禪

[illegible]

[illegible] (DDoS) [illegible]

[illegible]

[illegible] Arbor Networks [illegible] 50 [illegible] Radware [illegible] DDoS [illegible] Fortinet [illegible].

حمله منع سرویس توزیع شده چیست؟

بهطور خلاصه، یک حمله منع سرویس توزیع شده یک حمله سیلآسا بوده که ترافیک افسارگسیختهای را به سمت هاست یا سرور روانه میکند. یک هکر میتواند ترافیک سنگینی را ارسال کند تا به سرعت پهنای باند و منابع سرور از دسترس خارج شوند . در این حالت سرور دیگر قادر نیست به درخواستها رسیدگی کند . در این حالت ممکن است سرور دچار مشکل شده یا پهنای باند برای پاسخگویی به درخواستهای معتبر مشتریان وبسرویس شما در دسترس نباشد. همانطور که ممکن است حدس زده باشید تا زمانی که حمله ادامه پیدا کند خدماترسانی متوقف میشود که این حرف به معنای از دست دادن درآمدهای مالی شما از سرویسی است که آنرا ارائه کردهاید . حملات منع سرویس توزیع شده برای هر کسبوکار آنلاینی ویرانگر بوده و در هر ساعت از شبانهروز ممکن است رخ دهند. در نتیجه مهم است که بدانید این حمله چگونه عمل میکند و چطور باید آنرا در کوتاهترین زمان متوقف کنید . در مدت زمان بروز چنین حملاتی شما با یک منبع حملهکننده واحد سروکار ندارید تا با فیلتر کردن آدرس آیپی هکر حمله را متوقف کنید . هکرهایی که حملات منع سرویس توزیع شده را پیادهسازی میکنند در ابتدا سامانههای کاربران را آلوده میکنند . این سامانهها میتوانند کامپیوترهای شخصی، سامانههای توکار یا دستگاههای اینترنت اشیا باشند . در ارتباط با دستگاههای توکار و اینترنت اشیا هکرها بهطور مستقیم به میانافزاری که وظیفه کنترل دستگاه را عهدهدار است حمله میکنند. در ادامه هکرها از یک سامانه متمرکز که وظیفه ارسال دستورات را بر عهده دارد استفاده میکنند . سامانهای که به ماشینهای آلوده به بدافزار اعلام میدارد ترافیک را به سمت یک سایت ارسال کنند. شدت یک حمله به تعداد ماشینهایی که یک هکر موفق شده است آنها را آلوده کند بستگی دارد . بهطور معمول، تعداد این کامپیوترها ممکن است 1000 عدد یا حتی فراتر از 10 هزار دستگاه برود . مکانیزم بهکار گرفته شده در حملات منع سرویس توزیع شده در اغلب موارد پیچیده است . بهطور مثال هکرها میتوانند درخواستهای اتصال ناقص را ارسال کرده که این مکانیزم باعث به وجود آمدن حالت انتظار میشود . در این تکنیک بهطور مرتب درخواستهای جدیدی ارسال میشود . شما در حالت عادی میتوانید میزان ترافیکی را که از بابت یک حمله قادر به دفع آن هستید، محاسبه کنید . بهطور مثال، اگر ترافیک عادی شما برابر با 100 ارتباط ورودی در یک لحظه بوده و سرور در این وضعیت قادر است به فعالیتهای خود ادامه دهد، به معنای آن است که به احتمال زیاد ارتباط 100 ماشین روی ترافیک شما تاثیرگذار نخواهد بود . با این حال در یک حمله منع سرویس توزیع شده هزاران اتصال مبتنی بر آدرسهای آیپی مختلف در یک زمان به سرور حمله میکنند . اگر سرور نتواند در یک لحظه 10 هزار ارتباط را مدیریت کند، به معنای آن است که شما در برابر یک حمله منع سرویس توزیع شده آسیبپذیر خواهید بود . (شکل یک) به عبارت دقیقتر در یک لحظه ممکن است صدها یا هزاران ماشین (سرور، کامپیوترهای شخصی یا حتی دستگاههای موبایل) ترافیک خود را به سمت شما گسیل کنند. در عرض چند دقیقه عملکرد سایت کاهش پیدا کرده و منابع هدر میروند . در این حالت کاربران عادی موفق نخواهند شد به سایت شما دسترسی پیدا کنند .

