ÖN BİLGİ

Bu belgenin resmi adresi bulunamamıştır. Alternatif adreste yedeklenmiştir. Bu belge

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/Ddos%20Sald%C4%B1r%C4%B1lar%C4%B1%20ve%20Korunma%20Yollar%C4%B1.pdf

adresindeki makaleye çalışılarak elde edilen notlarımı kapsamaktadır. Bu çıkarılan notlar belgemde alıntılar ve/veya kişisel ilavelerim mevcuttur.

1)

Neden DDOS üzerine bir etkinlik düzenliyorsunuz Huzeyfe Önal?

Çünkü
- güvenliğin en önemli bileşeni erişilebilirliktir (availablity'dir).
- DDOS gün geçtikçe önemini arttıran bir konudur.
- DDOS tehdit sıralamasında en üstlerde yer alan bir konudur.

DDOS saldırısı yaşamadaki en büyük eksiklik
- temel ağ bilgisi eksikliği
- tecrübesizlik ve
- var olan cihazları doğru yapılandıramamadır.

(Page 3)

2)

Hatalı Bir Bilgi
- En güvenli sistem fişi çekilmiş bir sistemdir.

3)

Gelen DDOS saldırısı sizin sahip olduğunuz bant genişliğinden fazlaysa yapılabilecek çok şey yoktur. DDOS'a karşı yapılan önlemler sadece sistemin taşma noktasına gelmemesini sağlamak içindir.

NOT: DOS saldırılarını engellemek kolaydır. Lakin DDOS öyle değildir.

(Page 6, 7)

4)

DDOS görünümlü DOS saldırıları yapılabilmektedir. Yani örneğin tek bir sistemden spoof IP'lerle yapılan SYN Flood saldırıları gibi.

(Page 7)

5)

DDOS saldırısı binlerce, yüzbinlerce botnet makinesi ile gerçekleştirilir. Saldırgan kendisini botnet ağı ile gizlemiş olur. DDOS engellemesi zor bir saldırı türüdür.

(Page 8)

6)

DOS ve DDOS Hakkında Yanlış Bilinenler
- Linux DDOS'a karşı dayanıklıdır.
- Sistemimizde antivirus programı var. Kötücül yazılım bulaşmaz (Botnet olmayız).
- Donanım tabanlı firewall'lar DDOS'u engeller.
- Bizim IPS tek başına DOS'u ve DDOS'u engeller.

DOS ve DDOS engellenemez.

(Page 9)

7)

Yapılan çalışmalar DDOS saldırıların çok küçük bir kısmının bandwidth şişirme yöntemiyle gerçekleştiğini ortaya koymaktadır.

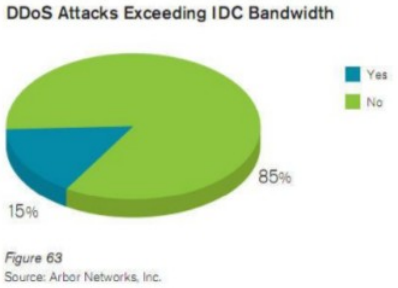


Figure 63
Source: Arbor Networks, Inc.

Attack Subclass	Number of Attacks	Percentage
Total Traffic	209	22.1%
TCP SYN	371	39.3%
TCP RST	49	5.2%
Protocol	12	1.3%
other	260	27.5%
DNS	23	2.4%
Bandwidth	20	2.1%

Resimde görüldüğü üzere TCP SYN, TCP RST,... gibi saldırılar çoğunluktayken bandwidth taşırma saldırıları sadece %2.1 'dir.

Benim Not: Hatırlarsan TCP SYN hedef sistemin bandwidth'ini değil RAM'ini taşırıyordu.

(Page 10)

8)

DOS veya DDOS saldırılarında amaç sistemlere sızma değildir. Amaç hedef sistemi, hedef sisteme giden yolları işlevsiz kılmadır. Örneğin epostaların hedefe gidememesine, telefon sistemlerinin hep meşgul vermesine, bankacılık sistemlerinde transaction'ların çalışamamasına neden olmak gibi....

(page 11)

9)

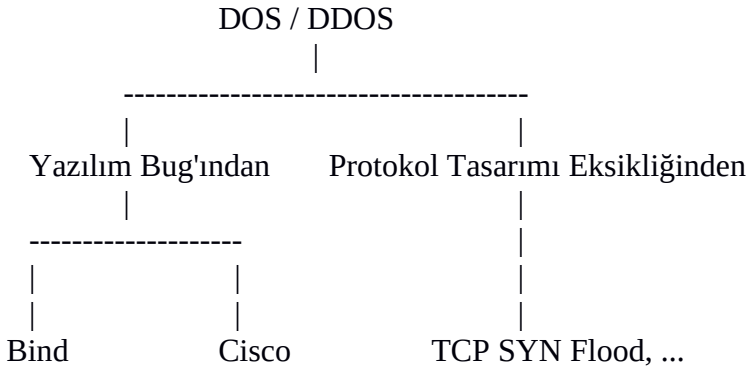
DOS ya da DDOS Niye Yapılır?

- Sistemde güvenlik açığı bulunamadığında zarar vermek amacıyla bu yola başvurulabilir.
- Politik sebeplerden ötürü bu yola başvurulabilir.
- Ticari rekabetten dolayı bu yola başvurulabilir.
- Keyfi & İmaj dolayısıyla bu yola başvurulabilir.

