DoS ile Mücadele

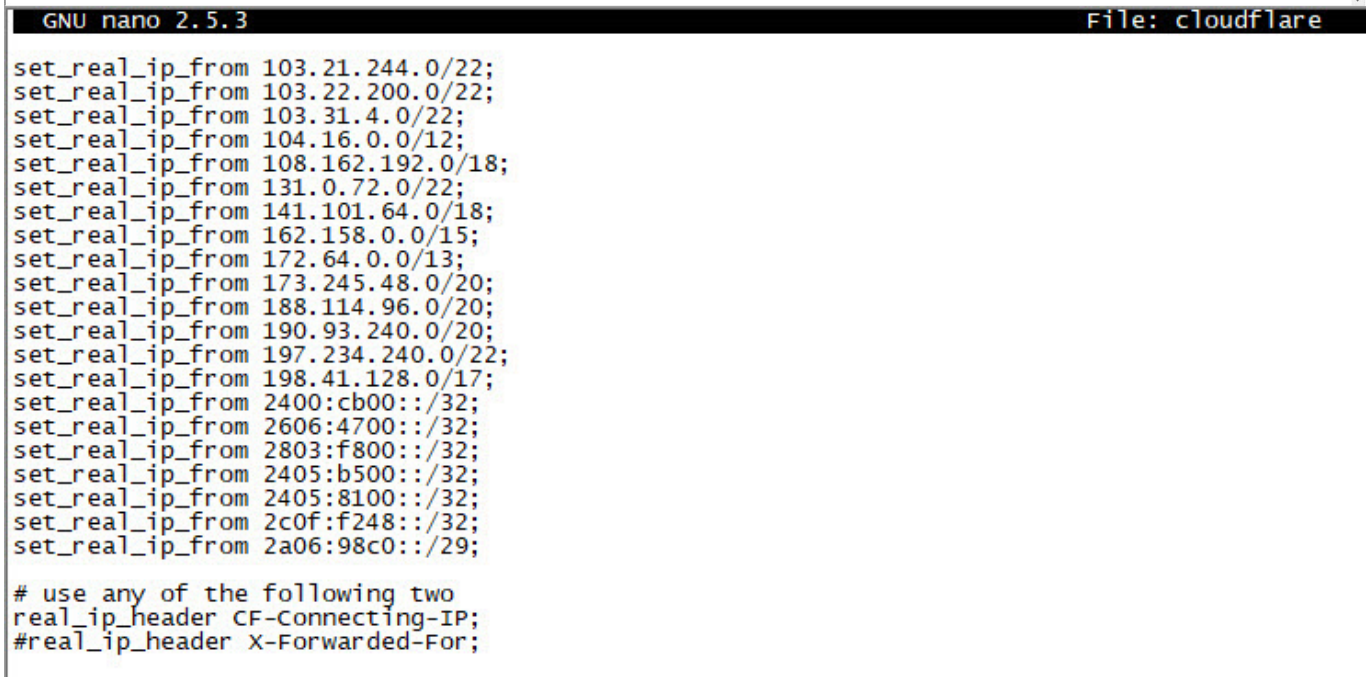
written by Mert SARICA | 1 March 2019

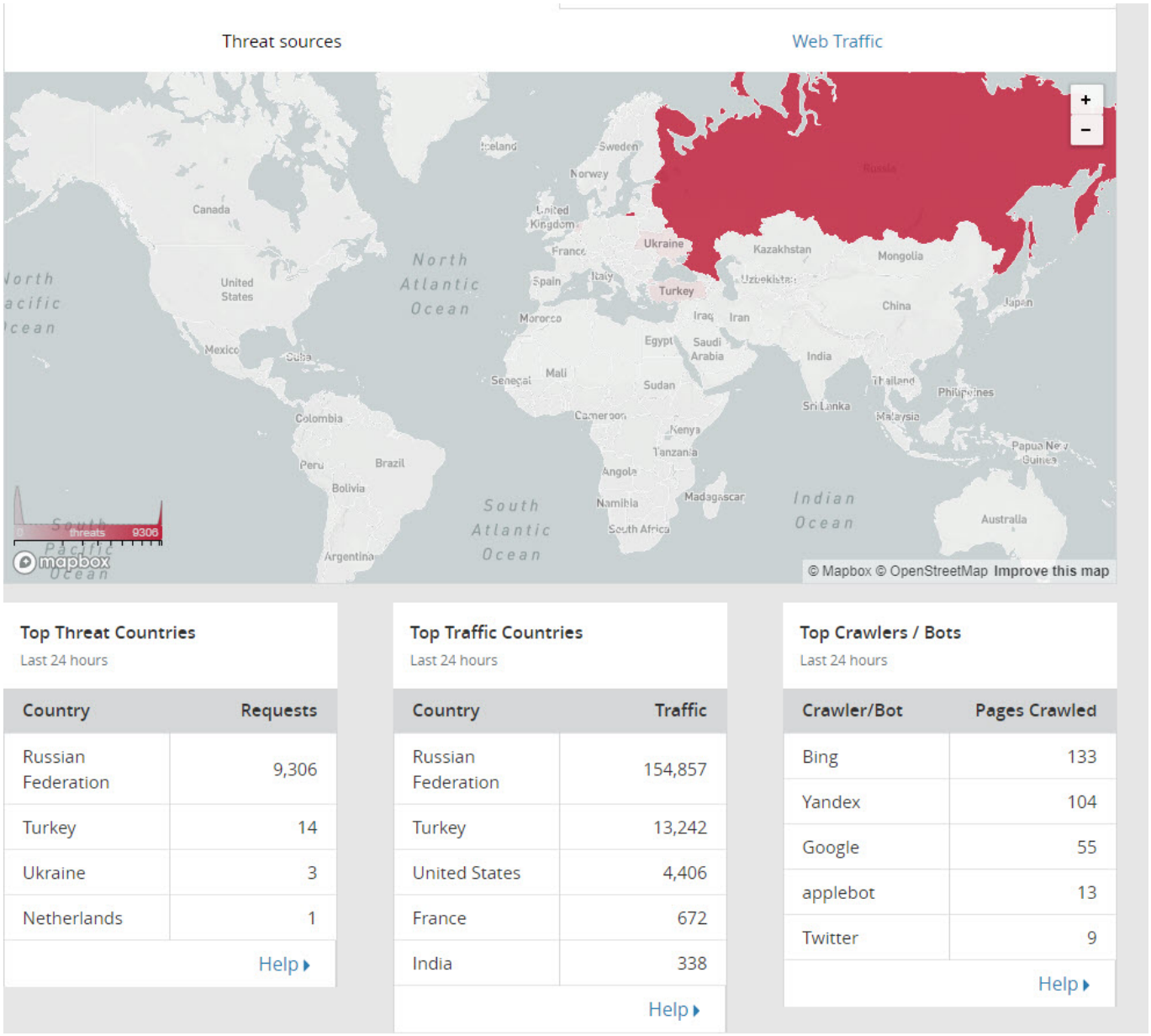
2009 yılından bu yana “Bilgi güçtür ve paylaşıldıkça artar!” sloganıyla siber güvenlik alanına meraklılar için özveriyle yaşatmaya çalıştığım blogumun bundan yıllar yıllar önce bir DDoS saldırısı ile karşı karşıya kaldığını ve daha sonrasında blogumu Cloudflare arkasına taşıdığımı anımsıyorum. Son birkaç yıldır ise DDoS ve DoS benzeri bir saldırı ile karşılaşmamış olmanın verdiği rehavet 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 farkettim. “Acaba bu defa neyi bozdum ?” 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 itibariyle bloguma rastgele parametreler içeren çok sayıda istekte bulunulduğunu farkettim. (HTTP DoS)

HTTP DoS saldırısını gerçekleştiren kaynak ip adreslerine bakıp,

Cloudflare’in ip adreslerini gördüğümde, rehavetin 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. :))





Top Threat Countries
Last 24 hours

Country	Requests
Russian Federation	9,306
Turkey	14
Ukraine	3
Netherlands	1

Help

Top Traffic Countries
Last 24 hours

Country	Traffic
Russian Federation	154,857
Turkey	13,242
United States	4,406
France	672
India	338

