



Dağıtık Servis Dışı Bırakma (DDoS) Saldırıları ve Korunma Yöntemleri

Bâkır EMRE
Uzman Araştırmacı

6. Kamu Kurumları Bilgi Teknolojileri Güvenlik Konferansı

TÜBİTAK, Feza Gürsey

8 Haziran 2011

- Siber Tehditler
- DoS Nedir?
- DDoS Nedir?
- Türkiye' de ve Dünya'da Belirtileri
- DDoS Çeşitleri
- Önlem Mekanizmaları
- Sonuç

286+ Milyon

Tehdit



Çok biçimlilik ve Web saldırı araçları gibi yeni dağıtım mekanizmaları, kötü amaçlı yazılım program varyantlarını artırmaya devam ediyor. 2010 yılında Symantec 286 milyon yeni, birbirinden farklı zararlı program tespit etti.

% 93 Artış

Web Saldırılarındaki

Websaldırı araç setlerinin hızlı artışı, Web-tabanlı saldırılarının 2010 yılında bir önceki yıla göre %93 oranında artış göstermesine neden oldu. Kısaltılmış URL'lerin kullanımı da bu artışta etkili oldu. 2010 yılındaki 3 aylık gözlem döneminde i ağlar üzerinde gözlemlenen kötü niyetli URL'lerin %65 i kısaltılmış URL'lerden oluşuyordu.

260,000

Her sızıntıda açığa çıkan kimlik sayısı

Yıl boyunca yaşanan saldırılarla gerçekleştirilen veri sızıntısı vakalarının her birisinin sonucunda ortaya çıkan ortalama kimlik sayısı



%42

Daha Fazla Mobil açık

Belirtiler, siber uzayın hem güvenlik araştırmacılarının hem de siber suçluların daha fazla ilgisini çekmeye başladığını gösteriyor. Zira bildirilen yeni mobil işletim sistem açıkları sayısı 2009 yılındaki 115 iken, çok keskin bir yükselişte 2010 yılında 163 e ulaştı



6,253

Yeni açık

Symantec 2010 yılında daha önceki hiç bir raporlama döneminde olmadığı kadar çok yeni açık saptadı. Daha da ötesinde yeni çözüm sağlayıcılar bir önceki yıla oranla %161 lik bir artışla 1.914 e ulaşan açıklardan etkilendiler.



14

Yeni Sıfır-gün Açığı

2010 yılında Internet Explorer, Adobe Reader ve Adobe Flash Player gibi yaygın olarak kullanılan uygulamalarda 14 yeni 0 gün açığı bulundu. Endüstriyel Kontrol Sistem yazılımı da istismar edildi. Stuxnet tek başına dört farklı sıfır-gün açığından yararlanması, ne kadar sofistike bir yapıya sahip olduğunun da bir göstergesi oldu.

%74

Eczacılık Sektörüne Yönelik Spam

2010 yılında saptanan tüm spam lerin neredeyse üçte biri eczacılık ürünlerine ilişkindi



1 Milyon +

Bot Bilgisayar

2010 yılında gözlemlenen en geniş botnet Rustock'un bir milyondan fazla bot u yönettiği gözlemlendi. Grum ve Cutwail gibi bunu izleyen diğer botnet'lerin her birisinin kontrolünde de yine yüzbinlerce bot bulunuyordu.



15\$

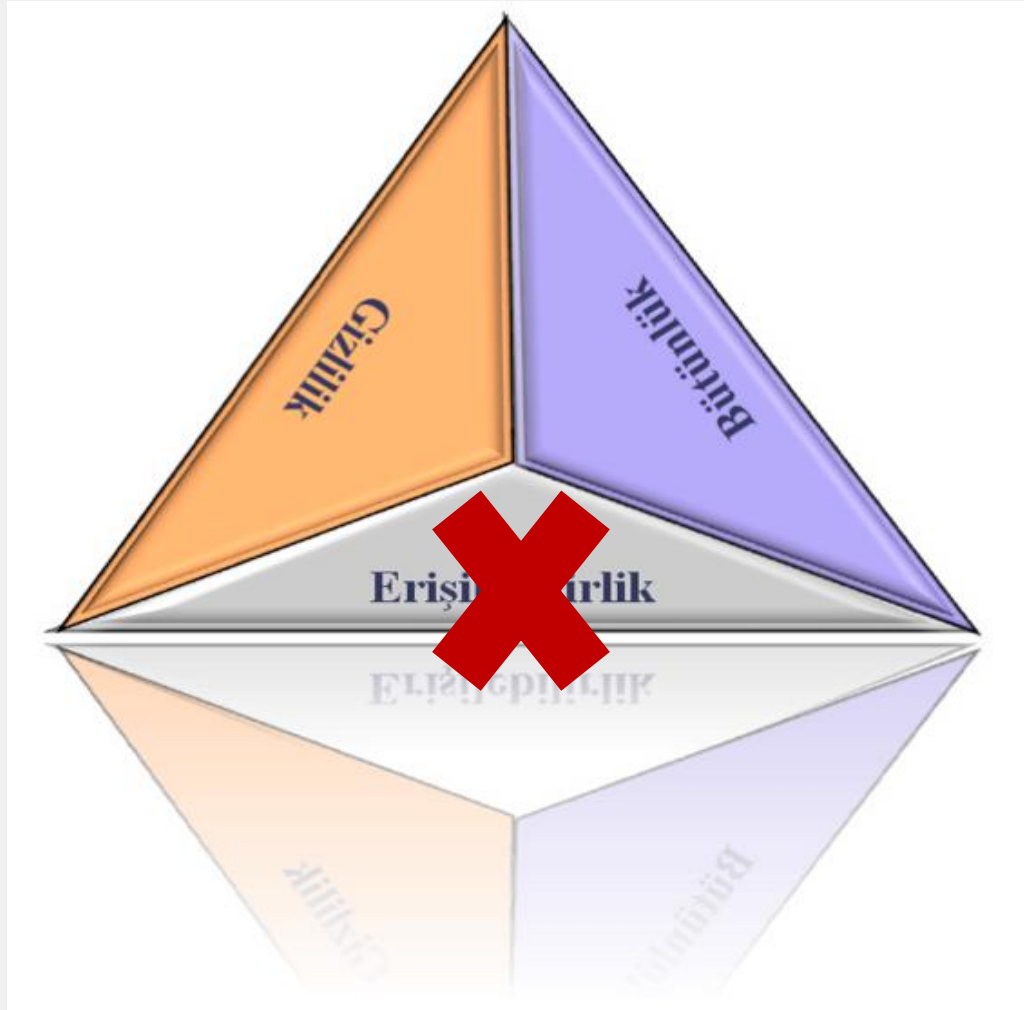
Her 10.000 Bot Bilgisayarın Fiyatı

Symantec 2010 yılında yeraltı forumlarında yer alan bir reklamda 10.000 bot-enfekte bilgisayarın liste fiyatının 15 Dolar olarak belirlendiğini gözlemledi. Tipik olarak spam ve rougware kampanyalarında yararlanan bot bilgisayarlar, 2010 yılında giderek artan biçimde DDoS atakları için de kullanılmaya başladı.