چگونه میتوانیم اطلاع پیدا کنیم یک حمله منع سرویس توزیع شده رخ داده است؟

حملات منع سرویس توزیع شده از آن جهت بدترین نوع حملات به شمار میروند که بدون هیچگونه هشداری از راه میرسند . در حالی که برخی از گروههای بزرگ هکری پیش از حمله هشدارهایی را ارسال میکنند، اما در اغلب موارد مهاجمان بدون هیچگونه هشداری به سایت شما حمله میکنند . در این حالت شما تنها زمانی از این موضوع مطلع خواهید شد که مشتریان شکایت میکنند که مشکلی رخ داده و قادر نیستند به سایت شما دسترسی پیدا کنند .

در ابتدا تصور نمیکنید یک حمله منع سرویس توزیع شده رخ داده است، در نتیجه فکر میکنید سرور یا هاست دچار مشکل شدهاند. در ادامه سرور را بررسی کرده و یکسری آزمایشهای اولیه انجام میدهید، اما فقط حجم بالایی از ترافیک را مشاهده میکنید که باعث شده بهکارگیری منابع به حداکثر ظرفیت ممکن برسد. در ادامه به سراغ بررسی این موضوع میروید که آیا برنامههایی در پسزمینه در حال اجرا هستند، اما بازهم هیچ نشانهای از یک مشکل را پیدا نمیکنید . مدت زمانی که صرف درک این موضوع میکنید که یک حمله منع سرویس توزیع شده رخ داده و مدت زمانی که صرف کم کردن آسیبها میکنید حداقل چند ساعت زمان خواهد برد . در این چند ساعت ارزشمند شما ممکن است ضرر مالی زیادی را متحمل شوید. در نتیجه هر چه سریعتر این حمله را تشخیص دهید میزان خسارت به بار آمده به حداقل میرسد .

[illegible]

[illegible]

BASEFARM MULTI LAYER DDOS PROTECTION
basefarm
ISP Scrubbing Center
MITIGATION SIGNALING
Basefarm Data Centers
Attacker
Legitime user
The Internet
VOLUMETRIC ATTACK
CLEAN TRAFFIC
CLEAN TRAFFIC
APPLICATION ATTACK
CLEAN TRAFFIC
Legitime user
ISP Network
Local Scrubbing Center
Customer Solutions
Attacker
ATTACKS FROM INTERNET
Attackers build networks of infected computers, known as 'botnets'
ISP SCRUBBING CENTER
Stops volumetric attacks in the ISP cloud. (ISP = Internet Service Provider)
LOCAL SCRUBBING CENTER
Stops application layer DDoS attacks & other advanced threats. Detect abnormal outbound activity

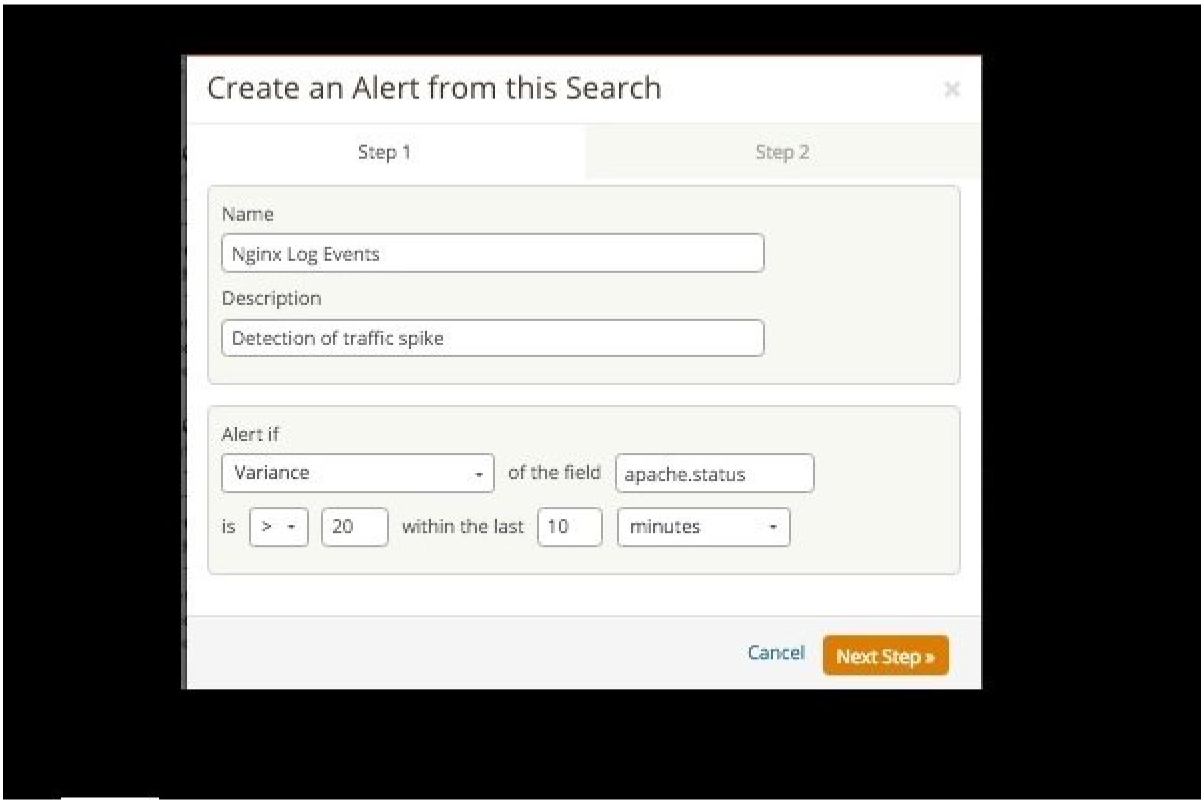
1 [illegible]

