Konsoldan Http Request Yapma

Saldırganlar botnet ağlarındaki makinelerine verdikleri emirle her birine konsoldan http request yaptırtarak DDOS saldırısı gerçekleştirebilmektedirler. Örneğin 2016 Eylül'ünde Amerika'daki DYN DNS sunucularına yapılan DDOS saldırısında saldırganlar internette nesnelerin interneti diye tabir edilen cihazları otomatize bir şekilde Mirai yazılımı ile taramışlardır. Taranan cihazlardan varsayılan kullanıcı adı ve şifre kullananların telnet'lerinde varsayılan kullanıcı adı ve şifre ile otomatize bir şekilde oturum açıp her birine tekrarlı bir şekilde konsoldan http request yaptırmışlardır. Böylece birçok kaynaktan (birçok zombinin konsolundan) hedef sunucuya talepte bulunarak saldırıyı gerçekleştirmişlerdir. Aşağıda konsoldan http request yapmanın yolları gösterilmiştir.

a. Netcat ile konsoldan http request yapma

(Yöntem I) : Netcat ile http request paket gönderimi şu şekildedir:

> nc -v www.includekarabuk.com 80

Not: v : verbose çıktı sundurur.

Output:

Connection to www.includekarabuk.com 80 port [tcp/http] succeeded!

HEAD / HTTP/1.1 // YAZ VE ENTER'LA
// BİR KEZ DAHA ENTER'LA

HTTP/1.1 200 OK
Date: Wed, 09 Nov 2016 12:22:15 GMT
Server: Apache/2.4.18 (Unix) OpenSSL/1.0.1e-fips mod_bwlimited/1.4 PHP/5.5.33
Last-Modified: Fri, 25 Mar 2016 00:27:36 GMT
ETag: "1660f56-6f-52ed4a139f557"
Accept-Ranges: bytes
Content-Length: 111
Connection: close
Content-Type: text/html

(Yöntem II) : Netcat ile http request paket gönderimi şu şekildedir:

// Netcat ile http talep gönderimi yaparken paketin ilk satırını yazıp ikinci satırını yazmak
// için bir kere ENTER yaptığımızda http request gönderimini tamamlayamadan ilk satırda
// paket yollanmaktadır. Netcat'te bu satır atlatma olayının iki kere işlemesinden dolayı
// paketler daha ilk satırda sonlanmaktadır. Bazı web sunucular bu şekilde yarım paket
// gönderimine hata dönmezken bazı web sunucular Host header'ı ilavesi de istediğinden
// 400 Bad Request hatası dönmektedir. Eğer netcat ile başarılı bir şekilde http request paket
// gönderimi yapmak istiyorsak string halinde oluşturacağımız http talep paketini input
// olarak netcat'e verebiliriz. Bu şekilde iki satırlık veya daha fazla satırlık http talep paketi
// netcat ile yollayabiliriz.

> echo -e "HEAD / HTTP/1.1\r\nHost: www.includekarabuk.com\r\n\r\n" | nc -v
www.includekarabuk.com 80

Not:

echo’nun -e parametresi: Tırnak karakterleri arasındaki escape özelliğindeki backslash’leri yorumlamayı etkinleştirir ve satır atlatma karakterlerini string olarak değil, işlevleri gibi okur.

netcat’in -v parametresi: Verbose çıktı sundurur.

Not 2:

echo ile netcat’e çıktılanan string’te (yani http request pakette) HEAD / HTTP/1.1’den sonra bir adet satır atlatma (\r\n) karakteri yer alır. Host: www.includekarabuk.com’dan sonra iki adet satır atlatma (\r\n\r\n) karakteri yer alır. İkinci satırda iki tane satır atlatma karakteri olması iki kere ENTER anlamındadır. Yani http request paketi sonlandırılmaktadır.

Output:

Connection to www.includekarabuk.com 80 port [tcp/http] succeeded!

