مشکل امنیتی کرم استوکس‌نت برای سیستم‌های صنعتی کشور

بازهم ویندوز، بازهم ناامنی

سعید نوری آزاد

پیشتر درباره امنیت در فضای مجازی و موضوع جنگ و جاسوسی سایبر صحبت کرده بودیم، اما موضوع مورد بحث امروز چیزی است که در تئوری و احتمالات نمی‌گنجد. موضوع سرقت است؛ سرقت اطلاعات صنعتی. آن‌هم نه در نیمه شب و در یک عملیات تعقیب و گریز همانند فیلم‌های مهیج و نه در خیال برخی مدیران شبکه، بلکه در ساعات اداری از داخل سیستم‌های مدیریت صنعتی کشور که تقریبا همه‌جا وجود دارند و در سیستم‌های شبکه CNG گرفته تا شبکه انتقال برق و نیروی دریایی به‌کار گرفته می‌شود. این جاسوسی یا سرقت اطلاعات توسط کسی نیست که بتوان آن را بازداشت یا از او بازجویی کرد. سرقت مقدار زیادی اطلاعات است توسط یک کرم رایانه‌ای.

پرده یکم: اخبار

حدود یک ماه پیش، یعنی ۲۰جولای امسال یک وب‌سایت بلاروس که کارش شناسایی بدافزارهای رایانه‌ای است، مثل هر روز آفتابی یا ابری یا شاید بارانی دیگر مشغول کار روزانه بود که با کرمی در منطقه خاورمیانه، هند و آسیای شرقی روبه‌رو شد. در آغاز این موضوع چندان عجیب نبود و تنها یک ویروس ساده قلمداد شد که می‌تواند مشکلاتی مانند صفحه آبی و خاموشی سیستم را ایجاد کند. در گزارشی که توسط نمایندگی ایرانی این شرکت هم منعکس شد آمده است: این بدافزار می‌تواند از طریق پورت یواس‌بی منتقل شود که بنا به طبیعت کرم‌های رایانه‌ای طبیعی به‌نظر می‌آید.

اما در تاریخ ۲۲ جولای شرکت سیمانتک که

IP Address	COMPUTER NAME	NETBIOS
[redacted].243.135	ADMIN-PC	WORKGROUP
[redacted].243.135	B-074B59C7DD934	WORKGROUP
[redacted].243.135	COMPUTER1	WORKGROUP
[redacted].243.135	GORJI-259E4B69A	WORKGROUP
[redacted].243.135	PEYMAN-PC	WORKGROUP
[redacted].243.135	USER-PC	WORKGROUP

منبع: symantec

تولیدکننده نرم‌افزار ضدویروس نورتن است، این خبر را منتشر کرد که توانسته است یک کرم رایانه‌ای به‌نام Stuxnet را روی بسیاری از سیستم‌های مشتریانش شناسایی کند (که در شماره ۲۹۲ کلیک به آن پرداختیم). در گزارش سیمانتک نیز آمده است این بدافزار کارکرد خاصی داشته و روی سیستم‌های صنعتی متمرکز است.

اخبار تکمیلی در این زمینه باز هم منتشر شد. کامپیوترورلد و بیزینس‌ویک نیز اطلاعاتی از این نوع را منتشر کردند. در گزارش‌های مختلف که به‌تدریج تکمیل شده، آمده است که این بدافزار روی سیستم‌های رایانه‌ای کنترلگرهای صنعتی محصول شرکت زیمنس آلمان موسوم به اسکادا کار اصلی خود را انجام می‌دهد. در یافته‌های شرکت‌های ضدویروسی مانند سیمانتک و کسپرسکی آمده است این بدافزار با انتقال از سیستم‌های مختلف خود را وارد شبکه‌های دارای سیستم‌های اسکادا می‌کند و با یافتن این سیستم‌ها با پنهان‌سازی خود در پشت پرده سیستم‌ها را کنترل کرده و اقدام به‌سرقت اطلاعات می‌کند.

پرده دوم: روش دزدی

این بدافزار می‌تواند سیستم میزبان را شناسایی کرده و با یافتن مسیر مناسب به اینترنت متصل شود سپس با کنترل سیستم اسکادا که رابط نرم‌افزاری سیستم‌عامل رایانه و سخت‌افزار زیمنس است اطلاعات مورد نظر خود را به مقصدهای از پیش مشخص شده بفرستد. مقصد این بدافزار از دیدگاه سیمانتک اول ایران سپس اندونزی و هند بوده است. اما از نظر برخی از شرکت‌ها مانند ESET آلودگی بیشتر در آمریکا بوده و سپس روسیه و ایران یک کشور حاشیه برای این موضوع بوده است.

