ماهنامه امنیت فناوری اطلاعات

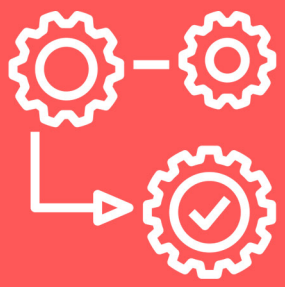
شهریور ۱۳۹۸

شبکه گستر

امنیت شما | وظیفه ما

فهرست مطالب

چکیده مدیریتی



در این شماره از ماهنامه امنیت فناوری اطلاعات شرکت مهندسی شبکه گستر به بررسی مهمترین رخدادها و رویدادهای مرتبط با امنیت فناوری اطلاعات در شهریور ماه ۱۳۹۸ پرداخته شده است.

در این ماه، شرکت امنیتی سوفوس از اجرای کارزاری فیشینگ (Phishing) خبر داد که در جریان آن مهاجمان با ارسال ایمیل‌هایی در ظاهر پیام‌های حاوی کد احراز هویت دو عاملی (2FA) و هدایت کاربران به سایتی مشابه سایت Instagram اقدام به سرقت نام کاربری و رمز عبور آنها در این شبکه اجتماعی می‌کردند. از نکات برجسته در خصوص این کارزار، استفاده صفحه جعلی از پودمان HTTPS از طریق یک گواهینامه معتبر بود. موضوعی که سبب نمایش نشان سبز رنگ در نوار ابزار مرورگر کاربر و در نتیجه واقعی جلوه کردن صفحه جعلی در نگاه قربانی می‌شود.

رویدادهای مرتبط با باج‌افزارها در شهریور نیز همچنان در صدر اخبار قرار داشتند. در این شماره، ضمن مرور ویژگی‌ها و عملکرد باج‌افزار جدید Nemty به بررسی گزارشی پرداخته شده که در آن STOP به‌عنوان فعال‌ترین باج‌افزار سال میلادی جاری معرفی شده است. بر اساس آمار ارائه شده در گزارش مذکور، در حالی که سال گذشته میلادی سهم باج‌افزار STOP از آلودگی‌ها ۵۰ درصد بوده، این سهم در سال ۲۰۱۹ به ۶۳٫۲ درصد افزایش یافته است. باج‌افزار STOP که نخستین نسخه آن در آذر ۱۳۹۷ شناسایی شد از روش‌های مختلفی برای آلوده کردن سیستم‌ها بهره می‌گیرد. در یکی از این روش‌ها، گردانندگان STOP با تزریق کد مخرب به برخی برنامه‌های موسوم به Crack، Key Generator و Activator و به‌اشتراک‌گذاری آنها در سطح اینترنت دستگاه کاربرانی را که اقدام به دریافت و اجرای این برنامه‌ها می‌کنند را به باج‌افزار آلوده می‌سازند. متأسفانه این شیوه، اصلی‌ترین دلیل انتشار موفق STOP در سطح کشور است.

همچنین بر طبق گزارشی که گروه پروژه صفر شرکت گوگل آن را به‌تازگی منتشر کرده مهاجمان برای مدت حداقل دو سال از طریق تعدادی سایت هک شده اقدام به آلوده‌سازی دستگاه‌های iPhone حتی در صورت به‌روز بودن آنها می‌کرده‌اند. یافته‌های کامل پروژه صفر در این شماره از ماهنامه امنیت فناوری اطلاعات شرکت مهندسی شبکه گستر قابل مطالعه است.

در آخرین ماه تابستان ۱۳۹۸، مهاجمان در چندین کارزار تبلیغ‌افزاری (Malvertising Campaign) با هدایت کاربران به صفحات اینترنتی حاوی بسته‌های بهره‌جو (Exploit Kit) اقدام به نصب بدافزارهای سارق رمز عبور، باج‌افزارها و جاسوس‌افزارها کردند. روش کار بسته‌های بهره‌جوی استفاده شده در جریان این کارزارها در این گزارش به تفصیل مورد بررسی قرار گرفته است.

معرفی اصلاحیه‌های امنیتی و یک ابزار جدید رمزگشایی منتشر شده در شهریور ماه ۱۳۹۸ از دیگر موضوعاتی هستند 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.

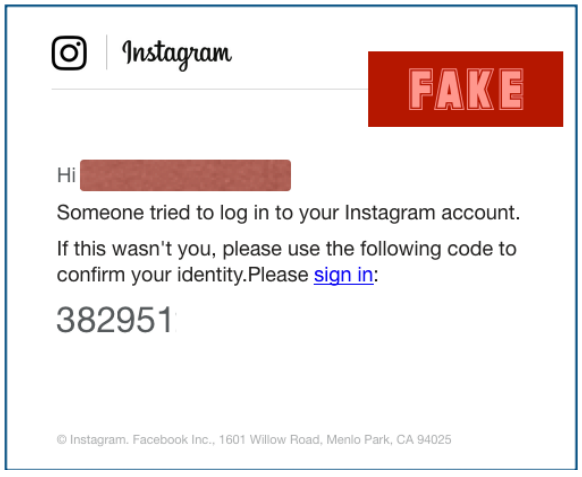
هشـدارهـای امنـیـتی

کاربران Instagram،
هدف کارزاری فیشینگ

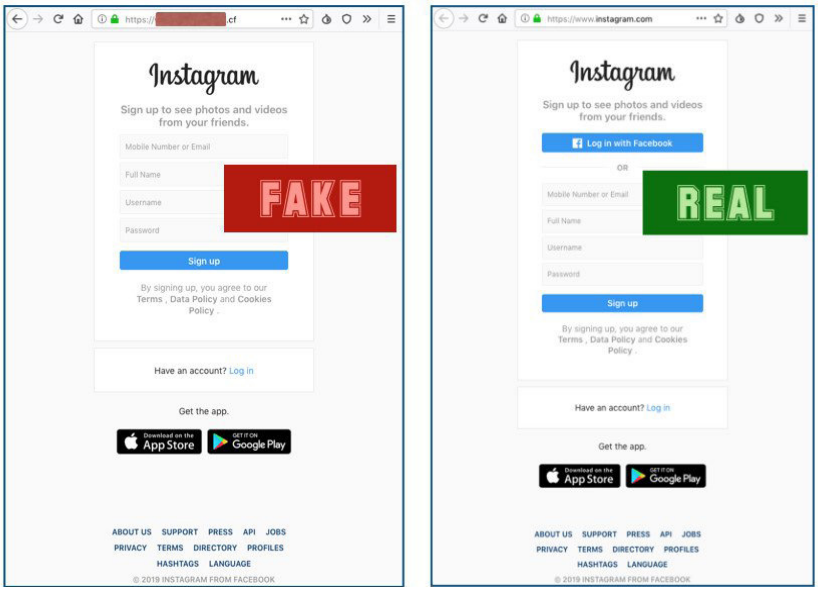
شرکت امنیتی سوفوس از اجرای کارزاری فیشینگ (Phishing) خبر داده که در جریان آن مهاجمان با ارسال ایمیل‌هایی در ظاهر پیام‌های حاوی کد احراز هویت دو عاملی (2FA) و هدایت کاربران به سایتی مشابه سایت Instagram اقدام به سرقت نام کاربری و رمز عبور آنها در این شبکه اجتماعی می‌کنند.

