امنیت فناوری اطلاعات

ویژه نامه نوروز ۱۳۹۹

شبکه گستر
امنیت شما | وظیفه ما

فهرست مطالب

چکیده مدیریتی

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 حوزه امنیت فناوری اطلاعات توجه خاص داشته است. در آستانه سال نو، 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 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.

"جعل عمیق"؛ سرگرمی یا تهدید جدی؟!

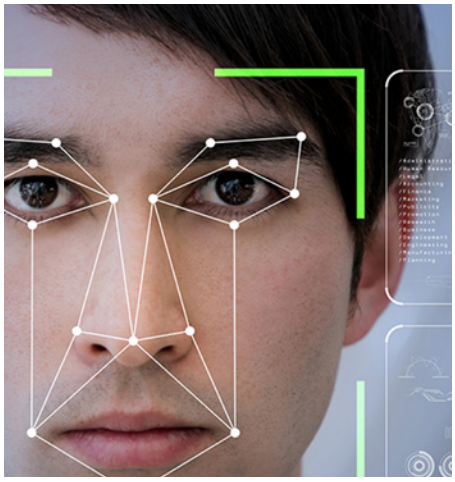
دست‌درازی به تصاویر با هدف فریب افراد و تغییر باور آنها، موضوع جدیدی نیست. آغاز استفاده از تصاویر دستکاری‌شده به دوران جنگ‌های جهانی اول و دوم باز می‌گردد. در آن ایام برخی دولت‌ها تلاش می‌کردند تا با تکنیک‌ها و روش‌های مختلف، عکس‌ها را به نحوی ویرایش کنند که در آنها، رخدادها آن‌طور که حقیقت نداشت به تصویر کشیده شود. در این حوزه، چیزی که اکنون را با گذشته متفاوت می‌کند پیشرفت‌های حاصل شده و خلق مفهومی جدید با عنوان "جعل عمیق" (Deepfake) است که ترکیب تصویر انسان در ویدئوها را ممکن می‌سازد. در این ویدئوهای جعلی فرد در حال انجام کار و در موقعیتی نشان داده می‌شود که در واقعیت هرگز اتفاق نیفتاده است.

اگر تا اندکی قبل، در اختیار داشتن فناوری‌های مبتنی بر "جعل عمیق" منحصر به سازمان‌ها و شرکت‌هایی خاص بود اکنون سایت‌هایی بر روی اینترنت در دسترس عموم هستند که در آنها ویدئوی ارسالی بر اساس مشخصه‌های مورد نظر کاربر تغییر و در اختیار او قرار می‌گیرد.

"جعل عمیق" مقابله با جنگ‌های اطلاعاتی را دشوارتر از هر زمانی می‌کند. ویدئوهای قابل‌دسترس در دیدگاه‌ها و پیام‌های منتشر شده در شبکه‌های اجتماعی منابعی رایگان و غنی برای تعالی و تکامل مستمر الگوریتم‌های "هوش مصنوعی" (Artificial Intelligence) و مدل‌های "یادگیری ماشین" (Machine Learning) مورد استفاده در "جعل عمیق" است.

به طور کلی، مهاجمان هر فناوری را که رسیدن به اهداف آنها را ممکن، تسهیل و تسریع می‌کند به استخدام خود در می‌آورند. دور از ذهن نیست که گروهی از مهاجمان با پشتوانه دولتی و با هدف تغییر باور عموم اقدام به ساخت فیلمی دروغین مبتنی بر "جعل عمیق" برای یک شخصیت مطرح سیاسی پیش از یک رخداد مهم نظیر برگزاری انتخابات کنند. یا ساخت ویدئویی را می‌توان متصور بود که در آن مدیرعامل یک شرکت معروف در بیانیه‌ای از کاهش درآمدها یا لزوم فراخوانی محصولات فروخته شده به دلیل وجود اشکالی مرگ‌بار در آنها خبر می‌دهد؛ موضوعی که منجر به کاهش سریع ارزش سهام و یا حتی مواردی به مراتب نگران‌کننده‌تر می‌شود. به عبارت دیگر "جعل عمیق" بالقوه ابزاری برای بروز یک هرج‌ومرج عظیم است.

پیش‌بینی می‌شود که فراگیری این فناوری و ورود گروه‌های غیرحرفه‌ای در حوزه "جعل عمیق"، منجر به افزایش حجم اطلاعات نادرست و دروغین اما قابل باورتر از همیشه شود.



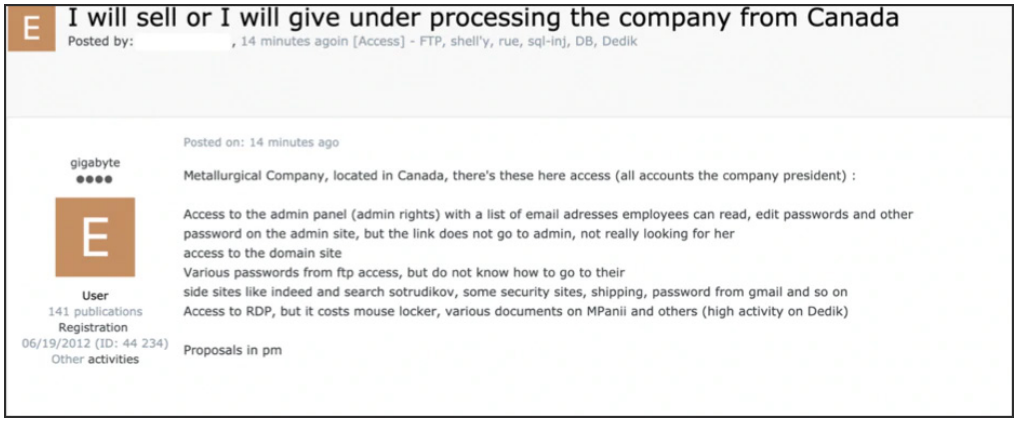
همچنین "جعل عمیق" می‌تواند ابزاری برای دور زدن سیستم‌های حافظتی مبتنی بر فناوری "تشخیص چهره" (Facial Recognition) باشد. ظهور این فناوری تقریباً به اواسط سال ۱۹۶۰ باز می‌گردد. از آن سال‌ها تا کنون، هدف همچنان شناسایی و تایید دقیق هویت افراد بوده است. هر چه زمان به جلوتر می‌رود، توان پردازشی، حافظه و فضای ذخیره‌سازی بیشتری در اختیار فناوری "تشخیص چهره" قرار می‌گیرد. به همین خاطر این فناوری با روش‌هایی خلاقانه در ساده کردن زندگی روزمره، از باز کردن قفل گوشی‌های هوشمند گرفته تا اعتبارسنجی شناسه گذرنامه‌ها در مرزها و حتی به‌عنوان ابزاری در خدمت قانون برای شناسایی تبهکاران در خیابان مورد استفاده قرار گرفته است. "جعل عمیق" می‌تواند یکی از راهکارهای مهاجمان برای فریب فناوری "تشخیص چهره" باشد.

