دیگه چه‌خبر؟

یک سال سازمانی

اگر شما هم جزو آن افرادی هستید که از خودتان می‌پرسید ما برای چه سازمان نظام صنفی رایانه‌ای داریم؟ بد نیست بدانید اخیرا پرویز رحمتی رییس سازمان نظام صنفی رایانه‌ای کشور در پنجمین سالگرد تاسیس این سازمان گفته، است: «به‌رغم تلطیف روابطی که با نهادهای مرتبط صورت گرفته اما هنوز در بسیاری از نهادهای دولتی به دلیل عدم آشنایی با نقش و جایگاه سازمان‌های مردم‌نهاد هنوز هم این مسیر توام با آزمون و خطا است.»

او همچنین در در خصوص لزوم وجود سازمان نظام صنفی رایانه‌ای گفت: «در پنجمین سال حیات سازمان با خود فکر می‌کنیم که اگر سازمان وجود نمی‌داشت، کمیته فنی استاندارد IT کشور را نداشتیم. طرح ساماندهی بازار با مشارکت وزارت بازرگانی اجرا نمی‌شد. کارگروه بررسی اشکالات قانون رسیدگی به جرایم رایانه ای وجود نداشت و به طور کلی دستاوردهای کوچک و متوسط را در سال گذشته نمی‌داشتیم. جامعه صنفی و سازمان نظام صنفی و اعضای آن به این حداقل‌ها دلخوش هستند ولی در عین حال فاصله میان آنچه که هست و آنچه که باید باشد فاصله بسیار معنی‌داری است.

بنیاد ICDL و همایش مدیران

از آنجا که کلا فصل تابستان فصل گرما و استخر و ICDL و دست بر قضا این آخری هم کم هواخواه ندارد بنیاد ICDL سرانجام پس از مدت‌ها بی‌خبری، چندی پیش جزییات برگزاری همایش سراسری مدیران مراکز سال ۸۹ را اعلام کرد. علیرضا سلطانی فرد مدیر اجرایی این بنیاد، با اشاره به اینکه امسال بنیاد ICDL قصد دارد به شیوه متفاوتی این همایش را برگزار کند اعلام کرده که کلیه مدیران ICDL کشور می‌توانند با مراجعه به سایت این بنیاد ثبت نام کرده و با بخش‌نامه جدید آن آشنا شوند.

نرم‌افزار تحت وب مدارس

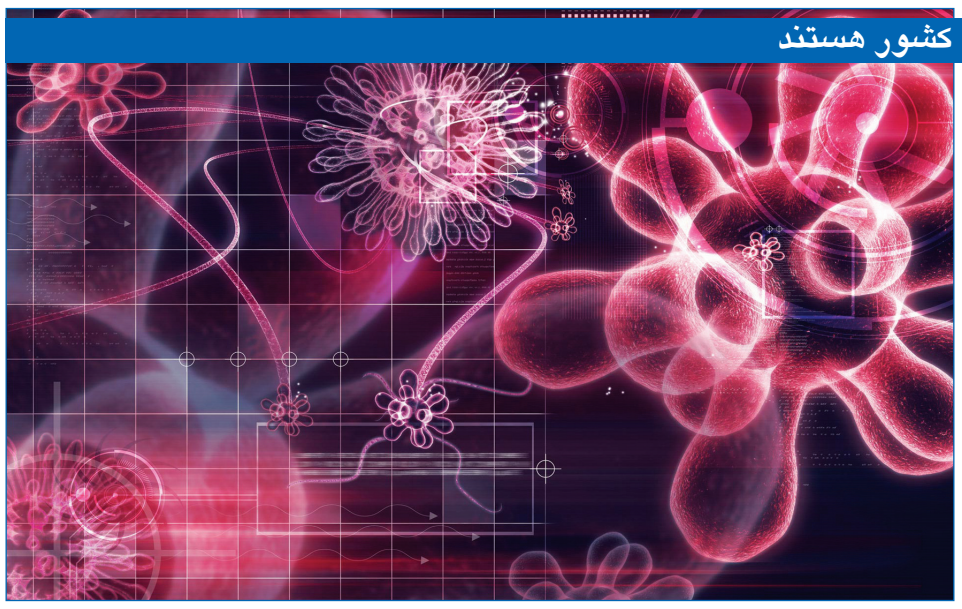
هفته گذشته شرکت نرم افزاری پایابنیان صنعت جدیدترین نرم‌افزار تحت وب مدارس موسوم به پایا مدرسه را به بازار معرفی کرد.این شرکت که مدعی است پایا مدرسه جامع‌ترین سیستم مدیریت مدارس است، هدف آن را پیشبرد سطح علمی مدارس، کاهش رفت و آمدهای غیر ضروری، ترویج فرهنگ استفاده از اینترنت و کامپیوتر در مدارس، کنترل و نظارت بیشتر مدیر بر عملکرد مدرسه و تعامل اولیا و مربیان اعلام کرده است.