0.07-100\$

Her Bir Kredi Kartının Fiyatı

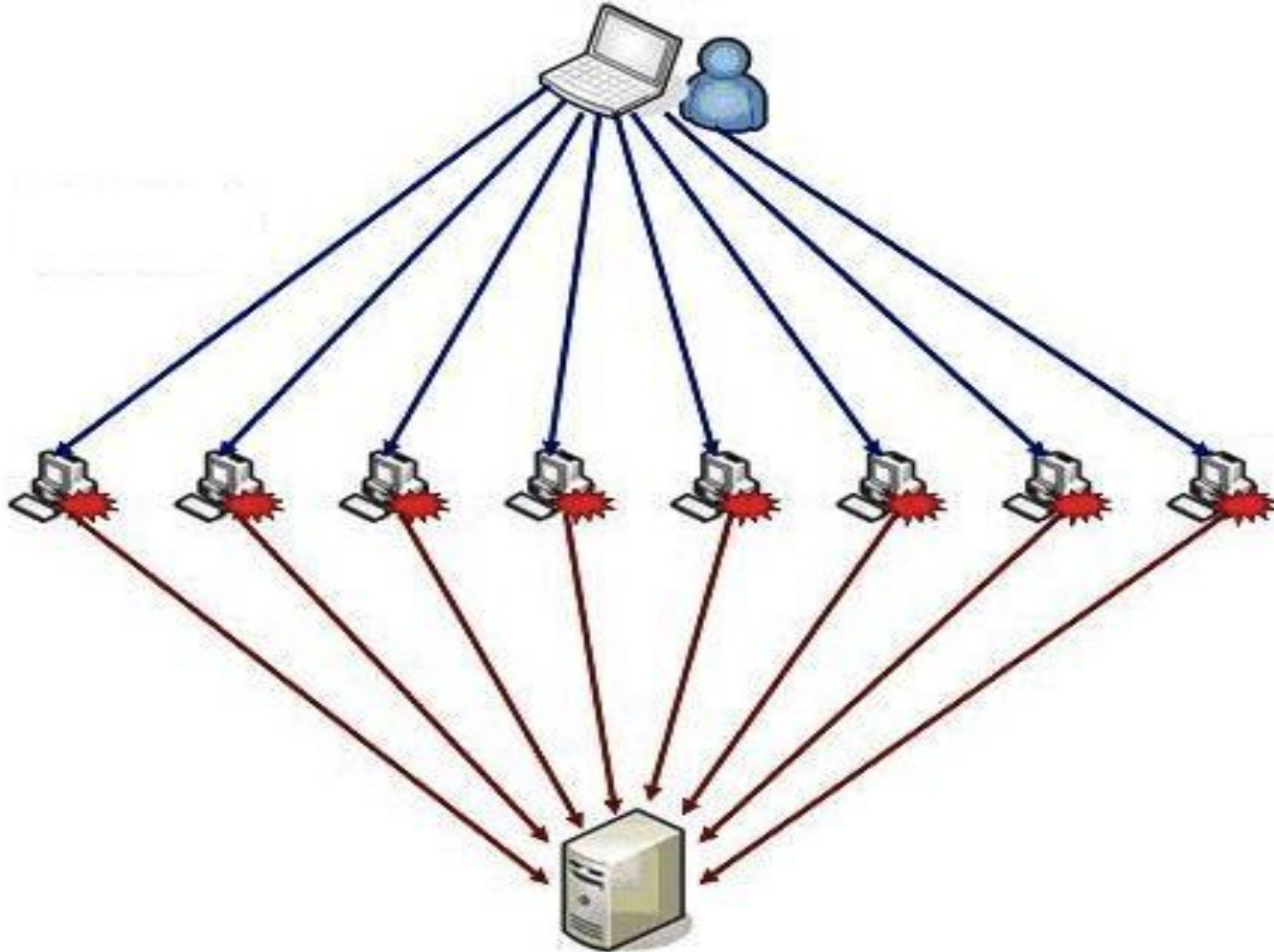
Bunlar, yer altı ekonomisinde her "çalınan" kart için ilan edilen fiyatlar. Aynen gerçek ekonomilere olduğu gibi, toplu alımlarda alıcılara indirimler de uygulandı.



Hedef olarak belirlenen sistemin kaynaklarını tüketerek temel görevini yerine getirememesini sağlamak için yapılan ve bilgi güvenliğinde erişilebilirliği hedef alan atak türüdür.

DDoS – Dağıtık Servis Dışı Bırakma Saldırıları

Koordineli olarak gerçekleşen, Botnet'lerin veya gönüllülük esasıyla oluşturulan ağdaki binlerce sistemin, kurban olarak belirlenen hedefe aynı anda saldırılmasına dağıtık servis dışı bırakma atağı denir.



- Bilinen ilk DDoS atađı 1999 yılında Minnesota Üniversitesi öğrencileri tarafından gerçekleştirildi
- 2000 – CNN, Yahoo, EBay, Datek gibi siteleri hedef alan ve Trinoo, TFN, StachleDraht, TFN2K gibi araçlar kullanılarak gerçekleştirildi.
- 2002 – Kök DNS sunucularını hedef alan DDoS atađı gerçekleştirildi.
- 2007 – Kök DNS sunucularını hedef alan 2. DDoS saldırıları
- 2007 – Estonya siber saldırıları
- 2008 – Gürcistan siber saldırıları
- 2010 – Wikileaks, Mavi Marmara, TİB, BTK, TÜBİTAK
- 2011 – PlayStation Network

```
$telnet www.mod.gov.il 80
```

```
Trying 195.160.241.193...
```

```
telnet: connect to address 195.160.241.193: Operation timed out
```

```
telnet: Unable to connect to remote host
```

```
Trying 195.160.241.193...
```

```
Connected to www.mod.gov.il (195.160.241.193).
```

```
Escape character is '^]'.  
^C
```

TARGET: **WWW.xxxxx.COM**: WEAPONS <http://xxx.xx.ru> FIRE FIRE FIRE!!!



Anon_Operation

CURRENT TARGET:
WWW.VISA.COM :: WEAPONS
<http://bit.ly/e6iR3X> ::: SET YOUR
LOIC TO --> irc.anonops.net &
FIRE FIRE FIRE!!! #WIKILEAKS
#DDOS

30 Nov ☆ Favorite ↶ Reply 🗑 Delete



wikileaks WikiLeaks ↻ by bemre

DDOS attack now exceeding 10 Gigabits a second.

30 Nov ☆ Favorite ↻ Undo Retweet ↶ Reply



wikileaks WikiLeaks ↻ by bemre

We are currently under a mass distributed denial of service attack.

28 Nov

ntvmsnbc

İstanbul 29°C / 19°C
değiştirCANLI
YAYINCANLI
YAYIN

ntvmsnbc'de ara



Seçim 2011 · Türkiye · Dünya · Ekonomi · Teknoloji · Kültür Sanat · NTV Spor · NTV Bilim · Yaşam · Sağlık · Eğitim

FOTO

VIDEO



Anasayfa / Teknoloji / İnternet

Güncelleme: 11:07 TSİ 07 Haziran, 2011 Salı

Kategoriler

Seçim 2011

Türkiye

Dünya

Ekonomi

Kültür Sanat

Teknoloji

İnternet

Hi-Tech

Mobil Yaşam

Bilişim

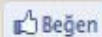
Ürün Rehberi

Yazılım - Oyun

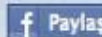
Kurumsal

Konsept-Yenilik

NTV Spor



3.545 kişi bunu beğendi. Arkadaşların arasında beğenen ilk sen ol.



3267



575

Anonymous'tan Türkiye'ye uyarı

İnternet sansürüyle Türkiye'nin temel hak ve özgürlükleri ihlal ettiğini söyleyen Anonymous (Anonim) "Sansür uygulayan kurumlara karşı harekete geçeceğiz" dedi.

#OPERATION TURKEY

Merhaba Türkiye,

Over the last few years, we have seen how the Turkish government has tightened its grip on the internet. It has blocked thousands of websites and blogs while abusive legal proceedings against online journalists persist. The government now wants to impose a new filtering system on the 22nd of August that will make it possible to keep records of everyone's internet activity.

Though it remains opaque why and how the system will be put in place, it is clear that the government is taking censorship to the next level.

These acts are inexcusable. Accessing and participating in the free flow of information is a basic human right. Anonymous will not stand by while the Turkish government violates this right. We will bring our support to circumvent censorship and retaliate against organizations imposing censorship.

Hundreds of thousands of people have protested against internet censorship but AKP government ignored the voice of the people and violently oppressed the protesters.

[Browse networks](#) > [AnonOps](#) > [#opTurkey](#)

Channel information

Network Name: AnonOps

Channel Name: #opTurkey

[Register](#) | [Home](#) | [My Polls](#) | [Create Poll](#) | [Login](#)



Tip: You can add any poll you see on Twiigs to your own website. Simply click on the "embed" link and follow the instructions on the proceeding page.

Status

- All
- Open
- Closed

Categories

- All
- Autos
- Beauty & Style
- Business
- Education
- Entertainment
- Finance
- Food
- Health
- Home & Garden
- Literature
- Local

Home

Most Popular

Most Recent

My Polls

[Create Poll](#)

Time: **Today** | [This Week](#) | [This Month](#) | [All Time](#)

All Polls

results 1 - 9 of 778

Who Was Your Best Dressed At The 2011 MTV Movie Awards?

- Selena Gomez in Giambattista Valli
- Rosie Huntington-Whiteley in Dolce & Gabbana
- Emma Stone in Bottega Veneta
- Kristen Stewart in Balmain
- Leighton Meester in Balmain
- Emma Watson in Marchesa
- Blake Lively in Michael Kors
- Mila Kunis in Balmain

Created on Jun 5, 2011

Vote

[View Results](#)

[more info](#)

[comment](#) | [embed](#) | [email](#)

Which target do we hit first?

