تحقیقی در مورد ویروس و راههای از بین بردن آن

حجم عظیم ویروس ها، کرم ها، ایرادات نرم افزارها و تهدیدهای ناشی از آنها، نرم افزارهـای ضـدویروس را تبـدیل بـه یکـی از ابزارهای لازم برای همه کامپیوترها نموده است. در صورت آلوده شدن یک کامپیوتر به ویروس بسته بـه نـوع آن ممکـن اسـت مصائب مختلفی برای سیستم کامپیوتری بوجود آید که در پاره ای موارد جبران آن ها هزینه هـای زیـادی را تحمیـل مـی کنـد. آسیب های بعضی از ویروس ها به گونه ای است که آثار سوء آن ها را به هیچ وجه نمی توان از بین برد. مستقل از نوع ویروسی که باید با آن مقابله شود نیاز به برنامه های ضد ویروس همواره وجود دارد و در شرایطی که محصـولات ضـد ویـروس متنـوعی تولید شده اند، انتخاب نرم افزار مناسب دغدغه کاربران می باشد.

این قسمت ضمن معرفی انواع ویروس ها، نحوه عمل کرد برنامه های ضدویروس و انـواع ویـروس هـایی کـه ضـدویروس هـا شناسایی و پاکسازی می کنند را معرفی می کند. همچنین اطلاعاتی که برای انتخاب ابزار مناسب لازم است بیان شده و تعدادی از برنامه های ضد ویروس با هم مقایسه خواهند شد.

ویروس چیست؟

ویروس های کامپیوتری برنامه هایی هستند که مشابه ویروس های بیولوژیک گسترش یافته و پس از وارد شدن بـه کـامپیوتر اقدامات غیرمنتظره ای را انجام می دهند. با وجودی که همه ویروس ها خطرناک نیستند، ولی بسیاری از آنها بـا هـدف تخریـب انواع مشخصی از فایل ها، برنامه های کاربردی و یا سیستم های عامل نوشته شده اند.

ویروس ها هم مشابه همه برنامه های دیگر از منابع سیستم مانند حافظه و فضای دیسک سخت، توان پردازنده مرکزی و سـایر منابع بهره می گیرند و می توانند اعمال خطرناکی را انجام دهند به عنوان مثال فایل های روی دیسک را پاک کـرده و یـا کـل دیسک سخت را فرمت کنند. همچنین یک ویروس می تواند مجوز دسترسی به دستگاه را از طریق شبکه و بدون احـراز هویـت فراهم آورد.

برای اولین بار در سال ۱۹۸۴ واژه «ویروس» در این معنا توسط فرد کوهن در متون آکادمیک مورد استفاده قرار گرفـت. در ایـن مقاله که «آزمایشاتی با ویروس های کامپیوتری» نام داشت نویسنده دسته ای خاص از برنامه ها را ویـروس نامیـده و ایـن نـام

گذاری را به لئونارد آدلمن نسبت داده است. البته قبل از این زمان ویروس ها در متن داستان های عملی و تخیلی ظاهر شده بودند.

انواع ویروس

انواع ویروس های رایج را می توان به دسته های زیر تقسیم بندی نمود:

boot sector :

boot sector اولین Sector بر روی فلاپی و یا دیسک سخت کامپیوتر است. در این قطاع کدهای اجرایی ذخیره شده اند که فعالیت کامپیوتر با استفاده از آنها انجام می شود. با توجه به اینکه در هر بار بالا آمدن کامپیوتر Boot sector مورد ارجاع قرار می گیرد، و با هر بار تغییر پیکربندی کامپیوتر محتوای boot sector هم مجددا نوشته می شود، لذا این قطاع مکانی بسیار آسیب پذیر در برابر حملات ویروس ها می باشد.

این نوع ویروس ها از طریق فلاپی هایی که قطاع boot آلوده دارند انتشار می یابند. Boot sector دیسک سخت کامپیوتری که آلوده شود توسط ویروس آلوده شده و هر بار که کامپیوتر روشن می شود، ویروس خود را در حافظه بار کرده و منتظر فرصتی برای آلوده کردن فلاپی ها می ماند تا بتواند خود را منتشر کرده و دستگاه های دیگری را نیز آلوده نماید. این گونه ویروس ها می توانند به گونه ای عمل کنند که تا زمانی که دستگاه آلوده است امکان boot کردن کامپیوتر از روی دیسک سخت از بین برود.

این ویروس ها بعد از نوشتن بر روی متن اصلی boot سعی می کنند کد اصلی را به قطاعی دیگر بر روی دیسک منتقل کرده و آن قطاع را به عنوان یک قطاع خراب (Bad Sector) علامت گذاری می کند.

Macro viruses:

این نوع ویروس ها مستقیما برنامه ها را آلوده نمی کنند. هدف این دسته از ویروس ها فایل های تولید شده توسط برنامه هایی است که از زبان های برنامه نویسی ماکرویی مانند مستندات Exel یا Word استفاده می کنند. ویروس های ماکرو از طریق دیسک ها، شبکه و یا فایل های پیوست شده با نامه های الکترونیکی قابل گسترش می باشد.

ویروس تنها در هنگامی امکان فعال شدن را دارد که فایل آلوده باز شود، در این صورت ویروس شروع به گسترش خود در کامپیوتر نموده و سایر فایل های موجود را نیز آلوده می نماید. انتقال این فایل ها به کامپیوتر های دیگر و یا اشتراک فایل بین دستگاه های مختلف باعث گسترش آلودگی به این ویروس ها می شود.

File infecting viruses:

فایل های اجرایی (فایل های با پسوند .exe و .com) را آلوده نموده و همزمان با اجرای این برنامه ها خود را در حافظه دستگاه بار نموده و شروع به گسترش خود و آلوده کردن سایر فایل های اجرایی سیستم می نمایند. بعضی از نمونه های این ویروس ها متن مورد نظر خود را به جای متن فایل اجرایی قرار می دهند.

ویروس های چندریخت(Polymorphic):

این ویروس ها در هر فایل آلوده به شکلی ظاهر می شوند. با توجه به اینکه از الگوریتم های کدگذاری استفاده کرده و ردپای خود را پاک می کنند، آشکارسازی و تشخیص این گونه ویروس ها دشوار است.

ویروس های مخفی:

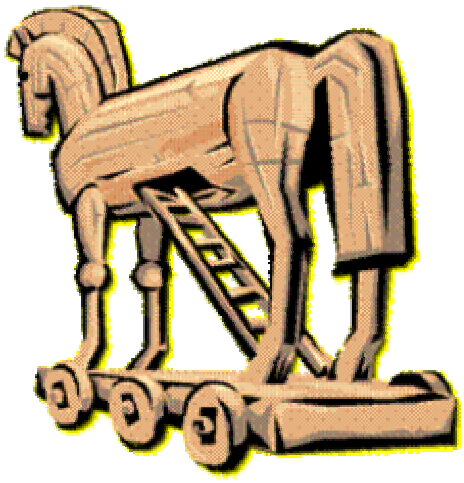
این ویروس ها سعی می کنند خود را از سیستم عامل و نرم افزارهای ضدویروس مخفی نگه دارند. برای این کار ویروس در حافظه مقیم شده و حائل دسترسی به سیستم عامل می شود. در این صورت ویروس کلیه درخواست هایی که نرم افزار ضدویروس به سیستم عامل می دهد را دریافت می کند. به این ترتیب نرم افزارهای ضدویروس هم فریب خورده و این تصور به وجود می آید که هیچ ویروسی در کامپیوتر وجود ندارد. این ویروس ها کاربر را هم فریب داده و استفاده از حافظه را به صورت مخفیانه انجام می دهند.

ویروس های چندبخشی

رایج ترین انواع این ویروس ها ترکیبی از ویروس های boot sector و file infecting می باشد. ترکیب انواع دیگر ویروس ها هم امکان پذیر است.

