Viruses

ترجمه : داود راستي

http://www.RastiSoft.com

مقدمه:
ويروسهاي و برنامه هاي مخرب كامپيوتري امروزه توجه كاربران را بسيار به خود جلب كرده اند.از يک طرف آنها نشان ميدهند كه ما چقدر آسيب پذيريم و از طرف ديگر بيانگر پيشرفت و مهارت بشرند. براي مثال ويروس مليسا (**Melissa**) كه در مارس 1999 ميلادي به يک مشكل بزرگ و گسترده تبديل شده بود , ويروس قدرتمندي بود كه شركت Microsoft و چندين شركت بزرگ ديگر را واداشت كه خدمات دهنده **E-mail** خود را بطور موقت متوقف كنند تا مانع گسترش آن شوند. ويروس **I Love You** نيز در سال 2000 ميلادي اثرات مخرب مشابهي را بوجود آورد. اين موضوع وقتي شما را بيشتر متعجب خواهد كرد كه بدانيد اين دو ويروس از ساختار بسيار ساده اي برخوردارند.
ما در اين مقاله سعي كرده ايم شما را بيشتر با ويروسهاي سنتي و مدرن امروزي آشنا كنيم و راه هاي مقابله با آنها را براي شما بيان كنيم. ولي بايد بدانيد افرادي هستند كه, همواره به دنبال راه هاي جديدي براي ايجاد ويروسهاي مخرب كامپيوتري هستند.

انواع مختلف برنامه هاي مخرب و ويروسهاي كامپيوتري

ويروسها (Virus) : يک ويروس برنامه كوچكي است كه خود را به يک برنامه معمولي ديگر مي چسباند. زماني كه آن برنامه اجرا ميشود , كد برنامه ويروس نيز اجرا ميشود و فرصت آن را پيدا ميكند كه اثرات مخرب خود را بر سيستم وارد كند و يا خود را به برنامه هاي ديگر كه هنوز آلوده نشده اند متصل و آنها را نيز آلوده كند.
اين گونه از برنامه هاي مخرب را به اين دليل ويروس ميخوانند كه مانند ويروسها در دنياي واقعي, عمل ميكنند. آنها بطور خودكار از يک كامپيوتر به كامپيوتر ديگر منتقل ميشوند مانند ويروسها در دنياي واقعي كه از يک جاندار به جاندار ديگري منتقل ميشوند.
ويروسها در دنياي پزشكي يک موجود زنده اي نيستند.بر خلاف سلول, ويروس زنده نيست و راهي براي انجام كاري يا توليد مثل ندارد. در عوض **DNA** خود را درون سلول زنده جاي ميدهد سپس از مكانيزم سلول استفاده كرده و توليد مثل ميكند.در بعضي موارد كل سلول آكنده از ويروس ميشود و ميميرد. و در بعضي موارد سلول ميتواند زنده بماند.
ويروسهاي كامپيوتري نيز بعضي از خصوصيات ويروسهاي واقعي را دارند .آنها براي آنكه بتوانند اثر خود را برروي سيستم بگذارند نياز دارند كه خود را به برنامه هاي ديگر متصل كنند. وقتي برنامه آلوده اجرا ميشود, برنامه ويروس نيز اجرا ميشود و خود را به برنامه هاي ديگر موجود برروي سيستم متصل كرده و آنها را نيز آلوده ميكند. بر اساس اين خصوصيات است كه اين گونه از برنامه هاي مخرب را ويروس ميخوانند.