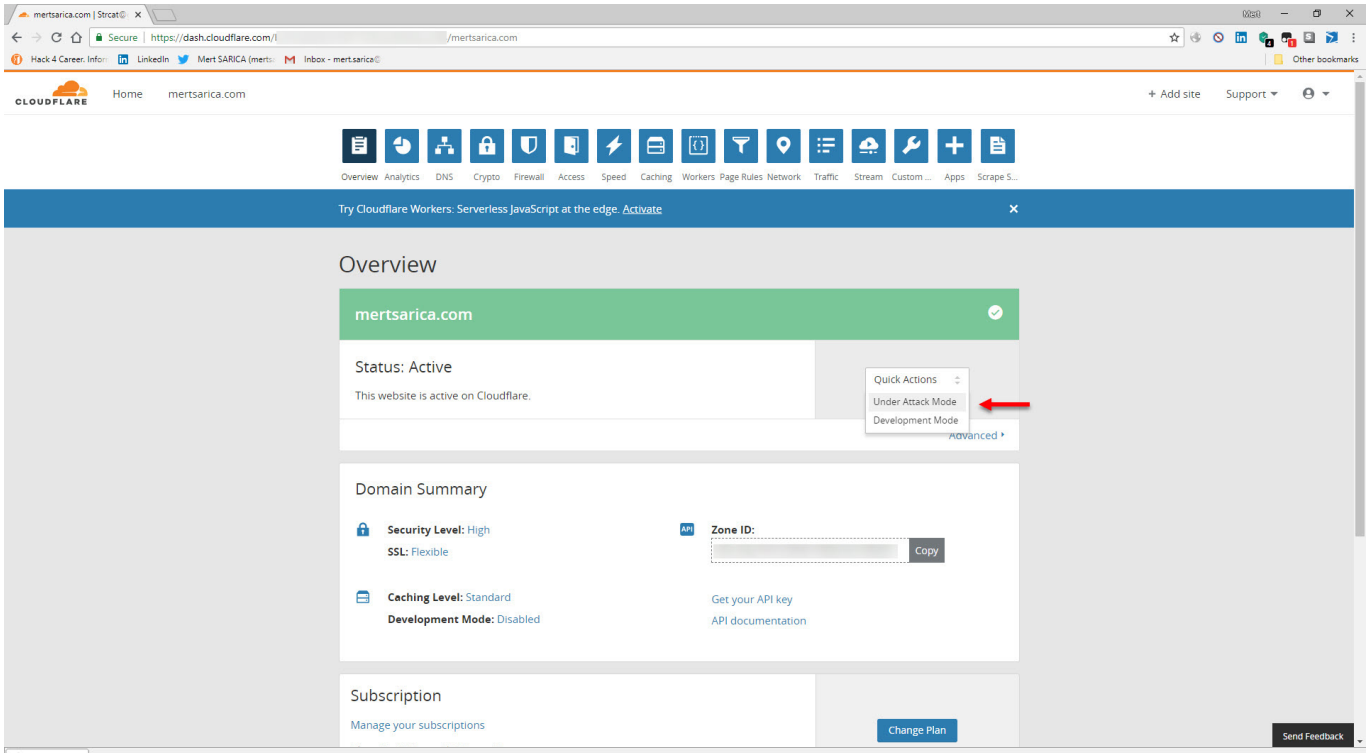
Help

Top Crawlers / Bots
Last 24 hours

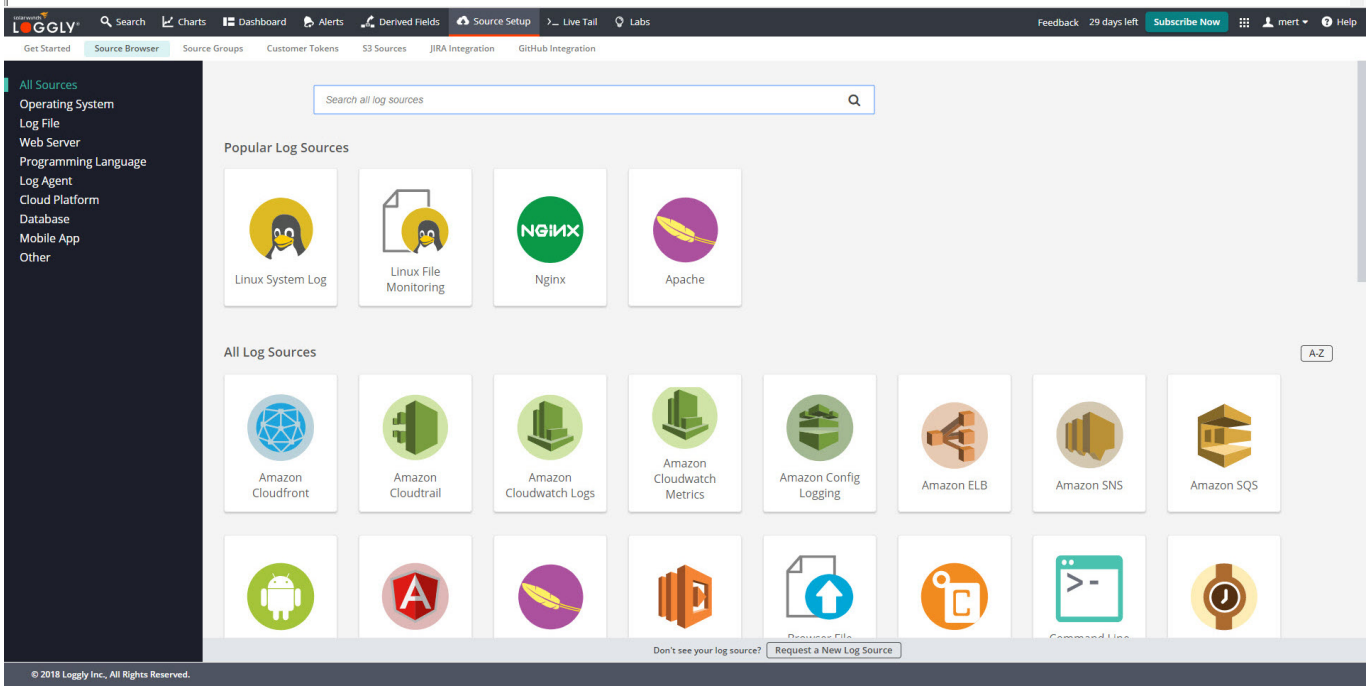
Crawler/Bot	Pages Crawled
Bing	133
Yandex	104
Google	55
applebot	13
Twitter	9

