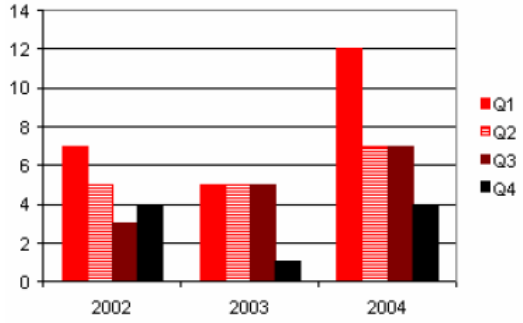
بررسی عوامل شیوع و گسترش کرم های اینترنتی و روشهای مقابله با آنها

محمدرضا فغانی
دانشگاه صنعتی اصفهان
mr_faghani@yahoo.com

چکیده : درسال های اخیر تقریبا هرماه خبری ناشی از تهدید کرم های اینترنتی برای کاربران شنیده ایم ، شیوع و گسترش این دسته از بدافزارها[1] نه تنها خطر آلودگی کاربران را دربر دارد بلکه بار ترافیکی شبکه را نیز به صورت نمایی افزایش می دهد[8]، این ترافیک ناشی از شیوع و گسترش خودکار این دسته از بدافزارها می باشد. آلودگی ناشی از تعدادی از این نوع بد افزارها خود موجب آسیب پذیری بیشتر کاربران به خطرات احتمالی دیگر می شود. در این مقاله پس از انتخاب یك مدل مناسب براي پخش يك كد ويروسی و راههايي كه اين گونه برنامه ها براي پخش شدن استفاده مي كنند درهر مرحله به معرفي راه كارهايي براي مقابله با انتشار آنها مي پردازيم.معرفي IDS ، فن آوری های جدیدی که در این زمینه به وجود آمدند مانند Honeypot، پيشنهاد توپولوژي هاي بهينه شبكه براي كنترل بهتر سرعت پخش، محدود كردن امكانات كاربران شبكه در بعضي از موارد از نظر مديريت شبكه از موارد بحث شده در این مقاله عنوان می باشند.

1- مقدمه

آخرين اطلاعات آماري گرفته شده بر مبناي مقايسه مجموع آلودگي به انواع بدافزارها در اولين فصل سال2004 نسبت به همان فصل در سال 2003 در نمودار زير ترسيم شده است[1].



شكل 1-1 مقايسه مجموع آلودگی ها در سال های 2002 تا 2004

اين پرش ناگهاني مي تواند به خاطر افزايش سرعت خود شبكه ونيز گستردگي روز افزون آن باشد، از دلائل ديگر اين مسئله مي توان به قدرتمندتر شدن زبان هاي برنامه نويسي و راحتي استفاده در عين پيچيدگي از آنها اشاره كرد. سيستم هاي پست الكترونيكي در عين غني شدن در تنوع سرويس هايي كه ارائه مي دهند، خود به صورت ناخواسته عامل موثري در پخش كرم هاي اينترنتي هستند و نويسندگان بد افزارها براي افزايش گستردگی آلودگي، اين گونه برنامه ها را در قالب نامه هايی با عناوين فريب دهنده قرار مي دهند. امروزه با توجه به مسئله پهنای باند و سرعت در امر ارتباطات، این مورد یعنی گسترش کرم های اینترنتی از این جهت که موجب افزایش بار ترافیکی شبکه نیز می شود، حائز اهمیت است.

---

[1] Malwares

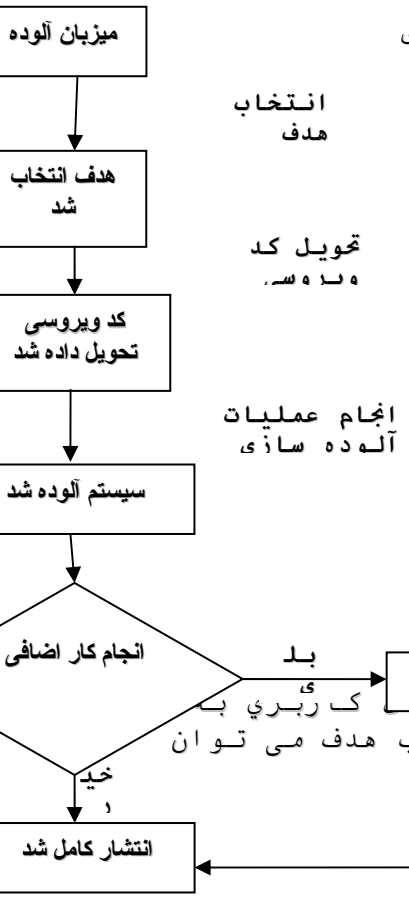
کرم های اینترنتی سالیانه ضرر های مالی بسیاری را به شرکت های مختلف می زند، از آن جهت که با نفوذ به داخل کامپیوتر کاربران این قابلیت را نیز دارند که اطلاعات محرمانه آنها را به سرقت برند و یا آن را در معرض دید دیگران قرار دهند. .لذا لازمه مبارزه با این گونه بدافزارها دانستن راه و روشهای نفوذ آنان است پس بایستی ابتدا این گروه از بد افزارها را بهتر بشناسیم.
براي اين كار مي بايست مكانيزم پخش شدن را بررسي كنيم تا بتوانيم با ارائه يك مدل مناسب براي پخش و نفوذ بد افزارها به بررسي راهكارهاي مقابله بپردازيم.