چگونگي انتشار ويروسها:
ويروسهاي اوليه برنامه هاي كوچكي بودند كه خود را به برنامه هاي معمولي مانند بازيها و يا واژه پردازها متصل ميكردند. كاربر ممكن است كه اين برنامه آلوده به ويروس را از راه هاي مختلف مانند اينترنت دريافت و اجرا كند. زماني كه برنامه آلوده اجرا شود , كد برنامه ويروس نيز به اجرا در مي آيد و در حافظه كامپيوتر جايي ميگيرد و اگر برنامه ديگري را برروي ديسک كامپيوتر پيدا كند, آن را نيز آلوده ميكند. زماني كه كاربر اين برنامه آلوده را برروي ديسكت به كاربران ديگر بدهد يا آن را برروي اينترنت قرار دهد و ديگر كاربران از آن استفاده كنند سيستم آنها نيز آلوده ميشود و به اين ترتيب ويروس گسترش پيدا ميكند.
مرحله گسترش ويروسها به اصطلاح سرايت خوانده ميشود. اگر فقط ويروسها به برنامه هاي ديگر سرايت ميكردند اوضاع چنان خطرناک نبود. شوربختانه بسياري از ويروسها بجز آلوده كردن برنامه هاي ديگر وظايف مخربي نيز بر عهده دارند.اين مرحله از عملكرد ويروس به اصطلاح "حمله" خوانده ميشود. اين مرحله ممكن است از چاپ يک پيام ساده برروي مانيتور تا ازبين بردن اطلاع موجود برروي كامپيوتر باشد. حمله ويروس ممكن است در تاريخ خاصي يا بعد از تكثير تعداد مشخصي از آن يا مواردي مشابه, صورت گيرد.
وقتي كه ويروس نويسان بيشتر در كار خود ماهر ميشدند ترفندهاي بيشتري ياد ميگرفتند. يكي از ترفندهاي مهم توانايي نوشتن برنامه هاي مقيم حافظه بود كه به ويروسها امكان ميداد تا زماني كه كامپيوتر روشن است در حافظه بمانند و برنامه هاي بيشتري را آلوده كنند.ترفند ديگر, توانايي آلوده كردن **Boot Sector** فلاپي

ديسک ها و ديسکهاي سخت بود **Boot Sectot** .شامل برنامه کوچکي است که به کامپيوتر ميگويد چگونه سيستم عامل (**operating system**) را Load و اجرا کند. اگر ويروس کد برنامه خود را در **Boot Sector** قرار دهد , هر بار که کامپيوتر راه اندازي ميشود , آن نيز اجرا ميشود و تا زماني که کامپيوتر روشن است فعال ميماند. ويروسهاي **Boot Sector** ميتوانند **Boot Sector** هر فلاپي ديسکي را که در کامپيوتر آلوده قرار ميگيرند, آلوده کنند و به اين ترتيب به راحتي توسط کاربران که از فلاپي ديسکهاي آلوده براي انتقال اطلاعات و برنامه هاي خود بين کامپيوترها استفاده ميکنند , منتشر شوند.
ويروسهاي قابل اجرا و ويروسهاي **Boot Sector** امروزه بسيار خطرناک نيستند. يکي از اين دلايل حجم بالاي برنامه هاي امروزي کامپيوتر است که معمولا آنها را برروي **CD** و يا **DVD** منتشر ميکنند. همانطور که ميدانيد برنامه هاي روي **CD** قابل ويرايش نيستندو ويروسها نميتوانند آنها را بعد از مرحله کپي برروي **CD** آلوده کنند. و به علت حجم بالاي برنامه ها نميتوان آنها را برروي فلاپي ديسکها منتقل کرد.ويروسهاي **Boot Sector** نيز کاهش يافتند زيرا سيستم عامل هاي امروزي از **Boot Sector** بخوبي محافظت ميکنند.ويروسهاي قابل اجرا و ويروسهاي Boot Sector باز هم وجود دارند ولي نميتوانند به سرعت و وسعت قديم منتشر شوند.