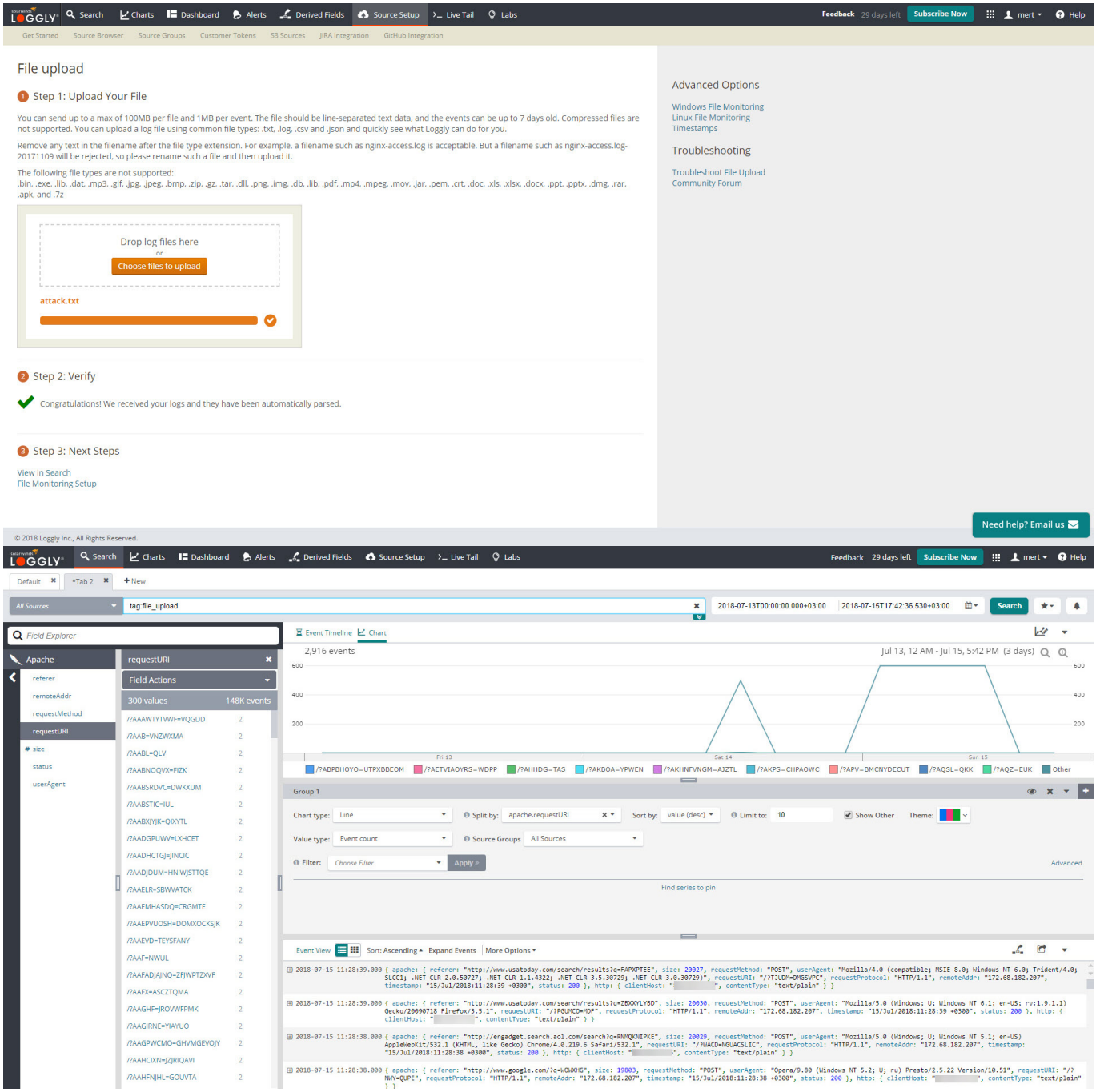
Help

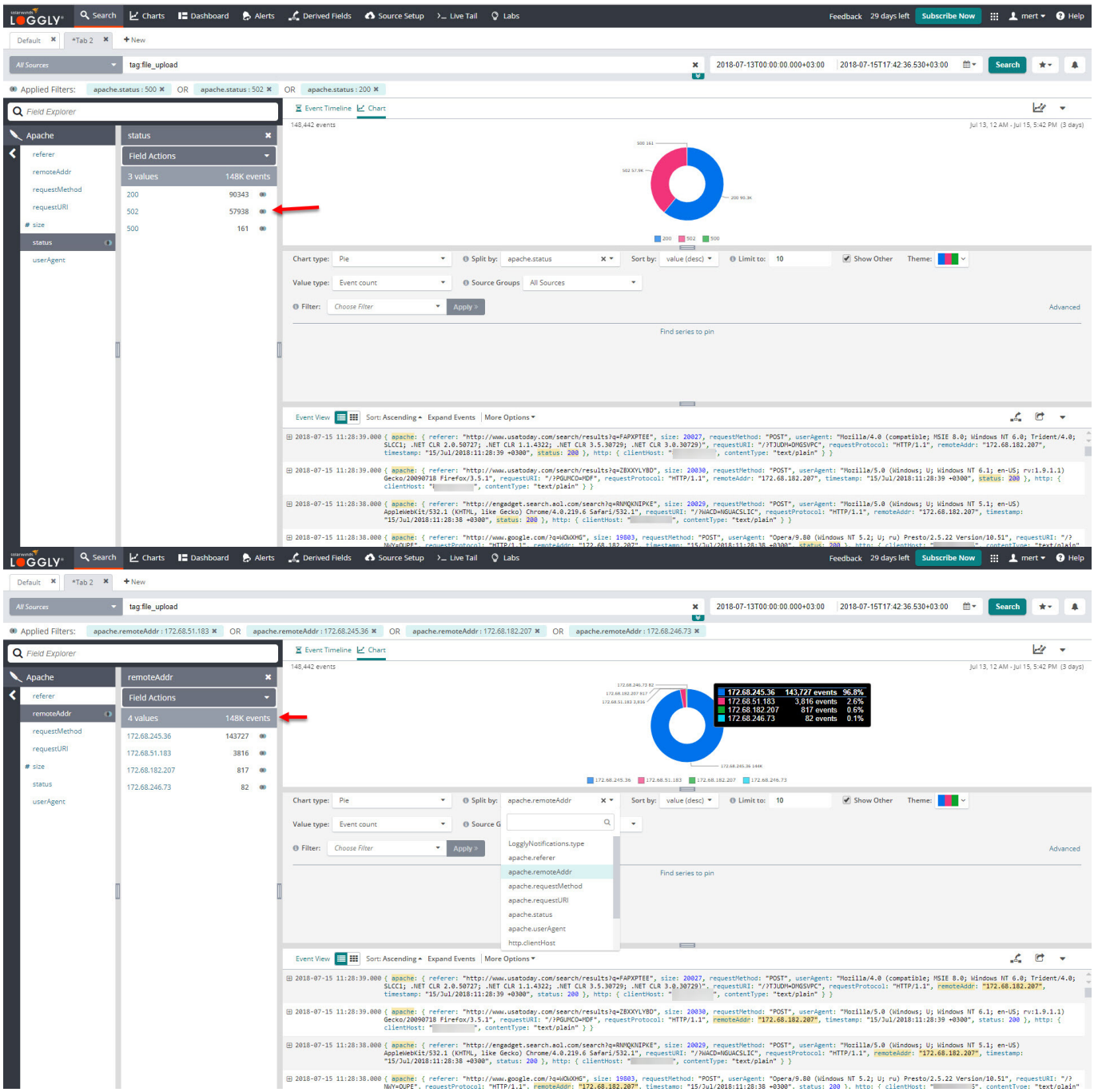
Ben bu araştırmaları yaparken bir yandan DoS saldırısı devam ettiği için saldırıları durdurmak için Cloudflare'in panelinden Under Attack özelliğini aktif hale getirdim ve saldırı anında etkisiz hale geldi. Akabinde saldırı ile ilgili istatistiki bilgiler toplamak için öncelikle komut satırından ardından da SolarWinds'in Loggly isimli web uygulamasından faydalandım. Loggly dışında çevrimdışı analiz için de bir yandan Apache Logs Viewer aracının çıktılarını inceledim. Analiz sonucuna göre ~24 saatte bloguma yaklaşık ~150.000 istek yapılmış ve bunlardan ~60.000 tanesi (502 HTTP Status) blogumu erişilemez hale getirmişti.