2- مدل كلي براي پخش

تجزيه و تحليل بسياري از بدافزارها نشان مي دهد كه آنها راههاي مشخصي را براي گسترش استفاده مي كنند.
در اين مقاله تعدادي از ويروس هايي كه در چند سال اخير دارای قدرت تخریب بیشتری بوده و گسترش فراوانی یافته اند را مورد بررسی قرار داده ایم.بررسی ها نشان داد که این دسته از بد افزارها تقریبا روشهای مشابهی را برای آلوده ساختن و گسترش استفاده می کنند. لذا با در نظرگرفتن یک مدل کلی راه های آلوده سازی آنها را مورد مطالعه قرار می دهیم.

3- مدل پخش

در شکل مقابل مدل کلی برای پخش یک کد ویروسی نشان داده شده است. در این مدل مراحلی را که یک بد افزار برای آلوده سازی انجام می دهد، به ترتیب آورده شده اند.



شکل 3-1 الگوریتم پخش بدافزارهای اینترنتی

3-1- انتخاب هدف

انتخاب هدف در واقع روشي است كه در آن بد افزار با كاربري به عنوان هدف مي گردد ، از روش هاي استفاده شده برای انتخاب هدف می توان

1. آدرس هاي IP
2. بدست آوردن آدرس هاي Email
3. انتقال فايل

را نام برد، روش ديگري كه در اين دسته مي توان اضافه كرد، آلودگي از طريق صفحه هاي وب است. در اين روش كه با سوء استفاده از آسيب پذيري[1] هاي موجود در سيستم عامل هاي مختلف ويا نرم افزارهای مرورگر همراه است، كاربربا ديدن يك صفحة وب حاوی بد افزار ممكن است به صورت ناخود آگاه آلوده شود.اين روش را در قسمت هاي بعد بيشتر توضيح خواهيم داد. از جملة اين ويروس ها مي توان Redlof وNimda را نام برد.

3-2- تحويل كد ويروسي به كاربر هدف

روشهايي كه مي تواند در اين قسمت استفاده شود از قرار زير است:

1. اشتراك هاي شبكه
2. پست الكترونيك
3. از طريق وب
4. دسترسي راه دور به كامپيوتر
5. يك Payload مرتبط با سرريز بافر

بعضي از بد افزارها هنگام تحويل كد ويروسي تنها قسمتي از كد آلوده را تحويل مي دهند و مابقي را هنگامي كه سيستم به صورت كامل تسخير شد انتقال خواهند داد، از جمله اين بدافزارها مي توان هيبريدهای كرم/ اسب تراوا را نام برد.

3-3- اجراي كد ويروسي

اجراي يك كد ويروسي مي تواند با راههاي زير در ارتباط باشد.

1. آسيب پذيري نرم افزارهاي پست الكترونيكي
2. دخالت كاربر
3. اجراي خودكار(براي مثال استفاده از كليدهاي شروع خودكار در ويندوز)
4. آسيب پذيري نرم افزارهاي مرور گروب
5. سرريزبافر

3-4- داشتن Payload

وقتي كه سيستم به صورت كامل تسخير شد، بدافزارها ممكن است Payload هايي را اجرا كنند، Payload به آن دسته از كارهايي كه توسط بدافزار علاوه بر آلوده سازی انجام مي شود، اطلاق می گردد. مانند به جا گذاشتن راهي براي نفوذ يا به اصطلاح در پشتي[2] ،پخش شدن در خود كامپيوتر و آلوده ساختن فايلهاي محلي و يا انجام Denial of Service دربرابر يك پايگاه وب.

3-5- انتقال اضافي

بعضي از بدافزارها مثلا براي داشتن حجم كمتر هنگام آلوده سازی كاربران، به انتقال قسمتي از خود مي پردازند. وقتي كامپيوتر كاربر به طور كامل تسخير شد مابقي كد انتقال پيدا خواهد كرد، اين انتقال مي تواند از طرق زير انجام شود.

1. FTP/TFTP
2. فايلهاي شبكه

4- جلوگيري از پخش شدن

با دانستن راه كارهايي كه بدافزارها براي گسترش استفاده مي كنند مي توان به راحتي به مقابله با آنها پرداخت.

---

[1] Vulnerabilities
[2] Backdoor

4-1- انتخاب هدف

در اين قسمت بدافزار به دنبال يك كاربر مي گردد يعنی همان سيستم هايي كه براي آلوده شدن مناسب هستند.

