فروردین

۱۳۹۹

ماهنامه

امنیت فناوری اطلاعات

شبکه گستر

امنیت شما | وظیفه ما

newsroom.shabakeh.net

@SGnewsroom

فهرست مطالب

چکیده مدیریتی

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

در این ماه چندین نهاد بین‌المللی و شرکت امنیتی در خصوص افزایش حملات باج‌افزاری بر ضد مراکز فعال در حوزه سلامت و درمان هشدار دادند که به نمونه‌های برجسته آنها در این ماهنامه پرداخته شده است.

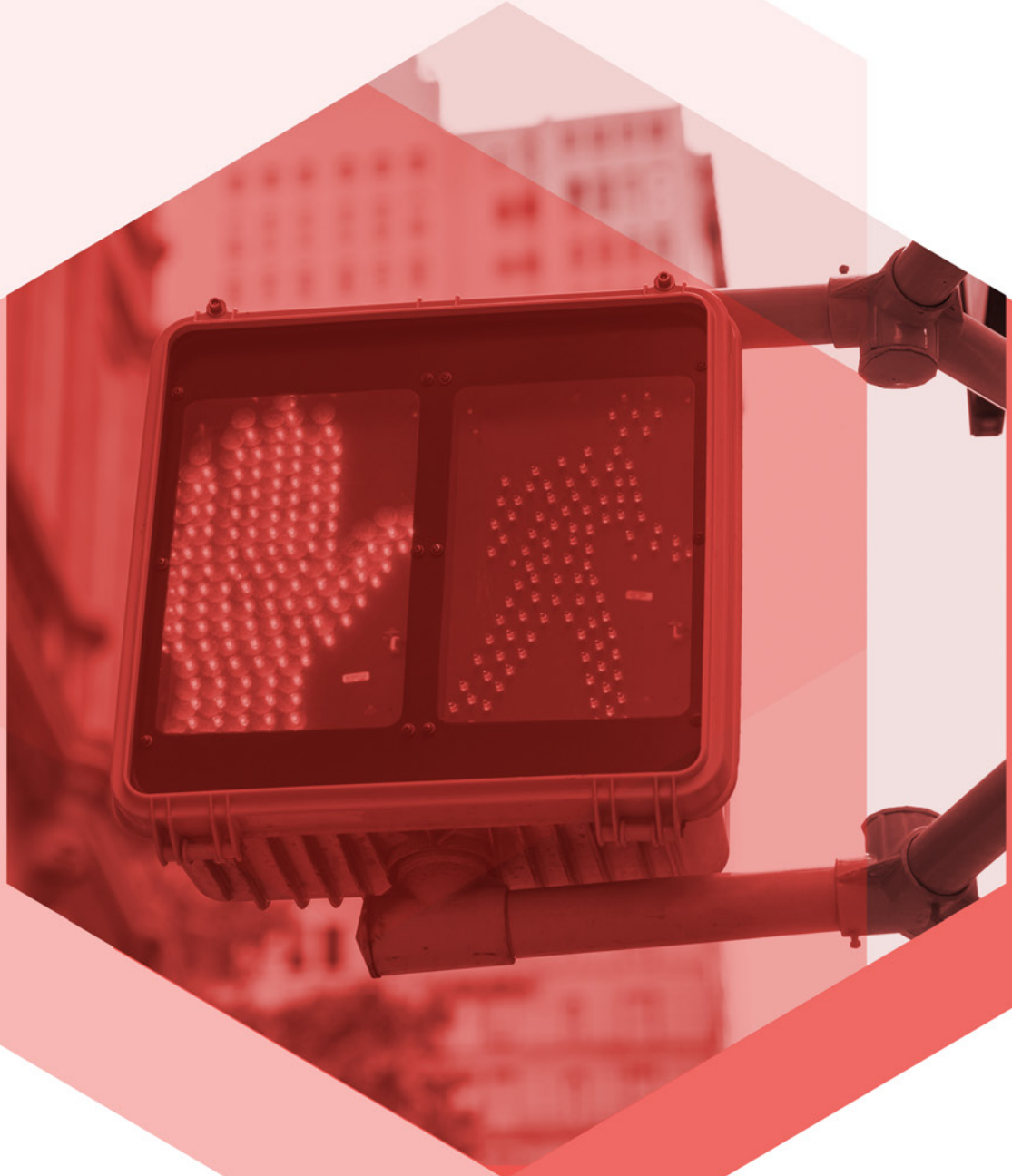
در فروردین ماه، شرکت‌های اپل، گوگل، موزیلا، وی‌ام‌ور، مایکروسافت، ادوبی، اینتل، اوراکل و سیسکو اقدام به انتشار اصلاحیه و توصیه‌نامه امنیتی برای برخی از محصولات خود کردند. سوءاستفاده از برخی از ضعف‌های ترمیم‌شده، مهاجم را قادر به در اختیار گرفتن کنترل سیستم می‌کند.

در ماهی که گذشت شرکت مهندسی شبکه گستر ویژه‌نامه‌ای را منتشر کرد که در آن ضمن مرور رویدادها و تجارب کسب شده در گذشته و با نگاهی به بدافزارها و تهدیدات سایبری در سال ۹۸ دورنمایی از مهمترین موضوعات و چالش‌های حوزه امنیت فناوری اطلاعات در سال ۹۹ ترسیم شده است. این شرکت در یک توصیه‌نامه نیز به نکاتی که رعایت آنها نقشی کلیدی در ایمن نگاه داشتن سازمان از گزند تهدیدات سایبری در جریان دورکاری دارند پرداخته است.

در اولین ماه سال ۱۳۹۹، شرکت بیت‌دیفندر از شناسایی حملاتی خبر داد که در جریان آن مهاجمان با هک کردن روترها و تغییر تنظیمات DNS، کاربران دستگاه‌های متصل به این تجهیزات را به سایت‌های تحت کنترل خود هدایت و با وعده ارائه آخرین اخبار در خصوص ویروس کرونا آنها را تشویق به دریافت و اجرای فایل مخرب بدافزار Oski می‌کردند. جزییات این حملات و چندین تهدید سایبری دیگر را در این ماهنامه بخوانید.

