
RAYESH
Research And Development Of Network Security Team
W32.Blaster
موضوع
Lord.Naykan (Sahand)
نویسنده
SecuringSystem
Yahoo ID
Lord.Naykan@Gmail.Com
Email
1382 - آذر
Remember Destroying And Terminating is Not An Art
UnderGround WhiteHat Hackers Group

مقدمه

پس از آنکه سایت ماکروسافت و همچنین windowsupdate.com در ساعت 2:14 به وقت ایران، در حدود دو ساعت غیر قابل دسترس شد. مسئولان امنیتی ماکروسافت اقدام های خود را جهت مقابله با این حمله DoS آغاز نمودند. (DoS یکی از روش های مورد علاقه هکران می باشد به صورتی که با ایجاد ترافیک در شبکه موجب از کار افتادن و اختلال در سیستم قربانی می شوند)
نکته : DoS مخفف کلمه Denial Of Service می باشد.
پس از صرف مدت زمان کوتاه مسئولان امنیتی سایت ماکروسافت، سایت windowsupdate.com را به windowsupdate.microsoft.com تغییر دادن و سپس با تغییرات در سیستم DNS خود باعث از بین رفتن این تحدید شدند. در عین حال یکی از نسخه های لینوکس را که در برابر حملات DoS مقاوم می باشد را برای این وب سایت انتخاب نمودند. (برای اولین بار ماکروسافت علنا و آشکارا از لینوکس به جای سیستم عامل ضعیف خود استفاده نمود)

سیستم هاي تحدید شده :

- Microsoft® Windows NT® 4.0
- Microsoft Windows® 2000
- Microsoft Windows XP
- Microsoft Windows Server™ 2003

توضیح مختصر از مشکل امنیتي سیستم عامل ویندوز :

RPC – Remote Procedure Call یک پروتکل می باشد و در سیستم عامل ویندوز نیز مورد استفاده قرار می گیرد. این پروتکل یک مکانیزم InterProcess ایجاد می کند. این Process این اجازه را می دهد که یک برنامه از یک کامپیوتری به کد اجرایی بر روی یک سیستم دیگر منتقل شود. RPC خود نیز از OSF – Open Software Foundation گرفته شده است، پس از آن ماکروسافت با افزودن چند محصول دیگر، برای سیستم عامل خود محصول جدیدو پرکاربردی را اضافه نمود.
این مشکل امنیتی در قسمتی از RPC که در ارتباط با تغییر پیغام در TCP/IP می باشد، پدید آمده است. به این دلیل که این برنامه رسیدگی نادرست به پیغام ها به عمل می آورد. این آسیب پذیری به خصوص، در DCOM – Distribute Component Object Modet که بر روی RPC قرار دارد بیشتر به چشم می خورد.
با پیدایش این مشکل هکر قادر است از راه دور دسترسی کامل بر روی سیستم قربانی داشته باشد و سپس با برنامه هایی نظیر Netcat و TFTP از اطلاعات سیستم قربانی استفاده نماید.
NetCat : نت کت که به چاقوی همه کاره ارتش الکترونیکی سوئیس معروف است. به نفوذگر این امکان را می دهد که به پورت های مختلف در شبکه و ... متصل شود. برای مثال از راه دور فایل اجرا کند و ... .
TFTP : یکی از بستگان FTP می باشد که وظیفه انتقال اطلاعات را داراست.

طرز کار کرم بلستر :

این کرم ها با استفاده از آسیب پذیری ویندوز از پورت 135 وارد سیستم می شوند و بسته به نوع کرم کارهای متفاوتی را انجام می دهند، از معمولترین کارها، اقدام به Denial Of Service بر روی windowsupdate.com می باشد.
نکته : ارسال یک SYN FLOOD بر روی پورت 80 برای windowsupdate.com که دارای 50 عدد Packets HTTP در هر دقیقه می باشد و هر پکت دارای 40 بایت.
اقدام به حملات داس بر روی رنج های IP
باعث Crash کردن DCOM می شود و در نتیجه کامپیوتر قربانی پس از 1 دقیقه راه اندازه می شود.

