دیدگاه

آنها ایران را میدان نبرد کرده اند

حامد شفیعی

■ رادیو ان‌پی‌آر در گزارشی با عنوان «آیا ایران می‌تواند جنگی سایبری علیه ایالات متحده راه اندازد؟» نوشت: کارشناسان امنیت سایبری بر این باورند که ایران منابع لازم برای تبدیل شدن به بازیگری اصلی در عرصه نبرد سایبری را در اختیار دارد. جفری کار، کارشناس نزاع سایبری (cyberconflict) و مشاور وزارت دفاع ایالات متحده در این زمینه می‌گوید: ایران منابع و توانمندی‌های لازم برای تبدیل شدن به بازیگری اصلی در عرصه نبرد سایبری را در اختیار دارد. شاید همه این اظهارنظرها موجب شده تا طی دو_سه سال اخیر ایران شاهد تهدیدات سایبری باشد. تهدیدهایی که خود را در پشت نام‌هایی همچون استاکس‌نت، دوکو، وایپر و شعله آتش مخفی کرده است. تمامی این اسامی سوار بر کدهای صفر و یکی هستند که هدف‌شان تخریب سیستم‌های اطلاعاتی و به سرقت بردن اطلاعات سیاسی و اقتصادی کشور است. روزی با عنوان استاکس‌نت به صنایع کشور حمله کرده و فناوری هسته‌ای را مورد تهدید قرار می‌دهند و روزی با دوکو برادر ناتنی زنگ خطر را به صدا درمی‌آورند.

روزی نیز با وایپر در صدد ایجاد اختلال در سیستم اقتصادی کشور برمی‌آیند و هدف تحریم نفتی را به وسیله این ویروس دنبال می‌کنند. حال هم که صحبت از شعله‌ای می‌کنند که از دو سال قبل فعالیت خود را برای تخریب اطلاعات کشور شروع کرده است. این نخستین باری نبود که صنایع استراتژیک ایران در معرض تهدیدات سایبری خارجی قرار می‌گرفت. کارشناسان معتقدند این اختلالات محصول سیاست‌های برخی دولت‌ها برای هدف قرار دادن سیستم‌های استراتژی ایران است. آنها این حملات را این‌گونه دسته‌بندی می‌کنند: مورد اول از این نوع حملات شیوع بدافزار استاکس‌نت در سال ۲۰۰۹ و ۲۰۱۰ بود. مورد دوم ویروس یا بدافزار دوکو بود که در یکی از شبکه‌های کامپیوتری موجود در اروپا کشف شد. به همین خاطر احتمال می‌رود که وایپر نیز یک بدافزار مشابه یا نمونه تغییریافته‌ای از بدافزار دوکو باشد که این بار شبکه ارتباطی صنایع نفت ایران را هدف گرفته است. مورد سوم ویروس رایانه‌ای موسوم به استارز بود؛ ویروسی که در ماه آوریل سال ۲۰۱۱ وجود آن در ایران گزارش و از سوی نهادهای امنیت سایبری کشور مهار شد. این بار نیز از بدافزاری به نام وایپر سخن به میان آمده است؛ ویروسی که گفته می‌شود عامل حمله سایبری به شبکه مجازی وزارت نفت بوده اما با هوشیاری کارشناسان ایرانی، در تحقق اهداف موفق نبوده است و مورد چهارم نیز بدافزار شعله آتش بوده که از آن به عنوان سلاح خاموشی نام می‌برند و کارشناسان معتقدند مخرب‌ترین سلاح فضای سایبری علیه ایران بوده است. اما حملات سایبری به ایران منجر به واکنش نهادهای بین‌المللی هم شده تا آنجا که سازمان ملل در گزارشی نسبت به این حملات نه تنها به ایران حتی به برخی از دیگر کشورها نیز هشدار داده است. هر چند که کارشناسان امنیتی بیان می‌کنند این حملات سایبری به احتمال زیاد یک حرکت دولتی بوده و از سوی یک دولت صورت گرفته است اما هنوز امکان ردیابی منشا این حمله به دست نیامده است. اما مسوولان رژیم صهیونیستی به صورت تلویحی اقدامات سایبری علیه ایران را به گردن گرفتند.