هدف از اجرای حملات فیشینگ، دستیابی به اطلاعات حساسی نظیر رمز عبور با بهره‌گیری از روش‌های موسوم به مهندسی اجتماعی است.

در کارزار اخیر نیز ایمیل ارسالی ظاهری کاملا مشابه با ایمیل‌های Instagram دارد. همانطور که در تصویر زیر پیداست، بغیر از چند اشتباه در درج نشانه‌های سجاوندی و از قلم انداختن یک فاصله خالی پیش از کلمه Please، پیام تفاوتی با پیام‌های واقعی Instagram نداشته و شاید کمتر کاربری متوجه جعلی بودن آن شود.



به گزارش شرکت مهندسی شبکه گستر به نقل از سوفوس، در صورت کلیک بر روی لینک sign in کاربر به صفحه‌ای اینترنتی با ظاهری کاملا مشابه با سایت Instagram هدایت می‌شود. نکته جالب استفاده صفحه جعلی از پودمان HTTPS از طریق یک گواهینامه معتبر است. موضوعی که سبب شده که نشان سبز رنگ نمایان شده در نوار ابزار مرورگر آن را از دید کاربر بی‌دقت واقعی‌تر نشان دهد.



این درحالی است که پسوند استفاده شده در دامنه نشانی سایت جعلی، cf - بجای com - است. cf. دامنه اینترنتی جمهوری آفریقای مرکزی است.

روش اجرای این کارزار فرصتی است برای یادآوری این نکته مهم که صرف استفاده از پودمان HTTPS در نشانی یک سایت به معنای معتبر بودن آن نیست و راهکار اصلی دقت به صحیح بودن نشانی (در اینجا instagram.com) است. همچنین استفاده از احراز هویت دو عاملی نیز همواره توصیه می‌شود.

باج‌افزاری نه چندان مؤدب

که از طریق RDP منتشر می‌شود

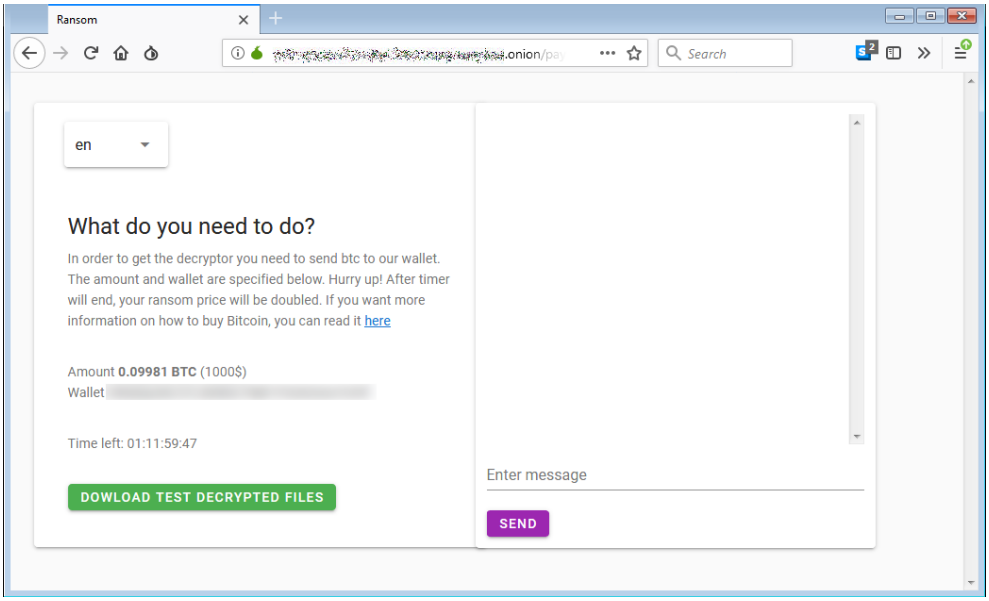
باج‌افزار جدیدی در حال انتشار است که پس از رمزگذاری فایل‌های ذخیره شده بر روی سیستم اقدام به الصاق پسوند nemty به آنها می‌کند. موضوعی که سبب نامگذاری این باج‌افزار به Nemty شده است.

اتصال از راه دور مهاجمان از طریق پودمان Remote Desktop - به اختصار RDP - به دستگاه‌های با رمز عبور ضعیف و اجرای فایل مخرب باج‌افزار روش انتشار Nemty گزارش شده است. در یک سال اخیر، بهره گیری از پودمان RDP به یکی از اصلی‌تری روش‌های انتشار باج‌افزارها به خصوص توسط مهاجمان حرفه ای تبدیل شده است. مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای کشور (ماهر) نیز به دفعات نسبت به تشدید حملات باج‌افزاری از طریق این پودمان هشدار داده است.

به گزارش شرکت مهندسی شبکه گستر، Nemty در ازای آنچه که بازگرداندن فایل‌ها به حالت اولیه می‌خواند مبلغ 0.09981 بیت‌کوین را از قربانی اخاذی می‌کند.

```
 ---=== NEMTY PROJECT ===---

[+] Whats Happen? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on you computer has extension .nemty
By the way, everything is possible to restore, but you need to follow our instructions. Otherwise, you cant return your data (NEVER).

[+] What guarantees? [+]

It's just a business. We absolutely do not care about you and your deals, except getting benefits.
If we do not do our work and liabilities - nobody will not cooperate with us.
It's not in our interests.
If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just we have the private key.
In practise - time is much more valuable than money.

[+] How to get access on website? [+]

  1) Download and install TOR browser from this site: https://torproject.org/
  2) Open our website: zjoxyw5mkacojk5ptn2iprkivg5clow72mjkyk5ttubzxprjjnwapkad.onion/pay

When you open our website, follow the instructions and you will get your files back.
```

فرایند پرداخت در سامانه‌ای صورت می‌گیرد که در شبکه ناشناس Tor میزبانی شده است. همچنین قابلیتی برای گفتگوی اینترنتی با مهاجم یا مهاجمان پشت پرده این باج‌افزار در نظر گرفته شده است.



