شنبه 03 فروردین 1392 - 10:19

بدافزارهای تهدیدآمیز سال گذشته/ معرفی برترین آنتی ویروسها

طراحی حملات سایبری فلیم و مینی فلیم علیه ایران، قطع دسترسی 350 هزار کاربر به اینترنت، باز شدن پای ویروسها به رایانه های مک و طراحی یو اس بی ویژه از بین بردن ویروسهای رایانه های شخصی و همچنین معرفی برترین آنتی ویروسهای سال از جمله رویدادهای مرتبط با ویروسها و بدافزارها بودند که در یکسال گذشته رخ داده است.

بدترین دستاوردهای فناوری

بدافزارهای تهدیدآمیز سال گذشته/ معرفی برترین آنتی ویروسها

طراحی حملات سایبری فلیم و مینی فلیم علیه ایران، قطع دسترسی 350 هزار کاربر به اینترنت، باز شدن پای ویروسها به رایانه های مک و طراحی یو اس بی ویژه از بین بردن ویروسهای رایانه های شخصی و همچنین معرفی برترین آنتی ویروسهای سال از جمله رویدادهای مرتبط با ویروسها و بدافزارها بودند که در یکسال گذشته رخ داده است.

به گزارش خبرنگار مهر، محققان در سالی که گذشت اعلام کردند که گروه‌هایی که مسئول حملات سایبری استاکس‌نت و فلیم بودند در مراحل اولیه هرکدام از حمله‌ها با یکدیگر همکاری داشته‌اند.

کسپراسکای اعلام کرد که تیم هر دو گروه حمله سایبری دست کم یکبار با یکدیگر به اشتراک کد منبع پرداخته اند. براساس اعلام کسپراسکای، آنچه ما دریافتیم شاهد بسیار قوی در این رابطه بود که سلاح های سایبری استاکس‌نت و فلیم به یکدیگر مرتبط هستند.

همکاری آمریکا و اسرائیل در طراحی ویروس "فلیم" علیه برنامه هسته ای ایران

براساس گزارشهای منتشر شده به نقل از مقامات غربی، همکاری آمریکا و رژیم صهیونیستی در طراحی ویروس مشهور به فلیم (Flame) برای اختلال در برنامه هسته ای ایران فاش شد.

براساس اعلام این مقامات آشنا با این عملیات، این اقدام با مشارکت سازمان امنیت ملی آمریکا، سازمان سیا و نیروی نظامی رژیم صهیونیستی صورت گرفته که دربرگیرنده استفاده از نرم افزار مخربی چون ویروس استاکس نت برای اختلال در تجهیزات غنی سازی هسته ای ایران بوده است.

یکی از مقامات عالی رتبه اطلاعات آمریکا با اشاره به این که این مسئله مرتبط به آماده شدن برای مبارزه با نوع دیگری از یک اقدام مخفیانه است، افزود، عناصر فلیم و استاکس نت بخشی از حملات گسترده تر است. گردآوری اطلاعات سایبر علیه برنامه هسته ای ایران راهی برای از بین بردن این برنامه خواهد بود.

نفوذ اسب تروا در مرکز دانلود برنامه های اجرایی اپل و گوگل

بر اساس یافته‌های کارشناسان کسپرسکی، اسب تروآی جدیدی در دو سرویس آنلاین App Store و Google Play منتشر شد که دفترچه تلفن کاربران را سرقت کرده و روی سرور مشخصی بارگذاری می‌کند.

کاوشگران ویروس شرکت کسپرسکی در پی درخواستی از سوی یک اپراتور روسی به نام MegaFon، برنامه موبایلی Find and Call را مورد بررسی قرار دادند و دریافتند که قسمتی از خدمات این نرم‌افزار با عنوان Find your friends بی سر و صدا و بدون آگاهی کاربران، اطلاعات و شماره های دفترچه تلفن آنها را روی سرور نویسندگان این برنامه بارگذاری می‌کند.

این در حالی است که هنگام بارگذاری یا همان "سرقت" اطلاعات دفترچه های تلفن، هیچ گزینه‌ای برای کسب اجازه از کاربران و رضایت آنها از انجام این کار وجود ندارد.

معرفی برترین آنتی ویروس های سال 2012

موسسه AV-Comparatives براساس جمع بندی تست های انجام شده بر روی آنتی ویروس های رایانه ای در طول سال 2012 چهار آنتی ویروس را به عنوان برترین های دنیا معرفی کرد.

