جدیدترین ابزارهای رمزگشایی منتشر شده در پنجمین ماه ۱۳۹۸ از دیگر موضوعاتی است که مطالعه آنها در این ماهنامه توصیه می‌شود.

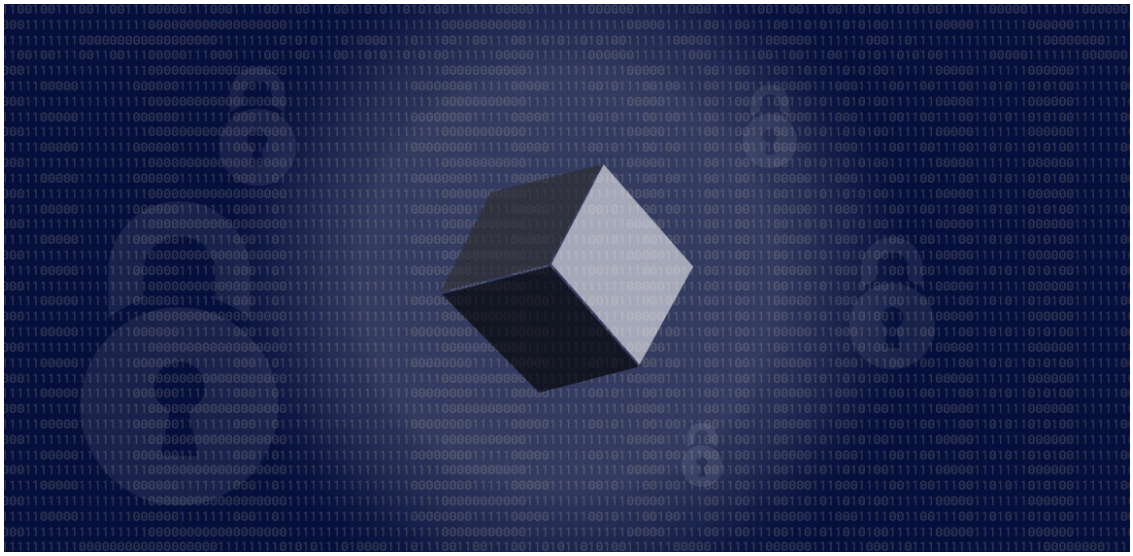
شرکت مهندسی شبکه گستر، ارائه‌دهنده محصولات و خدمات در زمینه امنیت شبکه از زمان تأسیس در سال ۱۳۷۰، همواره به امر آگاه‌سازی در زمینه امنیت فناوری اطلاعات به عنوان یکی از اصلی‌ترین راهکارهای مقابله با تهدیدات سایبری توجه خاص داشته است. امید است مطالب ماهنامه امنیت فناوری اطلاعات شرکت مهندسی شبکه گستر که حاصل تحقیق و پژوهش کارشناسان این شرکت است راهنمایی برای ارتقای دانش کاربران این حوزه باشد.

[۱] Removable Storage
[۲] Shortcut
[۳] Worm

هشدارهای امنیتی

کاربران و مؤسسات ایرانی هدف گسترده

باج‌افزار STOP



در هفته‌های اخیر گزارش‌های متعددی در خصوص مشاهده آلودگی بر روی سیستم برخی کاربران ایرانی به نسخه‌های جدید باج‌افزار STOP به شرکت مهندسی شبکه گستر واصل شده است.

STOP از جمله باج‌افزارهایی[1] است که در هر یک از نسخه‌های خود، پسوندی متفاوت از نسخه قبلی به فایل‌های رمزگذاری شده الصاق می‌کند. فهرست پسوندهای بکار گرفته شده توسط این باج‌افزار به شرح زیر است:

.STOP, .SUSPENDED, .WAITING, .PAUSA, .CONTACTUS, .DATASTOP, .STOPDATA, .KEYPASS, .WHY, .SAVEfiles, .DATAWAIT, .INFOWAIT, .puma, .pumax, .pumas, .shadow, .djvu, .djvuu, .udjvu, .djvuq, .uudjvu, .djvus, .djvur, .djvut .pdff, .tro, .tfude, .tfudeq, .tfudet, .rumba, .adobe, .adobee, .blower, .promos, .promoz, .promock, .promoks, .promorad, .promorad2, .kroput, .kroput1, .charck, .pulsar1, .klope, .kropun, .charcl, .doples, .luces,.luceq, .chech, .proden, .drume, .tronas, .trosak, .grovas, .grovat, .roland, .refols, .raldug, .etols, .guvara, .browec, .norvas, .moresa, .verasto, .hrosas, .kiratos, .todarius, .hofos, .roldat, .dutan, .sarut, .fedasot, .forasom, .berost, .fordan, .codnat, .codnat1, .bufas, .dotmap, .radman, .ferosas, .rectot, .skymap, .mogera, .rezuc, .stone, .redmat, .lanset, .davda, .poret, .pidon, .heroset, .myskle, .boston, .muslat, .gerosan, ,vesad, .horon, .neras, .truke, .dalle, .lotep, .nusar, .litar, .besub, .cezor, .lokas, .godes, .budak, .vusad, .herad, .berosuce, .gehad, .gusau, .madek, .tocue, .darus, .lapoi, .todar, .dodoc, .bopador, .novasof, .ntuseg, .ndarod, .access, .format, .nelasod, .mogranos, .cosakos, .nvetud, .lotej, .kovasoh, .masok, .Coharos

STOP که نخستین نسخه آن در آذر ۱۳۹۷ شناسایی شد از روش‌های مختلفی برای آلوده کردن سیستم‌ها بهره می‌گیرد.

