همه چیز درباره ویروس‌ها، کرم‌ها، اسب‌های تروا و فراتر از آن

« بخش آخر »

کلیه حقوق این مقاله متعلق به سایت امنیت وب و مترجم آن می باشد و هر گونه برداشت از آن فقط با ذکر نام سایت و نام نویسنده مجاز می باشد.

مترجم : رضا مددی / rzmadadi@yahoo.com

منبع : www.Sophos.com

تاریخ : ۲۳ اردیبهشت ۱۳۸۳

در صورتی که شما :

- یک مدیر شبکه هستید،
- فردی هستید که با دوستان خود دیسک مبادله می‌کند،
- از شبکه‌های محل کار خود استفاده می‌کنید،
- و یا فقط خواننده نامه‌های الکترونیکی هستید،

بدانید که این مطلب برای شماست!

ما حقایق را در باره ویروس‌های کامپیوتری بطور ساده و با زبانی قابل فهم برای شما بیان می‌کنیم.

فهرست مطالب

بخش اول

- چرا ویروس‌ها مهم هستند؟
- ویروس ها، اسب‌های تروا و کرم‌ها
- تعریفی ساده از ویروس، اسب تروا، کرم
- ویروس چیست؟
- ویروس چگونه بر روی کامپیوتر تاثیر می‌گذارد؟
- اسب‌های تروا
- کرم‌ها
- ویروس‌ها چه کارهایی می‌توانند انجام دهند؟
- خطر مربوط به ویروس‌ها در چه جاهایی وجود دارد؟
- جلوگیری کردن از ویروس‌ها
- ویروس‌های سکتور بوت
- ویروس‌های انگلی
- ویروس‌های ماکرو (کلان دستور)

بخش دوم

- نرم‌افزار ضد ویروس
- پویشگرها
- Checksummer ها
- نرم‌افزارهای کاشف (Heuristic)
- هزینه‌های پنهانی ویروس‌ها
- ویروس‌نویسان چه کسانی هستند؟
- آیا نوشتن ویروس همیشه نادرست است؟
- ویروس‌های گولزن (Hoax ها)
- Hoax ها چیستند؟
- چرا Hoax ها یک معضل هستند؟
- چه کارهایی را در مورد Hoax ها می‌توان انجام داد؟
- تاریخچه مختصری از ویروس‌ها
- ۱۰ ویروس برتر

بخش سوم

- پست الکترونیک
- آیا به صرف خواندن نامه، ویروسی می‌شویم؟
- ویروس‌هایی که بطور خودکار از طریق نامه‌ها گسترش می‌یابند
- خطرات فایل‌های پیوندی
- چگونه ویروس‌های پستی را متوقف کنیم؟
- اینترنت
- کلیک کردن و آلوده شدن؟
- آیا به صرف دیدن وب‌سایت‌ها، ویروسی می‌شویم؟
- دستورات برنامه‌نویسی وب‌سایت‌ها
- اسب‌های تروای «در پشتی» و اینترنت
- آیا کوکی‌ها خطرناک هستند؟
- حمله‌ها به سوی وب‌سرورها
- امنیت در شبکه

بخش چهارم

- تلفن‌های موبایل و کامپیوترهای کف‌دستی
- آیا ویروس‌های موبایل هم وجود دارند؟
- تلفن‌های WAP و ویروس‌ها
- خطرات آتی برای WAP
- سیستم‌عامل‌های کامپیوترهای کف‌دستی
- ویروس‌ها برای یخچال‌ها؟
- چگونگی محافظت از ابزارهای متحرک (Mobile)
- ده مرحله برای ایجاد امنیت در کار با کامپیوتر
- لینک‌های مفید

بخش چهارم

تلفن‌های موبایل و کامپیوترهای کف‌دستی

در دهه گذشته، جهان (منظور شبکه جهان گستر وب است) به کامپیوترهای شما آورده شد و این دهه همین کار برای تلفن‌های همراه (موبایل) شما انجام خواهد شد. به این ترتیب شما به کمک نسل‌های جدید تلفن‌های همراه همواره قادر خواهید بود تا به سایت‌ها و خدمات اینترنتی و همچنین فن‌آوری روز که به سرعت در حال پیشرفت است، دستیابی داشته باشید. اما همانطور که انتقال اطلاعات – حتی به صورت متحرک – آسانتر شده است، این امکان هم وجود دارد که خطرات امنیتی جدیدی هم بروز کند.