آزمون های موسسه AV-Comparatives هر ساله بر روی بیش از 23 آنتی ویروس برتر از نقاط مختلف دنیا انجام می شود و

محصولات شرکت های عرضه کننده آنتی ویروس از جنبه های مختلف مورد تست قرار گرفته و بررسی می شوند و گزارش آخر سال این موسسه براساس جمع بندی تست های انجام شده بر روی آنتی ویروس ها در طول سال منتشر می شود.

براین اساس در انتخاب برترین آنتی ویروس های سال 2012 ، چهار آنتی ویروس رایانه ای از میان 23 آنتی ویروس به عنوان برترین های دنیا معرفی شدند. در آزمون تشخیص امسال، آویرا با تکرار موفقیت سال گذشته خود، امسال نیز در رده اول جدول مقایسه ای آنتی ویروس ها قرار گرفت و نشان نقره به کسپرسکی و دو نشان برنز به طور مشترک به بیت دیفندر و اف سکیور اختصاص یافت.

تهدید سیستمهای مالی و تجاری توسط بدافزار "ناریلام"

شرکت امنیت رایانه سیمانتک هم در این سال یک کرم رایانه ای را شناسایی کرد که پایگاه داده های اس کیو ال مایکروسافت را تخریب کرده و آیتمهایی را با ارزشهای تصادفی جایگزین می کند، این بدافزار پایگاه داده های تجاری را هدف گرفته است.

شرکت امنیت رایانه سیمانتک به بخشهای تجاری در رابطه با بدافزار جدیدی هشدار داد که می تواند پایگاه داده ای شرکت را با دستکاری اطلاعات داخل آن را از بین ببرد.

این کرم که ناریلام نامگذاری شده پایگاه های داده ای اس کیو ال مایکروسافت را هدف گرفت و زمانی که داخل این پایگاه داده ای شد، کلمات خاصی را جستجو کرده و آنها را با ارزشهای تصادفی جایگزین کرده و یا جدولهای خاصی را حذف می کرد.

گفته می شود که اکثریت افرادی که دستگاه های آنها به این ویروس آلوده شده کاربران شرکتها و بخش تجاری هستند. بدافزار ناریلام که بدافزار استاکس‌نت را به ذهن تداعی می کند، برخی سازمانهای ایران، بریتانیا و آمریکا را هدف گرفته است.

ایران هدف حمله جاسوس افزار مینی فلیم

متخصصان شرکت امنیتی و ضد ویروس کسپرسکی یک جاسوس افزار جدیدی را به نام مینی فلیم (شعله کوچک) کشف کردند که منبع آن به همان نقطه ای نسبت داده شده که فلیم از آنجا آمده بود.

این ابراز جاسوسی توسط خالقان آن "جان" نام گرفته اما محققان کسپرسکی آن را مینی فلیم یا SPE نامیدند که از همان کارخانه بدافزار سازی آمده است که استاکس‌نت، دوکو، و گوس تولید شده است.

براساس گزارش کسپرسکی، تمام این بدافزارهای نام برده به علاوه "مینی فلیم" کار سازمانهای اطلاعاتی آمریکا است و درمرحله اول همه آنها سیستمهای کامپیوتری خاورمیانه راهدف گرفته اند و مینی فلیم نیز از این قائده مستثنی نیست؛ همچنین موارد مختلفی از این حملات در کشورهای ایران، کویت و قطر گزارش شده است.

جریمه 163 میلیون دلاری فروشنده آنتی ویروس تقلبی

دادگاه فدرال آمریکا در سالی که گذشت زنی را که براساس قوانین کمیسیون فدرال تجارت اقدام به اجرای یک باج افزار کرده و در پی آن یک میلیون نفر در شش کشور مجبور به خرید یک نرم افزار امنیتی قلابی شدند را به پرداخت 163 میلیون دلار متهم کرد.

یک دادگاه فدرال براساس شکایت کمیسیون فدرال تجارت این زن را که اقدام به راه اندازی این باج افزار برای فروش نرم افزار قلابی امنیتی خود کرده بود را متهم کرد. در این حکم آمده است که کریستی راس، متهم، باید به طور موقت زندانی شده و از فروش نرم افزار رایانه ای و دخالت در کاربر نرم افزار توسط مشتری به هر شکلی دور بماند.