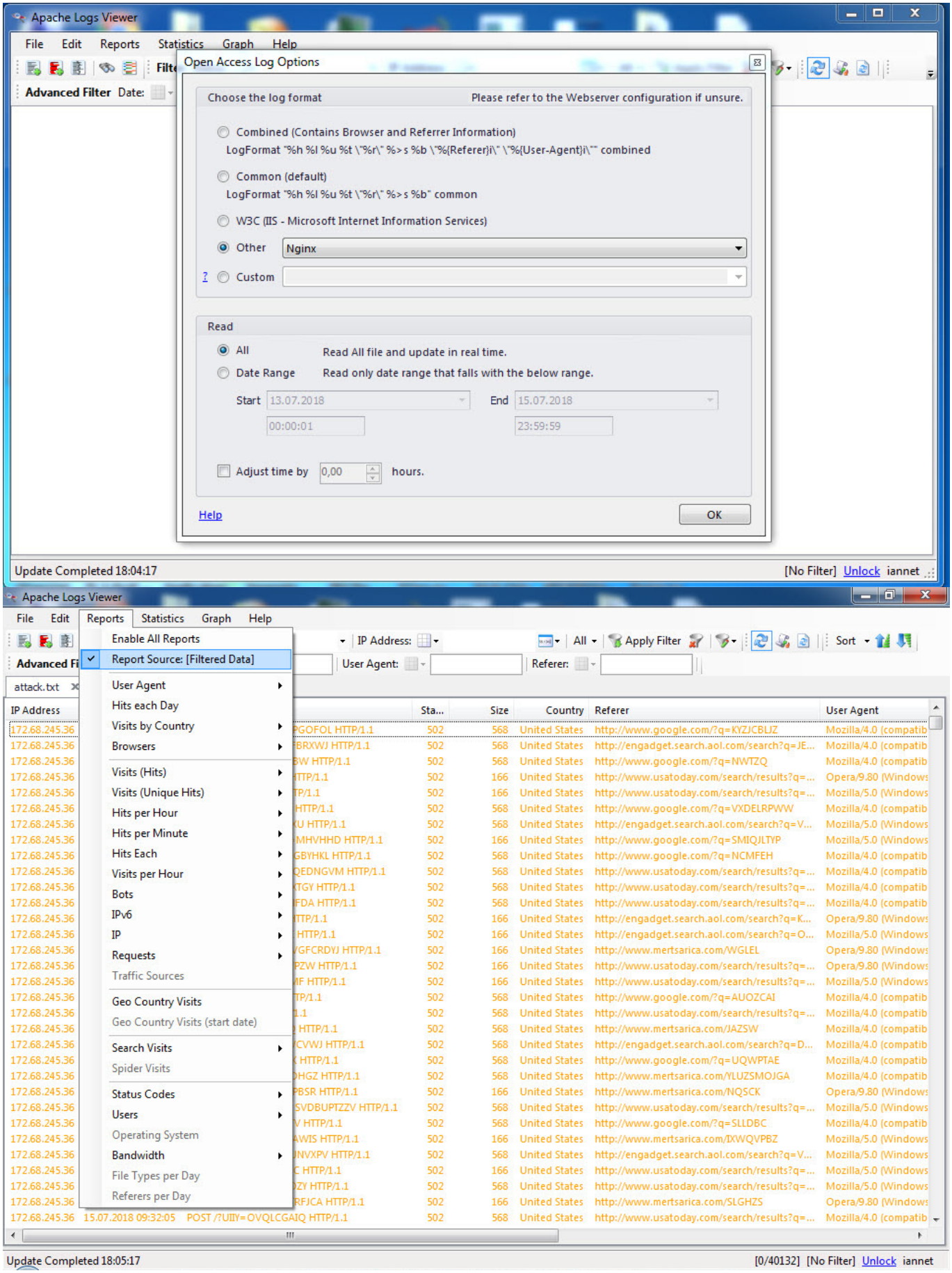

CLOUDFLARE
Home
mertsarica.com
+ Add site
Support
Overview
Analytics
DNS
Crypto
Firewall
Access
Speed
Caching
Workers
Page Rules
Network
Traffic
Stream
Apps
Try Cloudflare Workers: Serverless JavaScript at the edge. Activate
Overview
mertsarica.com
Status: Active
This website is active on Cloudflare.
Quick Actions
Under Attack Mode
Development Mode
Advanced
Domain Summary
Security Level: High
SSL: Flexible
Zone ID:
Copy
Caching Level: Standard
Development Mode: Disabled
Get your API key
API documentation
Subscription
Manage your subscriptions
Change Plan
Send Feedback

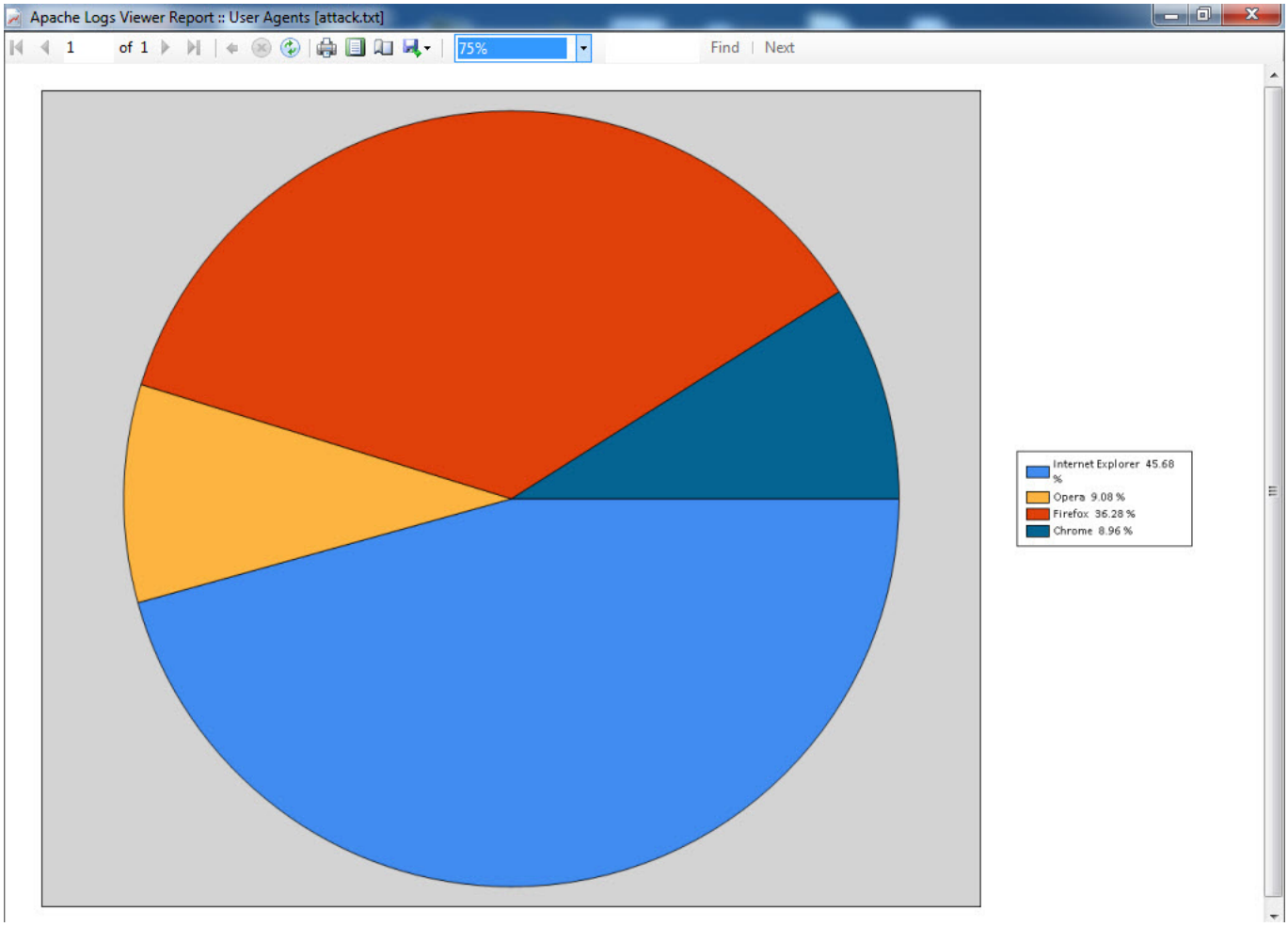
DO - Yeni
root@batcave:/var/log/nginx# grep "POST /?" access.log.1 > attack.txt
root@batcave:/var/log/nginx# grep "POST /?" access.log >> attack.txt
root@batcave:/var/log/nginx# wc -l attack.txt
148442 attack.txt
root@batcave:/var/log/nginx# tail -n 10 attack.txt
172.68.182.207 - - [15/Jul/2018:11:28:35 +0300] "POST /?LJSDYXIY=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 /?YPQU=JLIQD HTTP/1.1" 200 20030 "http://www.mertsarica.com/JVXREF" "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 /?YVCMQCQATC=WOVEBABC 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)"
172.68.182.207 - - [15/Jul/2018:11:28:36 +0300] "POST /?FCRKCPEH=ALROYF HTTP/1.1" 200 20028 "http://www.usatoday.com/search/results?q=OSPWR" "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/2018:11:28:37 +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=SWNWIS HTTP/1.1" 200 20030 "http://www.mertsarica.com/GYMNZTILN" "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=QUPE HTTP/1.1" 200 19803 "http://www.google.com/?q=WOWXHG" "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=RNMQKNIPKE" "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=ZBXXYLYBD" "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=DMGSVPC 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
Search
Charts
Dashboard
Alerts
Derived Fields
Source Setup
Live Tail
Labs
Feedback
29 days left
Subscribe Now
mert
Help
Get Started
Source Browser
Source Groups
Customer Tokens
S3 Sources
JIRA Integration
GitHub Integration
All Sources
Operating System
Log File
Web Server
Programming Language
Log Agent
Cloud Platform
Database
Mobile App
Other
Search all log sources
Popular Log Sources
Linux System Log
Linux File Monitoring
Nginx
Apache
All Log Sources
A-Z
Amazon Cloudfront
Amazon Cloudtrail
Amazon Cloudwatch Logs
Amazon Cloudwatch Metrics
Amazon Config Logging
Amazon ELB
Amazon SNS
Amazon SQS
Don't see your log source?
Request a New Log Source
© 2018 Loggly Inc., All Rights Reserved.