[illegible]

[illegible]

سرور با کد 503 پاسخ میدهد

در ویندوز شما میتوانید هشدارها را به گونهای تنظیم کنید که اگر یک رویداد خاص در Event Viewer اجرا شد از آن مطلع شوید . شما میتوانید هر موضوعی همچون خطاها، هشدارها یا هر نوع رویدادی را به یک وظیفه الصاق سنجاق کنید. اینکار باعث میشود تا پیش از آنکه یک موقعیت بحرانی شکل بگیرید موضوع را بررسی کنید . برای الصاق یک رویداد 503 ابتدا باید رویداد موردنظر خود را در Event Viewer پیدا کنید . برای این منظور
Event Viewer را باز کرده و روی رویداد موردنظر کلیک راست کنید . (شکل دو) اینکار باعث میشود تا صفحه پیکربندی، مکانی که در نظر دارید یک رویداد را برای ارسال یک ایمیل به مدیر یا تیمی از پژوهشگران پیکربندی کنید، در اختیارات قرار گیرد .



Name: Nginx Log Events

Description: Detection of traffic spike

Alert if Variance of the field apache.status is > 20 within the last 10 minutes

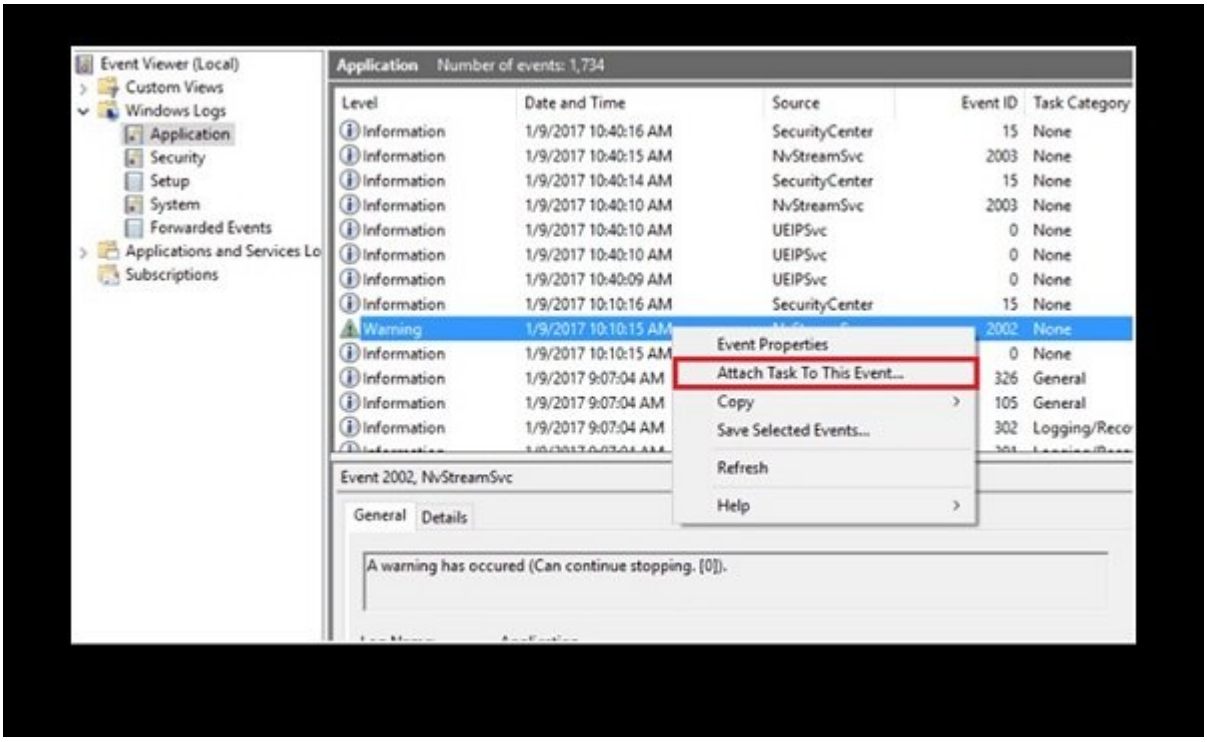
شکل **2**

TTL Time Out

شما بهطور معمول میتوانید سرور را برای آزمایش پهنای باند و ارتباطات پینگ کنید، اگر در نظر دارید فرآیند هشداردهی را خودکارسازی کرده بهطوری که پیش از وقوع یک حمله به شما اطلاعرسانی کند، این راهکار کمک چندانی به شما نمیکند . البته بعضی مواقع پینگ کردن سرور با اشتباهاتی نیز همراه است. برای آنکه بتوانید هشداردهی مبتنی بر پینگ را خودکارسازی کنید، چند سرویس روی وب وجود دارند که اجازه میدهند از هر نقطه در جهان سایت خود را پینگ کنید . این سرویسها را میتوانید به شکل منطقهای پیکربندی کرده تا فرآیند پینگ کردن را انجام دهند . از طریق این سرویسها، سایت شما در 24 ساعت شبانهروز و هفت روز کاری تحت نظارت قرار میگیرد. در نتیجه تیم فناوری اطلاعات میتواند در صورت بروز مشکل روی سرور به سرعت موضوع را بررسی کند . به واسطه آنکه حمله منع سرویس انکار شده به سرعت پهنای باند شما را مصرف میکند، زمان پینگ ممکن است بیش از اندازه طولانی شود . در این حالت سرویسهای فوق قادر هستند هشداری را برای تیم شما ارسال کرده تا به سرعت تدابیر امنیتی فنی را برای حل مشکل اعمال کنند.

[illegible] netstat [illegible]

[illegible] Wireshark [illegible] netstat [illegible] SYN [illegible]. [illegible]



3 [illegible]

(netstat [illegible]):

1. netstat –na [illegible].