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

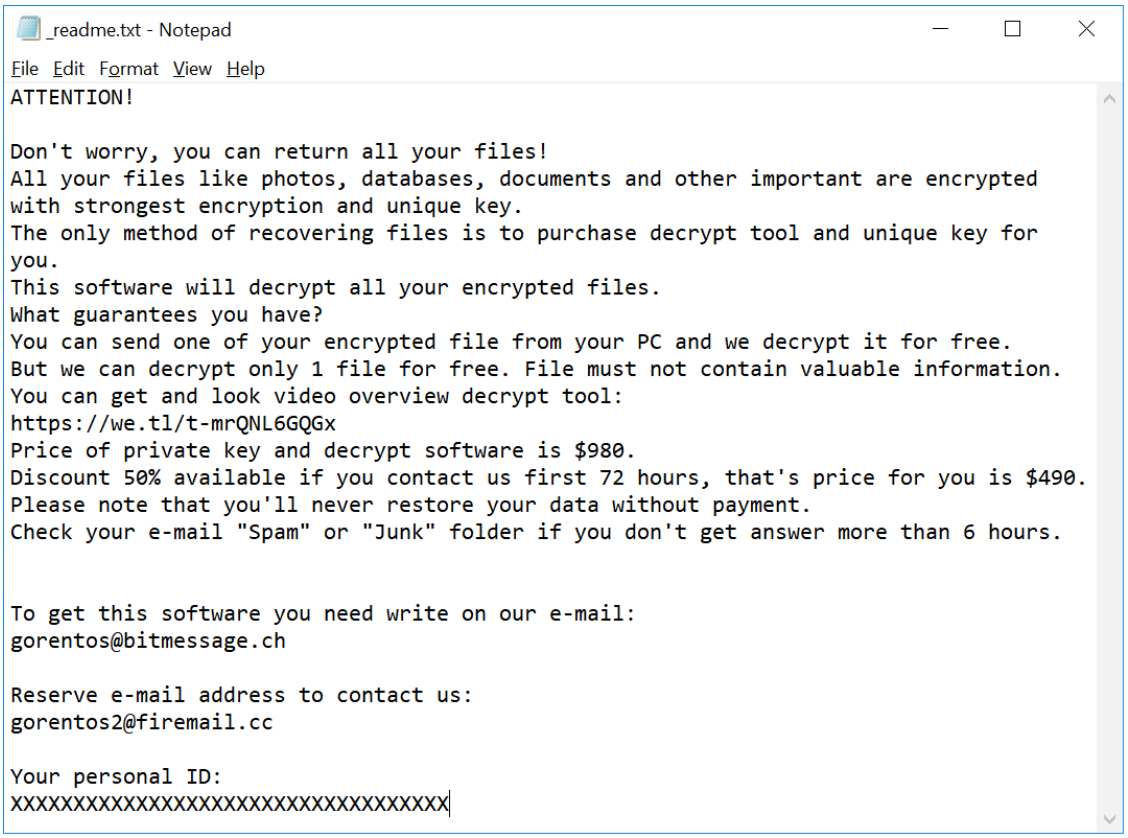
یکی دیگر از روش‌های مورد استفاده نویسندگان STOP برای انتشار این باج‌افزار، بکارگیری بسته بهره‌جوی Fallout است. این بسته بهره‌جو[2]، از آسیب‌پذیری CVE-2018-8174 در بخش مدیریت‌کننده کدهای VBScript و از آسیب‌پذیری CVE-2018-4878 در محصول Adobe Flash Player سوءاستفاده کرده و کد مخرب مورد نظر مهاجمان – در اینجا باج‌افزار –

[1] Ransomware
[2] Exploit Kit

را بر روی دستگاه قربانی به‌صورت از راه دور نصب و اجرا می‌کند. مهاجمان معمولا بسته‌های بهره‌جو را در سایت‌های با محتوای جذاب یا سایت‌های معتبر هک شده تزریق می‌کنند تا از این طریق در زمان مراجعه کاربر به سایت از آسیب‌پذیری‌های موجود در سیستم عامل و نرم‌افزارهای نصب شده بر روی دستگاه سوءاستفاده شود. لازم به ذکر است که شرکت مایکروسافت اردیبهشت ماه سال قبل، همزمان با عرضه اصلاحیه‌های ماه میلادی می آسیب‌پذیری CVE-2018-8120 را ترمیم کرد. شرکت ادوبی نیز آسیب‌پذیری CVE-2018-4990 را در به‌روزرسانی‌های APSA18-09 و APSA18-17 اصلاح و برطرف کرد. به‌روز بودن سیستم عامل Windows و نرم‌افزار پراستفاده Flash Player اصلی‌ترین راهکار برای ایمن نگاه داشتن دستگاه در برابر این بسته بهره‌جو محسوب می‌شود.

ایمیل‌های با پیوست و لینک مخرب نیز دیگر روش انتشار STOP است.

مبلغ اخاذی شده توسط این باج‌افزار ۹۸۰ دلار است که بر طبق آنچه که در اطلاعیه باج‌گیری[۱] آن درج شده است در صورتی که عملیات پرداخت ظرف ۷۲ ساعت نخست پس از آلودگی انجام شود قربانی مشمول تخفیفی ۵۰ درصدی شده و این مبلغ به ۴۹۰ دلار کاهش می‌یابد.



STOP با اجرای فرامینی اقدام به حذف کردن نسخه‌های موسوم به Shadow، غیرفعال نمودن قابلیت System Restore و متوقف ساختن سرویس‌های Windows Defender، System Recovery و BITS می‌کند.

در برخی نمونه‌ها از این باج‌افزار، از کلید رمزگذاری[۲] برون‌خط[۳] (و نه برخط[۴]) استفاده می‌شود. در این صورت بکارگیری این ابزار برای بازگرداندن فایل‌ها به حالت اولیه کارساز خواهد بود. توضیح این‌که به‌منظور شناسایی کلید رمزگذاری نیاز است که یک فایل رمز شده توسط باج‌افزار به همراه فایل اصلی آن (رمزگذاری نشده) در مسیر Settings | Bruteforcer به نرم‌افزار معرفی شود. حجم دو فایل معرفی شده می‌بایست بیشتر از ۱۵۰ کیلوبایت باشد.

۱ Ransom Note
۲ Encryption Key
۳ Offline
۴ Online

متأسفانه در حال حاضر راهکاری برای بازگردانی فایل‌های رمز شده توسط کلیدهای ایجاد شده در حالت برخط بدون در اختیار داشتن کلید فراهم نیست. با این حال در برخی مواقع به دلایلی نظیر مصادره سرورهای حاوی کلید یا شناسایی اشکالی در فرایند رمزگذاری این امکان فراهم می‌شود که فایل‌ها را به رایگان به حالت اولیه بازگرداند. بنابراین توصیه می شود که فایل‌هایی که پسوند آنها تغییر کرده را به همراه فایل اطلاعیه باج‌گیری آنها در محلی نگهداری کنید تا هر زمان که راه‌حلی جدید برای رمزگشایی کشف شد بتوان این فایل‌ها را بازگردانی کرد.

تأکید می‌گردد که مؤثرترین راهکار در مقابله با باج‌افزارها، پیشگیری از آلوده شدن سیستم‌ها به آنهاست. پس همچون همیشه بکارگیری روش‌های پیشگیرانه در مقابله با باج‌افزارها توصیه می‌شود.

