

# DoS ile Mücadele

written by Mert SARICA | 1 March 2019

2009 yılından bu yana “Bilgi güçtür ve paylaşıldıkça artar!” sloganıyla siber güvenlik alanına meraklılar için özveriyle yaşatmaya çalıştığım blogum bundan yıllar yıllar önce bir DDoS saldırısı ile karşı karşıya kaldığını ve daha sonrasında blogumu Cloudflare arkasına taşıdığımı anımsıyorum. Son birkaç yıldır ise DDoS ve DoS benzeri bir saldırı ile karşılaşmamış olmanın verdiği rahatlık ile ne işletim sistemi üzerinde OSSEC gibi bir HIDS’i, ne Cloudflare, ne WordPress ne de Nginx üzerinde bu tür saldırılara karşı (Wordfence rate limiting, modsecurity vs.) bir koruma özelliğini devreye almamıştım.

15 Temmuz 2018 tarihinde blogumu ziyaret etmeye çalıştığımda web sunucusunun geç yanıt verdiğini farkettilim. “Acaba bu defa neyi bozdu?” diye kendi kendime homurdandıktan hemen sonra ssh ile sunucuma bağlandığımda herhangi bir yavaşlık farketmedim. Web sunucusundaki yavaşlığın uygulama katmanı ve/veya veritabanı ile ilgili olduğunu düşünerek top komutunu bile çalıştırmadan direk web sunucusunun erişim kayıtlarına (access.log) göz attığımda, 14 Temmuz saat 14:03 itibarıyla bloguma rastgele parametreler içeren çok sayıda istekte bulunduğu farkettilim. (HTTP DoS)

```
GNU nano 2.5.3 File: attack.txt
172.68.245.36 -- [14/Jul/2018:14:03:08 +0300] "POST /?HWNT=BYIDSXK HTTP/1.1" 502 568 "http://www.mertsartica.com/KPXAQGR" Mozilla/5.0 (Windows; U; MSIE 7.0; Windows NT 6.0; en-US)
172.68.245.36 -- [14/Jul/2018:14:03:08 +0300] "POST /?UEPFCUZX-2TKZPAB HTTP/1.1" 502 166 "http://www.mertsartica.com/EEGLDERT" Opera/9.80 (Windows NT 5.2; ; ru) Presto/2.5.22 Version/10.51
172.68.245.36 -- [14/Jul/2018:14:03:08 +0300] "POST /?ILGOCYX=GRBJKZK HTTP/1.1" 502 568 "http://engadget.search.aol.com/search?q=6wz3z" Mozilla/4.0 (compatible; MSIE 8.0; windows NT 5.1; Trident/4.0; SV1; S
172.68.245.36 -- [14/Jul/2018:14:03:08 +0300] "POST /?NGRA-ZPBR HTTP/1.1" 502 568 "http://www.google.com/?q=QOHTDD" Mozilla/4.0 (compatible; MSIE 8.0; windows NT 5.2; win64; x64; Trident/4.0)
172.68.245.36 -- [14/Jul/2018:14:03:08 +0300] "POST /?DOLNTH=J3ALFXP HTTP/1.1" 502 568 "http://www.mertsartica.com/ENMP" Mozilla/4.0 (compatible; MSIE 8.0; windows NT 5.1; Trident/4.0; SV1; .NET CLR 2.0.50725
172.68.245.36 -- [14/Jul/2018:14:03:08 +0300] "POST /?UBHBBH=QZZVGVK HTTP/1.1" 502 166 "http://engadget.search.aol.com/search?q=6wz3z" Opera/9.80 (Windows NT 5.2; ; ru) Presto/2.5.22 Version/10.51
172.68.245.36 -- [14/Jul/2018:14:03:08 +0300] "POST /?NROSKKAD=K5VLMYRHN HTTP/1.1" 502 568 "http://www.mertsartica.com/ZMPTOVEX" Mozilla/4.0 (compatible; MSIE 8.0; windows NT 6.1; WOW64; Trident/4.0; SLCC2
172.68.245.36 -- [14/Jul/2018:14:03:08 +0300] "POST /?HAKZDAD=H3HJ HTTP/1.1" 502 568 "http://www.mertsartica.com/3JTHAE" Mozilla/4.0 (compatible; MSIE 8.0; windows NT 5.1; Trident/4.0; SV1; .NET CLR 2.0.50725
172.68.245.36 -- [14/Jul/2018:14:03:08 +0300] "POST /?LXKXKF=JCKXNGXK HTTP/1.1" 502 568 "http://www.google.com/?q=GDHEBAP" Mozilla/4.0 (compatible; MSIE 8.0; windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?TORC-YIPMEIEJBV HTTP/1.1" 502 568 "http://www.google.com/?q=ACASETIP" Mozilla/4.0 (compatible; MSIE 8.0; windows NT 6.0; Trident/4.0; SLCC1; .NET CLR 2.0.50725
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?HGXUOTO=SRQL HTTP/1.1" 502 166 "http://engadget.search.aol.com/search?q=DXKQUT" Mozilla/5.0 (Windows; U; windows NT 5.2; en-US; rv:1.9.1.3) Gecko/200905
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?NNVNLBQQ=CSX HTTP/1.1" 502 166 "http://engadget.search.aol.com/search?q=PEHOLB" Opera/9.80 (Windows NT 5.2; ; ru) Presto/2.5.22 Version/10.51
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?UEVLIG=UJMK HTTP/1.1" 502 568 "http://www.usatoday.com/search/results?q=ALP2SR" Mozilla/5.0 (Windows; U; windows NT 5.2; en-US; rv:1.9.1.3) Gecko/20090824
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?WBSOXGD=JMBH HTTP/1.1" 502 568 "http://www.google.com/?q=VYDKAZ" Mozilla/5.0 (Windows; U; MSIE 7.0; windows NT 6.0; en-US)
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?XPIHJJAOL=AFUBXNLMM HTTP/1.1" 502 166 "http://www.mertsartica.com/NXUCCO" Mozilla/5.0 (Windows; U; windows NT 5.2; en-US; rv:1.9.1.3) Gecko/20090824 Fi
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?URRHO=MLUBYTCO HTTP/1.1" 502 568 "http://www.google.com/?q=QDZXV" Mozilla/5.0 (Windows; U; windows NT 5.1; en-US) AppleWebKit/532.1 (KHTML, like Gecko)
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?XRUWYXMY HTTP/1.1" 502 166 "http://www.google.com/?q=VJCVT" Mozilla/5.0 (Windows; U; windows NT 5.2; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3 (.S
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?PHYB=MNOO HTTP/1.1" 502 568 "http://www.usatoday.com/search/results?q=ZASMA" Mozilla/5.0 (Windows; U; windows NT 5.1; en-US) AppleWebKit/532.1 (KHTML, li
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?GVLU=HNAUC HTTP/1.1" 502 568 "http://www.usatoday.com/search/results?q=QVZYW" Mozilla/4.0 (compatible; MSIE 8.0; windows NT 5.1; Trident/4.0; SV1; .NET
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?WJXJH=KXQXO HTTP/1.1" 502 166 "http://engadget.search.aol.com/search?q=6wz3z" Mozilla/4.0 (compatible; MSIE 8.0; windows NT 6.1; WOW64; Trident/4.0; SV1;
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?OHTNTYBSL=SMXLBXJ HTTP/1.1" 502 568 "http://engadget.search.aol.com/search?q=CTAUOTHEKO" Mozilla/4.0 (compatible; MSIE 8.0; windows NT 5.1; Trident/4.0; S
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?YMUQ=KZ HTTP/1.1" 502 568 "http://www.mertsartica.com/KXZBWSB" Mozilla/4.0 (compatible; MSIE 8.0; windows NT 6.0; Trident/4.0; SLCC1; .NET CLR 2.0.50725
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?VXHHRI=SHUKEKT HTTP/1.1" 502 568 "http://www.google.com/?q=FAZ3JGEO" Mozilla/5.0 (Windows; U; windows NT 5.1; en-US) AppleWebKit/532.1 (KHTML, like Ge
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?YFZPOORNO=UZSSZOZMI HTTP/1.1" 502 166 "http://www.google.com/?q=ZMZNIMS" Opera/9.80 (Windows NT 5.2; ; ru) Presto/2.5.22 Version/10.51
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?WZMIZIQ=MHMK1 HTTP/1.1" 502 568 "http://www.mertsartica.com/GDDRODAQR" Mozilla/5.0 (Windows; U; windows NT 5.1; en-US) AppleWebKit/532.1 (KHTML, like Ge
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?BLAZIN=FAINFJB HTTP/1.1" 502 568 "http://www.mertsartica.com/BJABV" Mozilla/5.0 (Windows; U; MSIE 7.0; windows NT 6.0; en-US)
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?YXQMK=OSROHA HTTP/1.1" 502 166 "http://engadget.search.aol.com/search?q=SSASAEKOV" Mozilla/5.0 (Windows; U; MSIE 7.0; windows NT 6.0; en-US)
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?URRHS=SHHTKAQ HTTP/1.1" 502 166 "http://www.usatoday.com/search/results?q=XFNVP" Mozilla/5.0 (Windows; U; windows NT 6.1; en-US; rv:1.9.1.3) Gecko/200905
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?WJLXGNS=ONLNGF HTTP/1.1" 502 568 "http://www.google.com/?q=KVGDKK" Mozilla/5.0 (Windows; U; windows NT 5.1; en-US) AppleWebKit/532.1 (KHTML, like Ge
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?VNSRA=SES HTTP/1.1" 502 166 "http://www.google.com/?q=BZBZHBF" Mozilla/5.0 (Windows; U; windows NT 5.2; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3 $
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?TOLMLTKI=VWVJ HTTP/1.1" 502 568 "http://www.mertsartica.com/FMIMGB" Mozilla/4.0 (compatible; MSIE 8.0; windows NT 5.2; win64; x64; Trident/4.0)
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?LFRFC=GLCH HTTP/1.1" 502 568 "http://www.mertsartica.com/DEWIRAEI" Mozilla/5.0 (Windows; U; windows NT 5.1; en-US) AppleWebKit/532.1 (KHTML, like Ge
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?YPIIUBKQ=AUUEKNAXNL HTTP/1.1" 502 166 "http://engadget.search.aol.com/search?q=AGRESNSI" Mozilla/5.0 (Windows; U; windows NT 5.2; en-US; rv:1.9.1.3) Ge
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?TAHERIBIK=ZREYK HTTP/1.1" 502 166 "http://www.google.com/?q=SWRFLGV" Mozilla/5.0 (X11; ; Linux x86_64; en-US; rv:1.9.1.3) Gecko/20090913 Firefox/3.5.3
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?LCTIYI=QBHK HTTP/1.1" 502 568 "http://www.usatoday.com/search/results?q=CAKUCHEU" Mozilla/4.0 (compatible; MSIE 8.0; windows NT 5.1; Trident/4.0; SV1; S
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?YVYQZCQZ=CCZKXKGT HTTP/1.1" 502 166 "http://www.usatoday.com/search/results?q=KHKGDQ" Mozilla/5.0 (Windows; U; windows NT 6.1; en-US; rv:1.9.1.3) Ge
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?ZMOWZC=ZRHGP HTTP/1.1" 502 166 "http://engadget.search.aol.com/search?q=KKALUYHK" Mozilla/5.0 (Windows; U; windows NT 5.2; en-US; rv:1.9.1.3) Gecko/200905
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?VJVF=JHBAJUCZ HTTP/1.1" 502 568 "http://www.google.com/?q=KSNMWB" Mozilla/5.0 (Windows; U; MSIE 7.0; windows NT 6.0; en-US)
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?YVYQZCQZ=CCZKXKGT HTTP/1.1" 502 166 "http://www.usatoday.com/search/results?q=KHKGDQ" Mozilla/5.0 (Windows; U; windows NT 6.1; en-US; rv:1.9.1.3) Ge
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?EENRUIJZ=ATKJ5 HTTP/1.1" 502 166 "http://engadget.search.aol.com/search?q=JPARCBV" Mozilla/5.0 (Windows; U; windows NT 6.1; en-US; rv:1.9.1.3) Gecko/200905
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?VJUC=FYCMCRWH HTTP/1.1" 502 568 "http://www.mertsartica.com/GEXDTP" Mozilla/4.0 (compatible; MSIE 8.0; windows NT 5.1; Trident/4.0; SV1; .NET CLR 2.0.50725
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?ZBBS=PAETRNA HTTP/1.1" 502 166 "http://engadget.search.aol.com/search?q=ALOUIDA" Mozilla/5.0 (Windows; U; windows NT 6.1; en-US; rv:1.9.1.3) Gecko/200905
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?ZBMTYFUIR=ESRR HTTP/1.1" 502 568 "http://engadget.search.aol.com/search?q=JQKINDX" Mozilla/5.0 (Windows; U; MSIE 7.0; windows NT 6.0; en-US)
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?ZEXFTA=QUWFK5KK HTTP/1.1" 502 568 "http://www.mertsartica.com/VLZAF" Mozilla/4.0 (compatible; MSIE 8.0; windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?QZETL=HQBRODQ HTTP/1.1" 502 166 "http://www.google.com/?q=VYJYK" Mozilla/5.0 (Windows; U; windows NT 6.1; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?QSBATZIBX=BKTSUABS HTTP/1.1" 502 166 "http://engadget.search.aol.com/search?q=3FXCIE" Mozilla/5.0 (X11; ; Linux x86_64; en-US; rv:1.9.1.3) Gecko/20090913
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?DNRDDHI=CBKPPD HTTP/1.1" 502 568 "http://www.google.com/?q=VYKZJHID" Mozilla/5.0 (Windows; U; windows NT 5.1; en-US) AppleWebKit/532.1 (KHTML, like Ge
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?ZLQ=GLZIMHW HTTP/1.1" 502 166 "http://www.google.com/?q=QWQVEJ" Mozilla/5.0 (Windows; U; windows NT 6.1; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?AIUIVXVDY=VAZGPKV HTTP/1.1" 502 568 "http://engadget.search.aol.com/search?q=3NLTCAWF" Mozilla/4.0 (compatible; MSIE 8.0; windows NT 5.1; Trident/4.0; SV
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?ZIFQ=ORSWBWRKH HTTP/1.1" 502 568 "http://www.mertsartica.com/KHXVLOU" Mozilla/4.0 (compatible; MSIE 8.0; windows NT 5.2; win64; x64; Trident/4.0)
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?ZIFLWV=ZCVKJUZKA HTTP/1.1" 502 568 "http://www.google.com/?q=BLQJPKZL" Mozilla/4.0 (compatible; MSIE 8.0; windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?ZLBDYQ=USU HTTP/1.1" 502 568 "http://www.mertsartica.com/MNVQX" Mozilla/4.0 (compatible; MSIE 8.0; windows NT 5.2; win64; x64; Trident/4.0)
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?ZLBDYQ=USU HTTP/1.1" 502 568 "http://www.google.com/?q=WHMAME" Mozilla/5.0 (Windows; U; windows NT 5.1; en-US) AppleWebKit/532.1 (KHTML, like Ge
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?HQOLBNYI=HQGTADQX HTTP/1.1" 502 166 "http://www.mertsartica.com/FAZRPZ" Mozilla/5.0 (Windows; U; windows NT 5.2; en-US; rv:1.9.1.3) Gecko/20090824 Firef
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?ZJWHU=RFIEIUP HTTP/1.1" 502 166 "http://www.usatoday.com/search/results?q=TYVDA" Mozilla/5.0 (Windows; U; windows NT 6.1; en-US; rv:1.9.1.3) Gecko/20090824
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?ZJWHU=RFIEIUP HTTP/1.1" 502 166 "http://www.usatoday.com/search/results?q=SAVOLDUP" Mozilla/5.0 (X11; ; Linux x86_64; en-US; rv:1.9.1.3) Gecko/200905
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?ZVHWJQHL=LQWYVADP HTTP/1.1" 502 568 "http://www.google.com/?q=ZOHSPAD" Mozilla/4.0 (compatible; MSIE 8.0; windows NT 5.2; win64; x64; Trident/4.0)
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?ZVHWJQHL=LQWYVADP HTTP/1.1" 502 166 "http://www.usatoday.com/search/results?q=SAVOLDUP" Mozilla/5.0 (X11; ; Linux x86_64; en-US; rv:1.9.1.3) Gecko/200905
172.68.245.36 -- [14/Jul/2018:14:03:09 +0300] "POST /?ZVHWJQHL=LQWYVADP HTTP/1.1" 502 166 "http://www.usatoday.com/search/results?q=6SQC" Mozilla/5.0 (Windows; U; windows NT 5.2; en-US; rv:1.9.1.3) Gecko/20090824
```

