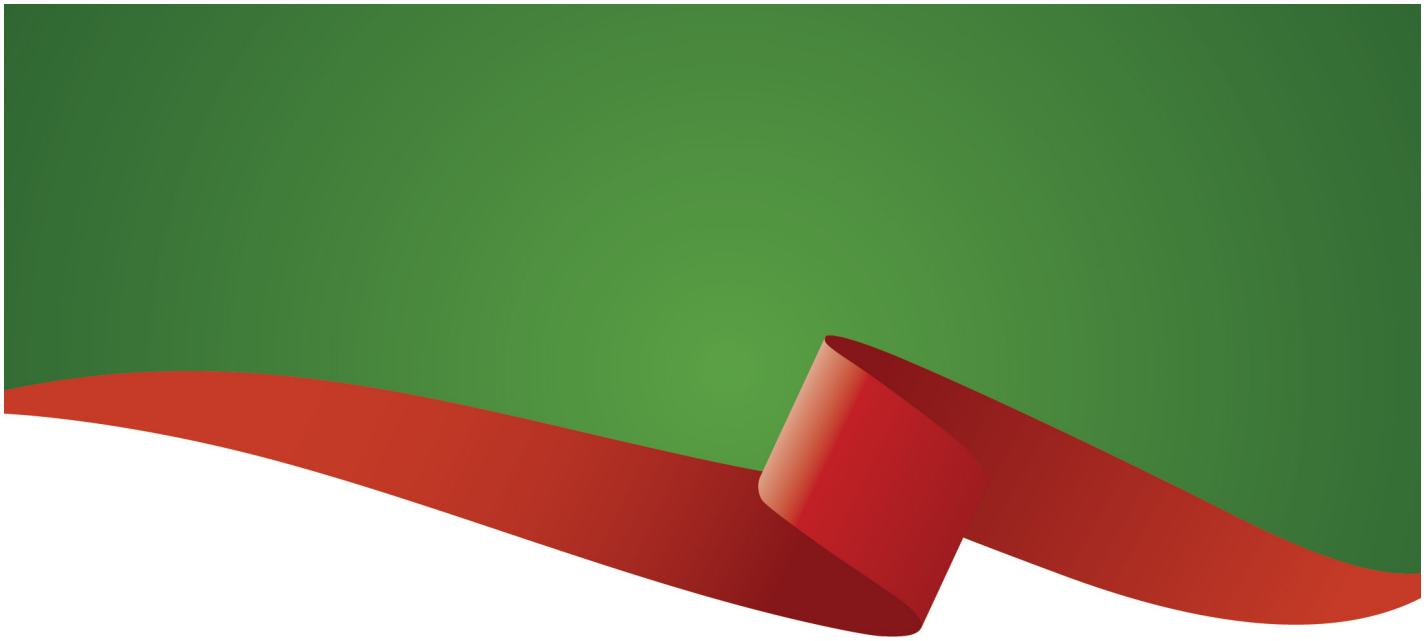
شبکه گستر

فصلنامه شرکت مهندسی شبکه گستر

امنیت فناوری اطلاعات

ویژه نامه سال

۹۶



شبکه گستر

فناوری اطلاعات تغییراتی بنیادین در زندگی روزمره و کاری مردم در اقصی نقاط جهان ایجاد کرده است. تغییراتی که سبب وابستگی هر چه بیشتر بشر به این فناوری، ارزشمندتر شدن داده‌های انتقال یافته بر روی آن و حیاتی‌تر شدن بسیاری از خدمات الکترونیکی شده است. آنچه که اکنون بیش از هر زمانی دیگر اهمیت پیدا می‌کند امنیت این داده‌ها و خدمات است. مساله‌ای که هم نهادهای قانونی و هم سازندگان محصولات امنیتی از تأمین کامل آن ناتوان بوده‌اند و همواره چالشی برای کاربران و سازمان‌ها و صد البته فرصتی برای تبهکاران بوده است. اینترنت با وجود تمامی محاسن آن، جولانگاهی بی‌نظیر برای مجرمان و بدخواهان است. بستری که آنها را قادر می‌سازد با کمترین ردپا مقاصد شوم و پلید خود را دنبال کنند.