سایر برنامه های مختل کننده امنیت:

برخی از محققین اسب های تروا(Trojan)، کرم ها و بمب های منطقی را در دسته ویروس ها قرار نمی دهند ولی واقعیت این است که این برنامه ها هم بسیار خطرناک بوده و می توانند خساراتی جدی به سیستم های کامپیوتری وارد نمایند.



اسب های تروا تظاهر می کنند که کاری خاص را انجام می دهند ولی در عمل برای هدف دیگری ساخته شده اند، به عنوان مثال برنامه ای که وانمود می کند که یک بازی است ولی در واقع اجازه دسترسی از راه دور یک کاربر به کامپیوتر را فراهم می آورد.

کرم ها برنامه هایی هستند که مشابه ویروس ها توان تکثیر کردن خود را دارند، ولی برعکس آنها برای گسترش خود نیاز به برنامه هایی دیگر ندارند تا آنها را آلوده کرده و تحت عنوان فایل های آلوده اقدام به انتقال و آلوده کردن دستگاه های دیگر نمایند. کرم ها معمولا از نقاط آسیب پذیر برنامه های e-mail برای توزیع سریع و وسیع خود استفاده می نمایند.

بمب های منطقی برنامه هایی هستند که در زمان هایی از قبل تعیین شده؛ مثلا یک روز خاص؛ اعمالی غیر منتظره انجام می دهند. این برنامه ها فایل های دیگر را آلوده نکرده و خود را گسترش نمی دهند.

علی رغم تنوع انواع برنامه های مخرب، برنامه های قوی ضد ویروس می توانند نسخه های مختلف آنها را شناسایی و از بین ببرند. در ادامه این متن برای سادگی به همه انواع این برنامه ها عنوان عمومی ویروس اطلاق می شود.

خطرات ویروسهای ایمیل و اسبهای تروا

استفاده گسترده از ایمیل راه ساده ای را برای گسترش محتویات مضر در شبکه ها پیش روی هکرها قرار داده است. هکرها براحتی می توانند از حصار ایجاد شده توسط یک فایروال از طریق نقب زدن از راه پروتکل ایمیل عبور کنند، زیرا فایروال محتویات ایمیل را بررسی نمی کند. CNN در ژانویه ۲۰۰۴ گزارش داد که ویروس MyDoom هزینه ای در حدود ۲۵۰ میلیون دلار را بدلیل آسیب های وارده و هزینه های پشتیبانی فنی بر شرکتها تحمیل کرده است، این در حالیست که NetworkWorld هزینه های مقابله با Blaster، SoBig.F، Wechia و سایر ویروسهای ایمیل تا سپتامبر ۲۰۰۳ را تنها برای شرکتهای ایالات متحده ۳/۵ میلیارد دلار ذکر کرد. (یعنی عدد ۳۵ با هشت تا صفر جلوش!!!)

بعلاوه، از ایمیل برای نصب اسبهای تروا استفاده می شود که مشخصاً سازمان شما را برای بدست آوردن اطلاعات محرمانه یا بدست گیری کنترل سرورتان، هدف می گیرند. این ویروسها که خبرگان امنیت از آنها بعنوان ویروسهای جاسوسی یاد می کنند، ابزار قدرتمندی در جاسوسی صنعتی بشمار میروند! یک مورد آن حمله ایمیلی به شبکه مایکروسافت در اکتبر۲۰۰۰ است که یک سخنگوی شرکت مایکروسافت از آن بعنوان "یک عمل جاسوسی ساده و تمیز" یاد کرد. برطبق گزارشها، شبکه مایکروسافت توسط یک تروای backdoor که به یک کاربر شبکه توسط ایمیل ارسال شده بود، هک شد.

خطر نشت و فاش شدن اطلاعات

سازمانها اغلب در آگاهی دادن به کارکنانشان نسبت به وجود مخاطرات دزدی داده های مهم شرکتهایشان ، کوتاهی می کنند. مطالعات مختلف نشان داده است که چگونه کارمندان از ایمیل بمنظور فرستادن اطلاعات حقوقی محرمانه استفاده می کنند. گاهی آنها اینکار را از روی ناراحتی یا کینه توزی انجام می دهند. گاهی بدلیل عدم درک مناسب از ضربه مهلکی است که در اثر این عمل به سازمان وارد می شود. گاهی کارمندان از ایمیل برای به اشتراک گذاری داده های حساسی استفاده می کنند که رسماً می بایست در داخل سازمان باقی می ماند.

بر طبق مطالعات و پرس وجوهای Hutton در انگلستان در سال ۲۰۰۳ نشان داده شد که صاحب منصبان دولتی و اعضاء هیات رئیسه BBC از ایمیل برای فاش ساختن اطلاعاتی که محرمانه بوده اند استفاده کرده اند. مقاله ای در مارس ۱۹۹۹ در PC Week به تحقیقی اشاره کرد که طی آن از میان ۸۰۰ پرسنل مورد مطالعه، ۲۱ تا ۳۱ درصد آنها به ارسال اطلاعات محرمانه ـ مانند اطلاعات مالی یا محصولات ـ به افراد خارج از شرکتشان اعتراف کرده اند.

خطر ایمیلهای دربردارنده محتویات بدخواهانه یا اهانت آور

ایمیلهای ارسالی توسط کارکنان که حاوی مطالب نژادپرستانه، امور جنسی یا سایر موضوعات ناخوشایند است، می تواند یک شرکت را از نقطه نظر قانونی آسیب پذیر نماید. در سپتامبر ۲۰۰۳ مشاوران شرکت مالی Holden Meehan مجبور به پرداخت ۱۰هزار پوند به یکی از کارکنان سابق بدلیل ناتوانی در محافظت وی در مقابل آزار ایمیلی! شدند. Chevron مجبور به پرداخت ۲/۲ میلیون دلار به چهار نفر از کارکنانش شد که به وضوح ایمیلهای آزاردهنده جنسی دریافت کرده بودند. تحت قانون انگلیس، کارفرمایان مسوول ایمیلهایی هستند که توسط کارکنانشان در مدت استخدامشان نوشته و ارسال می شود، خواه کارفرما راضی به آن ایمیل بوده باشد، خواه نباشد. مبلغی معادل ۴۵۰هزار دلار از شرکت بیمه Norwich Union طی یک توافق خارج از دادگاه بخاطر ارسال توضیحات مربوط به یک سری از مسابقات درخواست شد.

روشهای استفاده شده برای حمله به سیستم ایمیل

برای درک انواع تهدیدات ایمیلی که امروزه وجود دارد، نگاهی اجمالی به روشهای اصلی فعلی حملات ایمیلی می اندازیم:

ضمیمه هایی با محتوای آسیب رسان

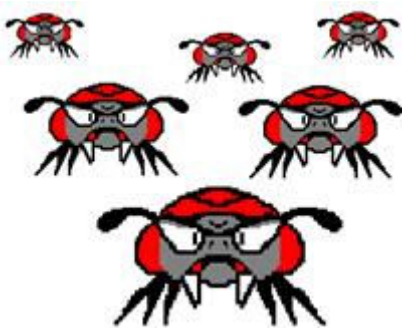
Melissa و LoveLetter جزو اولین ویروسهایی بودند که مساله ضمیمه های (Attachments) ایمیل و اعتماد را نشان دادند. آنها از اعتمادی که بین دوستان و همکاران وجود داشت استفاده می کردند. تصور کنید یک ضمیمه از دوستی دریافت می کنید که از شما می خواهد آن را باز کنید. این همانی است که در Melissa، AnnaKournikova،

SirCam و سایر ویروسهای ایمیلی مشابه اتفاق می افتاد. به محض اجرا شدن، چنین ویروسهایی معمولا خودشان را به آدرسهای ایمیلی که از دفترچه آدرس شخص قربانی بدست میاورند و به ایمیلهایی که صفحات وب ذخیره می کنند، ارسال می کنند. ویروس نویسان تاکید زیادی روی اجرای ضمیمه ای که توسط قربانی دریافت می شود، دارند.بنابراین برای نام ضمیمه ها از عناوین متفاوت و جذاب مانند SexPic.cmd و me.pif استفاده می کنند.