Nemty همچون بسیاری از باج‌افزارهای دیگر اقدام به حذف فایل‌های موسوم به Shadow Copy می‌کند.

ضمن اینکه از رمزگذاری فایل‌های با نام و پسوند DECRYPT.txt و فایل‌های با هر یک از پسوندهای زیر پرهیز می‌کند:

nemty, log, LOG, CAB, cab, CMD, cmd, COM, com, cpl, CPL, exe, EXE, ini, INI, dll, DLL, lnk, LNK, url, URL, ttf, TTF

بخشی از کد Nemty حاوی لینک به تصویری از ولادیمیر پوتین، رییس جمهور روسیه است. البته نوشته‌های روسی درج شده بر روی تصویر نشان می‌دهد که درج لینک نه از روی علاقه که احتمالا از روی نفرت صورت گرفته است.

در بخشی دیگر از کد نیز با عبارتی غیرمؤدبانه به صنعت ضدویروس تاخته شده است.

بسیاری از باج‌افزارهای با اصالت روسی اطمینان حاصل می‌کنند که دستگاه آلوده شده در کشوری از کشورهای عضو سابق اتحاد جماهیر شوروی قرار نداشته باشد. در غیر این صورت اجرای خود را با این هدف که گرفتار قوانین مشترک بین این کشورها نشوند متوقف می‌کنند. Nemty نیز بررسی می‌کند که آیا دستگاه در یکی از کشورهای روسیه، بلاروس، قزاقستان، تاجیکستان و اوکراین قرار دارد یا خیر. اما نه با این قصد که به فایل‌های آنها دست‌درازی نکند. بلکه علاوه بر رمزگذاری، مشخصه‌های بیشتری را از روی دستگاه‌های این کشورها جمع‌آوری می‌کند!

لازم به ذکر است که Nemty با نام‌های زیر قابل شناسایی است:

Bitdefender:
- Trojan.GenericKD.41613105

McAfee:
- RDN/Ransom

Sophos:
- Mal/Generic-S

اطلاعات بیشتر در خصوص Nemty در اینجا قابل دریافت و مطالعه است.

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

استفاده گسترده مهاجمان
از بسته‌های بهره‌جو در روزهای اخیر

طی روزهای گذشته، مهاجمان در چندین کارزار تبلیغ‌افزاری (Malvertising Campaign)، با هدایت کاربران به صفحات اینترنتی حاوی بسته‌های بهره‌جو (Exploit Kit) اقدام به نصب بدافزارهای سارق رمز عبور، باج‌افزارها و جاسوس‌افزارها کرده‌اند.

بسیاری از صفحات اینترنتی مذکور متعلق به سایت‌های هک شده‌ای هستند که در حال حاضر در کنترل مهاجمان قرار گرفته‌اند.

به‌محض مراجعه کاربر به هر یک از این صفحات، بسته بهره‌جو به‌صورت خودکار و بدون نیاز به دخالت کاربر اقدام به سوءاستفاده از آسیب‌پذیری (Vulnerability) نرم‌افزارهای نصب شده بر روی دستگاه کرده و کد مخرب را به اجرا در می‌آورد.

از جمله بدافزارهای منتشر شده در جریان این کارزارها می‌توان به اسب تروای بانکی Ramnit اشاره کرد. بسته بهره‌جوی استفاده شده برای انتشار اسب تروای مذکور، GrandSoft گزارش شده است.

Ramnit پس از اجرا بر روی دستگاه قربانی اقدام به سرقت اطلاعات حساسی از جمله اطلاعات اصالت‌سنجی وارد شده در سایت‌های بانکی، حساب‌های کاربری FTP و سوابق مرورگر (Browser) می‌کند. ضمن اینکه Ramnit دارای قابلیتی است که امکان تزریق کد (Code Injection) در سایت‌های فراخوانی شده در مرورگر کاربر - و در نتیجه دست‌درازی به آنها - را فراهم می‌کند.

Rig، دیگر بسته بهره‌جویی است که در هفته‌های اخیر در کارزارهای تبلیغ‌افزاری به‌منظور انتشار بدافزار Amadey بکار گرفته شده است. این بسته بهره‌جو از آسیب‌پذیری‌هایی همچون CVE-2018-15982 در نرم‌افزار Flash Player و CVE-2018-8174 در مرورگر Internet Explorer سوءاستفاده می‌کند.

به گزارش شرکت مهندسی شبکه گستر، بدافزار Amadey ضمن افزودن دستگاه قربانی به یک شبکه مخرب (Botnet)، اقدام به سرقت اطلاعات و دریافت و اجرای سایر بدافزارها می‌کند.

سومین بسته بهره‌جوی استفاده شده در این کارزارها، Fallout است که از آسیب‌پذیری CVE-2018-8174 در مرورگر Internet Explorer و از آسیب‌پذیری CVE-2018-4878 در محصول Flash Player سوءاستفاده کرده و کد مخرب مورد نظر مهاجمان را بر روی دستگاه قربانی به‌صورت از راه دور نصب و اجرا می‌کند.

Rig و Fallout هر دو در انتشار چند نمونه از بدافزارهای موسوم به سارق بریده‌دان (Clipboard Hijacker) نقش داشته‌اند.

برخی از این نمونه‌ها با تحت رصد قرار دادن بریده‌دان، در زمان قرار گرفتن نشانی کیف بیت‌کوین در آن، نشانی را با یک نشانی تحت کنترل نویسنده بدافزار جایگزین می‌کنند. بنابراین در صورت عدم دقت کاربر در زمان زدن دگمه ارسال، عملاً مبلغ وارد شده، بجای گیرنده واقعی، نصیب نویسنده بدافزار می‌شود.

از دیگر بسته‌های بهره‌جوی شاخص استفاده شده می‌توان به Radio اشاره کرد که از یک آسیب‌پذیری قدیمی با شناسه CVE-2016-0189 در مرورگر Internet Explorer سوءاستفاده می‌کند. باج‌افزار Nemty یکی از بدافزارهای منتشر شده توسط این بسته بهره‌جو بوده است.

علاوه بر Radio بسته بهره‌جوی RIG نیز در انتشار Nemty که به‌نظر می‌رسد نویسندگان آن به‌سرعت در حال تکامل و ارتقای این باج‌افزار هستند نقش داشته است.