باج‌افزارها؛ پیچیده‌تر از قبل

در سال ۱۳۹۸ برخی نویسندگان باج‌افزار از سیستم‌های از قبل آلوده شده به بدافزار دیگر یا از دستگاه‌های با پودمان RDP قابل دسترس بر روی اینترنت به‌منظور کپی فایل باج‌افزار و اجرای این نوع بدافزارهای مخرب بر روی آنها بهره گرفتند. اجرای موفق چنین حملاتی معمولاً مستلزم مشارکت گروه‌هایی از هکرهاست. اتحادی که نتیجه آن اجرای حملات هدفمند و گسترده‌ای است که در نهایت منجر به کسب سود بالا برای این تبهکاران و وارد آمدن خسارت‌های سنگین و بعضاً غیرقابل جبران برای قربانیان می‌شود. مرکز ارزیابی تهدیدات سازمان‌یافته پلیس اروپا (IOCTA) باج‌افزارها را اصلی‌ترین تهدیدی اعلام کرده که سازمان‌ها و کاربران در سال ۲۰۱۹ با آن روبرو بودند.

انتظار می‌رود که با استقبال مهاجمان از اجرای حملات هدفمند باج‌افزاری معاملات در بازارهای زیرزمینی تبهکاران سایبری از جمله در فروشگاه‌های موسوم به RDP نیز افزایش پیدا کند. فروشگاه‌های RDP، بسترهایی هستند که در آنها دسترسی RDP به ماشین‌های هک شده در اقصا نقاط جهان به فروش رسانده می‌شود.

نمونه‌ای از تبلیغات فروشندگان دسترسی‌های RDP در تصویر زیر قابل مشاهده است:



پیش‌بینی شرکت مک‌آفی درباره باج‌افزارها

شرکت مک‌آفی پیش‌بینی کرده که ضمن استمرار روند صعودی نفوذهای هدفمند به شبکه‌های سازمانی جهت آلوده‌سازی سیستم‌ها به باج‌افزار، از تکنیک‌های دیگری نیز به‌منظور اخاذی هر چه بیشتر یا مؤثرتر استفاده بشود. برای مثال در سال ۱۳۹۸، گردانندگان باج‌افزار Sodinokibi اعلام کردند که ضمن سرقت فایل‌ها و داده‌های قربانیان خود، در صورت پرداخت نشدن مبلغ اخاذی شده اقدام به افشای آنها خواهند کرد.

تغییر باور قدیمی

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

۲/۳ میلیون دلار

در سال ۱۳۹۸، مهاجمان Maze در حمله‌ای باج‌افزاری به شرکت Allied Universal، باجی ۲/۳ میلیون دلاری را از آن شرکت طلب کردند. مدتی بعد و با تحقق نیافتن این خواسته مهاجمان، ۷۰۰ مگابایت از داده‌های Allied Universal در تالارهای گفتگوی نفوذگران منتشر و در دسترس قرار گرفته شد.

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

انتظار می‌رود که تعداد آن دسته از حملات باج‌افزاری که سرقت داده‌های حساس سازمانی بخشی از سناریوی آنهاست افزایش چشم‌گیری پیدا کند.

پودمان RDP؛ استمرار سوءاستفاده

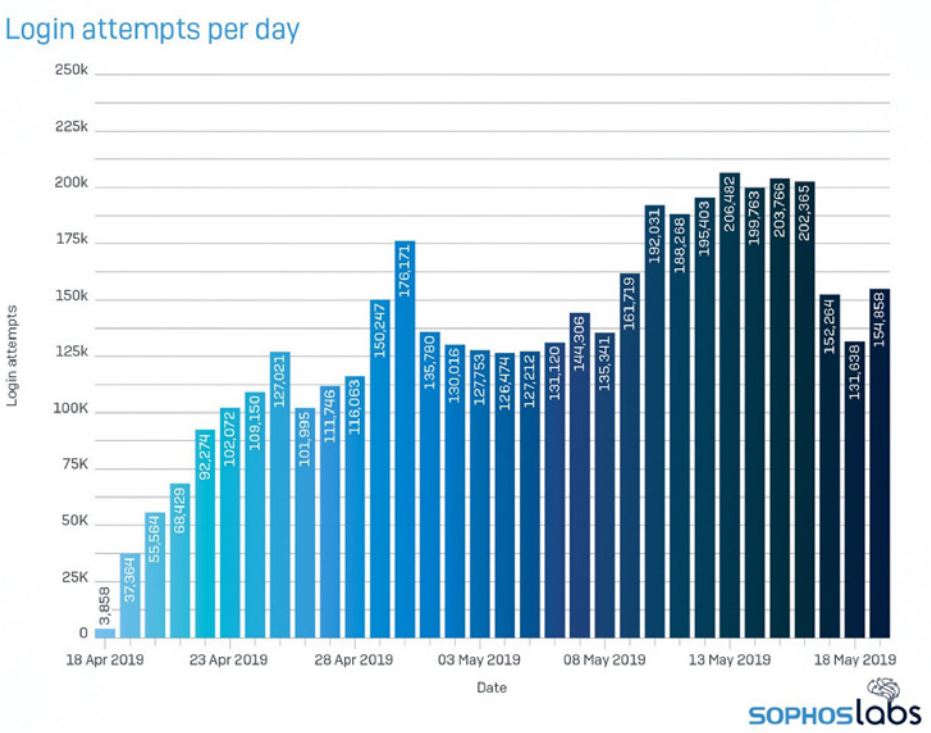
در سال‌های اخیر سوءاستفاده از پودمان Remote Desktop Protocol - به اختصار RDP - توسط مهاجمان سایبری افزایش چشمگیری داشته است.

