سایبر

«اینترنت»، منطقه آزاد نظامی است

■ یوجین کسپرسکی، موسس و مدیرعامل شرکت کسپرسکی که سال‌هاست به فعالیت در زمینه تولید نرم‌افزارهای امنیت اطلاعات پرداخته، معتقد است که باید دولت‌ها به جنگ سایبری نگاه دیگری داشته باشند. در زمانی که دولت‌ها ده‌ها میلیارد پوند صرف مسلح کردن خود در مقابل جنگ‌های سایبری می‌کنند، او خطاب به مقامات دولت‌ها می‌گوید که به جای هزینه کردن در مقابل جنگ‌های سایبری باید اینترنت را به منطقه آزاد نظامی تبدیل کنند. او معتقد است: تقریبا تمامی زوایای زندگی ما در دنیای پیشرفته کنونی به کامپیوترهایی بستگی پیدا کرده‌اند که همگی به اینترنت متصلند و تمامی این کامپیوترها در مقابل حملات سایبری آسیب‌پذیرند. به طور مثال، استاکس‌نت برنامه هسته‌ای ایران را تهدید کرد. استاکس‌نت ویروسی بود که برای تخریب فیزیکی تجهیزات غنی‌سازی اورانیوم برنامه‌ریزی شده بود. کسپرسکی همچنین مدعی است که استاکس‌نت پیشرو نرم‌افزارهایی بود که می‌توانند حتی از طریق یک ای‌میل ساده خسارات واقعی و جبران‌ناپذیری وارد کنند و در حالی‌که جاسوسان از بهره‌برداری از اینترنت بسیار خشنودند، مقامات نظامی هنوز با این تصور دست به گریبانند که جاسوسان سایبری می‌توانند تمامی امور آنها را فلج کنند. به گفته یوجین کسپرسکی، همان‌طور که می‌توان با وضع قوانین بین‌المللی از افزایش سلاح‌های هسته‌ای در جهان جلوگیری کرد، می‌توان با وضع قوانین خاص نیز از کشمکش‌های همه‌جانبه سایبری اجتناب و قوانینی را برای توسعه سلاح‌های سایبری وضع کرد. او با اشاره مجدد به استاکس‌نت و اینکه این بدافزار برای سرقت پول یا فریب کاربران طراحی نشده بود، می‌گوید: این بدافزار برای ضربه واردکردن به زیرساخت صنعتی طراحی شده بود و با توجه به اینکه در سراسر جهان اغلب زیرساخت‌های حیاتی به اینترنت متصل هستند، باید نگران این موضوع بود. مدیرعامل شرکت کسپرسکی به وجه تهدیدآمیز دیگری از این موضوع نیز می‌پردازد. او با اشاره به اینکه اغلب برنامه‌ها و نرم‌افزارهایی که در صنایع پیچیده نظیر صنایع هسته‌ای استفاده می‌شوند، قدیمی و متعلق به ۱۰ تا ۲۰ سال قبل هستند، تاکید می‌کند: همین موضوع آسیب‌پذیری صنایع ما را به شدت بالا می‌برد. همه خوشحال هستند که زیرساخت‌ها یا پایگاه‌های داده‌ای خود را به اینترنت متصل کرده‌اند، اما کهنه‌بودن سیستم‌ها و تازه‌بودن تهدیدات اینترنتی، می‌تواند بروز یک فاجعه را رقم بزند. این کارشناس امنیت تکامل برنامه‌های مخرب تحت وب را به چند فاز تقسیم می‌کند و می‌گوید: در آغاز فقط جوانانی بودند که برای سرگرمی ویروس‌هایی را از طریق فلاپی دیسک‌های قدیمی، منتشر می‌کردند. سپس کرم‌های رایانه‌ای آمدند. این کرم‌ها از راه وب و بدون وارد آوردن خطرات زیاد منتقل می‌شدند. اما در فاز سوم تبهکاران سایبری برای کسب درآمد یا باج‌خواهی شروع به فعالیت کردند و در بسیاری از موارد براساس سفارش نیز کارهای تبهکارانه انجام دادند. او می‌افزاید اما امروزه فاز چهارم فعالیت‌های مخرب آغاز شده که ایجاد شبکه باتنت‌ها و ارتش زامبی‌ها از آن جمله‌اند. یعنی انجام فرماندهی از راه دور بر ارتشی از سیستم‌ها و شبکه‌ها و هدایت آنها به اهداف مشخص و برنامه‌ریزی‌شده. این ارتش‌ها می‌توانند با برنامه‌ریزی در مراکز حساس مستقر شوند و به انجام کارهایی از جمله جمع‌آوری اطلاعات، نهان شدن و انجام عملیات در زمان برنامه‌ریزی‌شده و هجوم یکباره و سراسری به هدف، بپردازند. یوجین کسپرسکی در مورد مرز میان آزادی و محدودیت در فضای وب می‌گوید، می‌توان این حالت را چیزی شبیه آنچه در فرودگاه‌ها اتفاق می‌افتد در نظر داشت. ممکن است در یک جا برای امنیت، محدودیت‌های بسیاری در آزادی ایجاد شود و در یک جا آزادی مطلق وجود داشته باشد. به این ترتیب یک کاربر می‌تواند انتخاب کند که در کدام محیط مجازی فعالیت کند. حتی معتقدم باید برای ورود به بخش‌هایی از اینترنت گذرنامه طراحی کرد و متناسب با آن یک پلیس بین‌المللی یا پلیس سایبری جهانی به وجود آورد. در حال حاضر تبهکاران سایبری در حالی‌که در مرزهای فیزیکی یک کشور قرار دارند، فعالیت‌های خود را در سطح بین‌المللی انجام می‌دهند. از دیگر سو و با توجه به آنچه گفته شد، می‌توان به رویکرد دولت‌ها در زمینه جنگ سایبری نیز نگاه کرد. باراک اوباما چندی پیش حمله به زیرساخت‌های سایبری ایالات متحده را معادل حمله نظامی برشمرد و اعلام کرد که حمله سایبری می‌تواند واکنش نظامی آمریکا را در پی داشته باشد. در همین زمینه پیرو حمله و کشف بدافزار فلیم، معاون نخست‌وزیر رژیم صهیونیستی این حمله را منطقی خواند و در اظهاراتی بیان کرد برای هر کسی که تهدید ایران را قابل توجه می‌داند، منطقی است گام‌های مختلفی از حمله سایبری را بردارد تا به ایران صدمه بزند. رویکرد جهانی به این موضوع را می‌توان در هشدار اخیر سازمان ملل نیز دریافت. پیرو آسیب دیدن کشورهای خاورمیانه از حمله بدافزار فلیم (شعله آتش)، هماهنگ‌کننده امنیت سایبری در اتحادیه بین‌المللی ارتباطات دوربرد (ITU) وابسته به سازمان ملل مستقر در ژنو گفت: این هشدار محرمانه برای کشورهای عضو روشن خواهد کرد که بدافزار «فلیم» یک ابزار خرابکاری خطرناک است که بالقوه می‌تواند برای حمله به زیربنای حیاتی کشورها مورد استفاده قرار گیرد و کشورهای عضو باید در این‌باره هشیار باشند.