اصلی‌ترین راهکار در بی‌اثر کردن تهدیدات مبتنی بر بهره‌جو، نصب به‌موقع بسته‌ها و اصلاحیه‌های امنیتی (Service Packs and Updates) سیستم عامل و کلیه نرم‌افزارهای کاربردی نصب شده بر روی تمامی سیستم‌هاست. ضمن اینکه استفاده از ابزارهایی همچون WSUS و Bitdefender Patch Management برای مدیریت فرایند نصب اصلاحیه‌ها توصیه می‌شود.

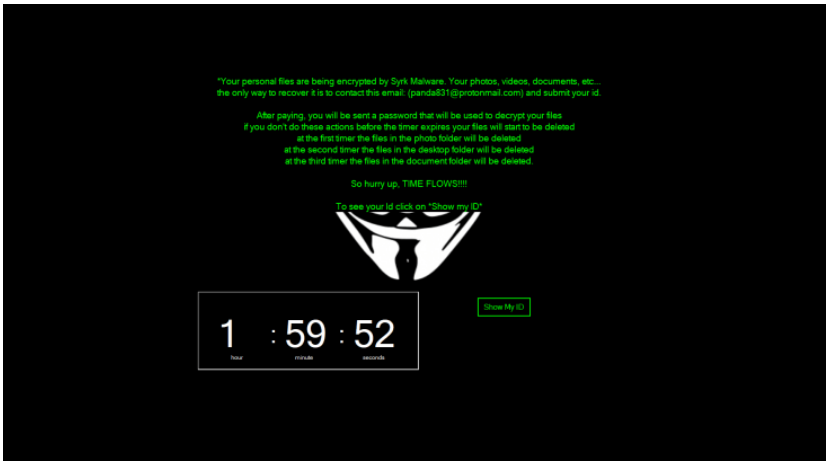
رویدادهای امنیتی

عرضه ابزار رمزگشایی برای قربانیان باج‌افزار Syrk

محققان موفق به ساخت ابزاری شده‌اند که قربانیان Syrk را قادر به رمزگشایی رایگان فایل‌های رمز شده توسط این باج‌افزار می‌کند.

به گزارش شرکت مهندسی شبکه گستر، این باج‌افزار که به نظر می‌رسد توسعه آن هنوز نهایی نشده است پس از غیرفعال کردن ضدویروس نصب شده بر روی دستگاه، اقدام به رمزگذاری فایل‌های کاربر با استفاده از الگوریتم AES-256 می‌کند.

نمونه‌ای از اطلاعیه باج‌گیری Syrk در تصویر زیر نمایش داده شده است.

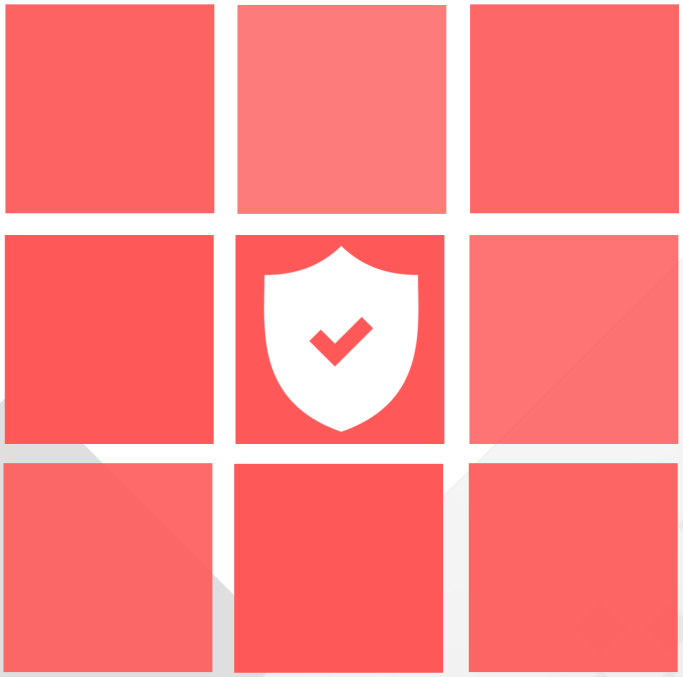


تزریق کد اجرایی باج‌افزار به فایلی در ظاهر با عملکرد هک بازی Fortnite و به اشتراک‌گذاری آن بر روی اینترنت اصلی‌ترین روش انتشار Syrk گزارش شده است.

خوشبختانه محققان امسی‌سافت موفق شده‌اند تا با شناسایی رمزگشایی که در کد باج‌افزار جاسازی شده ابزاری برای بازگرداندن رایگان فایل های رمزگذاری شده توسط این نسخه از Syrk ارائه کنند. ابزار مذکور در اینجا قابل دریافت و استفاده است.

همانطور که اشاره شد این باج‌افزار همچنان در حال توسعه بوده و احتمالا در نسخه‌های آتی Syrk باگ وجود رمزگشا در آن مرتفع خواهد شد. بنابراین همچون همیشه بکارگیری روش‌های پیشگیرانه در مقابله با باج‌افزارها برای ایمن ماندن از گزند این بدافزارهای مخرب توصیه می‌شود.

آسیب‌پذیری‌ها
و اصلاحیه‌های امنیتی



اصلاحیه‌های امنیتی مایکروسافت
برای ماه میلادی سپتامبر

به گزارش شرکت مهندسی شبکه گستر، سه‌شنبه ۱۹ شهریور، شرکت مایکروسافت اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی سپتامبر منتشر کرد. این اصلاحیه‌ها در مجموع، ۸۵ آسیب‌پذیری را در سیستم عامل Windows و برخی دیگر از محصولات مایکروسافت ترمیم می‌کنند. درجه اهمیت ۱۹ مورد از آسیب‌پذیری‌های ترمیم شده توسط اصلاحیه‌های مذکور "حیاتی" (Critical)، ۶۵ مورد "بااهمیت" (Important) و یک مورد "متوسط" (Moderate) 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.

آسیب‌پذیری‌های حیاتی ترمیم‌شده

CVE-2019-1291، CVE-2019-1290، CVE-2019-0788 و CVE-2019-0787 از جمله ضعف‌های امنیتی "حیاتی" ترمیم شده توسط اصلاحیه های این ماه هستند که بخش Remote Desktop Protocol - به اختصار RDP - سیستم عامل Windows از آنها تأثیر می‌پذیرد. مهاجم با ارسال یک درخواست دستکاری شده به پودمان RDP دستگاه مورد نظر قادر به بهره‌جویی (Exploit) از این باگ‌ها خواهد بود. در صورت موفقیت در بهره‌جویی، امکان اجرای هر نوع کد به‌صورت از راه دور (Remote Code Execution) و بدون نیاز به دخالت کاربر برای مهاجم فراهم می‌شود.

