وزارت علوم ، تحقيقات و فنّاوري
مؤسسه آموزش عالي پاسارگاد شيراز

بررسي و تحليلي بر

کـرم بلاستـر

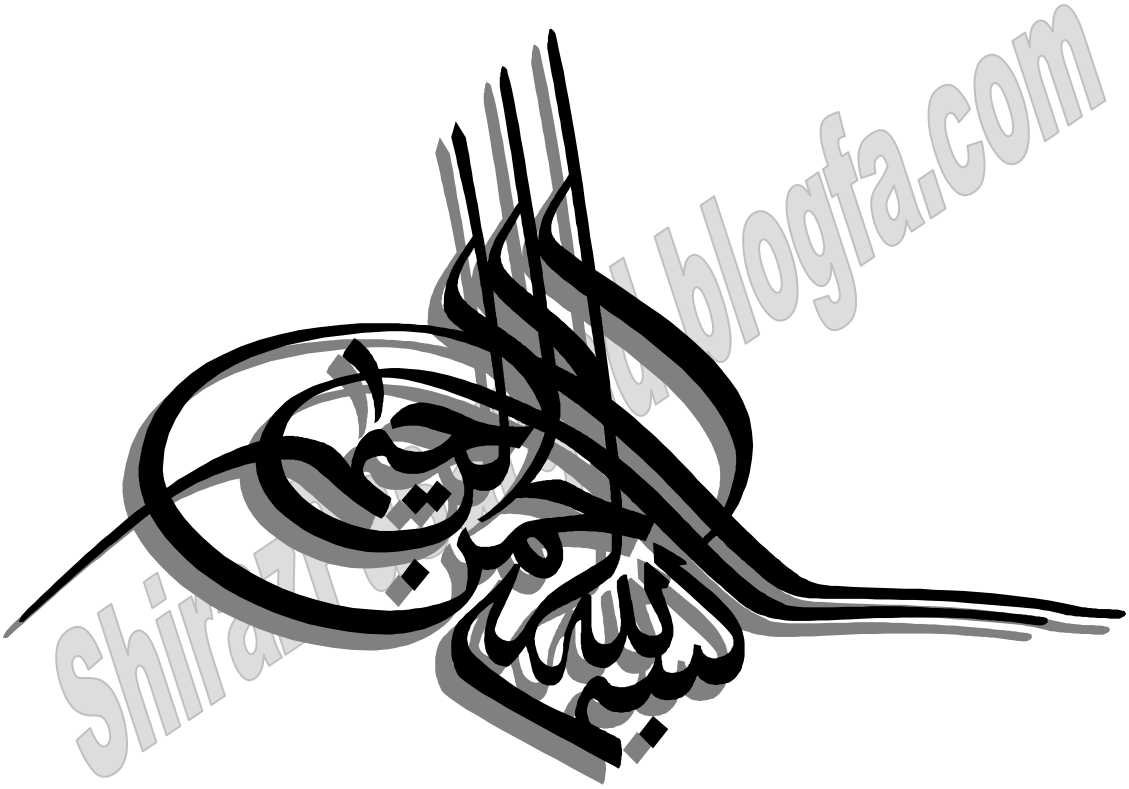
Blaster Worm

Analysis

استاد راهنما : جناب آقاي مهندس تميس

e-Mail: shiraz.pasargad@yahoo.com

دي ماه ۱۳۸۵



فهرست مطالب

فهرست تصاویر

مقدمه

با پيشرفت روز افزون علم و فنّاوري نياز بشر به كسب اطلاعات جديد بيش از پيش گشته و بهترين راه براي حصول سريع اين اطلاعات استفاده از شبكه ي جهاني وب (World Wide Web) مي باشد. ليكن اين امر با دشواري ها و مشكلات ويژه ای روبروست.

ناامني ها و حملاتي كه توسط مخربان انجام مي گيرد، بزرگترين مشكل در اين زمينه می باشد. به اعتقاد گروهي از افراد ساخت ويروس ها و كرم ها به منظور انجام حملات اينترني مي تواند معلول انتقام جويي فرد يا اسبابي جهت خودنمايي باشد.

بلاستر يكي از قدرتمندترين و سريعترين كرم هايي است كه توانست كاربران زيادي را با مشكل مواجه كند. سرعت انتشار آن سرسام آور بود و هدف آن تضعيف *بيل گيتس*، سرمايه گذار معروف شركت ميكروسافت گزارش شده است. اكنون بررسی هايي را كه در اين زمينه صورت گرفته است، از نظر می گذرانيم.

معرفي

نوع : كرم شبكه

تاريخ كشف : ١٢ آگوست ٢٠٠٣

قابليت انتشار : بله

سيستم عامل هاي مورد حمله قرار گرفته:

- ويندوز XP
- ويندوز ٢٠٠٠
- نسخه هاي تصحيح نشده ي ويندوز هاي ٢٠٠٣ و NT. البته اين دو سيستم عامل در معرض ابتلا هستند ولي بلاستر براي كپي شدن و حمله به آنها برنامه ريزي نشده است.

عملكرد:

ايجاد اختلال در ويندوز و Restart نمودن آن. بلاستر پس از نمايش كارد زير به كاربر ٦٠ ثانيه مهلت مي دهد تا كاربر در اين مدت كارهاي خود را ذخيره نمايد. پيام آن به شرح زير مي باشد:

« به دليل اينكه سرويس فراخواني پردازه ي از راه دور به صورت غير منتظره متوقف شده است، هم اكنون ويندوز بايد Restart شود. »

تصوير شماره ١) پيام بلاستر قبل از ريست كردن كامپيوتر آلوده.