- <http://www.tib.gov.tr/> 54%
- <http://www.osym.gov.tr/> 22%
- <http://www.tbmm.gov.tr/> 11%
- <http://www.turkiye.gov.tr/> 11%

Created on Jun 7, 2011

Total Votes: 1,518

Vote

[more info](#)

[comment](#) | [embed](#) | [email](#)

What should be the first target? / ilk hedef ne olmalı?

- <http://www.tib.gov.tr/> 44%
- <http://www.turkiye.gov.tr/> 6%
- <http://www.zaman.com.tr/> 9%
- <http://www.akparti.org.tr/> 34%
- <http://www.ihbarweb.org/> 5%

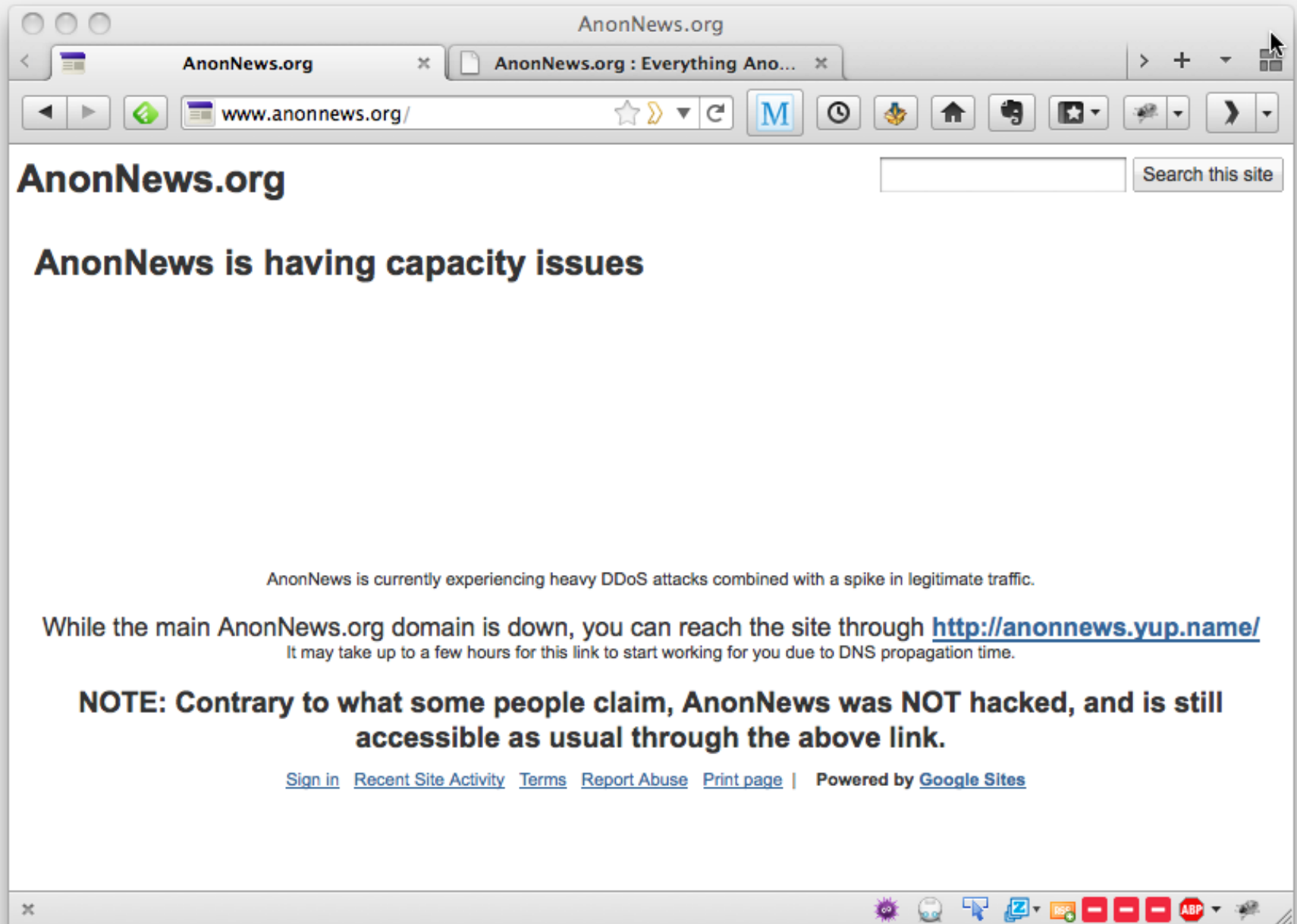
Created on Jun 7, 2011

Total Votes: 1,476

Vote

[more info](#)

[comment](#) | [embed](#) | [email](#)



The screenshot shows a web browser window with the title "AnonNews.org". The address bar displays "www.anonnews.org/". The main content area features the heading "AnonNews.org" and a search bar. Below this, a large heading reads "AnonNews is having capacity issues". A paragraph of text states: "AnonNews is currently experiencing heavy DDoS attacks combined with a spike in legitimate traffic." This is followed by a message: "While the main AnonNews.org domain is down, you can reach the site through <http://anonnews.yup.name/> It may take up to a few hours for this link to start working for you due to DNS propagation time." A bold note follows: "NOTE: Contrary to what some people claim, AnonNews was NOT hacked, and is still accessible as usual through the above link." At the bottom, there are links for "Sign in", "Recent Site Activity", "Terms", "Report Abuse", and "Print page", along with the text "Powered by Google Sites". The browser's taskbar at the bottom shows various system icons, including a virus icon, a clock, and several application icons.

AnonNews.org

www.anonnews.org/

AnonNews.org

AnonNews is having capacity issues

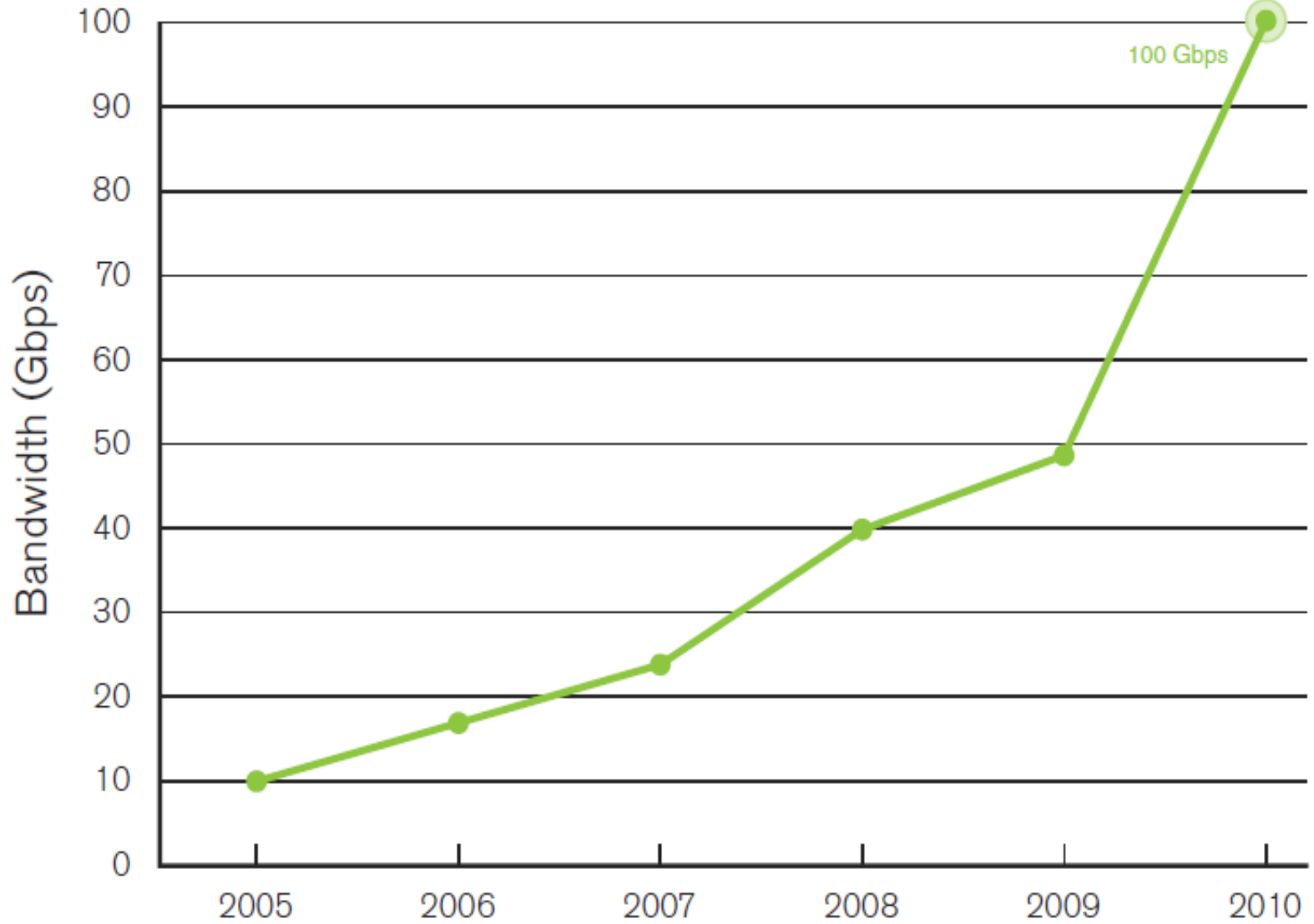
AnonNews is currently experiencing heavy DDoS attacks combined with a spike in legitimate traffic.