CVE-2019-1257، CVE-2019-1296 و CVE-2019-1295 دیگر آسیب‌پذیری‌های "حیاتی" ترمیم شده در این ماه هستند که نرم‌افزار SharePoint از آنها تأثیر می‌پذیرد. این اشکالات از حفاظت ناقص برخی توابع در این نرم‌افزار ناشی می‌شوند. سوءاستفاده از آسیب‌پذیری‌های مذکور امکان اجرای کد را به‌صورت از راه دور در بخش‌های موسوم به Application Pool و Server Farm Account این نرم افزار فراهم می‌کند.

CVE-2019-0719 و CVE-2019-0721 نیز دو آسیب‌پذیری به حملات اجرای کد به‌صورت از راه دور هستند که در Hyper-V - بستر مجازی‌سازی مایکروسافت قابل بهره‌جویی هستند. عدم اعتبارسنجی صحیح ورودی‌های ارسالی از سوی کاربر اصالت‌سنجی نشده از روی ماشین میهمان به Network Switch سرور میزبان موجب بروز این آسیب‌پذیری‌ها شده است. بنابراین با اجرای یک برنامه حاوی کد بهره‌جویی آسیب‌پذیری‌های مذکور بر روی سیستم عامل میهمان، اجرای کد بر روی سرور میزبان نیز برای مهاجم ممکن می‌شود.

CVE-2019-1138، CVE-2019-1217، CVE-2019-1221، CVE-2019-1237، CVE-2019-1298 و CVE-2019-1300 دیگر آسیب‌پذیری‌های "حیاتی" ترمیم شده در این ماه هستند که همگی از مدیریت ناصحیح حافظه در موتور چیدمان JavaScript/JScript مایکروسافت، معروف به Chakra که در مرورگرهای این شرکت مورد استفاده قرار می‌گیرد ناشی می‌شوند. سوءاستفاده از این اشکالات منجر به بروز اشکال در حافظه و فراهم شدن امکان اجرای کد بر روی دستگاه قربانی می‌شود.

CVE-2019-1208 و CVE-2019-1236، دو آسیب‌پذیری "حیاتی" در بخش VBScript Engine سیستم عامل Windows هستند که با مراجعه کاربر به یک سایت حاوی بهره‌جوی هر یک از این ضعف‌های امنیتی امکان اجرای کد بر روی دستگاه بدون نیاز به دخالت آن کاربر امکان‌پذیر می‌شود.

همچنین در اصلاحیه‌های این ماه یک آسیب‌پذیری اجرای کد به‌صورت از راه دور به شناسه CVE-2019-1280 در سیستم عامل Windows برطرف شده است. با اجرای یک فایل میانبر (LNK) توسط کاربر، امکان اجرای کد با سطح دسترسی کاربر فعلی بر روی دستگاه توسط مهاجم فراهم می‌شود.

CVE-2019-1306، آخرین اصلاحیه "حیاتی" ترمیم شده در این ماه است که Azure DevOps Server و Team Foundation Server از آن تأثیر می‌پذیرند. با باز شدن یک فایل دستکاری شده توسط کاربر در این بسترها، اجرای کد مورد نظر مهاجم با سطح دسترسی کاربر فعلی فراهم می‌شود.

آسیب‌پذیری‌های بااهمیت وصله‌شده

از میان آسیب‌پذیری‌های "بااهمیت" برطرف شده در این ماه، جزییات سه مورد زیر پیش‌تر به‌صورت عمومی منتشر شده بود:

- CVE-2019-1235 که ضعفی از نوع ترفیع امتیازی (Elevation of Privilege) در بخش Text Service Framework سیستم عامل Windows است.
- CVE-2019-1253 که یک آسیب‌پذیری به حملات ترفیع امتیازی در سیستم عامل Windows است.
- CVE-2019-1294 که اشکالی از نوع عبور از سد تنظیمات امنیتی (Security Bypass) در بخش Secure Boot سیستم عامل Window است.

همچنین سه آسیب‌پذیری با درجه "بااهمیت" که توسط اصلاحیه‌های ماه سپتامبر برطرف شده‌اند از قبل مورد بهره‌جویی مهاجمان قرار گرفته‌اند. این سه با شناسه‌های CVE-2019-1214، CVE-2019-1215 و CVE-2019-1279 همگی از نوع ترفیع امتیازی بوده و بخش Common Log File System Driver - به اختصار CLFS - در سیستم عامل Windows را هدف قرار می‌دهند.

سایر آسیب‌پذیری‌های با درجه "بااهمیت" این ماه عبارتند از:

CVE-2019-0712	CVE-2019-1233	CVE-2019-1249	CVE-2019-1264	CVE-2019-1274	CVE-2019-1289
CVE-2019-0928	CVE-2019-1240	CVE-2019-1250	CVE-2019-1265	CVE-2019-1277	CVE-2019-1292
CVE-2019-1142	CVE-2019-1241	CVE-2019-1251	CVE-2019-1266	CVE-2019-1278	CVE-2019-1293
CVE-2019-1209	CVE-2019-1242	CVE-2019-1252	CVE-2019-1267	CVE-2019-1281	CVE-2019-1297
CVE-2019-1216	CVE-2019-1243	CVE-2019-1254	CVE-2019-1268	CVE-2019-1282	CVE-2019-1299
CVE-2019-1219	CVE-2019-1244	CVE-2019-1256	CVE-2019-1269	CVE-2019-1283	CVE-2019-1301
CVE-2019-1220	CVE-2019-1245	CVE-2019-1260	CVE-2019-1270	CVE-2019-1284	CVE-2019-1302
CVE-2019-1230	CVE-2019-1246	CVE-2019-1261	CVE-2019-1271	CVE-2019-1285	CVE-2019-1303
CVE-2019-1231	CVE-2019-1247	CVE-2019-1262	CVE-2019-1272	CVE-2019-1286	CVE-2019-1305
CVE-2019-1232	CVE-2019-1248	CVE-2019-1263	CVE-2019-1273	CVE-2019-1287	

آسیب‌پذیری متوسط برطرف‌شده

CVE-2019-1259 نیز تنها آسیب‌پذیری با درجه اهمیت "متوسط" است که نرم‌افزار SharePoint از آن تأثیر می‌پذیرد.