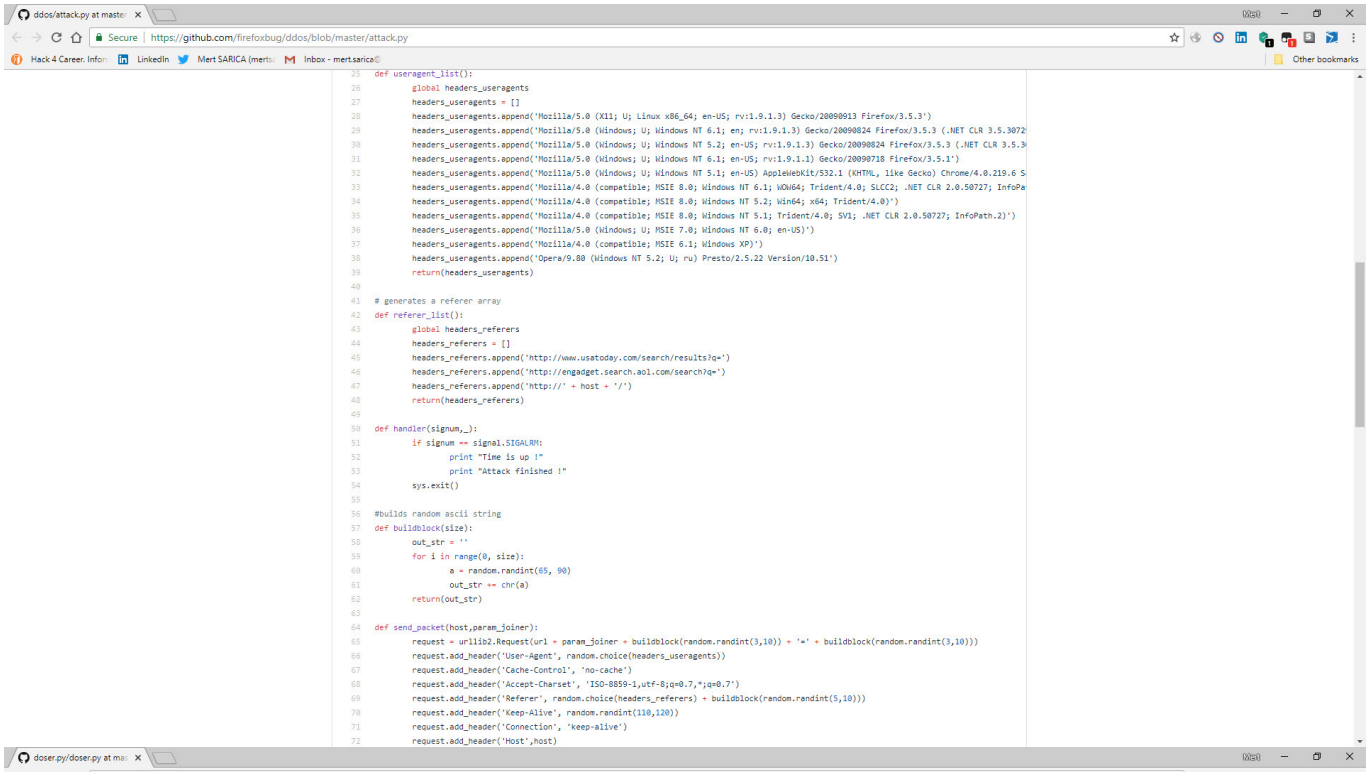

Search
Charts
Dashboard
Alerts
Derived Fields
Source Setup
Live Tail
Labs
Feedback 29 days left
Subscribe Now
mert
Help
Get Started
Source Browser
Source Groups
Customer Tokens
53 Sources
JIRA Integration
GitHub Integration
File upload
Step 1: Upload Your File
You can send up to a max of 100MB per file 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, .lib, .pdf, .mp4, .mpeg, .mov, .jar, .pem, .crt, .doc, .xls, .xlsx, .docx, .ppt, .pptx, .dmg, .rar, .apk, and .7z
Drop log files here
or
Choose files to upload
attack.txt
Step 2: Verify
Congratulations! We received your logs and they have been automatically parsed.
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
© 2018 Loggly Inc., All Rights Reserved.
Default
*Tab 2
+ New
All Sources
tag:file_upload
2018-07-13T00:00:00.000+03:00
2018-07-15T17:42:36.530+03:00
Search
Field Explorer
Apache
referer
remoteAddr
requestMethod
requestURI
size
status
userAgent
requestURI
Field Actions
300 values
148K events
/?AAAWTYTVWF=VQGDD 2
/?AAB=VNZWXMA 2
/?AABL=QLV 2
/?AABNOQVX=FIZK 2
/?AABSRDVC=DWKXUM 2
/?AABSTIC=IUL 2
/?AABXJYJK=QIXYTL 2
/?AADGPUWV=LXHCET 2
/?AADHCTGJ=JINCIC 2
/?AADJDUM=HNIWJSTTQE 2
/?AAELR=SBWVATCK 2
/?AAEMHASDQ=CRGMTE 2
/?AAEPVUOSH=DOMXOCKSJK 2
/?AAEVD=TEYSFANY 2
/?AAF=NWUL 2
/?AAFADJAJNQ=ZFJWPTZXVF 2
/?AAFX=ASCZTQMA 2
/?AAGHF=JROVWFPMK 2
/?AAGIRNE=YIAYUO 2
/?AAGPWCMO=GHVMGEVOJY 2
/?AAHCIXN=JZJRIQAVI 2
/?AAHFNJHL=GOUVTA 2
Event Timeline
Chart
2,916 events
Jul 13, 12 AM - Jul 15, 5:42 PM (3 days)
600
400
200
Fri 13
Sat 14
Sun 15
/?ABPBHOYO=UTPXBBEOM
/?AETVIAOYRS=WDPP
/?AHHDG=TAS
/?AKBOA=YPWEN
/?AKHNFVNGM=AJZTL
/?AKPS=CHPAOWC
/?APV=BMCNYDECUT
/?AQSL=QKK
/?AQZ=EUK
Other
Group 1
Chart type: Line
Split by: apache.requestURI
Sort by: value (desc)
Limit to: 10
Show Other
Theme:
Value type: Event count
Source Groups All Sources
Filter: Choose Filter
Apply
Advanced
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=FAPXPTEE", 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: "/?TJUDM=DMGSVPC", requestProtocol: "HTTP/1.1", remoteAddr: "172.68.182.207", timestamp: "15/Jul/2018:11:28:39 +0300", status: 200 }, http: { clientHost: "[redacted]", contentType: "text/plain" } }
2018-07-15 11:28:39.000 { apache: { referer: "http://www.usatoday.com/search/results?q=ZBXXYLYBD", 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: "/?PGUMCO=MDF", requestProtocol: "HTTP/1.1", remoteAddr: "172.68.182.207", timestamp: "15/Jul/2018:11:28:39 +0300", status: 200 }, http: { clientHost: "[redacted]", contentType: "text/plain" } }
2018-07-15 11:28:38.000 { apache: { referer: "http://engadget.search.aol.com/search?q=RNKQKNIPKE", 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: "/?WACD=NGUACSLIC", requestProtocol: "HTTP/1.1", remoteAddr: "172.68.182.207", timestamp: "15/Jul/2018:11:28:38 +0300", status: 200 }, http: { clientHost: "[redacted]", contentType: "text/plain" } }
2018-07-15 11:28:38.000 { apache: { referer: "http://www.google.com/?q=WOWXHG", size: 19803, requestMethod: "POST", userAgent: "Opera/9.80 (Windows NT 5.2; U; ru) Presto/2.5.22 Version/10.51", requestURI: "/?NWY=QUPE", requestProtocol: "HTTP/1.1", remoteAddr: "172.68.182.207", timestamp: "15/Jul/2018:11:28:38 +0300", status: 200 }, http: { clientHost: "[redacted]", contentType: "text/plain" } }


Search
Charts
Dashboard
Alerts
Derived Fields
Source Setup
Live Tail
Labs
Feedback
29 days left
Subscribe Now
mert
Help
tag:file_upload
2018-07-13T00:00:00.000+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
Apache
referer
remoteAddr
requestMethod
requestURI
size
status
userAgent
status
Field Actions
3 values
148K events
200
90343
502
57938
500
161
Event Timeline
Chart
148,442 events
Jul 13, 12 AM - Jul 15, 5:42 PM (3 days)
Chart type:
Pie
Split by:
apache.status
Sort by:
value (desc)
Limit to:
10
Show Other
Theme:
Value type:
Event count
Source Groups
All Sources
Filter:
Choose Filter
Apply
Advanced
Find series to pin
Event View
Sort: Ascending
Expand Events
More Options
remoteAddr
Field Actions
4 values
148K events
172.68.245.36
143727
172.68.51.183
3816
172.68.182.207
817
172.68.246.73
82
172.68.245.36 143,727 events 96.8%
172.68.51.183 3,816 events 2.6%
172.68.182.207 817 events 0.6%
172.68.246.73 82 events 0.1%
LogglyNotifications.type
apache.referer
apache.remoteAddr
apache.requestMethod
apache.requestURI
apache.status
apache.userAgent
http.clientHost