HTTP DoS saldırısını gerçekleştiren kaynak ip adreslerine bakıp,

Cloudflare'in ip adreslerini gördüğümde, rehabetin bedelinden çıkardığım ilk ders (lessons learned) Cloudflare'e yapılan istekleri web sunucuma göndermek (CF-Connecting-IP başlığı) oldu. :) Bir yandan saldırının tam olarak hangi ülkeden kaynaklandığını öğrenmek için Cloudflare'in Analytics sayfasındaki tehdit haritasına baktığımda DoS saldırısının Rusya'dan yapıldığını öğrendim. (Bu cümleyi yazdıktan sonra nedense aklıma Red Alert 2'deki Tanya geldi. :))

```
GNU nano 2.5.3 File: nginx.conf
#user www-data;
worker_processes auto;
pid /run/nginx.pid;

events {
    worker_connections 768;
    # multi_accept on;
}

http {
    include /etc/nginx/cloudflare;
    ##
    ## Basic Settings
    ##
    sendfile on;
    tcp_nopush on;
    tcp_nodelay on;
    keepalive_timeout 65;
    types_hash_max_size 2048;
    server_tokens off;
    client_max_body_size 40M;

    # server_names_hash_bucket_size 64;
    # server_name_in_redirect off;

    include /etc/nginx/mime.types;
    default_type application/octet-stream;

    ##
    ## SSL Settings
    ##
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2; # Dropping SSLv3, ref: POODLE
    ssl_prefer_server_ciphers on;

    ##
    ## Logging Settings
    ##
    access_log /var/log/nginx/access.log;
    error_log /var/log/nginx/error.log;

    ##
    ## Gzip Settings
    ##

    gzip on;
    gzip_disable "msie6";

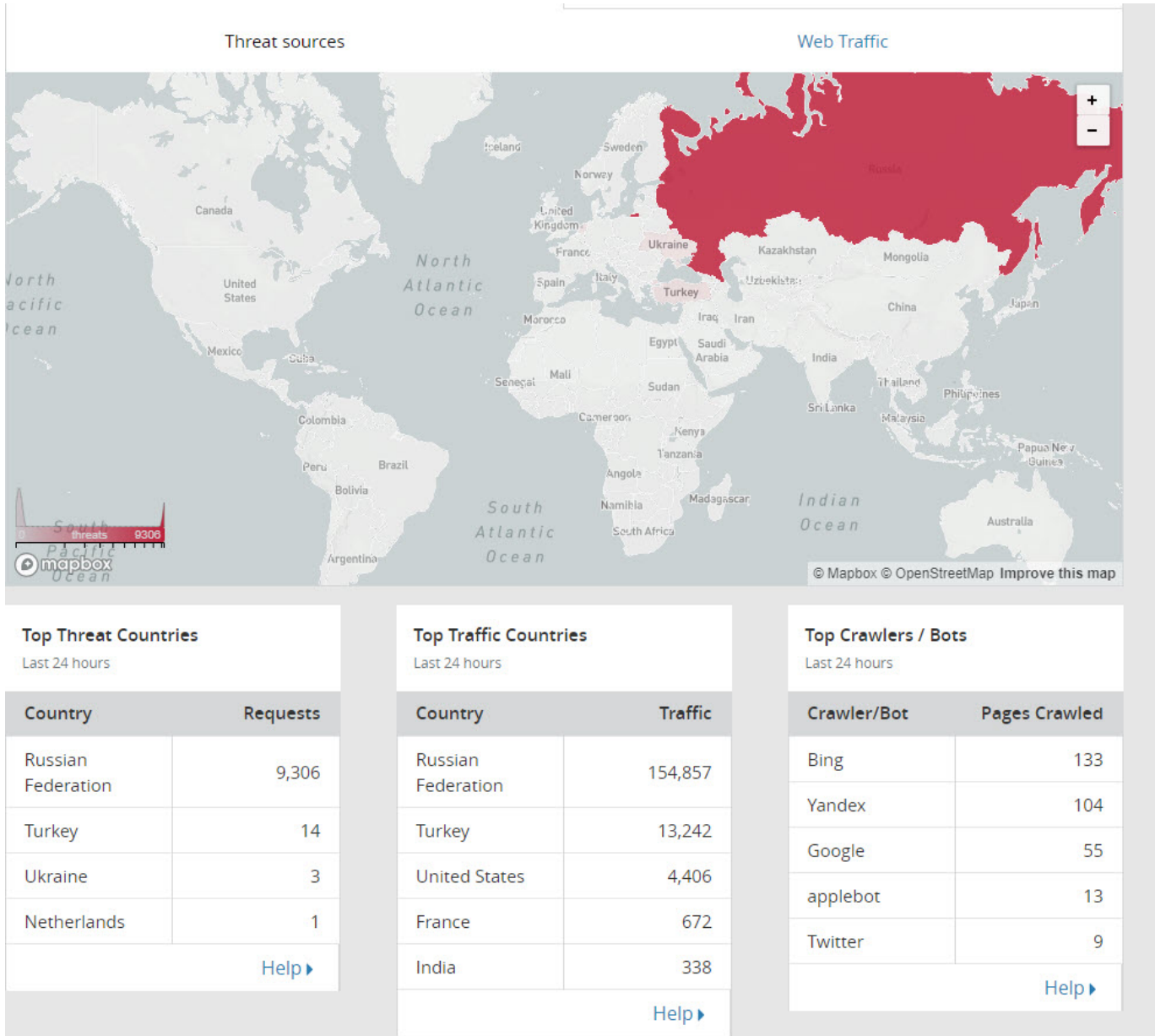
    # gzip_vary on;
    # gzip_proxied any;
    # gzip_comp_level 6;
    # gzip_buffers 16 8k;
    # gzip_http_version 1.1;
    # gzip_types text/plain text/css application/json application/javascript text/xml application/xml application/xml+rss text/javascript;

    ##
    ## Virtual Host Configs
    ##

    include /etc/nginx/conf.d/*.conf;
    include /etc/nginx/sites-enabled/*;
}

set_real_ip_from 103.21.244.0/22;
set_real_ip_from 103.22.200.0/22;
set_real_ip_from 103.31.4.0/22;
set_real_ip_from 104.16.0.0/12;
set_real_ip_from 108.162.192.0/18;
set_real_ip_from 131.0.72.0/22;
set_real_ip_from 141.101.64.0/18;
set_real_ip_from 162.158.0.0/15;
set_real_ip_from 172.64.0.0/13;
set_real_ip_from 173.245.48.0/20;
set_real_ip_from 188.114.96.0/20;
set_real_ip_from 190.93.240.0/20;
set_real_ip_from 197.234.240.0/22;
set_real_ip_from 198.41.128.0/17;
set_real_ip_from 2400:cb00::/32;
set_real_ip_from 2606:4700::/32;
set_real_ip_from 2803:f800::/32;
set_real_ip_from 2405:b500::/32;
set_real_ip_from 2405:8100::/32;
set_real_ip_from 2c0f:f248::/32;
set_real_ip_from 2a06:98c0::/29;

# use any of the following two
real_ip_header CF-Connecting-IP;
#real_ip_header X-Forwarded-For;
```