حدود سه دهه قبل، ویروس‌ها اصلی‌ترین تهدید برای سیستم‌ها و شبکه‌های کامپیوتری محسوب می‌شدند. برنامه‌های مخربی که معمولاً توسط افرادی ماجراجو و صرفاً با هدف جلب توجه کاربران به مهارت ویروس‌نویس نوشته می‌شدند.

اما سالهاست که دامنه تهدیدات کامپیوتری از ویروس‌های پر سروصدا فراتر رفته است. گردانندگان این تهدیدات نیز دیگر محدود به آن جوانان کنجکاو نیستند. کم نیستند ویروس‌نویسان و هکرهایی که سالانه میلیون‌ها دلار را از راه انتشار بدافزارهای مخرب یا اجرای حملات سایبری به جیب می‌زنند. ضمن اینکه بسیاری از دولت‌ها نیز با منابع بی‌پایان خود اقدام به حمایت از ساخت بدافزارها و اجرای حملاتی می‌کنند که نه تنها تحلیل هر یک از آنها ماه‌ها زمان می‌برد بلکه شناسایی آنها نیز در بسیاری موارد با تاخیرهای حتی چندساله صورت می‌گیرد.

در آستانه فرا رسیدن سال نو بر آن شدیم تا بر اساس رویدادها و تجارب کسب شده در گذشته به بررسی و پیش‌بینی اتفاقات حوزه امنیت فناوری اطلاعات در سال ۹۶ بپردازیم. با این امید که همگی با آمادگی هر چه بیشتر سال جدید را آغاز کنیم.

باج‌افزارها و روند آن‌ها در سال ۹۶

سوءاستفاده از اطلاعات ذخیره شده بر روی سیستم‌های کامپیوتری به سال‌ها قبل باز می‌گردد. در اواسط دهه ۸۰ میلادی یکی از کارکنان بخش IT یک شرکت بیمه در آمریکا قطعه کد مخربی را در سیستم نرم‌افزاری شرکت اضافه کرد تا اگر روزی از آن شرکت اخراج شد اطلاعات حیاتی سیستم حذف شود. دو سال بعد او از کار برکنار شد و در پی آن اطلاعات با ارزش این شرکت نیز حذف شد.

چند سال بعد ویروسی شناسایی شد که هر چند فایلی را از روی سیستم پاک نمی‌کرد اما به‌نحوی دسترسی کاربر به آن فایل‌ها را مسدود می‌کرد. نویسنده این ویروس اقدام به ارسال یک پاکت حاوی دیسکتی با برچسب AIDES به حدود ۲۰ هزار شخص، مؤسسه و شرکت مختلف کرده بود.

در پاکت ارسال شده، علاوه بر دیسکت، برگه‌ای قرار داشت که در یک طرف آن توضیحاتی در خصوص برنامه و نحوه اجرای آن و در طرف دیگر آن، با قلمی ریز، توافقنامه لیسانس درج شده بود. در توافقنامه به کاربر هشدار داده می‌شد که نرم‌افزار درون دیسکت رایگان نبوده و باید برای استفاده یک ساله ۱۸۹ دلار و برای استفاده مادام‌العمر ۳۸۹ دلار به یک نشانی پستی در آمریکا پرداخت شود و در صورتی که کاربر بدون پرداخت مبلغ، اقدام به اجرای برنامه کند سیستم او دچار اشکال می‌شود.

با اجرای برنامه درون دیسکت توسط کاربر بی‌توجه به توافقنامه، تغییراتی بر روی فایل Autoexec.bat اعمال شده و با هر بار راه‌اندازی دستگاه یک عدد به شمارشگر برنامه اضافه می‌شد. زمانی که مقدار شمارشگر به ۹۰ می‌رسید، پوشه‌های درایو C، مخفی و نام فایل‌های درون آنها رمز می‌شدند. پس از آن از قربانی خواسته می‌شد تا برای بازگرداندن وضعیت سیستم به حالت اولیه مبلغ ۱۸۹ دلار را به آن نشانی پستی در آمریکا ارسال کند.