4-1-1- آدرس هاي IP

اين روش توسط آن دسته از بدافزارهاي استفاده مي شود كه براي سوء استفاده از آسيب پذيري مشخصي تلاش مي كنند، بسياري از كرم هاي اينترنتی امروزي براي آلوده كردن كاربران از اين روش استفاده مي كنند از اين دسته از كرم ها مي توان Blaster را نام برد اين كرم از حمله هاي SYN Packet براى سوء استفاده از آسيب پذيري سرويس RPC استفاده مي كند. Slammer نيز با استفاده از UDP به توزيع خود مي پردازد، پس از آن كه اين كرم اجرا شد به يك حلقة بي انتها براى توليد آدرس هاى IP تصادفی مي رود، پس از آنكه هر IP توليد شد خودش را به آدرس IP توليد شده مي فرستد در اين صورت اگر سرور SQL اين بسته را دريافت كند آن را به صورت ناخواسته اجرا خواهد شد (سريزبافر[1]) و خود موجب يك منبع آلودگي ديگر مي شود.
Sasser.B نيز كه سومين ويروس خطرناك سال گذشته شناخته شد [2] از طريق توليد آدرس IP تصادفی به انتخاب كاربران جهت آلوده ساختن آنها اقدام می نمود، قابل توجه آن كه اين ويروس در هر ثانيه 5120 حمله را انجام مي دهد.
اين گونه حمله ها در اين چند سال اخير موجب تخريب بسياري شد. بيشتر سرورهاي آسيب پذير در دنيا به خاطر فعال بودن سرويس "خاموش شدن سيستم به محض خطاهاي سيستمي" در ويندوز به محض آلوده شدن به كرم هاي Blaster و Sasser در عرض يك دقيقه خود به خود خاموش مي شدند و ضررهاي مالي بسياري را به همراه آوردند.
كرم اينترنتي Slammer نيز موجب از كار افتادن سرورهاي SQL بسياري در دنيا شد و كاربران ديگر قادر به بازيابي اطلاعات خود تا مدتی نشدند.
در روش هاي گفته شده همگي ويروس ها پس از انتخاب كاربر آسيب پذير با برقراري يك ارتباط و يا ارسال يك بسته آلوده كد را انتقال مي دادند، پس مي توان براي جلوگيري از آلودگی توسط روش هاي فوق با نصب يك Firewall به كنترل بسته هاي اينترنتي وارد شده به كامپيوتر پرداخت و در صورتي كه بسته اي ناخواسته قصد ورود به سيستم را دارد مانع از ورود آن شد.
فن آوري قابل استفاده ديگر نيز وجود دارد و آن استفاده از[2] IDS است.
IDS به بررسي ارتباطات ورودي با پورت ها می پردازد، مثلا پورتهايی كه غير مجاز براي كاربران عادي هستند و يا پورت هايي كه سرويسي در آن ارائه نمي شود، غالبا ارتباط با اين گونه پورتها مربوط به فعاليت يك نفوذگر براي يافتن يك پورت آسيب پذير براي ورود مي باشد.
استفاده از فن آوري Honeypot نيز يك روش جالب در مقابله با كرم هاي اينترنتي به حساب مي آيد. با استفاده از آنها مي توان بار ترافيكي حاصل از فعاليت كرم هاي اينترنتي(ارسال بسته هاي آلوده به هدف هاي نامشخص) به سرورهايي كه بدين منظور طراحي شدند انتقال داد تا سرعت گسترش آن به جاهاي ديگر كاهش يابد. يك راه حل كه Honeypot مي تواند براي مقابله با اين چنين حملاتی پيش روي ما بگذارد(كند كردن پويش كامپيوتر كاربر ويا حتی متوقف ساختن آن) به نام Sticky Honeypot شناخته مي شود. اين كار بوسيلة نظارت بر IP هايي كه قابل استفاده نيستند انجام مي شود، هنگامي كه اين گونه Honeypot ها با يك پويش تصادفي مواجه مي شود ، وارد عمل شده و حمله كننده را كند مي كنند، اين كار بوسيله چند حقه در TCP انجام مي

---

[1] **Buffer Overflow**
[2] Intrusion Detection System

شود مانند Window size به مقدار صفر و یا قرار دادن حمله کننده در حالت hold. از این دسته Honeypot ها می توان LaBrea Tarpit را نام برد[10و9].

4-1-2- آدرس هاي Email

بسیاري از بدافزارها از طریق راههاي زیر به جمع آوري پست الکترونیک اشخاص مي پردازد.

1. جستجو در میان فایلهاي محلي کامپیوتر مانند EML , TXT, HTML , HTM, WAB, MHT, HLP , DBX (این روش تقریبا در تمام کرم های اینترنتی امروزی رایج است که از آنها می توان Netsky و Mydoom را نام برد).
2. جستجوي کلیدهاي رجیستری و یا شاخه هاي نرم افزارهاي پیغام رسان براي یافتن آدرس های پست الکترونیک افراد ویا شناسة کاربري آنها، از این دسته بد افزارها می توان Nyxem را نام برد.
3. فرستان درخواست HTTP GET براي پایگاههاي وب حاوي آدرس هاي پست الکترونیک مانندemail.people.yahoo.com براي بدست آوردن آدرس ها پست الکترونیک مانند کرم Evaman.C.

از آن جا که روش اول یك روش کاملا مجاز در سیاست امنیتی هر سیستم عامل وجود دارد، مي توان تنها با گذاشتن محدودیت بر روي دسترسي کاربران به بعضي از قالب هاي فایل مانع از جمع آوري پست الکترونیك توسط بدافزارها شد.
کاهش دادن حق دسترسي تا سطح مدیر شبکه براي دسترسي به شاخه هاي برنامه نصب شده نرم افزارهاي پیغام رسان و آن دسته از کلیدهاي رجیستری که حاوي پست الکترونیك و یا شناسة کاربري افراد هستند مي توانند مانع از دسترسي بدافزارها به آنها شود.
استفاده از Firewall نیز، راه بدافزار را برای استفاده از روش سوم به طور قطع خواهد بست.