بسیاری از کاربران سعی می کنند که از سرایت ویروسهای ایمیل جلوگیری کنند و فقط روی فایلهایی با پسوندهای مشخص مانند JPG و MPG کلیک می کنند. بهرحال بعضی ویروسها، مانند کرم AnnaKournikova، از پسوند چندتایی بمنظور گول زدن کاربر برای اجرای آن استفاده می کند. ویروس AnnaKournikova از طریق ضمیمه ایمیل و با عنوان 'AnnaKournikova.jpg.vbs' منتقل میشد که دریافت کننده را متقاعد می کرد که یک تصویر به فرمت JPG را از ستاره مشهور تنیس دریافت کرده است تا اینکه فایل ضمیمه یک اسکریپت ویژوال بیسیک حاوی کدهای آسیب رسان باشد.
بعلاوه، پسوند Class ID (CLSID) به هکرها این اجازه را می دهد که پسوند واقعی فایل را پنهان کنند و بدینوسیله این حقیقت که cleanfile.jpg یک برنامه HTML می باشد پنهان می ماند. این روش در حال حاضر نیز فیلترهای محتوای ایمیل را که از روشهای ساده بررسی فایل استفاده می کنند، فریب می دهد و به هکر امکان رسیدن به کاربر مقصد را به سادگی می دهد.

ایمیلهای راه اندازنده اکسپلویت های شناخته شده

اکسپلویت در حقیقت استفاده از شکافهای امنیتی موجود است. کرم Nimda اینترنت را با شگفتی مواجه کرد و با گول زدن بسیاری از ابزار امنیت ایمیل و نفوذ به سرورها و شبکه های بزرگ و سرایت کردن به کابران خانگی، اینترنت را فراگرفت. حقه بکارگرفته شده توسط Nimda این است که روی کامپیوترهایی که نسخه آسیب پذیری از IE یا Outlook Express را دارند، بطور خودکار اجرا می شود. Nimda از اولین ویروسهایی بود که از یکی از این شکافها بمنظور انتشار بهره برداری می کنند. برای مثال، انواعی از ویروس Bagle که در مارس ۲۰۰۴ ظهور کردند، از یکی از شکافهای اولیه Outlook برای انتشار بدون دخالت کاربر استفاده می کردند.



ایمیلهای با فرمت HTML دربردارنده اسکریپت

امروزه، تمام استفاده کنندگان ایمیل می توانند ایمیلهای HTML را ارسال و دریافت کنند. ایمیل با فرمت HTML می تواند اسکریپتها و محتویات فعالی را دربرگیرد که می توانند به برنامه یا کدها اجازه اجرا روی سیستم دریافت کننده را دهند.

Outlook و محصولات دیگر از اجزا IE برای نمایش ایملهای HTML استفاده می کنند، به این معنی که اینها شکافهای امنیتی موجود در IE را به ارث می برند!

ویروسهای بر پایه اسکریپتهای HTML خطر مضاعف توانایی اجرای خودکار را، وقتی که ایمیل آسیب رسان باز می شود، دارند. آنها به ضمیمه ها متوسل نمی شوند؛ بنابراین فیلترهای ضمیمه که در نرم افزارهای ضدویروس وجود دارند در نبرد با ویروسهای اسکریپت HTML بلااستفاده هستند. برای مثال ویروس BadTrans.B از HTML برای اجرای خودکار در هنگام بازشدن استفاده می کند و از یک اکسپلویت ایمیل با فرمت HTML برای انتشار استفاده می کند. در مقاله بعدی به روشهای مقابله خواهیم پرداخت.

طرز کار برنامه های ضد ویروس

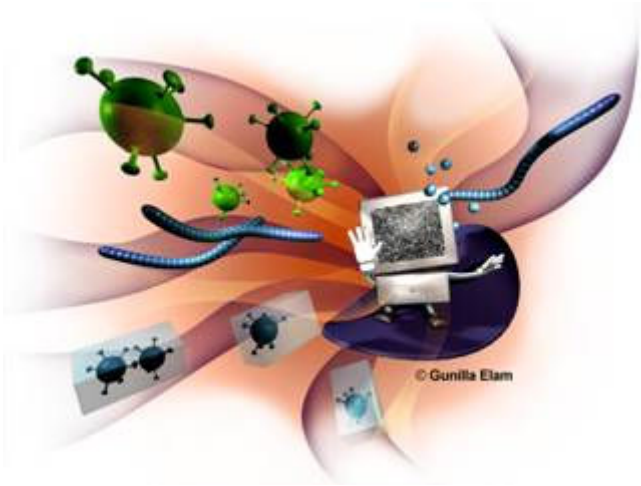
ضد ویروس اصطلاحی است که به برنامه یا مجموعه ای از برنامه ها اطلاق می شود که برای محافظت از کامپیوتر ها در برابر ویروس ها استفاده می شوند. مهم ترین قسمت هر برنامه ضد ویروس موتور اسکن (Scanning engine) آن است. جزئیات عملکرد هر موتور متفاوت است ولی همه آنها وظیفه اصلی شناسایی فایل های آلوده به ویروس را با استفاده از فایل امضای ویروس ها بر عهده دارند. فایل امضای ویروس یک رشته بایت است که با استفاده از آن می توان ویروس را به صورت یکتا مورد شناسایی قرار داد و از این جهت مشابه اثر انگشت انسان ها می باشد. ضد ویروس متن فایل های موجود در کامپیوتر را با نشانه های ویروس های شناخته شده مقایسه می نماید. در بیشتر موارد در صورتی که فایل آلوده باشد برنامه ضدویروس قادر به پاکسازی آن و از بین بردن ویروس است. در مواردی که این عمل ممکن نیست مکانیزمی برای قرنطینه کردن فایل آلوده وجود دارد و حتی می توان تنظیمات ضدویروس ها را به گونه ای انجام داد که فایل آلوده حذف شود.

بعضی از برنامه های ضد ویروس برای شناسایی ویروس های جدیدی که هنوز فایل امضای آنها ارائه نشده از روش های جستجوی ابتکاری استفاده می کنند. به این ترتیب داده های مشکوک در فایل های موجود در سیستم و یا فعالیت های مشکوک مشابه رفتار ویروس ها (حتی در صورتی که تعریف ویروسی منطبق با آنچه که در فایل مشکوک یافت شده موجود نباشد) علامت گذاری می شوند. اگر ضد ویروس فعالیت مشکوکی را مشاهده نماید، برنامه ای که فعالیت مشکوک انجام داده را قرنطینه نموده و به کاربر در مورد آن اعلام خطر می کند (به عنوان مثال اعلام می شود که برنامه مشکوک مایل به تغییر Windows Registry می باشد). دقت این روش پایین است و در بسیاری از مواقع در شناخت فایل های مشکوک به ویروس اشتباهاتی رخ می دهد.

در چنین مواقعی فایل قرنطینه شده برای شرکت های سازنده ضد ویروس ها ارسال می شود که پس از تحقیق و آزمایش آن، در صورتی که واقعا فایل آلوده به ویروس باشد نام، امضاء و مشخصات آن مشخص شده و پادزهر آن ارائه می گردد. در این صورت کد مشکوک تبدیل به یک ویروس شناخته شده می شود.

قابلیت های نرم افزار های ضدویروس

سطح محافظت نرم افزار بسته به جدید و بروز بودن آن متغیر است. محصولات جدیدتر قابلیت های مانند بروز رسانی خودکار، اسکن های زمان بندی شده، محافظت از سیستم به صورت ماندگار در حافظه و همچنین امکان یکپارچه شدن با برنامه های کاربردی اینترنتی مانند برنامه های e-mail و مرورگرهای وب را دارند. نسخه های قدیمی تر نرم افزارهای ضدویروس تنها یک اسکنر بودند که باید به صورت دستی راه اندازی می شدند. همه نرم افزار های ضدویروس در صورتی که به صورت منظم به روز رسانی شده و عملیات اسکن بر روی دیسک های سخت، تجهیزات قابل انتقال (مانند فلاپی و Zip disk) انجام شود می توانند دستگاه کامپیوتر را در برابر ویروس ها مقاوم کنند. در واقع نقطه برتری محصولات جدید ضد ویروس در قابلیت های آنها برای محافظت از سیستم در مواقعی است که کاربر دانش و یا دقت لازم برای به کارگیری آن را ندارد.