این ویروس را که به AIDS معروف شد می‌توان اولین باج‌افزار (Ransomware) تاریخ کامپیوتر قلمداد کرد.

باج‌افزار، بدافزاری است که هدف آن مسدود کردن دسترسی کاربر به دستگاه و / یا فایل‌های بااهمیت آن، ارعاب او و اخاذی در ازای بازگرداندن دسترسی است.

اوج شهرت این نوع بدافزارها، سال ۹۵ همزمان با انتشار گسترده باج‌افزارهای رمزگذار بود. به نحوی که بسیاری از صاحبنظران امنیت سایبری، سال ۲۰۱۶ میلادی را سال باج‌افزار نامیدند. باج‌افزارهای رمزگذار، فایل‌های کاربر را رمزنگاری می‌کنند. هدف از رمزنگاری، تغییر ساختار فایل است؛ به‌نحوی که تنها با داشتن کلید رمزگشایی بتوان به محتوای فایل دسترسی پیدا کرد. میزان قدرت رمزنگاری بر اساس تعداد بیت بکار رفته در کلید است. هر چه تعداد این بیت‌ها بیشتر باشد، شکستن رمزنگاری هم دشوارتر و در تعدادهای بالا عملاً غیرممکن می‌شود.

مدتی است که برخی از صاحبان باج‌افزارها اقدام به عرضه خدماتی موسوم به "باج‌افزار به عنوان سرویس" (Ransomware-as-a-Service) کرده‌اند. در این روش، دارنده باج‌افزار، آن را به عنوان یک خدمت به متقاضی اجاره می‌دهد. متقاضی که ممکن است در برنامه‌نویسی تخصصی نداشته باشد تنها وظیفه انتشار فایل حاوی باج‌افزار را بر عهده دارد. در نهایت بخشی از مبلغ اخاذی شده از قربانی به صاحب باج‌افزار و بخشی دیگر به اجاره‌کننده باج‌افزار می‌رسد.

در سال ۹۵ گزارش‌هایی نیز از حمله باج‌افزارها به دستگاه‌های موسوم به اینترنت اشیاء (IoT) منتشر شد. در همین سال دو محقق در کنفرانس RSA، یک نمونه باج‌افزار را ارائه کردند که ضمن قطع دسترسی به

دســـتگاه PLC تنظیمـــات آن را نیـــز تغییـــر مـــی‌داد.

آنچه مسلم است باج‌افزارهای رمزگذار یکی از تهدیدات پردرآمد برای ویروس‌نویسان محسوب می‌شوند. برآورد شده که در سال ۲۰۱۶، صاحبان باج‌افزار در مجموع ۱ میلیارد دلار درآمد داشته‌اند.

گسترش باج‌افزار به‌عنوان خدمات، فروش باج‌افزارهای سفارشی در بازارهای سیاه زیرزمینی، ادامه درآمدزایی این صنعت کثیف و وجود نسخه‌های کد باز، کاربران و کارشناسان امنیتی را در سال جدید نیز همچنان درگیر باج‌افزار خواهد کرد. اما تجارب تلخ قربانیان باج‌افزارهای رمزگذار در دو سال اخیر سبب شده که تا بسیاری از کاربران و سازمان‌ها اقدامات و تصمیمات پیشگیرانه مناسبی را اتخاذ کنند. ضمن اینکه تعداد زیادی از سازندگان ضدبدافزار نیز روش‌های جدیدی را برای شناسایی سریع این بدافزارهای مخرب ابداع و طراحی کرده‌اند.