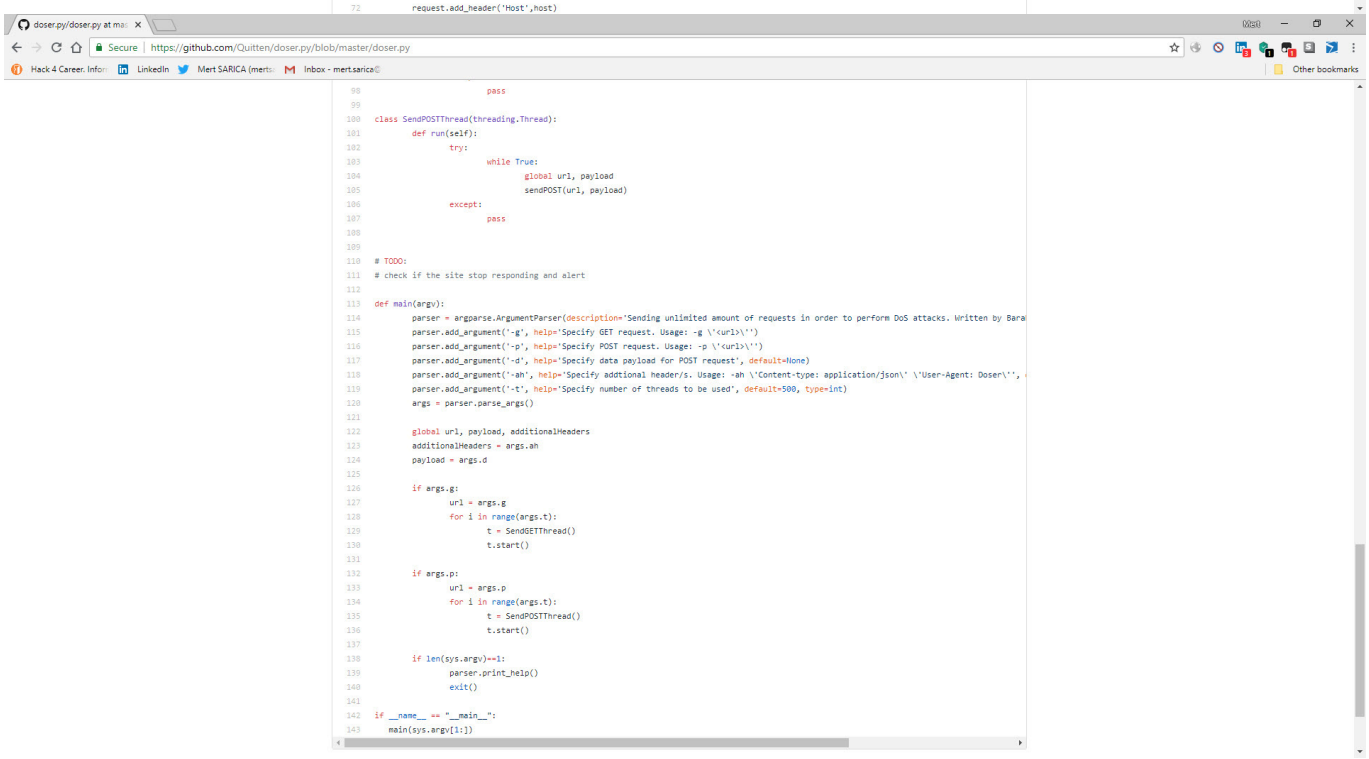

Apache Logs Viewer
File Edit Reports Statistics Graph Help
Advanced Filter Date:
Open Access Log Options
Choose the log format
Please refer to the Webserver configuration if unsure.
Combined (Contains Browser and Referrer Information)
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" 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
00:00:01
End
15.07.2018
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]
User Agent
Hits each Day
Visits by Country
Browsers
Visits (Hits)
Visits (Unique Hits)
Hits per Hour
Hits per Minute
Hits Each
Visits per Hour
Bots
IPv6
IP
Requests
Traffic Sources
Geo Country Visits
Geo Country Visits (start date)
Search Visits
Spider Visits
Status Codes
Users
Operating System
Bandwidth
File Types per Day
Referers per Day
IP Address:
All
Apply Filter
Sort
User Agent:
Referer:
attack.txt
IP Address
Sta...
Size
Country
Referer
User Agent
172.68.245.36 15.07.2018 09:32:05 POST /?UIIY=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



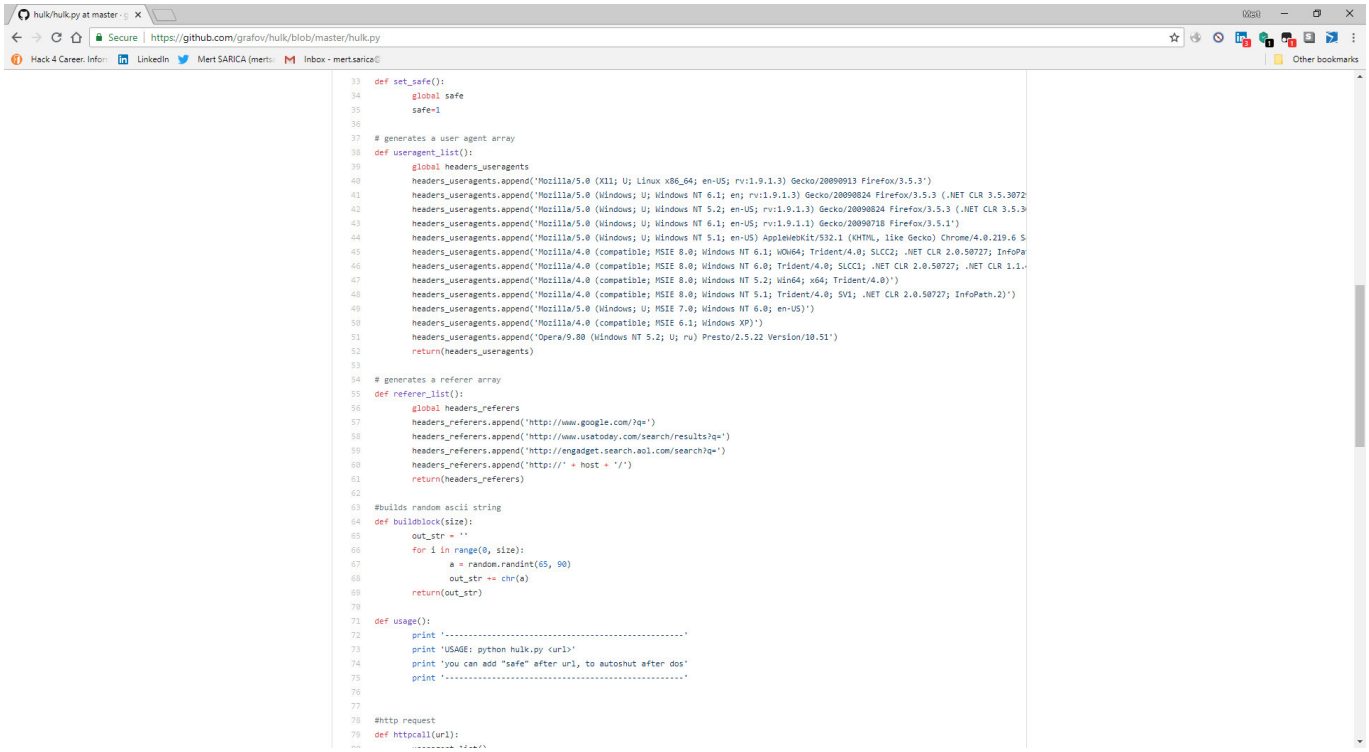
DoS saldırısı ile ilgili olarak, erişim kayıtları (access.log) üzerinden elde ettiğim bilgilere istinaden yapmış olduğum araştırmalar sonucunda birbirine benzeyen 3 farklı Python aracı (hulk.py , doser.py , attack.py) dikkatimi çekti. Bu araçların kaynak kodları ile bloguma yapılan DoS saldırısını karşılaştırdığımda,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