4-1-3- تبادل فایل

بعضي از انواع بدافزارها براي گسترش خود به استفاده از امکانات شبکه هاي محلي مي پردازند، کاربران مي توانند مثلا با استفاده از پروتکل Net Bios فایلها و چاپگرهاي خودشان را به اشتراك بگذارند، بسیاري از کاربران از فایلهاي یکدیگر در یك شبکة محلي به صورت مشترك استفاده مي کند و این خود باعث آن شده که بدافزارهایي مانند SDBOT اشتراك هاي شبکه اي را براي IP هاي تصادفي تولید شده توسط خودش پویش کنند. اگر اشتراك شبکه داراي حق دسترسي کامل باشد، تلاش خود را براي کپي کردن نسخه اي از خود درون شاخه های شروع[1] کامپیوترهای آسیب پذیر انجام مي دهد ،اگر اشتراك های شبکه دارای محدودیت ورود باشند این گونه بد افزارها معمولا با استفاده از لیستي از کلمات عبور و نام کاربر که در اختیار دارند تلاش خود را برای دسترسی به شاخه ادامه می دهند،. درصورت صحیح بودن شناسه کاربري و کلمة عبور وارد شده، بد افزار نسخه ای از خود را درون آن شاخه های شروع قرار می دهد. یکی از شاخه های شروع می تواند \Documents and Settings\All Users\Start Menu باشد.
روشهای دیگری نیز وجود دارد، مثلا Nimda با سو استفاده از IIS هاي آسیب پذیربه IIS web Directory traversal ، آدرس هدف هاي خودش را از بعضي از کلیدهاي رجیستری کامپیوتر آلوده شده بدست مي آورد[7].
همچنین Nimda با استفاده از آسیب پذیري "افزایش امکانات کاربري" مي تواند فرامیني را نیز روي کامپیوتر شخص آلوده، اجرا کند[7].

---

[1] Startup

بعضي از بدافزارها براي گسترش خود از نرم افزارهاي اشتراك عمومی Peer to Peerمانند Kazaa و يا Morpheus استفاده مي كنند.
BAGLE.J يك نسخه از خودش را با عنوان فريبنده در شاخة اشتراك گذاشته شده توسط اين گونه نرم افزارها كپي مي كند، مانند MacAfeeCrack.EXE ، اين امر باعث شده كاربرانی كه به دنبال نرم افزار خاصی هستند با بارگذاری[1] فايل مربوط و اجرای آن به اين بدافزار آلوده شوند مثالهاي ديگر از اين دسته مي تواند NETEKY.P و يا OPASERV باشد[7].
غير فعال كردن پروتكل NetBIOS ، استفاده از كلمات عبور قوي براي شاخه هاي به اشتراك گذاشته شده در پروتكل SMB ، از بين بردن آسيب پذيري هاي سيستم عامل و مرورگرها و نصب كردن Firewall مي تواند موجب جلوگيري از آلودگي هنگام تبادل فايل گردد.

4-2- تحويل كد ويروسي

در اين قسمت در مورد روشهايي كه بدافزارها براي انتقال كد آلوده به كاربر انجام مي دهند مطالبي را بيان مي كنيم.

4-2-1- اشتراك شبكه

در قسمت 4-1-3 مطالبي را در رابطه با چگونگي جلوگيري از استفاده از اين روش براي بدافزارها بيان كرديم از آن جمله استفاده از كلمات عبوري قوي و غيره.
مي توان با "فقط خواندني" كردن شاخه هاي اشتراك و يا شاخه های شروع براي كاربراني كه از دور[2] از اين شاخه ها استفاده مي كنند، مانع از قرار گرفتن بدافزارها روي اين شاخه ها شد. روش ديگر مي تواند بررسي محتواي فايلهايي كه در حال رد و بدل شدن هستند باشد. اين كار را بهتر است در حين تبادل فايل انجام داد تا آن كه فايل بصورت كامل روي كامپيوتر مستقر شود.
حداقل يك آنتي ويروس وجود دارد كه اين كار را انجام مي دهد و آن Edition Symantec Coporate 2004 است كه داراي ويژگي پويش فايلها بصورت real - time می باشد، عيب اين روش تنها اين است كه آنتي ويروس براي فدا نشدن سرعت مي بايستي از روش امضاي ويروس استفاده كند. در اين روش آنتي ويروس داراي يك پايگاه داده از امضاي ويروس هاي كشف شده است كه با استفاده از آن مي تواند فايلهاي حاوي ويروس ها را تشخيص دهد، لذا ويروس هاي جديد با اين روش قابل شناسايي نخواهد بود تا زماني كه يك امضاي مناسب براي آن پيدا شود.
استفاده از NIDS[3] راه ديگري براي جلوگيري از انتشار بدافزارها از طريق شبكه مي باشد.
NIDS بسته هاي اطلاعاتي در حال تبادل درون شبكه را تجزيه و تحليل مي كند اين فن آوري خود از تكنيكهايی مانند Packet Sniffing استفاده مي كند.نظارت مداوم بر روي بسته هاي اطلاعاتي موجب آن شده است كه NIDS در تشخيص دسترسي غير مجاز اشخاص وسيلة مناسبي باشد[12].
روش ديگر مي تواند استفاده از فن آوري هاي جديدي file integrity باشد. يك مثال بسيار شاخص در اين زمينه Tripwire است اين نرم افزار به جاي آنكه در تشخيص تكيه بر امضاهاي بدافزارها داشته باشد، يك تصوير[4] كلی از وضعيت سيستم در حالي كه به هيچ بدافزاري آلوده نيست همواره در اختيار

---

[1] Download
[2] Remote
[3] Network Intrusion Deteetion System
[4] Snapshot

دارد به محض مشاهدة تغييري در اين وضعيت به كاربر هشدار خواهد داد كه تغييري در وضعيت سيستم سالم انجام گرفته است[11].
از آن جا كه اين تغيير مبتني بر تصوير اوليه از كامپيوتر شما ونه بر مجموعه اي از امضاهاست مي تواند در تشخيص بدافزارهاي جديد بسيار موثر واقع گردد.