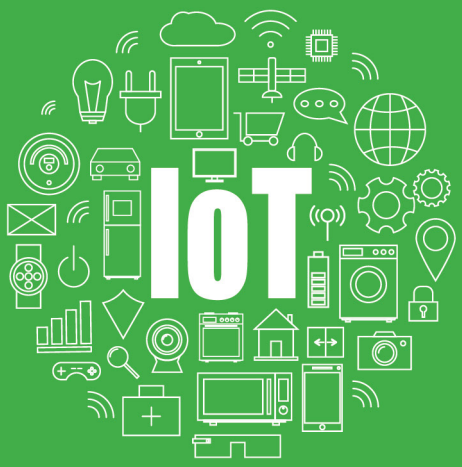
انتظار می‌رود سال جدید باج‌گیران سایبری ضمن خلق روش‌های انتشار جدید، اهداف خود را گسترده‌تر نموده و با تمرکز بیشتر بر روی دستگاه‌های با امنیت پایین‌تر، نظیر اینترنت اشیاء، همچنان بخش قابل توجهی از آلودگی‌ها را به این نوع از بدافزارهای مخرب اختصاص دهند. ضمن اینکه دور از انتظار نیست که روند افزایش تعداد و تنوع باج‌افزارها در جهان، در کشور خودمان نیز ادامه یافته و در سال جدید شاهد تعداد بیشتری از باج‌افزارهای ایرانی نیز باشیم.

بررسی و تحلیل

Dot Ransomware RaaS

اینترنت اشیاء
و افق‌های پیش روی آن در سال ۹۶

چندین سال است که کارشناسان در خصوص امنیت ضعیف وسایل و تجهیزات متصل به اینترنت، موسوم به اینترنت اشیاء هشدار داده‌اند. امنیت و پیکربندی آسیب‌پذیر این تجهیزات از یک سو و اتصال آنها به شبکه اینترنت از سویی دیگر، این دستگاه‌ها را به هدفی بسیار مناسب و در عین حال آسان برای مهاجمان سایبری تبدیل کرده است. یکی از اصلی‌ترین سوءاستفاده تبهکاران سایبری از این وسایل و تجهیزات، تسخیر نمودن آنها برای اجرای حملات "توزیع شده برای از کاراندازی سرویس" (DDoS) است. در جریان این حملات، لشکری از این تجهیزات هک شده 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 واقعی می‌شود. واقعیت آن است که دستگاه‌های موسوم به اینترنت اشیاء، 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. در سال ۹۵ شبکه مخرب Mirai در برخی از بزرگترین و مخرب‌ترین حملات توزیع شده برای از کاراندازی سرویس نقش داشت. در مهر ۹۵، یک شرکت فرانسوی ارائه دهنده خدمات میزبانی سرور بر روی بستر ابری به نام OVH از اجرای دو حمله توزیع‌شده برای از کاراندازی سرویس بر علیه تعدای از سرورهایی که توسط این شرکت میزبانی می‌شدند، خبر داد. این حملات در مجموع ۱ ترابیت بر ثانیه توان داشتند. منبع این حملات، بیش از ۱۴۵ هزار دستگاه ضبط تصویر دیجیتال و دوربین تحت شبکه بودند که هک شده و به تسخیر و تحت کنترل شبکه مخرب Mirai درآمده بودند. با در نظر گرفتن توان ایجاد ترافیک از ۱ تا ۳۰ مگابیت بر ثانیه توسط هر یک از دستگاه‌های این شبکه مخرب، گردانندگان آن عملاً قادر بودند که حملات از کاراندازی سرویس با توان ۱/۵ ترابیت بر ثانیه اجرا کنند. در حمله مشابه دیگر، سرورهای DNS شرکت Dyn هدف قرار گرفتند که در نتیجه آن، سرویس‌دهی سایت شرکت‌های بزرگی نظیر Pinterest، Twitter و PayPal دچار اختلال شد. در آبان ۹۵، شرکت Dyn، در بیانیه‌ای اعلام کرد که توسط میلیون‌ها دستگاه اینترنت اشیاء که تحت کنترل شبکه مخرب Mirai هستند، مورد حمله قرار گرفته است. متأسفانه سازندگان دستگاه‌ها و تجهیزات اینترنت اشیاء بندرت اقدام به عرضه اصلاحیه برای ترمیم ضعف‌های امنیتی دستگاه‌های ساخت خود بخصوص دستگاه‌های قدیمی‌تر می‌کنند. بسیاری از این دستگاه‌ها، هیچ مکانیزم امنیتی مناسبی در خود ندارند. کم نیستند سازندگانی که نه تنها استانداردهای امنیتی را طی مراحل برنامه‌نویسی در نظر نمی‌گیرند بلکه هیچ روالی نیز برای واکنش به رخدادها در زمان کشف ضعف‌های امنیتی در محصولات خود ندارند. ضمن اینکه بخش قابل توجهی از این دستگاه‌ها فاقد قابلیت به‌روزرسانی خودکار هستند و این خود می‌تواند مشکل را دو چندان کند. با توجه به امنیت ضعیف این دستگاه‌ها که عمدتاً در منازل و توسط کاربرانی که بسیاری از آنها تخصصی در حوزه امنیت IT ندارند مورد استفاده می‌گیرند انتظار می‌رود که سوءاستفاده مهاجمان از این تجهیزات همچنان ادامه یافته و حتی برخی مهاجمان از آنها برای رخنه به سیستم‌های منازل استفاده کنند. همچنین پیش‌بینی می‌شود بدافزارهای تحت سیستم عامل Linux ویژه این دستگاه‌ها نیز افزایش قابل توجهی داشته باشند.