Ben bu arařtırmaları yaparken bir yandan DoS saldırısı devam ettiđi iin saldırıları durdurmak iin Cloudflare'in panelinden Under Attack zelliđini aktif hale getirdim ve saldırı anında etkisiz hale geldi. Akabinde saldırı ile ilgili istatistiki bilgiler toplamak iin ncelikle komut satırından ardından da SolarWinds'in Loggly isimli web uygulamasından faydalandım. Loggly dıřında evrimdıřı analiz iin de bir yandan Apache Logs Viewer aracının ıktılarını inceledim. Analiz sonucuna gre ~24 saatte bloguma yaklaşık ~150.000 istek yapılmıř ve bunlardan ~60.000 tanesi (502 HTTP Status) blogumu eriřilemez hale getirmiřti.

Cloudflare Dashboard Overview for mertsarica.com

**Status:** Active

This website is active on Cloudflare.

**Quick Actions:** Under Attack Mode (highlighted with a red arrow), Development Mode

**Domain Summary:**

- Security Level: High
- SSL: Flexible
- Caching Level: Standard
- Development Mode: Disabled

**Subscription:** Manage your subscriptions | Change Plan

```

root@batcave: /var/log/nginx# grep "POST /?" access.log.1 > attack.txt
root@batcave: /var/log/nginx# grep "POST /?" access.log >> attack.txt
root@batcave: /var/log/nginx# wc -l attack.txt
188442 attack.txt
root@batcave: /var/log/nginx# tail -n 10 attack.txt
172.68.182.207 - - [15/Jul/2018:11:28:35 +0300] "POST /?LJSDYXIV=UALDYIH HTTP/1.1" 200 20026 "http://engadget.search.aol.com/search?q=HYAQIAGGIQ" "Mozilla/5.0 (windows; u; windows NT 5.2; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3 (.NET CLR 3.5.30729)"
172.68.182.207 - - [15/Jul/2018:11:28:36 +0300] "POST /?YVQW=LIJOD HTTP/1.1" 200 20030 "http://www.mertsarica.com/3VXREF" "Mozilla/4.0 (compatible; MSIE 8.0; windows NT 5.2; win64; x64; Trident/4.0)"
172.68.182.207 - - [15/Jul/2018:11:28:36 +0300] "POST /?YVCMQCQAT=MOVEBABC HTTP/1.1" 200 19805 "http://www.google.com/?q=OSAHMYSO" "Mozilla/4.0 (compatible; MSIE 8.0; windows NT 5.2; win64; x64; Trident/4.0)"
090824 Firefox/3.5.3 (.NET CLR 3.5.30729)
172.68.182.207 - - [15/Jul/2018:11:28:37 +0300] "POST /?PTDAC=RFB HTTP/1.1" 200 20027 "http://engadget.search.aol.com/search?q=IFNDDR" "Mozilla/5.0 (windows; u; windows NT 5.1; en-US) AppleWebKit/532.1 (KHTML, like Gecko) Chrome/4.0.219.6 Safari/532.1"
172.68.182.207 - - [15/Jul/2018:11:28:38 +0300] "POST /?OKO=SWNWS HTTP/1.1" 200 20030 "http://www.mertsarica.com/GYMNZITLN" "Mozilla/5.0 (windows; u; windows NT 5.1; en-US) AppleWebKit/532.1 (KHTML, like Gecko) Chrome/4.0.219.6 Safari/532.1"
172.68.182.207 - - [15/Jul/2018:11:28:38 +0300] "POST /?NWY=QUIPE HTTP/1.1" 200 19803 "http://www.google.com/?q=WXHG" "Opera/9.80 (Windows NT 5.2; u; ru) Presto/2.5.22 Version/10.51"
172.68.182.207 - - [15/Jul/2018:11:28:38 +0300] "POST /?WACD=NGUACSLIC HTTP/1.1" 200 20029 "http://engadget.search.aol.com/search?q=RMQKXPKK" "Mozilla/5.0 (windows; u; windows NT 5.1; en-US) AppleWebKit/532.1 (KHTML, like Gecko) Chrome/4.0.219.6 Safari/532.1"
172.68.182.207 - - [15/Jul/2018:11:28:39 +0300] "POST /?PGUMCO=MDF HTTP/1.1" 200 20030 "http://www.usatoday.com/search/results?q=ZBXXVLYBD" "Mozilla/5.0 (windows; u; windows NT 6.1; en-US; rv:1.9.1.1) Gecko/20090718 Firefox/3.5.1"
172.68.182.207 - - [15/Jul/2018:11:28:39 +0300] "POST /?TJUDM=DMSVPC HTTP/1.1" 200 20027 "http://www.usatoday.com/search/results?q=FAPXPTEE" "Mozilla/4.0 (compatible; MSIE 8.0; windows NT 6.0; Trident/4.0; SLCC1; .NET CLR 2.0.50727; .NET CLR 1.1.4322; .NET CLR 3.5.30729; .NET CLR 3.0.30729)"
root@batcave: /var/log/nginx#

```

Loggly Dashboard

Search all log sources

**Popular Log Sources:**

- Linux System Log
- Linux File Monitoring
- Nginx
- Apache

**All Log Sources:**

- Amazon Cloudfront
- Amazon Cloudtrail
- Amazon Cloudwatch Logs
- Amazon Cloudwatch Metrics
- Amazon Config Logging
- Amazon ELB
- Amazon SNS
- Amazon SQS
- Android
- Apache
- Apache
- Command Line
- Don't see your log source? Request a New Log Source

© 2018 Loggly Inc., All Rights Reserved.

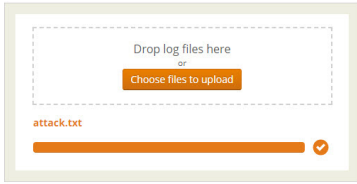
## File upload

### 1 Step 1: Upload Your File

You can send up to a max of 100MB per file and 1MB per event. The file should be line-separated text data, and the events can be up to 7 days old. Compressed files are not supported. You can upload a log file using common file types: .txt, .log, .csv and .json and quickly see what Loggly can do for you.

Remove any text in the filename after the file type extension. For example, a filename such as nginx-access.log is acceptable. But a filename such as nginx-access.log-20171109 will be rejected, so please rename such a file and then upload it.

The following file types are not supported: bin, exe, .lib, .dat, .mp3, .gif, .jpg, .jpeg, .bmp, .zip, .gz, .tar, .dll, .png, .img, .db, .llb, .pdf, .mp4, .mpeg, .mov, .jar, .pem, .crt, .doc, .xls, .xlsx, .docx, .ppt, .pptx, .dmg, .rar, .apk, and .7z



### 2 Step 2: Verify

✓ Congratulations! We received your logs and they have been automatically parsed.