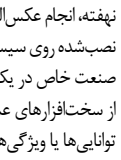
آیا «استاکس‌نت» قوی‌ترین «بدافزار» تاریخ است؟

ویروسی که جاسوس شد

شرق: کرم Stuxnet _ استاکس‌نت _ بدافزاری است که چنان در استفاده از آسیب‌پذیری‌های اصلاح‌نشده ماهر است و چنان در کار خود پیچیده عمل می‌کند که آن دسته از متخصصان امنیتی که در مورد آن تحقیق کرده‌اند، معتقدند که ممکن است این بدافزار کار متخصصانی با پشتوانه قوی باشد. این بدافزار همزمان چهار نقص امنیتی اصلاح‌نشده ویندوز را مورد سوءاستفاده قرار می‌دهد که سوءاستفاده از این تعداد آسیب‌پذیری برای یک بدافزار بسیار زیاد است. استاکس‌نت که نخستین بار در اواسط جولای توسط شرکت کوچک امنیتی VirusBlokAda در بلاروس گزارش شد، یک ماه بعد زمانی که مایکروسافت تایید کرد که این کرم در حال هدف قرار دادن سیستم‌های ویندوز در مدیریت سیستم‌های کنترل صنعتی بزرگ است، به شهرت رسید. این سیستم‌های کنترلی اغلب با عنوان SCADA (Supervisory Control And Data Acquisition) شناخته می‌شوند. این سیستم‌ها هر چیزی را، از سایت‌های نیروگاهی گرفته تا خطوط انتقال نفت، کنترل می‌کنند. محققان ابتدا اعتقاد داشتند که Stuxnet صرفا از یک آسیب‌پذیری اصلاح‌نشده در ویندوز سوءاستفاده کرده و از طریق درایوهای USB منتشر می‌شود. به گفته محققان سایمانتک، ایران جدی‌ترین هدف این کرم بوده و در ماه جولای نزدیک به ۶۰ درصد از تمامی سیستم‌های آلوده، در ایران قرار داشتند. در روز دوم آگوست، مایکروسافت یک به‌روزرسانی فوری برای اصلاح این نقص عرضه کرد. در این زمان Stuxnet به عنوان کرم سوءاستفاده‌کننده از میان‌برهای ویندوز شناخته می‌شد. اما برخلاف انتظار مایکروسافت، Stuxnet می‌توانست همزمان از چهار آسیب‌پذیری برای دسترسی به شبکه‌های شرکت‌ها استفاده کند. به گفته محققان، پیش از این دیده نشده است که یک بدافزار به طور همزمان از چهار آسیب‌پذیری اصلاح‌نشده استفاده کند. زمانی که این کرم به یک شبکه دسترسی پیدا می‌کند، به دنبال کامپیوترهای خاصی می‌گردد که سیستم‌های SCADA را که توسط نرم‌افزاری از شرکت زیمنس کنترل می‌شوند، مدیریت می‌کنند. محققان - Kaspersky و سایمانتک با در دست داشتن نمونه‌ای از - Stuxnet، کد این بدافزار را مورد بررسی و تحلیل عمیق قرار دادند تا به اطلاعات بیشتری در مورد آن دست پیدا کنند. این دو شرکت به طور جداگانه کد حمله‌ای را که سه آسیب‌پذیری اصلاح‌نشده دیگر ویندوز را هدف قرار داده بود، پیدا کردند. به گفته یکی از محققان Kaspersky، نخست ظرف مدت یک هفته تا یک هفته و نیم، حفره print spooler توسط محققان این شرکت پیدا شد. سپس حفره EoP (تغییر حق دسترسی) ویندوز نیز توسط این شرکت امنیتی کشف شد. پس از آن حفره دوم EoP نیز توسط محققان مایکروسافت پیدا شد. محققان سایمانتک نیز به طور جداگانه آسیب‌پذیری print spooler و دو آسیب‌پذیری EoP را در ماه آگوست پیدا کردند. هر دو شرکت نتایج فعالیت‌های خود را به مایکروسافت گزارش کردند که باعث شد آسیب‌پذیری print spooler به سرعت اصلاح شده و وعده اصلاح دو آسیب‌پذیری کم‌خطرتر EoP در به‌روزرسانی امنیتی بعدی نیز داده شود. اما عجایب - Stu net به اینجا ختم نمی‌شود. این کرم همچنین از یک حفره ویندوز که در سال ۲۰۰۸ توسط به روزرسانی MS08-067 اصلاح شده بود نیز استفاده می‌کند. این نقص امنیتی همان آسیب‌پذیری مورد استفاده کرم Conficker در اواخر سال ۲۰۰۸ و اوایل سال ۲۰۰۹ بود که به میلیون‌ها سیستم در سراسر جهان آسیب وارد کرد. زمانی که Stuxnet از طریق USB وارد یک شبکه می‌شود، با استفاده از آسیب‌پذیری‌های EoP حق دسترسی admin به سایر PCها را برای خود ایجاد می‌کند، سیستم‌هایی را که برنامه‌های مدیریت WinCC و PCS 7 SCADA اجرا می‌کنند پیدا می‌کند، کنترل آنها را با سوءاستفاده از یکی از آسیب‌پذیری‌های print spooler یا MS08-067 در اختیار می‌گیرد و سپس کلمه عبور پیش‌فرض زیمنس را برای در اختیار گرفتن نرم‌افزار SCADA آزمایش می‌کند. سپس