پرده سوم: چه چیزی دزدیده می‌شود؟

معمولا بدافزارهایی که در اخبار امنیتی از آنها صحبت می‌شود، روی سیستم‌های خانگی یا تجاری متمرکز هستند که اطلاعاتی مانند حریم خصوصی افراد یا اطلاعات مالی افراد را هدف قرار می‌دهد تا بتواند به منافع زود بازده برسد. از طرفی زیرساخت بدافزارها معمولا یک رایانه خانگی یا چیزی شبیه آن است اما این بدافزار مقصد اصلی خود را یک سیستم کنترل اتوماسیون صنعتی گران‌قیمت در نظر گرفته و هزینه بسیار بالایی برای تهیه و کار آزمایشگاهی روی آن پرداخت شده است.

این بدافزار مشخصا دو نوع اطلاعات را می‌تواند سرقت کند. نوع اول اطلاعات مربوط به نوع فعالیت سیستم‌های صنعتی کارخانجات یا سیستم‌های صنعتی مشابه است و دسته دوم اطلاعات مربوط به طرح‌های صنعتی و نیروگاهی مورد آزمایش در مراکز استفاده‌کننده این سیستم می‌شود. این اطلاعات برای هر کشوری درنقش محصول تمام فعالیت‌های صنعتی است.

پرده چهارم: اسکادا چیست؟

واژه اسکادا (SCADA) به مفهوم جمع‌آوری داده، نظارت و کنترل همه جانبه* به‌وجود آمده است. این سیستم که کنترلگر صنعتی است در شبکه‌های بزرگ صنعتی یک مدیر کامل است و تمام فعالیت‌های مدیریتی تخصصی را زیر نظر دارد. این سیستم در حکم چشم و گوش بالاترین سطح مدیریت فنی شبکه‌های انتقال نیرو (در سطح کشور)، سیستم‌های تولید قطعات و کارخانجات صنعتی با مقیاس بزرگ است و از ۳قسمت تشکیل شده است: ۱- سیستم محلی ۲- سیستم ارتباطی ۳- سیستم مرکزی.

در بخش اول و سوم که مربوط به کارهای کنترلی است، فعالیت‌هایی در حوزه‌های تخصصی انجام می‌شود اما در قسمت دوم که بخش ارتباطی است نکات قابل توجهی نهفته است. سیستم ارتباطی بخش مهمی از سیستم اسکادا است که بدون آن تصور داشتن کنترل از راه دور غیرممکن می‌گرداند. این بخش وظیفه ایجاد ارتباط بین «سیستم محلی» و «سیستم مرکزی» را به‌عهده دارد. در حقیقت این بخش، نقش شبکه عصبی بدن را بازی می‌کند، به این صورت که اطلاعات را از گوش و چشم (سیستم محلی) به مغز (سیستم مرکزی) مخابره کرده و از آنجا فرمان‌ها را به دسته‌ها (سیستم محلی) می‌فرستد.

اما اطلاعات در سطح ملی چگونه منتقل می‌شوند؟ رسانه‌های مورد استفاده این شبکه‌ها معمولا عبارتند از شبکه تلفن، سیستم مخابراتی رادیویی، سیستم شبکه ماکروویو، کابل‌های هم‌محور یا کواکسیال، شبکه فیبرنوری، سیستم مخابراتی PLC و ماهواره.

سیستم‌های شبکه‌بندی آنها نیز نوع خاصی است. برای ارسال اطلاعات از راه دور باید این اطلاعات به سیگنال الکتریکی تبدیل شوند که در ایران برای ارسال اطلاعات (ارتباط یک سرور با RTU) معمولا از تلفن،

طرح: funnyartpictures

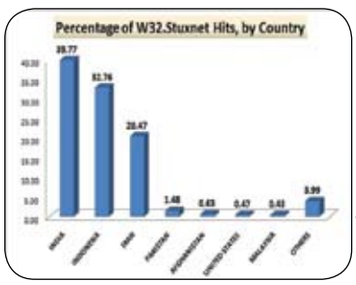
سیستم مخابراتی رادیویی، سیستم مخابراتی ماکروویو و به‌طور عمده از PLC استفاده می‌شود.