سیمانتک و نسخه تازه وارد سرور

گویا به تازگی بازار دانلود نرم افزار های امنیتی گرم تر ازگذشته شده است.چند روزپیش شرکت نرم افزاری سیمانتک نسخه سروری نرم افزار امنیتی خود با ویرایش ۳۲ و ۶۴ بیت را جهت دانلود رایگان بر سایت خود قرار داد. این نرم افزار با عنوان Symantec Endpoint Protection 11.0.6005.562 در حقیقت نسخه فایروال دار آنتی ویروس Symantec Antivirus Corporate Edition است امکاناتی نظیرتشخیص نفوذهای داخل به خارج و برعکس، کنترل برنامه های سیستم در دسترسی به اینترنت و همچنین کنترل دسترسی‌ها به سیستم شما از کامپیوترهای شبکه را فراهم می‌کند.

حافظه‌های فلش در حال آلوده کردن رایانه‌های کل کشور هستند

گسترش ویروس مرگبار



سرویس گزارش- انتشار سریع ویروسی رایانه‌ای موسوم به RootKit.T mpHider موجبات نگرانی جدی تحلیلگران امنیتی در کشور را فراهم آورده است.

به گزارش عصر ارتباط، طی هفته‌های اخیر اخبار متعددی در فضای مجازی از سوی کاربران که مبنی بر افزایش خطاهایی مانند Script Error و حتی در برخی موارد ظاهرشدن صفحه آبی و خاموش‌شدن ناگهانی دستگاه‌ها به گوش می‌رسید. گمانه‌زنی‌ها ورود یک ویروس جدید به ایران که ظاهرا با هیچ یک از آنتی‌ویروس‌های متعارف نیز قابل شناسایی نیست را افزایش داد؛ تمرکز این شکایت‌ها در وبلاگ‌ها و اجتماعات مجازی فارسی‌زبان نیز این احتمال را به وجود آورد که ویروس یاد شده یا در ایران طراحی‌شده یا دست‌کم هنوز هیچ منبع جهانی موفق به شناسایی آن نشده است.

نشانه‌های عجیب

ردگیری مجموعه این اخبار پراکنده در نهایت نگاه‌ها را متوجه انجمن اینترنتی گرین‌وی با آدرس greenway.ir کرد که در یکی از نوشته‌های اخیر خود خبر از وجود یک فایل عجیب در فهرست فایل‌های سیستم داده و نوشته است: «طی روزهای اخیر گزارش‌های زیادی از کار نکردن برنامه‌ها توسط تولیدکنندگان نرم‌افزار و همچنین کاربرها داشتیم. خطاهای اجرایی مانند Script Error یا عدم نمایش فیلم برنامه‌ها از حدود یک ماه پیش افزایش یافته و به نقطه بحرانی رسیده است. همچنین در این مدت توسط برخی از کاربران نیز مورد لطف قرار گرفته‌ایم که نتیجه همه این مشکلات با بررسی دو سیستم که دارای رفتارهای عجیب بوده‌اند وجود یک Rootkit جدید تشخیص داده شد. برای رفع مشکل در سیستم‌ها حتما توجه کنید که فایل .MRxNet sys از زیر فهرست system32drivers سیستم شما حذف شود.

این انجمن فنی در نوشته یاد شده از ویژگی‌های منحصر به فرد این فایل رفتار این فایل ابراز شگفتی کرده و نوشته است: «این فایل بسیار عجیب است، اولا روال‌های این درایور به درستی نوشته نشده و در نتیجه اجازه نصب درایور بعدی در زنجیره را نمی‌دهد. ثانیا فایل‌های مشابه، دارای امضا نیستند ولی این فایل دارای امضای دیجیتال است و ثالثا، با این که در قسمت مشخصات فایل، نام مایکروسافت آورده شده، اما امضا کننده فایل Realtek است.

در پایان این نوشته وعده مکاتبه با شرکت‌های امنیتی متخصص در زمینه ویروس‌ها داده شده تا منشا مشکل به طور قطع یافت و نمونه فایل به بانک اطلاعاتی ویروس‌کش‌های معروف اضافه شود. وعده‌ای که در نهایت ما را به سایت ویروس‌کش تازه‌وارد VBA32 رساند.

ویروس پول‌ساز

ویروس‌کش جوان و تقریبا گمنام VirusBlokAda که بیشتر با نام تجاری VBA32 شناخته شده اصالتا یک ویروس‌کش متعلق به بلاروس یا همان روسیه سفید است که در چند سال اخیر اندک اندک جای پایی هم در بازار نرم‌افزاری ایران برای خود باز کرده است.