حداقل توقعی که از یک برنامه ضد ویروس خوب می توان داشت این است که در برابر ویروس های boot-sector، ماکرو، اسب های تروا و فایل های اجرایی آلوده به ویروس و کرم اقدامات محافظتی لازم را به عمل آورد. از محصولات جدیدتر می توان انتظار محافظت در برابر صفحات وب، اسکریپت ها، کنترل های ActiveX و اپلت های جاوای خطرناک، همچنین کرم های e-mail را داشت.

تفاوت بین نسخه‌های ضد ویروس

همه نرم‌افزارهای ضد ویروس عمل واحدی را انجام می‌دهند که همان اسکن فایل‌ها و پاک‌سازی موارد آلوده می‌باشد. بعضی از آنها حتی از موتورهای اسکن یکسانی برای شناسایی ویروس‌ها بهره می‌گیرند. تفاوت اصلی بین این محصولات در کیفیت واسط کاربر، سرعت و دقت محصول و قابلیت‌های خاص (مانند اسکنرهای e-mail، بروز رسانی‌های خودکار زمان بندی شده، اسکن‌های ابتکاری و ...) می‌باشد.

در حال حاضر با توجه به اتصال اکثر کامپیوترها به شبکه اینترنت و خطرات گسترده‌ای که از این طریق کاربران را تهدید می‌کند تامین امنیت در برابر ویروس‌هایی که از طریق اینترنت انتقال می‌یابند اهمیت زیادی دارد. از سوی دیگر اینترنت می‌تواند به عنوان ابزاری برای بروز نگه‌داری نرم‌افزارهای ضدویروس مورد استفاده قرار گیرد.

حافظت e-mail

افزایش تعداد کرم‌هایی که از طریق e-mail توزیع می‌شوند نیاز همه افراد به محصولات ضد ویروسی که امنیت آنها را تامین کنند افزایش داده است. تعدادی از محصولات نرم‌افزاری نمی‌توانند امنیت مورد نیاز را برای همه کاربران تامین کنند. از سوی دیگر تمایل زیاد کاربران به یکپارچه سازی نرم افزارهای e-mail با برنامه‌های اداری (Office applications) باعث شده، شکاف‌های امنیتی موجود در نرم‌افزارهای اداری توسط کرم‌هایی مانند ILOVEYOU و W32.Klez به سادگی مورد استفاده قرار گیرد. در چنین مواردی اگر وصله‌های امنیتی سیستم قدیمی باشند(که این مساله بسیار رایج است)، تنها مشاهده یک نامه آلوده کافی است که کرم به دستگاه نفوذ کند.

مشکل اصلی در رابطه با امنیت e-mail به نحوه کار برنامه‌ها برمی‌گردد. برنامه‌های e-mail پیام‌ها را دریافت کرده و آنها را در پایگاه‌داده‌های خاص خود ذخیره می‌نمایند. از سوی دیگر برنامه‌های ضد ویروس فقط فایل‌هایی را که در قالب فایل‌سیستم‌های شناخته شده مانند Fat16، Fat32، NTFS و ... هستند را اسکن می‌کنند، بنابراین لزوما نمی‌توانند ساختمان داده‌ای را که برنامه e-mail برای ذخیره سازی اطلاعات استفاده می‌کند شناخته و پیام‌های ذخیره شده و فایل‌های ضمیمه آن را اسکن کند. این بدان معناست که هرگاه یک e-mail آلوده بر روی دستگاهی که وصله‌های جدید بر روی آن نصب نشده بار شود، نه تنها کامپیوتر آلوده می‌شود بلکه پاک کردن دستگاه به سادگی امکان پذیر نیست و حتی ممکن است همه e-mailها از دست بروند. به عنوان مثال کرم W32.Klez که کامپیوترهای زیادی را آلوده نمود، در گام اول برنامه‌های ضد ویروس را مورد هجوم قرار می‌دهد و در نتیجه برنامه آلوده شده قادر به پاک کردن محتویات صندوق‌های پستی کاربران نیست.

دو راه حل برای این مشکل وجود دارد، یا باید با دقت همه وصله های جدید مرورگر وب و برنامه‌های e-mail را گرفته و بر روی دستگاه نصب نمود و یا از برنامه‌های ضدویروسی استفاده کرد که به مرورگر و برنامه mail متصل شده و آنها را به روز نگه‌می‌دارند.

برای اینکه سیستم e-mail کاملا حافظت شده باشد، باید عملیات اسکن قبل از اینکه e-mail در جایی از حافظه ذخیره شود صورت گیرد. به عبارت دیگر برنامه e-mail داده را بعد از گرفتن از اینترنت به اسکنر ضدویروس ارسال می‌نماید تا عملیات لازم بر روی آن صورت گیرد.

همه نرم‌افزارهای e-mail قابلیت این نوع مجتمع شدن را ندارند. اما اسکنرهایی وجود دارند که به خوبی با بعضی از نسخه‌های Microsoft Outlook Express، Microsoft Outlook، Netscape Messenger، Netscape، Eudora Pro و Becky Internet Mail مجتمع می‌شوند. بعضی از اسکنرها ادعای مجتمع شدن با همه سرویس‌گیرنده‌های POP3 و MAPI را مطرح می‌کنند.

بروز رسانی نرم‌افزارهای ضدویروس

نصب برنامه ضد ویروس و رها کردن آن برای داشتن دستگاهی بدون ویروس و مقاوم در برابر حملات ویروس‌ها کافی نیست. هر روزه ویروس‌های جدیدی عرضه می‌شود و در سال‌های جدید انتشار سریع کرم‌ها از طریق اینترنت نرخ ایجاد ویروس را افزایش داده است. این مساله در ترکیب با افزایش دانش عمومی در مورد مشکلات امنیتی نرم‌افزارها و سیستم‌های عامل سرعت ایجاد ویروس‌های جدید را افزایش داده است. امروزه برای ایجاد یک ویروس نیاز به مهارت و تخصص زیاد نیست. تولید کنندگان ویروس‌ها می توانند ویروس‌هایی با تفاوت‌های اندک نوشته و در دنیای مجازی انتشار دهند. بنابراین علاوه بر خرید و نصب نرم‌افزار ضدویروس دقت در بروز نگه‌داشتن آن هم از اهمیت خارق‌العاده‌ای برخوردار است.

شرکت‌های تولید کننده نرم‌افزار برای مقابله با این مشکل قابلیت بروز رسانی خودکار را به محصولات جدید خود افزوده‌اند. بنابراین کاربران تنها با انتخاب گزینه مناسب از منوهای نرم‌افزار می‌توانند از بروز بودن نرم‌افزار خود مطمئن باشند.

چگونه کامپیوتر خود را در مقابل ویروسها مصون سازیم؟

در مقابله با ویروسهای کامپیوتری، مهمترین نکته ای که باید به خاطر داشت، اینست که امکان صدمه دیدن هر سیستمی وجود دارد. مهم نیست که از چه نرم افزار ضد ویروسی استفاده می کنید و تا چه اندازه اقدامات امنیتی را برای محافظت سیستم های خود بکار گرفته اید. همیشه این احتمال وجود دارد که یک ویروس جدید و ناشناخته به سیستم های مؤسسه شما نفوذ کرده و کارهای روزمره را مختل کند.