پورت هاي مورد استفاده:

- پورت ۱۳۵ TCP (DCOM RPC)
- پورت ۶۹ UDP (TFTP)
- پورت ۴۴۴۴ TCP (Remote Shell)

فهرست نام هاي مستعار ويروس:

- Lovesan
- Lovesan.H (F-Secure)
- Msblast.exe
- Tftp
- W32.Blaster.Worm (Symantec)
- W32/Blaster.worm.a
- W32/Blaster.worm.k
- W32/Lovsan.worm
- W32/Lovsan.worm.gen
- Win32.Poza (CA)
- Worm/Lovsan.G (Central Command)
- WORM_MSBLAST.A (Trend)
- WORM_MSBLAST.H (Trend)

شمار كامپيوترهاي آلوده شده در ۱۱ آگوست ۲۰۰۳ :

اروپا	۲۸۷,۹۸۳
آسيا	۳۸,۳۲۲
آمريكاي شمالي	۲۵,۷۸۳
آمريكاي جنوبي	۳,۱۸۰
آفريقا	۲,۱۹۶
استراليا و نيوزلند	۸۷۶
ناشناخته	۶۲۲
جمع كل	۳۵۸,۹۶۲

در اين ميان كشورهاي استراليا، دانمارک، آمريكا، فرانسه، مالزي، بلژيک، بريتانيا، كانادا، تايوان و آلمان به ترتيب بيشترين آلودگي را داشته اند؛ كه اين ميزان آلودگي فقط مربوط به روز اول شروع به كار بلاستر مي باشد !

تفسير

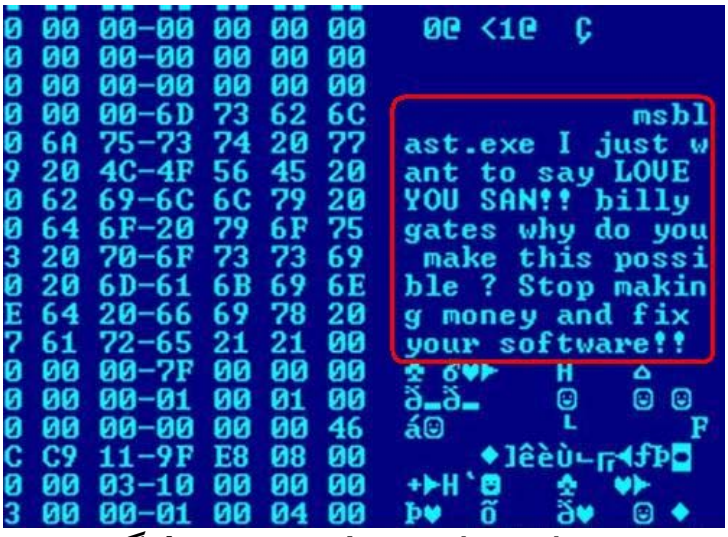
خانواده كرم Msblast / Win32 از يک فراخواني از راه دور استفاده مي كند (RPC [1]) و با استفاده از آسيب پذيري ويندوزهاي ۲۰۰۰ و XP به سيستم دسترسي پيدا مي كند. اين كرم مي تواند يک راه نفوذ براي نفوذ هرچه راحت تر حمله كننده ها (Attackers) به سيستم آلوده باز كند همچنين ممكن است تلاشي براي حمله ي DoS [2] روي بعضي از سيستم ها انجام دهد. (DoS Attack به معني يک حمله ي كامپيوتري براي جستجو و قطع دسترسي به اينترنت مي باشد.)

كرم بلاستر اولين بار در يازدهم آگوست سال ۲۰۰۳ ميلادي بود كه شروع به تكثير كرد. نرخ گسترش آن به حدّي زياد شد تا اين كه در ۱۳ آگوست به نقطه ي اوج خود رسيد؛ كه با فيلتر شدن بوسيله ي ISP [3] ها و تبليغات گسترده اي كه در مورد آن انجام شد، انتشارش فرونشست و سرعت آن كاهش يافت.

بلاستر داراي ۲ پيام مي باشد: (البته هيچ يک از اين دو پيام نمايان نمي شوند.)

- پسرم من فقط مي خواهم بگويم كه تو را دوست دارم!! (كه به اين دليل به آن كرم LoveSan مي گويند.)
- بيل گيتس چرا اين امكان پذير است ؟ پول جمع كردن را كنار بگذار و نرم افزارت را تعمير كن !! (اين پيام به بيل گيتس سرمايه گذار ميكروسافت و شخص مورد هدف قرار گرفته توسط كرم مي باشد.)

[1] Remote Procedure Call
[2] Denial of Service Attack (More information at http://en.wikipedia.org/wiki/Distributed_denial_of_service_attack)
[3] Internet Service Provider



تصوير شماره ۲) پيام مخفي بلاستر به شخص *بيل گيتس*.

سرانجام در ۲۹ آگوست سال ۲۰۰۳ جفري لي پارسون[1] ، فرد ۱۸ ساله از هاپکينز به خاطر ساخت نوع B[2] اين کرم دستگير شد. او به عنوان فرد پاسخ گو شناخته و محکوم به ۱۸ ماه زندان شد. جالب است بدانيد که در تاريخ ۲۰۰۳/۱۱/۵ شرکت ميکروسافت براي دستگيري توليد کننده ي اصلي اين کرم ۲۵۰,۰۰۰ دلار جايزه تعيين کرد.

تصوير شماره ۳) جفري لي پارسون (سازنده ی بلاستر نوع B)

[1] Jeffrey Lee Parson

[۲] - Worm.Msblast.B : اين نسخه از کرم شبيه به همان نسخه ي اصلي مي باشد، فقط نام فايل آن به PENIS32.exe تغيير يافته است.

تحليل

وقتي كه گونه هاي مختلف Win32/MSblast اجرا مي شوند، يک ورودي جديد به كليد زير در رجيستري ويندوز اضافه مي كنند:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\
CurrentVersion\Run

با افزودن اين كليد به رجيستري، بلاستر، به صورت اتوماتيک همراه با راه اندازي سيستم اجرا مي شود.

البته قبل از تغيير رجيستري، بررسي مي كند كه آيا كامپيوتر آلوده است يا نه؟ يا اينكه آيا بلاستر در حال اجرا مي باشد؟ اگر چنين باشد، كامپيوتر را براي بار دوم آلوده نمي كند.

سپس تلاش خود را براي گسترش از طريق آدرس IP [1] سيستم آلوده به ساير سيستم ها شروع مي كند؛ كه اين آدرس IP مي تواند به صورت تصادفي انتخاب شده يا با استفاده از الگوريتمي از آدرس IP سيستم آلوده و ساخت يک IP جديد به سيستم ديگر نفوذ كند.