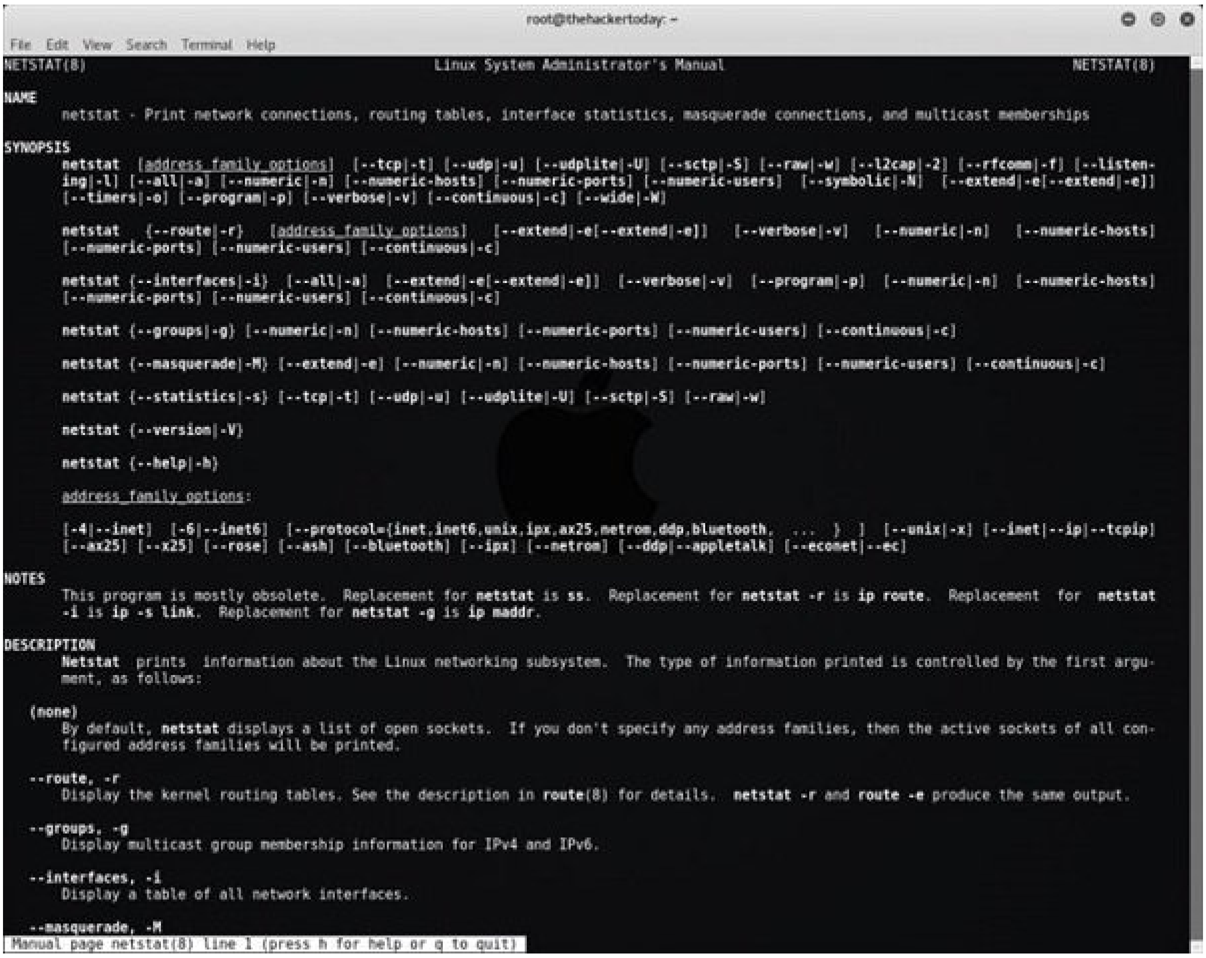
2. netstat -an | grep :80 | sort [illegible] 80 [illegible] http [illegible]. [illegible] single flood [illegible].

3. netstat -n -p|grep SYN_REC | wc –l [illegible] SYN_REC [illegible] DoS [illegible] mail bombs [illegible].

4. netstat -n -p | grep SYN_REC | sort –u [illegible].

5. ’{netstat -n -p | grep SYN_REC | awk ‘{print $5}’ | awk -F: ‘{print $1 [illegible] SYN_REC [illegible].