دستگاه‌های همراه
خطرها و تهدیدها در سال جدید

این روزها دستگاه‌های همراه به گنجینه‌ای از اطلاعات با ارزش مبدل شده‌اند. از جمله، عرضه برنامک‌های بانکی و گسترش بانکداری الکترونیکی سبب شده تا بسیاری کاربران امور بانکی خود را از طریق این دستگاه‌ها مدیریت کنند.

متأسفانه سیستم‌های عامل و برنامه‌های نصب شده بر روی این دستگاه‌ها وضعیت امنیتی امیدوارکننده‌ای ندارند. سیستم عامل Android که بر اساس آمار شرکت Gartner، بیش از ۸۵ درصد از بازار سیستم‌های عامل گوشی‌های هوشمند و دستگاه‌های همراه را در اختیار دارد، به‌عنوان آسیب‌پذیرترین نرم‌افزار سال ۲۰۱۶ معرفی شده است.

در چند سال اخیر، علاوه بر افزایش چشمگیر بدافزارهای تحت سیستم عامل Android، چندین ابزار ساخت جاسوس‌افزار ویژه این سیستم عامل نیز در اختیار همگان قرار گرفته است. این ابزارها، تبهکاران حتی با دانش برنامه‌نویسی کم را نیز قادر به تزریق کد جاسوس‌افزار به برنامک‌های مجاز می‌کنند. با نصب برنامک در ظاهر مجاز - اما مخرب شده - بر روی دستگاه قربانی، مهاجم قادر خواهد بود پیامک‌ها و نشانی‌های تماس ثبت شده بر روی دستگاه را سرقت کند، تماس‌های قربانی را شنود کند، صدا را با استفاده از میکروفون دستگاه ضبط کند، دوربین دستگاه را در کنترل بگیرد و تماس‌های ناخواسته برقرار کند.

در اکثر مواقع روش انتشار برنامک‌های مخرب، به اشتراک‌گذاری آنها در سایت های توزیع برنامک و یا سایت‌های مخرب است.

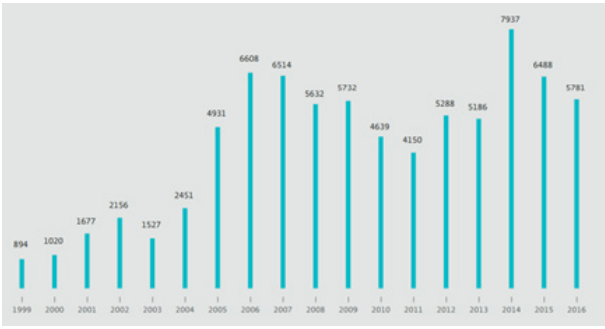
روش دیگر انتشار یک جاسوس‌افزار تحت سیستم عامل Android، نصب دستی آن بر روی دستگاه بدون اطلاع صاحب دستگاه است. حتی مواردی نیز مشاهده شده که یک دستگاه آلوده به این گونه بدافزارها به قربانی هدیه داده شده است.

پیش‌بینی می‌شود در سال آینده روند صعودی بدافزارهای ویژه دستگاه‌های همراه با اهداف جاسوسی و سرقت اطلاعات همچنان ادامه یابد.