نکته : این کرم ها از پورت های TCP 4444 و از پورت UDP 69 که برای نرم افزار TFTP مورد استفاده قرار می گیرد نیز جهت منتشر شدن استفاده می کنند.
نکته : این کرم ها خود را بر روی RUN رجیستری قرار می دهند تا پس از هر بار راه اندازی سیستم به صورت خودکار بر روی سیستم اجرا شوند.

آنالیز کرم های بلستر :

W32Blaster :

توضیح مختصر : این نسخه را می توان پدر کرم های بلستر نام گذاری کرد
حجم : 6.176 بایت
پس از ورود به سیستم فایل msblast را در شاخه windows/system32 قرار می دهد. سپس بر روی رجیستری "ms blast.exe = windows auto update" را در شاخه
HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN قرار می دهد.

و در ادامه خطاب به موسس ماکروسافت :
I Just Want to Say Love You San
Billy Gates Why Do You Make This Possible? Stop Maiking Money And Fix Your Software

W32Blaster.B :

توضیح : این نسخه طبق آمار گروه امنیتی Hat-Squad در ایران بیشتر به چشم می خورد.
حجم : 7.200 بایت
پس از ورود به سیستم فایل penis32.exe را در شاخه windows/system32 قرار می دهد. سپس بر روی رجیستری "peinis32.exe= updatw Windows auto" در شاخه
HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN قرار می دهد

W32Blaster.C :

توضیح : این نسخه نیز متشکر از یک Backdoor به همراه یک تروجان در کنار کرم می باشد. این کرم پس از ورود فایل Teekids.exe را در شاخه windows/system32 قرار می دهد و سپس بر روی رجیستری " Teekids.exe = .. Microsoft Intel XP " را در شاخه
HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN قرار می دهد.
نکته : لازم به ذکر است این کرم از 3 فایل استفاده می کند که عبارتند از :
Index.exe : در ابتدا این فایل وارد کامپیوتر شده سپس قطعات دیگر کرم را دریافت می کند و تحت عنوان W32Blaster.C.Worm توسط ضد ویروس ها شناسایی می شود.
حجم : 32.045 بایت
Root32.exe : یک ترکیب Backdoor که با نام Lithium توسط ضد ویروس ها شناسایی می شود.
حجم : 19.798 بایت
Teekids.exe : فایل اصلی کرم که با نام W32Blaster.C.Worm توسط آنتی ویروس ها شناسایی می شود.
حجم : 5.360 بایت

W32Blaster.D :

توضیح : این کرم نیز مانند نسخه اول در رجیستری خطاب به بیل گیتس سخن می گوید.
حجم : 11.776 بایت

پس از ورود فایل Mspatch را در شاخه windows/system32 قرار می دهد. سپس بر روی رجیستری "mspatch.exe = AntiVIrus Nonton " را در شاخه
HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RU قرار می دهد.
لازم به ذکر است :
I Just Want To Say Love You SAN
Billy Gates Why Do you Make This possible? Stop Making Money And Fix Your Software

W32Blaster.E :

توضیح : این کرم پس از اجرا اقدام به DoS آی پی 127.0.0.1 می کند. (این آی پی، در همه کامپیوترها رزرو شده می باشد و مورد استفاده قرار نمی گیرند ولی صرفا برای استفاده همان کامپیوتر برای خود مورداستفاده قرار می گیرد.)
حجم : 6.176 بایت
پس از اجرا فایل Mslaugh.exe را در شاخه windows/system32 قرار می دهد. و سپس بر روی رجیستری " mslaugh.exe = windows automation " را در شاخه
HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN قرار می دهد.
و سپس پیغام
Forget The Promise for me B/DAY this particular strain to me ANG3L – hope yer enjoying yerself and don't I Dedicate
را در رجیستری قرار می دهد.