علاوه بر مدیران شبکه که از این پودمان برای اتصال به سرورها و ایستگاه‌های کاری سازمان استفاده می‌کنند، در بسیاری از سازمان‌های کوچک و متوسط نیز از RDP برای برقرار نمودن ارتباط از راه دور پیمانکاران حوزه فناوری اطلاعات، به سرورهایی همچون حقوق و دستمزد، اتوماسیون اداری و غیره استفاده می‌شود.

SamSam از نخستین باج‌افزارهایی بود که در سال ۱۳۹۷، گردانندگان آن، نه از طریق ارسال هرزنامه‌های با پیوست یا لینک آلوده که با نفوذ به دستگاه‌های با پودمان RDP باز و رمز عبور ضعیف اقدام به رخنه به سازمان‌ها و اخاذی مبالغ هنگفت از آنها می‌کردند.

این روش انتشار SamSam به سرعت به الگویی برای سایر نویسندگان بدافزار تبدیل شد.

میلیون‌ها دستگاه با RDP قابل دسترس در بستر اینترنت نقشی اساسی در گسترش آلودگی‌ها در سطح جهان دارند. تصویر زیر تعداد تلاش مهاجمان برای ثبت ورود (Login) به دستگاه‌های با RDP باز را که شرکت سوفوس آنها را به‌عنوان Honeypot راه‌اندازی کرده است در بازه‌ای یک‌ماهه نشان می‌دهد.



مهاجمان از ابزارهایی نظیر Shodan برای شناسایی سرورهای با پودمان RDP قابل دسترس بر روی اینترنت استفاده کرده و در ادامه با بکارگیری ابزارهایی همچون NLBrute اقدام به اجرای حملات موسوم به "سعی‌وخطا" (Brute Force) می‌کنند.

هدف از اجرای حملات "سعی‌وخطا" رخنه به دستگاه از طریق پودمانی خاص - در اینجا RDP - با بکارگیری ترکیبی از نام‌های کاربری و رمزهای عبور رایج است. بنابراین در صورتی که دسترسی به پودمان RDP از طریق کاربری با رمز عبور ساده و غیرپیچیده باز شده باشد مهاجمان نیز به‌راحتی امکان اتصال به دستگاه را خواهند داشت. در ادامه نیز با استفاده از ابزارهایی همچون Mimikatz قادر به استخراج اطلاعات اصالت‌سنجی حساب‌های کاربری با سطح دسترسی بالا همچون حساب‌های Domain Admin و نفوذ به سایر سیستم‌ها خواهند بود.

متأسفانه در اکثر مواقع این سرورها هستند که پودمان RDP آنها در بستر اینترنت قابل دسترس است. سرورها بنا به ماهیت و عملکردشان عمدتاً حاوی اطلاعاتی بسیار حساس، با ارزش‌های مالی و معنوی بالا هستند. به‌همین خاطر در صورت موفقیت در رخنه به آنها منافع قابل‌توجهی متوجه مهاجمان خواهد شد.

انتخاب هدفمند

در برخی موارد نیز مهاجمان با انتخاب دقیق اهداف خود، پس از نفوذ به یکی از سرورهای با دسترسی RDP باز، اقدام به اجرای عملیات شناسایی (Reconnaissance) بر ضد کارکنانی خاص کرده و پس از استخراج اطلاعات مورد نیاز، آنها را با فیشینگ‌های هدفمند (Spear Phishing) مورد حمله قرار می‌دهند تا از این طریق به داده‌های حساس سازمانی نظیر اطلاعات اصالت‌سنجی لازم برای ورود به سامانه‌ها دست پیدا کنند.

توصیه

به تمامی مدیران و راهبران شبکه‌ها در هر اندازه‌ای توصیه می‌شود تحت هیچ شرایطی، حتی برای مدتی کوتاه دسترسی به شبکه سازمان را از طریق سازوکار RDP بدون در نظر داشتن توصیه‌ها و الزامات امنیتی فراهم نکنند.

سرویس‌های در معرض اینترنت، تهدید جدی علیه امنیت سازمان

سایر سرویس‌ها

سوءاستفاده مهاجمان از سرویس‌های قابل دسترس در بستر اینترنت به‌منظور رخنه به شبکه سازمان محدود به RDP نمی‌شود. در سال‌های اخیر، دامنه گسترده‌ای از این پودمان‌ها مورد توجه نفوذگران و گردانندگان بدافزار قرار گرفته است. از جمله آنها می‌توان به سرورهای پایگاه داده، روترهای خانگی، مودم‌های DSL، دستگاه‌های ذخیره‌ساز متصل به شبکه (NAS)، سیستم‌های VoIP و بسیاری از دستگاه‌های موسوم به اینترنت اشیا (IoT) اشاره کرد.

