عنوان: **از کجا به وب سرور شما حمله DOS شده است؟**
نویسنده: وحید نصیری
تاریخ: ۱۳۸۸/۰۳/۲۳ ۱۸:۳۹:۰۰
آدرس: www.dotnettips.info
برچسب‌ها: Security

اگر پیش فرض‌های IIS را تغییر نداده باشید، تمامی اعمال رخ داده در طی یک روز را در یک سری فایل‌های متنی در یکی از آدرس‌های زیر ذخیره می‌کند:

```
IIS 6.0: %windir%\System32\LogFiles\W3SVC<SiteID>
IIS 7.0: %systemDrive%\Inetpub\logfiles
```

اطلاعات فوق العاده ارزشمندی را می‌توان از این لاگ فایل‌های خام بدست آورد. اعم از تعداد بار دقیق مراجعه به صفحات، چه فایل‌هایی مفقود هستند (خطای 404)، کدام صفحات کندترین‌های سایت شما را تشکیل می‌دهند و الی آخر.
مایکروسافت برای آنالیز این لاگ فایل‌ها (که محدود به IIS هم نیست) ابزاری را ارائه داده به نام LogParser که این امکان را به شما می‌دهد تا از فایل‌های CSV مانند با استفاده از عبارات SQL کوئری بگیرید (چیزی شبیه به پروایدرهای LINQ البته در سال‌های 2005 و قبل از آن).
یکی از کاربردهای این ابزار، بررسی‌های امنیتی است.

سؤال؟ چگونه متوجه شوم کدام کامپیوتر در شبکه اقدام به حمله DOS کرده و سرور را دارد از پا در می‌آورد؟
از آنجائیکه در لاگ‌های IIS دقیقا IP تمامی درخواست‌ها ثبت می‌شود، با آنالیز این فایل ساده متنی می‌توان اطلاعات لازم را بدست آورد.

```
logparser.exe -i:iisw3c "select top 25 count(*) as HitCount, c-ip from
C:\WINDOWS\system32\LogFiles\W3SVC1\*.log group by c-ip order by HitCount DESC" -rtp:-1 > top25-ip.txt
```

دستور خط فرمان فوق، یک کوئری SQL را بر روی تمامی لاگ فایل‌های قرار گرفته در مسیر یاد شده اجرا کرده و نتیجه را در یک فایل متنی ذخیره می‌کند.
به این صورت می‌توان دقیقا متوجه شد که از کدام IP مشغول به زانو درآوردن سرور هستند.

اگر به این ابزار علاقمند شدید مطالعه مقاله زیر توصیه می‌شود:
Using LogParser 2.2 to Parse IIS Logs and Other Logs