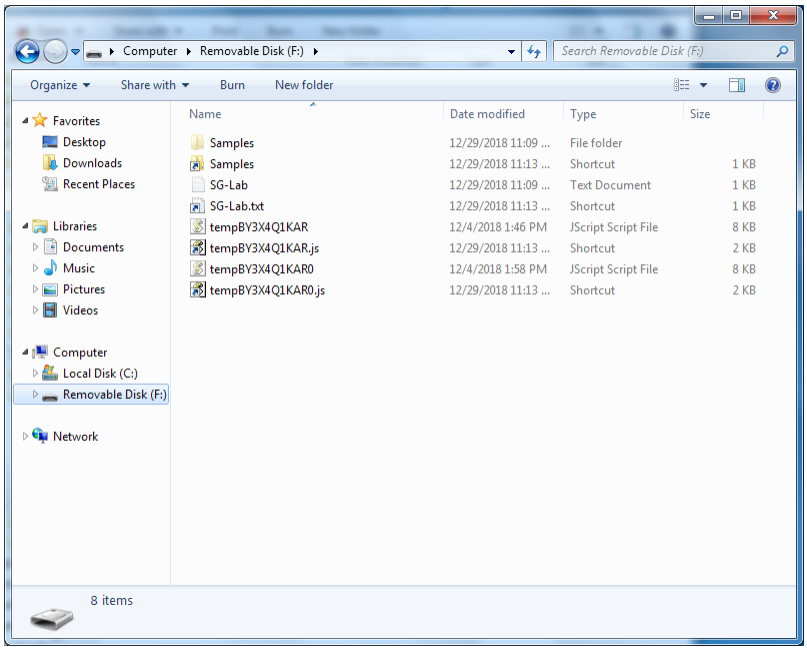
در اتاق خبر شبکه گستر بخوانید...

نسـخه جدید بدافـزار VJw0rm

در پی کاربران و مؤسسات ایرانی

در هفته‌های اخیر نسخه جدیدی از بدافزار VJw0rm با عملکرد کرم[۱] کاربران و مؤسسات ایرانی را هدف حملات خود قرار داده است.

به گزارش شرکت مهندسی شبکه گستر، روش انتشار این بدافزار بهره‌گیری از حافظه‌های جداشدنی موسوم[۲] به USB Flash است. بدین نحوه که علاوه بر کپی دو نمونه از خود بر روی حافظه متصل به دستگاه آلوده‌شده، تمامی پوشه‌ها و فایل‌های موجود بر روی آن را مخفی نموده و به ازای هر یک از آنها یک میانبر[۳] ایجاد می‌کند.



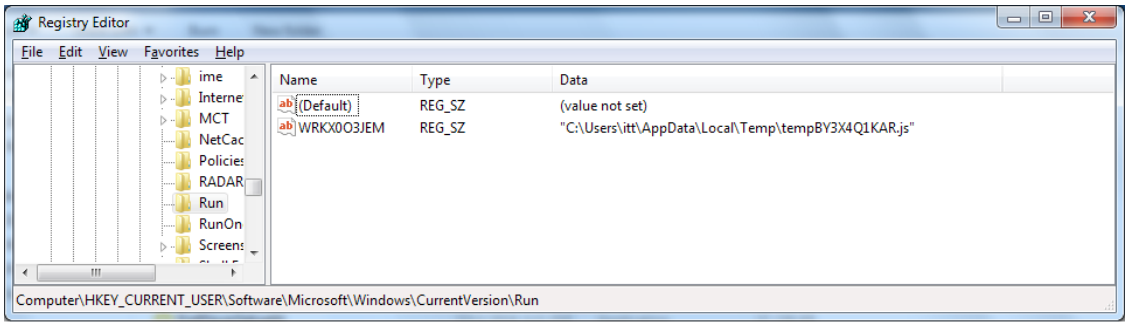
اجرای میانبر موجب فراخوانی فایل مخرب موجود در حافظه USB Flash و سپس اجرای فایل / پوشه اصلی می‌شود. با توجه به عدم نمایش فایل‌ها و پوشه‌های مخفی[۴] و سیستمی[۵] در حالت پیش‌فرض و نظر به اجرا شدن فایل یا پوشه مورد نظر کاربر احتمال مشکوک شدن کاربر به آلوده بودن حافظه تا حد بسیار زیادی کاهش می‌یابد.

۱ Worm
۲ Remvable Storage
۳ Shortcut
۴ Hidden
۵ System

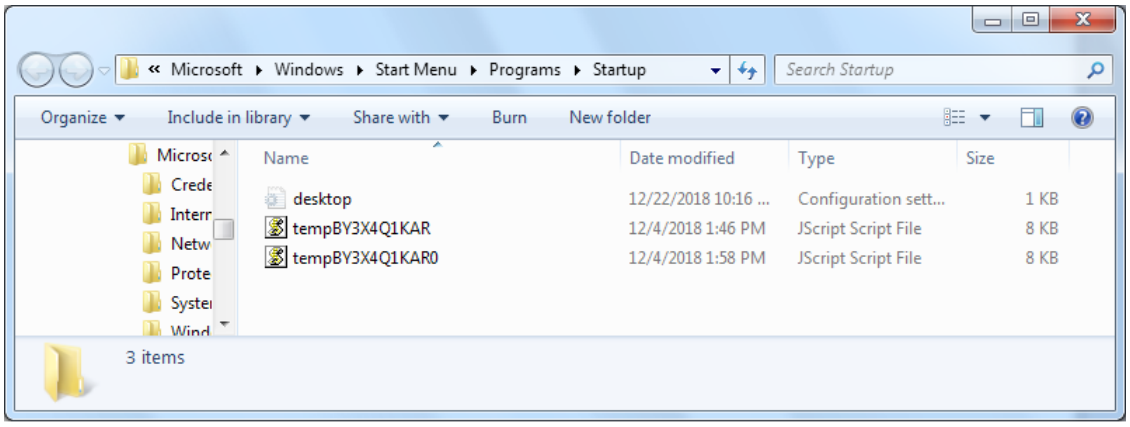
در ادامه بدافزار اقدام به کپی نسخه‌ای از خود در مسیرهای زیر می‌کند:

- %Temp%
- %UserProfile%\Downloads

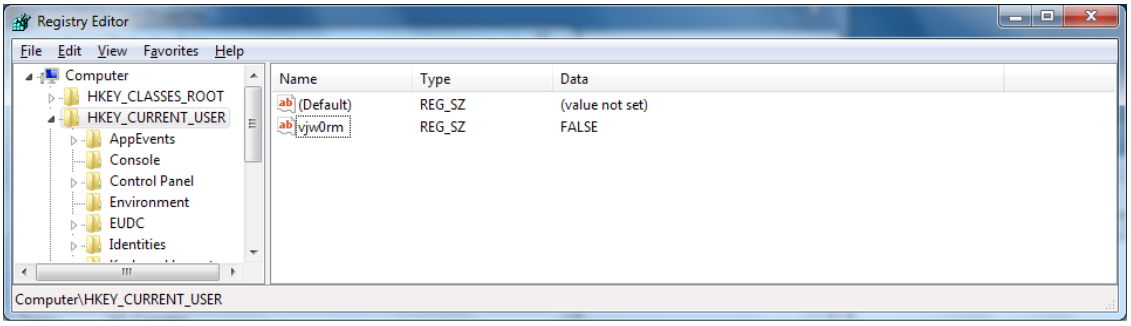
VJw0rm با ایجاد کلید زیر در محضرخانه[1] موجب اجرای خودکار خود در هر بار راه‌اندازی شدن سیستم عامل می‌گردد.