6. netstat -ntu | awk ‘{print $5}’ | cut -d: -f1 | sort | uniq -c | sort –n [illegible] (netstat [illegible]).



```
NETSTAT(8)                       Linux System Administrator's Manual                       NETSTAT(8)

NAME
       netstat - Print network connections, routing tables, interface statistics, masquerade connections, and multicast memberships

SYNOPSIS
       netstat  [address_family_options]  [--tcp|-t] [--udp|-u] [--udplite|-U] [--sctp|-S] [--raw|-w] [--l2cap|-2] [--rfcomm|-f] [--listen-
       ing|-l] [--all|-a] [--numeric|-n] [--numeric-hosts] [--numeric-ports] [--numeric-users]  [--symbolic|-N]  [--extend|-e[--extend|-e]]
       [--timers|-o] [--program|-p] [--verbose|-v] [--continuous|-c] [--wide|-W]

       netstat   {--route|-r}   [address_family_options]   [--extend|-e[--extend|-e]]   [--verbose|-v]   [--numeric|-n]   [--numeric-hosts]
       [--numeric-ports] [--numeric-users] [--continuous|-c]

       netstat {--interfaces|-i}  [--all|-a]  [--extend|-e[--extend|-e]]  [--verbose|-v]  [--program|-p]  [--numeric|-n]  [--numeric-hosts]
       [--numeric-ports] [--numeric-users] [--continuous|-c]

       netstat {--groups|-g} [--numeric|-n] [--numeric-hosts] [--numeric-ports] [--numeric-users] [--continuous|-c]

       netstat {--masquerade|-M} [--extend|-e] [--numeric|-n] [--numeric-hosts] [--numeric-ports] [--numeric-users] [--continuous|-c]

       netstat {--statistics|-s} [--tcp|-t] [--udp|-u] [--udplite|-U] [--sctp|-S] [--raw|-w]

       netstat {--version|-V}

       netstat {--help|-h}

       address_family_options:

       [-4|--inet]  [-6|--inet6]  [--protocol={inet,inet6,unix,ipx,ax25,netrom,ddp,bluetooth,  ...  }  ]  [--unix|-x] [--inet|--ip|--tcpip]
       [--ax25] [--x25] [--rose] [--ash] [--bluetooth] [--ipx] [--netrom] [--ddp|--appletalk] [--econet|--ec]

NOTES
       This program is mostly obsolete.  Replacement for netstat is ss.  Replacement for netstat -r is ip route.  Replacement  for  netstat
       -i is ip -s link.  Replacement for netstat -g is ip maddr.

DESCRIPTION
       Netstat  prints  information about the Linux networking subsystem.  The type of information printed is controlled by the first argu-