معاون نخست‌وزیر رژیم صهیونیستی در ادامه سیاست‌های خصمانه این رژیم در قبال ایران، آن‌چه حمله ویروس‌های کامپیوتری به ایران خوانده شده است را منطقی خواند. به گفته موشه یعالون برای هر کسی که تهدید ایران را قابل توجه می‌داند، منطقی است گام‌های مختلفی از جمله این گام را بردارد تا به آنها صدمه بزند. از سویی دیگر لابراتوار امنیت سایبری روسیه، کاسپرسکی، گزارش می‌دهد در حال حاضر ۱۸۹ مورد از تاثیرگذاری ویروس رایانه‌ای در ایران گزارش شده و این رقم در اسراییل ۹۸ مورد و در سودان ۳۲ مورد گزارش شده است. البته مواردی نیز در سوریه، لبنان، عربستان سعودی و مصر وجود داشته است. هرچند در مورد استاکس‌نت ایران به طور مستقیم از آمریکا و اسراییل به عنوان طراحی‌کنندگان این ویروس به منظور ضربه زدن به جمهوری اسلامی نام برده بود اما در مورد فلیم به طور غیرمستقیم اسراییل متهم شده است.

رامین مهمانپرست، سخنگوی وزارت امور خارجه ایران در گفت‌وگو با خبرنگاران اظهار داشت: برخی کشورها و رژیم‌های غیرمشروع ویروس‌ها را تولید می‌کنند. البته وی مستقیما به نام اسراییل اشاره نکرده اما ایران همواره اسراییل را یک رژیم نامشروع می‌داند. با این حال به گفته متخصصان امنیت شبکه، پنهان بودن این بدافزارها برای چندین سال پی‌درپی به آن معنی است که ماموریت‌های سایبری دیگری نیز در حال اجرا هستند که هنوز شناسایی نشده‌اند. متخصصان کاسپرسکی احتمال می‌دهند ساخت این بدافزارها توسط همان دولتی صورت گرفته که استاکس‌نت و دوکو را طراحی و منتشر کرده است.

«فلیم» مخرب‌ترین سلاح «سایبری»