مهاجمان می‌توانند نرم‌افزار programmable logic control (PLC) را مجددا برنامه‌ریزی تا دستورات جدید را مطابق میل خود صادر کنند. نکته قابل توجه این است که این کد حمله معتبر و قانونی به نظر می‌رسد، چرا که افرادی که پشت Stuxnet قرار دارند، حداقل دو گواهی دیجیتالی امضاشده را سرقت کرده‌اند. به گفته محقق شرکت امنیتی Kaspersky، سازماندهی و پیچیدگی اجرای کل بسته بسیار قابل توجه است. به عقیده وی، هر کسی که پشت این بدافزار قرار دارد، قصد دارد به تمام دارایی‌های شرکت یا شرکت‌های هدف خود دست یابد. یک محقق امنیتی دیگر نیز معتقد است که تیمی متشکل از افرادی با انواع تخصص‌ها و پیش‌زمینه‌ها از Rootkit گرفته تا پایگاه داده، این بدافزار را ایجاد کرده و هدایت می‌کنند. این بدافزار که تقریبا نیم‌مگابایت حجم دارد، به چندین زبان از جمله C، C++ و سایر زبان‌های شیءگرا نوشته شده است. به گفته وی، تیم ایجادکننده این بدافزار نیاز به سخت‌افزار فیزیکی واقعی برای تست داشته‌اند و به خوبی می‌دانند که یک کارخانه خاص چگونه کار می‌کند. بنابراین ایجاد و استفاده از این بدافزار قطعا یک پروژه بزرگ بوده است. یک راه که این مهاجمان با استفاده از آن ریسک شناسایی شدن را کم کرده‌اند، قرار دادن یک شمارنده در USB آلوده است که اجازه انتشار بدافزار از طریق یک USB خاص به بیش از سه کامپیوتر را نمی‌دهد. این به آن معناست که مهاجمان سعی کرده‌اند با جلوگیری از گسترش بیش از اندازه این بدافزار، آن را در سازمان هدف خود نگه داشته و به این ترتیب از شناسایی آن جلوگیری کنند. زمانی که این بدافزار وارد شبکه یک شرکت می‌شود، فقط در صورتی از آسیب‌پذیری MS08-067 استفاده می‌کند که بداند هدف، بخشی از یک شبکه SCADA است. در اغلب شبکه‌های SCADA هیچ‌گونه عملیات ثبت (logging) انجام نمی‌شود و این شبکه‌ها دارای امنیت محدود بوده و به ندرت اصلاحیه‌ای در مورد آنها منتشر می‌شود. همین مساله باعث می‌شود که سوءاستفاده از آسیب‌پذیری MS08-067 که مدت‌هاست اصلاح شده است، برای این کار موثر و مفید باشد. تمام این مسایل، تصویری ترسناک از Stuxnet می‌سازد. محققان سایمانتک و Kaspersky معتقدند که با توجه به شناسایی کاملی که این کرم انجام می‌دهد و پیچیدگی کار آن و خطرناک بودن حمله آن، این بدافزار حتی نمی‌تواند صرفا کار یک گروه حرفه‌ای جنایتکار سایبری باشد. محقق امنیتی شرکت سایمانتک معتقد است که این به هیچ عنوان نمی‌تواند کار یک گروه خصوصی باشد چرا که مهاجمان صرفا به دنبال اطلاعات برای حذف رقیب نبوده‌اند. آنها قصد داشته‌اند PLCها را مجددا برنامه‌ریزی کرده و کار سیستم‌ها را به چیزی غیر از آنچه که صاحبان آنها می‌خواهند، تغییر دهند که این چیزی بیش از جاسوسی صنعتی است. به گفته وی، منابع و هزینه مورد نیاز برای این حمله، آن را خارج از قلمرو یک گروه هک خصوصی قرار می‌دهد. این حمله به طور خاص ایران را هدف گرفته بود. محقق امنیتی Kaspersky معتقد است که با در نظر گرفتن تمامی این شرایط، محتمل‌ترین سناریو در مورد این بدافزار، یک گروه هک وابسته به سرویس‌های جاسوسی حکومتی یک کشور است. به گفته محقق امنیتی سایمانتک، این یک پروژه بسیار مهم برای افرادی است که در پشت آن قرار دارند که هزینه‌ها و ریسک بالایی نیز داشته است. همچنین اگرچه زیمنس ادعا می‌کند که ۱۴ سایت آلوده به Stuxnet که توسط این شرکت کشف شده‌اند، توسط این بدافزار خراب نشده یا تحت تاثیر آن قرار نگرفته‌اند، اما محققان امنیتی سایمانتک و - Kaspersky در این‌باره مطمئن نیستند. متخصصان در مورد زمان آغاز به کار این بدافزار اتفاق نظر ندارند. Kaspersky آغاز فعالیت این بدافزار را در جولای ۲۰۰۹ می‌داند، در حالی که سایمانتک معتقد است که شروع این حملات به ژانویه ۲۰۱۰ برمی‌گردد. اما همگی معتقدند که این کرم ماه‌ها بدون شناسایی شدن به کار خود ادامه داده است. این محققان فکر می‌کنند که این بدافزار توانسته باشد پیش از شناسایی شدن، به اهداف خود برسد.