While the main AnonNews.org domain is down, you can reach the site through <http://anonnews.yup.name/>
It may take up to a few hours for this link to start working for you due to DNS propagation time.

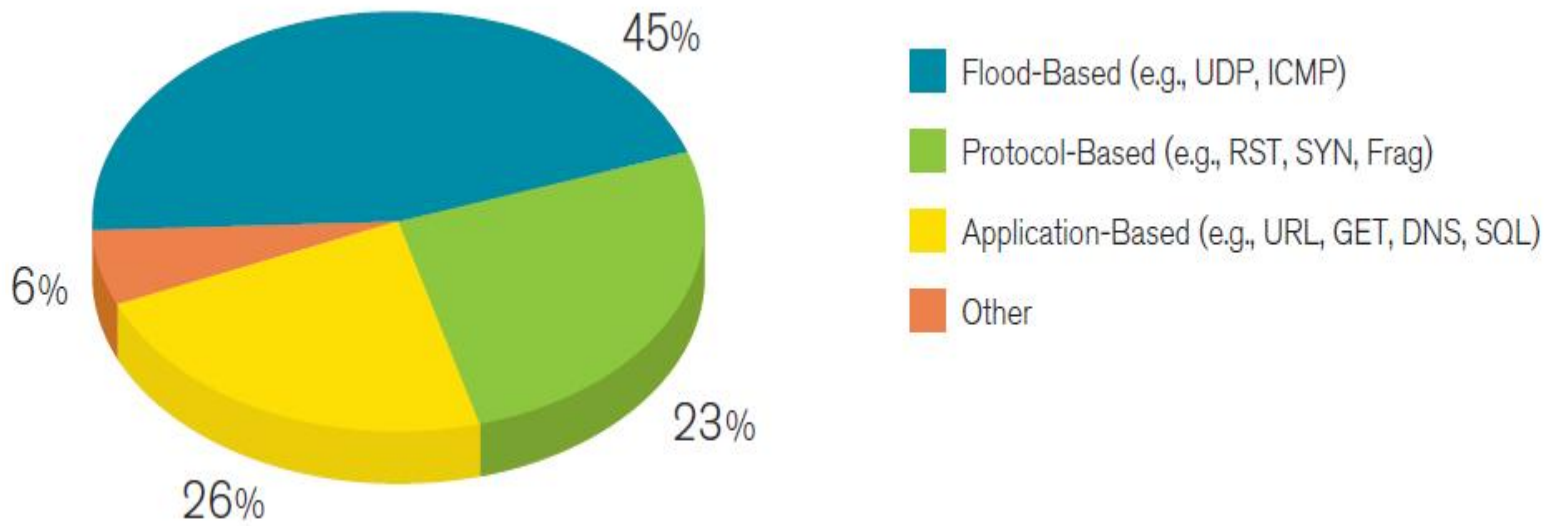
NOTE: Contrary to what some people claim, AnonNews was NOT hacked, and is still accessible as usual through the above link.

[Sign in](#) [Recent Site Activity](#) [Terms](#) [Report Abuse](#) [Print page](#) | Powered by [Google Sites](#)

DDoS Bantgeniřliđi saldırıları



Kaynak : Arbor Networks Inc.



Kaynak : Arbor Networks Inc.

OSI Katmanları - Servis Dışı Bırakma Saldırıları

- Uygulama zorlama
- Anlaşılamayan veriler ile uygulamayı etkisiz bırakma
- Başka bir kullanıcıya ait oturumu sonlandırma
- TCP SYN seli, UDP seli
- Fragmented IP paket gönderme,
• Büyük boyutlu ICMP paketleri gönderme.
- ARP spoof, wifi de-auth frame'leri gönderme.
- Ağ kablosunun çekilmesi, kesilmesi. Jamming

Uygulama (Application)
Katmanı

Sunum (Presentation)
Katmanı

Sunum (Presentation)
Katmanı

Taşıma (Transport) Katmanı

Ağ (Network) Katmanı

Veri Hattı (Data-Link)
Katmanı

Fiziksel (Physical) Katmanı



İNTERNETİN EN HIZLI YÜKSELEN GAZETESİ

YAZARLAR GÜNDEM SİYASET DÜNYA EKONOMİ YAŞAM MAGAZİN SPOR ME

İSTANBUL 17°C | İMKB ↓ 65,056 | DOLAR ↓ 1,581 | EURO ↑ 2,252 | 18 Mayıs 2011 Çarş

Gündem



Paylaş

Yorum Yaz

Yazdır

Favorim Yap

17.10.2007 03:11



« Önceki Haber Sonraki Haber »

Tavsiye et

Arkadaşların arasında bunu tavsiye eden ilk sen o

Telekom'a sabotaj

Masadan kalkıldı tam da o saatte Edirne, İstanbul, İzmir, Ankara ve Bursa'da fiber kablolar kesildi

Gülümhan GÜLTEN

62K

Beğen

[Grevden görüntüler için tıklayınız...](#)



Türk Telekom'da toplu sözleşme görüşmelerinin önceki gece saat 03.00 civarında uzlaşmazlıkla sonuçlanmasının hemen ardından 13 farklı yerde fiber optik kablolar kesildi. Türk Telekom Genel Müdürü Paul Doany, bunun bir sabotaj olduğunu iddia etti ve "Bu tür sabotajlar Türkiye'ye karşı yapılmış en büyük ayıptır" açıklamasını yaptı

Türk Telekom'da grev süreci devam ederken, şirket yönetimi sürpriz bir açıklama yaparak, sendikayla anlaşmazlığın netleştiği gece geç saatlerden itibaren Türkiye'nin 13 noktasında hatlara sabotaj yapıldığını iddia etti. Türk Telekom Yönetim Kurulu Başkanı ve Genel Müdürü Paul Doany, Türk Telekom Genel Müdür Yardımcısı Celalettin Dinçer, Pazarlama Direktörü Erem Demircan ve İnsan Kaynaklarından Sorumlu Başkan Gökhan Bozkurt yaptıkları açıklamada sabotajın yapılış biçiminin, grevde bulunan çalışanlar ya da onların görevlendirdiği kişiler tarafından yapıldığı izlenimi edindiklerini belirttiler.

Türk Telekom Genel Müdürü Doany, "Sendikanın ya da üyelerinin yaptığından nasıl eminsiniz" yönündeki soruya, "Bu şirket, şebekeyi çok uzun zamandır idare ediyor. Bu hatların doğal nedenlerden zarar görmediği çok belli. Eylemin kasti olduğu çok belli. Makas kullanılmış. Biz

Anasayfa > Dünya > 75 yaşındaki Gürcü kadın interneti çökertti

Yazdır

Arkadaşına Gönder

Yorum Yaz

Arşive Ekle

75 yaşındaki Gürcü kadın

06/04/2011 16:46

75 yaşında Gürcü bir kadın, ko
suçlanıyor.