اين الگوريتم به شرح زير مي باشد:

در ٤٠ درصد اوقات آدرس توليد شده به فرم A.B.C.0 بوده كه در آن A و B برابر با دو بخش اول آدرس كامپيوتر آلوده مي باشد. C نيز با استفاده از بخش سوم آدرس كامپيوتر آلوده محاسبه مي شود. در ٤٠ درصد اوقات كرم چک مي كند كه آيا C بزرگتر از ٢٠ مي باشد يا خير. اگر چنين باشد (يعني از ٢٠ بزرگتر باشد) يک مقدار تصادفي كمتر از ٢٠ از آن كم مي كند. بار اولي كه آدرس محاسبه شد مي كوشد تا به كامپيوتر با آن آدرس نفوذ كند. سپس بخش صفر آدرس را افزايش مي دهد (+١) و اين كار را تا رسيدن به عدد ٢٥٤ ادامه مي دهد.

با يک تقريب ٦٠ درصدي آدرس توليد شده توسط كرم كاملاً تصادفي خواهد بود.

[1] Internet Protocol Address

با يافتن آدرس مورد نظر و دسترسي به سيستم قرباني، داده هايي به پورت ۱۳۵ TCP [1] مي فرستد كه مي تواند از آسيب پذيري RPC DCOM [2] استفاده كند. بلاستر دو نوع داده به پورت ذكر شده مي فرستد. در ۸۰ درصد موارد داده ي مخصوص ويندوز XP و در ۲۰ درصد مواقع داده ي ويندوز ۲۰۰۰ فرستاده خواهد شد.

سپس از فرمان Cmd.exe براي ساخت يک پردازه ي مخفي واسط از راه دور استفاده مي كند كه به پورت ٤٤٤٤ TCP گوش كرده و به حمله كننده ها اجازه مي دهد كه دستورات خود را از راه دور بر روي سيستم آلوده اجرا كنند.

بعد از آن به پورت ٦٩ UDP [3] گوش فرا مي دهد. وقتي كه درخواستي از يک كامپيوتر دريافت مي شود مبني بر اينكه توانسته است با استفاده از RPC DCOM متصل شود ، فايل msblast.exe را به آن كامپيوتر فرستاده و از او مي خواهد كه آن فايل را اجرا كند (حجم فايل فوق الذكر برابر با ٦١٧٦ بايت مي باشد). اكنون اگر تاريخ جاري بين شانزدهم تا سي و يكم ماه آگوست يا ژانويه باشد و يا اينكه ماه جاري بين سپتامبر تا دسامبر باشد، مي كوشد تا يک حمله ي DoS به WindowsUpdate.Com انجام دهد (البته اين حمله با سايت هايي مثل : kimble.org, tuiasi.ro نيز مي شود.) كه در صورت عدم توانايي در يافتن راهي براي نفوذ به DNS [4] آن از آدرس IP ۲۵۵ . ۲۵۵ . ۲۵۵ . ۲۵۵ . اين حمله چنانچه حالات زير موجود باشد ، انجام مي گيرد:

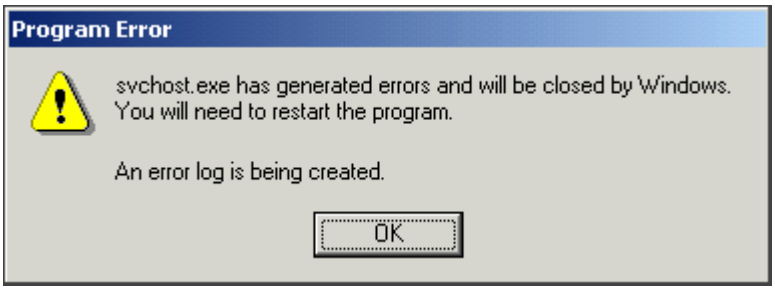
- كرم بر روي كامپيوتري اجرا شود كه از ويندوز XP استفاده كرده و آن كامپيوتر آلوده بوده و در مدت مفيد Restart شده باشد.
- كرم بر روي كامپيوتري اجرا شود كه از ويندوز ۲۰۰۰ استفاده كرده و در مدت مفيد Restart نشده باشد.
- كرم بر روي كامپيوتري اجرا شود كه از ويندوز ۲۰۰۰ استفاده كرده و از زمان آلوده شدن Restart شده باشد و هم اكنون مدير سيستم در حال كار كردن با سيستم باشد.

[1] Transmission Control Protocol
[2] Distributed Component Object Model (جهت اطلاعات بيشتر به آدرس زير مراجعه كنيد : http://en.wikipedia.org/wiki/Distributed_component_object_model)
[3] User Datagram Protocol
[4] Domain Name Server

تا زماني كه كرم نداند كـه سيـستم عـاملي كـه كـامپيوتر مقـصد از آن اسـتفاده مـي كنـد، چيست، آن را حدس مي زند. در ۸۰ درصد موارد ويندوز XP در نظـر گرفتـه شـده و ۲۰ درصد موارد ويندوز ۲۰۰۰. چنانچه اين حدس اشتباه بوده (و كامپيوتر مقصد قابل حملـه باشد) ، پردازه ي svchost.exe بـر روي آن كـامپيوتر مختـل شـده، كـامپيوتر متزلـزل مي گردد و آلودگي متوقف مي شود. وقتي كه svchost.exe دچار خطا مي شـود يـک پيام مانند زير در سيستم عامل ويندوز XP ظاهر مي گرددكه پس از آن ويندوز Restart خواهد شد:

تصوير شماره ٤) اختلال در پردازه ي SVCHOST.EXE در ويندوز XP

و همين پيام در ويندوز ۲۰۰۰ به صورت زير مي باشد:



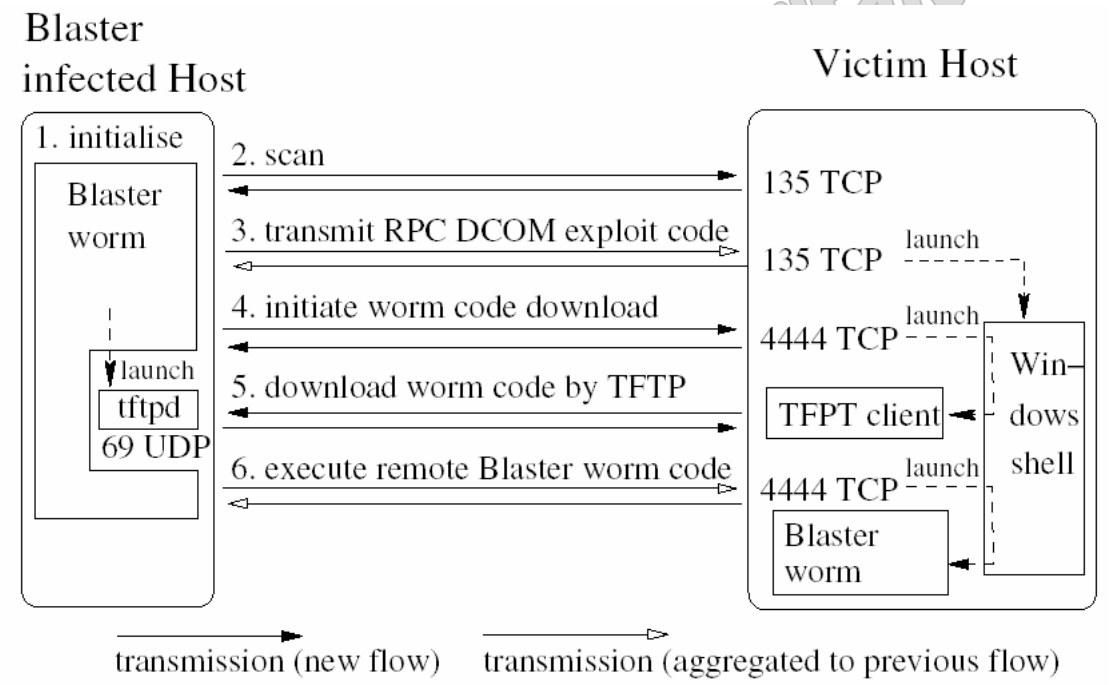
تصوير شماره ٥) اختلال در پردازه ي SVCHOST.EXE در ويندوز 2000

جمع بندي

مراحل كار كرم را مي توان در شش مرحله ي زير خلاصه نمود:

۱. راه اندازي كرم
۲. جستجوي طعمه از طريق پورت ۱۳۵ TCP
۳. ارسال كد آسيب پذير به سيستم قرباني از طريـق پـورت ۱۳۵ TCP
۴. شروع دانلود كد كرم (Msblast.exe) از طريق پورت ۴۴۴۴ TCP
۵. دانلود كرم با استفاده از پروتكل ارسال فايل (TFTP)
۶. اجراي كد بلاستر با استفاده از پورت ۴۴۴۴ TCP

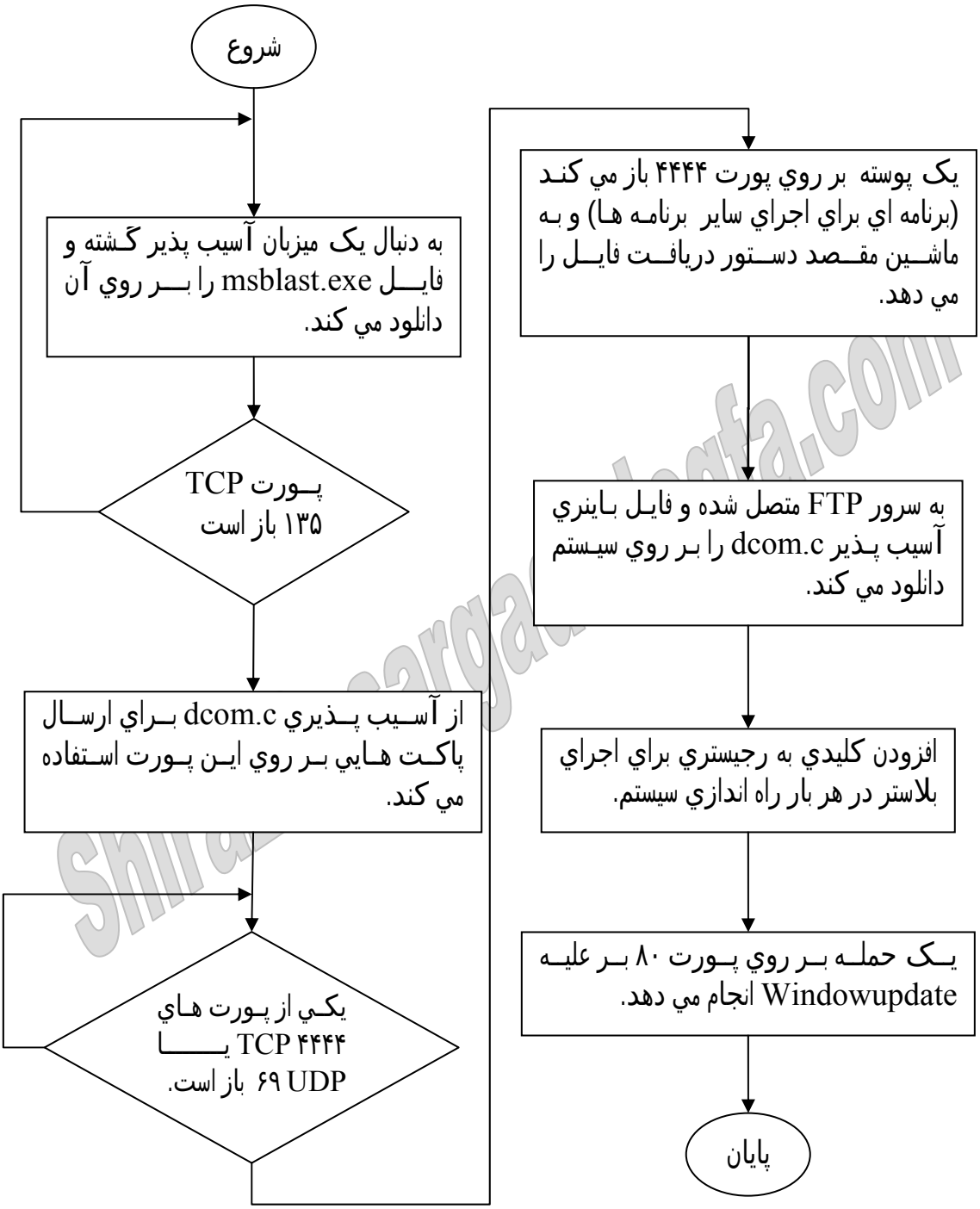
چنانچه مشاهده مي شود در تصوير زير مراحل مذكور به نمايش گذاشته شده اند :



تصوير شماره ٦) مراحل كار بلاستر

در تصوير فوق ، بلاک سمت چپ نمايي از سيستم آلوده و بلاک سمت راست نمـايي از سيستم قرباني مي باشد. اجراي بلاستر در سيستم آلـوده و طـي كـردن مراحـل شـش گانـه مذكور منجر به آلوده شدن سيستم قرباني و گسترش كرم مي شود.