یادداشت

«شعله آتش» به ما چه می‌گوید



علیرضا صالحی
دبیر کمیسیون افتای نصر

■ بروز یک حمله سایبری به وسعت و پیچیدگی استاکس‌نت در سال ۲۰۱۰، کارشناسان را با مفهوم واقعی جنگ سایبری آشنا کرد. جنگی که در آن زیرساخت‌های داده‌ای و در مفهومی وسیع‌تر، زیرساخت‌های سایبری یک کشور مورد هجوم قرار می‌گیرند و در آن همانند جنگ‌های کلاسیک، ابتدا جمع‌آوری داده‌های حیاتی مورد نیاز و سپس ضربه زدن به اهداف مورد نظر انجام می‌گیرد. استاکس‌نت با خود مفهوم جنگ سایبری را در سطحی عمومی مطرح و اکنون، نسل بعدی آن یعنی فلیم (شعله آتش) مفهومی دیگر تحت عنوان سلاح سایبری را معرفی می‌کند. اگر نگاهی به اظهارنظرهای کارشناسان و متخصصان امنیت طی دو سال گذشته و به ویژه با شیوع بدافزار استاکس‌نت داشته باشیم، در می‌یابیم که همگان کم‌وبیش در مورد جنگ‌های سایبری آینده هشدار داده‌اند. بروز حمله سایبری به وزارت نفت که به آشکارسازی بدافزار فلیم انجامید، ما را با این حقیقت روبه‌رو ساخت که جنگ سایبری را دیگر نه تنها به عنوان یک احتمال که به عنوان واقعیتی عینی باید پذیرفت. سرمایه‌گذاری دولتی، پیچیدگی فوق‌العاده بالا، هوشمندی در طراحی و روش تکثیر، تنوع عملکرد، ثبت هرگونه فعالیت کاربران، آنالیز ترافیک شبکه، بسترسازی برای فعالیت‌های مخرب آتی، ایجاد سکوی توسعه بدافزارهای آتی، قرار گرفتن در حالت نهفته، انجام عکس‌العمل متناسب با نوع آنتی‌ویروس نصب‌شده روی سیستم، هدف قراردادن یک کشور یا یک صنعت خاص در یک کشور خاص، تخریب نوع یا انواعی از سخت‌افزارهای عمومی یا خاص و... تنها نمونه‌هایی از توانایی‌ها یا ویژگی‌های بدافزار فلیم است. بدافزاری که از آن به عنوان جعبه ابزار بدافزاری یا یک سلاح واقعی سایبری نام برده می‌شود. خوشبختانه تجربه استاکس‌نت، سبب شد که مرکزی مانند ماهر که وظیفه پایش فضای سایبری و شناخت آسیب‌های آن را برعهده دارد، به خوبی وارد عمل شود و با تحلیل اطلاعات موجود و در زمان نسبتا مناسب، نسبت به این رخداد واکنش نشان دهد. اما این رخداد ابعاد نگران‌کننده دیگری را نیز در بردارد. شروع نامشخص فعالیت این بدافزار که بین دو تا هشت سال قبل تخمین زده می‌شود، ما را مطمئن می‌کند که این بدافزار، اولین و آخرین این سلاح‌ها نبوده و نخواهد بود. پیچیدگی ابعاد طراحی این سلاح سایبری که به بیان ساده صدبرابر بیشتر از یک بدافزار متعارف و ۲۰ برابر بیش از استاکس‌نت بوده است، این پیام را می‌رساند که باید منتظر سلاح‌هایی با تخریب بسیار بیشتر و تنوع عملکرد و گستردگی وسیع‌تر باشیم. ضمنا با توجه به اینکه سلاح سایبری کشف شده (فلیم) مربوط به تکنیک‌های طراحی چند سال قبل است، پیشرفت تکنیک‌های تولید بدافزارهای حال حاضر و آتی دور از انتظار نخواهد بود. حال با توجه به آنچه گفته شد، آیا تصور گزافی است که کشورمان را در شرایط جنگ سایبری فرض کنیم؟

امنیت

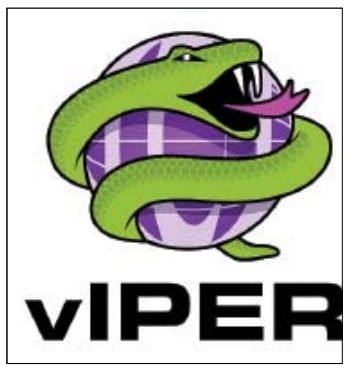
حلقه مفقود زنجیره تامین امنیت «سایبر»