W32Blaster.F :

توضیح : به نظر بسیاری از مسئولان امنیت این آخرین نسخه از کرم بلستر می باشد.
حجم : 11.808
این کرم نیز پس از اجرا Enbiei.exe را در windows/system32 را قرار می دهد. سپس در رجیستری " Enbiei.exe = www.hidro.4t.com را در شاخه
HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN قرار می دهد

در صورتی که یکی از این کرم ها سیستم شما را آلوده نموده اند به ترتیب مراحل زیر را مرحله به مرحله انجام دهید :

خارج کردن از فایل های اجرایی

ابتدا کلید های CTRL+ALT+DELET را با هم بفشارید. سپس دکمه Processe را فشار دهید و به جستجوی فایل ها (که در بالا به آنها اشاره شد) بپردازید و پس از یافتن یک بار بر روی آنها کلیک چپ کنید و سپس دکمه End Process را انتخاب کنید.
نکته : در این مکان فایل هایی که در همین لحظه در سیستم شما در حال اجرا می باشند قرار گرفته است و نشان داده می شود.

نکته : معمولا برنامه نویسان با نوشتن یک خط در برنامه خود، به ویروس اعلام می کنند در صورتی که سیستم در حالت خاموش شدن است، به رجیستری و آدرس شاخه ویندوز رفته و نگاه کند که هنوز فایل ها و آدرس در آنجا قرار دارد یا خیر. سپس در صورت وجود نیافتن، یک نسخه از خود دوباره در آن کپی کند.

ایمن سازی رجیستری

به شاخه رجیستری
HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN
رفته و سپس با توضیحاتی که در بالا یاد شد، به یافتن یکی از جزئیات بپردازید و سپس کلیک راست را بر روی گزینه مورد نظر زده و پس از آن Delet را انتخاب کنید.

نکته : با این کار، دیگر پس از دوباره راه اندازی سیستم، کرم ها قادر به بارگذاری مجدد نیستند.
نکته : برای رفتن به رجیستری این مراحل را طی کنید Start>RUN>Regedit

از بین بردن فایل های اصلی کرم

سپس با رفتن با شاخه system32 اقدام به جستجو فایل های ذکر شده و سپس delet کردن آن بپردازید.
پس از آن سیستم خد را دوباره راه اندازی کنید.

دوباره راه اندازی سرویس RPC

ابتدا بر روی Start کلید نمایید سپس Run را انتخاب کنید. در خط فرمان عبارت service.msc /s را تایپ کنید و سپس Enter را بفشارید. پس از آن در لیست موجود (Remote Procedure Call (RPC را کلیک راست را زده، از میان گزینه های موجود Recover را انتخاب کنید. در پنجره جدید هر سه گزینه Change Failure, Subswquent Failure First Failure, Second را به Service Restart تغییر دهید و Ok را کلیک کنید.
نکته : این قبل از انجام این کار سیستم از ویروس پاکسازی شده باشد.

ایمن سازي سيستم :

ماکروسافت برای این مشکل امنیتی Patch ایمن ساز را ارائه داده است ولی به دلیل اینکه کلا روی ماکروسافت از لحاظ امنیتی نمی شود حساب کرد در نتیجه ابتدا Start را کلیک کنید سپس Run را انتخاب نمایید. در خط فرمان dcomcnfg را تایپ کنید، سپس Enter را فشار دهید. در پنجره جدید بر روی Component service کلیک کنید سپس فولدر Computers را انتخاب نمایید. پس از آن بر روی آن Right Click کنید و سپس Properties را انتخاب کنید. پس از آن از میان Tab های موجود Properties Defualt را انتخاب کنید و پس از آن Uncheck کنید گزینه Computer Enable Distributed COM On This

افزايش زمان :

این روش باعث از بین رفتن مدت دوباره راه اندازی سیستم نخواهد شد ولی این امکان را به شما می دهد که به افزایش مدت زمان دوباره راه اندازی سیستم اقدام کنید.
برای مثال کامپیوتر شما در ساعت 9:00 شاهد پیغام دوباره راه اندازی است و در ساعت 9:01 سیستم شما دوباره راه اندازی می شود. حال کافیست ساعت ویندوز خود را به همان مقدار که احتیاج دارید به عقب بکشید.
علت وجود داشتن این باگ در کرم های بلستر : هکر ها برای کم کردن حجم ویروس خود دیگر یک Timer طراحی نکرده و در نتیجه از ساعت ویندوز برای این کار کمک گرفته اند.

امیدوارم از این مقاله لذت برده باشید
با تشکر لرد نایکان (سهند)