بدافزار پیشرفته lemon_Duck

به‌طور ویژه سرورهای Microsoft SQL در معرض حملات گسترده‌ای قرار دارند. برای مثال می‌توان به بدافزار پیشرفته Lemon_Duck اشاره کرد که در سال ۱۳۹۸ مهاجمان با بکارگیری آن اقدام به اجرای حملات رمز ربایی (Cryptojacking) بر ضد سازمان‌ها در بسیاری از کشورها از جمله ایران کردند. در جریان حملات این مهاجمان، فهرستی از نشانی‌های IP به‌صورت تصادفی ایجاد شده و پس از مورد هدف قرار دادن آنها، قابل دسترس بودن چندین درگاه از جمله TCP/1433 که درگاه پیش‌فرض MS-SQL است مورد بررسی قرار می‌گیرد. چنانچه درگاه 1433 بر روی دستگاه هدف باز باشد بدافزار اقدام به اجرای حملات موسوم به "سعی‌وخطا" (Brute-force) جهت رخنه به سرویس‌دهنده MS-SQL نصب‌شده بر روی دستگاه می‌کند. برای این منظور Lemon_Duck با بکارگیری رمزهای عبور زیر و مجموعه‌ای از هش NTLM تلاش می‌کند تا حساب کاربری sa در سرویس Microsoft SQL را هک کند. فهرست این رمزهای عبور به‌شرح زیر است:

“saadmin”, “123456”, “password”, “PASSWORD”, “123.com”, “admin@123”, “Aa123456”, “qwer12345”, “Huawei@123”, “123@abc”, “golden”, “123!@#qwe”, “1qaz@WSX”, “Ab123”, “1qaz!QAZ”, “Admin123”, “Administrator”, “Abc123”, “Admin@123”, “999999”, “Passw0rd”, “123qwe!@#”, “football”, “welcome”, “1”, “12”, “21”, “123”, “321”, “1234”, “12345”, “123123”, “123321”, “111111”, “654321”, “666666”, “121212”, “000000”, “222222”, “888888”, “1111”, “555555”, “1234567”, “12345678”, “123456789”, “987654321”, “admin”, “abc123”, “abcd1234”, “abcd@1234”, “abc@123”, “p@ssword”, “P@ssword”, “p@ssw0rd”, “P@ssw0rd”, “P@SSWORD”, “P@SSW0RD”, “P@w0rd”, “P@word”, “iloveyou”, “monkey”, “login”, “passw0rd”, “master”, “hello”, “qazwsx”, “password1”, “qwerty”, “baseball”, “qwertyuiop”, “superman”, “1qaz2wsx”, “f-ckyou”, “123qwe”, “zxcvbn”, “pass”, “aaaaaa”, “love”, “administrator”, “qwe1234A”, “qwe1234a”, “123123123”, “1234567890”, “88888888”, “111111111”, “112233”, “a123456”, “123456a”, “5201314”, “1q2w3e4r”, “qwe123”, “a123456789”, “123456789a”, “dragon”, “sunshine”, “princess”, “!@#$%^&*”, “charlie”, “aa123456”, “homelesspa”, “1q2w3e4r5t”, “sa”, “sasa”, “sa123”, “sql2005”, “sa2008”, “abc”, “abcdefg”, “sapassword”, “Aa12345678”, “ABCabc123”, “sqlpassword”, “sql2008”, “11223344”, “admin888”, “qwe1234”, “A123456”

به‌محض موفقیت در هک حساب کاربری مذکور، بدافزار با استفاده از پروسه sqlserver.exe فرامین مخرب را بر ضد ماشین‌های دیگر اجرا می‌کند.

لازم به ذکر است

یک جستجوی ساده در سایت BinaryEdge نشان می‌دهد که در حال حاضر حدود ۲۱ هزار سرویس‌دهنده SQL مستقر در شبکه سازمان های ایرانی با درگاه پیش‌فرض 1433 بر روی اینترنت قابل دسترس است.

باج‌افزارها

همچنین می‌توان به باج‌افزارهایی اشاره کرد که با نفوذ به دستگاه‌های ذخیره‌ساز متصل به شبکه که در بستر اینترنت به طریقی غیرامن در دسترس قرار گرفته‌اند، اقدام به رمزگذاری فایل‌های ذخیره شده بر روی آنها کرده و در ازای آنچه که مهاجمان بازگرداندن فایل‌ها به حالت اولیه می‌خوانند، مبلغی را از قربانی اخاذی می‌کنند.

حملاتی که مهاجمان در جریان آن با رخنه به روترهای میکروتیک، اسکریپت‌های استخراج‌کننده ارز رمز را بر روی دستگاه‌های متصل به این روترها به اجرا در می‌آورند نمونه‌ای دیگر از سوءاستفاده مهاجمان از سرویس‌های قابل دسترس در بستر اینترنت هستند.

اینترنت اشیاء

چندین سال است که کارشناسان در خصوص امنیت ضعیف وسایل و تجهیزات متصل به اینترنت، موسوم به اینترنت اشیاء هشدار داده‌اند. امنیت ضعیف و پیکربندی آسیب‌پذیر این تجهیزات از یک سو و اتصال آنها به شبکه اینترنت از سویی دیگر، این تجهیزات را به هدفی بسیار مناسب و در عین حال آسان برای مهاجمان تبدیل کرده است. یکی از اصلی‌ترین بهره‌جویی‌های تبهکاران سایبری از این وسایل و تجهیزات، تسخیر نمودن آنها برای اجرای حملات توزیع شده برای از کاراندازی سرویس (DDoS) است.

در این حملات، لشکری از این تجهیزات هک‌شده با ارسال درخواست‌های همزمان به سرور قربانی آن را بمباران می‌کنند. دریافت همزمان درخواست، از هزاران و در برخی مواقع ده‌ها هزار دستگاه با نشانی‌های IP مختلف، در نهایت، منجر به کندی و یا حتی توقف خدمات‌دهی سرور به کاربران می‌شود. واقعیت آن است که دستگاه‌های متصل به اینترنت، صرفاً دستگاه‌هایی با منابع محدود نیستند. بلکه کامپیوترهایی هستند که اگر به‌طور صحیح پیکربندی و ایمن‌سازی نشوند، می‌توانند به ابزاری مخرب در دست نفوذگران تبدیل شوند.