دو نمونه از فایل مخرب VJw0rm نیز در پوشه %Startup% کپی می‌شود که مکانیزمی دیگر برای اجرای خودکار بدافزار است.

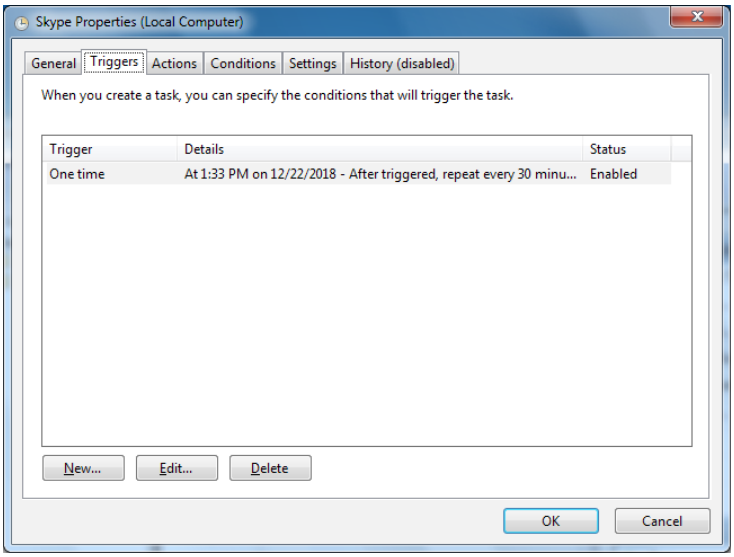


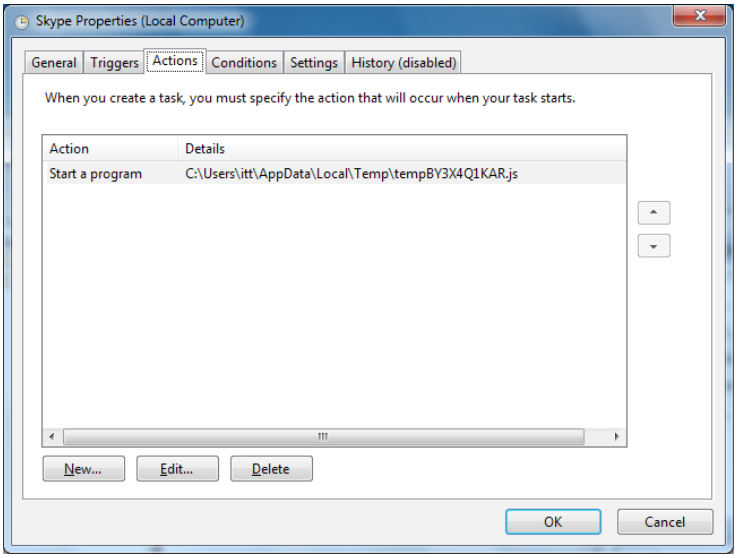
همچنین از طریق پروسه معتبر wscript.exe کلیدی تحت عنوان VJw0rm با مقدار False در مسیر HKEY_CURRENT_USER ایجاد می‌شود.



[1] Registry

از دیگر دست‌درازی‌های VJw0rm می‌توان به ایجاد یک فرمان زمانبندی شده[1] با عنوان Skype اشاره کرد که وظیفه آن اجرای فایل مخرب بدافزار در هر ۳۰ دقیقه یکبار است.





در این نسخه، بدافزار اقدام به برقراری ارتباط با نشانی lalik.linkpc[.]net بر روی درگاه ۷۶ می‌کند. به‌نظر می‌رسد نشانی مذکور متعلق به سایتی هک شده است که مهاجمان از آن به‌عنوان سرور فرماندهی[2] این نسخه از VJw0rm استفاده می‌کنند.

استفاده از ضدویروس به‌روز و قدرتمند و بکارگیری محصولات موسوم به Device Control می‌تواند سازمان را از گزند این تهدیدات ایمن نگاه دارد.

[1] Scheduled Task
[2] Command and Control - C&C

رویـدادهـای امنـیـتی

عرضه ابزار رمزگشایی برای قربانیان باج‌افزار LooCipher

شرکت امسی‌سافت ابزاری را ارائه کرده که قربانیان باج‌افزار LooCipher را قادر به بازگرداندن رایگان فایل‌های رمز شده خود می‌کند.

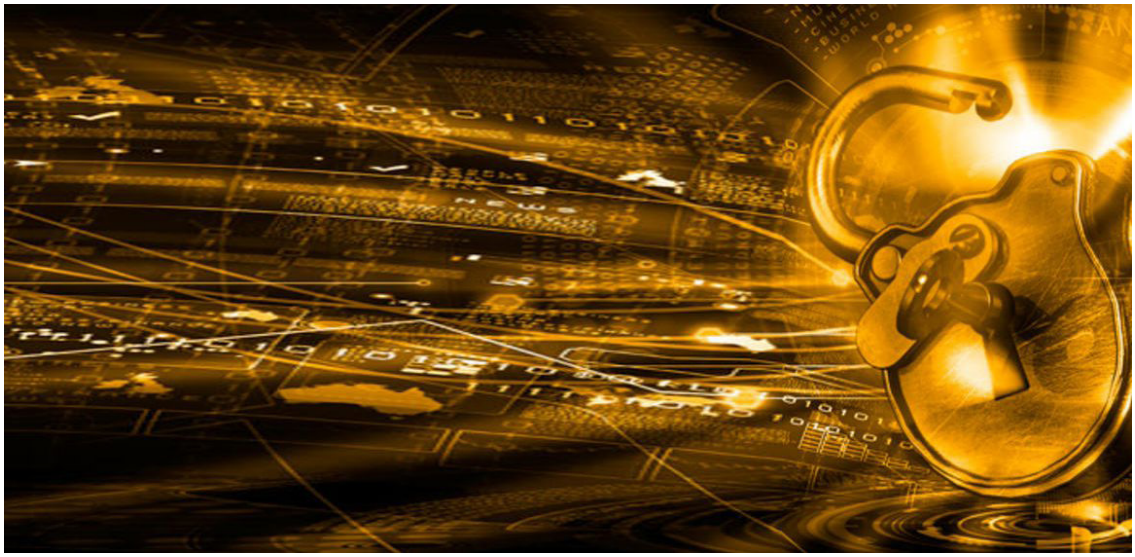
به گزارش شرکت مهندسی شبکه گستر، اصلی‌ترین روش انتشار LooCipher ارسال ایمیل‌های با پیوست فایل Word است که در آن ماکرویی[1] مخرب جاسازی شده است. وظیفه این ماکرو دریافت فایل باج‌افزار و اجرای آن بر روی دستگاه قربانی است. این باج‌افزار به فایل‌های رمزگذاری شده پسوند lcphr را الصاق می‌کند. نمونه‌ای از پنجره حاوی اطلاعیه باج‌گیری LooCipher در شکل زیر نمایش داده شده است.