«شعله»هایی که آرام‌آرام «اینترنت» را دربر می‌گیرد

شرق: طی روزهای گذشته یکی از اخبار مهمی که در سطح داخلی و بین‌المللی مطرح شده و بازتاب وسیعی هم داشت، بحث حمله سایبری و انتشار ویروسی با نام فلیم یا شعله آتش در فضای مجازی برخی از کشورهای کرانه باختری و ایران بوده است. درنهایت روز یکشنبه هفتم خرداد از سوی کارشناسان مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای (ماهر) این موضوع به نوعی تایید شد و کارشناسان این مرکز از ورود ویروسی جدی به کشور خبر دادند. در گزارش ماهر از این بدافزار با عنوان «شعله آتش» یاد شد و در بخشی از گزارش این مرکز آمده بود: این بدافزار در واقع پلتفرمی است که قابلیت دریافت و نصب ابزارهای گوناگون جهت فعالیت‌های مختلف را داراست. در حال حاضر هیچ کدام از اجزای پرشمار تشکیل‌دهنده این بدافزار توسط بیش از ۴۳ نرم‌افزار آنتی‌ویروس در دسترس مورد شناسایی قرار نمی‌گیرند. با این وجود ابزار شناسایی و پاکسازی این بدافزار در مرکز ماهر تهیه شده و از امروز در اختیار سازمان‌ها و شرکت‌های متقاضی قرار خواهد گرفت. اما در همین روزها کار بالاتر گرفت و بحث حمله جدید به سایت اینترنتی وزارتخانه‌هایی از جمله وزارت نفت بار دیگر مورد توجه قرار گرفت و پس از انتشار اخباری در این زمینه، روز گذشته روزنامه گاردین انگلیس هم در قالب گزارشی به هشدار کارشناسان در این خصوص اشاره کرد و مدعی شد: حمله سایبری ماه گذشته به وزارت نفت ایران و ترمینال اصلی صادرات نفت ایران از سوی پیچیده‌ترین کرم کامپیوتری که تاکنون ساخته شده بود صورت گرفته است. در ادامه این گزارش آمده بود: «به نظر می‌رسد این ویروس ابتدا در تعداد کمی از سازمان‌ها و نهادها در ایران، کرانه باختری، لبنان و امارات فرستاده شده است. این مساله به شکل اجتناب‌ناپذیری این شک را برمی‌انگیزد که رژیم صهیونیستی یا آمریکا به شکلی در این ماجرا دست داشته‌اند.» تحلیلگرانی که در رمزگشایی این کرم کامپیوتری موسوم به ۳۲W فلامر نقش داشته‌اند، نتوانسته‌اند منشاء این ویروس را شناسایی کنند اما می‌گویند تنها یک تیم حرفه‌ای با چندین ماه کار می‌تواند پشت این قضیه باشد. بنا بر گزارش گاردین آزمایشگاه «کرایسیس» در مجارستان اعلام کرده است: نتایج تحلیل‌های فنی ما حاکی از این فرضیه است که این کرم توسط یک آژانس دولتی با بودجه و تلاش قابل توجه ساخته شده و احتمالا به فعالیت‌های جنگ‌های سایبری مرتبط است. این آزمایشگاه افزود: این کرم کامپیوتری مطمئنا پیچیده‌ترین ویروسی است که تاکنون به آن برخورده‌ایم. مسلما این ویروس پیچیده‌ترین نرم‌افزار مخربی است که تاکنون کشف شده است. اما معاونت اجتماعی پلیس فضای تولید و تبادل اطلاعات نیروی انتظامی نیز در این زمینه به کاربران اینترنت هشدار داده و تلاش کرده است با اطلاع‌رسانی تا حدی جلو این مشکل را بگیرد. به گزارش پایگاه اطلاع‌رسانی صنعت این مرکز از کاربران اینترنت خواسته است به نامه‌های الکترونیکی ارسالی با عنوان «کنترل پهنای باند اینترنت» توجه نکنند چرا که به تازگی ای‌میلی در فضای اینترنت ایرانی برای مشترکان شرکت‌های ارایه‌دهنده خدمات اینترنت پرسرعت ای‌دی‌اس‌ال ارسال می‌شود که ضمن معرفی نرم‌افزاری با عنوان «کنترل پهنای باند اینترنت» برای رفع مشکلات پهنای باند کاربر، از گیرنده پیام می‌خواهد با کلیک روی لینک، این نرم‌افزار را دریافت کند. در این گزارش آمده است که متاسفانه این نرم‌افزار حاوی بدافزاری است که اطلاعات کاربران را به سرقت می‌برد. این نرم‌افزار فشرده‌شده که از خانواده keylogger‌ها محسوب