HTTP/1.1 200 OK
Date: Mon, 03 Jan 2022 16:34:01 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=fa80f95b2887bb48cb240205a83c69de; path=/
Vary: User-Agent
Content-Type: text/html; charset=UTF-8

Görüldüğü üzere http request'e karşılık http response gelmiştir ve çıktıya yansımıştır. Dolayısıyla bu işlem defalarca tekrarlanırsa DOS, birçok kişi tarafından defalarca tekrarlanırsa DDOS olacaktır.

b. Telnet ile konsoldan http request yapma

> telnet www.includekarabuk.com 80

Output:

Trying 46.45.187.221...
Connected to includekarabuk.com.
Escape character is '^]'.
HEAD / HTTP/1.1 // YAZ VE ENTER'LA
// BİR KEZ DAHA ENTER'LA

HTTP/1.1 400 Bad Request
Date: Wed, 09 Nov 2016 12:26:59 GMT
Server: Apache/2.4.18 (Unix) OpenSSL/1.0.1e-fips mod_bwlimited/1.4 PHP/5.5.33
Accept-Ranges: bytes
Connection: close
Content-Type: text/html

Görüldüğü üzere http request'e karşılık http response gelmiştir ve çıktıya yansımıştır.

Dolayısıyla bu işlem defalarca tekrarlanırsa DOS, birçok kişi tarafından defalarca tekrarlanırsa DDOS olacaktır.

c. curl ile konsoldan http request yapma

> curl www.includekarabuk.com

Output:
[Web Page Content]

Görüldüğü üzere http request'e karşılık http response gelmiştir ve çıktıya yansımıştır. Dolayısıyla bu işlem defalarca tekrarlanırsa DOS, birçok kişi tarafından defalarca tekrarlanırsa DDOS olacaktır.

d. openssl ile konsoldan http request yapma

> openssl s_client -quiet -crlf -connect www.includekarabuk.com:443

Not:

-quiet : Oturum ve sertifika bilgilerinin çıktıya basımını engeller.

-crlf : “Bazı web sunucularda” gerek duyulduğundan terminalde http talebini yazarken ENTER ile gelen line feed (\n) satır atlatma karakterini CR+LF (\r\n)’ye dönüştürür.

-connect : Hedef web sunucu alan adını veya ip’sini ve akabinde port bilgisini alır.

(*) Bazı web sunucularda paketler ilk satırda sonlanmıyorsa -crlf parametresi kullanılması gerekmemektedir.

Output:

```
depth=2 C = GB, ST = Greater Manchester, L = Salford, O = COMODO CA
Limited, CN = COMODO RSA Certification Authority
verify return:1
depth=1 C = US, ST = TX, L = Houston, O = "cPanel, Inc.", CN = "cPanel, Inc.
Certification Authority"
verify return:1
depth=0 CN = includekarabuk.com
verify return:1

HEAD / HTTP/1.1                          // YAZ VE ENTER'LA
Host: www.includekarabuk.com             // YAZ VE ENTER'LA
                                         // BİR KEZ DAHA ENTER'LA

HTTP/1.1 200 OK
Date: Mon, 03 Jan 2022 16:52:02 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
```

Set-Cookie: PHPSESSID=da446028407a8a6b971bb0b90f9a0258; path=/
Vary: User-Agent
Content-Type: text/html; charset=UTF-8

Görüldüğü üzere http request'e karşılık http response gelmiştir ve çıktıya yansımıştır. Dolayısıyla bu işlem defalarca tekrarlanırsa DOS, birçok kişi tarafından defalarca tekrarlanırsa DDOS olacaktır.

Not: Openssl ile “https” talebi yapılmaktadır.

Kaynak

Tez Raporu/İnternetten Edinilmiş Kıymetli Bilgiler/Elden Geçirdiğim Notlar/Mirai Zararlısı Nedir?

https://netsec.ws/?p=292

https://osric.com/chris/accidental-developer/2018/01/using-nc-netcat-to-make-an-http-request/

https://github.com/openssl/openssl/issues/10213

https://makandracards.com/makandra/45025-how-to-make-http-https-requests-yourself-with-nc-telnet-openssl

https://unix.stackexchange.com/questions/370932/openssl-command-s-client-always-says-400-bad-request

https://stackoverflow.com/questions/1552749/difference-between-cr-lf-lf-and-cr-line-break-types

https://www.openssl.org/docs/man1.0.2/man1/openssl-s_client.html

https://www.openssl.org/

https://en.wikipedia.org/wiki/OpenSSL

https://serverfault.com/questions/1034960/is-there-an-equivalent-of-using-curl-with-a-specified-certificate-for-openssl

https://www.misterpki.com/openssl-s-client/