البته قرنطینه کردن کل سیستم ها و قطع ارتباط اینترنت و پست الکترونیکی مؤسسه با دنیای خارج، می تواند کمک بزرگی در کاهش خطرا ت ویروسها باشد، اما در دنیای فن آوری اطلاعات امروز، این چنین اقداماتی عملی نبوده و قابل اجرا نیست. نکات زیر می تواند راهنمای خوبی برای محافظت سیستم های یک مؤسسه باشد. نکاتی ساده و واضح که البته اغلب اوقات فراموش می شوند:

تعریف سیاست های امنیتی برای مؤسسه

مهم است که بدانید تا چه اندازه و در چه نقاطی نیاز به اقدامات محافظتی دارید. باید مشخص شود که چه نوع اطلاعاتی در مؤسسه داریم و هر یک تا چه حد قابل دسترسی برای هر یک از افراد مؤ سسه ا ست

باید بدانیم چه افرادی، چه مسئولیتهایی در اجرای اقدامات محافظتی مؤسسه دارند و این افراد چگونه با یکدیگر در تبادل اطلاعات هستند.
در نهایت نیز ارتباط این افرا د با کاربران عادی موسسه چگونه بوده و چه راهنمایی و آموزشهایی در مواقع خطر و بروز ویروس به آنان ارائه خواهند کرد.

کنترل و محافظت تمام نقاط وروری در موسسه

با پیشرفت فن آوری و توسعه ارتباطات، روش ها و نقاط متعددی برای ورود و نفوذ ویروسهای کامپیوتری به درون یک موسسه وجود دارد. پیام های الکترونیکی آلوده، کامپیوترهای قابل حمل، دیسکت های ویروسی و....

بروز کردن نرم افزارهای ضد ویروس

بسیاری موسسات درباره بروز کردن فایلهای اطلاعاتی نرم افزار جهت شناسایی ویروسهای جدید آگاهی لازم را دارند ولی اغلب موسسات، از اهمیت بروز نمودن فایلهای اجرایی نرم افزارخود بی اطلاع هستند. بروز کردن فایلهای اجرایی به نرم افزار ضد ویروس این امکان را می دهد که از روش های قویتر و سریعتر در شناسایی و پاکسازی ویروسها بهره گیرند.

استفاده کاربران از نرم افزارهای ضد ویروس

نرم افزارهای ضد ویروس نصب شده بر روی سرویس دهنده های (server) موسسه قابلیت کنترل تمام فعالیتهای شبکه را دارا هستند ولی گاه اتفاق می افتد که کاربران خارج از شبکه موسسه بطور شخصی با کامپیوتر کار می کنند و یا فایلها و پیامهای رمز شده دریافت می کنند که قابل کنترل در سرویس دهنده های موسسه نیستند تا زمانی که توسط کاربر بر روی کامپیوتر خود رمز گشایی شود.

کلیه نرم افزارهای مورد استفاده را بروز نگه دارید

نرم افزارهای سیستم عامل، مرورگرها(Browser)، پست الکترونیکی و نرم افزارهای کاربردی موسسه خود را بروز نگه داشته و از Upgrade و Patch هایی که شرکت های تولید کننده نرم افزار هر از چند گاهی ارائه می کنند ، استفاده کنید.

بطور دائم و مستمر بایگانی تهیه کنید.

اگر بایگانی مناسب داشته باشید، در صورت آلودگی به ویروس، بدون نگرانی می توانید فایلهای سالم را از بایگانی جایگزین فایلهای آسیب دیده کنید. بایگانی پیامهای الکترونیکی را نیز فراموش نکنید.
همیشه بعد از تهیه بایگانی، کنترل کنید که بایگانی بطور صحیح انجام شده و در صورت لزوم می توانید فایلها را از بایگانی خارج و جایگزین فایلهای موجود نمائید.

موسسه خود را مشترک مراکز اطلاع رسانی کنید.

از طریق اینترنت می توانید مشترک بسیاری از این مراکز اطلاع رسانی شده و بطور مستمر خبرنامه های آنان را دریافت کنید. خبرنامه هایی درباره ویروسهای جدید، نگارش های جدید نرم افزار، نقاط ضعف نرم افزارها و....

کاربران مؤسسه را آموزش دهید

به کاربران عادی مؤسسه یاد دهید تا در صورت مشاهده ویروس کامپیوتری به چه نحو عمل کرده، چه کسی را مطلع کنند، چه کارهایی را انجام ندهند و خلاصه دستپاچه نشوند تا صدماتی بدتر و شدیدتر از صدمات ویروسها ببار آورند.

در صورت استفاده از پیام الکترونیکی و نرم افزارهای مربوط به آن در داخل مؤسسه، اقدامات زیر را انجام دهید.

نرم افزارهای پیام الکترونیکی مانند Out Look Express این امکان را فراهم می کنند که بدون باز کردن پیام، بتوان متن داخل پیام را مشاهده کرد. بسیاری از ویروسها قادرند، با استفاده از این امکان، فعال شده و آلودگی ببار آورند.

لذا در این نرم افزارها امکان Preview Pane را غیر فعال کنید.

در اغلب حالات، نرم افزار word بعنوان Editor در نرم افزارهای پست الکترونیکی انتخاب شده اند، بدین معنا که فایلهای متن بطور خودکار با استفاده از word باز می شوند.

تعدادی از ویروسها قادرند که با تغییر و آلوده ساختن فایل Normal.Dot. نرم افزارword پخش شده و شیوع یابند. لذا مناسب است که این فایل را بصورت Read - Only درآورید.

بجای ارسال فایلهای متنی بصورت .Doc از حالت RTF، استفاده کنید و بجای فایلهای spread Sheet بصورت .XLS از حالت esr. استفاده نمائید.

در حالات .RTF و .CSR گروه بزرگی از ویروسها (ویروسهای macro) قادر به فعالیت نیستند البته این روش در مقابل تمام ویروسها مؤثر نبوده و صد در صد نیست.

اغلب کاربران نیازی به استفاده از امکانات windows Sript Hosting ندارند و لذا می توان این امکان را غیرفعال نمود. گروهی از ویروسها از این امکان استفاده کرده و باعث آلودگی می شوند.

برای غیر فعال کردن این امکان مراحل زیر را دنبال کنید:

Control panel--> Add/Remove Program--> windows setup--> Accessories-->windows script host

اگر مؤسسه شما دارای سرویس دهنده خاص پیامهای الکترونیکی نیست و قادر نیستید در همان ابتدای ورود پیام به داخل مؤسسه، محتوای آنرا کنترل کنید، با استفاده از امکانات نرم افزارهای پست الکترونیکی مثل Out look Express می توانید قوانین خاص خود را برای کنترل پیامها بر روی کامپیوتر کاربران تعریف کنید.

این امکان معمولا" تحت عنوان Inbox Rules تعریف می شود.

پیوست (attachment) پیام های الکترونیکی بزرگترین منبع و منشأ پخش ویروسها ا ست . به کاربران مؤسسه خود بیاموزید که در باز کردن و استفاده از پیوست ها دقت زیادی بعمل آورند و پیام و پیوست هایی که از افراد بیگانه و ناشناس دریافت می کنند را بدون باز کردن حذف نمایند و دیگر پیوست ها را نیز پس از ضبط بر روی کامپیوتر و کنترل آنها توسط نرم افزارهای ضد ویروس، استفاده کنند.

پیامهای الکترونیکی دروغ و یا شوخی، یکی دیگر از موارد ایجاد مزاحمت و نگرانی بین کاربران است. به کاربران بیاموزیید که از ارسال اینگونه پیام ها به یکدیگر خودداری کرده و تنها در صورت اثبات صحت این پیامها، تنها فرد مسئول در موسسه اقدام به اطلاع رسانی درباره آن نمایند.

ویروسها معمولا" با اجرا شدن یک فایل اجرایی، فعال می شوند و اغلب اوقات این فایلهای اجرایی بصورت پیوست از طریق پیام های الکترونیکی توسط ویروس ارسال و توزیع میشود.
اغلب کاربران عادی لزومی به دریافت فایلهای اجرایی ندارند لذا می توان در همان ابتدای ورود پیام ها به سرویس دهندهای موسسه، پیامهایی که دارای پیوست EXE / VBS و یا SHS. هستند را جدا کرده و برای کنترل بیشتر قرنطینه کرد.