### 3 Step 3: Next Steps

View in Search  
File Monitoring Setup

#### Advanced Options

Windows File Monitoring  
Linux File Monitoring  
Timestamps

#### Troubleshooting

Troubleshoot File Upload  
Community Forum

Need help? Email us

#### Field Explorer

- requestURI
- Field Actions
- remoteAddr: 300 values, 148K events
- requestMethod: /?AAAWTYTWV=VGGDD: 2
- requestURI: /?AAB=VNZWMA: 2
- requestURI: /?AABL=QLV: 2
- # size: /?AABNQVX=FIZK: 2
- status: /?AABSROVCH=DKXUM: 2
- userAgent: /?AABSTIC=IUL: 2
- /?AABXJYK=QIXYL: 2
- /?AADGFWW=LXHCET: 2
- /?AADHCTG=HJNCIC: 2
- /?AADJDM=HNIWSTTQE: 2
- /?AAELR=SBWATCK: 2
- /?AAEMHASDQ=CRGMTE: 2
- /?AAEPVUSH=DOMXOCKSK: 2
- /?AAEVD=TEYSFANY: 2
- /?AAP=NWUL: 2
- /?AAFADJANQ=ZFWZTVP: 2
- /?AAX=ASCZTQMA: 2
- /?AAGH=JROVWFMK: 2
- /?AAGRNE=YIAYUO: 2
- /?AAGPWCMD=GHYMGEVOY: 2
- /?AAHCXN=JZIRQAW: 2
- /?AAHFNHL=GOUVTA: 2

2018-07-13T00:00:00+03:00
2018-07-15T17:42:36:530+03:00
Search

2,916 events

Group 1

Chart type: Line | Split by: apache.requestURI | Sort by: value (desc) | Limit to: 10 | Show Other | Theme: [Colorful]

Value type: Event count | Source Groups: All Sources

Filters: Choose Filter | Apply

Find series to pin

Event View | Sort: Ascending | Expand Events | More Options

```

2018-07-15 11:28:39.000 { apache: { referer: "http://www.usatoday.com/search/results?q=FAXPTEE", size: 20027, requestMethod: "POST", userAgent: "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; Trident/4.0; SLCC1; .NET CLR 2.0.50727; .NET CLR 1.1.4322; .NET CLR 3.5.30729; .NET CLR 3.0.30729)", requestURI: "/?TUDH=DNMSVPC", requestProtocol: "HTTP/1.1", remoteAddr: "172.68.182.287", timestamp: "15/Jul/2018:11:28:39 +0300", status: 200 }, http: { clientHost: "" }, contentType: "text/plain" } }
2018-07-15 11:28:39.000 { apache: { referer: "http://www.usatoday.com/search/results?q=ZKXLYBD", size: 20038, requestMethod: "POST", userAgent: "Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.1) Gecko/20090718 Firefox/3.5.1", requestURI: "/?RBUJCH=HGF", requestProtocol: "HTTP/1.1", remoteAddr: "172.68.182.207", timestamp: "15/Jul/2018:11:28:39 +0300", status: 200 }, http: { clientHost: "" }, contentType: "text/plain" } }
2018-07-15 11:28:38.000 { apache: { referer: "http://engadget.search.aol.com/search?q=RNQNLNPE", size: 20039, requestMethod: "POST", userAgent: "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; AppleWebKit/532.1 (KHTML, like Gecko) Chrome/4.0.219.6 Safari/532.1", requestURI: "/?NACD=NBUCSLIC", requestProtocol: "HTTP/1.1", remoteAddr: "172.68.182.287", timestamp: "15/Jul/2018:11:28:38 +0300", status: 200 }, http: { clientHost: "" }, contentType: "text/plain" } }
2018-07-15 11:28:38.000 { apache: { referer: "http://www.google.com/?q=KIDMG", size: 19883, requestMethod: "POST", userAgent: "Opera/9.80 (Windows NT 5.2; U; ru) Presto/2.5.22 Version/10.51", requestURI: "/?M=QPE", requestProtocol: "HTTP/1.1", remoteAddr: "172.68.182.207", timestamp: "15/Jul/2018:11:28:38 +0300", status: 200 }, http: { clientHost: "" }, contentType: "text/plain" } }
                    
```

LOGGLY Search Charts Dashboard Alerts Derived Fields Source Setup Live Tail Labs Feedback 29 days left Subscribe Now

All Sources tag\_file\_upload 2018-07-13T00:00:00+03:00 2018-07-15T17:42:36:530+03:00 Search

Applied Filters: apache.status: 500 OR apache.status: 502 OR apache.status: 200

Field Explorer

Field	Values	Count
status	200	90343
	502	57938
	500	161

148,442 events

Chart type: Pie Split by: apache.status Sort by: value (desc) Limit to: 10 Show Other Theme: [Colorful]

Value type: Event count Source Groups: All Sources

Event View Sort: Ascending Expand Events More Options

```

2018-07-15 11:28:39.000 { apache: { referer: "http://www.usatoday.com/search/results?q=FAKPXTEE", size: 20027, requestMethod: "POST", userAgent: "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; Trident/4.0; SLCC1; .NET CLR 3.0.50727; .NET CLR 3.1.4322; .NET CLR 3.5.30729; .NET CLR 3.0.30729)", requestURI: "/?PID=MSNSRPC", requestProtocol: "HTTP/1.1", remoteAddr: "172.68.182.207", timestamp: "15/Jul/2018:11:28:39 +0300", status: 200 }, http: { clientHost: "172.68.182.207", contentType: "text/plain" } }
2018-07-15 11:28:39.000 { apache: { referer: "http://www.usatoday.com/search/results?q=ZKXVLY8D", size: 20030, requestMethod: "POST", userAgent: "Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.1) Gecko/20090718 Firefox/3.5.1", requestURI: "/?PGUQ=HDF", requestProtocol: "HTTP/1.1", remoteAddr: "172.68.182.207", timestamp: "15/Jul/2018:11:28:39 +0300", status: 200 }, http: { clientHost: "172.68.182.207", contentType: "text/plain" } }
2018-07-15 11:28:38.000 { apache: { referer: "http://engadget.search.aol.com/search?q=RMQOINPKE", size: 20029, requestMethod: "POST", userAgent: "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; AppleWebKit/532.1 (KHTML, like Gecko) Chrome/4.0.219.6 Safari/532.1", requestURI: "/?PID=MSNSRPC", requestProtocol: "HTTP/1.1", remoteAddr: "172.68.182.207", timestamp: "15/Jul/2018:11:28:38 +0300", status: 200 }, http: { clientHost: "172.68.182.207", contentType: "text/plain" } }
2018-07-15 11:28:38.000 { apache: { referer: "http://www.google.com?q=QUMQD", size: 19883, requestMethod: "POST", userAgent: "Opera/9.80 (Windows NT 5.2; U; rv) Presto/2.5.22 Version/10.51", requestURI: "/?PID=MSNSRPC", requestProtocol: "HTTP/1.1", remoteAddr: "172.68.182.207", timestamp: "15/Jul/2018:11:28:38 +0300", status: 200 }, http: { clientHost: "172.68.182.207", contentType: "text/plain" } }

```

LOGGLY Search Charts Dashboard Alerts Derived Fields Source Setup Live Tail Labs Feedback 29 days left Subscribe Now

All Sources tag\_file\_upload 2018-07-13T00:00:00+03:00 2018-07-15T17:42:36:530+03:00 Search

Applied Filters: apache.remoteAddr: 172.68.51.183 OR apache.remoteAddr: 172.68.245.36 OR apache.remoteAddr: 172.68.182.207 OR apache.remoteAddr: 172.68.246.73

Field Explorer

Field	Values	Count
remoteAddr	172.68.245.36	143727
	172.68.51.183	3816
	172.68.182.207	817
	172.68.246.73	82

148,442 events

Chart type: Pie Split by: apache.remoteAddr Sort by: value (desc) Limit to: 10 Show Other Theme: [Colorful]

Value type: Event count Source Groups: All Sources

Event View Sort: Ascending Expand Events More Options

```

2018-07-15 11:28:39.000 { apache: { referer: "http://www.usatoday.com/search/results?q=FAKPXTEE", size: 20027, requestMethod: "POST", userAgent: "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; Trident/4.0; SLCC1; .NET CLR 3.0.50727; .NET CLR 3.1.4322; .NET CLR 3.5.30729; .NET CLR 3.0.30729)", requestURI: "/?PID=MSNSRPC", requestProtocol: "HTTP/1.1", remoteAddr: "172.68.182.207", timestamp: "15/Jul/2018:11:28:39 +0300", status: 200 }, http: { clientHost: "172.68.182.207", contentType: "text/plain" } }
2018-07-15 11:28:39.000 { apache: { referer: "http://www.usatoday.com/search/results?q=ZKXVLY8D", size: 20030, requestMethod: "POST", userAgent: "Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.1) Gecko/20090718 Firefox/3.5.1", requestURI: "/?PGUQ=HDF", requestProtocol: "HTTP/1.1", remoteAddr: "172.68.182.207", timestamp: "15/Jul/2018:11:28:39 +0300", status: 200 }, http: { clientHost: "172.68.182.207", contentType: "text/plain" } }
2018-07-15 11:28:38.000 { apache: { referer: "http://engadget.search.aol.com/search?q=RMQOINPKE", size: 20029, requestMethod: "POST", userAgent: "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; AppleWebKit/532.1 (KHTML, like Gecko) Chrome/4.0.219.6 Safari/532.1", requestURI: "/?PID=MSNSRPC", requestProtocol: "HTTP/1.1", remoteAddr: "172.68.182.207", timestamp: "15/Jul/2018:11:28:38 +0300", status: 200 }, http: { clientHost: "172.68.182.207", contentType: "text/plain" } }
2018-07-15 11:28:38.000 { apache: { referer: "http://www.google.com?q=QUMQD", size: 19883, requestMethod: "POST", userAgent: "Opera/9.80 (Windows NT 5.2; U; rv) Presto/2.5.22 Version/10.51", requestURI: "/?PID=MSNSRPC", requestProtocol: "HTTP/1.1", remoteAddr: "172.68.182.207", timestamp: "15/Jul/2018:11:28:38 +0300", status: 200 }, http: { clientHost: "172.68.182.207", contentType: "text/plain" } }

```

Apache Logs Viewer

File Edit Reports Statistics Graph Help

Open Access Log Options

Choose the log format Please refer to the Webserver configuration if unsure.

Combined (Contains Browser and Referrer Information)  
 LogFormat "%h %l %u %t \"%r\" %> s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined

Common (default)  
 LogFormat "%h %l %u %t \"%r\" %> s %b" common

W3C (IIS - Microsoft Internet Information Services)

Other Nginx

Custom

---

Read

All Read All file and update in real time.

Date Range Read only date range that falls with the below range.