4-2-2- پست الكترونيك

بسياري از بدافزارها امروزه از اين روش براي گسترش خود استفاده مي كنند. همانطور كه در قسمت 4-1-2 بحث شد آن ها آدرس پست الكترونيك ديگران را روي كامپيوتركاربر آلوده جمع آوري مي كنند و به آنها پست الكترونيك حاوي بدافزار ، با عناوين فريبنده ارسال مي كنند.
كرم Netsky كه خطرناك ترين كرم در سال 2004 نام گرفت با استفاده از اين روش به گسترش خود پرداخت[2و7].
بسياري از كرم هاي امروزی ديگر نيز همانند MYDOOM با استفاده از SMTP engine داخلي خودشان از روي كامپيوتر شخصي افراد آلوده شده، اقدام به ارسال بدافزار به آدرس های پستی جمع آوري شده مي كنند. بعضي ديگر ممكن است از سرور هايSMTP ديگري كه در دنيا به صورت مجاني براي ارسال نامه در نظر گرفته شده اند استفاده كنند.
از آن جا كه پروتكل SMTP اساسا بر اين مبنا كه هرماشين بتواند به هر ماشين ديگري نامه ارسال كند[RFC 821] نوشته شده است، لذا تنها روش جلوگيري، مانع شدن كامپيوتر شخصي از دادن سرويس روي پورت 25 است اين كار را مي توان بوسيله يك Firewall با گذاشتن محدوديت و يا حتي بستن پورت 25 انجام داد. اين كار براي اكثر كاربران محدوديتي را براي ارسال و يا دريافت نامه ايجاد نمي كند زيرا اكثر كاربران از سرويس هاي مجاني قابل اطمينان درون خود اينترنت استفاده مي كنند. پس با اين كار مانع از گسترش اين دسته از كرم هاي اينترنتي خواهيم شد و از آلودگي سايرين نيز به شدت جلوگيري خواهد شد.
كاهش دادن چندگانگي[1] راههاي ارسال و دريافت پست الكترونيك مي تواند راه كار موثر ديگري براي جلوگيري از گسترش بيش از حد بد افزارها گردد. در اين روش به جاي استفاده از چند Mail server از تعدادي محدود استفاده مي كنيم تا بتوانيم ارسال و دريافت محتويات نامه را بهتر بررسي كنيم.
MTA[2]ها مكان هاي مناسبي جهت نصب و پياده سازي امكانات نرم افزاري و سخت افزاري امنيتی همچون ضد ويروس های مناسب هستند.
با استفاده از ضد ويروس هايي كه به همين منظور طراحي شده اند مي توانيم جلوي نامه حاوي بدافزار را، قبل از رسيدن به دست گيرنده بگيريم.
استفاده از ضد ويروس هايي با امكانات مكاشفه اي[3] هستند ونه بر مبناي امضاي ويروس، مي تواند نقش موثري در جلوگيري از پخش شدن كرم هاي اينترنتي داشته باشد.
پوش مكاشفه اي رفتار فايل را مورد بررسي قرار مي دهد و اگر متوجه امر غير عادی مثلا آنكه فايل قصد خرابكاري دارد، آن را بعنوان بدافزار معرفي مي كند اين كار در يافتن بدافزارهايي كه هنوز امضايي براي آنها يافت نشده و به پايگاه داده نرم افزار ضد ويروس اضافه نشده اند بسيار موثر خواهد بود[13].

4-2-3- وب

---

[1] Multiplicity
[2] Mail Transfer Agent
[3] Heurisitic

پايگاههای وب حاوي صفحاتي با کدهای مخرب، روش ديگري از آلوده سازي توسط بدافزارها مي باشد. برخي از نفوذ گران از اين روش براي راهيابي به کامپيوتر استفاده مي کنند. آنها قادرند با سو استفاده از برخي آسيب پذيري موجود در سيستم عامل و يا نرم افزارهاي مرورگر، صفحات وبي را طراحي می کنند که صرفا با ديدن آن صفحه، بدافزار بر روي کامپيوتر کاربر نصب و اجرا شود. آسيب پذيري هاي بسياري از اين دست در سيستم عامل ويندوز و مرورگر IE وجود دارد که مي توان برای اطلاعات بيشتر به منابع [3و4] مراجعه کرد.
بهترين اقدام براي اين گونه آسيب پذيري ها، پيش گيري است. از آن جا که نويسندگان بدافزار پس از اعلام عمومي شرکت سازندة مرور گرويا سيستم عامل مبني بر وجود شکاف امنيتي درون نرم افزار توليدي خود، اقدام به انتشار patch و يا Hot fix مربوط مي کنند، اين افراد از آگاهي نداشتن کاربران سوء استفاده مي کنند و اقدام به نوشتن برنامه اي براي استفاده از آسيب پذيري مذکور می نمايند. لذا بهتر است با آگاه ساختن کاربران با اين گونه آسيب پذيري ها و لزوم به روز رساني نرم افزارها و سيستم عامل، آنها را از قرار گرفتن در معرض اين گونه حملات برهانيم.
اگر درون شبکه از پروکسي هاي وبي استفاده شود که صفحات وب را قبل از تحويل به کاربر تجزيه و تحليل امنيتی کند، ديگر امروزه شاهد آن نخواهيم بود که کامپيوترهاي بسياری در دنيا به نرم افزارهاي Spyware آلوده باشند. از جمله اين وب پروکسی ها می توان به Trend Micro Inter Scan اشاره کرد.