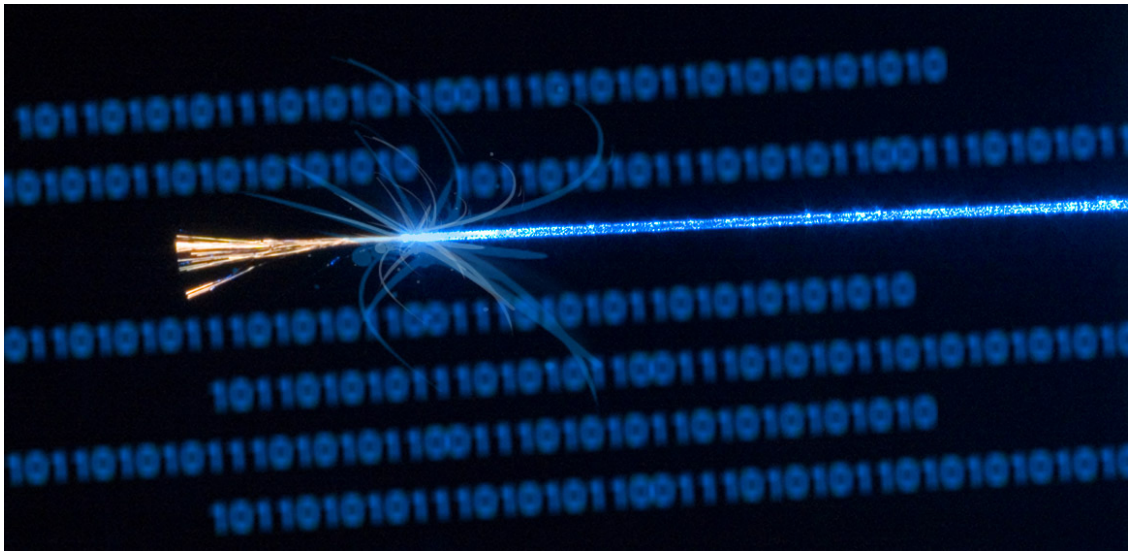
شرکت مهندسی شبکه گستر، ارائه‌دهنده محصولات و خدمات در زمینه امنیت شبکه از زمان تأسیس در سال ۱۳۷۰، همواره به امر آگاه‌سازی در زمینه امنیت فناوری اطلاعات به‌عنوان یکی از اصلی‌ترین راهکارهای مقابله با تهدیدات سایبری توجه خاص داشته است. امید است مطالب ماهنامه امنیت فناوری اطلاعات شرکت مهندسی شبکه گستر که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

هشدارهای امنیتی



سرقت اطلاعات

با رخنه به روترها



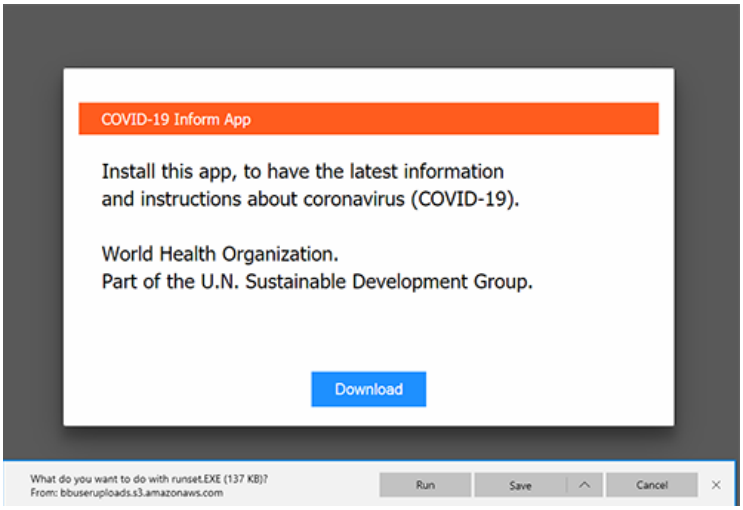
شرکت بیت‌دیفندر از شناسایی حملاتی خبر داده که در جریان آن مهاجمان با هک کردن روترها و تغییر تنظیمات DNS، کاربران دستگاه‌های متصل به این تجهیزات را به سایت‌های تحت کنترل خود هدایت و با وعده ارائه آخرین اخبار در خصوص ویروس کرونا آنها را تشویق به دریافت و اجرای فایل مخرب بدافزار Oski می‌کنند.

این حملات یکی از تازه‌ترین نمونه‌ها از بهره‌جویی تبهکاران سایبری از همه‌گیری جهانی ویروس کووید ۱۹ است.

به گزارش شرکت مهندسی شبکه گستر به نقل از شرکت ضدویروس بیت‌دیفندر، مهاجمان با شناسایی روترهای قابل دسترس بر روی اینترنت و اجرای حملات موسوم به سعی و خطا (Brute-force) اقدام به در اختیار گرفتن کنترل آنها می‌کنند.

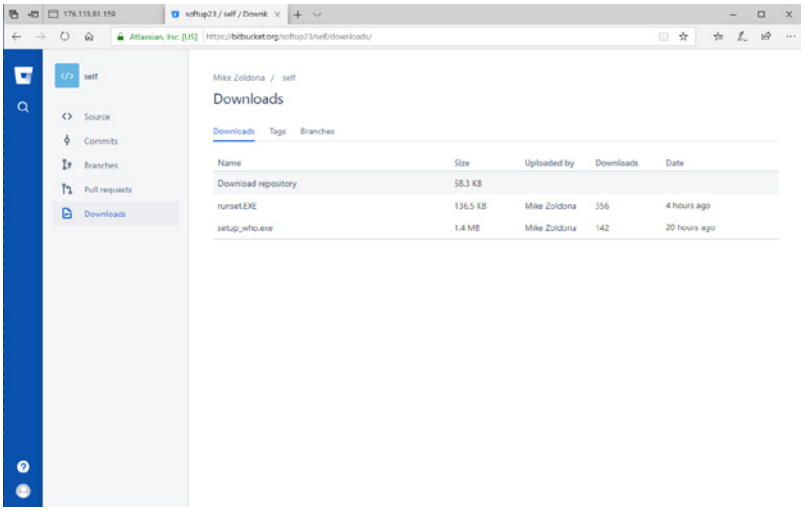
پس از تغییر نشانی DNS روتر هک شده در زمان فراخوانی سایت‌هایی خاص در مرورگر دستگاه‌های متصل به آن، کاربر به صفحات وب مورد نظر مهاجمان هدایت می‌شود.