همچون همیشه نصب به‌موقع اصلاحیه‌های امنیتی، به خصوص در موارد با آسیب‌پذیری‌های با درجه "حیاتی" و "بااهمیت" به تمامی کاربران و راهبران شبکه توصیه می‌گردد.

اصلاحیه‌های امنیتی ادوبی
برای ماه میلادی سپـتـامبـر

به گزارش شرکت مهندسی شبکه گستر، سه‌شنبه ۱۹ شهریور، شرکت ادوبی مجموعه اصلاحیه‌های امنیتی ماه میلادی سپتامبر خود را منتشر کرد.

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

- Flash Player
- Application Manager

دو مورد از آسیب‌پذیری‌های ترمیم شده توسط این اصلاحیه‌ها، نرم‌افزار Flash Player را تحت تأثیر قرار می‌دهند. آسیب‌پذیری‌های مذکور با شناسه‌های CVE-2019-8070 و CVE-2019-8069، "حیاتی" (Critical) گزارش شده و مهاجم با بهره‌جویی از هر یک از آنها قادر به اجرای کد بر روی دستگاه قربانی خواهد بود.

با نصب به‌روزرسانی ماه سپتامبر برای Flash Player، نسخه این نرم‌افزار به 32.0.0.255 ارتقاء می‌یابد.

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

- https://helpx.adobe.com/security/products/flash-player/apsb19-46.html
- https://helpx.adobe.com/security/products/application_manager/apsb19-45.html

یادآوری می‌شود سوءاستفاده نفوذگران از آسیب‌پذیری‌های Flash Player به‌خصوص در حملات مبتنی بر وب و "دانلودهای سر راهی" (Drive-by Download) یکی از روش‌های رایج آلوده کردن دستگاه‌ها محسوب می‌شود و به همین خاطر نصب اصلاحیه‌های این نرم‌افزار دارای اهمیت بسزائی است. البته خوانندگان اطلاع دارند که امکان به‌روزرسانی خودکار نرم‌افزارهای ادوبی با نشانی‌های IP ایرانی وجود نداشته و کاربران و مدیران شبکه باید با استفاده از روش‌ها و ابزارهای دیگر اقدام به این کار کنند.

هشدار مرکز ماهر در خصوص وجود آسیب‌پذیری حیاتی
در سرویس‌دهنده ایمیل Exim

مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای کشور (ماهر) با انتشار مطلبی نسبت به وجود یک آسیب‌پذیری حیاتی با شناسه CVE-2019-15846 در سرویس‌دهنده ایمیل Exim هشدار داده است.

به گفته این مرکز این دومین بار در سال جاری است که ضعفی از نوع RCE (با امکان حمله از راه دور) در این سرویس‌دهنده شناسایی می‌شود. با سوءاستفاده از آسیب‌پذیری مذکور مهاجم قادر خواهد بود تا کدهای مخرب خود را با سطح دسترسی root بر روی سرور میزبان اجرا کند.

نسخه‌های آسیب‌پذیر معرفی شده، شامل 4.92.1 و همه نسخه‌های قبل از آن می‌باشد.

ماهر تأکید کرده که در صورت استفاده از این سرویس‌دهنده لازم است بی‌درنگ نسبت به به‌روزرسانی Exim به نسخه 4.92.2 اقدام شود. عمده سرویس‌دهندگان آسیب‌پذیر متعلق به شرکت‌های میزبانی هستند.

مشروح اطلاعیه ماهر در اینجا قابل دریافت و مطالعه است.

ماجرای جاسوسی دو ساله
از صاحبان iPhone

بر اساس گزارشی که گروه پروژه صفر شرکت گوگل آن را به‌تازگی منتشر کرده مهاجمان برای مدت حداقل دو سال از طریق تعدادی سایت هک شده اقدام به آلوده‌سازی دستگاه‌های iPhone حتی در صورت به‌روز بودن آنها می‌کرده‌اند.

با مراجعه به این سایت‌ها که حاوی کد بهره‌جوی (Exploit) چندین آسیب‌پذیری حیاتی و تا آن زمان ناشناخته در سیستم عامل iOS بوده‌اند بدون اطلاع و دخالت کاربر فرایند بهره‌جویی از دستگاه انجام شده و در ادامه یک ابزار رصد یا به عبارتی دقیق‌تر جاسوس‌افزار بر روی گوشی نصب می‌شده است. بنابراین تنها مراجعه به هر یک از این سایت‌ها از طریق iPhone برای آلوده شدن گوشی کفایت می‌کرده است.

به گزارش شرکت مهندسی شبکه گستر، در اوایل ماه فوریه سال میلادی جاری، گروه تحلیل تهدید شرکت گوگل (TAG)، در جریان بررسی سایت‌های هک شده موفق به شناسایی پنج زنجیره آسیب‌پذیری می‌شود که تمامی نسخه‌های ۱۰ تا ۱۲ سیستم عامل iOS از آنها تأثیر می‌پذیرفته‌اند. مهاجمان با بکارگیری این زنجیره‌ها قادر به عبور از سد لایه‌های حفاظتی گوشی‌های iPhone می‌شده‌اند.

در مجموع، آسیب‌پذیری‌های ناشناخته استفاده شده در زنجیره‌های مذکور ۱۴ مورد اعلام شده که در این میان، تعداد ۷ مورد مربوط به مرورگر Safari، ۵ مورد مرتبط با هسته iOS و ۲ مورد نیز در ارتباط با بخش Sandbox این سیستم عامل است.

با مراجعه کاربر به یکی از سایت‌های حاوی کد بهره‌جو با استفاده از iPhone، سایت دستگاه را مورد بررسی قرار داده و در صورت آسیب‌پذیر بودن آن اقدام به اجرای جاسوس‌افزار بر روی آن می‌کرده است. هدف مهاجمان در استفاده از این جاسوس‌افزار، جمع‌آوری فایل‌ها و اطلاعات شخصی کاربر و ارسال آنها به سرور تحت کنترل خود گزارش شده است.

گفته می‌شود این سایت‌ها حداقل از سال ۲۰۱۷ به تسخیر مهاجمان در آمده بودند.

این جاسوس‌افزار به بانک داده کلیه برنامک‌های نصب شده بر روی گوشی نظیر WhatsApp، Telegram و iMessage دسترسی داشته و عملا امکان استخراج هر نوع اطلاعات ذخیره شده توسط برنامک‌ها را دارا بوده است.

جاسوس‌افزار، زنجیره کلید دستگاه شامل اطلاعات اصالت‌سنجی، گواهینامه‌ها و توکن‌های استفاده شده در سرویس‌هایی نظیر Single Sign-on را که برای دسترسی به برخی حساب‌ها از آنها استفاده می‌شود نیز سرقت می‌کرده است.