میلاد امیریان‌فر

■ تدوین استراتژی و اجرای آن یا مدیریت استراتژیک همه واژگانی است که بسیاری از مدیران ارشد و البته فرماندهان نظامی کشور با آن آشنایی دارند اما باید به این مساله توجه کرد که مدیریت استراتژیک در مساله تامین امنیت فضای سایبر ماهیتی بسیار پویا و متغیر دارد که شاید با تعاریف رایج از موضوع مدیریت استراتژیک تا حد قابل توجهی فاصله داشته باشد. شاید گفتن این جمله که با یک ویروس ۱۵ کیلوبایتی رایانه‌ای می‌توانید هزاران بمب اتمی را کنترل کنید ولی همین هزاران بمب اتمی به هیچ عنوان نمی‌توانند این ویروس ۱۵ کیلوبایتی را از بین ببرند، خود به خوبی بیانگر ماهیت متفاوت تهدیدات سایبری است. بنابراین با توجه به موارد گفته‌شده بدیهی است که تامین امنیت در فضای سایبر در واقع مرهون یک زنجیره بسیار گسترده و کلیدی و بعضا پیچیده است که تعاریف و مشخصات خاص خود را دارد و هیچ شباهتی با سایر تهدیدات امنیتی ندارد و به سبب پویایی و ماهیت دایما در حال تغییر آن وجود ضعف در هر حلقه بلافاصله منجر به شکست و متلاشی شدن آن می‌شود. اهمیت تامین امنیت فضای سایبر با نگاه استراتژیک امروز بیش از هر روز دیگری برای دفاع از مرزهای مجازی و واقعی کشور خودنمایی می‌کند. در همین خصوص پیرامون مولفه‌های این زنجیره استراتژیک بسیار صحبت شده است اما تا به حال در مورد مدیریت این مولفه‌ها با استفاده از یک تصویر کلی شاید کمتر سخن به میان آمده است. به نظر می‌رسد تسریع در بهینه‌سازی مراکز SOC: Security Operation Center در معاونت فناوری اطلاعات همه سازمان‌ها و ارگان‌ها با دید مدیریت استراتژیک یکی از مواردی باشد که با توجه به اتفاقات اخیر باید بیشتر مد نظر مدیران این بخش‌ها قرار بگیرد. بهینه‌سازی همان‌طور که اشاره شد با توجه به ماهیت بسیار پویا و متغیر محیط سایبر باید خارج از چارچوب برنامه‌های جامع سازمانی ادامه یابد، شاید تدوین برنامه‌های غلتان Rolling Planning راهکار مناسبی برای تامین امنیت حال حاضر زیرساخت‌های سایبری و غیرسایبری کشور با توجه به تهدیدات جاری باشد.