نمـودار جريـان صـفحه ي بعـد رفتـار كـرم را در سيـستم آلـوده و جريـان كـار آن را نشان مي دهد.



نمودار جریان مراحل کار بلاستر

بررسي كد منبع بلاستر

بلاستر اولين بار به زبان ويژوال بيسيک نوشته شده بود و کدهاي منتشر شده از اين ويروس همگی به زبان C مي باشند. ويروس يا کرم بلاستر با استفاده از نرم افزار IDAPro که يک نرم افزار قوي براي برررسي فايل هاي دودويي مي باشد، رمز گشايي شد. نکته ي قابل توجه اين است که IDA کد منبع را توليد نمي کند بلکه کمکي براي فهم بيشتر فايل دودويي است. اکنون بخش هايي از کد منبع اين کرم را مورد بررسي قرار مي دهيم:

تعاريف سراسري مهم

```
const char msg1[]="I just want to say LOVE YOU SAN!!";
const char msg2[]="billy gates why do you make this possible ?"
" Stop making money and fix your software!!";
```

اين دو رشته به صورت سراسري تعريف شده اند و چنانچه گفته شد هيچ وقت نمايش داده نمي شوند و تقريباً مخفي مي باشند.

```
#define MSBLAST_EXE "msblast.exe"
```

با تعيين نام کرم به عنوان يک متغير #define نويسنده اين انعطاف را دارد که نام اجرايي کرم را تغيير دهد.

```
#define MSRCP_PORT_135 135
```

MS-RPC/DCOM بر روي پورت ۱۳۵ اجرا مي شود. که مي توان با استفاده از سيستم امنيتي[1] بر روي اين پورت از بهره دادن کامپيوتر جلوگيري کرده و مانع از پخش آن مي شود.

```
#define TFTP_PORT_69 69
```

پورت ۶۹ براي اجراي پروتکل TFTP در نظر گرفته شده است. وقتي که کرم به يک قرباني حمله مي کند، او را مجبور به دانلود کرم با استفاده از اين پروتکل مي نمايد. بنابر اين کرم از يک سرويس TFTP براي ارسال فايل استفاده مي نمايد پس با استفاده از

[1] FireWall

سيسيتم امنيتي بر روي پورت ۶۹ UDP مـي تـوان بـه طـور كامـل از آلـوده شـدن ميزبـان جلوگيري كرد.

```
#define SHELL_PORT_4444 4444
```

برنامه ي واسط بر روي پورت ۴۴۴۴ شروع به كار مي كنـد كـه بـا بـستن آن مـي تـوان از انتشار ويروس جلوگيري كرد.

بررسي هاي آغازين

چنانچه گفته شد، كرم، قبل از شروع به كار كامپيوتر قرباني را مورد برسي قرار مي دهد.

```
RegCreateKeyEx ( HKEY_LOCAL_MACHINE,
"SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run", 0, NULL,
REG_OPTION_NON_VOLATILE, KEY_ALL_ACCESS, NULL, &hKey, 0);
RegSetValueExA(hKey, "windows auto update", 0, REG_SZ, MSBLAST_EXE, 50);
RegCloseKey(hKey);
```

اين كد يک كليد جديد در رجيستري، براي اجراي خودكار كرم ايجاد مي كند. بـراي از بين بردن كرم بايد ابتدا اين كليد را از رجيستري حذف كرد.

```
CreateMutexA(NULL, TRUE, "BILLY");
if (GetLastError() == ERROR_ALREADY_EXISTS)
ExitProcess(0);
```

با اين تكه از كد كرم چک مي كند كه سيستم بـراي بـار دوم آلـوده نـشود. يـک مـشكل اساسي كه كرم ها با آن مواجه هستند ايـن اسـت كـه آنهـا كامپيوترهـاي آلـوده را مجـدداً آلوده مي كنند كه نهايتاً منجر به از كار افتادن آن مـي شـود و يـک سيـستم از كـار افتـاده نمي تواند كرم را پخش كند. روشي كه بلاستر براي بررسي اين مشكل دارد، ساخت يک شئ سراسـري بـه نـام BILLY مـي باشـد. يـک روش بـراي جلـوگيري از آلـوده شـدن سيستم ، ساخت يک Mutex با نام Billy مي باشد. پس از راه اندازي سيستم كرم فريب خورده و بر روي سيستم اجرا نمي شود.

```
winxp1_or_win2k2 = 1;
if ((rand()%10) > 7)
winxp1_or_win2k2 = 2;
```

اکنون باید دید که کاربر از چه سیستم عاملي استفاده مي کند. (WinXP يا 2000) کرم مجبور است که این را حدس بزند. روشي که بلاستر براي حدس زدن این مطلب استفاده مي کند این است که در ۸۰ درصد اوقات فرض مي کند که کاربر از ویندوز XP استفاده م کند و در سایر موارد ویندوز را ۲۰۰۰ فرض مي کند. و داده هاي مخصوص هرکدام را ارسال مي نماید.