می‌شود، حاوی دو فایل اجرایی به نام‌های network. exe و password. exe است و در مراحل نصب از کاربر می‌خواهد تا برای اتصال نرم‌افزار فایل اول و برای ورود کلمه عبور فایل دوم را اجرا کند. در صورت اجرای این دو فایل، این نرم‌افزار جاسوسی روی سیستم قربانی نصب شده و در صورتی که قربانی اطلاعات حساسی نظیر اطلاعات حساب‌های بانکی در هنگام خریدهای اینترنتی (شماره کارت رمز دوم، تاریخ انقضای کارت، CVV2) را استفاده کند، آن اطلاعات به راحتی برای مجرم ارسال می‌شود. همچنین این نرم‌افزار امکان سرک کشیدن به فعالیت‌های کاربر را نیز دارد و در فواصل زمانی کوتاه‌مدت نیز ضمن عکسبرداری از صفحه دسک‌تاپ کاربر، آن تصاویر را نیز برای مجرم ارسال می‌کند. به گزارش ایسنا، اگرچه در سال‌های اخیر بحث حملات سایبری و ترور مجازی در سطحی جدی در کشورها مطرح بوده و در بسیاری موارد کشورهایی چون آمریکا و رژیم صهیونیستی سعی کرده‌اند خود را قربانی این حملات نشان دهند اما مدت‌هاست کارشناسان و متخصصان فضای مجازی از دست داشتن این کشورها در آلوده‌سازی فضای سایبری و حملات آنها خبر می‌دهند. در زمینه انتشار ویروس شعله آتش هم تاکنون منابع متعددی از این دو کشور نام برده و آنها را طراح این بدافزار خوانده‌اند. به عنوان مثال روزنامه گاردین در این‌باره نوشت: «اگرچه هیچ‌کس نمی‌تواند با اطمینان بگوید که چه کسی مسوول ساخت این ویروس جدید است اما تنها برخی از کشورها توانایی ساخت چنین ویروسی را دارند و در این میان رژیم صهیونیستی و آمریکا در ساخت چنین ویروس‌هایی پیشرو هستند.» سال گذشته هم تحقیقات روزنامه نیویورک‌تایمز نشان داده بود که ویروس استاکس‌نت یک عملیات مشترک از سوی آمریکا و رژیم صهیونیستی برای تضعیف برنامه هسته‌ای ایران بوده است. البته معاون نخست‌وزیر رژیم صهیونیستی نیز در قبال انتشار چنین خبری موضع منفی نگرفته و آنچه حمله ویروس کامپیوتری «فلیم» به ایران خوانده شده است را «منطقی» خوانده است. موشه یعالون، معاون نخست‌وزیر رژیم صهیونیستی روز سه‌شنبه ساعاتی پس از آنکه موسسه «کاسپرسکی» مدعی حمله ویروس کامپیوتری «فلیم» به ایران شد، در اظهاراتی بی‌اساس به رادیو رژیم صهیونیستی گفت: برای هر کسی که تهدید ایران را قابل توجه می‌داند، منطقی است گام‌های مختلفی از جمله این گام را بردارد تا به آنها صدمه بزند. وی که رژیم متبوعش تنها دارنده تسلیحات هسته‌ای در خاورمیانه است، با ادعای اینکه این رژیم از فناوری برتری برخوردار است، گفته بود: این دستاوردها انواع امکانات را برای ما فراهم می‌کنند. اما اگرچه این ویروس در میان متخصصان دنیا به عنوان جدی‌ترین و پیچیده‌ترین ویروس شناخته شده اما با این حال متخصصان ایرانی برای کنترل و از بین بردن نتایج منفی آن برنامه‌ریزی‌های متعدد کرده و به نتایجی نیز رسیده‌اند. در همین زمینه برای نخستین بار در دنیا، ابزار پاک‌سازی بدافزار شعله آتش از سوی مرکز ماهر تولید و قرار بر آن شد که این ابزار از طریق سایت مرکز ماهر در اختیار کاربران قرار بگیرد. بر اساس اعلام مرکز ماهر و با توجه به طراحی صورت‌گرفته، بدافزار شعله آتش به کمک این ابزار از روی سیستم کاربران حذف می‌شود و در صورت تایید کاربران اطلاعات این بدافزار به منظور آنالیز بیشتر به مرکز ماهر ارسال خواهد شد. این نخستین باری است که ابزار پاک‌سازی این بدافزار تولید می‌شود و مرکز ماهر ایران آمادگی دارد تا در این زمینه با مراکز ماهر دیگر کشورها و همچنین تولیدکنندگان داخلی و خارجی آنتی‌ویروس برای قرار دادن این ابزار در بانک اطلاعاتی خود، همکاری کند.