ابزار امسی‌سافت در اینجا قابل دریافت و استفاده است.

توضیح این‌که به‌منظور شناسایی کلید رمزگشایی نیاز است که یک فایل رمز شده توسط باج‌افزار به همراه فایل اصلی آن (رمزگذاری نشده) به نرم‌افزار معرفی شود.

[1] Macro

انتشار ابزاری برای بازگرداندن فایل‌های رمز شده توسط باج‌افزار eCh0raix



یک محقق امنیتی ابزاری را ارائه کرده که امکان بازگرداندن فایل‌های رمزگذاری شده توسط اکثر نسخه‌های باج‌افزار eCh0raix را فراهم می‌کند. eCh0raix که با نام QNAPCrypt نیز شناخته می‌شود به‌طور خاص دستگاه‌های موسوم به ذخیره‌ساز متصل به شبکه[1] ساخت شرکت کیونپ را مورد هدف قرار می‌دهد.

به گزارش شرکت مهندسی شبکه گستر، روش انتشار این باج‌افزار سوءاستفاده از آسیب‌پذیری‌های امنیتی این تجهیزات و اجرای حملات سعی‌وخطا[2] برای رخنه به دستگاه‌های با سیستم عامل غیر به‌روز یا رمزهای عبور پیش‌فرض / ضعیف است.

نخستین نسخه از باج‌افزار eCh0raix بیشتر از یک سال قبل منتشر شد.

eCh0raix پس از رمزگذاری هر فایل، به آن پسوند encrypted را الصاق می‌کند.

خوشبختانه یک محقق امنیتی با بهره‌جویی از اشکالی در فرایند رمزگذاری این باج‌افزار موفق به ساخت ابزاری شده که با استفاده از آن بازگرداندن فایل‌های قفل شده توسط اکثر نسخه‌های eCh0raix ممکن می‌شود.

ابزار مذکور در اینجا قابل دریافت و استفاده است.

توضیح اینکه eCh0raix با نام‌های زیر شناسایی می‌شود:

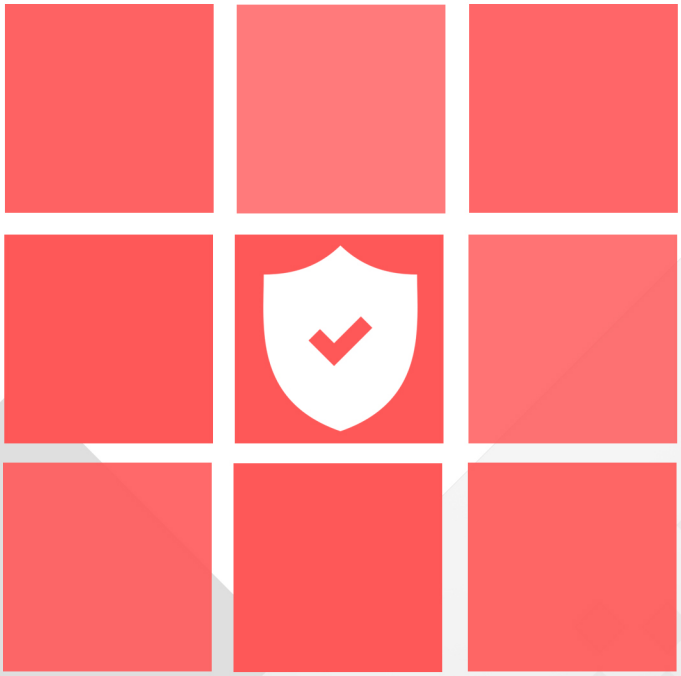
Bitdefender:
- Trojan.Linux.Ransom.D
- Trojan.Ransom.Linux.Cryptor.A

McAfee:
- LNX/Ransom-GPJ!DA34C9A18D96
- LNX/Ransom-GPJ!B904BAFEBE75

Sophos:
- Linux/Ransm-G
- Mal/Generic-S

[1] Network-attached Storage - NAS
[2] Brute-force

آسیب‌پذیری‌ها
و اصلاحیه‌های امنیتی



اصلاحیه‌های امنیتی مایکروسافت
برای ماه میلادی اوت

به گزارش شرکت مهندسی شبکه گستر، سه‌شنبه ۲۲ مرداد، شرکت مایکروسافت اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی اوت منتشر کرد. این اصلاحیه‌ها در مجموع، ۹۷ آسیب‌پذیری را در سیستم عامل Windows و برخی دیگر از محصولات مایکروسافت ترمیم می‌کنند. درجه اهمیت ۳۱ مورد از آسیب‌پذیری‌های ترمیم شده توسط اصلاحیه‌های مذکور "حیاتی"[۱]، ۶۵ مورد "بااهمیت"[۲] و یک مورد نیز "متوسط"[۳] 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 اهمیت 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 اهمیت "بااهمیت" برطرف و ترمیم می‌گردند.

هیچ یک از آسیب‌پذیری‌های ترمیم شده در این ماه، روز صفر[۴] محسوب نمی‌شوند. اما در میان همین آسیب‌پذیری‌ها، دو مورد بیش از سایرین جلب توجه می‌کنند. این دو با شناسه‌های CVE-2019-1181 و CVE-2019-1182 ضعف‌هایی بسیاری بحرانی در پودمان Remote Desktop Protocol – به اختصار RDP – هستند. به‌منظور بهره‌جویی از آنها تنها کافی است که یک درخواست دستکاری شده بر روی پودمان RDP به سیستم ارسال شود. با این کار، بدون هر گونه نیاز به دخالت کاربر، عملا درگاهی برای اجرای فعالیت‌های مخرب نظیر ایجاد حساب کاربری جدید با دسترسی کامل، نصب بدافزار و حتی مشاهده داده‌ها، تغییر و یا حذف آنها برای مهاجم باز می‌شود. آسیب‌پذیری RDP یادآور بهره‌جوی معروف BlueKeep است که با تبدیل بدافزارهایی همچون WannaCry به کرمی مخرب موجب آلودگی صدها میلیون دستگاه را در کشورهای مختلف در مدتی بسیار کوتاه شد. مایکروسافت با تأکید فراوان از کاربران خواسته تا در اسرع وقت نسبت به نصب اصلاحیه‌های مربوطه برای ترمیم این آسیب‌پذیری‌ها اقدام کنند.