Tavsiye et

Bir kişi bunu tavsiye etti. Ar

28 Mart tarihinde Gürcistan ile aras
gördüğü için Ermenistan ülke çapını
kalmıştı. Kesintinin gerekçesiyle bir kadının bakır hurda
araması. Gürcistan İçişleri Bakanlığı sözcüsü, yaşlı bir emekli
kadının yerde bakır hurda ararken iki ülke arasındaki
fiberoptik bağlantıya hasar verdiğini itiraf ettiğini açıkladı.
Gürcistan'ın Ksani köyünde yaşayan kadının yaşından dolayı
tutuksuz yargılanmasına karar verildi. Suçlu bulunması



260 milyar dolarlık borsa bir kepçe darbesiyle çöktü

Yol çalışmasında bir kepçe veri kablolarını kopardı. Borsa idaresi hasardan işlem saati yaklaşırken haberdar oldu. Taşeron tamircileri grevdeki sendika durdurdu



Radikal Gazetesi
Facebook'ta

Beğen

25,950 kişi Radikal Gazetesi'ni beğenmiştir

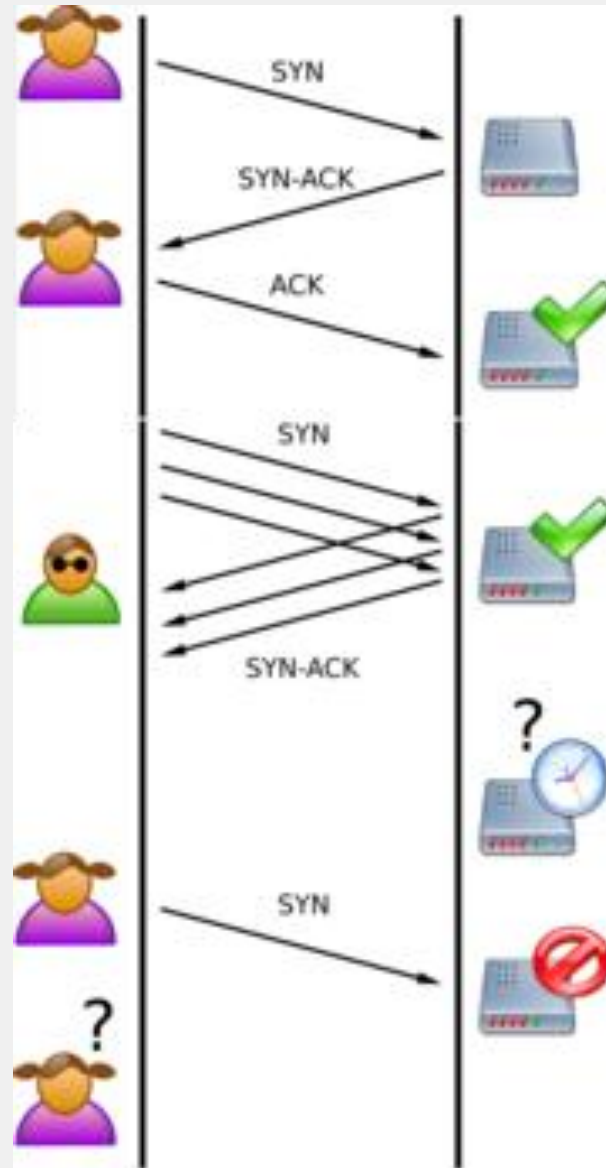
```
aireplay-ng -0 100 -a 00:1F:33:DB:81:44 wlan0
```

```
bt ~ # aireplay-ng -0 100 -a 00:1F:33:DB:81:44 wlan0
18:51:21 Waiting for beacon frame (BSSID: 00:1F:33:DB:81:44) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
18:51:21 Sending DeAuth to broadcast -- BSSID: [00:1F:33:DB:81:44]
18:51:22 Sending DeAuth to broadcast -- BSSID: [00:1F:33:DB:81:44]
18:51:23 Sending DeAuth to broadcast -- BSSID: [00:1F:33:DB:81:44]
18:51:24 Sending DeAuth to broadcast -- BSSID: [00:1F:33:DB:81:44]
18:51:25 Sending DeAuth to broadcast -- BSSID: [00:1F:33:DB:81:44]
18:51:26 Sending DeAuth to broadcast -- BSSID: [00:1F:33:DB:81:44]
18:51:27 Sending DeAuth to broadcast -- BSSID: [00:1F:33:DB:81:44]
18:51:28 Sending DeAuth to broadcast -- BSSID: [00:1F:33:DB:81:44]
```

home\$ ping -c 1 -s 65000 saldırılacak-adres

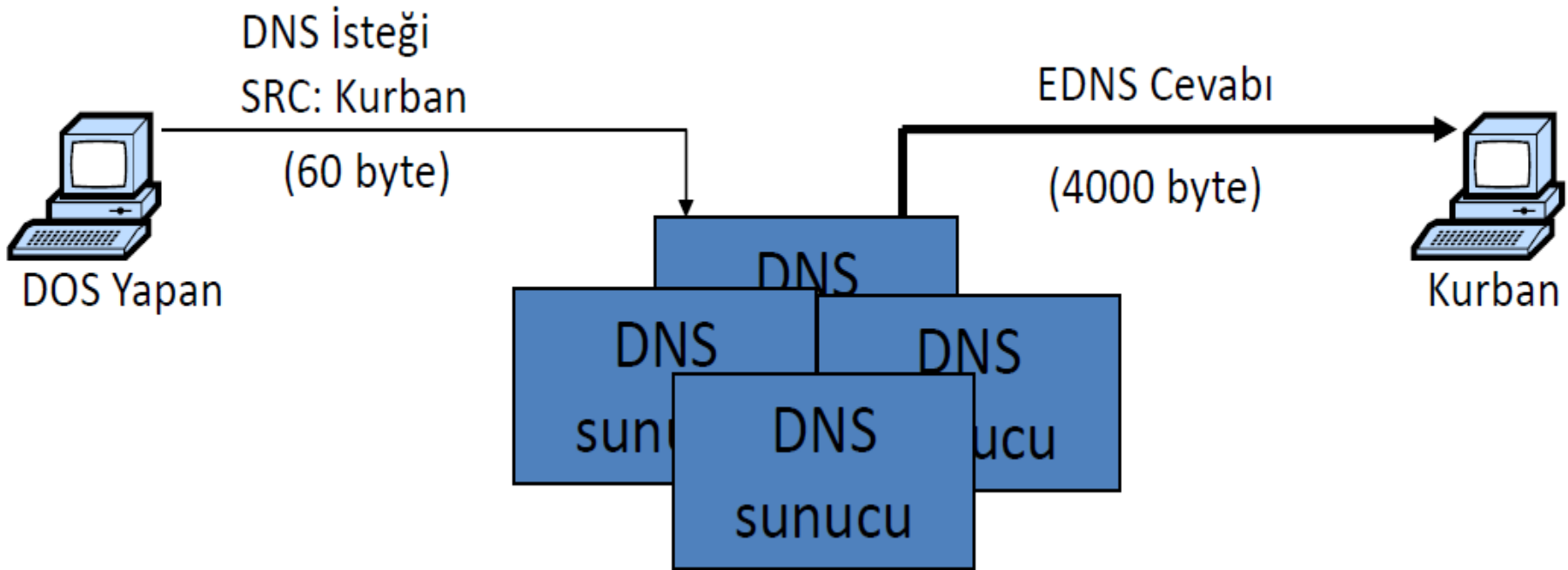
```
13:03:13.601413 IP 85.103.136.12 > 37.16.121.122: icmp
13:03:13.653449 IP 85.103.136.12 > 37.16.121.122: icmp
13:03:13.707553 IP 85.103.136.12 > 37.16.121.122: icmp
13:03:13.761700 IP 85.103.136.12 > 37.16.121.122: icmp
13:03:13.815786 IP 85.103.136.12 > 37.16.121.122: icmp
13:03:13.867905 IP 85.103.136.12 > 37.16.121.122: icmp
13:03:13.921988 IP 85.103.136.12 > 37.16.121.122: icmp
13:03:13.976094 IP 85.103.136.12 > 37.16.121.122: icmp
13:03:14.030193 IP 85.103.136.12 > 37.16.121.122: icmp
13:03:14.082312 IP 85.103.136.12 > 37.16.121.122: icmp
13:03:14.136409 IP 85.103.136.12 > 37.16.121.122: icmp
13:03:14.190522 IP 85.103.136.12 > 37.16.121.122: icmp
13:03:14.244606 IP 85.103.136.12 > 37.16.121.122: icmp
13:03:14.296722 IP 85.103.136.12 > 37.16.121.122: icmp
13:03:14.350840 IP 85.103.136.12 > 37.16.121.122: icmp
13:03:14.544201 IP 85.103.136.12 > 37.16.121.122: ICMP echo request, id
26629, seq 1, length 1472
```