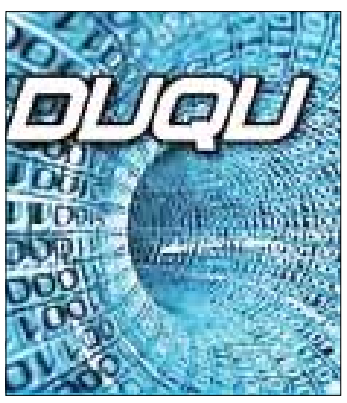
همه در موردش زیاده‌روی کردند

دوکو، برادر ناتنی

به تدریج که اطلاعات بیشتری درباره ویروس دوکو (Duqu) منتشر می‌شود و برنامه ویروس تحت بررسی دقیق‌تر قرار می‌گیرد، اکنون برخی کارشناسان امنیتی معتقدند که جنجال درباره این ویروس بیش از حد بوده و شاید درباره اهمیت و میزان خطر ویروس دوکو زیاده‌روی شده باشد. بر اساس اعلام شرکت مهندسی شبکه گستر، شک و تردید کارشناسان به دلیل اطلاعات محدودی است که درباره فعالیت و عملکرد ویروس دوکو تا به حال منتشر شده است. تا به حال فقط شرکت Symantec یک گزارش درباره این ویروس منتشر کرده که نشان می‌دهد هدف اصلی آن سیستم‌های مدیریت صنعتی است. به عقیده کارشناسان Symantec نویسنده این ویروس جدید باید همان نویسنده ویروس استاکس‌نت باشد. در این گزارش گفته شده که ویروس دوکو فقط وظیفه جمع‌آوری اطلاعات درباره سیستم‌های مدیریت صنعتی را دارد و احتمال داده می‌شود براساس این اطلاعات، ویروس اختصاصی و ویژه‌ای برای حمله و رخنه به سیستم‌های مدیریت صنعتی ساخته شود. به گزارش پایگاه اطلاع‌رسانی فناوری اطلاعات- ایتنا- شرکت Symantec تاکنون اطلاعات دقیقی درباره مراکزی که آلوده به ویروس دوکو شده‌اند، منتشر نکرده و ادعای قبلی خود را که گفته بود چندین واحد صنعتی در اروپا آلوده شده‌اند، پس گرفته و اکنون اعلام کرده فقط یک واحد صنعتی قربانی ویروس دوکو شده است. به اعتقاد کارشناسان، اگر موضوع مشابهت برنامه‌نویسی بین دو ویروس دوکو و استاکس‌نت وجود نداشت، ویروس دوکو تا این حد مورد توجه و بحث قرار نمی‌گرفت. مشابهت بخش‌هایی از برنامه این دو ویروس، فقط از این جهت می‌تواند مورد توجه قرار گیرد که بالاخره یک نفر به فکر استفاده از برنامه ویروس استاکس‌نت افتاده است. باید توجه داشت اگر هدف اصلی ویروس دوکو جمع‌آوری اطلاعات از سیستم‌های مدیریت صنعتی است، این کار را ویروس استاکس‌نت قبلا انجام داده است. اگر هم قرار است اطلاعات جدیدی به دست آورده شود، استفاده دوباره و علنی از برنامه ویروس استاکس‌نت، یک اقدام ناشیانه است که از افراد و مراکزی که پشت این‌گونه فعالیت‌های جاسوسی هستند، بعید به نظر می‌رسد. اگر در مراحل بعدی تحقیق و بررسی روی ویروس دوکو مشخص شود که این ویروس اهداف دیگری را دنبال می‌کند، شاید آن موقع ارزش توجه و پیگیری بیشتری داشته باشد وگرنه در حالت فعلی، ویروس دوکو هم ویروسی است مانند هزاران ویروسی که روزانه ظاهر و کشف می‌شوند. کاربران ضدویروس‌های McAfee از هفته گذشته با داشتن فایل‌های به‌روزرسانی حداقل DAT 6501 یا جدیدتر، در برابر گونه‌های مختلف ویروس دوکو در امان بوده و قادر به شناسایی آنها هستند. گزارش جدیدی که شرکت Dell Secure Works منتشر کرده، ارتباط بین ویروس مشهور استاکس‌نت و ویروس جدید دوکو را مورد تردید قرار می‌دهد. همچنین در این گزارش، به نبود مدرک و سندی که نشان دهد هر دو ویروس توسط یک شخص یا یک گروه نوشته شده‌اند، اشاره شده است. شاید شباهت‌هایی بین برنامه و عملکرد دو ویروس وجود داشته باشد ولی دلیل و مدرک قاطعی برای نشان دادن ارتباط مستقیم بین دو ویروس استاکس‌نت و دوکو وجود ندارد. هر دو ویروس دوکو و استاکس‌نت ویروس‌های پیچیده‌ای هستند که از چندین بخش مختلف تشکیل شده‌اند. تنها شباهت برنامه این دو ویروس، در یکی از چندین بخش مختلفی است که در مجموع برنامه ویروس را تشکیل می‌دهند. هر دو ویروس از یک روش یکسان برای رمزگشایی فایل‌هایی خاص و قراردادن آنها روی کامپیوتر قربانی، استفاده می‌کنند. همچنین روش رمزگذاری و مخفی‌سازی فایل‌های مرتبط با ویروس، در هر دو ویروس یکسان و مشابه هستند. با این حال، استفاده از یک برنامه مخفی‌سازی یکسان، نشان‌دهنده ارتباط دو ویروس نمی‌تواند باشد. این‌گونه برنامه‌های مخفی‌سازی که اصطلاحا Rootkit نامیده می‌شوند، امروزه در ویروس‌های مختلف به کار گرفته می‌شوند. این برنامه و روش خاص مخفی‌سازی که در ویروس دوکو و استاکس‌نت مورد استفاده قرار گرفته، قبلا در ویروس‌های Black Energy و Rustock نیز مشاهده شده است. به نکته دیگری که برای اثبات ارتباط دو ویروس دوکو و استاکس‌نت اشاره می‌شود، استفاده از یک گواهینامه دیجیتال به‌سرقت‌رفته در هر دو ویروس است. این نکته کاملا صحیح است ولی دسترسی به این گواهینامه‌های سرقت‌شده از چندین منبع مختلف امکان‌پذیر است و احتمال دارد در آینده، از این گواهینامه در برنامه‌های مخرب دیگر هم استفاده شود. ویروس استاکس‌نت برای رخنه و نفوذ به سیستم‌های مورد نظر خود از چهار نقطه ضعف ناشناخته استفاده می‌کرد. ویروس دوکو از هیچ نقطه ضعفی استفاده نمی‌کند و ساختار این ویروس نشان می‌دهد که انتشار و گسترش گسترده ویروس، از اولویت‌های نویسنده آن نبوده است. ویروس دوکو یک برنامه قوی و پیچیده است و شاید چند سال قبل به عنوان یک ویروس خارق‌العاده به حساب می‌آمد ولی امروز ویروس‌های هوشمند و پیچیده کم نیستند و نباید اینچنین مجذوب دوکو شد.