صفحات مذکور حاوی پیامی مشابه شکل زیر است تا بدین طریق کاربر متقاعد به دریافت و نصب برنامه‌ای که در ظاهر از سوی سازمان بهداشت جهانی (WHO) در خصوص اخبار کووید ۱۹ ارائه گردیده شود.



اگر چه با نگاه داشتن موشواره (Hover) بر روی دگمه Download نشانی معتبر https://google[.]com/chrome نمایش داده می‌شود اما تابعی که با رویداد موسوم به on-click فراخوانی می‌گردد موجب دریافت فایل از نشانی تحت کنترل مهاجمان می‌شود. ضمن اینکه آن نشانی نیز با استفاده از TinyURL کوتاه و ظاهری معتبر به خود گرفته است.

به محض کلیک کاربر بر روی دگمه Download بدافزار Oski با یکی از نام‌های runset.EXE،covid19informer.exe و setup_who.exe بر روی دستگاه قربانی دریافت می‌شود. فایل‌های مخرب مورد استفاده این مهاجمان بر روی سرویس‌دهنده Bitbucket میزبانی می‌شوند.



Oski بدافزار سارق اطلاعات (Info Stealer) جدیدی است که نخستین نسخه از آن در اواخر سال میلادی گذشته شناسایی شد. از جمله قابلیت‌های Oski می‌توان به استخراج اطلاعات اصالت‌سنجی وارد شده در مرورگرها، رمزهای عبور کیف‌های ارز رمز و عبارات خاص ذخیره شده در بانک‌های داده اشاره کرد.

بیت‌دیفندر روترهای ساخت لینک‌سیز را هدف این حملات اعلام کرده است. در عین حال برخی منابع مورد هدف قرار گرفتن روترهای دی-لینک را نیز گزارش کرده‌اند.

به صاحبان و کاربران روترهای لینک‌سیز و دی-لینک توصیه می‌شود ضمن تغییر رمز عبور دسترسی به پنل کنترلی آنها اطلاعات اصالت‌سنجی حساب کاربری ابری (Cloud Account Credential) یا هر حساب کاربری دارای دسترسی از راه دور به این تجهیزات را تغییر دهند.

مشروح گزارش بیت‌دیفندر در اینجا قابل دریافت و مطالعه است.

آسیب‌پذیری‌ها و اصلاحیه‌های امنیتی

اصلاحیه‌های امنیتی مایکروسافت

برای ماه میلادی آوریل

به گزارش شرکت مهندسی شبکه گستر، سه‌شنبه، ۲۶ فروردین، شرکت مایکروسافت اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی آوریل منتشر کرد. این اصلاحیه‌ها در مجموع، ۱۱۵ آسیب‌پذیری را در سیستم عامل Windows و برخی دیگر از سرویس‌ها و نرم‌افزارهای مایکروسافت ترمیم می‌کنند. درجه حساسیت ۱۹ مورد از آسیب‌پذیری‌های ترمیم شده توسط اصلاحیه‌های مذکور "حیاتی" (Critical) و سایر آنها "بااهمیت" (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 "بااهمیت" برطرف و ترمیم می‌گردند.

از نکات قابل توجه در خصوص مجموعه اصلاحیه‌های این ماه، ترمیم سه آسیب‌پذیری روز-صفر (Zero-day) زیر است:

- CVE-2020-0938 و CVE-2020-1020 که هر دو ضعفی با درجه حساسیت "حیاتی" و از نوع "اجرای کد به صورت از راه دور" (Remote Code Execution) در Adobe Font Manager Library در سیستم عامل Windows هستند.
- CVE-2020-0935 که یک آسیب‌پذیری از نوع "ترفیع امتیازی" (Elevation of Privilege) بوده و نرم‌افزار OneDrive از آن تأثیر می‌پذیرد.

پیش‌تر مایکروسافت اعلام کرده بود که آسیب‌پذیری‌های CVE-2020-0938 و CVE-2020-1020 مورد سوءاستفاده مهاجمان قرار گرفته‌اند. بر طبق اطلاعیه فنی Microsoft آسیب‌پذیری‌های مذکور از مدیریت نادرست فونت‌های دستکاری شده از نوع Multi-master با قالب Adobe Type 1 PostScript در Adobe Font Manager Library ناشی می‌شوند.

آسیب‌پذیری‌های "حیاتی"

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

CVE-2020-0687 که ضعفی از نوع "اجرای کد به‌صورت از راه دور" است که از نحوه مدیریت ناصحیح فونت‌های ذخیره شده در حافظه توسط Font Library ناشی می‌شود. مهاجم می‌تواند با هدایت قربانی به سایت مخرب و در ادامه تشویق او به اجرای یک فایل حاوی فونت دستکاری شده از این آسیب‌پذیری بهره‌جویی کند. سوءاستفاده موفق از آسیب‌پذیری مذکور کنترل کامل سیستم را در اختیار مهاجم قرار می‌دهد.

CVE-2020-0907 دیگر آسیب پذیری "حیاتی" این ماه است در نتیجه مدیریت نادرست اشیاء (Object) توسط بخش Graphics Components مهاجم را قادر به اجرای کد به‌صورت از راه دور می‌کند.

CVE-2020-0929، CVE-2020-0931 و CVE-2020-0932 هر سه ضعفی از نوع "اجرای کد به‌صورت از راه دور" هستند که نرم‌افزار SharePoint از آنها تأثیر می‌پذیرد. ارسال یک بسته دستکاری شده به نسخه آسیب‌پذیر SharePoint مهاجم را قادر به اجرای کد در بخش موسوم به Application Pool و سرور SharePoint می‌کند.