Taşıma Katmanında DoS



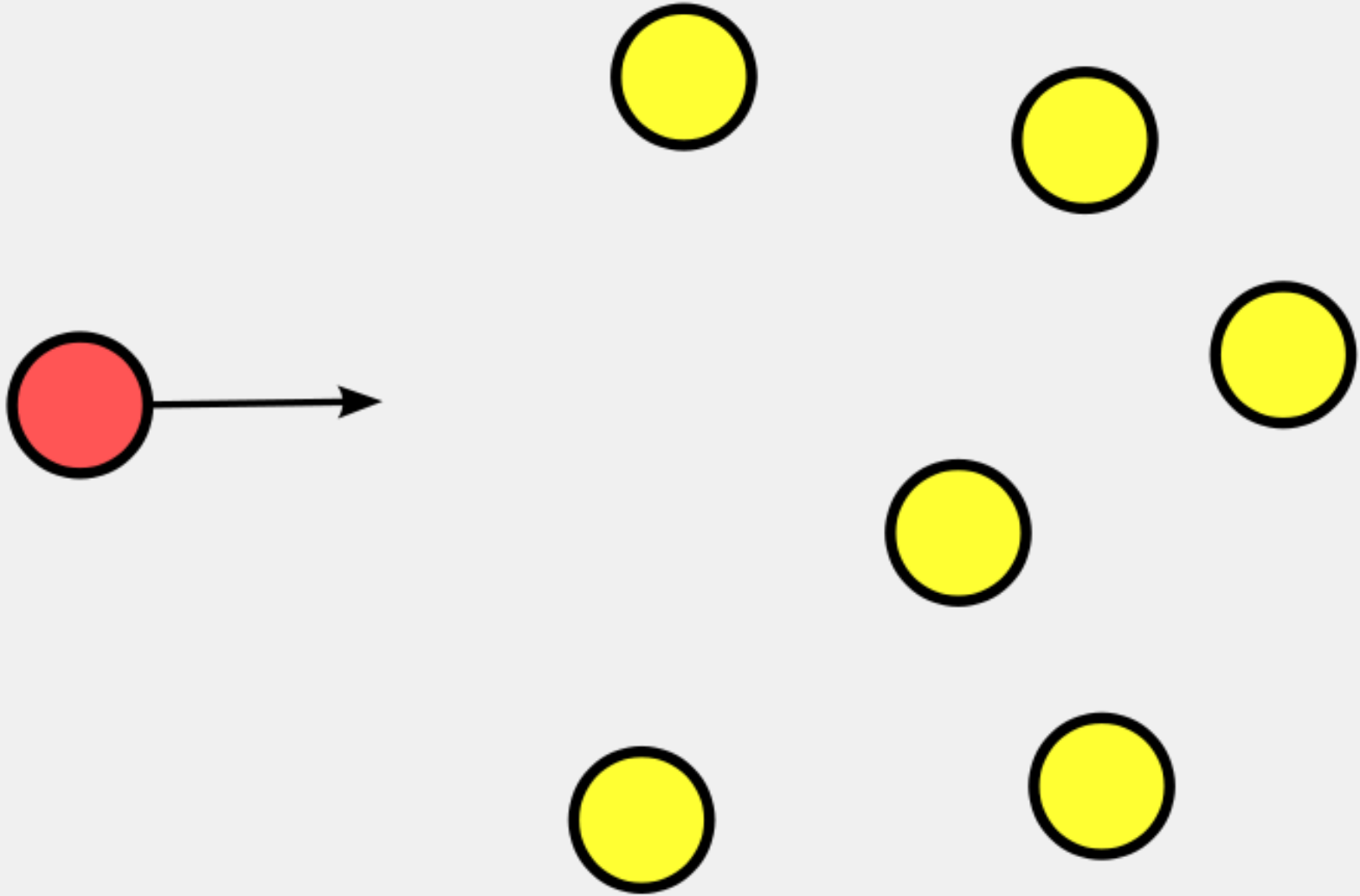
Uygulama Katmanında DoS

DNS Amplification Saldırısı ile hedef olarak belirlenen sisteme kurbandan geliyormuş gibi istekte bulunulabilir