درباره دوکو

ویروسی با اهداف خاص



دوکو ـ Duqu ـ یک ویروس جدید است که فقط مراکز و موسسات خاصی را در اروپا، آفریقا و خاورمیانه مورد هدف قرار می‌دهد.

■■■

این ویروس چه ارتباطی به ویروس استاکس‌نت دارد؟

بسیاری از بخش‌های این ویروس کاملا مشابه ویروس مشهور استاکس‌نت است. در بعضی قسمت‌ها، برنامه ویروس دوکو خط به خط مشابه استاکس‌نت است. به همین دلیل به این ویروس، نام‌های استاکس‌نت دوم یا استاکس‌نت پسر داده شده است.

چرا نام دوکو روی این ویروس گذاشته شده است؟

دوکو به صورت «دی یو-کی یو» تلفظ می‌شود. این ویروس فایل‌هایی با پیشوند DQ روی کامپیوتر قربانی ایجاد می‌کند.

زمان ظهور این ویروس چه تاریخی بوده است؟

ویروس دوکو حدود هفت هفته قبل برای اولین بار مشاهده شده ولی برخی گزارشات حاکی از آن است که این ویروس از دی ماه سال گذشته فعال بوده است.

ویروس دوکو چه کار می‌کند؟

این ویروس روی شبکه‌هایی که آلوده کرده است، اقدام به جمع‌آوری اطلاعات می‌کند.

ویروس دوکو چگونه عمل می‌کند؟

ویروس ابتدا اقدام به آلوده کردن کامپیوتر می‌کند. نحوه این آلودگی به‌طور کامل و دقیق مشخص نیست ولی روش‌های مختلف از جمله حافظه‌های USB و فریب از طریق مهندسی اجتماعی (Social Engineering)، گزارش شده است. پس از آلوده کردن کامپیوتر، ویروس با یک مرکز فرماندهی که در کشور هند است، تماس برقرار می‌کند. (در حال حاضر، این ارتباط قطع شده است.) از طریق این مرکز، دستورات جدید و انواع برنامه‌های مخرب دریافت شده و روی کامپیوتر قربانی به اجرا درمی‌آید. همچنین اگر کامپیوتر آلوده، به شبکه وصل باشد، کل شبکه توسط ویروس برای شناسایی نقاط ضعف احتمالی، کنترل و بررسی شده و نتیجه به دست آمده به مرکز فرماندهی ارسال می‌شود.

هدف اصلی ویروس دوکو چیست؟

در حال حاضر اهداف خاص ویروس دوکو مشخص نیست. احتمال داده می‌شود که ویروس در حال ایجاد بسترهای لازم برای انجام یک حمله خاص است. ساختار فعلی ویروس دوکو هیچ‌گونه امکانات حمله و تخریب ندارد ولی در هر لحظه می‌تواند از طریق ارتباط با مرکز فرماندهی، این نوع قابلیت‌ها را به دست آورد.

قربانیان ویروس دوکو چه افراد و مراکزی هستند؟

درباره قربانیان اصلی ویروس دوکو اختلاف نظر وجود دارد. برخی معتقدند که این ویروس برای حمله به مراکز صدور گواهینامه‌های دیجیتالی (Certificate Authority) طراحی شده و برخی دیگر، سیستم‌های مدیریت صنعتی خاصی را قربانی و هدف اصلی ویروس دوکو می‌دانند.

نویسندگان و گردانندگان ویروس دوکو چه کسانی هستند؟

با توجه به شباهت بسیار زیاد بین ویروس استاکس‌نت و دوکو، احتمال داده می‌شود همان تشکیلاتی که مسوول ساخت و توزیع ویروس استاکس‌نت بودند، پشت ویروس دوکو هم باشند. با آنکه به اثبات نرسیده، تقریبا همه کارشناسان، دولت آمریکا و اسراییل را عامل اصلی ساخت و انتشار ویروس استاکس‌نت دانسته‌اند. از طرف دیگر، برخی کارشناسان، شباهت برنامه‌نویسی بین دو ویروس را چندان با اهمیت ندانسته و کپی‌برداری از ویروس‌های قدیمی برای ساخت ویروس‌های جدید را یک امر عادی و متداول می‌دانند.