بازه برقراری ارتباطی جاسوس‌افزار با سرور فرماندهی خود هر ۶۰ ثانیه یکبار اعلام شده است.

گوگل پس از شناسایی این کارزار، وجود آسیب‌پذیری‌ها را به شرکت اپل گزارش کرد. در اعلام گوگل فرصتی یک هفته‌ای برای ترمیم این آسیب‌پذیری‌ها به اپل داده شده بود. اپل نیز در ۷ فوریه با عرضه نسخه 12.1.4 سیستم عامل iOS، اشکالات و باگ‌های امنیتی گزارش شده را ترمیم کرد.

در دنیای امنیت فناوری اطلاعات معمول است چنانچه سازنده در مهلت تعیین شده - که در عرف سه ماه است - آسیب‌پذیری را برطرف نکند، کاشف اقدام به افشای وجود آن به‌صورت عمومی می‌کند. مهلت‌های یک هفته‌ای گوگل به سازندگان محصولات نرم‌افزاری انتقادات برخی شرکت‌ها را در پی داشته است.

با این حال علیرغم ترمیم آسیب‌پذیری‌ها توسط اپل در ۷ فوریه، گوگل اعلام عمومی آن را به هفته گذشته موکول کرده بود.

با توجه به بهره‌جویی مهاجمان از این آسیب‌پذیری‌ها، به تمامی کاربران iPhone توصیه می‌شود چنانچه تا کنون سیستم عامل گوشی خود را به نسخه جدید ارتقا نداده‌اند در زودترین زمان ممکن نسبت به انجام آن اقدام کنند.

مشروح گزارش گوگل در اینجا قابل مطالعه است.

اصلاحیه‌های عرضه شده
در شهریور ۱۳۹۸

در شهریور ماه، علاوه بر مایکروسافت و ادوبی، شرکت‌های گوگل، اپل، سیسکو، سوپرمایکرو، موزیلا و وی‌اِم‌وِر و بنیاد وردپرس اقدام به انتشار اصلاحیه و توصیه‌نامه امنیتی برای برخی از محصولات خود کردند.

در این ماه شرکت گوگل در سه نوبت با عرضه به‌روزرسانی اقدام به ترمیم آسیب‌پذیری‌های امنیتی مرورگر Chrome کرد. بهره‌جویی از برخی از آسیب‌پذیری‌های مذکور مهاجم را قادر به در اختیار گرفتن کنترل سیستم می‌کند. آخرین نسخه عرضه شده از این مرورگر 77.0.3865.90 است. فهرست اشکالات مرتفع شده در این نسخه نیز در اینجا قابل دریافت و مشاهده است.

پنجم شهریور، شرکت اپل نیز با انتشار به‌روزرسانی، ضعف‌هایی امنیتی را در سیستم‌های عامل زیر ترمیم و اصلاح کرد:

- watchOS
- iOS
- macOS Mojave
- tvOS

سوءاستفاده از برخی از این ضعف‌ها امکان در اختیار گرفتن کنترل سیستم را برای مهاجم فراهم می‌کند. توضیحات بیشتر در خصوص به‌روزرسانی‌های منتشر شده در لینک‌های زیر قابل مطالعه است:

- https://support.apple.com/en-us/HT201222
- https://support.apple.com/en-us/HT210549
- https://support.apple.com/en-us/HT210548
- https://support.apple.com/en-us/HT210550

به گزارش شرکت مهندسی شبکه گستر، در این ماه، سیسکو در چندین نوبت اقدام به انتشار به‌روزرسانی‌های امنیتی کرد. این به‌روزرسانی‌ها در مجموع، ۳۳ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت ۵ مورد از این آسیب‌پذیری‌ها "حیاتی" (Critical) و ۱۲ مورد از آنها "بالا" (High) گزارش شده است. آسیب‌پذیری به حملاتی همچون اجرای کد به‌صورت از راه دور و عبور از سد تنظیمات امنیتی، از جمله اشکالات مرتفع شده توسط به‌روزرسانی‌های جدید است. توضیحات کامل در مورد به‌روزرسانی‌های عرضه شده در اینجا قابل دسترس است.

در اواسط شهریور ماه، شرکت سوپرمایکرو با عرضه به‌روزرسانی، ضعف‌هایی از نوع اصالت‌سنجی با متن ساده، رمزگذاری ضعیف و سیستم احراز هویت آسیب‌پذیر را در بخش Baseboard Management Controller - به اختصار BMC - بسترهای X9، X10 و X11 محصولات خود برطرف کرد. توصیه‌نامه سوپرمایکرو که در آن به این ضعف‌های امنیتی پرداخته شده در اینجا قابل مطالعه است.

شرکت موزیلا نیز با انتشار به‌روزرسانی، چندین آسیب‌پذیری را در مرورگر Firefox ترمیم کرد. سوءاستفاده از برخی از ضعف‌های مذکور به مهاجم امکان می‌دهد تا به‌صورت از راه دور اقدام به آلوده کردن دستگاه آسیب‌پذیر کند. جزییات بیشتر در اینجا، اینجا و اینجا قابل مطالعه است.

۱۵ شهریور ماه هم بنیاد وردپرس نسخه 5.2.3 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 دریافت است.

وی‌اِم‌وِر دیگر شرکتی بود که در شهریور ماه ۱۳۹۸ اقدام به انتشار به‌روزرسانی برای محصولات خود کرد. محصولات زیر از شش آسیب‌پذیری ترمیم شده توسط این به‌روزرسانی‌ها تأثیر می‌پذیرند:

- VMware vSphere ESXi
- VMware vCenter Server
- VMware Workstation Pro / Player
- VMware Fusion Pro / Fusion
- VMware Remote Console for Windows
- VMware Remote Console for Linux
- VMware Horizon Client for Windows
- VMware Horizon Client for Linux
- VMware Horizon Client for Mac

توضیحات کامل در این خصوص در لینک‌های زیر قابل مطالعه است.

- https://www.vmware.com/security/advisories/VMSA-2019-0013.html
- https://www.vmware.com/security/advisories/VMSA-2019-0014.html

همچنین در شهریور ماه مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای کشور (ماهر) در مطلبی به بررسی یک آسیب‌پذیری خطرناک در برخی محصولات شرکت زیمنس پرداخت که مشروح آن در اینجا قابل دریافت است.