Security Response
@msftsecresponse

August 2019 Security Update includes fixes for wormable RCE vulnerabilities in Remote Desktop Services (RDS), affecting all in-support versions of Windows. These should be patched quickly. For more information, see msrc-blog.microsoft.com/2019/08/13/pat...

10:09 PM · Aug 13, 2019 · TweetDeck

۱ Critical
۲ Important
۳ Moderate
۴ Zero-day

CVE-2019-1201، دیگر آسیب‌پذیری قابل‌توجهی است که توسط اصلاحیه‌های ماه اوت مایکروسافت ترمیم شده است. نرم‌افزار Word از این ضعف امنیتی که از نحوه نادرست مدیریت اشیا در حافظه ناشی می‌شود تأثیر می‌پذیرد. با باز شدن یک فایل دستکاری شده Word توسط قربانی مهاجم قادر به اجرای کد مورد نظر خود به‌صورت از راه دور بر روی دستگاه می‌شود. باید توجه داشت حتی فراخوانی فایل مذکور در بخش پیش‌نمایش نرم‌افزار Outlook موسوم به Outlook Preview Pane نیز نتیجه‌ای یکسان با اجرای آن در بر خواهد داشت.

از دیگر آسیب‌پذیری‌های حائز اهمیتی که این ماه ترمیم شده‌اند می‌توان به موارد نیز اشاره کرد.

- CVE-2019-0736 – ضعفی در بخش Client پودمان DHCP مورد استفاده در سیستم عامل Windows که با سوءاستفاده از آن از طریق ارسال یک بسته دستکاری شده به این بخش امکان اجرای کد به‌صورت راه دور برای مهاجم فراهم می‌شود.
- CVE-2019-1188 – اشکالی در نحوه مدیریت فایل‌های موسوم به میانبرا که بهره‌جویی از آن موجب اجرای خودکار یک فایل بالقوه مخرب بر روی دستگاه و تسریع انتشار آن در سطح شبکه می‌شود.
- CVE-2019-0720 و CVE-2019-0965 – دو آسیب‌پذیری امنیتی در نرم‌افزار مجازی‌سازی Hyper-V که با سوءاستفاده از آنها از روی ماشین Guest، امکان اجرای کد بر روی دستگاه Host فراهم می‌شود.

جزییات بیشتر در خصوص اصلاحیه‌های امنیتی عرضه شده مایکروسافت در ماه میلادی اوت در اتاق خبر شرکت مهندسی شبکه گستر قابل دریافت و مطالعه است.

اصلاحیه‌های امنیتی ادوبی
برای ماه میلادی اوت

۲۲ مرداد، شرکت ادوبی مجموعه اصلاحیه‌های امنیتی ماه میلادی اوت خود را منتشر کرد. اصلاحیه‌های مذکور، در مجموع، ۱۱۹ ضعف امنیتی را در هشت محصول زیر ترمیم می‌کنند:

- Acrobat / Reader
- After Effects CC
- Character Animator CC
- Premiere Pro CC
- Prelude CC
- Creative Cloud Desktop Application
- Experience Manager
- Photoshop CC

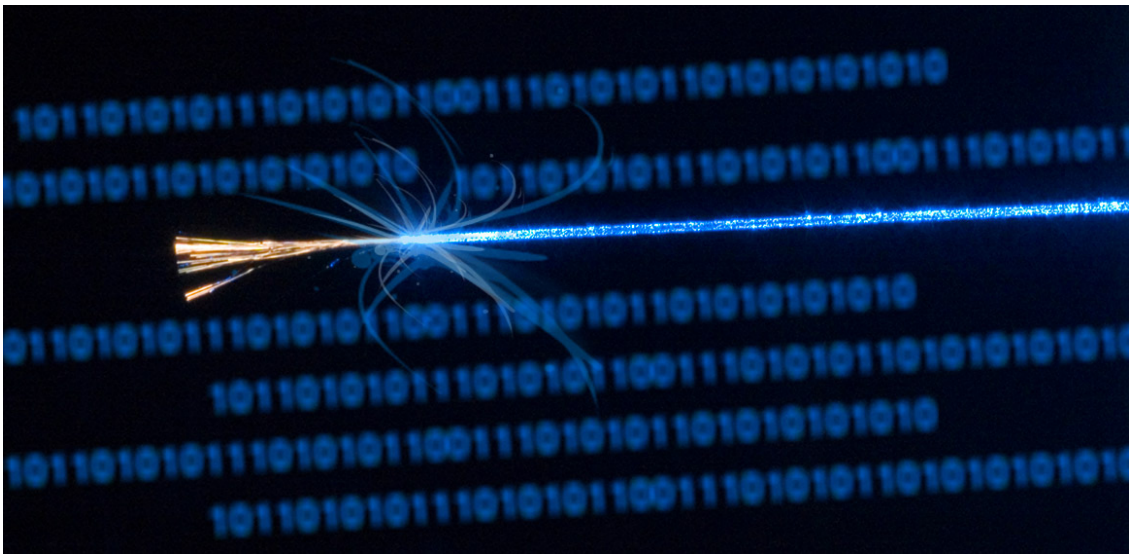
۷۶ مورد از آسیب‌پذیری‌های ترمیم شده توسط این اصلاحیه‌ها، بر روی مجموعه نرم‌افزارهای Acrobat / Reader اثرگذار هستند. بسیاری از این ضعف‌های امنیتی در دسته آسیب‌پذیری به حملات اجرای کد به‌صورت از راه دور قرار می‌گیرند. بدین‌ترتیب باز کردن یک PDF دستکاری شده در هر یک از نسخه‌های آسیب‌پذیر مجموعه نرم‌افزارهای Acrobat / Reader منجر به اجرای کد بالقوه مخرب تزریق شده در فایل خواهد شد. با نصب به‌روزرسانی ماه اوت، نسخه نگارش‌های جاری نرم‌افزارهای Acrobat DC و Acrobat Reader DC به 2019.012.20036 و نگارش‌های ۲۰۱۷ آنها به 2017.011.30144 تغییر خواهد کرد.