ويروسهاي ايميل (E-mail viruses) : يک **E-mail viruse** کدبرنامه مخربي است که در بدنه يک ايميل جاي ميگيرد و از طريق آن منتشر ميشود و سپس به بصورت خودکار با استفاده از آدرس ايميلهاي موجود در **Address Book** فرد قرباني, منتشر ميگردد و سيستم آنها را نيز آلوده ميسازد و بدين ترتيب بسرعت گسترش پيدا ميکند.
E-mail viruseها مدرنترين ويروسهاي امروزي هستند . يکي از بارزترين آنها, ويروسي بنام مليسا (**Melissa**) است که در مارس سال 1999 مشکلات بزرگي را ايجاد کرد. مليسا در اسناد ايجاد شده توسط برنامه **Microsoft Word**جاي ميگيرد و از طريق ايميل منتشر ميشود. داستان به اين صورت آغاز شد که فردي ويروس مليسا را در يک سند **Word** جايي داد و آن را در يک گروه خبري اينترنت (**newsgroup**) قرار داد. کاربران زيادي اين سند را دريافت و باز کردند و در اين موقع ويروس برروي کامپيوتر آنها فعال شد. ويروس مليسا سند آلوده را از طريق ايميل براي 50 آدرس ايميل اولي که در **Address Book** کامپيوتر آلوده قرار داشت ,ارسال کرد و همين کار را در کامپيوتر هاي آلوده ديگر هم انجام داد. عنوان ايميل هاي ارسالي دوستانه بود و نام شخص گيرنده نيز در آن قرار داشت. بنابراين شخص گيرنده ايميل را باز ميکرد و کامپيوتر او نيز آلوده ميشود. به اين ترتيب ويروس مليسا سريعتر از آنچه که تصور ميشد گسترش يافت و بسياري از شرکتهاي بزرگ را وادار کرد که براي مدتي خدمات دهنده ايميل خود را متوقف کنند.
ويروس **I Love You** که در 4 مي 2000 ظاهر شد حتي ساده تر از مليسا بود. اين ويروس برنامه کوچکي بود که به ايميلي با عنوان **I Love You** متصل (**attachment**) شده بود. زماني که کاربر اين ايميل را باز ميکرد و برروي برنامه الحاق شده به آن, دبل کيليک ميکرد, کد برنامه مخرب اجرا ميشد و خود را در **Address Book** کامپيوتر فرد قرباني کپي ميکرد.
ويروس مليسا از خاصيت زبان برنامه نويسي موجود در **Microsoft Word** به نام **VBA** يا **Visual Basic for Applicatin**) بهره بر. **VBA** يک زبان کامل برنامه نويسي است که ميتوان از آن براي نوشتن برنامه هايي که امکان ويرايش فايلهاي موجود برروي سيستم و فرستادن ايميل را دارند , استفاده کرد. همچنين ويژگي مفيد و در اين حال خطرناک **auto-execute** يا اجرا خودکار را نيز دارد.برنامه نويس ميتواند برنامه خود را در اسناد **Word**قرار دهد و به محض اينکه کاربر سند را باز کند برنامه نيز اجرا ميشود و اين خاصيتي بود که ويروس مليسا از آن بهره گرفته بود. هرکس که سند آلوده به مليسا را باز ميکرد , ويروس بطور خودکار فعال ميشد. اين ويروس علاوه بر فرستادن سند آلوده از طريق ايميل براي ديگر کاربران , فايل مرکزي **NORMAL.DOT** را نيز آلوده کرده و کد خود را در آن کپي ميکرد. بنابراين از آن به بعد تمام اسنادي که توسط کاربر ايجاد ميشد آلوده به ويروس مليسا بود.
برنامه **Microsoft Word** و ديگر برنامه هاي مايکروسافت خاصيتي بنام **Macro Virus Protection** براي جلوگيري از ويروسهايي مانند مليسا دارند. زماني که اين ويژگي فعال باشد (که بطور پيش فرض فعال است) , خاصيت **auto-execute** غير فعال ميشود. بنابراين زماني که سند سعي کند که کد برنامه موجود در خود را اجرا کند , يک پنچره اخطار براي کاربر نمايش داده ميشود. شوربختانه بسياري از کاربران با ويروسهاي ماکرو آشنا نيستند و اين پيغام را ناديده ميگيرند و برنامه درون سند را بدون مطمئن بودن از صحت آن , اجرا ميکنند. بعضي از کاربران نيز از قبل ويژگي **Macro Virus Protection** را غير فعال ميکنند. بنابراين ويروسهاي مانند مليسا براحتي منتشر ميشوند.