تلاش براي حمله

```
if (!scan_local) {
ClassA = (rand() % 254)+1;
ClassB = (rand() % 254);
ClassC = (rand() % 254);
}
```

اگر کرم نتواند سیستمي را به صورت محلي یافت کند از یک روش تصادفي براي انتخاب آدرس IP استفاده مي کند. کرم از دامنه هاي بدي (بالاي ۲۲۴) استفاده مي کند. این کار باعث یک سري ترافیک هایي مي شود که این ترافیک هاي عجیب یک راه آسان براي کشف فعالیت کرم مي باشد.

```
void blaster_increment_ip_address()
{
for (;;) {
if (ClassD <= 254) {
ClassD++;
return;
}
ClassD = 0;
ClassC++;
if (ClassC <= 254)
return;
ClassC = 0;
ClassB++;
if (ClassB <= 254)
return;
ClassB = 0;
ClassA++;
if (ClassA <= 254)
continue;
ClassA = 0;
return;
}
}
```

بلاستر با استفاده از زيربرنامه ي فوق ، آدرس IP را به صورت افزايشي محاسبه مي نمايد.

حمله

```
#define MYLANG MAKELANGID(LANG_ENGLISH, SUBLANG_DEFAULT)
#define LOCALE_409 MAKELCID(MYLANG, SORT_DEFAULT)
GetDateFormat( LOCALE_409, 0, NULL, "d", daystring, sizeof(daystring));
GetDateFormat( LOCALE_409, 0, NULL, "M", monthstring, sizeof(monthstring));
if (atoi(daystring) > 15 && atoi(monthstring) > 8)
CreateThread(NULL, 0, blaster_DoS_thread, 0, 0, &ThreadId);
```

اكنون زمان بررسي تاريخ جاري مي باشد. كرم تاريخ را چک کرده و اگر در محدوده ي زير باشد، حمله ي DoS خود را عليه ميكروسافت انجام مي دهد كه همه ساله و بر اساس تاريخ محلي انجام مي شود:

۱۶ آگوست تا ۳۱ آگوست

۱۶ سپتامبر تا ۳۰ سپتامبر

۱۶ اكتبر تا ۳۱ اكتبر

۱۶ نوامبر تا ۳۰ نوامبر

۱۶ دسامبر تا ۳۱ دسامبر

```
for (;;)
blaster_spreader();
```

كار آخر برنامه اين است كه به شكل كرم در آمده و به ساير سيستم ها نفوذ كند كه اين عمل با استفاده از يک حلقه ي بي نهايت و فراخواني پردازه ي آلوده كننده، انجام مي شود. اين كرم داراي دو زير برنامه مهم مي باشد كه كليه عمليات اصلي را انجام مي دهند. يكي براي گسترش كرم و ديگري براي حمله به ميكروسافت.

مقابله

حذف دستي بلاستر

جهت مقابله و حذف بلاستر از كامپيوتر بايد مراحل زير طي شود:

۱. باز گرداندن اتصال اينترنت به حالت اوليه : در بسياري از حالات

در هر دو سيستم عامل ويندوز XP و 2000 ، تغيير تنظيمات RPC به شما اجازه مي دهد كه بدون Restart شدن بتوانيد به اينترنت متصل شويد. براي اين منظور گام هاي زير را بايد انجام داد:

- در منوي Start گزينه ي Run را انتخاب نموده تا كادر مربوطه باز شود.
- عبارت Services.MSC / S را تايپ نموده و كليد OK را بزنيد.
- در قاب سمت راست عبارت Remote Procedure Call (RPC) را بيابيد.
- بر روي آن راست ـ كليک كرده و از قسمت Properties بخش Recovery را انتخاب نماييد.
- اكنون تمام ليست هاي باز شونده را به عبارت Restart the Service تغيير داده و كليد OK را بزنيد.

۲. كار پردازش كرم را پايان دهيد: براي اين منظور از پنجره ي Task Manager و بخش پردازش ها عبارت Msblast.exe را يافته و با انتخاب آن و زدن دكمه ي End Process به كار بلاستر پايان مي دهيم.

۳. تغييرات اعمال شده به رجيستري را خنثي نماييم: (توصيه مي شود قبل از اعمال هرگونه تغيير بر رجيستري ، يک نسخه ي پشتيبان از آن تهيه كنيد.) پنجره ي Registry Editor را باز نموده و كليد زير را بيابيد:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

در قاب سمت راست Windows auto update را حذف نموده و از رجيستري خارج شويد.

اكنون با خيال راحت مي توانيد كرم بلاستر را به فراموشی بسپاريد.

قطعه كدي جهت حذف بلاستر

اين كد كه به زبان دلفي نوشته شده است، بلاستر را به صورت خودكار حذف نموده و با قرار دادن مقدار رشته اي Anti-Blaster كه حاوي مقدار رشته ای C:\WINDOWS\system32\anti_blaster.exe " /protect " مي باشد؛ در كليد زير

از رجيستري (همان كليدي كه بلاستر جهت آلوده كردن سيستم استفاده مي نمود.) از آلوده شدن سيستم جلوگيري مي كند:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

شرح برنامه به صورت زير می باشد:

شروع

```
uses
  TlHelp32, windows, ShellAPI;
```

بررسي وجود فايل با نام .FileName

```
function FileExists(const FileName : string) : boolean;
var
  Handle: THandle;
  FindData: TWin32FindData;
begin
 result := false;
 Handle := FindFirstFile(PChar(FileName), FindData);
 if Handle <> INVALID_HANDLE_VALUE then
  begin
   result := true;
   Windows.FindClose(Handle);
  end;
end;
```

افزودن كاراكتر "\ " به مسير فايل

```
function AddBackSlash(PathName : string) : string;
begin
 if (length(PathName)>0) and (PathName[length(PathName)]<>'\') then
   Result:=PathName'\'+
  else
   Result:=PathName;
end;
```

مسير ويندوز را بر مي گرداند

```
function SystemDirectory : string;
var
  SysDir : PChar;
begin
 getmem(SysDir, Max_Path;(
 try
  GetSystemDirectory(SysDir,Max_Path;(
  Result:=AddBackSlash(String(SysDir((
 finally
  freemem(SysDir, Max_Path;(
 end;
```

```
end;
```