شک و تردیدها در مورد حضور ویروس اقتصاد کشور

«وایپر» جایگزین استاکس‌نت می‌شود؟



آرام حامدی: باگذشت بیش از یک ماه از بروز اختلال‌های عملیاتی در وزارت نفت، هنوز هیچ‌کسی به واقع نمی‌داند که عامل اصلی این اختلال‌ها چه بوده است. همچنین هیچ‌گونه مستندات فنی، حتی برای کارشناسان و دست‌اندرکاران امنیت فناوری اطلاعات در کشور منتشر نشده است. اما با این حال، طبق تایید مسوولان وزارت نفت، عامل اصلی بروز مشکلات فعلی در این وزارتخانه، نفوذ یک ویروس رایانه‌ای موسوم به «وایپر» در شبکه داخلی این مرکز بزرگ سازمانی اعلام شده است. در ابتدا وجود این ویروس به علت فعالیت‌های تخریبی که برای آن بیان شد (مانند سوزاندن مادربورد یا پاک‌کردن غیرقابل بازگشت هارددیسک در محیط ویندوز) توسط بسیاری از کارشناسان مورد تایید قرار نگرفت اما تحقیقات فنی تازه‌ای که توسط شرکت ایمن رایانه، نماینده رسمی و انحصاری شرکت امنیتی Panda Security در ایران انجام شده، نشان می‌دهد که نفوذ ویروس «وایپر» یا دست‌کم نفوذ ویروس دیگری با عملکردهای کاملا شبیه به «وایپر» به برخی مراکز سازمانی کشور امکان‌پذیر بوده است. جالب اینجاست که طیفی از سازمان‌های تابعه وزارت نفت ایران که به نرم‌افزارها یا سخت‌افزارهای امنیتی شرکت Panda Security یا برخی دیگر از نرم‌افزارهای ضدویروس مجهز بوده‌اند، با اختلال‌های ناشی از ویروس وایپر مواجه نشده‌اند. براساس گزارش‌های تاییدشده، تنها بخش‌هایی از این وزارتخانه آلوده شده‌اند که از «یک نوع خاص از برنامه‌های ضدویروس» استفاده می‌کرده‌اند... به همین دلیل شایبه وجود حفره‌های امنیتی اصلاح‌نشده در این نوع ضدویروس که اخیرا (در اواخر اسفندماه ۱۳۹۰) در رسانه‌های معتبر جهان منتشر شده بود، قوت بیشتری یافته سست. از طرف دیگر، نشریه معتبر - Virus Bu letin در شماره اکتبر ۲۰۱۱ (آبان ۱۳۹۰) خود از پراکندگی نسبتا وسیع یک ویروس عجیب و غریب تنها در کشور «کوبا» خبر داد. جالب اینکه هیچ کدام از ضدویروس‌ها به جز یکی، که اتفاقا همان ضدویروس مذکور در پاراگراف قبل است، حملات «موفقیت‌آمیز» این ویروس را تایید یا منتشر نکرده‌اند! روند گزارش‌دهی نیز به نحوی است که گویا فقط کامپیوترهای مجهز به همین ضدویروس به صورت هدفدار مورد حمله واقع شده‌اند. این ویروس که در آن زمان، W32/VRBAT نامگذاری شد، تنها در عرض چند روز، هزاران هارددیسک را فقط در محدوده کشور کوبا از کار انداخت و سپس به طور ناگهانی کاملا محو شد! در این میان پرسش‌های متفاوتی درخصوص حضور این ویروس رایانه‌ای مطرح شد از جمله آنکه آیا شبکه اصلی وزارت نفت، توسط حمله یک بدافزار رایانه‌ای فوق‌العاده خطرناک با عنوان وایپر آلوده شده؟ آیا این وزارتخانه از درون و توسط یک حمله عامدانه توسط یک عامل انسانی روبه‌رو بوده است؟ آیا نفوذگران، از طریق اینترنت و با استفاده از حملات هدفدار یا ابزار هک موفق به نفوذ به درون شبکه وزارت نفت شده‌اند؟ آیا سرور اتوماسیون اداری یا سرورهای اینترنت ادارات و مراکز زیرمجموعه این وزارتخانه در اثر یک اشتباه کوچک عملیاتی با اختلال گسترده مواجه شده‌اند؟ آیا مهاجمان از طریق دسترسی به سرور میزبان اطلاعات وب‌سایت‌های این وزارت توانسته‌اند راه نفوذ به درون شبکه عریض و طویل وزارت نفت را پیدا کنند یا ده‌ها سوال دیگر که هرکدام می‌توانند پاسخی باشند برای اختلالات گسترده در ارتباطات درون و برون‌سازمانی مهم‌ترین وزارتخانه اقتصادی کشور. اما نکته اینجاست که طیفی از سازمان‌های تابعه وزارت نفت ایران که به نرم‌افزارها یا سخت‌افزارهای امنیتی شرکت Panda Security یا برخی دیگر از نرم‌افزارهای ضدویروس مجهز بوده‌اند، با اختلال‌های ناشی از ویروس وایپر مواجه نشده‌اند. آیا حفره‌های امنیتی جدیدی که در این نوع ضدویروس کشف و در تاریخ ۲۷ اسفند ۱۳۹۰ در برخی از رسانه‌ها منتشر شده، می‌توانسته در نفوذ این ویروس به درون سرورها و رایانه‌های سازمانی و نیز رایانه‌های خانگی موثر بوده باشد؟ آیا ویروس VRBAT تنها برای ضربه زدن به یک یا چند برند خاص ضدویروس طراحی، تولید و منتشر شده است؟ با کنار هم نهادن تمام گزینه‌های بالا می‌توان فرضیه بسیار قدرتمندتری را نتیجه گرفت: حمله صورت‌گرفته در کشور کوبا را می‌شود نوعی تمرین و آزمایش (بخوانید رزمایش) برای حمله یا حملات بعدی به اهداف مهم و استراتژیک کشورهای دیگر جهان از جمله ایران در نظر گرفت.

همه چیز در مورد «وایپر»

ویروسی که برای حمله به ایران طراحی شد

محمدمهدی واعظی‌نژاد: بهتر است یادآوری شود که ویروس Viper هیچ ارتباطی با ویروس Wipe که از تهدیدات امنیتی سال گذشته به شمار می‌رود، نداشته و اشتباهاتی که در این خصوص مطرح می‌شود، به دلیل نداشتن دانش و تخصص فنی و همچنین شباهت نزدیک اسمی آنها به یکدیگر است. Viper فقط برای حمله سایبری به جمهوری اسلامی ایران، طراحی و منتشر شده است. هدف اصلی این نرم‌افزار مخرب، تاسیسات زیربنایی ایران است که با توجه به شواهدی که از حمله و نفوذ آن به وزارتخانه‌ها و سازمان‌های مهم کشورمان موجود است، این فرضیه قوت بیشتری می‌گیرد. گفتنی است که تاکنون به جز ایران، هیچ گزارشی از فعالیت‌های مخرب این ویروس در سایر کشورها گزارش نشده است. Viper در اصطلاح لغوی به معنای «آدم خائن و بدنهاد» است که از همین نام نیز برای نفوذ در رایانه‌ها استفاده می‌کند.