آیا ویروس‌های موبایل هم وجود دارند؟

در زمانی که مقاله مزبور نگارش می‌شد، علیرغم شایعات رسانه‌ای و Hoax ها، ویروسی که بتواند تلفن‌های موبایل را آلوده کند وجود نداشت.

ویروس‌هایی وجود داشته‌اند که پیغام‌هایی را برای تلفن‌ها ارسال می‌کرده‌اند. برای مثال، کرم VBS/Time-A که خود را از طریق پست الکترونیک گسترش می‌دهد، از مودم برای فرستادن پیام‌های متنی (SMS) به شماره‌های منتخبی از تلفن‌های همراه استفاده می‌کند. ویروس معروف Love Bug هم قادر بود متن‌هایی را به دستگاه‌های فکس و تلفن‌های همراه ارسال کند. با همه اینها، این ویروس‌ها نمی‌توانستند تلفن‌های همراه را آلوده کرده یا به آنها صدمه‌ای وارد کنند.

اما همانطور که تلفن‌های همراه مدام در حال پیشرفت هستند، بقیه چیزها هم تغییر می‌کنند!

آیا ابزارهای همراه، اطلاعات را به خطر می اندازند؟

ابزارهای همراه (متحرک) به عنوان مکانی برای نگهداشتن اطلاعات از امنیت کافی (به اندازه کامپیوترها) برخوردار نیستند چرا که :

- ممکن است براحتی مفقود شده یا مورد سرقت واقع شوند.
- قطع شدن انرژی منبع تغذیه آنها می‌تواند باعث از دست رفتن اطلاعات شود.
- در آنها اطلاعات دارای پشتیبان نیستند.

به همان اندازه که ابزارهای همراه پیچیده‌تر می‌شوند می‌توانند در مقابل ویروس‌ها و یا هکرها هم آسیب‌پذیرتر شوند.

تلفن‌های WAP و ویروس‌ها

تکنولوژی جدیدی که در این زمینه بیشترین صحبت‌ها در مورد آن صورت می‌گیرد، تکنولوژی WAP(Wireless Application Protocol) است.

سیستم WAP اطلاعات و خدمات اینترنتی را برای تلفن‌های همراه و خدمات‌دهندگان فراهم می‌کند. این سیستم بر پایه مدلی شبیه به مدل ارتباطات وب قرار گرفته و در آن مرورگر تلفن شما فقط دستورات منتشر شده توسط یک سرور مرکزی را اجرا خواهد کردکه در اینصورت تواناییهای ویروس‌ها بسیار کاهش خواهد یافت.

ویروس می‌تواند خود سرور را آلوده کند، اما بازهم از شانس کمی برای گسترش خود و یا آلوده کردن کاربران برخوردار خواهد بود چرا که :

اولا در یک سیستم WAP جایی برای آنکه یک ویروس بتواند خود را کپی کند یا بتواند در آنجا به زندگی خود ادامه دهد وجود ندارد. برخلاف کامپیوترها، تلفن‌های WAP برنامه‌ها را ذخیره نمی‌کنند. این تلفن‌ها کدهای مورد نیاز خود را Download کرده و هیچ نسخه‌ای از آنها را نگهداری نمی‌کنند مگر به صورت موقت در حافظه Cache مرورگر.

ثانیا ویروس این امکان را هم ندارد که از کاربری به کاربر دیگر سرایت کند، زیرا هیچ ارتباطی بین تلفن‌های مشتریان وجود ندارد.

در نظریه‌ها، یک «ویروس» می‌تواند باعث توزیع لینک‌هایی به سایت‌های مخرب WAP شده و یا اینکه کاربران را برای استفاده از برنامه‌های آسیب‌آور فریب دهد، اما اینکار هم مستلزم آن است که ویروس کدهای اجرایی سرور را برای اتصال به تلفن‌های WAP در اختیار داشته باشد.