4-2-4- دسترسي از دور[1] به کامپيوتر

اين امکان که بيشتر توسط مديران شبکه براي نگهداري و نظارت از راه دور مورد استفاده قرار مي گيرد، بهتر است که از طريق VPN[2] انجام شود. Spida نمونه اي از کرم هاي اينترنتي است که از ضعيف بودن کلمات عبور براي وارد شدن به سيستم از دور استفاده می کند. انتخاب کلمات کلمات عبور قوي يکي ديگر از مسائلي مي باشد که بايد توسط مديران شبکه رعايت شود.

4-2-5- payload مرتبط با سرزير بافر

سرزير بافر هنگامي اتفاق مي افتد که در برنامه، حافظه بافر چك نشود در اين موقع حمله کننده مي تواند با سوء استفاده از اين موضوع کد خود را هنگام سرزير درون بافر قرار دهد، لذا کد وي هنگام اجراي محتويات بافر اجرا خواهد شد. SASSER کرمي که در سال گذشته به سرعت در بين کامپيوترهاي آسيب پذير به مشکل موجود در بافر LSASS.EXE پخش شد، از اين موضوع استفاده کرده بود.
همان طور که در قسمت 4-2-3 نيز گفته شد، بهترين راهکار موثر براي اين موضوع استفاده از نرم افزارهاي مطمئن و به روز نگه داشتن آنان است. غير فعال کردن سرويس هاي که به ندرت استفاده مي شوند، نصب يك firewall و يا يك IDS مي تواند در اين قسمت موثر واقع شود، مي توان از سرويس هايي که به ندرت استفاده مي شوند می توان RPC[3] را در سيستم عامل ويندوز نام برد، کاربران عادي شبکه معمولا هيچ گاه از DCOM اين سرويس استفاده نمي کنند. اما مشکلي که در اين سرويس وجود داشت موجب آن شد که ويروس Blaster به سرعت در بين کامپيوترهاي شخصي پخش شود و ضررهاي مالي بسياري را بوجود آورد. در مورد سر ريز بافر در قسمت 4-3-5 بيشتر توضيح داده خواهد شد.

---

[1] Remote

[2] Virtual Private Network connection

[3] -Remote Procedure call

4-3- اجراي كد ويروسي

با اين فرض كه بدافزار بر روي كامپيوتر قرار گرفته است، در اين قسمت، بحث را با چگونگي راههاي اجرا ادامه مي دهيم ، زيرا كه بدافزار قرار گرفته روي كامپيوتر تا زماني كه اجرا نشود اساساً خطرناك نخواهدبود.

4-3-1- آسيب پذيري نرم افزارهاي پست الكترونيكي

اين نرم افزارها مي توانند ناخود آگاه فايلهاي حاوي بدافزارها را اجرا كنند كه ممكن است اين كار به طرق زير انجام شود.

1. اجراي ناصحيح بدافزار توسط نرم افزار نامه خوان

از آن جا كه نامه هاي الكترونيكي HTML ذاتاً صفحات وب هستند همان خطراتي كه در قسمت 4-2-3 بيان شد براي نرم افزارهايي كه براي نمايش نامه هاي HTML از مرورگر اصلي سيستم عامل استفاده مي كنند در اين جا نيز مطرح مي شود. يك حمله كننده مي تواند از بعضي آسيب پذيري هاي موجود در اجراي خود كار بعضي از قالب هاي فايلها سوء استفاده كند، مانند تغيير در MIME header كه برخي از بدافزارها از جمله Nimda اين كار را انجام مي دهند [7].

براي جلوگيري از اين گونه آسيب پذيری ها نصب patch های لازم و به روز نگهداشتن برنامه مي تواند از بروز اين گونه حملات جلو گيري كند.

2. سرريز بافر

بعضي از نرم افزارهاي پست الكترونيك مي تواند مانند ديگر نرم افزارها نسبت به مشكل سرريز بافر آسيب پذير باشند. لذا شخص نفوذگر مي تواند به راحتي از اين مسئله سوء استفاده كند.

استفاده از آنتي ويروس هايي با قابليت پويش مكاشفه اي و به روز بودن اين گونه نرم افزارها مي تواند خطر اين گونه حملات را كاهش دهد.

3. دخالت كاربر

بسياري از بدافزارها با استفاده از تكنيك هاي مهندسي اجتماعي اقدام به فريفتن كاربران با ارسال نامه هايي محتوي بدافزار، با عناوين فريبنده مي كنند.كاربران نيز ممكن است از روي حس كنجكاوي ضميمه نامه را دانلود كرده و آن را اجرا نمايند. تنها راه حل جلوگيري از اين روش، آموزش كاربران و آگاه ساختن آنها از اين گونه روش هاي مهندسي اجتماعي مي باشد.

4-2-4- دخالت كاربر

همان طور كه در قسمت قبل نيز توضيح داده شد. بسياري از كاربران اصرار دارند برنامه هايي را كه دليلي براي اعتماد به آنها وجود ندارد را، اجرا كنند و اين نتيجه اي است كه در شيوع ناگهاني كرم Mydoom ديده شد (Sophos) همان طور كه در قبل نيز اشاره شد، آموزش و آگاه ساختن كاربران تنها راه جلوگيري از اين روش است.