از کجا بدانیم آلوده به ویروس دوکو شده‌ایم؟

ضدویروس McAfee از اوایل هفته گذشته، با فایل‌های بروزرسانی DAT 6501، قادر به شناسایی ویروس دوکو است. البته احتمال دارد که گونه‌های جدید و جهش‌یافته این ویروس در طی روزهای آینده ظاهر شود. لذا به همه کاربران توصیه می‌شود، ضدویروس خود را همواره به‌روز نگهدارند.

اهمیت و خطر ویروس دوکو تا چه حد جدی است؟

در حال حاضر با از کار انداختن مرکز فرماندهی این ویروس، فعالیت چندانی از ویروس دوکو مشاهده نمی‌شود. البته امکان دارد که این ویروس قادر باشد با مراکز فرماندهی متعددی ارتباط برقرار کند. هنوز ساختار ویروس دوکو به دقت بررسی نشده و مشخص نیست که ویروس قابلیت برقراری ارتباط با دیگر مراکز فرماندهی را داشته باشد. از طرف دیگر، برخی کارشناسان معتقدند که تنها شباهت برنامه‌نویسی بین دو ویروس دوکو و استاکس‌نت باعث مطرح شدن گسترده این ویروس جدید شده اگرنه هزاران ویروس هم‌ردیف ویروس دوکو هر روز ظاهر و کشف می‌شوند.

ویروس دوکو را چه شخص و مرکزی کشف کرده است؟

این موضوع فعلا محرمانه است و فقط گفته می‌شود که توسط یک گروه از کارشناسان امنیتی این ویروس کشف شده است. البته یک شرکت امنیتی کوچک در مجارستان هم ادعای کشف این ویروس را دارد.