واژه‌نامه

WAP (Wireless Application Protocol)
پروتکل نقل و انتقال برنامه‌های بیسیم

WML (Wireless Markup Language)
زبان نشانه‌گذاری بیسیم (مانند HTML یا همان زبان نشانه‌گذاری فرامتن)

WML Script : زبانی برنامه‌نویسی شبیه به جاوا اسکریپت

Cards : صفحه‌های طراحی شده با WML

Deck : بـه مجموعـه‌ای از صفحات مرتبط با هم گویند که یک مرورگر WAP بدون نیاز به Download های اضافه، می‌تواند به همه آنها دسترسی داشته باشد.

خطرات آتی برای WAP

سیسـتم WAP نسـخه‌ای از HTTP - پـروتکل مـورد اسـتفاده برای نقل و انتقال صـفحات فرامتن وب - را مورد استفاده قرار داده که می‌تواند مندرجاتی بسیار پیچیده‌تر از آنچه که در حال حاضر توسط مرورگرهای WAP پردازش می‌شود را نقل و انتقال کند.

ممکن است نسل‌های آینده مرورگرها بتوانند فایل‌هایی را Download کنند - مانند اسناد - که شامل ویروس‌های نوع ماکرو باشند.

بـنابر عملکرد سیستم WAP، در آینده‌ای نزدیک سرورها قادر خواهند بود تا خود، اطلاعاتـی را به تلفن‌های همراه وارد کنند. همانطور که با این تکنولوژی می‌توان کاربران را از اطلاعات روز (مانند برآیندهای مالی یا نتایج ورزشی) و یا نامه‌های جدیدشان باخبر کرد، تکـنولوژی «فشـار (اطلاعـات)» همچنیـن قادر خواهد بود تا اطلاعاتی را بدون نیاز به هیچ اقدامی از جانب شما بر روی حافظه Cache ذخیره کند.

کدهای مخرب می‌توانند با در اختیار گرفتن این سیستم باعث گسترش خود شوند.

مشکلات بالقوه دیگری نیز وجود دارد. برای نمونه سایت‌های مخرب WAP که خود را بـه عـنوان خدمـات‌دهندگانـی مفید معرفی می‌کنند، می‌توانند باعث از کار افتادن مرورگر کاربر و یا پر شدن حافظه شوند.

واژه‌نامه

XML (eXtensible Markup Language) : زبـان نشـانه‌گذاری قابل توسعه که برای استفاده در شبکه جهان‌گستر وب توصیه می‌شود.

WTLS (Wireless Transport Layer Security) : امنیـت لایـه انـتقال بیسیم، متد رمزنگاری که در شبکه تلفن‌های همراه مورد استفاده قرار می‌گیرد.

سیستم‌عامل‌های کامپیوترهای کف‌دستی

کامپـیوترهای کـف دسـتی و دسـتیاران شخصی دیجیتال (PDA) با احتمالی زیاد، باعث خلق فرصت‌های جدیدی برای ویروس‌ها در آینده‌ای بسیار نزدیک خواهند شد.

کامپـیوترهای کف‌دستی (Palmtop) و PDA ها از سیستم‌عامل‌هایی که مخصوص آنهـا نوشته شده و یا برای کار با آنها تغییر مقیاس یافته‌اند - مانند EPOC ، PalmOS و

PocketPC (و سابقا ویندوز CE) - استفاده می‌کنند. چنین سیستم‌هایی در نهایت قادر خواهند بود تا نسخه‌هایی از برنامه‌های رایج کامپیوترهای رومیزی را مورد استفاده قرار دهند. این کار باعث خواهد شد تا آنها هم همانند کامپیوترهای رومیزی در برابر کدهای مخرب آسیب‌پذیر شوند. از اوایل سال ۲۰۰۱ همواره ویروس‌هایی وجود داشته‌اند که سیستم‌های کف‌دستی را آلوده کرده‌اند.

همچنین کامپیوترهای کف‌دستی برای هماهنگ کردن اطلاعات خود با کامپیوترهای رومیزی (اطلاعاتی مانند اطلاعات دفترچه‌های آدرس یا تاریخ قرارها یا ...)، مرتبا در حال تماس با منزل یا محل کار هستند. هماهنگ سازی اطلاعات به این شکل، به ویروس‌ها اجازه می‌دهند تا به سادگی منتشر شوند.

هنوز هیچکس نمی‌داند که در آینده کدام یک موفق‌تر خواهد بود : کامپیوترهای متحرک یا تلفن‌های همراه هوشمند، اما هر اتفاقی هم که رخ دهد، خطرات امنیتی، همگام با پیشرفت ارتباطات کامپیوترهای متحرک، افزایش خواهند یافت.