در مورد ويروس **I Love You** تا زماني كه كاربر برروي برنامه الحاقي درون ايميل دبل كيليک نكند , فعال نميشود. چيزي كه باعث تحريک كاربر براي باز كردن برنامه الحاقي شد عنوان ايميل بود.

كرمها (Worms) : يک برنامه كوچک است كه با استفاده از ضعف امنيتي يا به اصطلاح حفره هاي امنيتي شبكه هاي كامپيوتر منتشر ميشوند و اثرات مخرب خود را بر جاي ميگذارند.
كرمها برنامه هاي هستند كه ميتوانند خود را از يک كامپيوتر بروي كامپيوتر ديگري, از طريق شبكه كپي كند. يک كپي از **Worm** ميتواند از طريق شبكه هاي كامپيوتري بسرعت گسترش يابد. براي مثال در 19 جولاي سال 2001 ,برنامه مخرب **Code Red** كه يكي از انواع كرمهاست توانست خود از طريق شبكه جهاني اينترنت در مدت فقط 9 ساعت 250000 بار تكثير كند و سيستمهاي بسياري را آلوده كند.
كارشناسان اعلام كردند كه **Code Red** ميتواند آسيبهاي بزرگي به شبكه جهاني اينترنت وارد كند. اين **Worm** توانست ترافيک اينترنت را بهنگام تكثير خود بشدت آهسته كند ولي نه آنقدر بد كه كارشناسان پيش بيني كرده بودند.هر كپي از **Code Red** شبكه اينترنت را براي يافتن خدمات دهنده هاي وبي كه از **Windows NT**و يا **Windows 2000** بهره مي بردند , جستجو ميكرد و اگر خدمات دهنده مورد نظر ضعف امنيتي داشت , يک نسخه از خود را برروي آن كپي ميكرد و كپي آن نيز دوباره همين عمل را براي يافتن خدمات دهنده هاي ديگر, انجام ميداد. اين **Worm** توانست صدها هزاران نسخه از خود را ايجاد كند.

Code Redبراي انجام سه عمل زير طراحي شد:

- در 20 روز اول هر ماه خود را تكثير كند.
- صفحات خدمات دهنده وب مورد حمله واقع شده را با صفحه اي كه جمله "**Hacked by Chinese**" رانمايش ميدهد,جايگزين كند.
- حمله هماهنگ و همه جانبه اي را به كامپيوتر خدمات دهنده وب سايت كاخ سفيد آمريكا , به منظور از كار انداختن آن انجام دهند.

دولت آمريكا براي جلوگيري از آسيب رسيدن به وب سايت كاخ سفيد (**http://www.whitehouse.gov**) تصميم گرفت كه **IP Address** آن را عوض كند و همچنين يک اخطار عمومي مبني بر اثرات مخرب **Code Red** منتشر كرد و به كاربران**Windows NT** و **Windows 2000** استفاده از وصله هاي امنيتي (**security patch**) براي رفع حفره ي امنيتي كه **Code Red** براي نفوذ در كامپيوترها از آن استفاده ميكند , را توصيه كرد.

اسبهاي تروا (Trojan horses) : برنامه هاي ساده اي مانند يک بازي كوچک هستند كه علاوه بر برنامه اصلي, شامل كدهاي مخربي نيز هستند و هنگام اجراي برنامه , اثرات نامطلب خود را نشان ميدهند. براي مثال ممكن است اطلاعات موجود برروي ديسک سخت شما را از بين ببرند و كارهايي از اين قبيل. اسبهاي تروا برخلاف ويروسها بطور خودكار منتقل نميشوند.