پرهیز از بکارگیری رمزهای عبور ساده یا تکراری، اطمینان از نصب بودن آخرین به‌روزرسانی‌ها و اصلاحیه‌های امنیتی، اعمال پیکربندی امن و غیرفعال کردن پودمان‌ها و درگاه‌های غیر مورد نیاز بر روی این تجهیزات اصلی ترین راهکارها در ایمن نگاه داشتن سازمان از گزند این نوع تهدیدات است.

ادامه حیات WannaCry، بیانگر واقعیتی تلخ

۲۲ اردیبهشت ۱۳۹۶، منابع متعدد از انتشار گسترده باج‌افزار جدیدی با عنوان WannaCry خبر دادند. باج‌افزاری که با خاصیت کرم‌گونه و با بهره‌جویی (Exploit) از یک ضعف امنیتی در بخش SMB سیستم عامل Windows از روی نخستین دستگاه آلوده شده، به‌سرعت خود را در سطح شبکه و اینترنت تکثیر می‌کرد. سرعت و گستره انتشار این باج‌افزار در نوع خود بی‌نظیر بود. به‌نحوی که در مدتی بسیار کوتاه، بیش از ۲۰۰ هزار دستگاه در ۱۵۰ کشور جهان به WannaCry گرفتار شدند.

ماجرای آسیب‌پذیری مورد استفاده WannaCry به حدود سه سال قبل و انتشار اسناد محرمانه‌ای باز می‌گردد که در جریان آن فایل‌های سرقت شده از یک گروه نفوذگر حرفه‌ای با نام Equation که وابستگی اثبات شده‌ای به "سازمان امنیت ملی" دولت آمریکا (NSA) دارد توسط گروه Shadow Brokers بر روی اینترنت به اشتراک گذاشته شدند. در بین این فایل‌ها، بهره‌جوهایی به چشم می‌خوردند که از یک ضعف امنیتی روز صفر (Zero-day) در بخش سیستم عامل Windows که به EternalBlue موسوم شد سوءاستفاده می‌کردند. یک ماه پیش از درز این اطلاعات، شرکت مایکروسافت اصلاحیه‌ای با شناسه MS17-010 را به‌منظور ترمیم آسیب‌پذیری مذکور عرضه نموده بود.

نجات غیرمنتظره

در پی انتشار این باج‌افزار، محققی با نام Marcus Hutchins اقدام به ثبت دامنه‌ای هم‌نام با دامنه‌ای کرد که در کد WannaCry به آن اشاره شده بود. هدف او صرفاً ردیابی آلودگی‌ها به این باج‌افزار در نقاط مختلف جهان بود. اما این کار او تصادفاً سبب از کار افتادن گونه‌هایی از این باج‌افزار شد.

برخی ویروس‌نویسان فرامینی را در کد بدافزار خود درج می‌کنند که در صورت فعال شدن آنها، انتشار بدافزار متوقف می‌شود. به این نوع کدها Kill Switch گفته می‌شود. نویسندگان WannaCry نیز در یکی از توابع برنامه‌نویسی خود درخواستی را به دامنه مذکور ارسال می‌کردند. بر طبق این تابع در صورت دریافت پاسخ از این دامنه باج‌افزار از اجرای فرامین مخرب خودداری می‌کرد. به‌نظر می‌رسد صاحبان WannaCry قصد داشته‌اند که در شرایط خاص با راه‌اندازی این دامنه انتشار باج‌افزار را متوقف کنند. ثبت زود هنگام این دامنه توسط Hutchins عملاً سبب فعال‌سازی Kill Switch باج‌افزار حداقل در برخی گونه‌های آن و در نتیجه کاهش مقطعی روند آلودگی‌ها شد.

اما کشف این Kill Switch نیز به حیات WannaCry پایان نداد. به‌سرعت عده‌ای از مهاجمان ناشناس اقدام به اعمال تغییرات در کد باج‌افزار به‌نحوی کردند که در آن از Kill Switch صرف‌نظر می‌شد. اما این نسخ دستکاری شده از WannaCry، خود، حاوی باگی بودند که در نهایت موجب می‌شد که باج‌افزار قادر به رمزگذاری فایل‌ها نباشد؛ اما در عین حال نسخ مذکور قابلیت انتشار بر روی دستگاه‌های فاقد اصلاحیه را دارا بودند.

عاملی که موجب انتشار گسترده WannaCry شد عدم نصب اصلاحیه‌ای (MS17-010) بود که قبل از ظهور این باج‌افزار توسط مایکروسافت عرضه شده بود. جالب اینکه علیرغم گذشت حدود سه سال از عرضه اصلاحیه مذکور و اطلاع‌رسانی‌های گسترده در خصوص لزوم نصب آن، همچنان این باج‌افزار در صدر بدافزارهای فعال در برخی سازمان‌ها قرار دارد. موضوعی که به روشنی از عدم توجه بسیاری از راهبران نسبت به ضرورت نصب اصلاحیه‌های امنیتی حکایت دارد.

WannaCry بدافزاری است که به دلیل ماهیت باج‌افزاری خود به سرعت کاربر را از آلوده بودن سیستم به آن آگاه می‌کند. حال آنکه بدافزارهای مخربی همچون جاسوس‌افزارها می‌توانند برای مدت‌ها بر روی دستگاه‌ها ماندگار بمانند. لذا اطمینان از نصب بودن اصلاحیه‌های امنیتی سیستم‌های عامل و کلیه برنامه‌های کاربردی یکی از ضروری‌ترین اقدامات در ایمن نگاه داشتن سازمان از گزند تهدیدات سایبری است.