(Page 12)

10)

DOS ya da DDOS Neyden Kaynaklanır?



Bind: DNS Sunucu Yazılımı
Cisco: Cisco cihazlarının yazılımları

(Page 13)

11)

DOS veya DDOS saldırılarının yapılabilmesindeki temel sebep zamanında protokol tasarımlarının güvenlik kaygısıyla oluşturulmamış olmasıdır. Şimdi ise OSI layer'ındaki bir katmanda yapılacak güncelleme eski OSI Layer'ları kullanan tüm bilişim cihazlarını işlevsiz kılacaktır. İşte bu çıkmaz sokaktan dolayı DOS veya DDOS başımızdan tam anlmıyla savamadığımız bir problemdir.

12)

DOS Sadece İnternette mi Geçerlidir?
DOS temelde bir saldırı şeklidir ve ağ kavramının geçerli olduğu her ortamda gerçekleştirilebilir.

(page 14)

13)

DOS saldırıları
- yerel ağda gerçekleşir.
- kablosuz ağda gerçekleşir.
- internet ağında gerçekleşir.

(page 14)

14)

Yerel Ağlarda DOS Nasıl Yapılır
Yerel ağlarda zorunlu bir kullanıma sahip ARP protokolü yapısı gereği bir kontrole sahip olmadığından cihazların birbirlerini yanlış tanımalarına olanak verebilmektedir.

Yerel ağda DOS saldırısı kısmına gelecek olursak Yerel ağdaki tüm sistemlere arp paketleri ile router'ın MAC'ini yanlış gösterirsek – yani man in the midde değil de, tek yönlü bir arp spoofing yaparsak – ağdaki host'ların router'la irtibatını koparmış oluruz. Böylece yerel ağda komple DOS saldırısı yapılmış olacaktır. Ancak bu göndereceğimiz zararlı ARP paketlerini bir defa değil tekrar tekrar göndermek durumundayız. Aksi takdirde host'lar internet bağlantılarını düzeltmek için ARP broadcast'i yaparak tekrar router'ı bulabilirler ve bağlantılarını onarabilirler. O yüzden tekrar tekrar zararlı ARP paketini göndererek DOS saldırısı yerine getirilmiş olacaktır.

Yerel ağlarda bahsettiğimiz DOS'ları yapmak için nemesis tool'unu kullanabiliriz:

```
> nemesis arp -d eth0 -r -v -S 10.20.1 -D 10.2.0.255 -H 00:01:02:03:04:05
        -M FF:FF:FF:FF:FF:FF
```

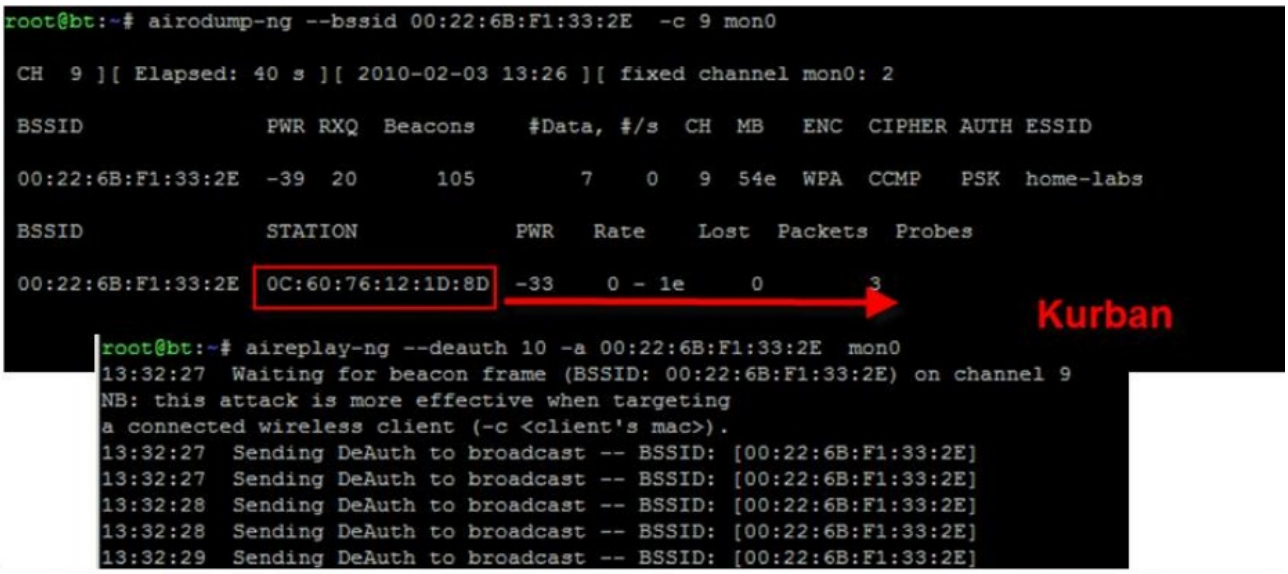
Bu tool'un bu şekilde kullanımının arkasında yatan fikir şu şekildedir: nemesis ile bir ARP paketi hazırlıyoruz. Bu arp paketinin kaynak IP kısmına (-S parametresine) router'ın IP'sini koyuyoruz. Böylece bu ARP paketini alacak cihazlar paketin router'dan geleceğini sanacaklar. Sonra hazırlamakta olduğumuz ARP paketinin hedef IP kısmına ise (-D parametresine) broadcast adresi koyuyoruz. Böylece yerel ağdaki tüm cihazlara hazırladığımız paketin gitmesini sağlamış oluyoruz. -H ile router'dan geldiği sanılan paketin içerisine güya router'ın MAC'ini koyuyoruz. Böylece bu arp paketini alacak host'lar router'dan geldiğini sandıkları ARP paketinin içerisindeki sözde MAC'i arp tablolarına router'ın MAC'i diye not düşeceklerdir. Bunun sonucunda host'lar ne zaman internet paketi yollamaya kalksalar yanlış MAC'e paketlerini yollayacaklarından, yani router'ın MAC'inini yanlış bildiklerinden paketleri router'a ulaşamayacaktır ve internet erişimi sağlayamacaklardır. Bunun nihayetinde DOS atağı yerel ağda amacına ulaşmış olacaktır.