راه هاي پيشگيري

شما ميتوانيد با انجام چند عمل ساده جلوي آسيب رسيدن به سيستم خود از طرف انواعي از ويروسها بگيريد.
اگر شما واقعا از ويروسهاي سنتي و قديمي بيمناک هستيد . از سيستم عاملهاي **secure operating system**مانند **Windows NT**, **Windows 2000/XP**و **UNIX** استفاده كنيد. بدليل آنكه اين گونه از سيستم عاملها در مقابل ويروسهاي **Boot Sector** و اجرايي سنتي امنيت بيشتري دارند.
اگر از سيستم عامل هاي غير **secure operating system** بهره ميگيريد از نرم افزارهاي **virus protection software** ياضد ويروس استفاده كنيد.
اگر شما برنامه هاي نامشخص و غير مطمئن را اجرا نمي كنيد, گام بزرگي براي محافظت كامپيوتر خود از ويروسهاي سنتي برداشته ايد. علاوه بر اين بايد خاصيت **floppy disk booting** كه امكان بوت شدن كامپيوتر از طريق فلاپي ديسک را ميدهد غير فعال كنيد تا سيستم شما در مقابل ويروسهاي **Boot Sector** كه ممكن است ديسكت آلوده به آن را بطور اتفاقي در ديسكگردان قرار دهيد, محافظت شود.
حتما مطمئن شويد كه ويژگي **Macro Virus Protection** در برنامه هاي مايكروسافت فعال باشد و هرگز برنامه هاي موجود در اسناد را تا زماني كه از عمل كرد آنها اطمينان حاصل نكرديد , اجرا نكنيد.

در مواردي مانند ويروس **I Love You** بهترين محافظت آن است كه هرگز تا از نوع فايل الحاقي به ايميل مطمئن نشده ايد برروي آن دبل كيليک نكنيد كه اجرا شود. فايلهاي با پسوند **EXE,COM,VBS** قابل اجرا هستند و ممكن است نوع عمل كرد آنها به سيستم شما آسيب برسانند. فايلهاي گرافيگي مانند **JPG** و **GIF** و همچنين بعضي از فايلها مانند **XLS** (**spreadsheets**) از نوع داده اي هستند و نمي توانند به سيستم شما آسيب برسانند بجز فايلهايي كه ممكن است داراي مشكل ويروسهاي ماكرو باشند مانند اسناد **Word** و **Excel,** كه ميتوانيد با فعال كردن ويژگي **Macro Virus Protection** مانع آسيب رساندن آنها به سيستم خود شويد.
شما با بكار گيري اين اقدامات ساده ميتوانيد بطور وسيعي كامپيوتر خود را در مقابل انواع ويروسها و برنامه هاي مخرب محافظت كنيد.

چه كساني و چرا ويروسها و برنامه هاي مخرب را خلق ميكنند؟

انسانها ويروسهاي كامپيوتري را خلق ميكنند. بعضي از افراد برنامه هاي مخربي مي نويسند كه اين برنامه ها ممكن است براي نمايش يک پيغام ساده و احمقانه تا انجام اعمال تخريبي مانند از بين بردن داده هاي برروي سيستم طراحي شده باشند .

اين افراد براي كار خود چه دليلي دارد؟

- نخست به همان علت رواني كه فردي پنچره اتومبيل شخص ديگري را ميشكند يا چرخ آن را بدون دليل پنچر ميكند.بعضي از اين افراد اگر تخصصي در برنامه نويسي داشته باشند سعي ميكنند تمام انرژي و توان خود را صرف ايجاد برنامه ها و ويروسهاي مخرب كنند.

- دليل دوم را ميتوان اينگونه بيان كرد كه بعضي افراد از تخريب كردن و از منفجر كردن اشيا مانند اتومبيل و از اين قبيل لذت ميبرند .براي مثال بعضي از كودكان ياد ميگيرند كه چگونه با باروت و مواد انفجاري, بمب هاي كوچک بسازند و از آنها استفاده كنند و رفته رفته با گذر زمان وقتي مهارت بيشتر مي يابند بمب هاي بزرگتر و خطرناكتر ايجاد ميكنند كه ممكن است به خود و يا اطرافيان خود آسيب برسانند. ايجاد ويروس و برنامه هاي مخرب را ميتوان ايجاد يک بمب خطرناک در كامپيوتر دانست كه ميتوان با آن به كامپيوترهاي زيادي در سرتاسر جهان آسيب رساند.