Start: 13.07.2018 End: 15.07.2018  
00:00:01 23:59:59

Adjust time by 0,00 hours.

[Help](#) OK

Update Completed 18:04:17 [No Filter] [Unlock](#) iannet

Apache Logs Viewer

File Edit Reports Statistics Graph Help

Enable All Reports

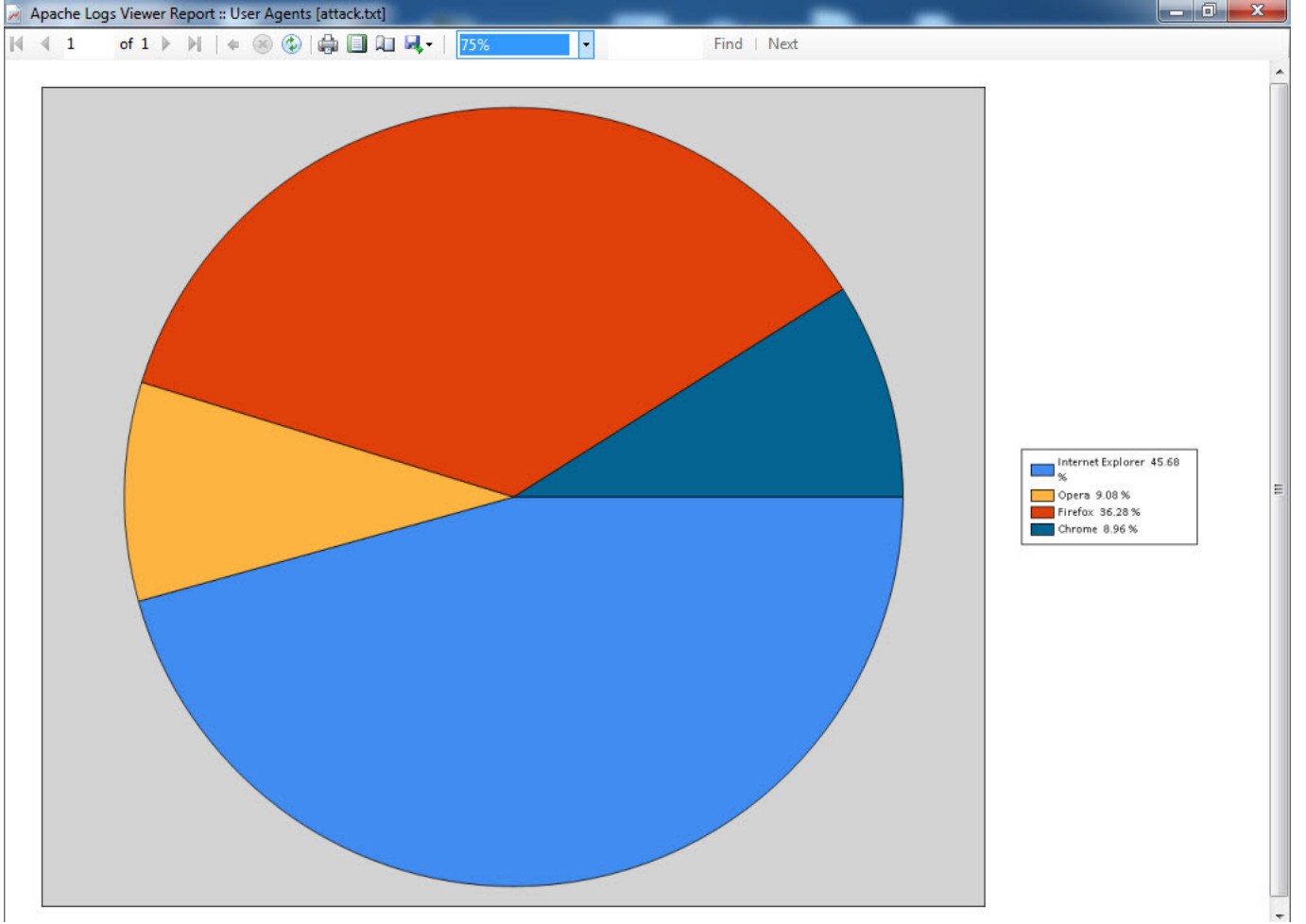
Report Source: [Filtered Data]

IP Address:  | User Agent:  | Referrer:

All Apply Filter Sort

IP Address	Sta...	Size	Country	Referer	User Agent	
172.68.245.36	PGOFOL HTTP/1.1	502	568	United States	http://www.google.com/?q=KYZJCBLJZ	Mozilla/4.0 (compatib
172.68.245.36	BRXWJ HTTP/1.1	502	568	United States	http://engadget.search.aol.com/search?q=JE...	Mozilla/4.0 (compatib
172.68.245.36	W HTTP/1.1	502	568	United States	http://www.google.com/?q=NWTZQ	Mozilla/4.0 (compatib
172.68.245.36	HTTP/1.1	502	166	United States	http://www.usatoday.com/search/results?q=...	Opera/9.80 (Windows
172.68.245.36	TP/1.1	502	166	United States	http://www.usatoday.com/search/results?q=...	Mozilla/5.0 (Windows
172.68.245.36	HTTP/1.1	502	568	United States	http://www.google.com/?q=VXDELRPWW	Mozilla/4.0 (compatib
172.68.245.36	U HTTP/1.1	502	568	United States	http://engadget.search.aol.com/search?q=V...	Mozilla/5.0 (Windows
172.68.245.36	MHVHHD HTTP/1.1	502	166	United States	http://www.google.com/?q=SMIQLJLTP	Mozilla/5.0 (Windows
172.68.245.36	GBYHKL HTTP/1.1	502	568	United States	http://www.google.com/?q=NCMFEH	Mozilla/4.0 (compatib
172.68.245.36	QEDNGVM HTTP/1.1	502	568	United States	http://www.usatoday.com/search/results?q=...	Mozilla/4.0 (compatib
172.68.245.36	TGY HTTP/1.1	502	568	United States	http://www.usatoday.com/search/results?q=...	Mozilla/4.0 (compatib
172.68.245.36	FDA HTTP/1.1	502	568	United States	http://www.usatoday.com/search/results?q=...	Mozilla/4.0 (compatib
172.68.245.36	HTTP/1.1	502	166	United States	http://engadget.search.aol.com/search?q=K...	Opera/9.80 (Windows
172.68.245.36	HTTP/1.1	502	166	United States	http://engadget.search.aol.com/search?q=O...	Mozilla/5.0 (Windows
172.68.245.36	VGFCRDVJ HTTP/1.1	502	166	United States	http://www.mertsarica.com/WGLEL	Opera/9.80 (Windows
172.68.245.36	PZW HTTP/1.1	502	166	United States	http://www.usatoday.com/search/results?q=...	Opera/9.80 (Windows
172.68.245.36	MF HTTP/1.1	502	166	United States	http://www.usatoday.com/search/results?q=...	Mozilla/5.0 (Windows
172.68.245.36	TP/1.1	502	568	United States	http://www.google.com/?q=AUOZCAI	Mozilla/4.0 (compatib
172.68.245.36	HTTP/1.1	502	568	United States	http://www.usatoday.com/search/results?q=...	Mozilla/4.0 (compatib
172.68.245.36	HTTP/1.1	502	568	United States	http://www.mertsarica.com/JAZSW	Mozilla/4.0 (compatib
172.68.245.36	CVWJ HTTP/1.1	502	568	United States	http://engadget.search.aol.com/search?q=D...	Mozilla/4.0 (compatib
172.68.245.36	HTTP/1.1	502	568	United States	http://www.google.com/?q=UQWPTAE	Mozilla/4.0 (compatib
172.68.245.36	DHGZ HTTP/1.1	502	568	United States	http://www.mertsarica.com/YLUZSMOJGA	Mozilla/4.0 (compatib
172.68.245.36	PBSR HTTP/1.1	502	166	United States	http://www.mertsarica.com/NQSKC	Opera/9.80 (Windows
172.68.245.36	SVDBUPTZZV HTTP/1.1	502	568	United States	http://www.usatoday.com/search/results?q=...	Mozilla/5.0 (Windows
172.68.245.36	V HTTP/1.1	502	568	United States	http://www.google.com/?q=SLLDDBC	Mozilla/4.0 (compatib
172.68.245.36	AWIS HTTP/1.1	502	166	United States	http://www.mertsarica.com/DXWQVPBZ	Mozilla/5.0 (Windows
172.68.245.36	JNVXPV HTTP/1.1	502	568	United States	http://engadget.search.aol.com/search?q=V...	Mozilla/5.0 (Windows
172.68.245.36	C HTTP/1.1	502	166	United States	http://www.usatoday.com/search/results?q=...	Mozilla/5.0 (Windows
172.68.245.36	ZY HTTP/1.1	502	568	United States	http://www.usatoday.com/search/results?q=...	Mozilla/5.0 (Windows
172.68.245.36	RFJCA HTTP/1.1	502	166	United States	http://www.mertsarica.com/SLGHZS	Opera/9.80 (Windows
172.68.245.36	15.07.2018 09:32:05 POST /?UII=OVQLCGAIQ HTTP/1.1	502	568	United States	http://www.usatoday.com/search/results?q=...	Mozilla/4.0 (compatib