CVE-2020-0968 و CVE-2020-0970 آسیب‌پذیری‌هایی از نوع "بروز اختلال در حافظه" (Memory Corruption) در بخش Scripting Engine مرورگر Internet Explorer هستند. باگ‌های مذکور می توانند به نحوی موجب بروز اختلال در حافظه شوند که موجب اجرای کد مورد نظر مهاجم با سطح دسترسی کاربر فعلی شوند. 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.

CVE-2020-0969 نیز ضعفی از نوع "بروز اختلال در حافظه" است که موتور چیدمان JavaScript/JScript مایکروسافت، معروف به Chakra در مرورگر Edge از آن تأثیر می‌پذیرد. سوءاستفاده از این اشکال منجر به بروز اشکال در حافظه و فراهم شدن امکان اجرای کد بر روی دستگاه قربانی می‌شود.

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

CVE-2020-0910	CVE-2020-0927	CVE-2020-0948
CVE-2020-0949	CVE-2020-0950	CVE-2020-0965
CVE-2020-0967	CVE-2020-0974	CVE-2020-1022
CVE-2020-0938	CVE-2020-1020	

آسیب‌پذیری‌های "بااهمیت"

از میان آسیب‌پذیری "بااهمیت" این ماه موارد زیر بیش سایرین جلب توجه می‌کنند:

CVE-2020-0760 که ضعفی از نوع "اجرای کد به‌صورت از راه دور" در مجموعه نرم‌افزاری Office است. باز کردن یک سند دستکاری شده مهاجم را قادر به اجرای کد مورد نظر خود با سطح دسترسی کاربر فعلی می‌کند.

CVE-2020-0784 که ضعفی از نوع "ترفیع امتیازی" در DirectX است که امکان اجرای کد دودویی در سطح Kernel را برای مهاجم فراهم می‌کند.

CVE-2020-0956، CVE-2020-0957 و CVE-2020-0958 که هر سه، ضعفی از نوع "ترفیع امتیازی" هستند که همچون مورد قبل امکان اجرای کد دودویی در سطح Kernel را برای مهاجم مهیا می‌کنند.

CVE-2020-1004 دیگر آسیب‌پذیری "ترفیع امتیازی" در این ماه است که بخش Graphics Component از آن تأثیر می‌پذیرد. سوءاستفاده موفق از این آسیب‌پذیری مهاجم را قادر به اجرای پروسه‌هایی خاص با سطح دسترسی ارتقا یافته می‌کند.

CVE-2020-1005 که ضعفی از نوع "افشای اطلاعات" (Information Disclosure) در Graphics Component است که از مدیریت ناصحیح اشیاء در حافظه توسط نرم‌افزار ناشی می‌شود. بهره‌جویی از این آسیب‌پذیری می‌تواند به‌طور بالقوه منجر به افشای اطلاعاتی شود که در ادامه حمله مورد استفاده مهاجم قرار بگیرد.

CVE-2020-1027 ضعفی از نوع "ترفیع امتیازی" در Windows Kernel است که سوءاستفاده از آن مهاجم را قادر به اجرای کد با سطح دسترسی ارتقا یافته می‌کند.

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

CVE-2020-0699	CVE-2020-0794	CVE-2020-0821
CVE-2020-0835	CVE-2020-0888	CVE-2020-0889
CVE-2020-0895	CVE-2020-0899	CVE-2020-0900
CVE-2020-0906	CVE-2020-0913	CVE-2020-0917
CVE-2020-0918	CVE-2020-0919	CVE-2020-0920
CVE-2020-0923	CVE-2020-0924	CVE-2020-0925
CVE-2020-0926	CVE-2020-0930	CVE-2020-0933
CVE-2020-0934	CVE-2020-0935	CVE-2020-0936
CVE-2020-0937	CVE-2020-0938	CVE-2020-0939
CVE-2020-0940	CVE-2020-0942	CVE-2020-0943
CVE-2020-0944	CVE-2020-0945	CVE-2020-0946
CVE-2020-0947	CVE-2020-0952	CVE-2020-0953
CVE-2020-0954	CVE-2020-0955	CVE-2020-0959
CVE-2020-0960	CVE-2020-0961	CVE-2020-0962
CVE-2020-0964	CVE-2020-0966	CVE-2020-0971
CVE-2020-0972	CVE-2020-0973	CVE-2020-0975

CVE-2020-0976	CVE-2020-0977	CVE-2020-0978
CVE-2020-0979	CVE-2020-0980	CVE-2020-0981
CVE-2020-0982	CVE-2020-0983	CVE-2020-0984
CVE-2020-0991	CVE-2020-0992	CVE-2020-0993
CVE-2020-0994	CVE-2020-0995	CVE-2020-0996
CVE-2020-0999	CVE-2020-1000	CVE-2020-1001
CVE-2020-1002	CVE-2020-1003	CVE-2020-1006
CVE-2020-1007	CVE-2020-1008	CVE-2020-1009
CVE-2020-1011	CVE-2020-1014	CVE-2020-1015
CVE-2020-1016	CVE-2020-1017	CVE-2020-1018
CVE-2020-1019	CVE-2020-1020	CVE-2020-1026
CVE-2020-1029	CVE-2020-1049	CVE-2020-1050
CVE-2020-1094		

اصلاحیه‌های عرضه شده
در فرودین ۱۳۹۹

در فروردین ۱۳۹۹، شرکت‌های اپل، گوگل، موزیلا، وی‌ام‌ور، مایکروسافت، ادوبی، اینتل، اوراکل و سیسکو اقدام به انتشار اصلاحیه و توصیه‌نامه امنیتی برای برخی از محصولات خود کردند.

در ۶ فروردین، شرکت اپل با انتشار به‌روزرسانی، ضعف‌هایی امنیتی را در iTunes، iOS & iPadOS، Safari، watchOS، tvOS و macOS ترمیم و اصلاح کرد. سوءاستفاده از برخی از ضعف‌های مذکور، مهاجم را قادر به در اختیار گرفتن کنترل سیستم می‌کند. اپل در ۲۷ فروردین نیز اقدام به عرضه نسخه 11.4.1 محصول Xcode برای ترمیم یک آسیب‌پذیری از نوع "نشت اطلاعات" (Information Disclosure) به شناسه CVE-2020-5260 در این بستر توسعه نرم‌افزار کرد.