همچنین استفاده گسترده تر از این دستگاه‌ها در محیط‌های کار و ورود به سامانه‌های سازمانی از این طریق، دستگاه‌های همراه را به درگاهی برای رخنه به سازمان‌ها مبدل خواهد کرد. بعلاوه، تبادل اطلاعاتی سازمانی در برنامک‌های پیام‌رسان غیر امن بر روی دستگاه‌های همراه، فرصت جدیدی برای سارقان سایبری جهت سرقت اطلاعات سازمانی فراهم خواهد کرد.

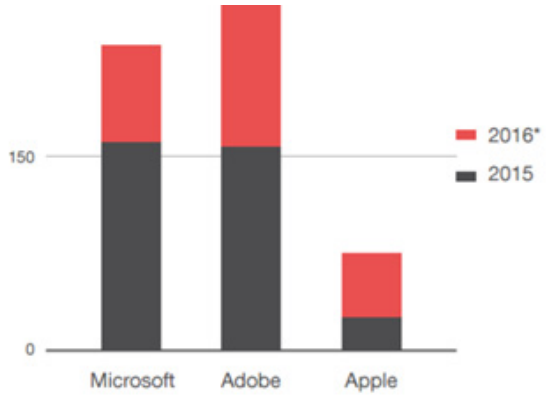
آسیب‌پذیری‌های امنیتی در سال ۹۶

یکی از روش‌های پیشرفته و البته مؤثر انتشار بدافزار و رخنه به سیستم، بهره‌جویی از آسیب‌پذیری‌های امنیتی سیستم‌عامل یا نرم‌افزارهای نصب شده بر روی دستگاه قربانی است. به برنامه مخربی که امکان سوءاستفاده مهاجم از آسیب‌پذیری را فراهم کند بهره‌جو (Exploit) گفته می‌شود. به آن آسیب‌پذیری امنیتی نیز که اصلاحیه‌ای برای آن عرضه نشده است ضعف امنیتی روز صفر (Zero-day) اطلاق می‌شود. سالهاست که برخی تبهکاران ابزارهایی موسوم به بسته بهره‌جو (Exploit Kit) را در بازارهای سیاه اینترنتی به فروش می‌رسانند. همانطور که از نام آن پیداست این ابزارها حاوی مجموعه‌ای از بهره‌جوها هستند. مهاجم با بکارگیری این ابزارها قادر است کد مخرب را بر روی دستگاه با سیستم عامل یا نرم‌افزار آسیب‌پذیر اجرا کند. راهکار مقابله با این نوع روش انتشار و رخنه، نصب تمام اصلاحیه‌های امنیتی عرضه شده از سوی شرکت سازنده نرم‌افزار است. موضوعی که متأسفانه توسط بسیاری از کاربران و حتی برخی مدیران شبکه نادیده گرفته می‌شود. هر چند در دو سال اخیر تعداد آسیب‌پذیری‌های امنیتی نسبتاً کاهش یافته اما این به معنای بهبود کامل وضعیت نیست. برای مثال یکی از آسیب‌پذیری‌های شناسایی شده در سال ۲۰۱۶ با شناسه CVE-2016-2060 میلیون‌ها دستگاه با سیستم عامل Android را تهدید می‌کند. یا در نمونه‌ای دیگر آسیب‌پذیری موسوم به DROWN و با شناسه CVE-2016-0800 در زمان کشف در اوایل سال ۲۰۱۶ در ۳۳ درصد سایت‌های مبتنی بر پودمان HTTPS شناسایی شده بود. در سال جدید نیز بسته‌های بهره‌جو یکی از ابزارهای انتشار بدافزارها و اجرای حملات مهاجمان حرفه‌ای خواهد بود. سواستفاده از ضعف‌های امنیتی روز صفر نیز همچنان روش رایج در تهدیدات پیشرفته و مستمر (Advanced Persistent Threat) خواهد بود.



تعداد ضعف‌های امنیتی شناسایی شده - منبع ESET

در سال ۲۰۱۶ تعداد آسیب‌پذیری‌های محصولات شرکت ادوبی از محصولات شرکت مایکروسافت پیشی گرفت. تعداد آسیب‌پذیری‌های شرکت اپل نیز چندان کم نبود. انتظار می‌رود در سال جدید نیز روند نزولی آسیب‌پذیری‌های محصولات مایکروسافت حفظ شود.