این نرم افزار تقلبی که معمولا از آن با عنوان باج افزار یا ضد ویروس قلابی یاد می شود یک نوع نرم افزار باج گیری برای فریب دادن کاربر است.

افزایش بدافزارهای سیستمهای اندروید و iOS

کارشناسان امنیتی اعلام کردند: دستگاه هایی که از سیتم عامل های آندروید و iOS برخوردارند به قربانیان جدید مجرمان سایبر تبدیل شده که امنیت آنها را با بدافزارها تهدید می کنند.

مک افی (McAfee) شرکت امنیتی رایانه اظهار داشت امروز بیش از هر زمان دیگری طی چهار سال گذشته تلفن های همراه هوشمند و تبلت ها مورد حمله انواع کرمها، ویروسها بوت نتها ، تروجانها و اسپمها قرار گرفته اند.

قطع شدن دسترسی 350 هزار کاربر به اینترنت

ویروس DNS Changer باعث شد حداکثر 350 هزار کاربر نتوانند به شبکه جهانی وصل شوند.

این ویروس که اولین بار در سال 2007 فعال شده بود، با تغییر کامل تنظیمات مربوط به سیستم‌های نام‌گذاری فضاها و وب‌سایت‌های اینترنتی (DNS)، دسترسی به صفحات اینترنتی را به صفحه‌ها و سرورهای آلوده و حاوی بدافزار هدایت می‌کند. بنابراین کاربران آلوده به این ویروس به طور خودکار به سرورهایی هدایت می‌شوند که کاملاً تحت کنترل هکرها و مجرمان اینترنتی قرار دارند. پلیس فدرال وب سایتی طراحی کرد که کاربران با مراجعه به آن می‌توانستند متوجه شوند آیا کامپیوترشان به این ویروس آلوده شده یا نه.

گفته شده افرادی که در طراحی و فعال سازی این ویروس دخالت داشته‌اند از این کلاهبرداری و خرابکاری اینترنتی حدود 9 میلیون پوند سود اقتصادی برده باشند.

ابداع یو اس بی ویروس کش

پاک کردن ویروسها از رایانه ممکن است در اکثر مواقع کار دشواری باشد، اما اکنون با ابداع یک یو اس بی می‌توان به مثابه حرفه‌ای‌های این عرصه تنها با اتصال یو اس بی به پورت خود اقدام به ویروس کشی کنید.

یو اس بی ویروس کش با نام " فیکس می استیک" (FixMeStick) می تواند فایلهایی که سایر برنامه های ضد ویروس از دست داده اند را با یک نرم افزار قدرتمند ضد ویروس که معمولا توسط تکنسینهای رایانه استفاده می شود را پیدا کند.

تنها کاری که کاربر باید انجام دهد این است که یو اس بی را به پورت ویژه خود در رایانه متصل کند و یو اس بی خودکار وارد عمل می شود.

باز شدن پای ویروس ها به رایانه های مک

از دیرباز اعتقاد بر این بود که رایانه های "مک" نسبت به رایانه های شخصی برپایه ویندوز از ضریب ایمنی بالایی برخوردارند و در شرایطی که ویندوزها همواره مورد هجوم مداوم ویروسها قرار گرفته اند "مک ها" از یک دیوار محکم در مقابل این حملات برخوردار بوده اند.

شرکت روسی آنتی ویروسهای "دکتر وب" اعلام کرد که ویروسی با عنوان "فلش بک" به 600 هزار رایانه "مک" آسیب رسانده است.

در پی اعلام این خبر، اپل کد امنیتی بستن این حفره را عرضه کرد. این ویروس تا حدی خطرناک به نظر می رسد که حتی 274 مکینتاش متصل به شبکه در مقر مرکزی اپل در کوپرتینوی کالیفرنیا نیز آلوده شده اند. "فلش بک" با استفاده از یک نفوذپذیری "جاوا" در وب مرورگرهای سافاری به سیستم عامل مک حمله می کند. در ابتدا، این کرم با پنهان شدن در نرم افزار "فلش" به رایانه های مک راه یافت اما در ادامه هجوم خود، راهها و متدهای تهاجمی تری را برای انجام حملات خود پیدا کرد.