به گزارش شرکت مهندسی شبکه گستر، در فروردین ماه، گوگل در چندین نوبت با عرضه به‌روزرسانی اقدام به ترمیم آسیب‌پذیری‌های امنیتی مرورگر Chrome کرد. آخرین نسخه این مرورگر که در ۲۷ فروردین انتشار یافت 81.0.4044.113 است. فهرست اشکالات مرتفع شده در اینجا، اینجا و اینجا قابل دریافت و مشاهده است.

در ماهی که گذشت شرکت موزیلا، با ارائه نسخه 75، چندین آسیب‌پذیری و باگ را در مرورگر Firefox برطرف کرد. جزییات کامل در اینجا قابل مطالعه است.

وی‌ام‌ور دیگر شرکتی بود که در فروردین ۱۳۹۹ اقدام به انتشار به‌روزرسانی کرد. محصولات VMware Directory Service و VMware vRealize Log Insight از این به‌روزرسانی‌ها تأثیر می‌پذیرند. بهره‌جویی از آسیب‌پذیری ترمیم شده توسط به‌روزرسانی VMware Directory Service مهاجم را قادر به دستیابی به اطلاعات حساس و به‌صورت بالقوه در اختیار گرفتن کنترل سیستمی که vCenter Server بر روی آن نصب است می‌کند. جزییات بیشتر در خصوص این به روزرسانی‌ها در اینجا و اینجا قابل مطالعه است.

۲۶ فروردین، شرکت مایکروسافت بر طبق زمانبندی معمول خود اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی آوریل منتشر کرد که پیش‌تر در این خبر به آن پرداخته شد. از نکات قابل توجه در خصوص مجموعه اصلاحیه‌های این ماه مایکروسافت، ترمیم سه آسیبپذیری روز-صفر (Zero-day) در برخی محصولات این شرکت است.

در همین تاریخ شرکت ادوبی نیز با ارائه به‌روزرسانی، چندین آسیب‌پذیری امنیتی را در ColdFusion، After Effects و Digital Editions ترمیم کرد.

همچنین در فروردین، اوراکل مطابق با برنامه زمانبندی شده سه‌ماهه خود، با انتشار ۳۹۷ به‌روزرسانی اقدام به ترمیم آسیب‌پذیری‌های امنیتی در بیش از ۲۰ محصول ساخت این شرکت کرد که جزییات کامل در خصوص آن در اینجا قابل دریافت است.

اینتل نیز از جمله شرکتی‌هایی بود که در فروردین ۱۳۹۹ چند آسیب‌پذیری را در برخی از محصولات خود ترمیم کرد. بهره‌جویی از بعضی از آنها سطح دسترسی مهاجم را بر روی دستگاهی که به آن دسترسی محلی (Local Access) دارد ارتقا می‌بخشد. اطلاعات بیشتر در توصیه‌نامه‌های زیر ارائه شده است:

- Data Migration Software Advisory INTEL-SA-00327
- PROSet/Wireless WiFi Software Advisory INTEL-SA-00338
- Driver and Support Assistant Advisory INTEL-SA-00344
- Modular Server Compute Module Advisory INTEL-SA-00351
- Binary Configuration Tool for Windows Advisory INTEL-SA-00359
- NUC Firmware Advisory INTEL-SA-00363

در فروردین ۹۹، سیسکو در چندین نوبت اقدام به عرضه به‌روزرسانی‌های امنیتی کرد. این به‌روزرسانی‌ها در مجموع، ۱۶ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت ۴ مورد از این آسیب‌پذیری‌ها، "حیاتی" و ۱۰ مورد از آنها "بالا" (High) گزارش شده است. آسیب‌پذیری به حملاتی همچون "اجرای کد به صورت از راه دور" (Remote Code Execution)، "از کاراندازی سرویس" (Denial of Service) و "ترفیع امتیازی" (Privilege Escalation)، از جمله اشکالات مرتفع شده توسط به‌روزرسانی‌های جدید است. توضیحات کامل در مورد به‌روزرسانی‌های عرضه شده در اینجا قابل دسترس است.

رویدادها و وقایع امنیتی

مراکز درمانی

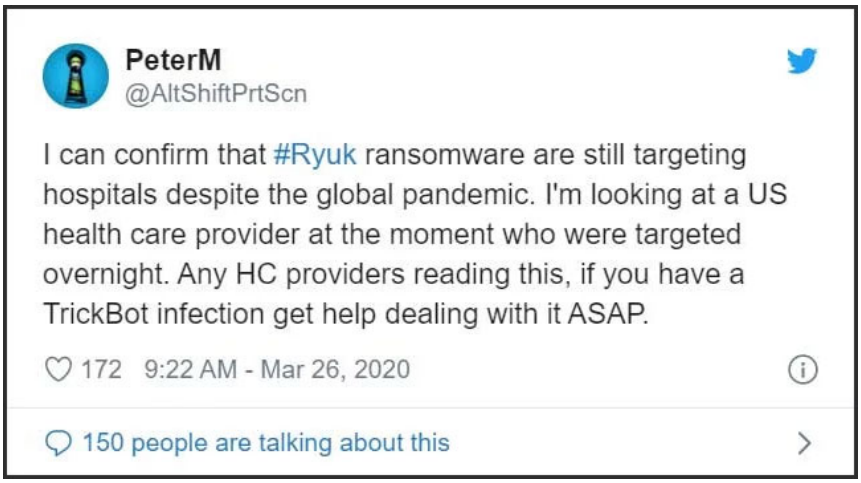
مراقب حملات باج‌افزاری باشند

در روزهای اخیر چندین نهاد بین‌المللی و شرکت امنیتی در خصوص افزایش حملات باج‌افزاری بر ضد مراکز فعال در حوزه سلامت و درمان هشدار داده‌اند.

در یکی از جدیدترین موارد، پلیس بین‌الملل (Interpol) خبر داده که علیرغم وضعیت بحرانی شیوع ویروس کرونا شاهد افزایش چشم‌گیر تلاش مهاجمان برای حمله باج‌افزاری به سازمان‌ها و زیرساخت‌هایی است که نقشی کلیدی در مقابله با این ویروس همه‌گیر دارند.