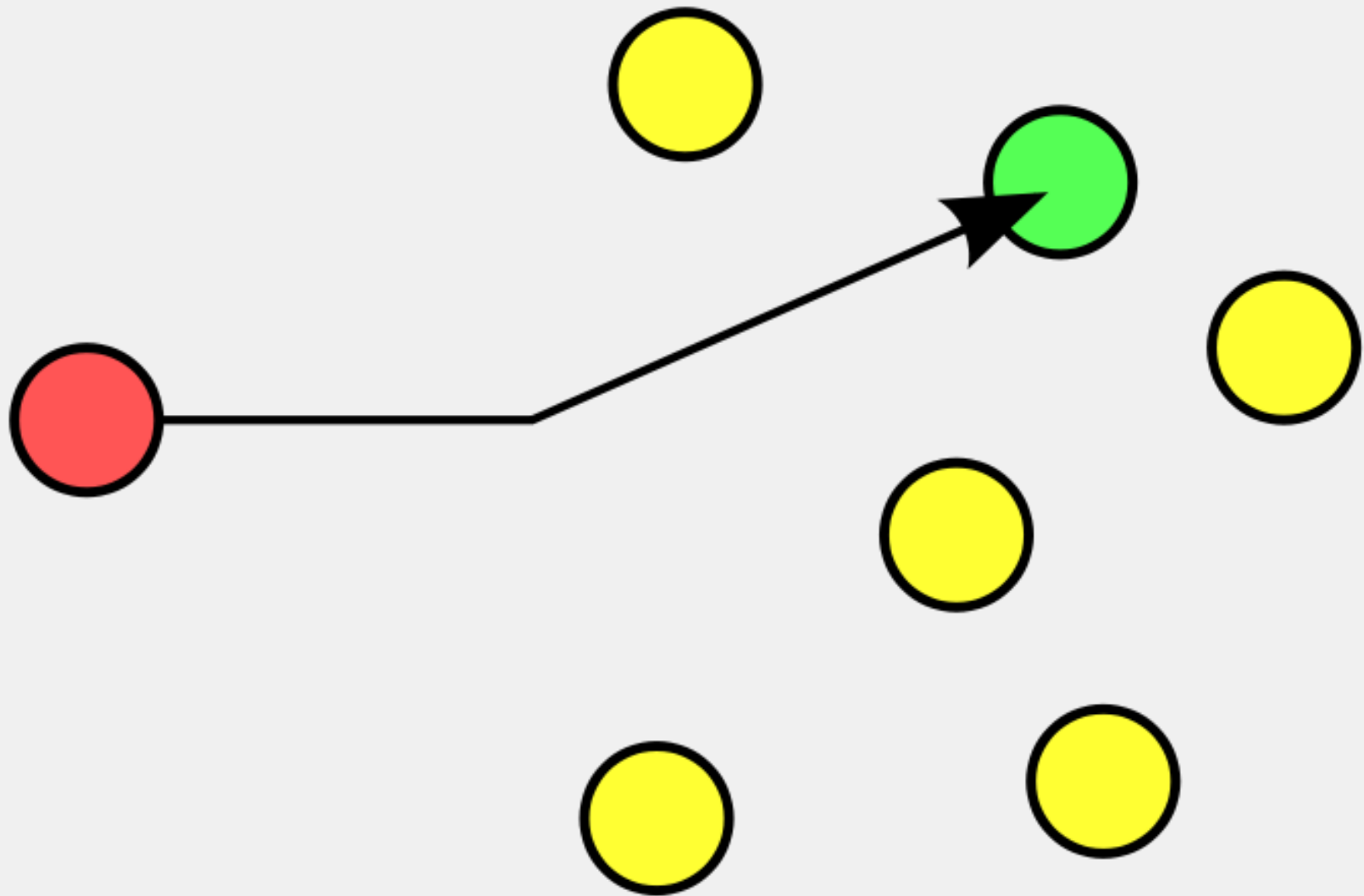


Internette herkese açık dns sunucu sayısı ~600,000

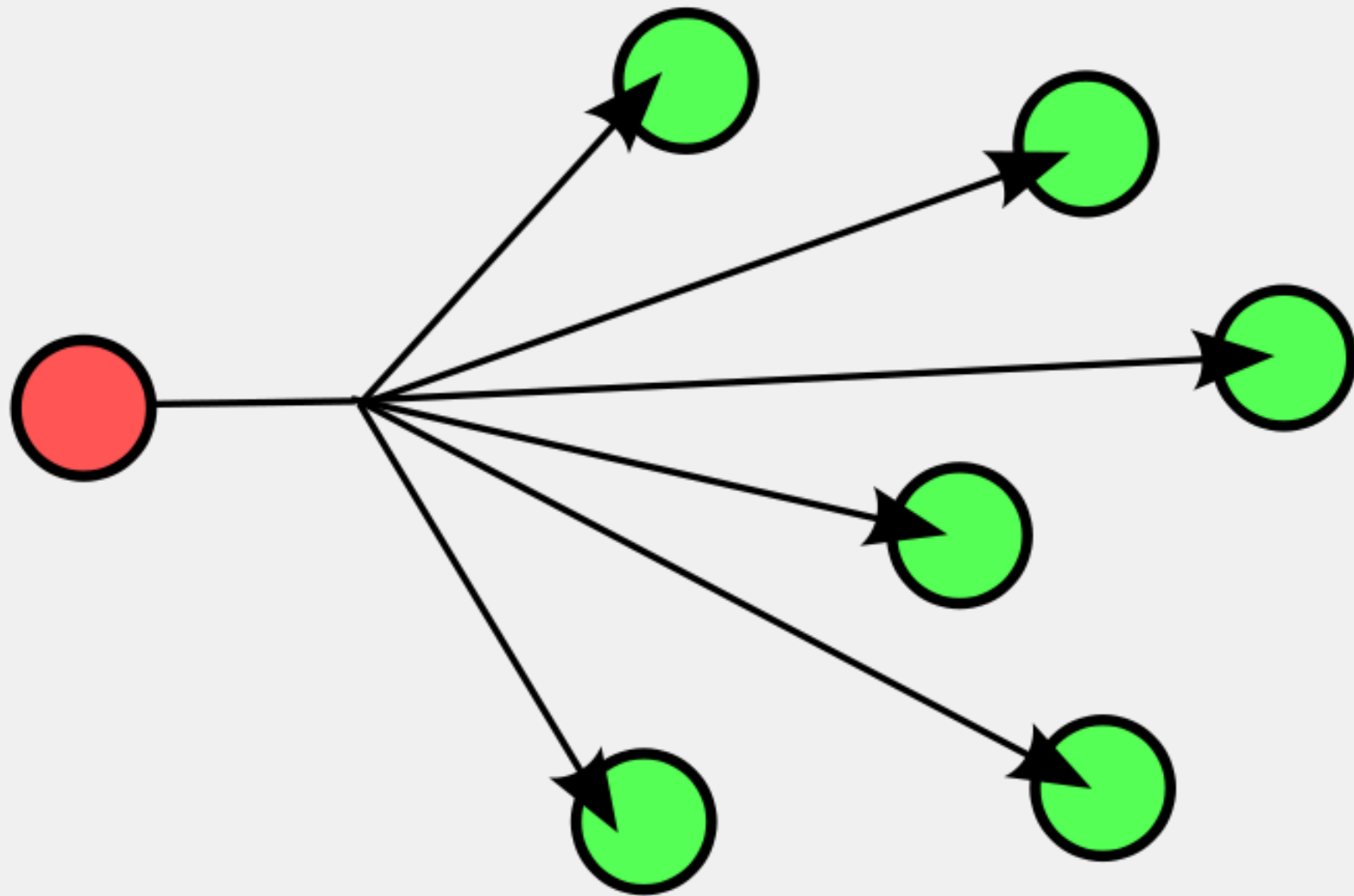
Yönlendirme Şemaları

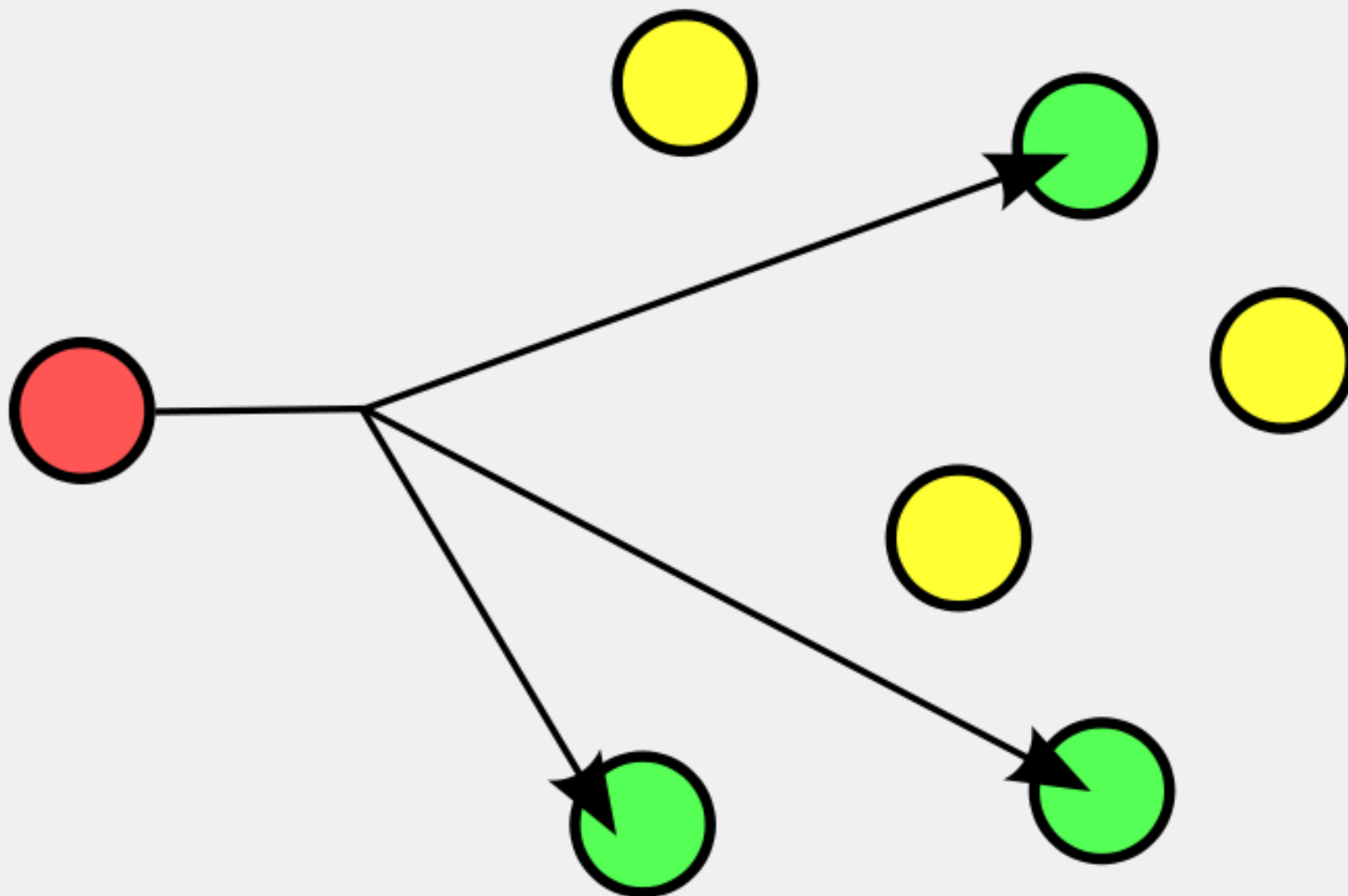


Unicast

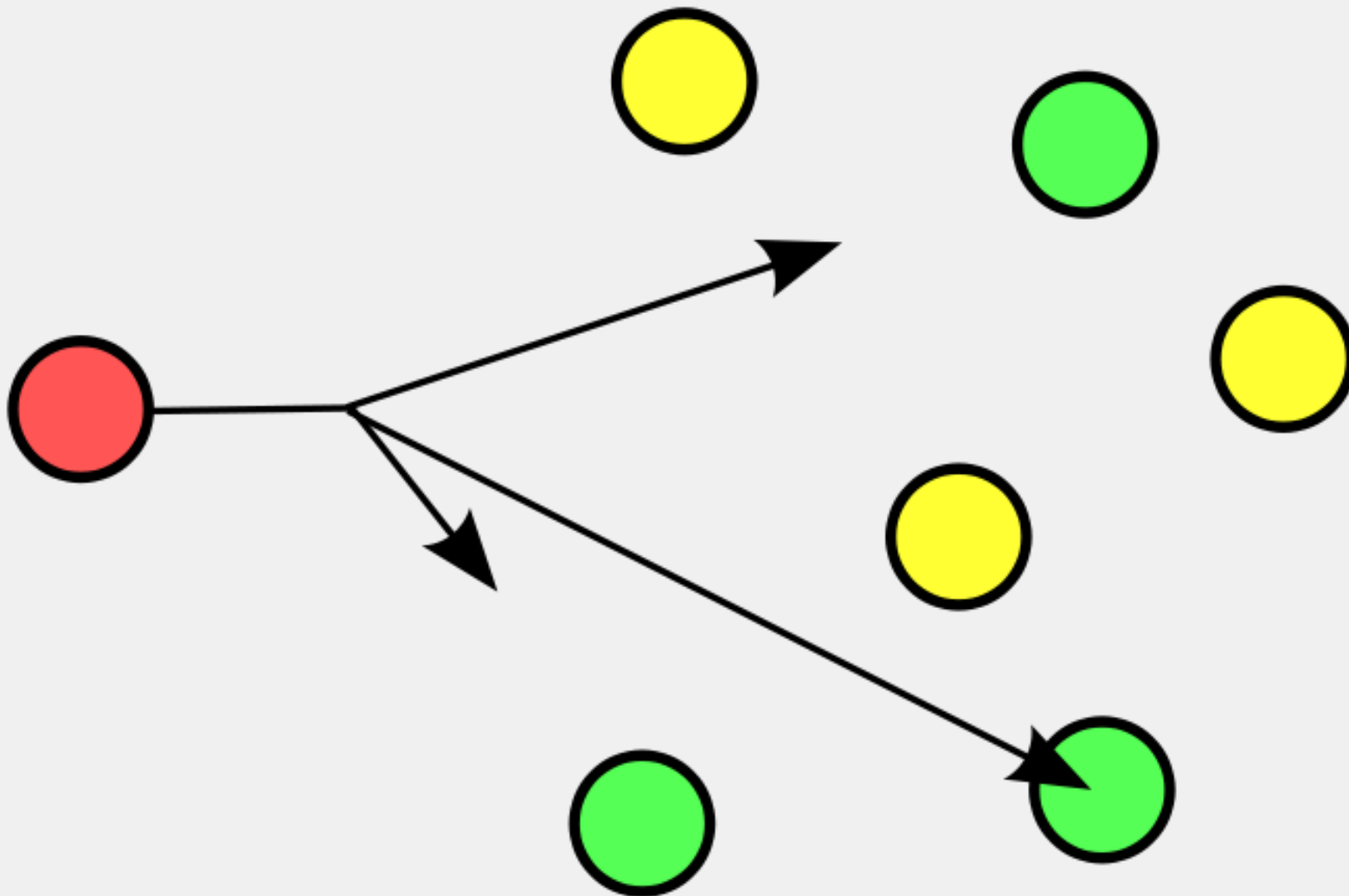


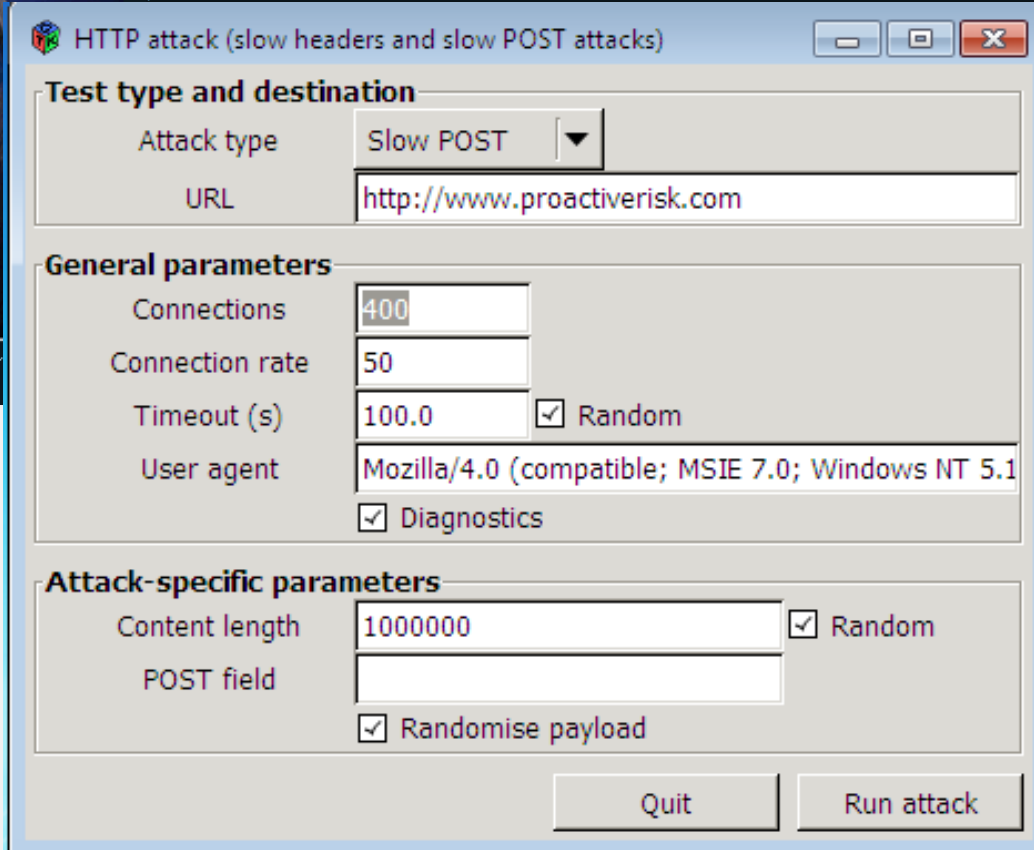
Broadcast





Anycast





Güvenlik Duvarı Yönetim Arayüzü - Yeni Limit Tanımı

Adı: Upload Limit Arayüzleri:

Not:

Limitsiz

Bu eylem ile tanımlı kuraldan geçen trafik için (Özellikle DDOS saldırılarına karşı kullanılmalıdır):

Toplam izin verilecek bağlantı sayısı:

Toplam izin verilecek max. farklı kaynak adresi:

Bir kaynak adresinin, açabileceği max bağlantı sayısı:

10 saniyede açılacak bağlantı sayısı
[Varsayılan politikalarda, ileri seçenekler kısmında durdurma ve kayıt özellikleri ayarlanabilir]

Bu limiti aşan kaynak adresinin tüm bağlantılarını sonlandır.

Durum tablosu zaman aşımı süresi (sn)

Kuralın çalışma oranı (%)

Güvenlik Duvarı Yönetim Arayüzü - bce1:tgs_vpn[193.140.74.32]

Topoloji

İnternete bağlı (varsayılan ağ geçidi bu arayüz üzerindedir)

Bir iç ağa bağlıdır

Bu arayüz için bir iç ağ tanımı oluşturabilirsiniz ->

Varsayılan Politikalar

Filtre Politikaları **Paket Normalleme**