بررسي مي كند كه آيا كاربر جاري مدير سيستم است يا خير.

```
function IsAdmin: Boolean;
const
  SECURITY_NT_AUTHORITY: TSIDIdentifierAuthority = (Value: (0, 0, 0, 0, 0,
5;((
  SECURITY_BUILTIN_DOMAIN_RID = $00000020;
  DOMAIN_ALIAS_RID_ADMINS     = $00000220;
var
  hAccessToken       : THandle;
  ptgGroups          : PTokenGroups;
  dwInfoBufferSize   : Cardinal;
  psidAdministrators : PSID;
  x                  : Integer;
begin
 Result := false;
 if not OpenThreadToken(GetCurrentThread, TOKEN_QUERY, TRUE,
hAccessToken) then
  begin
   if GetLastError <> ERROR_NO_TOKEN then Exit;
   if not OpenProcessToken(GetCurrentProcess, TOKEN_QUERY, hAccessToken)
then Exit;
  end;
 try
  GetTokenInformation(hAccessToken, TokenGroups, nil, 0, dwInfoBufferSize;(
  if GetLastError <> ERROR_INSUFFICIENT_BUFFER then Exit;
  GetMem(ptgGroups, dwInfoBufferSize;(
  try
   if not GetTokenInformation(hAccessToken, TokenGroups, ptgGroups,
dwInfoBufferSize, dwInfoBufferSize) then Exit;
   if not AllocateAndInitializeSid(SECURITY_NT_AUTHORITY, 2,
SECURITY_BUILTIN_DOMAIN_RID, DOMAIN_ALIAS_RID_ADMINS, 0, 0, 0,
0, 0, 0, psidAdministrators) then Exit;
    try
     for x := 0 to ptgGroups^.GroupCount - 1 do
      begin
       if EqualSid(psidAdministrators, ptgGroups^.Groups[x].Sid) then
        begin
         Result := true;
         Break;
        end;
      end;
    finally
   FreeSid(psidAdministrators;(
   end;
  finally
  FreeMem(ptgGroups;(
  end;
```

```
 finally
 CloseHandle(hAccessToken;(
 end;
end;

function Upper(s : string) : string;
var
  i : integer;
begin
 result := s;
 for i := 1 to length(result) do result[i] := UpCase(result[i;([
end;

var OSVersionInfo : TOSVersionInfo;
   regkey        : hkey;
   s             : string;
   SSHandle      : THandle;
   Continue      : boolean;
   ProcEntry     : TProcessEntry32;
   Disp          : dword;
Begin
```

نسخه ي سيستم عامل ويندوز را مشخص مي كند. اگر سيستم قابل آلوده شدن با بلاستر نباشد (مثلاً ويندوز ۹۸ باشد) پيام مناسب را نمايش مي دهد.

```
 OSVersionInfo.dwOSVersionInfoSize := SizeOf(OSVersionInfo;(
 GetVersionEx(OSVersionInfo;(
 if (OSVersionInfo.dwPlatformId <> VER_PLATFORM_WIN32_NT) or
(OSVersionInfo.dwMajorVersion < 5) then
  begin
  MessageBoxA(0, 'Your system can''t be infected by the Blaster Worm. So running
the cleaner is not neccessary.', 'Uninfectable system', mb_ok or mb_systemmodal or
MB_ICONINFORMATION;(
  halt(0;(
  end;
```

شروع برنامه و پاک کردن

```
 if paramcount = 0 then
  begin
```

آيا ما مدير سيستم هستيم ؟

```
   if not IsAdmin then
    begin
     MessageBoxA(0, 'You have to run this tool as a system administrator!',
'Administrator priviledges needed', mb_ok or mb_systemmodal or
MB_ICONINFORMATION;(
     halt(0;(
```

```
end;
```

پنجره ي خوش آمد گويي را نمايش مي دهد.

```
MessageBoxA(0, 'This tiny little program will delete the Blaster Worm and will
protect your PC from further infections.', 'Welcome', mb_ok or mb_systemmodal or
MB_ICONINFORMATION;(
```

يک کليد جديد به رجيستري اضافه مي کند که آن کليد در هر باز راه اندازي سيستم ، نرم افزار را اجرا مي کند و نام آن 'Anti-Blaster' مي باشد.

```
if not CopyFile(pchar(paramstr(0)), pchar(SystemDirectory + 'anti_blaster.exe'),
false(
 then MoveFileEx(pchar(paramstr(0)), pchar(SystemDirectory + 'anti_blaster.exe'),
MOVEFILE_DELAY_UNTIL_REBOOT;(

RegOpenKeyEx(hkey_local_machine,
'SOFTWARE\Microsoft\Windows\CurrentVersion\Run', 0, KEY_ALL_ACCESS,
regkey;(
RegSetValueEx(regkey, 'Anti-Blaster', 0, REG_SZ, pchar(s), length(s;((
RegCloseKey(regkey;(

s := ""+SystemDirectory + 'anti_blaster.exe" /protect;'
RegOpenKeyEx(hkey_local_machine,
'SOFTWARE\Microsoft\Windows\CurrentVersion\Run', 0, KEY_ALL_ACCESS,
regkey;(
RegSetValueEx(regkey, 'Anti-Blaster', 0, REG_SZ, pchar(s), length(s;((
RegCloseKey(regkey;(

s := ""+SystemDirectory + 'anti_blaster.exe" /uninstall;'
RegCreateKeyEx(hkey_local_machine,
'SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Anti-Blaster', 0, nil,
REG_OPTION_NON_VOLATILE, KEY_ALL_ACCESS, nil, regkey, @disp;(
RegSetValueEx(regkey, 'UninstallString', 0, REG_SZ, pchar(s), length(s;((
RegSetValueEx(regkey, 'DisplayName', 0, REG_SZ, pchar('Anti-Blaster'),
length('Anti-Blaster;(('
RegCloseKey(regkey;(
```

اگر بلاستر پيدا شود ، آن را حذف مي کند

```
if FileExists(pchar(SystemDirectory + 'MSBLAST.Exe')) then
 begin
```

پردازش (Process) مخصوص کرم را پيدا کرده و آن را حذف مي کند

```
SSHandle := CreateToolhelp32Snapshot(TH32CS_SnapProcess, 0;(
ProcEntry.dwSize := Sizeof(ProcEntry;(
Continue := Process32First(SSHandle, ProcEntry;(
while Continue do
```

```
    begin
     if  Upper(ProcEntry.szExeFile) = 'MSBLAST.EXE' then
      TerminateProcess(OpenProcess(PROCESS_TERMINATE, false,
ProcEntry.th32ProcessID), 0;(
     Continue := Process32Next(SSHandle, ProcEntry;(
    end;
   CloseHandle(SSHandle;(
```