به گزارش شرکت مهندسی شبکه گستر، مایکروسافت نیز بتازگی از بهره‌جویی گردانندگان باج‌افزار REvil - که با نام Sodinokibi نیز شناخته می‌شود - از دستگاه‌های VPN و تجهیزات مورد استفاده در درگاه شبکه بیمارستان‌ها به‌منظور نفوذ به شبکه این مراکز خبر داده است. قبلاً هم نمونه‌هایی از سوءاستفاده باج‌افزارهای DoppelPaymer و Ragnarok از آسیب‌پذیری CVE-2019-19781 در Citrix Application Delivery Controller،Citrix Gateway و Citrix SD-WAN WANOP گزارش شده بود.

علاوه بر مایکروسافت برخی محققان از جمله PeterM از شرکت سوفوس نیز از فعالیت گسترده REvil بر ضد مراکز درمانی خبر داده‌اند.



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

این در حالی است که برخی گروه‌های باج‌گیر اعلام کرده‌اند که به دلایل بشردوستانه! و شرایط بحرانی ناشی از شیوع ویروس کرونا حمله به مراکز بهداشتی و درمانی را متوقف می‌کنند. از جمله این گروه‌ها می‌توان به گردانندگان Maze اشاره کرد که داده‌هایی را که پیش‌تر از یکی از شرکت‌های تست دارو سرقت کرده بودند به رایگان برگردانده‌اند.

ضمن سپاس از تلاش‌های دلسوزانه و خستگی‌ناپذیر نظام سلامت و درمان کشور به تمامی مدیران و راهبران شبکه این مراکز توصیه می‌شود که بیش از هر زمانی توجه ویژه به اجرای کامل راهکارها و اقدامات مورد نیاز برای مقابله با باج‌افزارها داشته باشند.

گزارش‌ها


باج‌افزارهای جدید
۲،۵۰۰،۰۰۰
۲،۰۰۰،۰۰۰
۱،۵۰۰،۰۰۰
۱،۰۰۰،۰۰۰
۵۰۰،۰۰۰
سه‌ماهه دوم
سه‌ماهه سوم
سه‌ماهه چهارم
۲۰۱۷
سه‌ماهه اول
سه‌ماهه دوم
سه‌ماهه سوم
سه‌ماهه چهارم
۲۰۱۸
سه‌ماهه اول
۲۰۱۹

مهمترین چالش‌های حوزه
امنیت فناوری اطلاعات در سال ۹۹

تبهکاران سایبری هر فناوری را که رسیدن به اهداف آنها را ممکن، تسهیل و تسریع کند به استخدام خود در می‌آورند.

اگر چه سازندگان محصولات امنیتی نیز همواره در حال تکامل امکانات موجود و ارائه قابلیت‌های جدید برای مقابله مؤثر با تهدیدات سایبری هستند اما با این وجود در بسیاری از مواقع مهاجمان با خلق روش‌های جدید در نهایت موفق به رخنه به سامانه‌های اهداف خود می‌شوند.

تجارب یک دهه اخیر نشان می‌هد که سازمان‌ها نمی‌توانند از اطلاعات، شبکه و سامانه‌های خود در مقابل چیزی دفاع کنند که درک صحیحی از آن ندارند. شناخت دقیق تهدید اولین گام در یافتن و پیاده‌سازی راهکار امنیتی مناسب در برابر آن است.

مروری بر اصلی‌ترین تهدیدات سال ۹۸ نشان می‌دهد که آموزش کاربران و آگاهی مدیران و راهبران فناوری اطلاعات نقشی بسیار کلیدی در خنثی‌سازی تهدیدات سایبری دارد.

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 توجه خاص داشته است. شرکت مهندسی شبکه گستر در ویژه‌نامه‌ای، ضمن مرور رویدادها و تجارب کسب شده در گذشته و با نگاهی به بدافزارها و تهدیدات سایبری در سال ۹۸ دورنمایی از مهمترین موضوعات و چالش‌های حوزه امنیت فناوری اطلاعات در سال ۹۹ را ترسیم کرده است. امید است مطالب این ویژه‌نامه که حاصل تحقیق و پژوهش کارشناسان این شرکت است راهنمایی برای ارتقای دانش کاربران این حوزه باشد.

برای دریافت این ویژه‌نامه بر روی تصویر زیر کلیک کنید.

توصیه‌نامه امنیتی
دورکاری امن کارکنان

ویروس کووید ۱۹ نخستین بار در آذر ماه در شهر ووهان چین شناسایی شد. در حالی که ابتدا از بیماری ناشی از این ویروس با عنوان ذات‌الریه یاد می‌شد کمیسیون ملی بهداشت چین در دی ماه به‌صورت رسمی شیوع کووید ۱۹ را در این کشور گزارش کرد. یک ماه بعد سازمان بهداشت جهانی شیوع این ویروس را یک همه‌گیری محدود (Outbreak) و تهدیدی برای سلامت عموم در سطح بین‌الملل اعلام کرد. این سازمان در ۲۱ اسفند ۱۳۹۸ خبر داد که کووید ۱۹ به مرحله همه‌گیری جهانی (Epidemic) رسیده است. دبیرکل سازمان ملل انتشار این ویروس را بدترین بحران جهانی از زمان پایان جنگ جهانی دوم در ۷۵ سال گذشته توصیف کرده است.

کشورهای مختلف هر یک با سیاست‌هایی خاص به مقابله با این ویروس پرداخته‌اند. از جمله این سیاست‌ها که در ایران نیز در حال اجراست، فاصله‌گذاری اجتماعی است. از اقدامات مؤثر در ایجاد فاصله‌گذاری اجتماعی انجام دورکاری کارکنان از منزل بجای حضور فیزیکی در محل کار است.

علاوه بر فراهم بودن ارتباط اینترنتی مناسب، انضباط، خودانگیزشی و روالی جامع و مشخص، اطمینان از تأمین امنیت سیستم‌ها و داده‌های ذخیره و تبادل شده از نکات حائز اهمیت در انجام اثربخش و امن دورکاری است.