4-3-3- اجراي خودكار

هنگامي كه بدافزار روي كامپيوتر شخصي قرار گرفتن با قلاب كردن خودش به بعضي از كليدهاي رجيستري يا روش هاي ديگر. اين امكان را براي خود فراهم مي سازد كه با هر بار اجراي سيستم عامل خود نيز اجرا شود.

براي اين كار نيز مي توان سطح دسترسي نرم افزارها را به محل هاي شروع[1] محدود كرد تا ديگر امكان اضافه شدن بدافزارها به آن قسمت ها وجود نداشته باشد.

4-3-4- آسيب پذيري مرور گرهاي وب

راه ديگري كه بدافزارها براي آلوده سازي كامپيوتر هاي شخصي مورد استفاده قرار مي دهند، استفاده از آسيب پذيري هاي موجود در مرورگرهاست. مثلاً REDLOF از آسيب پذيري Unpatched VM Activex براى اجراى كد خود استفاده مي كند[7].مثالهاي جالبي در اين رابطه را می توان در [3] مشاهده كرد..نصب Patch ، Hotfix ها و به روز رساني سيستم عامل همان طور كه قبلاً نيز اشاره شد مي تواند جلوي اجرا شدن كدهاي ويروسي را از اين طريق بگيرد.

4-3-5- سرريز بافر

در طول مقاله قبلاً هم به اين موضوع پرداختيم اما تحقيقات نشان مي دهد مبارزه با اين گونه حملات از 3 نقطه حائز اهميت است. اول برنامه نويسي صحيح دوم جلوگيري از سوء استفاده و سوم محدود كردن امكان سوء استفاده. اولين اين نكات يعني برنامه نويسي صحيح بر روي تغييرات در ابزارهاي برنامه نويسي و كاهش خطرات احتمالي ناشي از صنعت برنامه نويسي متمركز مي شود.

بسياري از حمله هاي ناشي از ضعف برنامه نويسي مانند سرريز در بافر نتيجه عدم تسلط برنامه نويس است، لذا آموزش برنامه نويسان براي تشخيص و اصلاح اين گونه اشتباهات يك راه حل موثر در رفع اين معضل به شمار مى رود،. براي اين هدف فن آوري هاى بسياري من جمله Systrace براي مقيد ساختن برنامه هاي در حال اجرا به بازار آمد. Systrace به مدير شبكه امكان آن را مي دهد كه فعاليت هاي يك فايل قابل اجرا يا يك برنامة در حال اجرا را محدود نمايد. برنامه ها به محض اجرا نظارت خواهد شد و از انجام دادن كارهاي غير مجاز منع مي شوند، ولي مشكل عمده اين قضيه نيز وقت گير بودن تنظيمات براي هر برنامه است. اما در كل بسياري از مشكلات را در اين زمينه كاهش مي دهد.براى اطلاعات بيشتر راجع به اين گونه فن آورى ها مقاله در [5] بيان گرديده است.راهكار تازه اى كه شركت مايكروسافت همراه با شركت اينتل براى مقابله با اين امر ابداع كردند فن آورى جديد Hyper-Threading است، در سال 2001 شركت اينتل براى پردازنده هاى جديد خود به نام Itanium كه مخصوص سرور هاى پرقدرت طراحى شده بود اين امكان را فراهم آورده بود كه در صورت برخورد با فعاليت غير عادى ناشى از كرم هاى اينترنتى به صورت خودكار با فعال نمودن Execute Disable Bit روند آلوده سازى را متوقف كند، اما به خاطر نياز امروز اين دو شركت بر آن شدند كه اين فن آورى را به كامپيوترهاى شخصى نيز اضافه كنند كه براى اطلاعات بيشتر مى توان از [4] استفاده نمود

4-4- داشتن Payload

بعضي از بدافزارها پس از آن كه درون سيستم فعال شدند ممكن است به انجام برخي فعاليت هاي جانبى ديگر بپردازند كه به آنها اصطلاحاً payload گفته مي شود.

Payload مي تواند شامل از كار انداختن نرم افزارهاي سيستمي در حال اجرا بر روي كامپيوتر كاربر باشد مانند كاري كه LOVELORN انجام مي دهد، مي تواند حملات DOS[2] را بر روي يكي از پايگاه وب انجام دهد مانند كاري

---

[1] -Start up

[2]-Denial of service

كه BLASTER بر روي پايگاه windowsupdate.com كرد، از بين بردن فايلهايي سالم و تكثير خودش مانند ZAFI.B ، از جمله Payload هايي است كه عموما توسط بد افزار ها انجام می شود برای اطلاعات بیشتر راجع به این کرم ها می توان از [7] استفاده کرد.
براي مقابله با اين گونه فعاليت ها لزوم وجود Firewall و يك ضد ويروس با امكان روش مكاشفه اي به صورت توأمان الزامي است. قرار دادن فايلها و برنامه هاي مهم درون شاخه هايي با امكان دسترسي و تغيير، تنها در سطح مدير شبكه از راه كارهاي اساسي براي جلوگيري از انجام اين دسته از فعاليت هاست.

5-4- انتقال اضافي

برخي از بدافزارها پس از اجرا شدن اقدام به انتقال باقيماندة خود از مكان هايي كه قبلاً نويسندگان بدافزار مشخص شده است مي كنند.
بسياري از آنان از TFTP اين كار را انجام مي دهند، SASSER ، BLASTER و انواع آنها اين كار را با برقراري يك ارتباط UDP از طريق TFTP انجام مي دهند.
SOBIG.F مي تواند رأس ساعت و روز مشخصي كد خود را با اتصال به برخي از سرورهايي كه قبلاً توسط نويسنده و يا نويسندگان آن مد نظر گرفته شده به روز رساني كند.
تنها راه جلوگيري از اين امكان يعني انتقال باقي مانده و يا اضافه كردن امكانات جديد به بدافزار كه توسط اتصال آن با دنياي خارج صورت مي گيرد تنها با محدود كردن ارتباط با دنياي خارج امكان پذير است كه اين كار را مي توان به راحتي با نصب يك firewall انجام داد.