سایت ایرانی این ویروس‌کش با آدرس vba32-ir.com اولین سایتی است که به خبر انتشار RootKit.T mpHider واکنش نشان داد. در بخش اخبار این سایت ویروس mpHider ویروس خطرناک خوانده شده و آمده است: «این ویروس که از طریق حافظه‌های فلش منتشر شده و روی سیستم‌های کاربران ایرانی نیز دیده شده، به محض باز کردن حافظه فلش روی سیستم می‌نشیند و یک فایل با پسوند SYS تولید و در پوشه System32\Drivers ویندوز کپی می‌کند.»

در این سایت ادعا شده mpHider برای اولین بار توسط نرم‌افزارهای شرکت امنیتی VirusBlockAda کشف و ردیابی شده است و می‌تواند مشکلات مهمی مانند ایجاد خطای Blue Page و Reset شدن سیستم‌ها را روی کامپیوترهای آلوده شده به وجود بیاورد. از کار انداختن قفل‌های نرم‌افزاری روی دیسک‌های نوری از دیگر اثرات آلوده شدن سیستم‌های کامپیوتری به این روت‌کیت هستند. در این صورت کاربرانی که از این نرم‌افزارها استفاده می‌کنند یا تولیدکنندگانی که روی محصولات خود این نرم‌افزار را استفاده کرده‌اند، دچار مشکل خواهند شد.

به گزارش این سایت این ویروس دارای امضای Realtek است. در نتیجه در صورتی که این شرکت نتواند برای مقابله با آن اقدامی کند، از کار افتادن سخت‌افزارهای این شرکت روی سیستم‌ها از دیگر عواقب انتشار و توزیع این ویروس جدید خواهد بود.

RealTek همان غول صنایع نیمه‌هادی تایوانی‌هاست که کارت‌های صدایش بسیار در ایران شناخته شده هستند ولی محصولاتش طیف گسترده‌ای از تلویزیون‌های دیجیتالی تا تجهیزات شبکه را شامل می‌شود.

ناگفته نماند VBA32 نهایت استفاده را هم از این ویروس مرگبار و تازه‌وارد کرده و در همین سایت لینک شناسایی و پاک‌سازی این ویروس هم ارایه شده است.

گسترش سریع

تماس با عباس گنج‌خانی که لابراتوارش در شرکت بازیابی طلایی ژرف اولین گزارش‌ها درباره این ویروس جدید را منتشر کرده، جزییات بیشتری از ابعاد جدید این آلودگی را به دست می‌دهد.

مدیرعامل ژرف با اشاره به این که لزوما پاک کردن فایل MRxNet.sys مشکلات کاربران با mpHider را حل نخواهد کرد، گفت: «این فایل RootKit فقط ساخته می‌شود تا مانع دیده‌شدن ویروس اصلی شود و استفاده از آنتی ویروس در چنین شرایطی کاملا ضروری است. چون آنتی‌ویروس علاوه بر حذف روت‌کیت یاد شده رجیستری را هم اصلاح می‌کند که با توجه به تغییراتی که mpHider در قسمت SERVICES رجیستری ویندوز انجام می‌دهد اصلاح این بخش هم ضروری است.»

او با اشاره به مکاتبات صورت گرفته میان VBA32 و Realtek گفت: «بدون شک این ویروس خاص به ویژه با توجه به داشتن امضای شرکت RealTek در لابراتوارهای ویروس‌شناسی سراسر جهان در حال بحث است ولی احتمال آن که این ویروس در واقع بر اثر یک کارکرد نادرست یکی از راه‌اندازهای Realtek به وجود آمده باشد بسیار اندک است. چون این تغییرات پس از فعال شدن ویروس اعمال می‌شود.»

به گفته گنج‌خانی تا کنون دست‌کم ۳۰ درصد رایانه‌های آمارگیری شده توسط لابراتوار شرکت ژرف دارای این ویروس بوده‌اند و با توجه به این نکته که این ویروس از طریق حافظه‌های فلش منتقل می‌شود و استفاده از این حافظه‌ها در ایران بسیار رایج است احتمال گسترده‌تر شدن ابعاد آلودگی هم می‌رود.

او ضمن اشاره به این نکته که حتی نمونه‌هایی از این آلودگی در رایانه‌ها و حتی سرورهای بانک‌های معتبر کشور هم یافت شده است، هشدار داد: «چون سرورها معمولا قابلیت اتصال به حافظه‌های فلش را ندارند وجود mpHider روی این دستگاه‌ها احتمال تکثیر آن از طریق شبکه را بالاتر برده است. در واقع خطر واقعی هنگامی بروز می‌کند که مشخص بشود این ویروس یا نسخه‌های جدیدتر آن علاوه بر حافظه‌های فلش امکان انتقال از طریق شبکه را هم دارد که در این صورت سرعت گسترش و خسارات وارده توسط mpHider وارد فاز بسیار جدی‌تری خواهد شد.»