سیستم‌های عامل از رده خارج؛ بیشتر از قبل

سالهاست که ویروس‌نویسان و نفوذگران به‌شدت به استفاده از نقاط ضعف سیستم‌های عامل - به ویژه سیستم عامل پرطرفدار Windows - روی آورده‌اند. وجود یک نقطه ضعف خطرناک در سیستم عامل می‌تواند سبب دور زدن قوی‌ترین نرم‌افزارهای ضدویروس یا دیواره‌های آتش شود!

شرکت مایکروسافت علاوه بر عرضه اصلاحیه فوری در مواقع اضطراری، در سه‌شنبه دوم هر ماه میلادی نیز اصلاحیه‌های امنیتی جدید خود را منتشر می‌کند. کمتر سه‌شنبه دوم ماه میلادی را می‌توان یافت، که مایکروسافت اصلاحیه‌ای "حیاتی" (Critical) را برای سیستم عامل Windows عرضه نکرده باشد.

این در حالی است که پشتیبانی این شرکت از سیستم‌های عامل Windows 7 و Windows Server 2008/2008 R2 در ۲۴ دی ماه ۹۸ به پایان رسید و عملاً مایکروسافت عرضه اصلاحیه‌های امنیتی برای این سیستم‌های عامل را متوقف کرده است. بنابراین نفوذگران با اطلاع از جزئیات نقاط ضعف جدید کشف شده در سیستم‌های عامل پشتیبانی شده که توسط شرکت مایکروسافت منتشر می‌شوند می‌توانند با مهندسی معکوس این نقاط ضعف را در این سیستم‌های عامل از رده خارج نیز شناسایی نموده و از آنها سوءاستفاده کنند.

آمار منابع مختلف نشان می‌دهد که علیرغم اطلاع‌رسانی‌ها و هشدارهای قبلی، نسخ مذکور همچنان سهم قابل‌توجهی از سیستم‌های عامل نصب شده بر روی ایستگاه‌های کاری و سرورها را به خود اختصاص داده‌اند.

حتی در مواردی وجود سیستم‌های عامل Windows XP و Windows Server 2003 که سال‌ها از پایان پشتیبانی آنها توسط مایکروسافت می‌گذرد نیز در برخی سازمان‌ها به چشم می‌خورد.

باید توجه داشت علاوه بر مایکروسافت، سازندگان محصولات امنیتی نظیر ضدویروس هم دیر یا زود، پشتیبانی از سیستم‌های عامل Windows 7 و Windows Server 2008/2008 R2 را متوقف خواهند کرد.

ارتقای سیستم‌های عامل قدیمی و از رده خارج به نسخ جدیدتر و قابل پشتیبانی در اسرع وقت توصیه اکید می‌شود.

کمبود نیروی متخصص؛ همچنان یک دغدغه پرچالش

یکی از اصلی ترین چالش‌هایی که مدیران امنیت سازمان‌ها با آن روبرو هستند، جذب کارکنان متخصص در حوزه امنیت فناوری اطلاعات است. کمبود نیروی متخصص همچنان به ایران نیست؛ بر اساس گزارشی که در اواخر سال ۱۳۹۸ شرکت کربن بلک آن را منتشر کرد ۷۹ درصد از سازمان‌ها یافتن نیروی نخبه در حوزه امنیت را موضوعی بسیار پرچالش توصیف می‌کنند. ۷۰ درصد هم نه فقط جذب نیروی کاردان امنیت که حتی استخدام نیروی متخصص فناوری اطلاعات را نیز کاری چالشی می‌دانند.

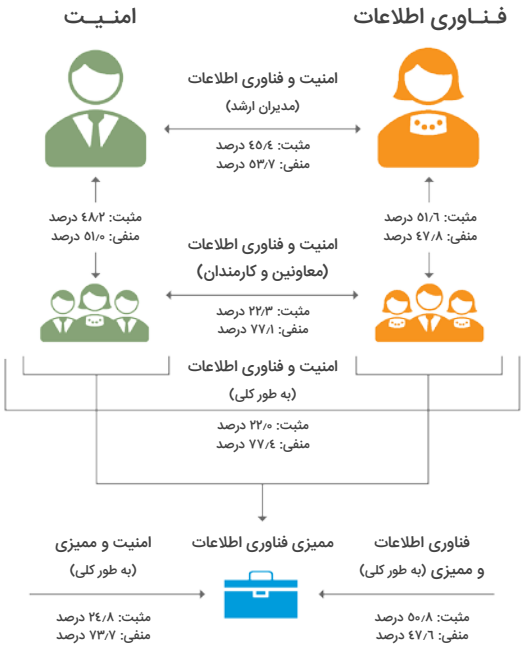
٪۷۰

درصد نه فقط جذب نیروی کاردان امنیت که حتی استخدام نیروی متخصص فناوری اطلاعات را نیز کاری چالشی می‌دانند.

٪۷۹

درصد یافتن نیروی نخبه در حوزه امنیت را موضوعی "بسیار" یا "فوق‌العاده" چالش‌برانگیز می‌دانند.

روابط منابع انسانی فعال در بخش‌های فناوری اطلاعات و امنیت نیز در بسیاری از موارد وضعیت چندان آرمانی ندارد. در یک بررسی انجام شده توسط شرکت کربن بلک، در ۷۷/٤ درصد موارد ارتباط میان کارکنان این بخش ها با مدیران ارشدشان نامناسب است. ۵۳/۷ درصد ارتباط مدیران این بخش ها را نیز پرتنش توصیف کرده اند.



نتایج نظرسنجی از کارکنان در خصوص ارتباطات میان آنها | منبع: گزارش Cybersecurity Outlook -وی‌ام‌ور کربن بلک - زمستان ۱۳۹۸

به‌نظر می‌رسد که آموزش کارکنان موجود و افزایش دانش آنها در بخش‌های مرتبط با نیازهای امنیت فناوری اطلاعات سازمان می‌تواند تا حدودی راهگشای این مشکل پرچالش باشد.