ویروس ها چگونه منتشر می شوند

اگر کسی چیزی در مورد کامپیوتر ها نداند این را می داند که ویروسها مخرب هستند و باید کامپیوتر خود را در برابر هجوم آنها حافظت کند. کمپانی های ضد ویروس (آنتی ویروس) تعداد زیادی ویروس را ساپورت می کنند. ولی هیچ کدام از آنها کامل نیستند. آنتی ویروسهای امروزی بیشتر عمل حفاظت را به طور واکنشی انجام می دهند تا به صورت کنشی. یعنی برای اینکه آنتی ویروس شما متوجه ویروس جدید در کامپیوتر شود باید تا آخرین بیت وارد کامپیوتر شما شود و شروع به فعالیت کند.
سناریوی پخش یک ویروس جدید در اینترنت و عکس العمل شرکت های آنتی ویروس در برابر آن به صورت زیر است:

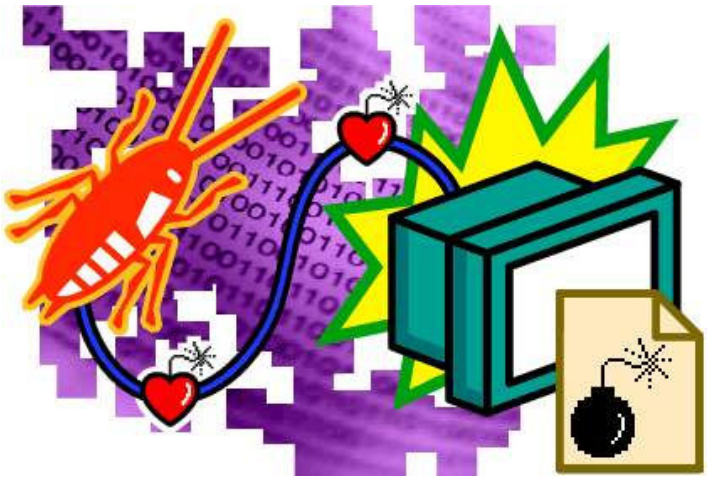
ابتدا یک ویروس به طور متوسط صد هزار کامپیوتر را مورد هجوم قرار می دهد.
سپس شرکت های آنتی ویروس شروع به ساختن پکیج برای آنها می کنند.
در مرحله بعد این پکیج در اختیار عموم قرار می گیرد.
مشکل این است که ممکن است کامپیوتر شما قبل از ساختن این پکیج مورد حمله قرار گیرد. مشکل دیگر این است که اکثر افراد آنتی ویروس کامپیوتر خود را « به روز » یا « up to date » نمی کنند. کمپانی های ضد ویروس بیشتر به صورت اکتشافی عمل می کنند. و این کار را بوسیله برنامه های آشکار سازی انجام می دهند. این برنامه ها کلیه اعمالی را که در کامپیوتر بوسیله برنامه های دیگر انجام می شود تحت نظر می گیرند و هر گاه این اعمال با کارهایی که یک ویروس در کامپیوتر انجام می دهد مطابقت کند آن را به عنوان یک ویروس شناسایی می کنند.سپس جلوی فعالیت آن را می گیرند و همچنین وجود ویروس را به کاربر گوشزد می کنند. با عمل کردن این برنامه آشکار ساز در نرم افزار آنتی ویروس هر گاه یک برنامه فعالیت مشکوکی انجام دهد به کاربر هشدار می دهد و احتمالاً جلوی انتشار ویروس گرفته می شود. این عمل باعث می شود کامپیوتر ها کمتر آلوده شوند.
نرم افزار آنتی ویروس باید به گونه ای تنظیم شود که که روزانه به طور اتوماتیک اجرا شود که شامل به روز کردن و اسکن کردن است.
برنامه های اکتشافی (Heuristics) این فرصت را می دهند که زودتر جلوی انتشار ویروس ها گرفته شود. هر چند استفاده از این برنامه ها یک راه صددرصد فراگیر نیست. ولی بسیار مشکل گشا است. و حساسیت این برنامه ها به تنظیم سطح حفاظت (Level Setting) در نرم افزار آنتی ویروس بستگی دارد. یعنی آنتی ویروسی که در کامپیوتر شما نصب شده است و تنظیمات آن به کشف ویروسها کمک می کند.

چه چیزی ویروس نیست؟!

بدلیل سوء شهرتی که ویروسهای کامپیوتری کسب کرده‌اند، به آسانی هر مشکل کامپیوتری بر گردن ویروسها انداخته می‌شود.
در این مقاله در ابتدا به بعضی موارد و مشکلات که ممکن است دلیلی بغیر از ویروس داشته باشند، اشاره می‌شود:

- مشکلات سخت‌افزاری: ویروسی وجود ندارد که بتوانند به بعضی از قطعات سخت‌افزاری مانند چیپ‌ها، بردها و مونیتور آسیب برساند.
- صدای بوق در هنگام راه‌اندازی کامپیوتر بدون تصویر: این حالت معمولا بدلیل یک مشکل سخت‌افزاری در هنگام روند بوت رخ می‌دهد. به مستندات کامپیوتر خود برای فهمیدن معنی انواع بوقها در هنگام بوت مراجعه کنید.
- کامپیوتر کل ۶۴۰ کیلوبایت اول از حافظه را نشان نمی‌دهد. این می‌تواند نشانه ویروس باشد، اما قطعی نیست. بعضی از درایورهای سخت‌افزار مانند مونیتور یا کارت SCSI ممکن است بخشی از این قسمت از حافظه را استفاده کنند. به سازنده یا فروشنده کامپیوتر خود مراجعه کنید تا دلیل این امر را بفهمید.
- دو برنامه ضدویروس نصب‌شده دارید و یکی از این دو، ویروسی را گزارش می‌کند: در حالیکه که این می‌تواند نشانه ویروس باشد اما ممکن است امضا یا اثر یکی از این ضدویروسها در حافظه باشد که توسط دیگری به صورت ویروس تشخیص داده شده است.
- در حال استفاده از Microsoft Word هستید که Word به شما گزارش وجود یک ماکرو در یک فایل را می‌دهد. به این معنی نیست که ماکرو ویروس است.
- یک فایل یا سند خاص را نمی‌توانید باز کنید: این الزاما نشانه وجود ویروس نیست. امتحان کنید که آیا می‌توان فایل دیگر یا نسخه پشتیبان همین فایل را باز کرد. اگر بقیه باز می‌شوند، امکان خراب بودن فایل اولیه وجود دارد.
- برچسب روی هارد تغییر کرده‌است. هر دیسک اجازه داشتن یک برچسب را دارد. می‌توانید توسط DOS یا Windows به یک دیسک برچسبی اختصاص دهید.
- هنگام اجرای ScanDisk ، آنتی‌ویروس نورتون یک فعالیت شبه‌ویروسی را گزارش می‌کند. دو راه حل در پیش‌رو دارید:
  - Auto-Protect نورتون را موقتا غیرفعال کنید و ScanDisk را اجرا کنید.
  - Optionهای ScanDisk را در هنگام اجرا تغییر دهید.

در حقیقت، موارد فوق تنها چند مورد از تصورات اشتباه در مورد ویروس‌هاست.



تصورات غلط

در مورد تصورات غلطی که در مورد ویروسها وجود دارد، داستانها و اتفاقات جالبی وجود دارد. جالب اینجاست که افراد زیادی نیز هستند که با اینکه اطلاعات زیاد و یا صحیحی راجع به ویروسها ندارند، ولی خود به گونه دیگری فکر می‌کنند و به این ترتیب به خود اجازه اظهار نظر در این مورد را می‌دهند. این افراد دچار سندرمی به نام False Authority یا اعتبار کاذب هستند.