* تا سپتامبر ۲۰۱۶

سهم آسیب‌پذیری‌های شناسایی شده در محصولات سه شرکت مایکروسافت، ادوبی و اپل در سال های ۲۰۱۵ و ۲۰۱۶ - منبع: Trend Micro

همچنین افزایش استفاده کاربران از دستگاه‌های همراه احتمالاً سبب تمرکز بیشتر مهاجمان برای بهره‌جویی از آسیب‌پذیری‌های آنها و شناسایی ضعف‌های امنیتی روز صفر در آنها خواهد شد.

افزایش تهدیدات پیشرفته و مستمر و گسترش تسلیحات سایبری

تهدیدات پیشرفته و مستمر (Advanced Persistent Threat) به روش‌های پیچیده و پیشرفته سایبری برای بدست آوردن اطلاعات بطور مخفیانه و در طولانی مدت از فرد یا گروهی از افراد گفته می‌شود. گردانندگان این تهدیدات معمولاً گروه‌های حرفه‌ای نفوذگر و در بسیاری مواقع یک دولت یا حداقل گروهی با حمایت‌های دولتی هستند. همچنین رقابت بر سر ساخت و گسترش تسلحیات سایبری، بر خلاف تسلیحات پیشرفته دیگر، تنها محدود به کشورهای توسعه یافته نیست. حتی کشورهایی با منابع کمتر نیز قادرند موازنه قدرت را در دنیای سایبری بر هم بزنند. جنگهایی که در آنها موقعیت جغرافیایی، منابع طبیعی، مساحت و جمعیت کشور نقش پررنگی ندارند.

بسیاری از دولتها، تسلیحات سایبری را به عنوان ابزاری برای فعالیت‌های جاسوسی می‌دانند. اطلاع از آنچه کشورهای دوست و دشمن انجام می‌دهند، می تواند احتمال غافلگیر شدن یک دولت را کاهش دهد. در این کشورها، ساخت تسلیحات سایبری همچون بدافزارهای فوق پیچیده و همچنین طرحریزی حملات پیشرفته سایبری بخشی از پروژه امنیت ملی است.

در دنیای سایبری، فاصله میان توانایی‌های دولت‌ها و قابلیت‌های در اختیار کاربران عادی، هر روز بیشتر می‌شود. با بودجه‌های میلیارد دلاری و نیروهای متخصص، ارتش‌های سایبری به سرعت در حال تکامل هستند. به نحوی که می‌توان گفت دنیای سایبری بعد از زمین، آسمان، دریا و فضا پنجمین دامنه عملیاتی است.

حالا این سئوال پیش می‌آید که آیا دولت‌ها با آگاهی از این موضوع که این سلاح‌ها می‌توانند در اختیار افراد خرابکار و بر ضد افراد بی‌گناه و زیرساخت‌های اساسی قرار بگیرند، از آنها استفاده می‌کنند؟ این تصمیمی است که هر دولت با بررسی خطرات و عواقب احتمالی آن، اتخاذ می‌کند.

زمانی که دولتی اقدام به ساخت یک سلاح سایبری می‌کند، باید به فکر ساخت سیستمی برای مقابله با آن نیز باشد. باید در نظر بگیرد اگر سلاح، مهندسی معکوس شده و بر ضد سازنده و متحدانش استفاده شود، چه نتیجه‌ای خواهد داشت و چگونه باید به آن واکنش نشان داد؟

پیش‌بینی می‌شود در سال ۹۶ شاهد تهدیدات پیشرفته و مستمر بیشتر و استفاده گسترده‌تر از تسلیحات سایبری باشیم. ضمن اینکه سیستم‌های کنترل صنعتی (ICS) یکی از حساس‌ترین اهداف این تهدیدات خواهند بود. بر اساس گزارش شرکت FireEye، بیش از ۳۰ درصد آسیب‌پذیری‌های شناسایی شده در این سیستم‌ها ترمیم نشده‌اند.