       ment, as follows:

   (none)
       By default, netstat displays a list of open sockets.  If you don't specify any address families, then the active sockets of all con-
       figured address families will be printed.

   --route, -r
       Display the kernel routing tables. See the description in route(8) for details.  netstat -r and route -e produce the same output.

   --groups, -g
       Display multicast group membership information for IPv4 and IPv6.

   --interfaces, -i
       Display a table of all network interfaces.

   --masquerade, -M
 Manual page netstat(8) line 1 (press h for help or q to quit)
```

شکل **4**

7. فرمان `netstat -anp |grep ‘tcp|udp’ | awk ‘{print $5}’ | cut -d: -f1 | sort | uniq -c | sort –n` تعداد ارتباطات مرتبط با آدرسهای آیپی را که از طریق پروتکلهای TCP یا UDP به سرور متصل شدهاند، شمارش کرده و نشان میدهد .

8. فرمان `netstat -ntu | grep ESTAB | awk ‘{print $5}’ | cut -d: -f1 | sort | uniq -c | sort –nr` به جای آنکه همه ارتباطات را مورد بررسی قرار دهد ارتباطات ایجاد شده (ESTABLISHED) را بررسی کرده و تعداد ارتباطات مرتبط با هر آدرس آیپی را نشان میدهد .

9. فرمان `netstat -plan|grep :80|awk {‘print $5’}|cut -d: -f 1|sort|uniq -c|sort -nk 1` آدرس آیپی و ارتباط مرتبط با آن را نشان داده و فهرست میکند . ارتباطاتی که از طریق پورت 80 انجام شدهاند . پورت 80 در اصل در ارتباط با درخواستهای مرتبط با یک صفحه وب مبتنی بر پروتکل HTTP مورد استفاده قرار میگیرد .
از طریق بهکارگیری فرمانهای فوق موفق خواهید شد یک آدرس آیپی را که آماده است برای اجرای یک حمله DDoS مورد استفاده قرار گیرد، شناسایی کنید .

نویسنده :
حمیدرضا_تائبی
منبع :
thehacktoday
loggly
tutorialspoint
tomsitpro
iplocation
dzone
دسته بندی:

ترفند امنیت
امنیت
پرونده ویژه
تاریخ انتشار :
12:05 - 28/04/1397
برچسب:
DDoS - حمله منع سرویس انکار شده - حمله منع سرویس توزیع شده - کد 503 - فرمان netstat

---

نشانی
□□□□:https://www.shabakeh-mag.com/security/13061/%D8%B1%D8%A7%D9%87%DA%A9%D8%A7%D8%B1%D9%87%D8%A7%DB%8C%DB%8C-%D8%A8%D8%B1%D8%A7%DB%8C-%D8%B4%D9%86%D8%A7%D8%B3%D8%A7%DB%8C%DB%8C-%D9%88-%D8%AF%D9%81%D8%B9-%D8%AD%D9%85%D9%84%D9%87-%D9%85%D9%86%D8%B9-%D8%B3%D8%B1%D9%88%DB%8C%D8%B3-%D8%AA%D9%88%D8%B2%DB%8C%D8%B9-%D8%B4%D8%AF%D9%87-ddos