ادامه تلاش‌ها برای مختل کردن روند کسب‌وکارها

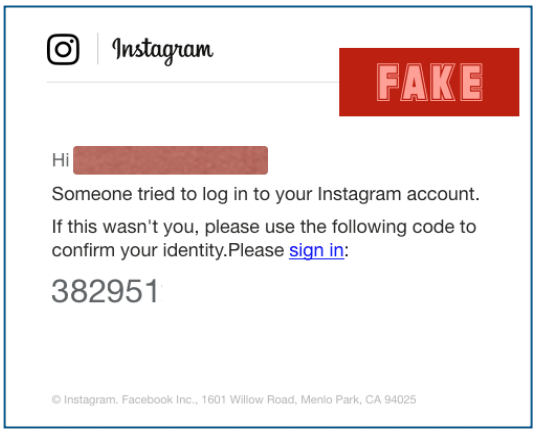
در سالی که گذشت بروز اختلال در روند کسب‌وکارها در نتیجه حملات سایبری یکی از اصلی‌ترین سرخط های اخبار امنیت فناوری اطلاعات در جهان بود. بر طبق آماری که کرود استرایک ارائه کرده ۳۶ درصد از موارد بررسی شده توسط این شرکت امنیتی به نحوی مرتبط با از کار افتادن کسب و کار سازمان بوده است. این اختلالات عمدتاً به سبب باج‌افزارها، بدافزارهای مخرب و حملات از کاراندازی سرویس بوده است. در حالی که در نمونه‌های باج‌افزاری هدف اصلی مهاجمان کسب منافع مالی است، اما تأثیر اختلال ناشی از آن بر روی کسب‌وکار ممکن است برای سازمان پرهزینه‌تر از مبلغ اخاذی شده باشد و این دقیقاً همان چیزی است که مهاجمان باج افزار در پی آن هستند. در سال ۹۸ میانگین مبالغ اخاذی شده از سوی مهاجمان در حملات هدفمند سازمانی نیز روندی رو به رشد در مقایسه با سال قبل از آن داشتند.

فیشینگ؛ کماکان ماندگار

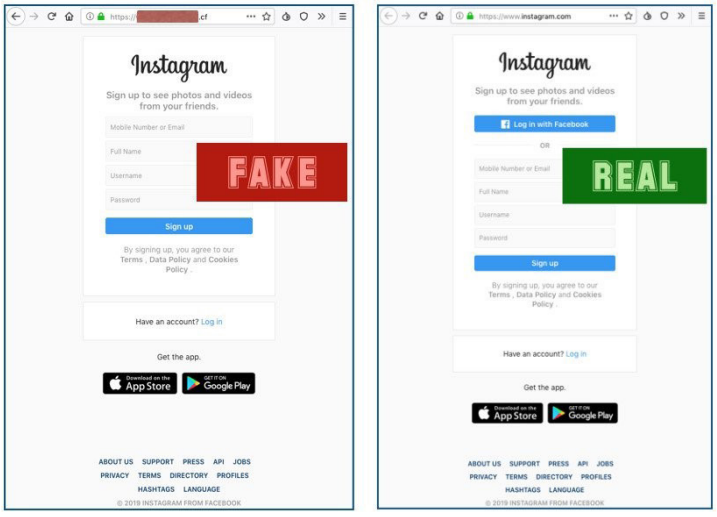
کرود استرایک گزارش کرده که حملات فیشینگ هدفمند با هدف رخنه اولیه به یک شبکه در ۳۵ درصد از کیس های مورد بررسی توسط این شرکت در سال ۲۰۱۹ نقش داشته است که در مقایسه با سال قبل از آن ۲ درصد رشد را نشان می دهد.

همچنین با توجه به افزایش استفاده از سازوکارهای اصالت سنجی چندعاملی انتظار می رود که مهاجمان بیشتری به بهره جویی از این سازوکار روی بیاورند. برای مثال در سالی که گذشت شرکت امنیتی سوفوس از اجرای کارزاری فیشینگ 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.

در آن کارزار نیز ایمیل ارسالی ظاهری کاملا مشابه با ایمیل‌های Instagram داشت. 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.



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.

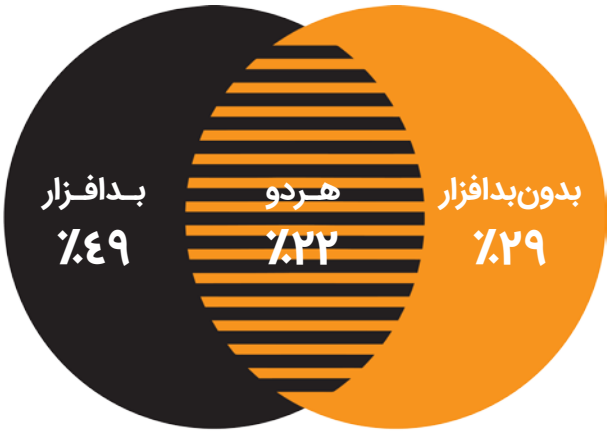
روش اجرای این کارزار فرصتی است برای یادآوری این نکته مهم که صرف استفاده از پودمان HTTPS در نشانی یک سایت به معنای معتبر بودن آن نیست و راهکار اصلی دقت به صحیح بودن نشانی (در اینجا instagram.com) است. همچنین استفاده از احراز هویت دو عاملی نیز همواره توصیه می‌شود.

زنجیره تأمین؛ حملاتی به‌شدت مخرب

حملات موسوم به زنجیره تأمین (Supply Chain) همواره یکی از بی سروصداترین اما مخرب ترین نوع تهدیدات سایبری بوده اند.
در این نوع کارزارها، مهاجمان با بهره‌جویی از اجزای آسیب‌پذیر در زنجیره تأمین یک سازمان به آن رخنه و یا آن را دچار اختلال می‌کنند.
اگر چه سهم این حملات در مقایسه با سایر انواع حملات کم برآورد شده اما این نوع حملات می توانند برای مدتها مخفی و در مقایسه با سایر روش ها تأثیرات به مراتب زیان‌بارتری را متوجه سازمان کنند.