(page 15)

15)

Kablosuz Ağlarda DOS
Kablosuz ağlarda kullanılan protokol güncel olsun veya olmasın – WEP/WPA/WPA2 farketmez – ağın içerisinde üye host'lara DOS yapmak mümkündür. Örneğin aircrack-ng ailesinden olan airomon-ng ile makinamızı monitor moda geçirip airodump-ng ile kablosuz ağdaki cihazları sıraladıktan sonra içlerinden herhangi birinin MAC'ini seçip aireplay-ng ile o MAC adresine (o host'a) router'dan geliyormuş gibi deauthenticate paketlerini gönderebiliriz ve böylece router'la olan

iletişimini koparabiliriz. Göndereceğimiz deauthenticate paketlerini tekrar tekrar gönderirsek o kadar süre bağlantısı kopuk kalacaktır. O yüzden deauthenticate gönderim sıklığı cihazın router'la olan bağlantısını onarma hızını aşarsa DOS işlemini başarıyla gerçekleştirebilmiş olacağız.



Yukarıda görüldüğü üzere ilk resimde kurbanın MAC adresi seçiliyor. Ardından o MAC adresine ikinci resimde görüldüğü gibi 10 tane deauthenticate paketi gönderiliyor ve cihazın router'la olan bağlantısı koparılıyor. Bu 10 sayısı ne kadar çok olursa cihaz o kadar internet erişimi sağlayamacaktır ve DOS amacına ulaşmış olacaktır.

(Page 16)

16)

C&C Server
"Command and Control" (C&C) servers are centralized machines that are able to send commands and receive outputs of machines part of a botnet. Anytime attackers who wish to launch a DDoS attack can send special commands to their botnet's C&C servers with instructions to perform an attack on a particular target, and any infected machines communicating with the contacted C&C server will obey by launching a coordinated attack.

Note : “command and control” demek komuta ve kontrol demekmiş.

https://security.radware.com/ddos-knowledge-center/ddospedia/command-and-control-server/

17)

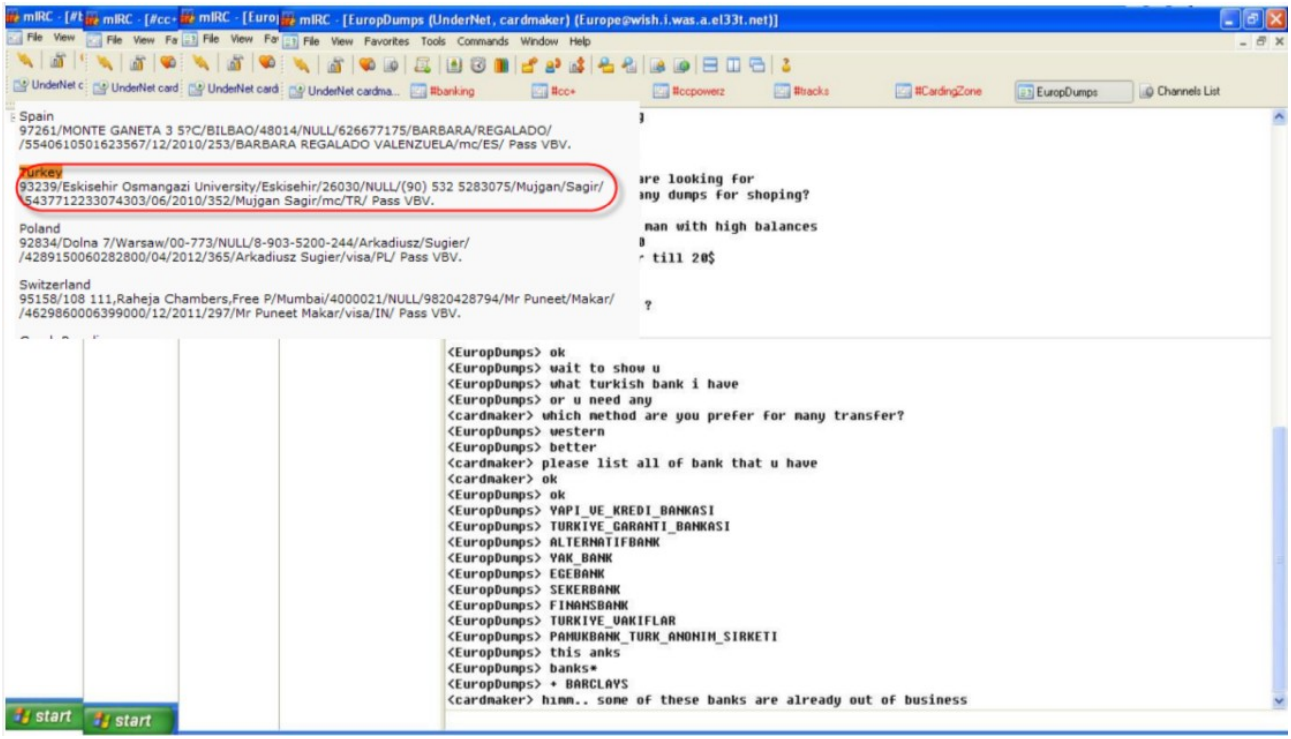
Botnet Kullanma Nedenleri
- SPAM yapmak için kullanılırlar.
- Google reklamlarından daha fazla para kazanmak için kullanılırlar.
- Google adword servisinde ilk sıralara oynamak için kullanılırlar.
- Anketlere flood yaparak manipule etmek için kullanılırlar.
- DDOS yapmak için kullanılırlar.