واژه‌نامه

EPOC : سیستم‌عاملی برای کامپیوترهای کف‌دستی

PDA : دستیار شخصی دیجیتال (نوعی کامپیوتر کف‌دستی)

PalmOS : سیستم‌عاملی برای کامپیوترهای کف‌دستی

PocketPC : سیستم‌عامل شرکت مایکروسافت برای کامپیوترهای کف‌دستی (بعد از سیستم‌عامل ویندوز CE)

UPNP (Universal Plug and Play) : سیستم نصب و استفاده عمومی، سیستمی از مایکروسافت برای فعال کردن ارتباطات بین کامپیوترهای متحرک و سایر ابزار

ویروس‌ها برای یخچال‌ها؟

ابزارهای گوناگون بسیاری در حال حاضر از طریق رابط‌های مادون قرمز یا امواج رادیویی کم‌قدرت با یکدیگر به صحبت می‌پردازند (در ارتباط هستند) که این کار خطرات امنیتی جدیدی را پدید می‌آورد.

تکنولوژی بلوتوث (Bluetooth) استانداردی برای برقراری ارتباطات اطلاعاتی به کمک امواج رادیویی کم‌قدرت در فاصله‌های بسیار کوتاه – در حدود ۱۰ متر – می‌باشد. کامپیوترها، تلفن‌های همراه، دستگاه‌های فکس و حتی لوازم خانگی مانند ضبط‌های تصویری و یا یخچال‌ها می‌توانند از تکنولوژی بلوتوث برای پی بردن به اینکه چه وسایلی

در نزدیکیشان چه خدماتی را ارائه می‌کنند، استفاده کرده و ارتباطات ناپیدایی را با آنها برقرار کنند.

نرم‌افزارهایی که بتوانند سیستم بلوتوث را مورد استفاده قرار دهند، بوجود آمده‌اند. برای نمونه تکنولوژی Sun's Jini به ابزارها این امکان را می‌دهد که بتوانند ارتباط‌ها را شکل داده، به طور خودکار کدهای جاوا را مبادله کرده و کنترل راه‌دوری از سرویس‌ها فراهم کنند. خطری که در اینجا وجود دارد آن است که یک کاربر غیرمجاز یا کدی مخرب بتواند با سوء استفاده از سیستم بلوتوث برای مختل کردن کار سرویس‌ها اقدام کنند.

بلوتوث و Jini طوری طراحی شده‌اند که تضمین دهند فقط کدهای امن از منابع شناخته شده می‌توانند دستورات حساس را رد و بدل کنند. با توجه به این اقدامات بعید به نظر می‌رسد که ویروسی شیوع پیدا کند، اما اگر ویروسی بتواند سیستم‌های امنیتی را دور بزند، قدرت کمی برای متوقف کردن آن وجود خواهد داشت.

واژه‌نامه

3G (Third generation) : نسل سوم، فن‌آوری ابزارهای متحرک

Bluetooth : ارتباطات اطلاعاتی با امواج رادیویی کوتاه برد

Jini : فن‌آوری تبادل کدهای جاوا بین ابزارها

MExE (Mobile station application Execution Environment) : جانشین احتمالی WAP که امکان download کردن کدهای جاوا در تلفن‌ها را برای فراهم‌کنندگان خدمات ایجاد می‌کند.

چگونگی محافظت از ابزارهای متحرک (Mobile)

با تکامل فن‌آوری PDA و ابزارهای متحرک، اقدامات امنیتی هم باید در حد مطلوبی نگاه داشته شوند. مهمترین این موارد، جایی است که شما در آنجا از اقدامات ضد ویروسی استفاده می‌کنید.

پویش در دروازه نقل و انتقال اطلاعات یا در زمان انتقال آنها

در آینده‌ای نزدیک، شاید بهترین راه محافظت از ابزارهای متحرک، بررسی کردن اطلاعات به هنگام دریافت یا ارسال آنها می‌باشد. برای نمونه در تلفن‌های همراه دروازه WAP شاید مکانی مناسب برای نصب ضد ویروس‌ها باشد.