بدافزارهای بدون فایل؛ فراگیرتر از قبل

به گفته کرود استرایک در ۵۱ درصد از رخدادهای گزارش شده به این شرکت در سال ۲۰۱۹ مهاجمان در برخی از مراحل حمله از تکنیک‌های موسوم به Malware-free بهره گرفته بودند که در آنها بدافزار نقش نداشته است. تکنیک‌های Malware-free شامل (اما نه محدود به) استفاده از PowerShell، اسکریپت‌نویسی، Mshta و WMI است. جالب اما نگران‌کننده این که در ۲۹ درصد از موارد نیز تنها از تکنیک Malware-free استفاده شده است. هدف مهاجمان از بکارگیری این تکنیک حذف رد پا و دشوار کردن کار سازمان در شناسایی به موقع حمله و واکنش به آن است. به همین خاطر سازمان ها نیازمند ابزارهای رصدی هستند که استفاده‌های مخرب از این ابزارها را از استفاده های مجاز آنها تفکیک می‌کند.



درصد حملات به تفکیک تکنیک | منبع: کروداسترایک - ۱۳۹۸

در سیستم عامل Windows بیش از یکصد ابزار وجود دارد که به صورت بالقوه قابلیت مورد استفاده قرار گرفتن در جریان حملات سایبری را دارند.

در جریان این حملات از ابزارهای معتبر از قبل نصب شده (Pre-installed) بر روی سیستم استفاده می‌کنند. در سیستم عامل Windows بیش از یکصد ابزار وجود دارد که به صورت بالقوه قابلیت مورد استفاده قرار گرفتن در جریان حملات سایبری را دارند.
برخی کارشناسان دلیل استقبال مهاجمان از ابزارهای از قبل نصب شده را کاهش تعداد آسیب پذیری های روز صفر و تلاش و زحمت زیاد مورد نیاز برای کشف آنها می دانند. بهبودهای لحاظ شده در مرورگرها، کشف چنین آسیب پذیری هایی را بسیار دشوار می کند. همچنین برنامه های موسوم به Bug bounty موجب تسریع کشف این ضعف های امنیتی و بهبود در محصولات حداقل برندهای معروف شده است. ضمن اینکه در برخی بسترهای بسیار حساس اجرای هر گونه پروسه مگر پروسه های معتبر غیرمجاز تلقی می شود که این تکنیک نیز می تواند این سازوکارهای امنیتی را دور بزند. همه دلایل در کنار یکدیگر موجب شده که استقبال از LOTL در سالهای اخیر افزایش پیدا کند. عمده ابزارهای معتبری که مورد بهره جویی تبهکاران سایبری قرار می گیرد به شرح زیر است:

- PowerShell
- VB scripts
- WMI
- Mimikatz
- PsExec

به طور کلی تمامی این ابزارها کاربردهای مجازی بر روی دستگاه ها دارند لذا تشخیص اینکه مورد بهره جویی قرار گرفتن آنها با اهدافی مخرب توسط قربانی و محصولات امنیتی، کاری بسیار دشوار محسوب می شود. اجرای عملیاتی همچون سرقت داده ها، دسترسی از راه دور به دستگاه و بروز اختلال در عملیات بدون استفاده از هر گونه بدافزار و برنامه مخرب کاملا ممکن و شدنی است.

جدول زیر ۵ تکنیک با بیشترین استفاده را در سال ۲۰۱۹ نمایش می دهد.

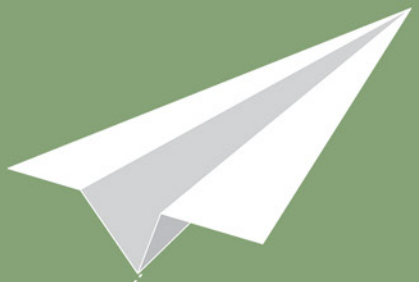
رنـک	نـوع
۱	Credential Dumping
۲	PowerShell
۳	Account Discovery
٤	Scripting
٥	Command Line

پنج تکنیک مخرب با بیشترین استفاده در سال ۲۰۱۹ بر مبنای استاندارد MITRE ATT&CK | منبع: کروداسترایک - ۱۳۹۸

مؤثرین راهکارها در مقابله با این تهدیدات نیز در جدول زیر قابل مشاهده است:

مقـــاوم ســـازی	Credential Dumping	PowerShell	Account Discovery	Scripting	Command Line
پیکربندی Active Directory	■				
حفاظت از دسترسی به اطلاعات اصالت‌سنجی	■				
پیکربندی سیستم عامل	■		■		
سیاست‌های رمز عبور	■				
سامانه Privileged Account Management	■				
حفاظت از پروسه‌های با سطح دسترسی بالا (Privileged Process Integrity)	■	■			
آموزش کاربران	■				
امضای کد		■			
غیرفعال یا حذف کردن قابلیت یا برنامه		■		■	
ایزوله کردن برنامه و بسترهای موسوم به Sandboxing				■	
جلوگیری از اجرا					■

فهرست مؤثرترین تکنیک‌های مقاوم‌سازی | منبع: کروداسترایک - ۱۳۹۸



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.

تـــارنـــمـــای شـــرکت www.shabakeh.net

خدمات پس از فروش و پشتیبانی my.shabakeh.net

مـــرکـــز آمـــوزش events.shabakeh.net

اتاق خبـــر newsroom.shabakeh.net

شبکه گستر
شـــرکت مـهـنـدسی شـبـکـه گسـتـر

تهران خیابان شهید دستگردی (ظفر) شماره ۲۷۳
تلفن / دورنگار: ۴۲۰۵۲ - ۰۲۱
رایانامه: info@shabakeh.net