بهبود
روش‌های شناسایی

نسل اول نرم‌افزارهای ضدویروس تنها قادر به کشف و پاکسازی ویروس‌هایی بودند که فرمول شناسایی آنها را در بانک اطلاعاتی خود داشتند. بنابراین باید حداقل یک دستگاه در سطح جهان به ویروس آلوده می‌شد تا کارشناسان شرکت ضدویروس قادر به شناسایی آن و اضافه کردن فرمول تشخیص ویروس جدید شوند.

با گذشت زمان ویروس‌نویسان نوع جدیدی از بدافزارها با عنوان چندریختی (Polymorphic) را خلق کردند. در این بدافزارها، درهم‌ساز (Hash) هر گونه با گونه دیگر آن ویروس متفاوت بود. اقدامی که روش شناسایی ضدویروس‌ها را بی‌اثر می‌کرد. از سوی دیگر، تعداد بدافزارهای جدید نیز روند بسیار صعودی داشته است. برای مثال بر اساس آمار شرکت امنیتی McAfee در هر ثانیه بیش از پنج بدافزار منحصر به فرد جدید در سطح جهان ظاهر و منتشر می‌شود.

در سال‌های اخیر شرکت‌های سازنده ضدویروس تلاش‌های فراوانی برای ارائه راهکارهای مبتنی بر هوش مصنوعی برای شناسایی خودکار بدافزارهای جدید کرده‌اند اما کاملاً مشخص است که بسیاری از بدافزارها موفق به دور زدن این فناوری‌ها می‌شوند.

با این حال انتظار می‌رود در سال جدید نیز همچنان اخبار امیدوارکننده‌ای از کارآمدتر شدن فناوری‌های شناسایی انواع تهدیدات داشته باشیم.

شبکه گستر

شرکت مهندسی شبکه گستر که در سال ۱۳۷۰ تأسیس گردیده، اولین شرکت ایرانی است که در زمینه نرم افزارهای ضدویروس فعالیت تخصصی و متمرکزی را آغاز کرد. در ابتدا، همکاری مشترکی بین شرکت مهندسی شبکه گستر و شرکت انگلیسی S & S International (تولید کننده ضد ویروس 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 محبوب ترین 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 بین المللی فعالیت خود را بر روی نرم افزارهای ضدویروس McAfee ادامه داد. در حال حاضر نیز شرکت شبکه گستر به عنوان فروشنده مجاز (Authorized Reseller) در منطقه خاورمیانه، به ارائه محصولات و خدمات درایران اقدام می نماید.

در سال ۱۳۸۴ شرکت مهندسی شبکه گستر موفق به کسب نمایندگی رسمی و انحصاری شرکت آلمانی Astaro، سازنده محصولات "مدیریت یکپارچه تهدیدات" (Unified Threat Management - UTM) 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 به عنوان نماینده شرکت Sophos ادامه فعالیت داده و اکنون محصولات Astaro سابق را تحت نام جدید Sophos و دیگر محصولات امنیت شبکه این شرکت را در ایران عرضه می نماید.

از سال ۱۳۹۱ نیز، شرکت مهندسی شبکه گستر عرضه محصولات ضد ویروس Bitdefender را به عنوان نماینده و توزیع کننده (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 است. ضد ویروس چابک‌تر، مدیریت آسان‌تر و محصولی مقرون به صرفه‌تر، انتظاراتی بودند که برخی کاربران و مدیران شبکه‌های کوچک و متوسط داشتند و 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 و طولانی مدت‌ترین پروژه‌های طراحی، نصب، راه اندازی و پشتیبانی محصولات نرم‌افزاری ضدویروس و سخت افزاری فایروال در کشور بوده است.

این شرکت علاوه بر خدمات دهی 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.


شبکه گستر

شرکت مهندسی شبکه گستر

تهران ۱۹۶۸۶، خیابان شهید دستگردی، شماره ۲۷۳

تلفن/دورنگار ۴۲۰۵۲ - ۰۲۱

تارنمای شرکت www.shabakeh.net

سامانه پشتیبانی help.shabakeh.net

خدمات پس از فروش my.shabakeh.net

مرکز آموزش events.shabakeh.net

اتاق خبر newsroom.shabakeh.net