Update Completed 18:05:17 [0/40132] [No Filter] [Unlock](#) iannet



DoS saldırısı ile ilgili olarak, erişim kayıtları (access.log) üzerinden elde ettiğim bilgilere istinaden yapmış olduğum araştırmalar sonucunda birbirine benzeyen 3 farklı Python aracı (hulk.py , doser.py , attack.py) dikkatimi çekti. Bu araçların kaynak kodları ile bloguma yapılan DoS saldırısını karşılaştırdığımda, gelen isteklerin POST isteği olması sebebiyle doser.py aracı ile bu saldırının gerçekleştirildiği fikri ağır basmış oldu.



```
ddos/attack.py at master · firebug/ddos · GitHub
Secure | https://github.com/firebug/ddos/blob/master/attack.py
Hack 4 Career: Info LinkedIn Mert SARICA (mertsarica) Inbox - mertsarica@

25 def useragent_list():
26     global headers_useragents
27     headers_useragents = []
28     headers_useragents.append("Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.1.3) Gecko/20090913 Firefox/3.5.3")
29     headers_useragents.append("Mozilla/5.0 (Windows; U; Windows NT 6.1; en; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3 (.NET CLR 3.5.3072)
30     headers_useragents.append("Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3 (.NET CLR 3.5.3072)
31     headers_useragents.append("Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.1) Gecko/20090718 Firefox/3.5.1")
32     headers_useragents.append("Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; AppleWebKit/532.1 (KHTML, like Gecko) Chrome/4.0.219.6 S
33     headers_useragents.append("Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; InfoP
34     headers_useragents.append("Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Win64; x64; Trident/4.0)")
35     headers_useragents.append("Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; SV1; .NET CLR 2.0.50727; InfoPath.2)");
36     headers_useragents.append("Mozilla/5.0 (Windows; U; MSIE 7.0; Windows NT 6.0; en-US)");
37     headers_useragents.append("Mozilla/4.0 (compatible; MSIE 6.1; Windows XP)");
38     headers_useragents.append("Opera/9.80 (Windows NT 5.2; U; ru) Presto/2.5.22 Version/10.51")
39     return(headers_useragents)
40
41 # generates a referer array
42 def referer_list():
43     global headers_referers
44     headers_referers = []
45     headers_referers.append("http://www.usatoday.com/search/results?q=")
46     headers_referers.append("http://engadget.search.aol.com/search?q=")
47     headers_referers.append("http:// + host + '/'")
48     return(headers_referers)
49
50 def handler(signum, _):
51     if signum == signal.SIGALRM:
52         print "Time is up !"
53         print "Attack finished !"
54         sys.exit()
55
56 #builds random ascii string
57 def buildblock(size):
58     out_str = ""
59     for i in range(0, size):
60         a = random.randint(65, 90)
61         out_str += chr(a)
62     return(out_str)
63
64 def send_packet(host, param_joiner):
65     request = urllib2.Request(url = param_joiner + buildblock(random.randint(3,10)) + "+" + buildblock(random.randint(3,10)))
66     request.add_header("User-Agent", random.choice(headers_useragents))
67     request.add_header("Cache-Control", "no-cache")
68     request.add_header("Accept-Charset", "ISO-8859-1,utf-8;q=0.7;q=0.7")
69     request.add_header("Referer", random.choice(headers_referers) + buildblock(random.randint(5,10)))
70     request.add_header("Keep-Alive", random.randint(10,120))
71     request.add_header("Connection", "keep-alive")
72     request.add_header("Host", host)
```

```
doserpy/doser.py at master · Quitten/doser.py · GitHub
Secure | https://github.com/Quitten/doser.py/blob/master/doser.py
Hack 4 Career: Info LinkedIn Mert SARICA (mertsarica) Inbox - mertsarica@

90     pass
91
92 class SendPOSTThread(threading.Thread):
93     def run(self):
94         try:
95             while True:
96                 global url, payload
97                 sendPOST(url, payload)
98         except:
99             pass
100
101 # TODO:
102 # check if the site stop responding and alert
103
104 def main(argv):
105     parser = argparse.ArgumentParser(description="Sending unlimited amount of requests in order to perform DoS attacks. Written by Bara
106     parser.add_argument('-g', help="Specify GET request. Usage: -g '<url>'")
107     parser.add_argument('-p', help="Specify POST request. Usage: -p '<url>'")
108     parser.add_argument('-d', help="Specify data payload for POST request", default=None)
109     parser.add_argument('-ah', help="Specify additional header/s. Usage: -ah '<Content-type: application/json' '\<User-Agent: Doser>'")
110     parser.add_argument('-t', help="Specify number of threads to be used", default=500, type=int)
111     args = parser.parse_args()
112
113     global url, payload, additionalHeaders
114     additionalHeaders = args.ah
115     payload = args.d
116
117     if args.g:
118         url = args.g
119         for i in range(args.t):
120             t = SendGETThread()
121             t.start()
122
123     if args.p:
124         url = args.p
125         for i in range(args.t):
126             t = SendPOSTThread()
127             t.start()
128
129     if len(sys.argv)==1:
130         parser.print_help()
131         exit()
132
133 if __name__ == "__main__":
134     main(sys.argv[1:])
```

```
hulk/hulk.py at master · grafov/hulk/blob/master/hulk.py
Secure | https://github.com/grafov/hulk/blob/master/hulk.py
Hack 4 Career: Info | LinkedIn | Mert SARICA (mert) | Inbox - mertsarica@

33 def set_safe():
34     global safe
35     safe=1
36
37 # generates a user agent array
38 def useragent_list():
39     global headers_useragents
40     headers_useragents.append("Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.1.3) Gecko/20090913 Firefox/3.5.3")
41     headers_useragents.append("Mozilla/5.0 (Windows; U; Windows NT 6.1; en; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3 (.NET CLR 3.5.3072)
42     headers_useragents.append("Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3 (.NET CLR 3.5.3072)
43     headers_useragents.append("Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.1) Gecko/20090718 Firefox/3.5.1")
44     headers_useragents.append("Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; AppleWebKit/532.1 (KHTML, like Gecko) Chrome/4.0.219.6 S
45     headers_useragents.append("Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; InfoPa
46     headers_useragents.append("Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; Trident/4.0; SLCC1; .NET CLR 2.0.50727; .NET CLR 1.1.
47     headers_useragents.append("Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Win64; x64; Trident/4.0)")
48     headers_useragents.append("Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; SV1; .NET CLR 2.0.50727; InfoPath.2)")
49     headers_useragents.append("Mozilla/5.0 (Windows; U; MSIE 7.0; Windows NT 6.0; en-US)")
50     headers_useragents.append("Mozilla/4.0 (compatible; MSIE 6.1; Windows XP)")
51     headers_useragents.append("Opera/9.80 (Windows NT 5.2; U; ru) Presto/2.5.22 Version/10.51")
52     return(headers_useragents)
53
54 # generates a referer array
55 def referer_list():
56     global headers_referers
57     headers_referers.append("http://www.google.com/?q=")
58     headers_referers.append("http://www.usatoday.com/search/results?q=")
59     headers_referers.append("http://engadget.search.aol.com/search?q=")
60     headers_referers.append("http://* + host = /*")
61     return(headers_referers)
62
63 #builds random ascii string
64 def buildblock(size):
65     out_str = ""
66     for i in range(0, size):
67         a = random.randint(65, 90)
68         out_str += chr(a)
69     return(out_str)
70
71 def usage():
72     print '-----'
73     print 'USAGE: python hulk.py curl'
74     print 'you can add "safe" after url, to autoshtut after dos'
75     print '-----'
76
77
78 #http request
79 def httpcall(url):
80     .....
```

Blogumun WordPress yönetici paneline de göz gezdirdiğimde, Aranılan Terimler kısmındaki i\_love\_brother\_This\_is\_not\_an\_attack\_This\_is\_a\_test arama terimi dikkatimi çekti. Bu terim ile ilgili göndermiş olduğum bir tweete yapılan yorumda da olduğu gibi, blogumun DDoS testlerinde akla ilk gelen blog olabileceğini de dikkate alarak Cloudflare'in yönetim paneli üzerinden Rusya ip adreslerini engelledim.



**Mert SARICA** @MertSARICA · 17 Tem

Sevginin de böylesi işte :)

Dimensi ▾ eşit ▾  Uygula

18-06-18 – 17-07-18 ▾

### Aranılan Terimler

- Hacker avı
- x
- i\_love\_brother\_This\_is\_not\_an\_attack\_This\_is\_a\_test
- linux
- hack



1



13



**musa şana**

@musa\_sana

Takip et

@MertSARICA adlı kullanıcıya yanıt olarak

ddos testlerinde akla ilk gelen blog :)

22:08 - 17 Tem 2018

3 Beğeni



17 Temmuz tarihinde yapılan kısa süreli benzer bir saldırıda bu defa kaynak IP adreslerini görebildiğim için DoS saldırısının Fransa'da bulunan bir ip adresinden (51.254.122.14) gerçekleştirildiğini gördüm ve bu sefer de Fransa ip adreslerini Cloudflare'in yönetim paneli üzerinden engelledim.

```
root@batcave:/var/log/nginx# grep "POST /?" access.log.1 | cut -d " " -f 1 | sort | uniq -i
```

```
51.254.122.14
```

```
root@batcave:/var/log/nginx#
```

IP Whois Kaydı (51.254.122.14)

```
-----
Lookup results for 51.254.122.14 from whois.ripe.net server:
inetnum:          51.254.0.0 - 51.255.255.255
descr:            FR-OVH-20150522
country:          FR
admin-c:          OTC2-RIPE
tech-c:           OTC2-RIPE
status:           LEGACY
mnt-by:           OVH-NIT
created:          2015-05-26T08:55:56Z
last-modified:    2015-05-27T15:52:47Z
source:           RIPE
org:              ORG-053-RIPE
organisation:     ORG-053-RIPE
org-name:         OVH SAS
org-type:         LIR
address:          2 rue Kellermann
address:          59100
address:          Roubaix
address:          FRANCE
phone:            +33972101007
abuse-c:          AR15333-RIPE
admin-c:          OTC2-RIPE
admin-c:          OK217-RIPE
admin-c:          GH84-RIPE
mnt-ref:          OVH-NIT
mnt-ref:          RIPE-NCC-HU-NIT
mnt-by:           RIPE-NCC-HU-NIT
mnt-by:           OVH-NIT
created:          2004-04-17T11:23:17Z
last-modified:    2017-10-30T14:48:06Z
source:           RIPE # Filtered
role:             OVH Technical Contact
address:          OVH SAS
address:          2 rue Kellermann
address:          59100 Roubaix
address:          France
admin-c:          OK217-RIPE
tech-c:           GH84-RIPE
tech-c:           SL18162-RIPE
nic-hdl:          OTC2-RIPE
abuse-mailbox:    abuse@ovh.net
mnt-by:           OVH-NIT
created:          2004-01-28T17:42:20Z
last-modified:    2014-09-05T10:47:15Z
source:           RIPE # Filtered
route:            51.254.0.0/15
descr:            OVH
origin:           AS16276
mnt-by:           OVH-NIT
created:          2015-05-28T17:50:05Z
last-modified:    2015-05-28T17:50:05Z
source:           RIPE
-----
```

## Access Rules

Firewall rules can be based on IP address, IP address range, Autonomous System Number (ASN) or country.