- Kumandan adına bilgi çalma amacıyla kullanılabilirler.
- Geliştirilen bir malware'i yaymak amacıyla kullanılabilirler.

(Page 21)

18)

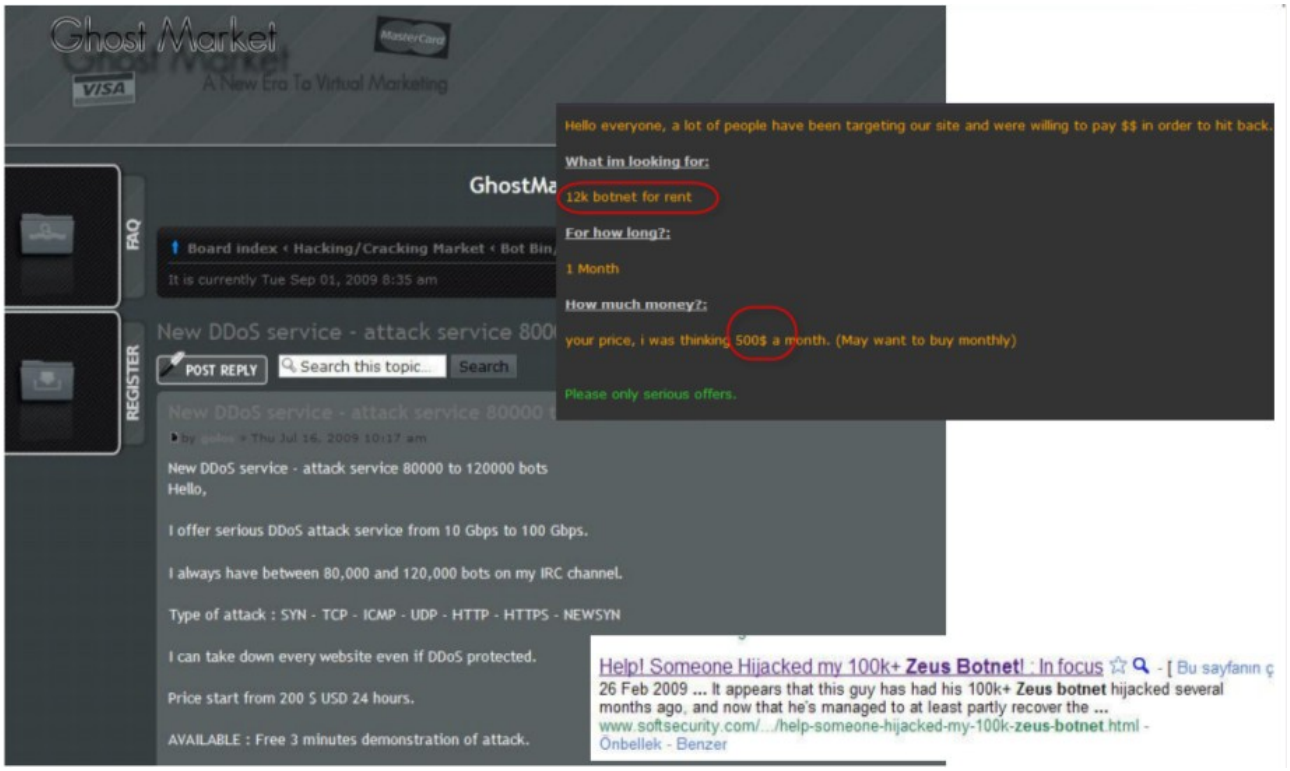
Aşağıda hacker'ların kullandığı iletişim kanalı olan IRC üzerinden botnet'lerce çalınan kredi kartı bilgileri yer almaktadır:



(Page 22)

19)

Aşağıda botnet alım satımlarının yapıldığı bir web sitesi görmektesin:

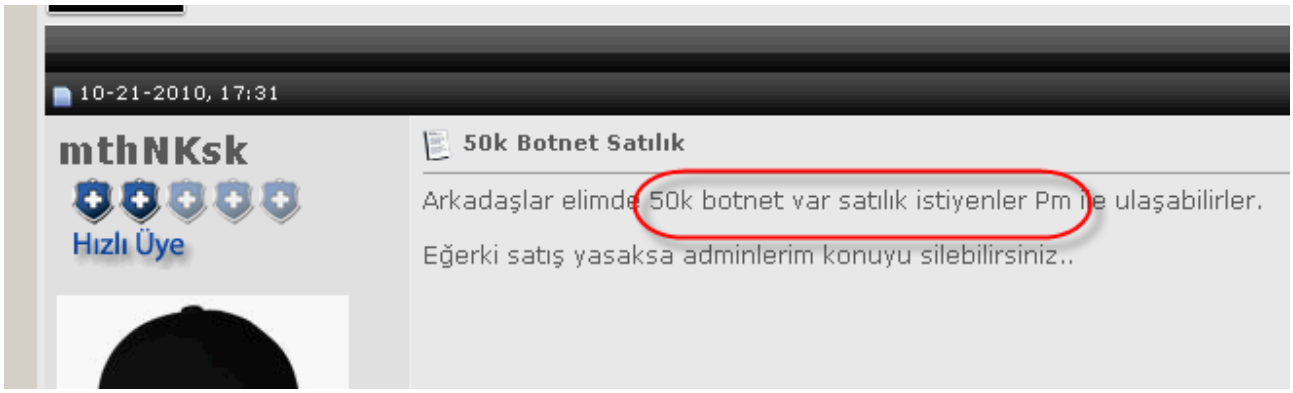


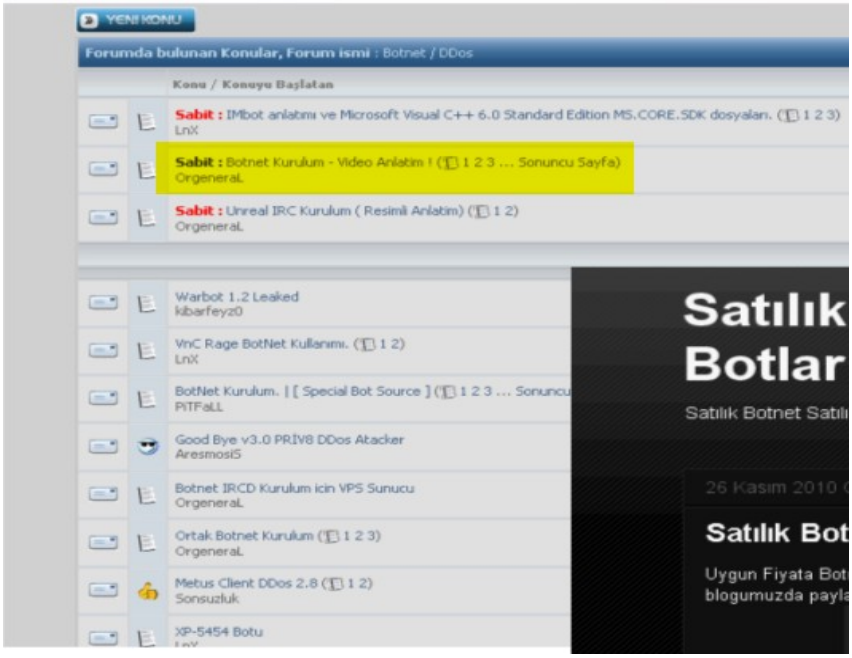
Sağ alt köşede oluşturduğu botnet'in çalındığını söyleyen bir arama sorgusu görmektesin.

(page 23)

20)

Türkiye'de botnet piyasasına dair bazı örnekler



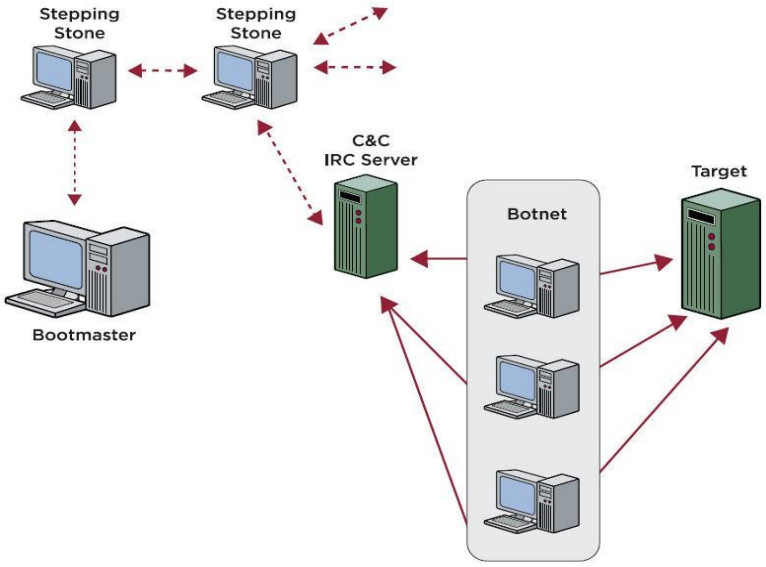


Yukarıdaki son resimde gördüğün üzere Botnet Nasıl Kurulur şeklinde forumlarda konu başlıkları yer alabilmektedir.