- دليل سوم را ميتوان به علاقه بعضي افراد به خودنمائي ربط داد. اينگونه افراد اگر در برنامه نويسي خبره باشند سعي ميكنند تا از آن براي مطرح كردن خود استفاده كنند. آنها اگر مشكل امنيتي در يک سيستم ببينند سعي ميكنند قبل از آنكه فرد ديگري به آن نفوذ كند , خود آنها اين كار را انجام دهند.

البته بسياري از افرادي كه به ايجاد برنامه هاي مخرب مي پردازند به اين نكته توجه ندارند كه كار آنها باعث واردكردن زيان به ديگران ميشود.از بين بردن داده هاي موجود برروي ديسک سخت افراد ديگر ميتواند زيان بزرگي به آنها وارد كند.مدت زماني كه كارمندان يک شركت بزرگ براي رفع مشكلات ايجاد شده توسط يک ويروس كامپيوتري , صرف ميكنند ميتواند ضرر مالي فراواني به شركت وارد كند. حتي پيغام هاي ساده و احمقانه كه بعضي از ويروسها برروي مانيتور نمايش ميدهند ميتواند زيان آور باشد چون كاربر ناچار است زماني را براي خلاص شدن از اين مشكل صرف كند.از اين رو قانون برخورد شديدي را با كساني كه ويروس و برنامه هاي مخرب ايجاد ميكنند , به عمل مي آورد.

تاريخچه ويروسها و برنامه هاي مخرب

ويروسهاي سنتي در اواخر دهه 80 ميلادي بطور چشمگيري مطرح شدند و ميتوان چند دليل را براي اين امر بيان كرد.يكي از دلايل آن گسترش استفاده از كامپيوترهاي شخصي (**PC**)بود.در سال 1982 شركت **IBM** كامپيوترهاي شخصي خود را كه به **PC** معروف شد وارد بازار كرد و در سال 1984 شركت **Apple** كامپيوترهاي خود را عرضه كرد. در دهه 80 استفاده از كامپوترهاي **PC** به سرعت در مشاغل مختلف ,خانه ها و كالجها گسترش يافت.
دليل دوم را ميتوان استفاده مردم از تابلو اعلانات كامپيوتري (**computer bulletin board**) دانست. كاربران ميتوانستند با استفاده از خط تلفن و مودم به اين **bulletin board** متصل شوند و برنامه هاي مختلف موجود در آنها را دريافت كنند. بازي هاي كامپيوتري و واژه پردازها بترتيب محبوبترين برنامه هايي بودند كه كاربران دريافت ميكردند. اين وضعيت موقعيت مناسبي را براي گسترش برنامه هاي مخرب از نوع اسب تروا (**Trojan horse**) را

فراهم کرد.خوشبختانه اینگونه از برنامه ها سریع شناساي میشوند و میتوان کاربران دیگر را از خطرات آنها آگاه کرد.
یکي دیگر از دلایل گسترش ویروسهاي کامپیوتري در دهه 80 را میتوان استفاده فراوان از فلاپي دیسکها در آن سالها دانست. در آن موقع حجم برنامه ها بسیار کم بود و کاربران براي انتقال آنها از فلاپي دیسک استفاده میکردند این امر باعث میشد که یک برنامه آلوده براحتي بین کاربران دیگر رد و بدل شود. در آن زمان بسیاري از کامپیوتر ها دیسک سخت نداشتند و کاربر سیستم خود را با استفاده از دیسکت هاي شامل سیستم عامل بودند, راه اندازي میکردند.
این سه فاکتور از عمده ترین دلایل گسترش ویروسها در دهه 80 بود.

امید است که مطالب این مقاله براي شما مفید واقع شده باشد. بزودي مقالات بیشتري درباره ویروسها و برنامه هاي مخرب دیگر و همچنین راه هاي مقابله با آنها , در سایت ***RastiSoft*** ارائه خواهد شد.

ترجمه : داود راستي

RastiSoft is yours!
http://www.RastiSoft.com