طراحی و سازماندهی

این ویروس، به چندین زبان مختلف از جمله C، C++ و سایر زبان‌های شیءگرا نوشته شده است. Viper، چنان در نفوذ به سیستم‌ها، حتی با عبور از فایروال‌های قدرتمند و با تنظیمات صحیح و پیچیده همچون ISA ماهر است که به طور یقین، متخصصانی با پشتوانه فنی قوی و دارای انواع تخصص‌ها، آن را ایجاد کرده و هدایت می‌کنند. با توجه به شناسایی کاملی که این ویروس انجام می‌دهد، پیچیدگی کد، خطرناک بودن حمله آن، نفوذ به مراکز خاص و همچنین منابع و هزینه‌های مورد نیاز برای انجام این حمله به همراه ریسک بالایی که پروژه در پی داشته است، تنها دولت ملی می‌تواند توانایی‌های آن را داشته باشد.

تغییرات در سیستم

هنوز از فایل‌ها و سرویس‌هایی که توسط این ویروس در سیستم آلوده ایجاد می‌شود، اطلاعاتی در دست نیست و همچنین مشخص نیست که چه تغییراتی در Registry ویندوز به وجود می‌آید اما همان‌طور که اشاره شد، تمامی فایل‌ها از روی هارددیسک حذف شده و چنانچه فایلی نیز باقی بماند از هر نوع فرمت نوشتاری همچون doc, docx, pdf, xls و... و حتی فرمت‌های تصویری، پس از باز شدن فایل مربوطه، تمامی اطلاعات آن یکباره پاک می‌شود. اگرچه ممکن است هیچ تغییری در حجم فایل‌ها ایجاد نشود و در ظاهر، فایل‌ها دارای محتویات باشند، اما در اصل، فاقد هرگونه اطلاعاتی بوده و اطلاعات آنها نیز غیرقابل بازیابی است. در ضمن، هنوز مدارکی در دست نیست که این ویروس، اطلاعاتی را از طریق HTTP به آدرس‌های مشخصی که سرورهای آن هستند، ارسال می‌کند یا خیر. با این تفاسیر، حذف تمامی فایل‌ها، حتی فایل‌های سیستمی سیستم عامل، از مهم‌ترین مشخصه‌های این ویروس محسوب می‌شود.

جلوگیری

هم‌اکنون، هیچ‌یک از آنتی‌ویروس‌ها نیز قادر به شناسایی و پاک‌سازی این ویروس نیستند. با این وجود، انجام فعالیت‌های زیر توسط همه مدیران و کاربران سیستم می‌تواند باعث جلوگیری یا کاهش خطر این ویروس شود:

• غیر فعال کردن ویژگی AutoRun یا AutoPlay سیستم برای جلوگیری از اجرای خودکار فایل‌های قابل اجرا در درایوهای قابل جابه‌جایی

• تهیه نسخه‌های پشتیبان از داده‌ها و اطلاعات، به صورت مرتب و در فاصله‌های زمانی کم و مشخص و نگهداری آنها روی یک سیستم دیگر، جدا از شبکه

• غیرفعال کردن درایوهای قابل جابه‌جایی و تمامی درایورها (Floppy , CD , DVD) از طریق Setup سیستم و در نظر گرفتن یک رمز عبور قوی برای setup

اصلاح نقاط آسیب‌پذیر نرم‌افزارهای نصب‌شده در سیستم

•به‌روزرسانی سیستم عامل و نصب آخرین وصله‌های امنیتی روی آن

• به روزرسانی نرم‌افزار آنتی‌ویروس در فاصله‌های زمانی کوتاه‌مدت و فعال کردن گزینه automatic updates برای دریافت خودکار آخرین updateها

محدود کردن شدید دسترسی به آدرس‌های اینترنتی، با استفاده از فایروال و Router تا زمان برطرف شدن خطر و رفع تهدید

• استفاده از رمز عبور پیچیده که ترکیبی از عدد، حروف بزرگ و کوچک و نمادهاست برای کلمه عبور کاربران، به نحوی که این رمزها توسط dictionary attackها به راحتی قابل شناسایی و کشف نبوده و در عین حال، برای کاربران هم به‌یادماندنی باشد.

• همه ارتباطات ورودی از اینترنت به سرویس‌های سازمان را که نباید در دسترس عموم باشد، با استفاده از فایروال deny کرده و تنها به سرویس‌هایی اجازه دهید که به مردم خدمات ارایه می‌دهند.

هرگز نباید با یوزر administrator به سیستم login کرد. کاربران و برنامه‌ها هم باید پایین‌ترین سطح دسترسی لازم را داشته باشند.