در این توصیه‌نامه به مواردی که رعایت آنها نقشی کلیدی در ایمن نگاه داشتن سازمان از گزند تهدیدات سایبری در جریان دور کاری دارند پرداخته شده است.

برای دریافت توصیه‌نامه بر روی تصویر زیر کلیک کنید.

افتای ریاست جمهوری با همکاری شبکه گستر

شبکه گستر

شرکت مهندسی شبکه گستر

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

دو سال رخنه به سروهای MSSQL برای استخراج ارز رمز

یافته‌های جدید نشان می‌دهند که از ماه می سال ۲۰۱۸ میلادی، یک شبکه مخرب بدافزاری (Malware Botnet) با اجرای حملات سعی‌وخطا (Brute-force) بر ضد سرورهای Microsoft SQL - به اختصار MSSQL - و در اختیار گرفتن کنترل حساب‌های کاربری با سطح دسترسی admin اقدام به اجرای اسکریپت‌های استخراج‌کننده ارز رمز (Cryptocurrency Mining Script) بر روی سیستم عامل این سرورها می‌کرده است. این شبکه مخرب همچنان فعال بوده و در هر روز به‌طور میانگین تقریباً ۳ هزار سرور جدید MSSQL را به تسخیر خود در می‌آورد. ادامه مطلب را در اینجا بخوانید.

انتشار بدافزار LimeRAT با یک تکنیک رمزگذاری در Excel

مهاجمان در کارزاری جدید با استفاده از یک تکنیک قدیمی رمزگذاری در فایل‌های Excel در حال انتشار تروجان LimeRAT هستند. ادامه مطلب را در اینجا بخوانید.

سوءاستفاده از کووید ۱۹ برای رونویسی MBR یا حذف همیشگی داده‌ها

در حالی که ویروس کرونا (کووید ۱۹) به مرحله همه‌گیری جهانی رسیده، برخی تبهکاران سایبری، بدافزارهایی را توسعه داده‌اند که سیستم‌های آلوده به آنها را با رونویسی بخش موسوم به Master Boot Record - به اختصار MBR - یا با از بین بردن فایل‌ها دچار اختلال می‌کنند. ادامه مطلب را در اینجا بخوانید.

عملکرد بالقوه مخرب بیش از ۱۲ هزار برنامه اندرویدی

بر اساس یک تحقیق جامع دانشگاهی که نتایج آن به‌تازگی منتشر شده در بیش از ۱۲۷۰۰ برنامه مبتنی بر سیستم عامل Android رفتارهایی مخفی و مشابه با عملکرد درب‌پشتی دیده می‌شود. ادامه مطلب را در اینجا بخوانید.

حمله گسترده به سرورهای Elasticsearch

در هفته‌های اخیر یک هکر با رخنه به آن دسته از سرویس‌دهندگان Elasticsearch که در بستر اینترنت، بدون رمز عبور قابل دسترس بوده‌اند اقدام به حذف محتوای آنها کرده است. Elasticsearch موتور جستجویی است که به زبان Java نوشته شده است. ادامه مطلب را در اینجا بخوانید.

xHelper مانا در کنار تروجانی با عملکرد ماتریوشکا

حدود یک سال قبل شرکت کسپرسکی حملات گسترده‌ای را شناسایی کرد که در جریان آنها تروجان xHelper بر روی گوشی‌های هوشمند مبتنی بر Android نصب می‌شد. اکنون این شرکت از تداوم فعالیت این بدافزار خبر داده است. مشخصه اصلی xHelper ماندگاری آن است؛ به‌نحوی که حتی پس از حذف برنامه آن و یا حتی بازگردانی تنظیمات کارخانه‌ای دستگاه، همچنان فعال باقی می‌ماند. در این مطلب این توانایی ویژه xHelper مورد بررسی قرار گرفته است. ادامه مطلب را در اینجا بخوانید.

صدها هزار سرور Exchange، همچنان آسیب‌پذیر

بر اساس گزارشی که شرکت رپیدسون آن را منتشر کرده است، تنها تعداد بسیار اندکی از سازمان‌ها اقدام به نصب اصلاحیه یک آسیب‌پذیری خطرناک در Microsoft Exchange Server کرده‌اند. این بی‌توجهی در حالی صورت می‌گیرد که پیش‌تر نیز برخی منابع از مورد بهره‌جویی قرار گرفتن آسیب‌پذیری مذکور با شناسه CVE-2020-0688 توسط چندین گروه از مهاجمان با حمایت دولتی خبر داده بودند. ادامه مطلب را در اینجا بخوانید.

dark_nexus، فراتر از بات‌نت‌های معمول

بات‌نت جدیدی در صحنه تهدیدات سایبری ظاهر شده که محققان توانایی فوق‌العاده آن را مایه شرمساری سایر بات‌نت‌ها توصیف کرده‌اند. شرکت امنیتی بیت‌دیفندر اعلام کرده که این بات‌نت جدید با نام dark_nexus مجهز به امکانات و قابلیت‌هایی خاص بوده و فراتر از بات‌نت‌های معمول این روزها عمل می‌کند. ادامه مطلب را در اینجا بخوانید.

ترمیم ضعفی حیاتی در vCenter Server

شرکت وی‌ام‌ور اقدام به عرضه به‌روزرسانی امنیتی برای ترمیم ضعفی "حیاتی" (Critical) در بستر مدیریت زیرساخت مجازی vCenter Server کرده است. بهره‌جویی (Exploit) از این آسیب‌پذیری به شناسه CVE-2020-3952 مهاجم را قادر به دستیابی به اطلاعات حساس و به‌صورت بالقوه در اختیار گرفتن کنترل سیستمی که vCenter Server بر روی آن نصب است می‌کند. به این آسیب‌پذیری بر طبق استاندارد CVSSv۳ بالاترین درجه حساسیت (۱۰) تخصیص داده شده است. ادامه مطلب را در اینجا بخوانید.

اصلاح صدها آسیب‌پذیری در محصولات Oracle

سه‌شنبه، ۲۶ فروردین، Oracle مطابق با برنامه زمانبندی شده سه‌ماهه خود، با انتشار ۳۹۷ به‌روزرسانی، اقدام به ترمیم آسیب‌پذیری‌های امنیتی در بیش از ۲۰ محصول ساخت این شرکت کرد. ادامه مطلب را در اینجا بخوانید.