Value	Applies to	Action
France (FR) HTTP Flood Sebebiyle	This website	<input type="button" value="Block"/> <input type="button" value="Edit"/> <input type="button" value="X"/>
51.254.122.14 HTTP Flood	This website	<input type="button" value="Block"/> <input type="button" value="Edit"/> <input type="button" value="X"/>
Russian Federation (RU) HTTP Flood Sebebiyle	This website	<input type="button" value="Block"/> <input type="button" value="Edit"/> <input type="button" value="X"/>

23 Temmuz tarihinde yapılan yeni bir DoS saldırısında bu defa blogumun arama sayfasına çok sayıda i\_love\_you\_brother arama terimi gönderildiğini gördüm. Bu defa kaynak IP adresini (31.223.24.59) görebildiğim için IP adresinin kayıt bilgilerine baktığımda bu defa saldırının Türkiye'den yapıldığını gördüm.

```
root@batcave: /var/log/nginx# grep 1_love_you access.log | head -n 10
31.223.24.59 - - [23/Jul/2018:20:04:32 +0300] "GET /?s=1_love_you_brother HTTP/1.1" 200 14217 "-" "Mozilla/5.0 (windows NT 6.1) AppleWebKit/537.2 (KHTML, like Gecko) Chrome/22.0.1216.0 Safari/537.2"
31.223.24.59 - - [23/Jul/2018:20:04:32 +0300] "GET /?s=1_love_you_brother HTTP/1.1" 200 14217 "-" "Mozilla/5.0 (windows NT 6.2) AppleWebKit/537.11 (KHTML, like Gecko) Chrome/23.0.1271.26 Safari/537.11"
31.223.24.59 - - [23/Jul/2018:20:04:32 +0300] "GET /?s=1_love_you_brother HTTP/1.1" 200 14218 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_6_8) AppleWebKit/535.19 (KHTML, like Gecko) Chrome/18.0.1025.11 Safari/535.19"
31.223.24.59 - - [23/Jul/2018:20:04:33 +0300] "GET /?s=1_love_you_brother HTTP/1.1" 200 14216 "-" "Mozilla/5.0 (windows NT 6.0; WOW64) AppleWebKit/535.19 (KHTML, like Gecko) Chrome/18.0.1025.45 Safari/535.19"
31.223.24.59 - - [23/Jul/2018:20:04:34 +0300] "GET /?s=1_love_you_brother HTTP/1.1" 200 14217 "-" "Mozilla/5.0 (windows NT 6.2; WOW64) AppleWebKit/537.1 (KHTML, like Gecko) Chrome/19.77.34.5 Safari/537.1"
31.223.24.59 - - [23/Jul/2018:20:04:34 +0300] "GET /?s=1_love_you_brother HTTP/1.1" 200 14218 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_2) AppleWebKit/537.11 (KHTML, like Gecko) Chrome/23.0.1271.6 Safari/537.11"
31.223.24.59 - - [23/Jul/2018:20:04:35 +0300] "GET /?s=1_love_you_brother HTTP/1.1" 200 14216 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_2) AppleWebKit/535.24 (KHTML, like Gecko) Chrome/19.0.1055.1 Safari/535.24"
31.223.24.59 - - [23/Jul/2018:20:04:35 +0300] "GET /?s=1_love_you_brother HTTP/1.1" 200 14217 "-" "Mozilla/5.0 (windows NT 6.2) AppleWebKit/536.3 (KHTML, like Gecko) Chrome/19.0.1061.1 Safari/536.3"
31.223.24.59 - - [23/Jul/2018:20:04:35 +0300] "GET /?s=1_love_you_brother HTTP/1.1" 200 14218 "-" "Mozilla/5.0 (windows NT 6.1; WOW64) AppleWebKit/537.1 (KHTML, like Gecko) Chrome/22.0.1207.1 Safari/537.1"
31.223.24.59 - - [23/Jul/2018:20:04:35 +0300] "GET /?s=1_love_you_brother HTTP/1.1" 200 14217 "-" "Mozilla/5.0 (windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/35.0.2309.372 Safari/537.36"
root@batcave: /var/log/nginx#
```

The screenshot shows the WHOIS IP Lookup Tool interface. The search bar contains the IP address 31.223.24.59. The results are displayed in a structured format, including the following information:

- Source:** whois.ripe.net
- IP Address:** 31.223.24.59
- RIPE Database query service:** The objects are in RPSL format.
- Abuse contact:** '31.223.24.0 - 31.223.24.255' is 'li@turknet.net.tr'
- inetnum:** 31.223.24.0 - 31.223.24.255
- netname:** AnkaraPOP\_XdsIDynamic
- descr:** TurkNet-SG
- country:** TR
- admin-c:** TL143-RIPE
- tech-c:** TL143-RIPE
- status:** ASSIGNED PA
- mnt-by:** NNT-TURKNET-WNT
- created:** 2011-07-26T13:53:03Z
- last-modified:** 2011-07-26T13:53:03Z
- source:** RIPE
- person:** TurkNet LIR
- address:** TurkNet Iletisim Hizmetleri A.S.
- address:** Buyukdere Cad. Ercan Han No.121
- address:** Gayrettepe / Istanbul / Turkey
- phone:** +90 212 355 17 00
- nic-hdl:** TL143-RIPE
- created:** 2009-03-09T10:03:41Z
- last-modified:** 2011-08-24T12:18:33Z
- source:** RIPE
- mnt-by:** NNT-TURKNET-WNT
- Information related to '31.223.0.0/17AS12735':**
- route:** 31.223.0.0/17
- descr:** TurkNet Iletisim Hizmetleri A.S
- origin:** AS12735
- mnt-by:** NNT-TURKNET-WNT
- created:** 2011-05-16T14:17:07Z
- last-modified:** 2011-05-16T14:17:07Z
- source:** RIPE

The query was served by the RIPE Database Query Service version 1.91.2 (WAGWU).

Bana olan sevgisini sele dönüştürme konusunda ısrarcı olan bu Rus kardeşim ile sistematik olarak mücadele edebilmek ve benzer durumlarla mücadele etmek durumunda kalanlara yol gösterme adına çeşitli araçlardan faydalanmaya karar verdim.

İlk olarak gerçekleştirilen genel DoS saldırılarından hızlıca haberdar olabilmek için OSSEC HIDS yazılımını işletim sistemine kurdum. Buna ilaveten bu saldırıyı tespit edebilmek için de özel olarak bir kural hazırlayıp bu kuralı /var/ossec/rules/http\_dos\_rules.xml adı altında kaydettikten sonra kuralı içeren dosyayı da /var/ossec/etc/ossec.conf dosyasına kaydettim. ossec-logtest aracı ile de kuralın düzgün çalıştığını kontrol ettikten sonra OSSEC'i yeniden başlatıp attack.py ile bloguma ufak bir DoS saldırısı gerçekleştirdim. Saldırı sonucunda OSSEC başarıyla bu saldırıyı tespit edip beni e-posta ile hemen uyardı.

```

<include>cmsserver_rules.xml</include>
<include>vpopmail_rules.xml</include>
<include>vmpp3d_rules.xml</include>
<include>courier_rules.xml</include>
<include>web_rules.xml</include>
<include>web_appsec_rules.xml</include>
<include>apache_rules.xml</include>
<include>nginx_rules.xml</include>
<include>php_rules.xml</include>
<include>mysql_rules.xml</include>
<include>postgresql_rules.xml</include>
<include>ids_rules.xml</include>
<include> squid_rules.xml</include>
<include>firewall_rules.xml</include>
<include>apparmor_rules.xml</include>
<include>cisco-ios_rules.xml</include>
<include>netscreenfw_rules.xml</include>
<include>sonicwall_rules.xml</include>
<include>postfix_rules.xml</include>
<include>sendmail_rules.xml</include>
<include>imap_rules.xml</include>
<include>mailscanner_rules.xml</include>
<include>dovecot_rules.xml</include>
<include>ms-exchange_rules.xml</include>
<include>racon_rules.xml</include>
<include>vpn_concentrator_rules.xml</include>
<include>spanid_rules.xml</include>
<include>msauth_rules.xml</include>
<include>mcafee_av_rules.xml</include>
<include>trend-osec_rules.xml</include>
<include>ms-se_rules.xml</include>
<!-- <include>policy_rules.xml</include> -->
<include>zeus_rules.xml</include>
<include>solaris_bsm_rules.xml</include>
<include>vmware_rules.xml</include>
<include>ms_dhcp_rules.xml</include>
<include>asterisk_rules.xml</include>
<include>ossec_rules.xml</include>
<include>attack_rules.xml</include>
<include>dropbear_rules.xml</include>
<include>unbound_rules.xml</include>
<include>sysmon_rules.xml</include>
<include>opensmtpd_rules.xml</include>
<include>exit_rules.xml</include>
<include>openbsd-dhcpd_rules.xml</include>
<include>local_rules.xml</include>
</rules>

```

```

<syscheck>
<!-- Frequency that syscheck is executed -- default every 20 hours -->
<frequency>7200</frequency>
<!-- Directories to check (perform all possible verifications) -->
<directories check_all="yes"> /etc,/usr/bin,/usr/sbin</directories>
<directories check_all="yes"> /bin,/sbin,/boot</directories>
<!-- Files/directories to ignore -->
<ignore> /etc/mtab</ignore>
<ignore> /etc/hosts.deny</ignore>
<ignore> /etc/mail/statistics</ignore>
<ignore> /etc/random-seed</ignore>
<ignore> /etc/random-seed</ignore>
<ignore> /etc/adjtime</ignore>

```

Get Help Exit Write Out Read File Where Is Replace Cut Text Uncut Text Justify To Spell Cur Pos Go To Line Read 23 Lines Prev Page Next Page First Line Last Line Where Is Next To Bracket Mark Text Copy Text Indent Text Unindent Text Undo Redo

GNU nano 2.5.3

File: http\_dos\_rules.xml

```

<!-- @(#) $Id: ./var/ossec/rules/http_dos_rules.xml, 2018/07/23 Mert SARICA Exp $

```

```

- HTTP DoS attacks/vulns specific rules for OSSEC.
- Copyright (C) 2012 Daniel B. Cid (dcid@dcid.me)
- All rights reserved.
- This program is a free software; you can redistribute it
- and/or modify it under the terms of the GNU General Public
- License (version 2) as published by the FSF - Free Software
- Foundation.
- License details: http://www.ossec.net/en/licensing.html
-->

```

```

<!-- Collection of rules for common web attacks that we are seeing in the wild.
- The real goal is to stop bots and automated attacks from doing further damage
- on sites that are not updated.
-->