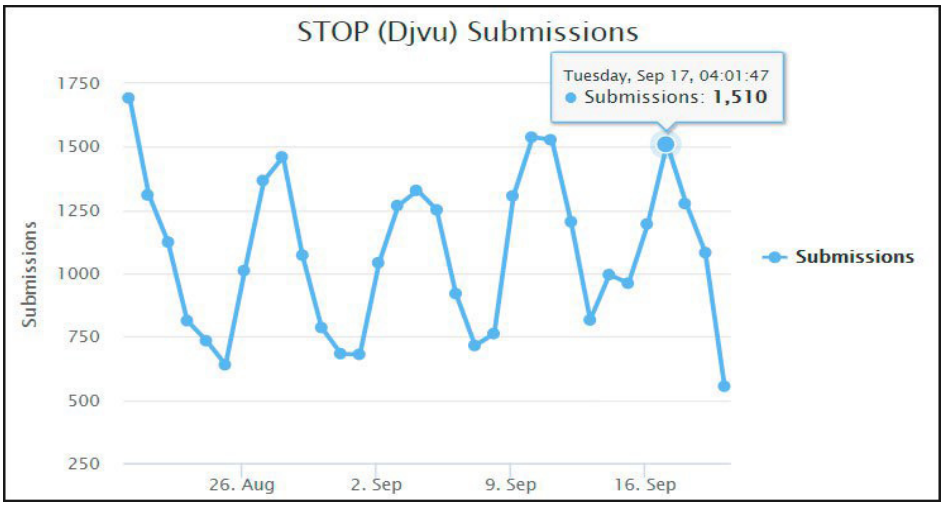
گـزارش‌هـا

STOP؛
فعال‌ترین باج‌افزار حال حاضر

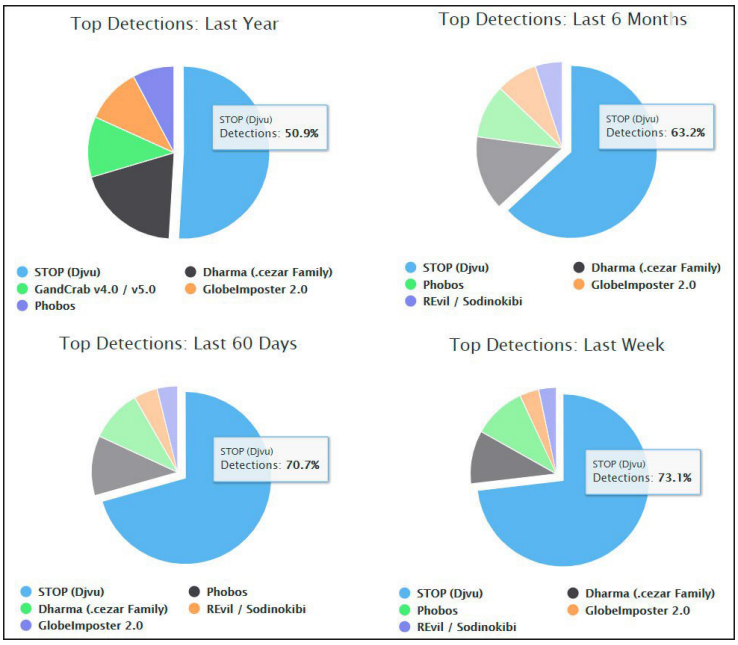
بر اساس گزارشی که سایت BleepingComputer آن را منتشر کرده، STOP، فعال‌ترین باج‌افزار سال میلادی جاری بوده است.

از جمله منابع BleepingComputer در انتشار این گزارش آمار سایت ID-Ransomware است. این سایت با در اختیار داشتن الگوی شناسایی صدها باج‌افزار قربانی را قادر می‌کند تا نام باج‌افزار را شناسایی کند. ضمن اینکه در صورت وجود ابزار رمزگشایی برای آن باج‌افزار کاربر به مسیری صحیح برای دریافت ابزار مربوطه هدایت می‌شود.

بر طبق این گزارش، به‌طور میانگین در هر روز ۲۵۰۰ نمونه باج‌افزار به سایت ID-Ransomware ارسال می‌شود. از این میان، بین ٦٠ تا ۷۰ درصد آنها نمونه‌هایی از باج‌افزار STOP هستند.



بررسی دقیق‌تر آمار نشان می‌دهد در حالی که سال گذشته میلادی سهم STOP از این ارسال‌ها تنها کمی بیش از ۵۰ درصد بوده، این سهم در سال ۲۰۱۹ به ۶۳/۲ درصد افزایش یافته است.



به گزارش شرکت مهندسی شبکه گستر، 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 را به باج‌افزار آلوده می‌سازند. متأسفانه این شیوه، اصلی‌ترین دلیل انتشار موفق STOP در سطح کشور است. به‌خصوص آنکه در زمان اجرای چنین برنامه‌هایی بسیاری از کاربران اقدام به غیرفعال کردن موقت ضدویروس خود کرده و همین مدت کم، برای اجرا شدن باج‌افزار و شروع فرایند رمزگذاری کافی خواهد بود.

از جمله برنامه‌های مورد استفاده توسط نویسندگان STOP می‌توان به Crack نرم‌افزارهای KMSPico، Cubase، Photoshop و برنامه‌های ضدویروس اشاره کرد.

حتی برخی از این نمونه‌ها مجهز به بدافزار سارق رمز عبور Azorult هستند و بنابراین خرابکاری آنها تنها محدود به رمزگذاری فایل‌های کاربر نبوده و چه بسا اطلاعات حساس قربانی نیز از طریق این بدافزار به دست مهاجمان رسانده شود.

یکی از ویژگی‌های باج‌افزار STOP عرضه و انتشار نسخه‌های متعددی از آن است. تا زمان نگارش این مطلب حداقل ۱۵۹ نسخه از این باج‌افزار شناسایی شده است.

خوشبختانه در برخی نمونه‌ها از این باج‌افزار، از کلید رمزگذاری آفلاین (و نه آنلاین) 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 این دو فایل معرفی شده می‌بایست بیشتر از ۱۵۰ کیلوبایت باشد.

علیرغم انتشار گسترده STOP در مقایسه با باج‌افزارهای هم قطار خود کمتر مورد توجه رسانه ها قرار گرفته است. شاید یکی از اصلی‌ترین دلایل آن غیرهدفمند بودن حملات STOP - بر خلاف باج‌افزارهایی همچون GandCrab که به‌طور خاص سازمان‌های بزرگ را مورد حمله قرار می‌دادند -باشد. با این حال شرکت مهندسی شبکه گستر نیز در این چندین نوبت نسبت به انتشار گسترده این باج‌افزار در ایران هشدار داده است.

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

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	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