Agent Tesla، اکنون قادر به سرقت رمز عبور WiFi

شرکت ملوربایتس از تجهیز نسخ جدید Agent Tesla به یک ماژول اختصاصی برای استخراج رمزهای عبور WiFi از روی دستگاه‌های آلوده به این بدافزار خبر داده است. احتمال داده می‌شود که از اطلاعات سرقت شده برای گسترش آلودگی بر روی دستگاه‌های متصل به این شبکه‌های WiFi استفاده شود. ادامه مطلب را در اینجا بخوانید.

انتشار کرونایی Trickbot

بر اساس آمار ارائه شده از سوی مایکروسافت، در حال حاضر TrickBot بیشترین سهم از بدافزارهای انتشار یافته از طریق ایمیل‌ها و پیوست‌های مخرب با موضوع جعلی کرونا را به خود اختصاص داده است. ادامه مطلب را در اینجا بخوانید.

اخبار شبکه گستر

ایستاده در کنار هم

در مبارزه با ویروس کرونا

این روزها در نبرد با ویروس کرونا هستیم. نبردی که با تصمیمات به موقع، اقدامات پیشگیرانه و صبر و بردباری، پیروز خواهیم شد.

در شبکه گستر، اولویت سلامت همکاران و مشتریان و همچنین تضمین خدمات‌دهی بدون وقفه و اختلال است و ما قدم‌های لازم و ممکن را در این راه برداشته‌ایم.

شیوع ویروس کرونا در فکر همه ما و در همه خبرها است. شبکه گستر نیز از نزدیک شرایط جاری و تغییرات کسب و کار را دنبال می‌کند تا همچنان پاسخگوی نیازهای مشتریان خود باشد.

- با کاهش تعداد همکاران حاضر در محل شرکت، ضمن همراهی با طرح ملی فاصله‌گذاری اجتماعی، احتمال ابتلای همکاران به ویروس کرونا را کاهش داده‌ایم
- امکانات دور کاری را برای اکثریت همکاران شبکه گستر فراهم آورده‌ایم تا همچنان آماده خدمات‌دهی باشیم
- شما مشتریان گرامی همچنان می‌توانید از طریق خطوط تلفن پنج رقمی ۴۲۰۵۲-۰۲۱ و سامانه ۲۴ ساعته خدمات پس از فروش و پشتیبانی shabakeh.net با شبکه گستر در تماس باشید

در وضعیت کنونی استفاده از خدمات اینترنتی و سرویس‌های از راه دور، مناسب‌ترین و ایمن‌ترین راههای تماس و خدمات‌دهی هستند. لذا تا بهبود وضعیت و رفع محدودیت‌های وضع شده، تمام قرارهای نصب، رفع اشکال، ارتقاء و ... به صورت ارتباط از راه دور (Remote) توسط کارشناسان شبکه گستر انجام خواهد گرفت.

شرکت‌های بین‌المللی Bitdefender، McAfee و Sophos نیز هر یک با انتشار اطلاعیه‌ای از تمهیداتی که در شرایط حاضر برای استمرار و پایداری محصولات و خدمات خود بکار گرفته‌اند، اطمینان خاطر داده اند.

در صورت داشتن شرایط و یا نیاز خاص، لطفا با ما مطرح کنید. بدون تردید، درخواست شما را بی پاسخ نخواهیم گذاشت.

هر چند که ایام سختی را می گذرانیم ولی

دور گردون گر دو روزی بر مراد ما نرفت
دائماً یکسان نباشد حال دوران غم مخور

این پیام را می توانید در قالب نامه رسمی از طرف مدیرعامل شبکه گستر از اینجا دریافت کنید.

محصولات بیت دیفندر؛
رایگان برای مراکز بهداشتی و درمانی

به منظور حمایت و همراهی با فعالان حوزه سلامت در مبارزه با ویروس کرونا، شرکت بیت‌دیفندر اقدام به عرضه رایگان کلیه محصولات سازمانی خود به مراکز و موسسات بهداشتی و درمانی در سراسر جهان و از جمله در ایران نموده است.

تمام مراکز و موسسات بهداشت و درمان در هر اندازه‌ای، از یک درمانگاه کمک‌های اولیه تا تمام بیمارستان‌های علوم پزشکی، می‌توانند به مدت شش ماه، بدون محدودیت تعداد کاربر، بطور رایگان، هر یک از محصولات ضدویروس و دیگر محصولات سازمانی بیت‌دیفندر را انتخاب کرده و آنرا در شبکه سازمانی خود بکار گیرند.

در پایان دوره شش ماهه، بر اساس وضعیت مقابله با ویروس کرونا و شرایط مراکز درمانی، این طرح قابل تمدید تا یکسال خواهد بود.

مراکز و موسسات بهداشتی و درمانی که از محصولات ضدویروس دیگری بغیر از بیت‌دیفندر استفاده می کنند، با استفاده از این طرح، از خدمات نصب و راه اندازی رایگان محصولات بیت دیفندر نیز برخوردار خواهند بود.

مراکز و موسسات بهداشتی و درمانی که در حال حاضر از محصولات بیت‌دیفندر استفاده می کنند نیز می توانند از برخی مزایای این طرح برخوردار شوند.

با توجه به اینکه هدف اصلی از اجرای این طرح، حمایت از نیروهای خط مقدم مبارزه با ویروس کرونا است، مراکز و موسسات فعال در حوزه سلامت که مستقیماً خدمات پزشکی و درمانی ارائه می‌کنند، مشمول طرح رایگان محصولات بیت‌دیفندر خواهند بود. لذا این طرح شامل ادارات و بخش‌های ستادی حوزه سلامت نمی‌باشد.

برای کسب اطلاعات بیشتر و بهره‌مندی از این طرح، می‌توانید با دفتر فروش شرکت مهندسی شبکه گستر ۴۲۰۵۲-۰۲۱ تماس حاصل نموده و یا فرم اطلاعات اولیه را در اینجا تکمیل کنید تا در اسرع وقت به درخواست شما رسیدگی گردد.

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