همچون ما قبل و البته در روالی غیرمعمول، این ماه نیز هیچ اصلاحیه‌ای برای محصول Flash Player ارائه نشده است.

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

- https://helpx.adobe.com/security/products/acrobat/apsb19-41.html
- https://helpx.adobe.com/security/products/after_effects/apsb19-31.html
- https://helpx.adobe.com/security/products/character_animator/apsb19-32.html
- https://helpx.adobe.com/security/products/premiere_pro/apsb19-33.html
- https://helpx.adobe.com/security/products/prelude/apsb19-35.html
- https://helpx.adobe.com/security/products/creative-cloud/apsb19-39.html
- https://helpx.adobe.com/security/products/experience-manager/apsb19-42.html
- https://helpx.adobe.com/security/products/photoshop/apsb19-44.html

آسـیب‌پـذیری‌هـای بحـرانی VxWorks؛
بیش از ۲ میلیارد دستگاه در معرض خطر



محققان شرکت آرمیس از شناسایی ۱۱ ضعف امنیتی در VxWorks خبر داده‌اند.

VxWorks، یکی از پراستفاده‌ترین سیستم‌های عامل موسوم به بلادرنگ[۱] است که در بیش از ۲ میلیارد دستگاه خاص صنایع زیرساختی، هوا فضا، نظامی، خودروسازی و الکترونیکی، ماشین‌آلات صنعتی، دستگاه‌های پزشکی و تجهیزات شبکه از آن استفاده شده است. بسیاری از دوربین‌های اینترنتی، سوئیچ‌های شبکه‌ای، روترها، فایروال‌ها، تلفن‌های VoIP، چاپگرها، محصولات ویدئو کنفرانس، چراغ‌های راهنمایی، آسانسورها، دستگاه‌های پایش وضعیت بیماران[۲]، ماشین‌های MRI، مودم‌های ماهواره‌ای و حتی مریخ‌نوردها و به‌طور کلی بخش قابل‌توجهی از دستگاه‌های معروف به اینترنت اشیا[۳] بر پایه این سیستم عامل کار می‌کنند.

به گزارش شرکت مهندسی شبکه گستر، از این ۱۱ آسیب‌پذیری که به URGENT/11 معروف شده‌اند، ٦ مورد دارای درجه اهمیت حیاتی هستند. بهره‌جویی از این آسیب‌پذیری‌ها مهاجم را قادر به در اختیار گرفتن کنترل دستگاه‌های با این سیستم عامل، به‌صورت از راه دور و بدون نیاز به هر گونه دخالت کاربر می‌کند.

ضعف‌های مذکور از نحوه مدیریت بخش IPnet TCP/IP Networking Stack توسط این سیستم عامل ناشی می‌شود. IPnet TCP/IP Networking Stack از نسخه ٦٫٥ (حدود ۱۳ سال قبل) به VxWorks اضافه شد. گرچه هر ۱۱ ضعف امنیتی متوجه نسخه ٦٫٥ و نسخه‌های بعد از آن نیست اما هر یک از نسخه‌های عرضه شده طی ۱۳ سال گذشته حداقل از یکی از این آسیب‌پذیری‌های حیاتی تأثیر می‌پذیرند.

VxWorks توسط شرکت ویـند ریـور سـیسـتمز توسعه داده شده و اکنون این شرکت با مشارکت آرمیـس در حال انتشار اصلاحیه‌های امنیتی برای ترمیم آسیب‌پذیری‌های مذکور است. اما از آنجا که محصولات مبتنی بر این سیستم عامل توسط شرکت‌های دیگر ساخته و عرضه شده‌اند باید امیدوار بود که خیلی زود این سازندگان اقدام به عرضه اصلاحیه یا حداقل انتشار توصیه‌نامه‌هایی برای مقاوم‌سازی موقت محصولات خود کنند.

جزییات کامل در خصوص URGENT/11 در اینجا قابل دریافت و مطالعه است.

۱ Real-time
۲ Patient Monitor
۳ Internet of Things - IoT

اصلاحیه‌های عرضه شده
در مرداد ۱۳۹۸

در مرداد ماه، علاوه بر مایکروسافت و ادوبی، شرکت‌های گوگل، پالوآلتو نت‌ورکز، فورتینت، پالس سیکیور، سیسکو و وی‌اِم‌وِر اقدام به انتشار اصلاحیه و توصیه‌نامه امنیتی برای برخی از محصولات خود کردند.

در این ماه شرکت گوگل در دو نوبت با عرضه به‌روزرسانی اقدام به ترمیم آسیب‌پذیری‌های مرورگر Chrome کرد. بهره‌جویی از برخی از آسیب‌پذیری‌های مذکور مهاجم را قادر به در اختیار گرفتن کنترل سیستم می‌کند. آخرین نسخه عرضه شده این مرورگر 76.0.3809.100 است. فهرست اشکالات مرتفع شده در این نسخه نیز در اینجا قابل مشاهده است.

به گزارش شرکت مهندسی شبکه گستر، در اوایل مرداد ماه، آژانس CISA آمریکا نسبت به وجود آسیب‌پذیری در بخش مدیریت کننده ارتباطات VPN محصولات امنیتی Palo Alto، FortiGuard و Pulse هشدار داد. این آژانس به راهبران شبکه توصیه کرده تا با مراجعه به توصیه‌نامه‌های منتشر شده از سوی شرکت‌های سازنده این محصولات نسبت به ترمیم آسیب‌پذیری‌ها اقدام کنند. این توصیه‌نامه‌ها در اینجا، اینجا و اینجا قابل دریافت است.

در این ماه، سیسکو در چندین نوبت اقدام به انتشار به‌روزرسانی‌های امنیتی کرد. این به‌روزرسانی‌ها در مجموع، ۶۳ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت ۶ مورد از این آسیب‌پذیری‌ها "حیاتی" و ۲۲ مورد از آنها "بالا"[1] گزارش شده است. اشکالات مرتفع شده توسط به‌روزرسانی‌های جدید دامنه گسترده‌ای از آسیب‌پذیری‌ها – از جمله اجرای کد به‌صورت از راه دور، عبور از سد تنظیمات امنیتی، از کاراندازی سرویس و ترفیع امتیازی را در بر می‌گیرد. توضیحات کامل در مورد به‌روزرسانی‌های عرضه شده در اینجا قابل دسترس است.