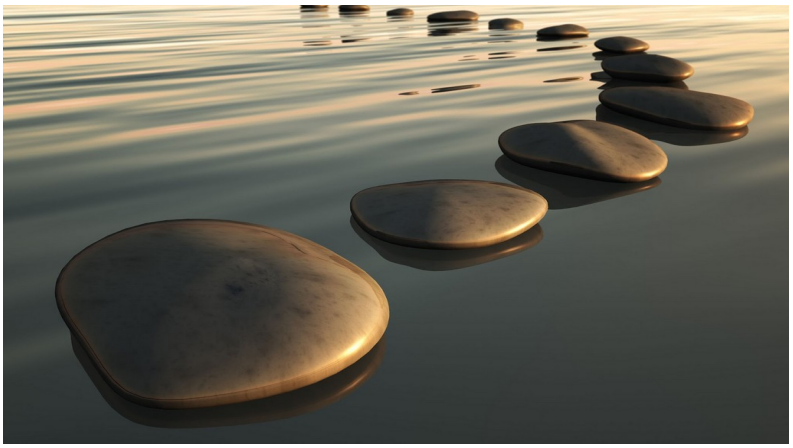
(Page 24)

21)

C&C sunucusunun yer aldığı bir botnet ağı:



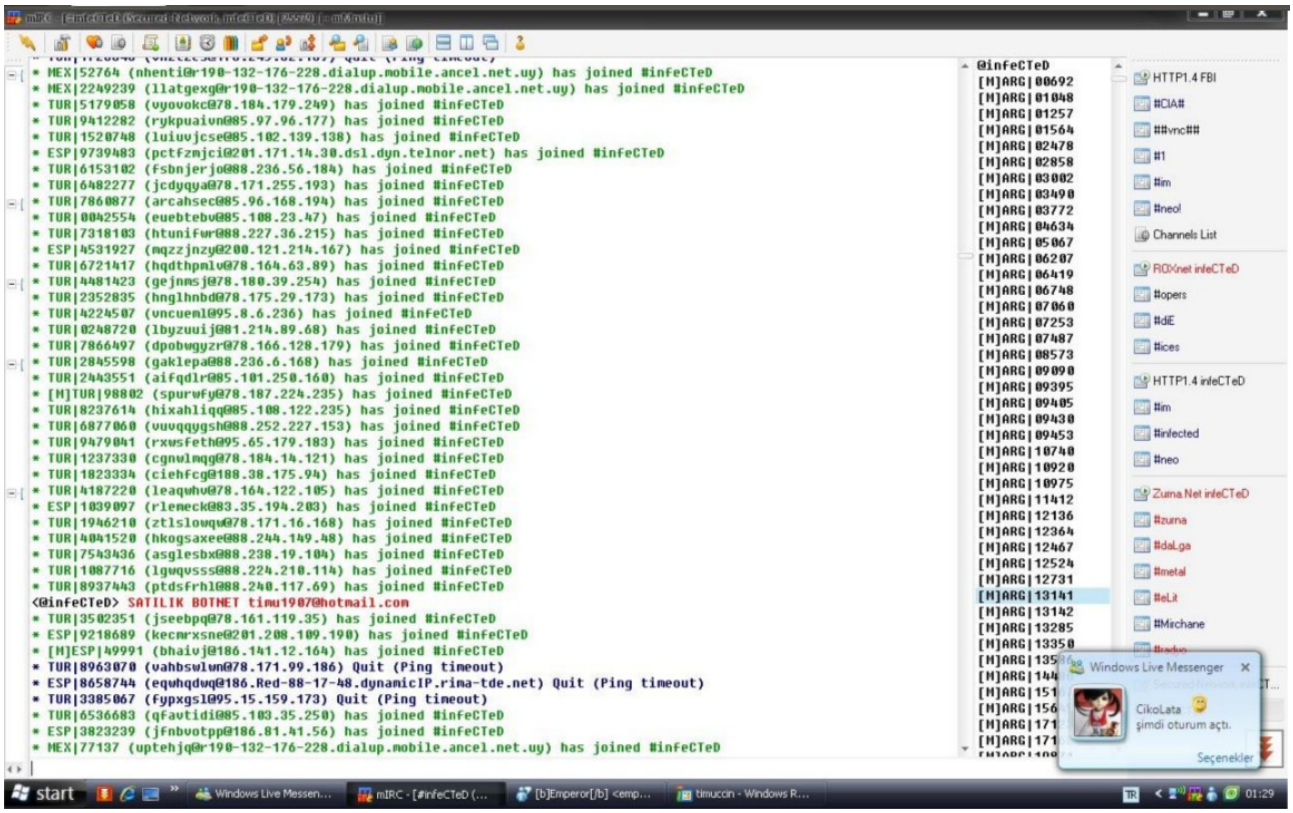
NOT: Stepping stone bir nevi tehlikeli alana giderken su yüzeyinde adım atılabilecek taşlar gibidir.