پرده پنجم: چه اتفاقی افتاده است؟

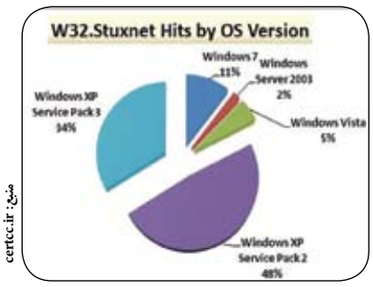
بی‌بی‌سی در گزارش ویژه‌ای اعلام کرد: «سیستم‌های صنعتی ایران به کرم جاسوسی به‌نام استاکس‌نت آلوده‌اند که احتمالا اطلاعات صنعتی و محرمانه زیادی را از ایران خارج کرده است. تیم کارشناسی بی‌بی‌سی معتقد است که این حمله سایبری می‌تواند در آینده نتایج مخربی برای بخش‌های امنیت اطلاعات ایران داشته باشد.»

معاون وزیر صنایع نیز پیش از این در گفتگویی از تشکیل تیمی برای مقابله با این مشکل خبر داده بود.

یکی از کارشناسان مرکز آگاهی‌رسانی، پشتیبانی و امداد (آپا) پژوهشکده امنیت ارتباطات و فناوری



منبع: certcc.ir



منبع: certcc.ir

اطلاعات مرکز تحقیقات مخابرات ایران در گفتگو با جام‌جم اظهار داشت: «اطلاعات زیادی توسط این بدافزار از سیستم‌های آلوده به خارج ارسال شده است. وی ادامه داد مقصد اولیه این اطلاعات دو سرور در مالزی بوده، اما از مقصد نهایی اطلاعات هنوز اطلاعاتی نداریم. وی اظهار داشت پس از بررسی این مشکل با اطلاع‌رسانی در سایت آپا و قرار دادن مسیر فایل‌های اصلاحیه اقدام امدادی را آغاز کردیم.

وی در پاسخ به این‌که آیا اطلاع‌رسانی یا ابلاغیه‌ای به مراکز زیر پوشش ارسال شده است، گفت: «با ارسال ابلاغیه‌ای، راهکار جلوگیری از این مشکل به آنها داده شده است و مراکز زیادی این اقدام را انجام داده‌اند اما همچنان مراکزی وجود دارند که سهل‌انگاری می‌کنند.»

دکتر شیخی ریاست مرکز آپای شیراز که در دانشگاه شیراز مسوولیت کار روی مسایل امنیتی و بدافزارها را برعهده دارد، به خبرنگار جام‌جم گفت: «مشکل راه‌حل پیش‌گیرانه ساده‌ای داشت و آن این‌که سیستم‌های اتوماسیون نباید با هیچ شبکه متصل به اینترنت ارتباط برقرار می‌کردند که به‌دلیل بی‌اطلاعی یا سهل‌انگاری برخی مراکز این مشکل تا حدود زیادی گسترش یافت.»

پرده آخر: چند دیدگاه

دیدگاه اول آن است که زیرساخت آسیب‌پذیر این سیستم یعنی سیستم‌عامل ویندوز فرش قرمزی برای متخاصمان بوده است.

دیدگاه دوم آن‌که شرکت‌هایی مانند ZDI که خریدار معایب سیستم‌های امنیتی هستند به هر شکل از این نقص آگاه شده‌اند و با سرمایه‌گذاری روی آن توانسته‌اند اقدام وسیعی برای نیل به اهداف خود داشته باشند.

دیدگاه سوم هم می‌گوید: اطلاع‌رسانی غیرتخصصی و خوش‌خیالی برخی مسوولان امنیتی کشور درباره امنیت اطلاعات باعث این مشکل شده است. در بسیاری از دانشگاه‌های کشور مسوولان شبکه و رایانه صرفا با رابطه به مدیریت می‌رسند و نه با تخصص آن‌هم بدون استفاده از نیروهای زبده یا حداقل استفاده از همفکری دیگر کارشناسان. از طرفی گزارش‌های تبلیغاتی شرکت‌هایی مانند سیمانتک یا شرکت‌هایی که قصد آغاز سرمایه‌گذاری در کشورها را دارند این نکته را می‌رساند که این می‌تواند یک مانور باشد تا برخی شرکت‌ها با یکدیگر مقابله کنند. در این رابطه نیز مک‌میلان سخنگوی زیمنس می‌گوید: «این نظریه که ایران هدف اصلی کرم استاکس‌نت است نادرست است چراکه ما فقط به‌گزارش شرکت سیمانتک که تولید کننده ضدویروس نورتن است استناد می‌کنیم.»

* Supervisory Control And Data Acquisition