ولفگانگ استیلر که بعنوان یک متخصص ویروس بصورت بین‌المللی مطرح است، و نویسنده برنامه ضدویروس Integrity Master است می‌گوید: "امروزه خبرگان امنیت کامپیوتر – افرادی که لایق این عنوان هستند- تمایل به داشتن یک زمینه خوب از نحوه عمل ویروسها دارند و می‌توانند نصایح خوبی در این زمینه ارائه دهند. " اما هنگامی که از وی درباره صاحب‌نظران ویروس پرسیده می‌شود، او کلمات خود را بدقت و با احتیاط کامل انتخاب می‌کند.

استیلر می‌گوید " این افراد نسبت به مردم عادی درک بیشتری از ویروس‌ها دارند." او اضافه می‌کند: " بعضی ادعا می‌کنند که این افراد بدرستی ویروسها را می‌شناسند، اما تعدادی را دیده‌ام که هیچی نمی‌دانند یا حتی بدتر، دچار تصور غلطی از ویروس هستند. با توجه به این نکته که آنان متخصصان امنیت کامپیوتر هستند، تصورات غلطشان بار منفی بیشتری نسبت به مردم عادی دارد. گفتار و نظرهای اشتباه، زمانی که از زبان این افراد شنیده می‌شوند، نتایج زیانبارتری دارند. "

افرادی که عناوین شغلی مرتبطی نیز ندارند، گاهی دچار سندرم اعتبار کاذب هستند. برای مثال یک کاربر که به ویروس برمی‌خورد، ممکن است برای فهمیدن نحوه مقابله با آن به هرکسی مراجعه کند. در چنین شرایط شخص پاسخگو ممکن است تا درجه متخصص رسمی ویروس نیز ارتقاء یابد!!

دونتمن می‌گوید" شغل یک ویراستار مجله کامپیوتر ایجاب می‌کند که وی در مورد خیلی چیزها مقدار کمی بداند. او گستره وسیعی از دانش با عمق کم در اختیار دارد، مگر در چند مورد خاص!"

او اضافه میکند " گزارشگران و ویراستاران صنعت کامپیوتر می‌توانند بخوبی صحبت‌کنند و بنویسند. اگر شما بتوانید در مورد یک موضوع، حتی اگر در مورد آن چیزی ندانید، تعابیر خوبی بیان کنید، شانس خود را برای این که متخصص در آن زمینه شناخته شوید بالا برده‌اید، مخصوصا توسط افرادی که در مورد آن موضوع هیچ‌چیز نمی‌دانند. "

سندرم اعتبار کاذب دو میل مهم را در فرد برمی‌انگیزد. اول اینکه فرد واقعا دوست دارد که به دیگران کمک کند؛ و دیگر اینکه دوست دارد بر کامپیوتر احساس کنترل داشته باشد. و این دو گرایش باعث تاثیرپذیری فرد در مقابل این سندرم می‌شود.

مارچلو، یک کاربر معمولی که یک ایمیل دروغین دریافت کرد، پیامی روی CompuServe فرستاد و به کاربران هشدار داد که هر پیامی که در عنوانش عبارت "Good Times" را دارد، باز نکنند (مبادا که بـه چینـی ویروسـی آلـوده شـوند). بطـرز مضحکی مارچلو از عبارت "Good Times" در عنوان پیام هشدارهنده خود استفاده کرده بود!!!

یک متخصص ویروس به شوخی یک پیام برای مارچلو فرستاد و به او گفت که آلوده کردن کامپیوتر دیگران با ویروس Good Times را متوقف کند. مارچلو وقتی از جزئیات نامه دروغین مطلع شد، پاسخ داد "از کمک شما متشکرم. متاسـفم، مـن گـول خورده بودم. اما بهرحال من نگران کامپیوتر و شغلم بودم"

نتیجه گیری

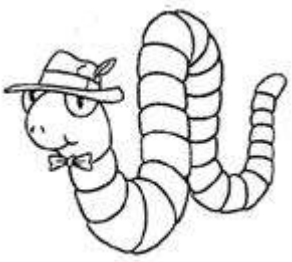
هدف از این مطالب تغییر عقاید شما درباره افسانه‌هایی که در مورد ویـروس‌هـا شـنیده‌ایـد، نیسـت. بلکـه از شـما مـی‌خـواهیم پرسشهای خود را از افرادی بپرسید که در زمینه ویروسهای کامپیوتر صاحب تخصص و آگاهی هستند. به این ترتیب می‌تـوان از "کوری عصاکش کور دگر شود" جلوگیری کرد و از تعداد افرادی که تمام خرافه‌ها راجع به ویروسها را باور دارند، کاست.

بطور خلاصه:

- بیشتر افراد دانش و تخصص بسیار کمی در زمینه ویروسهای کامپیوتری دارند.
- افراد با دانش کم اغلب به سندرم اعتبار کاذب دچار می‌شوند.
- سندرم اعتبار کاذب معمولا به شیوع ترس و خرافات در مورد ویروسهای کامپیوتر می‌انجامد.

دوتمن به بهترین نحو جمع‌بندی می‌کند: "اگر انسانها احتیاط بیشتری در مورد اینکه به چه کسی و چگونه و تا چه حدی اعتماد کنند، بخرج میدادند، ما بعنوان انجمن متخصصان بیشتر می‌دانستیم و بهتر شناخته می‌شـدیم. بنـابرانی مسـیرهای کمتـری بـه سمت اطلاعات بد یا غیرموثق پدید می‌آمد."

کرمهای اینترنتی مفید



خبرگزاری BBC در می ۲۰۰۱ خبر از ظهور و گسترش کرمی به نام کرم پنیر (Cheese worm) داد. محتوای خبـر نشـان از فعالیت این کرم علیه هکرها میداد، نه به نفع آنان!

«یک ویروس مفید در حال گشت در اینترنت است و شکاف امنیتی کامپیوترها را بررسی و در صورت یافتن، آنها را می‌بندد. هدف این کرم، کامپیوترهای با سیستم عامل لینوکس است که توسط یک برنامه مشابه اما زیان‌رسان قبلا مورد حمله قرار گرفته‌اند.»

اما این کرم توسط شرکت‌های تولید آنتی‌ویروس تحویل گرفته نشد! چراکه آنان معتقد بودند هر نرم‌افزاری که تغییراتی را بدون اجازه در یک کامپیوتر ایجاد کند، بالقوه خطرناک است.

در مارس همین سال یک برنامه زیان‌رسان با عنوان Lion worm (کرم شیر) سرویس‌دهندگان تحت لینوکس بسیاری را آلوده و درهای پشتی روی آنها نصب کرده بود تا ایجادکنندگان آن بتوانند از سرورها بهره‌برداری کنند. کرم همچنین کلمات عبور را می‌دزدید و به هکرهایی که از این ابزار برای ورود غیرمجاز استفاده می‌کردند، می‌فرستاد. این درهای پشتی می‌توانستند برای حملات DoS نیز استفاده شوند.

کرم پنیر تلاش می‌کرد بعضی از خسارات وارده توسط کرم شیر را بازسازی کند. در حقیقت کرم پنیر شبکه‌هایی با آدرسهای مشخص را پیمایش می‌کرد تا آنکه درهای پشتی ایجاد شده توسط کرم شیر را بیابد، سپس برای بستن سوراخ، وصله آنرا بکار می‌گرفت و خود را در کامپیوتر ترمیم‌شده کپی می‌کرد تا برای پیمایش شبکه‌های دیگر با همان شکاف امنیتی از این کامپیوتر استفاده کند.

مدیران سیستمها که متوجه تلاشهای بسیاری برای پیمایش سیستمهایشان شده بودند، دنبال علت گشتند و کرم پنیر را مقصر شناختند. ارسال گزارشهای آنها به CERT باعث اعلام یک هشدار امنیتی گردید.

این برنامه با مقاصد بدخواهانه نوشته نشده بود و برای جلوگیری از فعالیت هکرهای مزاحم ایجاد گشته بود. اما بهرحال یک «کرم» بود. چرا که یک شبکه را می‌پیمایید و هرجا که میرفت خود را کپی می‌کرد.