(Page 25)

22)

Botnet cihazları IRC ile çalıştırılır. Yani IRC programı üzerinden botnet'ler yönetilebileceği gibi bir web tabanlı IRC sayfası üzerinden de yönetilebilir. Aşağıda IRC üzerinden botnet'lerin yönetimine dair bir görüntü görmektesin:



http://www.cyber-warrior.org/forum/botnet-genis-anlatim-_408702,0.cwx
(Page 26)

23)

Botnet Kurmaya Dönük Bir Örnek
Haziran ayında çok kullanılan Wordpress portal'ının Türkçe web sayfası hack'lendi. Hacker'lar bu hack işlemi ile hedef sunucuya sızıp bir sonraki wordpress blog sürümüne uzaktan yönetim amaçlı kod yerleştirdiler. İlgili siteden son sürüm wordpress blog paketini indiren herkes sistemlerini hacker'ların yönetimine teslim etmiş oldular.

(Page 27)

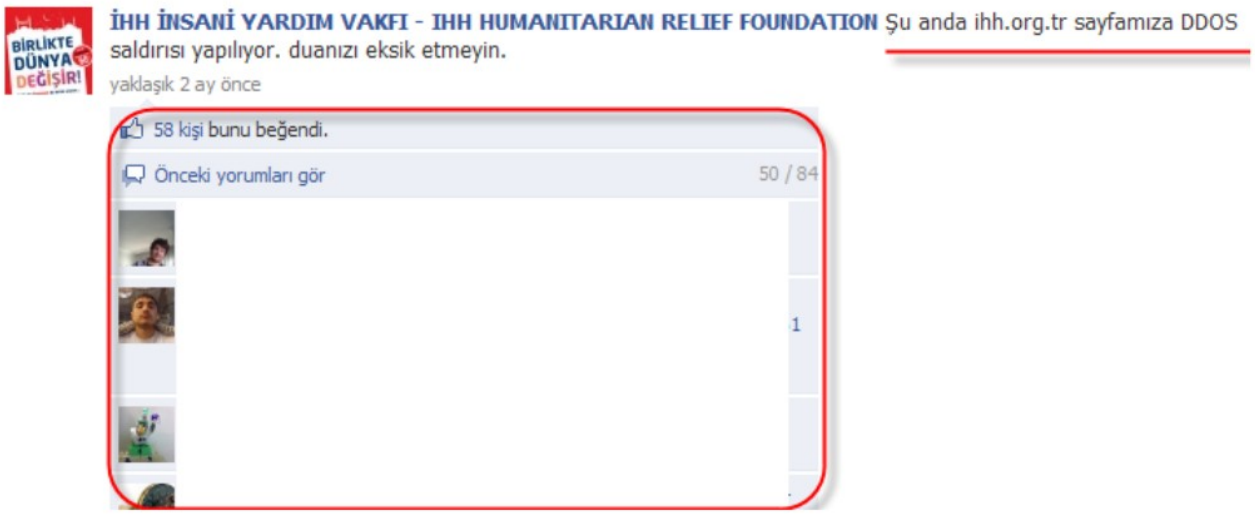
24)

2007 yılında Root DNS sunucularına DDOS saldırısı yapılmıştır.

(Page 30)

25)

2010 Yılında Mavi Marmara olayından sonra İsrail IP adreslerinden bize ciddi miktarda DDOS saldırısı yapıldı. Örneğin İHH'ya dönük yapılan DDOS saldırısı sonrası IHH yetkilisinin döndüğü cevap:



Bunun üzerine Türkiye'den gönüllülerin oluşturduğu ekip tarafından DDOS saldırısı düzenleniyor ve İsrail'in hükümet siteleri ulaşılamaz duruma getiriliyor. İsrail'li yetkililer bunun üzerine Türkiye'den gelen istekleri engelleyerek saldırıyı dindirdiler.

İsrail Türkiye'den gelen istekleri engellediğinde İsrail sitesine Türkiye'den yapılan telnet teşebbüsü başarısız olurken

huzeyfe@kali ~$ telnet www.mod.gov.il 80

Output:

Trying 195.160.241.193
telnet: connect to address 195.160.241.193: Operation time out
telnet: Unable to connect to remote host

Amerika'dan yapılan telnet teşebbüsü başarılı olmuştu:

huzeyfe@server ~$ telnet www.mod.gov.il 80

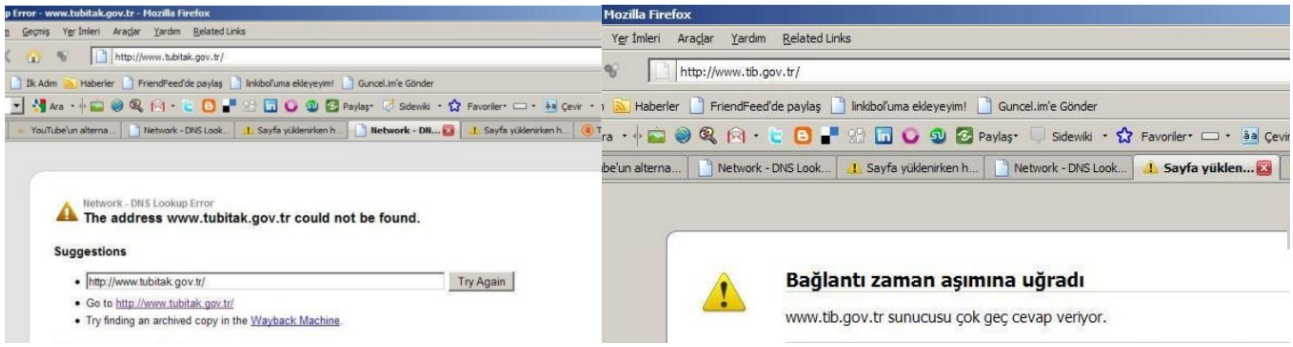
Output:

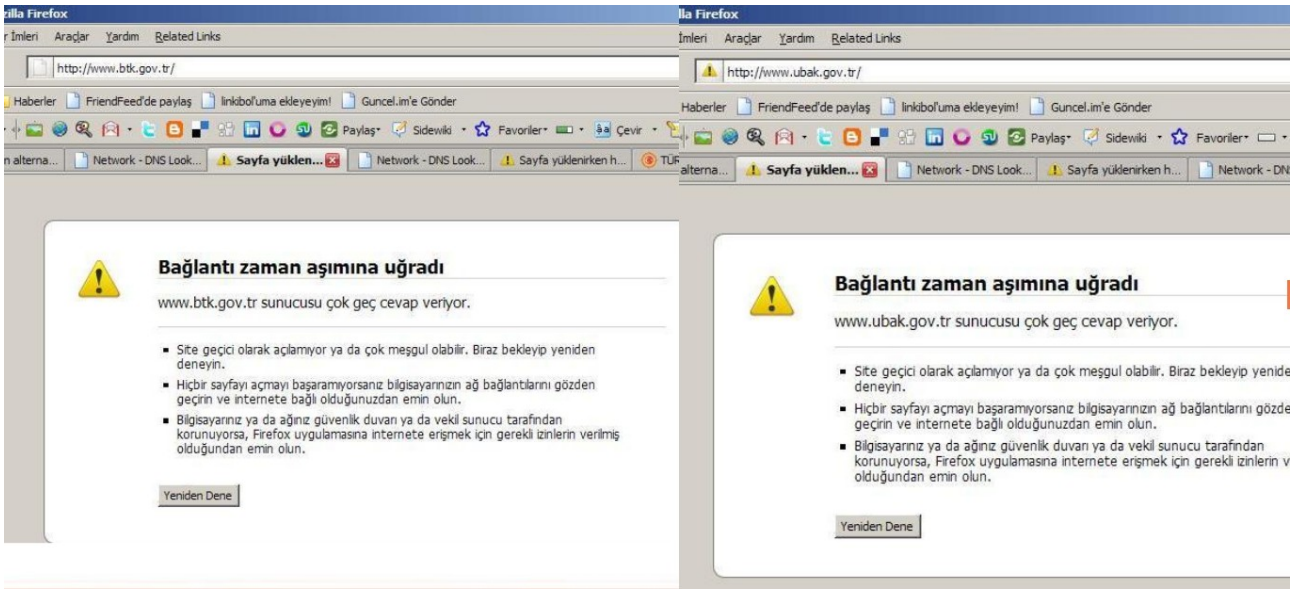
Trying 195.160.241.193
Connected to www.mod.gov.il (195.160.241.193)
Escape character is '^]'

(Page 31-32)

26)

Devlet Sitelerine Yönelik Toplu DDOS





(Page 34)

27)

Wikileaks olayının patlak vermesi sonrası çift taraflı DDOS saldırıları başladı. Bir taraf Wikileaks.org sistemlerine yönelik DDOS atağı yaparken diğer taraf Wikileaks'i savunmak üzere DDOS atağı yaptı. Wikileaks'i savunmak adına DDOS'a destek vermek için gönüllü kişiler botnet kurulumu yaptılar ve kendilerini botnet ağlarına zombi olarak kattılar. Böylece tarihte ilk defa zombi sayısı çok yüksek seviyeye ulaştı. Ancak gönüllü olarak botnete katılanların IP adresleri kayıt altına alındı.

(Page 38)

28)

Yerli hacker'lar henüz kurumsal sistemlere yönelik DDOS saldırılarına başlamadılar. Genellikle yerli hacker'lardan hosting firmalarına ve e-ticaret sitelerine yönelik DDOS saldırıları görülmektedir.

(Page 40)

29)

DDOS atak çeşitleri temelde iki sınıfa ayrılır:

1. Bandwidth Doldurmaya Dönük DDOS
    - UDP Flood, ICMP Flood vs...
2. Kaynak Tüketmeye Dönük DDOS
    - Syn Flood, ACK/FIN Flood, GET/POST Flood, UDP Flood, DNS Flood

(Page 41, 43)

30)

Bandwidth Şişirmeye Dönük DDOS // Hatları yorma
- Önlemenin yolu yoktur.
- Internet Service Provide (ISP) seviyesinde engellenebilir.
- L7 protokollerinden yararlanılarak gelen DDOS ataklarındaki trafik çeşitli yöntemlerle 6'da birine düşürülebilir.

Kaynak Tüketmeye Dönük DDOS // Cihazları Yorma
- Amaç ağ güvenlik sistemlerinin kapasitesini zorlama ve kaldıramayacakları yük bindirmedir.
- Session bilgisi tutan ağ güvenlik cihazlarını session'a boğma yapılabilir

(Page 46)