تمام ارتباطات به صورت غیر رمز از این دروازه عبور می‌کنند، بنابراین این مکان می‌تواند فرصت ایده‌آلی را برای انجام پویش‌های ضد ویروسی فراهم کند.

در کامپیوترهای کف‌دستی، شما می‌توانید در زمان هماهنگ سازی اطلاعات بین این کامپیوترها و کامپیوترهای سنتی از اعمال محافظتی ضد ویروسی استفاده کنید. در این موارد، برای جلوگیری از کمبود قدرت یا حافظه کامپیوترهای کف‌دستی، کامپیوترهای سنتی می‌توانند قسمت عمده‌ای از اجرای نرم‌افزار ضدویروس را بر عهده بگیرند.

پویش ویروس در ابزارهای متحرک

از آنجایی که ابزارهای متحرک هر چه بیش از پیش به هم متصل می‌شوند، نظم دادن انتقال اطلاعات در یک نقطه مرکزی مشکل‌تر از پیش خواهد شد. راه حل این مشکل قرار دادن نرم‌افزار ضد ویروسی بر روی هر یک خواهد بود - البته در صورتیکه آنها از حافظه و قدرت پردازش کافی برخوردار باشند.

ده مرحله برای ایجاد امنیت در مقابله با ویروسها و کرمها

غیر از استفاده از نرم‌افزارهای ضد ویروسی، اقدامات ساده بسیار زیادی وجود دارند که شما می‌توانید از آنها برای کمک به محافظت از خود و شرکتتان در مقابل ویروس‌ها استفاده کنید.

در این قسمت، ده مورد از برترین موارد برای «کار بدون مشکل با کامپیوتر» آورده شده است.

روش‌های ایجاد امنیت در کار با کامپیوتر

۱- از اسناد در قالب‌های doc. و xls. استفاده نکنید.

فایل‌های خود در برنامه Word را با فرمت RTF(Rich Text Format) و در برنامه Excel با فرمت CSV(Comma Separated Values) ذخیره کنید. فرمت‌های ذکر شده از برنامه‌نویسی ماکرو پشتیبانی نمی‌کنند، در نتیجه می‌توانند از گسترش ویروس‌های ماکرو که به مراتب از عمومی‌ترین تهدیدات ویروسی به شمار می‌آیند جلوگیری کنند. به افراد دیگر هم بگویید که فایل‌هایشان را به جای فرمت‌های doc. یا xls. با فرمت‌های rtf. یا csv. برای شما تهیه کنند.

با این حال باز هم مواظب باشید، چرا که بعضی ویروس‌های ماکرو از عمل FileSaveAs RTF جلوگیری کرده، فایل را باقالب doc. ذخیره کرده اما از پسوند rtf. برای آن استفاده می‌کنند. برای بدست آوردن امنیتی مطلق می‌توانید از فایل‌های فقط متنی (text) استفاده کنید.

۲- برنامه‌ها یا اسناد غیر درخواستی را اجرا نکنید.

اگر از پاک بودن (عاری بودن از ویروس) چیزی مطمئن نیستید، آن را ویروسی فرض کنید. به افراد مشغول در سازمانتان سفارش کنید تا برنامه‌ها یا اسناد غیر مجاز (بدون منبع معتبر یا مشکوک) که Screen Saver ها و فایل‌های طنز هم شامل آنها می‌شوند

را از اینترنت دریافت نکنند. روشی را پیاده کنید که طبق آن قبل از استفاده از هر برنامه‌ای، مجوزی توسط یک مدیر IT برای آن صادر شده و پاک بودن آن بررسی شود.

۳- تمام اخطارهای دریافتی را فقط برای فرد مورد تایید ارسال کنید.

Hoax ها، خود به اندازه ویروس‌ها از مشکلات بزرگ محسوب می‌شوند. به کاربران بگویید که هشدارهای ویروسی را به هیچ یک از دوستان، همدانشگاهیان و یا هر فرد دیگری که آدرسش را دارند، ارسال نکنند. سیاستی برای شرکت خود اتخاذ کنید بطوری که تمام هشدارها برای شخص یا قسمت مشخصی از شرکت ارسال شود.

۴- در دروازه ورود، فایل‌های با پسوند مضاعف را بلوکه کنید.

بعضی ویروس‌ها برنامه بودن خود را با استفاده از «پسوند مضاعف» بعد از نامشان می‌پوشانند مانند txt.vbs. . چنین فایل‌هایی را در دروازه ورود بلوکه کنید.