زمانیکه بحث کرم پنیر مطرح شد، بعضی متخصصان امنیت شبکه‌های کامپیوتری احساس کردند که ممکن است راهی برای مبارزه با شکافهای امنیتی و هکرهای آسیب‌رسان پیدا شده باشد. یکی از بزرگترین علتهای وجود رخنه‌های امنیتی و حملات در

اینترنت غفلت یا تنبلی بسیاری از مدیران سیستمهاست. بسیاری از مردم سیستمهای خود را با شکافهای امنیتی به امان خدا! رها می‌کنند و تعداد کمی زحمت نصب وصله‌های موجود را می‌دهند.

بسیاری از مدیران شبکه‌ها از ورود برنامه‌ها و بارگذاری وصله‌ها ابراز نارضایتی می‌کنند. این نکته‌ای صحیح است که یک وصله ممکن است با برنامه‌های موجود در کامپیوتر ناسازگار باشد. اما در مورد یک کرم مفید که وجود شکافهای امنیتی در سیستمها را اعلام می‌کند، چه؟ این روش مشکل مدیرانی را که نمی‌توانند تمام شکافهای امنیتی را ردیابی کنند، حل می‌کند. بعضی می‌گویند که برنامه‌های ناخواسته را روی سیستم خود نمی‌خواهند. در پاسخ به آنها گفته می‌شود «اگر شکاف امنیتی در سیستم شما وجود نداشت که این برنامه‌ها نمی‌توانستند وارد شوند. یک برنامه را که سعی می‌کند به شما کمک کند، ترجیح می‌دهید یا آنهایی را که به سیستم شما آسیب می‌رسانند و ممکن است از سیستم شما برای حمله به سایرین استفاده کنند؟ »

این آخری، یک نکته مهم است. رخنه‌های امنیتی کامپیوتر شما فقط مشکل شما نیستند؛ بلکه ممکن است برای سایر شبکه‌ها نیز مساله‌ساز شوند. ممکن است فردی نخواهد علیه بیماریهای مسری واکسینه شود، اما بهرحال بخشی از جامعه‌ای است که در آن همزیستی وجود دارد.

آنچه که در این میان آزاردهنده است این است که هرساله برای امنیت اتفاقات بدی رخ میدهد، و هرچند تلاشهایی برای بهبود زیرساختهای امنیتی انجام می‌گیرد، اما برای هر گام به جلو، دو گام باید به عقب بازگشت. چرا که هکرها باهوش‌تر و در نتیجه تهدیدها خطرناکتر شده‌اند. و شاید بدلیل تنبلی یا بار کاری زیاد مدیران شبکه باشد.

در بیشتر موارد، مشکلات بزرگ امنیتی که هر روزه درباره آنها می‌خوانید، بخاطر وجود حملاتی است که برروی سیستمهایی صورت می‌گیرد که به علت عدم اعمال وصله‌ها، هنوز مشکلات قدیمی را درخود دارند.

بنابه عقیده بعضی، اکنون زمان استفاده از تدبیر براساس کرم! و ساختن کرمهای مفید برای ترمیم مشکلات است. البته هنوز اعتراضات محکمی علیه استفاده از آنها وجود دارد. اما در مواجهه با شبکه های zombie (کامپیوترهای آلوده ای که برای

حملات DoS گسترده، مورد استفاده قرار می گیرند) که تعداد آنها به دهها‌هزار کامپیوتر میرسد، مـی تواننـد یـک شـبه! توسـط کرمهای مفید از کار انداخته شوند.

البته، یک کرم مفید هنوز یک کرم است و بحث دیگری که در اینجا مطرح می شود این است که کرمها ذاتـا غیرقابـل کنتـرل هستند، به این معنی که کرمهای مفید هم باعث بروز مشکلات ترافیک می شوند و بصورت غیرقابل کنترلی گسترده می گردنـد. این مساله در مورد بیشتر کرمها صدق می کند، اما دلیل آن این است که تاکنون هیچ کس یک کرم قـانونی! و بدرسـتی برنامـه نویسی شده ایجاد نکرده است. می توان براحتی کنترلهای ساده ای همچون انقضاء در زمان مناسب و مدیریت پهنای باند را کـه این تاثیرات ناخوشایند را محدود یا حذف کند، برای یک کرم مفید تصور کرد.

اشکال وارده به ایجاد یک کرم قانونی و مناسب این است که زمان زیادی می طلبد، بسیار بیشتر از زمانی که یک کرم گسـترش پیدا می کند. در پاسخ می توان گفت بیشتر کرمها از مسائل تازه کشف شده بهره نمـی برنـد. بیشـتر آنهـا از شـکافهای امنیتـی استفاده می کنند که مدتهاست شناخته شده اند.

تعدادی پرسش وجود دارد که باید پاسخ داده شوند. چه کسـی ایـن کرمهـا را طراحـی و مـدیریت مـی کنـد؟ دولـت، CERT، فروشندگان یا اینکه باید تشکل هایی براه انداخت؟ برای ترمیم چه ایراداتی باید مورد اسـتفاده قـرار گیرنـد؟ رونـد اخطـار بـرای سیستمهایی که توسط یک کرم مفید وصله شده اند، چیست؟ آیا پیامی برای مدیر شـبکه بگـذارد؟ کـه البتـه هـیچ کـدام موانـع غیرقابل حلی نیستند.

بهرحال، بهترین کار مدیریت صحیح سیستمهایتان است، بنحوی که با آخرین ابزار و وصله های امنیتی بروز شده باشند. در ایـن صورت دیگر چندان نگران وجود کرمها در سیستمهایتان نخواهید بود.

آنچه که نمی توان در مورد آن با اطمنیان صحبت کرد، امن و موثر بودن یـک کـرم مفیـد اسـت، کـه ایـن مطلـب مطالعـات و تحقیقات جدی را می طلبد. بعلاوه اینکه، اگر برنامه نوشته شده در دنیای بیـرون متفـاوت از آزمایشـگاه رفتـار کنـد، چـه کسـی مسوولیت آنرا می پذیرد؟ مساله بعدی اینست که تحت قانون جزایی بعضی کشورها، هک کردن یک سیستم و تغییـر دیتـای آن بدون اجازه زیان محسوب می شود و چنانچه این زیان به حد مشخصی مثلا ۵هزار دلار برسد، تبهکاری بحساب می آیـد، حتـی اگر قانون جنایی حمایتی برای نویسندگان کرمهای مفید درنظر بگیرد. ایده اصلی در این بین، اجازه و اختیـار بـرای دسـتیابی بـه

کامپیوتر و تغییر دیتای آن یا انجام عملیاتی بر روی آن است. از منظر قانونی، این اجازه می تواند از طرقی اعطاء شود. بعلاوه اینکه سیستمهایی که امنیت در آنها رعایت نشود، اساسا به هر کس اجازه تغییر دیتا را می دهند.

خوشبختانه، روشهای محدودی برای اخذ اجازه وجود دارد. برای مثال، ISPها از پیش بواسطه شرایط خدمات رسانی به مشتریانشان اجازه تغییر دیتا را دارند. یک ISP معتبر ممکن است حتی سرویس بروز رسانی رایگان یک برنامه ضدویروس را نیز به مشتریانش ارائه کند.

راه دیگر اخذ اجازه از طریق پروانه های دولتی است. مثلا در بعضی کشورها، افسران پلیس این قدرت را دارند که بتوانند تحت قوانین محدود و شرایط خاصی وارد فضای خصوصی افراد شوند. مثال دیگر در مورد سارس است. افراد می توانند بخاطر سلامت عمومی قرنطینه شوند، اما فقط توسط افرادی که اختیارات دولتی دارند.

در آخر توجه شما را به یک مساله جلب می کنیم: اجرای قوانین سلامت بیشتر بصورت محلی است، در حالیکه اینترنت ماهیت دیگری دارد. ممکن است بتوان در بعضی کشورها به سوالات مربوط در مورد نوشتن و گسترش کرمهای مفید جواب داد، اما کاربران کشورهای دیگر را شامل نمی شود.