5- نتيجه گيري

همانطور كه در مقاله اشاره شد، بد افزارها بعنوان يك تهديد جدی برای امنيت اينترنت و پايداری آن به شمار می آيند.بدافزار چه در قالب ويروس، كرم، اسب تراوا و يا مخلوطي از آنها همواره در كنار كاربران كامپيوتر خواهد بود.
تا زماني كه بدافزارها پيچيده تر و گسترش يافته تر مي شوند، ابزارها و روش هاي مبارزه با آنها نيز در حال پيشرفت خواهند بود.
اين يك وظيفة اخلاقي هر مدير شبكه اي است كه با فن آوري در علم روز همگام باشد.
از آنجا كه تجربه به ما مي گويد فاجعة بعدي كه ممكن است توسط بدافزارها در دنياي شبكه روي دهد از روش ها و راه كارهايي در آن استفاده شده است كه تاكنون محقق نگرديده اند لذا اين وظيفه هر كاربر در هر سطحي است كه آگاهي لازم را در اين زمنيه داشته باشد و كارهاي بسياري را هر چند ساده برای كاهش امكان گسترش انجام دهند. كارهايي از قبيل به روزرساني نرم افزارهايي كه با دنياي خارج در ارتباط هستند. نصب Hotfix, patch مربوط به آنها، نصب Firewall و ضد ويروس هايي با امكانات پويش مكاشفه اي ، مجهز كردن سرور ها به پردازنده های جديدی كه در مقاله به آن اشاره شد و راه های امنيتی كه در موارد خاص می توانند به كار آيند از راه كارهای عملی بيان شده در مقاله برای جلوگيری از گسترش و شيوع بد افزارها می باشند، زيرا همانطور كه گفته شد بد افزارها علاوه بر آلودگی و ايجاد آسيب پذيری بيشتر در مقابل ساير حملات، باعث افزايش بی رويه ترافيك شبكه نيز می شوند.
يك راه صددرصد جوابگو براي جلوگيري از ورود بد افزار وجود ندارد، ولي همواره پيش گيري بسيار بهتر از درمان بوده است. تغيير دادن سياست هاي استفاده از شبكه براي كاربران توسط مديران شبكه، الزام به نصب و به روز رساني نرم افزارهاي ضد ويروس چه در سمت خدمات دهنده و چه در سمت كاربری، استفاده از فن آوري IDS براي كنترل ترافيك شبكه، استفاده از فن

آوري حفاظت در برابر نامه هاي ناخواسته[1]، كنترل فرستنده نامه و آموزش كاربران براى آشنايى با مبانى امنيت شبكه مي تواند راه كارهاي موثري براي كاهش و يا حتي توقف گسترش بدافزاها باشد.

6- مراجع

[1]: Trend Microsystems, “The Trend of Malware Today: Annual Virus Round-up and 2005 Forecast” http://www.trendmicro.com/en/security/white-papers/ (15 February, 2005)

[2]: Sophos Reports on New Spam Tactics and Top Ten Viruses for 2004 in Annual Threat Analysis www.sophos.com/pressoffice/pressrel/us/20041208yeartopten.html (2005)

[3]: Umbrella, “Large number of unpatched MSIE vulnerabilities” http://umbrella.name/originalvuln/msie/

[4]: Microsoft, Intel “A Winning Combination or Security, Stability, and Responsiveness” http://www.intel.com/business/bss/infrastructure/security/xdbit_ds.pdf (2004)

[5]: V.Kiriansky, D.Bruening, S.Amarasinghe , “Secure Execution Via Program Shepherding” *Laboratory for Computer Science Massachusetts Institute of Technology* http://cag-www.lcs.mit.edu/dynamorio/security-usenix.pdf

[6]: Microsoft Security Bulletin MS001-020 www.microsoft.com/technet/security/bulletin/MS01-020.mspx

[7]: Trend Microsystems Virus Encyclopedia http://www.trendmicro.com/en/security/encyclopedia/overview.htm

[8]: Gabor Szappanos , “Model of Viral Propagation”, *SecurityFocus* http://www.securityfocus.com/infocus/1265 (July 17,2000)

[9]: Tony Bautts, “Slow Down Internet Worms with Tarpit”, *SecurityFocus* www.securityfocus.com/infocus/1723 (August 21, 2003)

[10]: Laurent Oudot, “Fighting Internet Worms with Honeypot”, *SecurityFocus* www.securityfocus.com/infocus/1740 (October 23, 2003)

[11]: Tripwire, Inc. “Tripwire for Servers: Frequently Asked Questions.” http://www.tripwire.com/products/servers/faqs.cfm (21 January 2004)

[12]: Paul Innella and Oba McMillan “An Introduction to IDS”, *SecurityFocus* http://www.securityfocus.com/infocus/1520 (December 6, 2001)

[13]: Markus Schmall, “Heuristic Techniques in AV Solutions: An Overview” ,*Security Focus* http://www.securityfocus.com/infocus/1542

[1]-**Spam Protectin**