برای مثال شاید فایلهایی مانند Love-Letter-For-You.TXT.VBS یا AnnaKournikova.JPG.VBS در اولین نظر یک فایل متنی یا تصویری بی‌ضرر به نظر برسند، در حالیکه هر دو از ویروس‌های معروف می‌باشند. شما باید هر فایلی با پسوند مضاعف را در دروازه پست الکترونیک بلوکه کنید.

۵- انواع ناخواسته فایل‌ها را در دروازه پست الکترونیک بلوکه کنید.

امروزه بسیاری از فایل‌ها از فایل‌های با نوع VBS (Visual Basic Script) و SHS (Windows scrap object) برای انتشار خود استفاده می‌کنند. بعید به نظر می‌رسد که سازمان شما به دریافت چنین انواعی از فایل‌ها نیاز داشته باشد، بنابراین آنها را در همان دروازه پست الکترونیک بلوکه کنید.

۶- ترتیب درایوهای بوت را برای کامپیوترتان تغییر دهید.

بسیاری از کامپیوترها با اینکه حتما از دیسک سخت بوت می‌شوند، اما تنظیمشان طوری است که ابتدا سعی می‌کنند فایل‌های سیستمی را از فلاپی بخوانند و در صورت عدم موفقیت به دیسک سخت رجوع کنند. مسؤول مربوط به امور IT در شرکتتان باید تنظیمات CMOS را طوری تغییر دهد که کامپیوتر به طور پیش‌فرض ابتدا از دیسک سخت بوت شود. در این صورت حتی اگر دیسکت آلوده‌ای در درایو کامپیوتر جا مانده باشد، در راه‌اندازی بعدی کامپیوتر، آن را از طریق سکتور بوت خود آلوده نخواهد کرد.

در هر زمانی که نیاز به بوت کردن کامپیوتر از فلاپی داشته باشید، می‌توانید تنظیمات را به حالت قبل بازگردانید.

۷- قبل از اینکه دیسکتی را به کاربری دهید، آن را در حالت «قفل نوشتن» قرار دهید.

یک فلاپی که در مقابل نوشتن اطلاعات قفل شده باشد، آلوده نخواهد شد.

۸- اطلاعیه‌های امنیتی شرکت‌های نرم‌افزاری را پیگیری کنید.

گوش به زنگ اخبارهای امنیتی باشید و فایل‌های اصلاحیه (Patch) را برای محافظت در مقابل تهدیدات ویروس‌های جدید دریافت کنید.

برای اطلاعات بیشتر قسمت « لینک‌های مفید» را مطالعه کنید.

۹- در یکی از سرویس‌های هشدار دهنده ویروس عضو شوید.

یک سرویس اعلام خطر می‌تواند شما را از به وجود آمدن ویروس‌های جدید باخبر کرده و شناسه‌های ویروسی را به شما ارائه کند بطوری که نرم‌افزار ضد ویروس شما قادر به شناسایی آنها شود.

برای عضویت در یکی از این سرویس‌ها می‌توانید به آدرس www.sophos.com/virusinfo/notifications مراجعه کنید.

۱۰- مرتبا از تمام برنامه‌ها و اطلاعاتتان پشتیبان تهیه کنید.

در صورتی که توسط ویروسی آلوده شوید، قادر خواهید بود تا تمام برنامه‌ها و اطلاعات از دست رفته را بازگردانید.

لینک‌های مفید

برای بدست آوردن اطلاعات بیشتر می‌توانید به آدرس‌های زیر مراجعه کنید.

اطلاعاتی راجع به ویروس‌ها

www.sophos.com/virusinfo/analyses

ویروس‌های ترساننده و Hoax ها

www.sophos.com/virusinfo/hoaxes
www.vmyths.com

اطلاع‌رسانی خودکار در مورد ویروس‌های جدید

www.sophos.com/virusinfo/notifications

اطلاعیه‌های امنیتی مایکروسافت

www.microsoft.com/security

مرکز امنیتی نت‌اسکیپ

www.netscape.com/security

اطلاعات امنیتی جاوا

www.java.sun.com/security

سازمان WildList

www.wildList.org

اطلاعیه‌های مربوط به ویروس

www.virusbtn.com