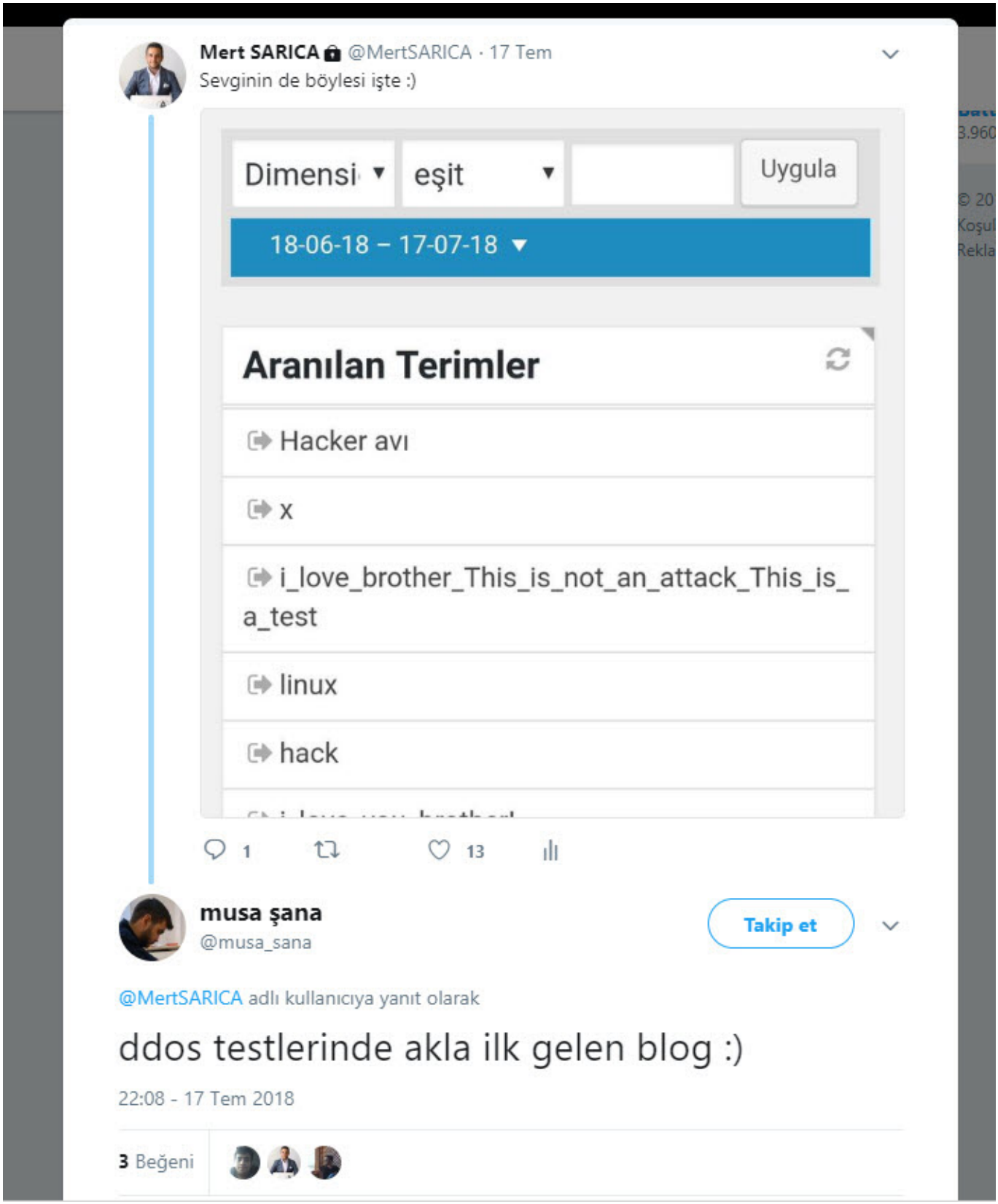

```
def useragent_list():
        global headers_useragents
        headers_useragents = []
        headers_useragents.append('Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.1.3) Gecko/20090913 Firefox/3.5.3')
        headers_useragents.append('Mozilla/5.0 (Windows; U; Windows NT 6.1; en; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3 (.NET CLR 3.5.3072
        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 3.5.3
        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')
        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
        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
        headers_useragents.append('Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Win64; x64; Trident/4.0)')
        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)')
        headers_useragents.append('Mozilla/5.0 (Windows; U; MSIE 7.0; Windows NT 6.0; en-US)')
        headers_useragents.append('Mozilla/4.0 (compatible; MSIE 6.1; Windows XP)')
        headers_useragents.append('Opera/9.80 (Windows NT 5.2; U; ru) Presto/2.5.22 Version/10.51')
        return(headers_useragents)

# generates a referer array
def referer_list():
        global headers_referers
        headers_referers = []
        headers_referers.append('http://www.usatoday.com/search/results?q=')
        headers_referers.append('http://engadget.search.aol.com/search?q=')
        headers_referers.append('http://' + host + '/')
        return(headers_referers)

def handler(signum,_):
        if signum == signal.SIGALRM:
                print "Time is up !"
                print "Attack finished !"
        sys.exit()

#builds random ascii string
def buildblock(size):
        out_str = ''
        for i in range(0, size):
                a = random.randint(65, 90)
                out_str += chr(a)
        return(out_str)

def send_packet(host,param_joiner):
        request = urllib2.Request(url + param_joiner + buildblock(random.randint(3,10)) + '=' + buildblock(random.randint(3,10)))
        request.add_header('User-Agent', random.choice(headers_useragents))
        request.add_header('Cache-Control', 'no-cache')
        request.add_header('Accept-Charset', 'ISO-8859-1,utf-8;q=0.7,*;q=0.7')
        request.add_header('Referer', random.choice(headers_referers) + buildblock(random.randint(5,10)))
        request.add_header('Keep-Alive', random.randint(110,120))
        request.add_header('Connection', 'keep-alive')
        request.add_header('Host',host)
```



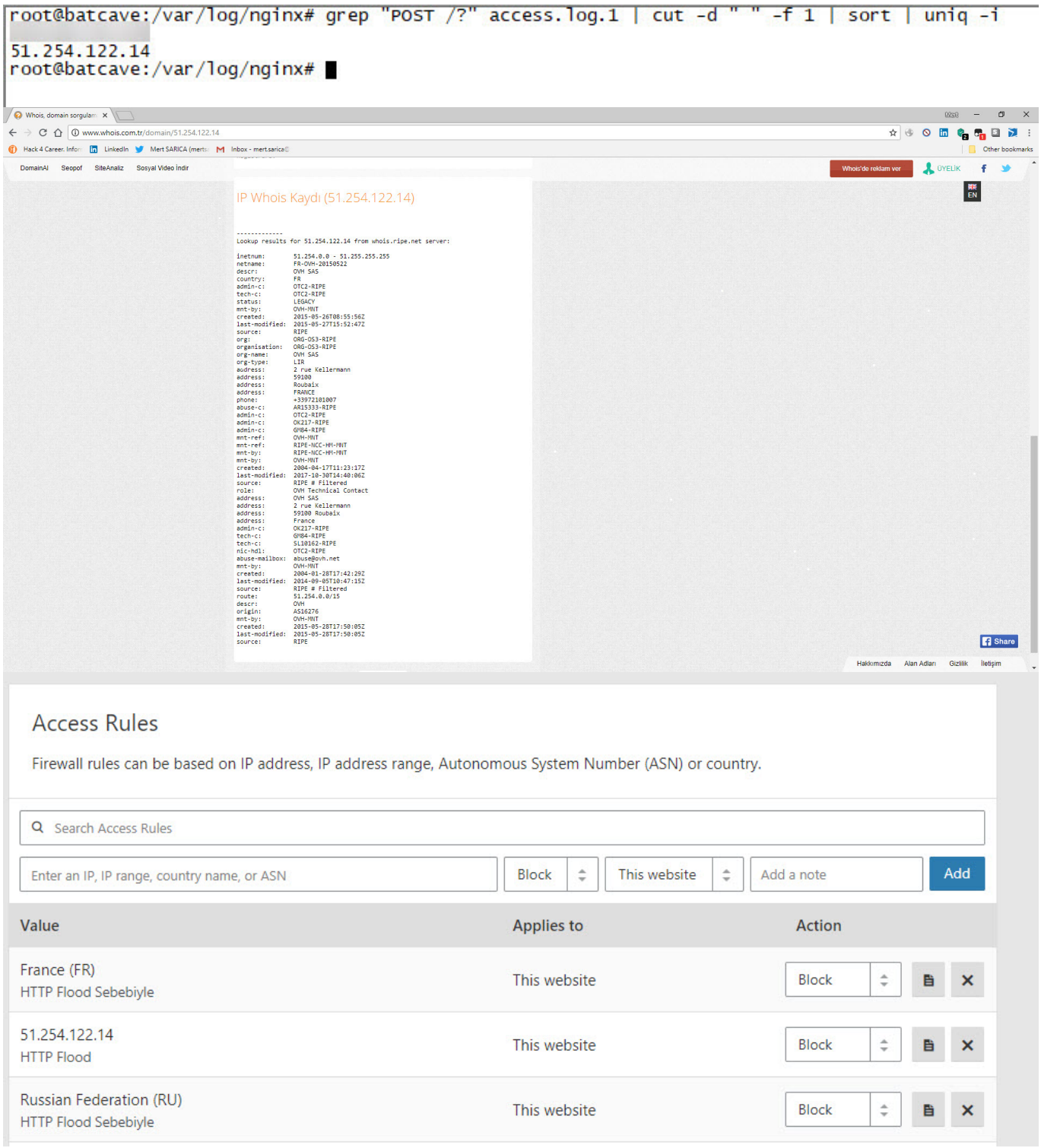

```
                        pass

class SendPOSTThread(threading.Thread):
        def run(self):
                try:
                        while True:
                                global url, payload
                                sendPOST(url, payload)
                except:
                        pass


# TODO:
# check if the site stop responding and alert

def main(argv):
        parser = argparse.ArgumentParser(description='Sending unlimited amount of requests in order to perform DoS attacks. Written by Bara
        parser.add_argument('-g', help='Specify GET request. Usage: -g \'<url>\'')
        parser.add_argument('-p', help='Specify POST request. Usage: -p \'<url>\'')
        parser.add_argument('-d', help='Specify data payload for POST request', default=None)
        parser.add_argument('-ah', help='Specify addtional header/s. Usage: -ah \'Content-type: application/json\' \'User-Agent: Doser\'', 
        parser.add_argument('-t', help='Specify number of threads to be used', default=500, type=int)
        args = parser.parse_args()

        global url, payload, additionalHeaders
        additionalHeaders = args.ah
        payload = args.d

        if args.g:
                url = args.g
                for i in range(args.t):
                        t = SendGETThread()
                        t.start()

        if args.p:
                url = args.p
                for i in range(args.t):
                        t = SendPOSTThread()
                        t.start()

        if len(sys.argv)==1:
                parser.print_help()
                exit()

if __name__ == "__main__":
   main(sys.argv[1:])
```