```

```

<group name="web,appsec,attack">

```

```

<!-- Checking POST & GET HTTP DoS Attack
-->

```

```

<rule id="41501" level="1">
<if_sid>31100</if_sid>
<match>GET |POST </match>
<regex>/?\D+=\D+HTTP/1.1</regex>
<description>Probably a non-malicious site search</description>
</rule>

```

```

<!-- If we see frequent /?VXVFII=FXSF HTTP/1.1 then it is probably a HTTP DoS. -->

```

```

<rule id="41502" level="9" frequency="10" timeframe="20">
<if_matched_sid>41501</if_matched_sid>
<same_source_ip />
<description>Probably a HTTP DoS Attack (doser.py, attack.py or hulk.py)</description>
</rule>

```

```

<!-- Checking GET HTTP DoS Attack
-->

```

```

<rule id="41503" level="9">
<if_sid>31100</if_sid>
<match>GET /?s=i_love_you_brother</match>
<description>HTTP DoS Attack (i_love_you_brother)</description>
</rule>
-->

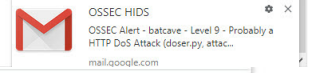
```

```

</group>

```

```
root@ubuntu:~/dos# python attack.py http://www.mertsarica.com/
Debug : thread=5 time=30 http://www.mertsarica.com/
Time is up !
Attack Finished !
root@ubuntu:~/dos#
```



## OSSEC Alert - batcave - Level 9 - Probably a HTTP DoS Attack (doser.py, attack.py or hulk.py) Inbox x



**OSSEC HIDS** <mert.sarica@gmail.com>  
to me

11:20 PM (0 minutes ago) ☆ ↶ ⋮



### Be careful with this message

Gmail could not verify that it actually came from mert.sarica@gmail.com. Avoid clicking links, downloading attachments, or replying with personal information.

Report As Spam

Report As Phishing



OSSEC HIDS Notification.  
2018 Jul 23 23:20:18

Received From: batcave->/var/log/nginx/access.log  
Rule: 41502 fired (level 9) -> "Probably a HTTP DoS Attack (doser.py, attack.py or hulk.py)"  
Src IP: [REDACTED]  
Portion of the log(s):

```
-- [23/Jul/2018:23:20:17 +0300] "GET /?FLEDNO=IQOKGUIYA HTTP/1.1" 200 19955 "http://www.usatoday.com/search/results?q=MDPNECW" "Mozilla/5.0 (Windows; U; Windows NT 6.1; en; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3 (.NET CLR 3.5.30729)"
-- [23/Jul/2018:23:20:15 +0300] "GET /?ECO=NYNGERU HTTP/1.1" 200 19952 "http://engadget.search.aol.com/search?q=JHYFFX" "Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.1) Gecko/20090718 Firefox/3.5.1"
-- [23/Jul/2018:23:20:15 +0300] "GET /?ECO=NYNGERU HTTP/1.1" 200 19957 "http://engadget.search.aol.com/search?q=JHYFFX" "Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.1) Gecko/20090718 Firefox/3.5.1"
-- [23/Jul/2018:23:20:15 +0300] "GET /?ECO=NYNGERU HTTP/1.1" 200 19957 "http://engadget.search.aol.com/search?q=JHYFFX" "Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.1) Gecko/20090718 Firefox/3.5.1"
-- [23/Jul/2018:23:20:15 +0300] "GET /?NBQRRYKCS=WSHMMVEU HTTP/1.1" 200 19955 "http://engadget.search.aol.com/search?q=VHJAOOBNE" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Win64; x64; Trident/4.0)"
-- [23/Jul/2018:23:20:15 +0300] "GET /?NBQRRYKCS=WSHMMVEU HTTP/1.1" 200 19956 "http://engadget.search.aol.com/search?q=VHJAOOBNE" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Win64; x64; Trident/4.0)"
-- [23/Jul/2018:23:20:13 +0300] "GET /?ECO=NYNGERU HTTP/1.1" 200 19955 "http://engadget.search.aol.com/search?q=JHYFFX" "Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.1) Gecko/20090718 Firefox/3.5.1"
-- [23/Jul/2018:23:20:13 +0300] "GET /?GRFB=INLOWJKU HTTP/1.1" 200 19956 "http://www.mertsarica.com/HWEARASA" "Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.1) Gecko/20090718 Firefox/3.5.1"
-- [23/Jul/2018:23:20:13 +0300] "GET /?NBQRRYKCS=WSHMMVEU HTTP/1.1" 200 19954 "http://engadget.search.aol.com/search?q=VHJAOOBNE" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Win64; x64; Trident/4.0)"
-- [23/Jul/2018:23:20:13 +0300] "GET /?NBQRRYKCS=WSHMMVEU HTTP/1.1" 200 19957 "http://engadget.search.aol.com/search?q=VHJAOOBNE" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Win64; x64; Trident/4.0)"
-- [23/Jul/2018:23:20:13 +0300] "GET /?NBQRRYKCS=WSHMMVEU HTTP/1.1" 200 19957 "http://engadget.search.aol.com/search?q=VHJAOOBNE" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Win64; x64; Trident/4.0)"
-- [23/Jul/2018:23:20:11 +0300] "GET /?GRFB=INLOWJKU HTTP/1.1" 200 19956 "http://www.mertsarica.com/HWEARASA" "Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.1) Gecko/20090718 Firefox/3.5.1"
```

OSSEC HIDS ile benim sevgi dolu Rus kardeşimin DoS saldırısını tespit etmek yeterli olmayacağı için fail2ban aracı ile bu iki tür DoS saldırısını tespit eden özel bir kural yazıp, bu yazıda da belirtildiği şekilde Cloudflare

API'si üzerinden saldırganın ip adresini yasaklayan betikten faydalandım. Hazırladığım kuralı kontrol etmek için fail2ban-regex aracından faydalandıktan sonra attack.py ile bloguma saldırarak Cloudflare tarafından ip adresimin başarıyla yasaklandığını gördüm ve Rus kardeşimin yeni saldırıları için kedi fare oyunundaki yerimi sağladım. :)

```
GNU nano 2.5.3 File: /etc/fail2ban/filter.d/nginx-dos.conf
[Definition]
# Probably a HTTP Dos Attack (doser.py, attack.py or hulk.py)
failregex = ^<HOST> \- .* \("(POST|GET).*(/[A-Z]+=[A-Z]+ HTTP/1.1)\".* .+$

# HTTP Dos Attack (i_love_you_brother)
# ^<HOST> \- .* \("(POST|GET).*(/?s=i_love_you_brother HTTP/1.1)\".* .+$

# HTTP Dos Attack (this_is_another_test)
# ^<HOST> \- .* \("(POST|GET).*(/?s=).*(_).*(_).*(_).* (HTTP/1.1)\".* .+$

# HTTP Dos Attack (x_y_z)
# ^<HOST> \- .* \("(POST|GET).*(/?s=).*(_).*(_).* (HTTP/1.1)\".* .+$

# HTTP Dos Attack (python-requests)
# ^<HOST> \- .* (\python-requests/.)*\".* .+$

ignoreregex =

root@batcave:/var/log/nginx# fail2ban-regex /var/log/nginx/access.log /etc/fail2ban/filter.d/nginx-dos.conf

Running tests
=====
Use failregex filter file : nginx-dos, basedir: /etc/fail2ban
Use log file : /var/log/nginx/access.log
Use encoding : UTF-8

Results
=====
Failregex: 6317 total
|- #) [# of hits] regular expression
| 1) [2006] ^<HOST> \- .* \("(POST|GET).*(/[A-Z]+=[A-Z]+ HTTP/1.1)\".* .+$
| 2) [4311] ^<HOST> \- .* \("(POST|GET).*(/?s=).*(_).*(_).* (HTTP/1.1)\".* .+$
|_

Ignoreregex: 0 total

Date template hits:
|- [# of hits] date format
| [25807] Day(?P<_sep>[-/])MON(?P=_sep)Year [ :]?24hour:Minute:Second(?:\.Microseconds)?(?: Zone offset)?
|_

Lines: 25807 lines, 0 ignored, 6317 matched, 19490 missed [processed in 3.11 sec]
Missed line(s): too many to print. use --print-all-missed to print all 19490 lines
root@batcave:/var/log/nginx#

root@batcave:~# service fail2ban restart
root@batcave:~# tail -f /var/log/fail2ban.log
2018-07-26 21:44:57,925 fail2ban.jail [12335]: INFO Jail 'nginx-dos' uses pyinotify
2018-07-26 21:44:57,925 fail2ban.filter [12335]: INFO Set jail log file encoding to UTF-8
2018-07-26 21:44:57,929 fail2ban.jail [12335]: INFO Initiated 'pyinotify' backend
2018-07-26 21:44:57,931 fail2ban.filter [12335]: INFO Set maxRetry = 3
2018-07-26 21:44:57,932 fail2ban.filter [12335]: INFO Added logfile = /var/log/nginx/access.log
2018-07-26 21:44:57,934 fail2ban.filter [12335]: INFO Set findtime = 60
2018-07-26 21:44:57,935 fail2ban.actions [12335]: INFO Set banTime = 6000
2018-07-26 21:44:57,935 fail2ban.filter [12335]: INFO Set jail log file encoding to UTF-8
2018-07-26 21:44:57,939 fail2ban.jail [12335]: INFO Jail 'sshd' started
2018-07-26 21:44:57,944 fail2ban.jail [12335]: INFO Jail 'nginx-dos' started
2018-07-26 21:45:24,929 fail2ban.filter [12335]: INFO [nginx-dos] Found
2018-07-26 21:45:24,932 fail2ban.filter [12335]: INFO [nginx-dos] Found
2018-07-26 21:45:24,996 fail2ban.filter [12335]: INFO [nginx-dos] Found
2018-07-26 21:45:25,263 fail2ban.filter [12335]: INFO [nginx-dos] Found
2018-07-26 21:45:25,489 fail2ban.filter [12335]: INFO [nginx-dos] Found
```



# Error 1006

Ray ID: 4408f2cf9f909c3b • 2018-07-26 18:32:21 UTC

Access denied

## What happened?

The owner of this website (www.mertsarica.com) has banned your IP address ( ).

Cloudflare Ray ID: 4408f2cf9f909c3b • Your IP: • Performance & security by Cloudflare

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.