فايل را حذف مي كند. اگر در حال اجرا باشد ، به ويندوز اجازه ي حذف آن را در راه اندازي بعدي مي دهد

```
  if not DeleteFile(pchar(SystemDirectory + 'MSBLAST.Exe')) then
   MoveFileEx(pchar(SystemDirectory + 'MSBLAST.Exe'), nil,
MOVEFILE_DELAY_UNTIL_REBOOT;(
```

كليد رجيستري كه كرم بلاستر به آن اضافه كرده را حذف مي كند

```
  RegOpenKeyEx(hkey_local_machine,
'SOFTWARE\Microsoft\Windows\CurrentVersion\Run', 0, KEY_ALL_ACCESS,
regkey;(
  RegDeleteValue(regkey, 'windows auto update;('
  RegCloseKey(regkey;(
```

طي پيامي موفقيت عمليات را اعلام مي نمايد

```
  if MessageBoxA(0, 'The worm was successfully cleaned and the install protection
was installed correctly. Its defnitly a good idea to install the Microsoft patch now. Do
you want to visit the download page of the patch now?', 'Disinfection successful',
mb_yesno or mb_systemmodal or MB_ICONQUESTION) = idyes then
   ShellExecute(0, 'open',
'http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS03-
026.asp', nil, nil, sw_shownormal;(
  end else
```

اكنون سيستم ديگر آلوده نمي باشد

```
   MessageBoxA(0, 'The worm was NOT found on your computer. The install
protection that prevents the worm from installing was installed successfully.', 'System
not infected', mb_ok or mb_systemmodal or MB_ICONINFORMATION;(
 end;
```

اگر كاربر بخواهد نرم افزار را حذف كند ، اين كار را انجام مي دهد

```
if paramstr(1) = '/uninstall' then
 begin
```

آيا ما مدير سيستم هستيم ؟

```
  if not IsAdmin then
   begin
```

```
    MessageBoxA(0, 'You have to run this tool as a system administrator!',
'Administrator priviledges needed', mb_ok or mb_systemmodal or
MB_ICONINFORMATION;(
    halt(0;(
   end;
```

کليد اجراي خودکار نرم افزار آنتي بلاستر را حذف مي کند

```
  RegOpenKeyEx(hkey_local_machine,
'SOFTWARE\Microsoft\Windows\CurrentVersion\Run', 0, KEY_ALL_ACCESS,
regkey;(
  RegDeleteValue(regkey, 'Anti-Blaster;('
  RegCloseKey(regkey;(
```

موجوديت Uninstall نرم افزار آنتي بلاستر را حذف مي کند

```
  RegDeleteKey(hkey_local_machine,
'SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Anti-Blaster;('
```

فايل 'anti_blaster.exe' را حذف مي کند

```
  MoveFileEx(pchar(SystemDirectory + 'anti_blaster.exe'), nil,
MOVEFILE_DELAY_UNTIL_REBOOT;(
```

و پيام موفقيت عمل حذف را نمايش داده و از کاربر درخواست راه اندازي مجدد را مي نمايد

```
  MessageBoxA(0, 'To complete the uninstallation of Anti-Blaster you have to reboot
your system!', 'Reboot needed', mb_ok or mb_systemmodal or
MB_ICONINFORMATION;(
  halt(0;(
 end;

// Create the worm mutex to prevent further installations (global and session only(
 CreateMutex(nil, false, 'Global\BILLY;('
 CreateMutex(nil, false, 'BILLY;('
```

نرم افزار متوقف مي شود. بلاستر از بين رفته و اکنون سيستم در امنيت کامل به سر مي برد.

```
 sleep(infinite;(
end.
```

پيوست

جهت اطلاعات بيشتر بـه بعـضي از كلمـات و اصـطلاحات مـورد اسـتفاده در شـبكه هـاي كامپيوتري اشاره اي مختصر شده است.

TCP : پروتكلي رايج در لايه حمـل از مجموعـه ي پروتكـل هـاي TCP/IP . اين سرويس به منظور برقراري ارتباط قابل اطمينان بين دو فرآيند در طول انواع شـبكه هـا طراحي شده است.

UDP : علاوه بر TCP ، UDP هم به عنـوان بخـشي از پروتكـل TCP/IP بـه كار مي رود. اين سرويس اساساً يک سرويس غير قابل اطمينان مي باشد.

RPC : RPC يک پروتكل مي باشد كه باعث مي شـود كـه يـک زيربرنامـه بـر روي كامپيوتری ديگر اجرا شود بدون اين كه برنامه نويس كدي در رابطـه بـا ايـن فعـل و انفعال بنويسد.

DoS Attack : اين حمله يک تلاش بـراي ايـن اسـت كـه يـک منبـع را بـراي كاربرش غير قابل دسترسي نمود. مثلاً هدف يک سرويس دهنده ي وب مي باشد و حملـه براي اين منظور است كه صفحات وب ميزبان بر روي اينترنت غير قابل دسترسي باشد. اين عمل يک جرم كامپيوتري و نقض قانون استفاده صحيح از اينترنت مي باشد.

منابع

پيرهادي ، محمود. *شبکه هاي کامپيوتري*. نشر آفتاب گرافيک. چ اول ۱۳۸۰.

Internet Resources :

1. www.microsoft.com
http://www.microsoft.com/security/encyclopedia/details.aspx?name=Win32%2fMsblast
2. www.wikipedia.org
http://en.wikipedia.org/w/index.php?title=Blaster_worm&redirect=no
3. www.symantec.com
http://www.symantec.com/security_response/writeup.jsp?docid=2003-081113-0229-99
4. www.ca.com
http://www3.ca.com/securityadvisor/virusinfo/virus.aspx?id=36265
5. www.micsymposium.org
http://www.micsymposium.org/mics_2005/papers/paper57.pdf
6. www.tik.ee.ethz.ch
http://www.tik.ee.ethz.ch/~ddosvax/publications/papers/dimva2005-duebendorfer-et-al-blaster_sobig.pdf
7. www.antivirus.about.com
http://antivirus.about.com/cs/virusencyclopedia/p/blaster.htm