وی‌اِم‌وِر دیگر شرکتی بود که در مرداد ماه ۱۳۹۸ اقدام به انتشار و عرضه به‌روزرسانی برای ترمیم دو آسیب‌پذیری امنیتی کرد. محصولات زیر از آسیب‌پذیری‌های ترمیم شده توسط این به‌روزرسانی‌ها تأثیر می‌پذیرند:

- vSphere ESXi
- Workstation Pro / Player
- Fusion Pro / Fusion

سوءاستفاده از این ضعف‌ها موجب نشت اطلاعات بالقوه حساس یا از کار افتادن سرویس‌دهی محصول آسیب‌پذیر می‌شود. توضیحات کامل در این خصوص در اینجا قابل مطالعه است.

همچنین در این ماه مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای کشور (ماهر) به بررسی به‌روزرسانی امنیتی ماه اوت سیستم عامل Android پرداخت که مشروح آن در اینجا قابل دریافت است.

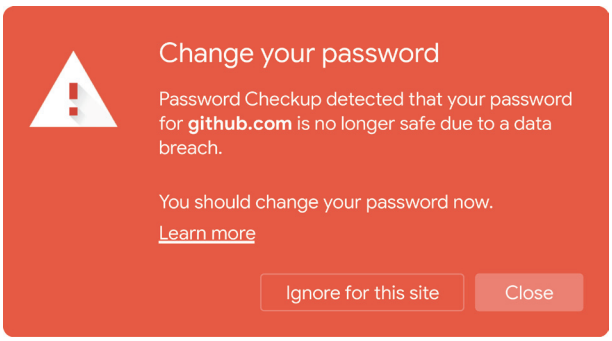
[1] High

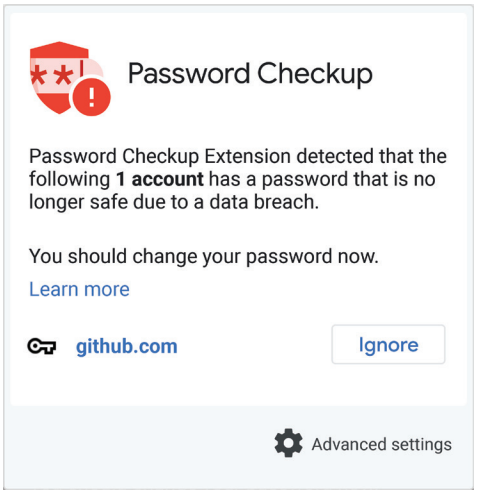
گـزارش‌هـا

آماری جالب از داده‌های استخراج شده
توسط یک افزونه امنیتی

بر اساس مطالعه انجام شده توسط کارشناسان شرکت گوگل و یک محقق دانشگاه استنفورد، ۱/۵ درصد از ثبت‌های ورود[۱] در بستر وب، با استفاده از رمزهای عبور افشا شده انجام می‌شود. در استخراج این آمار، داده‌های جمع‌آوری شده توسط افزونه Google Password Checkup مورد استناد قرار گرفته است.

به گزارش شرکت مهندسی شبکه گستر، Password Checkup، یک سرویس اطلاع‌رسانی در خصوص اطلاعات اصالت‌سنجی[۲] نامن است. Password Checkup پس از ثبت ورود کاربر در مرورگر مجهز به این افزونه، درهم‌ساز[۳] اطلاعات اصالت‌سنجی وارد شده را به گوگل ارسال می‌کند. در ادامه، اطلاعات ارسالی با بانک داده‌ای حاوی ٤ میلیارد نام کاربری و رمز عبور افشا شده مورد مقایسه قرار گرفته و در صورت مشاهده هر گونه تطابق، در هشدارهایی مشابه تصاویر زیر از کاربر خواسته می‌شود تا نسبت به تغییر رمز عبور خود اقدام کند.





۱ Login
۲ Credentials
۳ Hash

در این مطالعه آمار جمع‌آوری شده توسط Password Checkup در فاصله بین ۱۶ بهمن تا ۱۳ اسفند سال گذشته لحاظ شده است. بر این اساس از میان ۲۱,۱۷۷,۲۳۷ ثبت ورود رصد شده، در ۳۱۶,۵۳۱ موارد (۱/۵ درصد) از رمز عبوری استفاده شده که اطلاعات آن به نحوی در بانک داده مذکور موجود بوده است. همچنین بر طبق این مقاله نمایش هشدار منجر به تغییر رمز عبور توسط ۲۶ درصد این کاربران شده است. ۶۰ درصد رمزهای عبور تغییر یافته نیز امن‌تر گزارش شده‌اند.

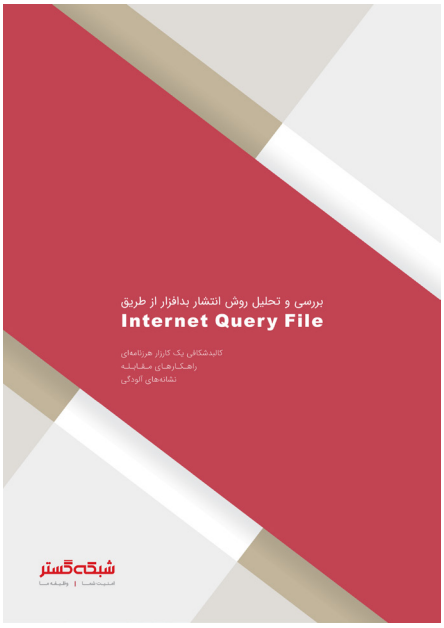
باید توجه داشت که افرادی که اقدام به نصب افزونه Password Checkup کرده‌اند در دسته کاربرانی قرار می‌گیرند که حداقل تا حدودی نسبت به ملاحظات امنیتی آگاه هستند. بنابراین انتظار می‌رود که آمار واقعی بسیار فراتر از آمار ۱/۵ درصدی حاصل شده در جریان این مطالعه باشد. موضوعی که این محققان نیز به آن اذعان داشته‌اند:

> *“Our detection rate is lower than the 6.9% reported by Thomas et al. [54] for 751 million Google accounts and 1.9 billion breached credentials. Possible reasons include the user population that adopted our extension is more security conscious— thus avoiding reuse as a behavior—or that dormant accounts have a higher reuse rate, which by nature our extension cannot observe as we perform checks at login time.”*

مشروح این مقاله با عنوان "Protecting accounts from credential stuffing with password breach alerting" که در سومین هفته از مرداد ماه در سمپوزیوم امنیتی یوزنیکس ارائه شد در اینجا قابل دریافت و مطالعه است.


آخرین اخبار امنیت فناوری اطلاعات
@SGnewsroom
SCAN ME

در اتاق خبر
شبکه گستر بخوانید...



شبکه گستر

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.

ISO 9001:2008
Cert No 9150.C528

شرکت مهندسی شبکه گستر

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

تلفن / دورنگار	۰۲۱-۴۲۰۵۲
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