گذرگاه

«دوکو»، ناشناخته و مرموز

فریبا یاراحمدی

■ اواخر مهر ماه سال گذشته و درست یکسال بعد از انتشار خبر بدافزار استاکس‌نت در زیر ساخت‌های صنعتی سایبری کشور این بار اما مجددا برای اولین بار بی‌بی سی خبر از ظهور بدافزاری دیگر می‌دهد. بد افزاری که به گفته محققان شواهدی در آن یافته‌اند از اینکه کرم استاکس‌نت که باعث نگرانی در کشورهای مختلف شد ممکن است دوباره در شکل تازه‌ای ظاهر شود. ماجرا به حدی جدی شد که گفته شد دوکو، می‌تواند پیش‌درآمدی بر یک حمله از نوع استاکس‌نت در آینده باشد. این کشف توسط شرکت امنیت اینترنتی سیمانتک انجام شد. یکی از مشتریان این شرکت آنها را از این تهدید آگاه کرده بود. این کرم تازه «دوکو» نامگذاری شده زیرا فایل‌هایی با مقدمه «DQ» ایجاد می‌کند. تحلیل اولیه نشان داد که دوکو تقریبا همانند استاکس‌نت است و احتمالا توسط نویسندگان همان بدافزار یا کسانی که به کد اصلی آن دسترسی داشته‌اند ایجاد شده است. نکته جالب توجه آن بود که اعلام شد دوکو برای حمله به سیستم‌های صنعتی مانند تاسیسات اتمی ایران طراحی نشده بلکه کار آن جمع‌آوری اطلاعات برای حملات آینده است. مساله زمانی اهمیت بیشتری پیدا کرد که به گفته یکی از کارشناسان سیمانتک این یک کار تفننی نیست، بلکه از آخرین تکنیک‌های پیشرفته استفاده می‌کند که به این معنی است که توسط کسی که هدف خاصی در ذهن داشته طراحی شده است. اندکی بعد اما جزییات بیشتری درخصوص این بدافزار مرموز منتشر شد. بنابر اعلام کارشناسان مک‌آفی، این بدافزار از یک نقطه ضعف در بخش Kernel سیستم عامل Windows برای آلوده کردن کامپیوترهای قربانی و ایجاد ارتباط با سرور مرکز فرماندهی استفاده می‌کند. این نقطه ضعف تا به حال ناشناخته بوده و در حال حاضر اصلاحیه‌ای برای رفع آن از سوی شرکت مایکروسافت منتشر نشده است. همچنین این بدافزار از طریق یک فایل اولیه که مرحله نصب فایل‌های اصلی ویروس را انجام می‌دهد، روی کامپیوتر قربانی نصب و فعال می‌شود. این فایل که اصطلاحا به آن Installer یا Dropper گفته می‌شود، در قالب یک فایل Word است و در صورت باز کردن این فایل DOC مخرب، با سوءاستفاده از نقطه ضعف Kernel، مجوزهای لازم برای نصب فایل‌های اصلی ویروس Duqu روی کامپیوتر فراهم و به این‌ترتیب ویروس فعال می‌شود. اندکی بعد اما متخصصان کسپرسکی موفق شدند ابعاد تازه‌ای از فعالیت این بدافزار را منتشر کنند. به اعتقاد متخصصان آزمایشگاه کسپرسکی، این پلتفرم که Tilded نامگذاری شده است (به دلیل تمایل ایجادکننده‌های آن به استفاده از فایل‌هایی که با نماد نویسه tilde (~) شروع می‌شوند)، برای ایجاد استاکس‌نت و دوکو و نیز برنامه‌های مخرب دیگر استفاده شده است. ارتباط بین دوکو و استاکس‌نت در حین تجزیه و تحلیل یکی از رویدادهای مرتبط با دوکو آشکار شد. در حین بررسی سیستم آلوده که گمان می‌رفت در آگوست سال ۲۰۱۱ مورد حمله قرار گرفته باشد، یک درایور شناسایی شد که با درایور استفاده شده به وسیله یکی از نسخه‌های استاکس‌نت مشابه بود. گرچه شباهت آشکاری بین دو درایور وجود داشت، تفاوت‌هایی نیز در جزییات آنها مانند تاریخ امضای گواهی دیجیتال به چشم می‌خورد. فایل‌های دیگری که امکان نسبت دادن آنها به فعالیت استاکس‌نت وجود داشته باشد، شناسایی نشد، اما نشانه‌هایی از فعالیت دوکو وجود داشت. پردازش اطلاعات به دست آمده و جست‌وجوی بیشتر در پایگاه داده برنامه‌های مخرب آزمایشگاه کسپرسکی امکان آشکار کردن یک درایور دیگر با ویژگی‌های مشابه را میسر کرد. این درایور بیش از یک سال پیش کشف شد، اما فایل آن در ژانویه سال ۲۰۰۸، یک سال قبل از ایجاد درایورهای استفاده شده به وسیله استاکس‌نت کامپایل شده بود. متخصصان آزمایشگاه کسپرسکی مجموعا هفت نوع درایور با ویژگی‌های مشابه را شناسایی کردند. لازم به ذکر است که هیچ اطلاعاتی تاکنون درباره سه مورد از آنها به دست نیامده است، به خصوص اینکه با کدام برنامه مخرب استفاده شده‌اند. الکساندر گوستف، متخصص ارشد امنیت در آزمایشگاه کسپرسکی، اظهار داشت: «درایورهای برنامه‌های مخربی که هنوز شناخته نشده‌اند را نمی‌توان به فعالیت تروجان‌های استاکس‌نت و دوکو نسبت داد. شیوه‌های انتشار استاکس‌نت، ممکن است آلودگی‌های بسیاری را با استفاده از این درایورها موجب شده باشد و به دلیل تاریخ کامپایل، نمی‌توان آنها را به تروجان هدفمندتر دوکو نیز نسبت داد. معتقدیم که این درایورها یا در نسخه قدیمی‌تر دوکو استفاده شده‌اند یا برای آلودگی با استفاده از برنامه‌های مخرب کاملا متفاوتی به کار رفته‌اند که گذشته از این، پلتفرم یکسانی دارند و احتمالا توسط یک تیم ایجاد شده‌اند. دوکو اما همچنان مرموز ماند و هیچ وقت به اندازه استاکس‌نت حداقل در مطبوعات عمومی مورد توجه قرار نگرفت و جالب‌تر اینجا بود که چندی بعد خبر دیگری از سوی متخصصان آزمایشگاه‌های کسپرسکی اعلام شد که هکرهایی که پشت بات نت Duqu قرار دارند، فعالیت استراق سمع خود را متوقف کرده‌اند. به گزارش شرکت کسپرسکی، تمامی فایل‌های ۱۲ سرور دستور و کنترل شناخته شده برای دوکو، در تاریخ ۲۰ اکتبر ۲۰۱۱ پاک شده‌اند. دوکو البته امروز دیگر آنچنان که باید در صدر نیست چرا که جای خود را به بدافزاری به نام فلیم داده؛ بدافزاری که بسیار پیچیده‌تر از دوکو و حتی استاکس‌نت است.