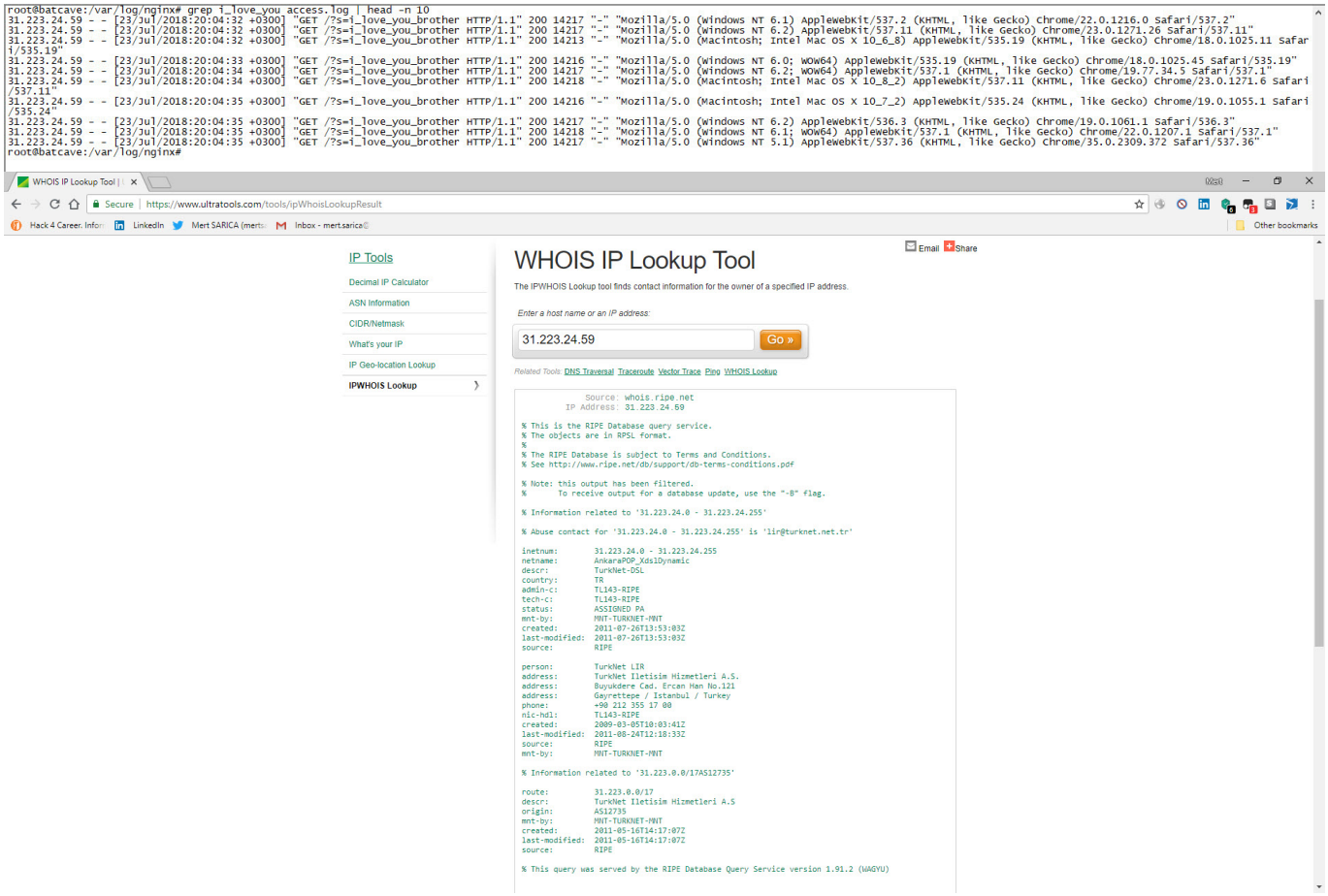
Blogumun WordPress yönetici paneline de göz gezdirdiğimde, Aranılan Terimler kısmındaki i_love_brother_This_is_not_an_attack_This_is_a_test arama terimi dikkatimi çekti. Bu terim ile ilgili göndermiş olduğum bir tweete yapılan yorumda da olduğu gibi, blogumun DDoS testlerinde akla ilk gelen blog olabileceğini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



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.



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



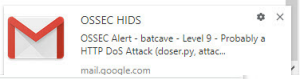
Bana olan sevgisini sele dönüştürme konusunda ısrarcı olan bu Rus kardeşim ile sistematik olarak mücadele edebilmek ve benzer durumlarla mücadele etmek durumunda kalanlara yol gösterme adına çeşitli araçlardan faydalanmaya karar verdim.

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.

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 ×

OSSEC HIDS <mert.sarica@gmail.com> 11:20 PM (0 minutes ago)
to me

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:
Portion of the log(s):

- - [23/Jul/2018:23:20:17 +0300] "GET /?FLEDNO=IQOKGUIUYA 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=VHJAOOBNF" "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=VHJAOOBNF" "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=VHJAOOBNF" "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=VHJAOOBNF" "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=VHJAOOBNF" "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"

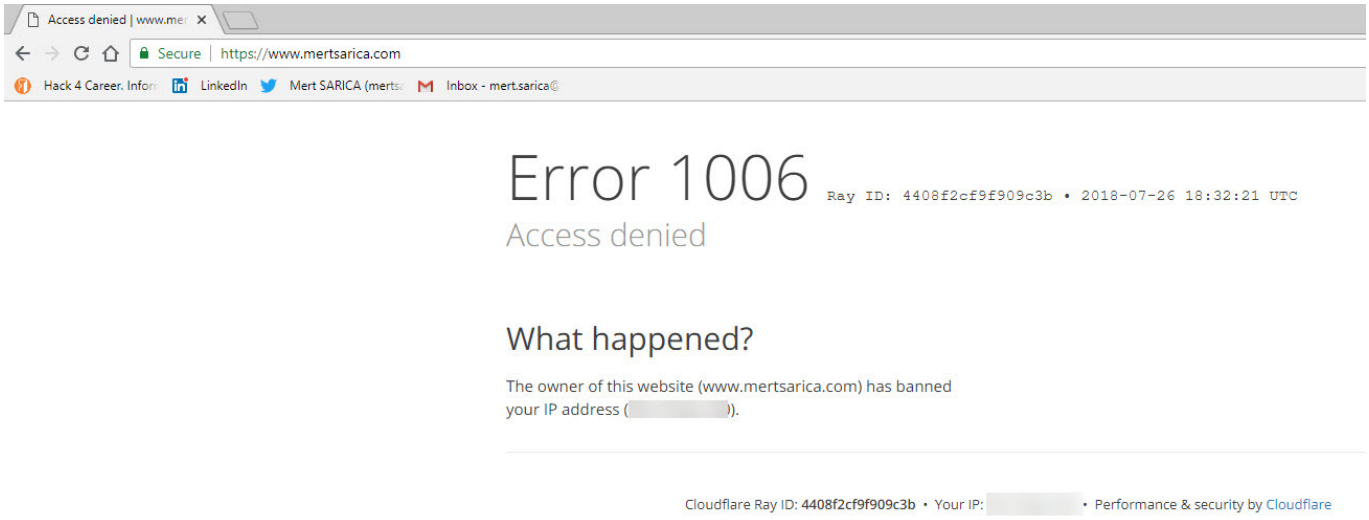
OSSEC HIDS ile benim sevgi dolu Rus kardeşimin DoS saldırısını tespit etmek yeterli olmayacağı için fail2ban aracı ile bu iki tür DoS saldırısını tespit eden özel bir kural yazıp, bu yazıda da belirtildiği şekilde Cloudflare

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 sağlamlaştırdım. :)

```
  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
```



Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.