<input type="checkbox"/> Bu arayüzden, sadece kendi ağ bloğuna ait trafik dışarı ÇIKAR . Farklı kaynak adreslerini durdur. Öm: Bu arayüzde adres dönüşümü yapılmaktadır, çıkan paketlerde kaynak adresi bu ağa ait olmalıdır.	Kayıt No: Arayüz Politikası: Anti-spoof-dışarı
<input type="checkbox"/> Bu arayüze, sadece kendi ağ bloğuna ait trafik GELİR . Farklı kaynak adreslerini durdur. Öm: Arayüzün arkasında sadece kendi ağa ait trafik üretilir, paketlerde farklı bir kaynak adres bulunamaz.	Kayıt No: Arayüz Politikası: Anti-spoof-içeri
<input type="checkbox"/> Bu arayüze ait ağ trafiği, bu birimin diğer arayüzlerine dışarıdan GELEMEZ . Diğer arayüzlerde kaynak adres bu ağdan olamaz. Bu ağın adreslerinin trafiği sadece bu arayüz arkasında üretilir.	Kayıt No: Arayüz Politikası: Özel ağ
<input type="checkbox"/> Birimin diğer arayüzlerine ait ağların trafiği, bu arayüzün ağından GELEMEZ . Diğer arayüz adresleri burada kaynak adres olamaz. Diğer ağların adreslerinin trafiği bu arayüzün arkasında üretilemez.	Kayıt No: Arayüz Politikası: Özel arayüz
<input type="checkbox"/> Bu arayüz üzerinden yönetim servisine ERİŞİLEMEZ .	Kayıt No: Yönetim kapısı kuralı

- White-list veya gray-list olarak kullanılabilir

www.countryipblocks.net/

- Black-List olarak

www.shadowserver.org

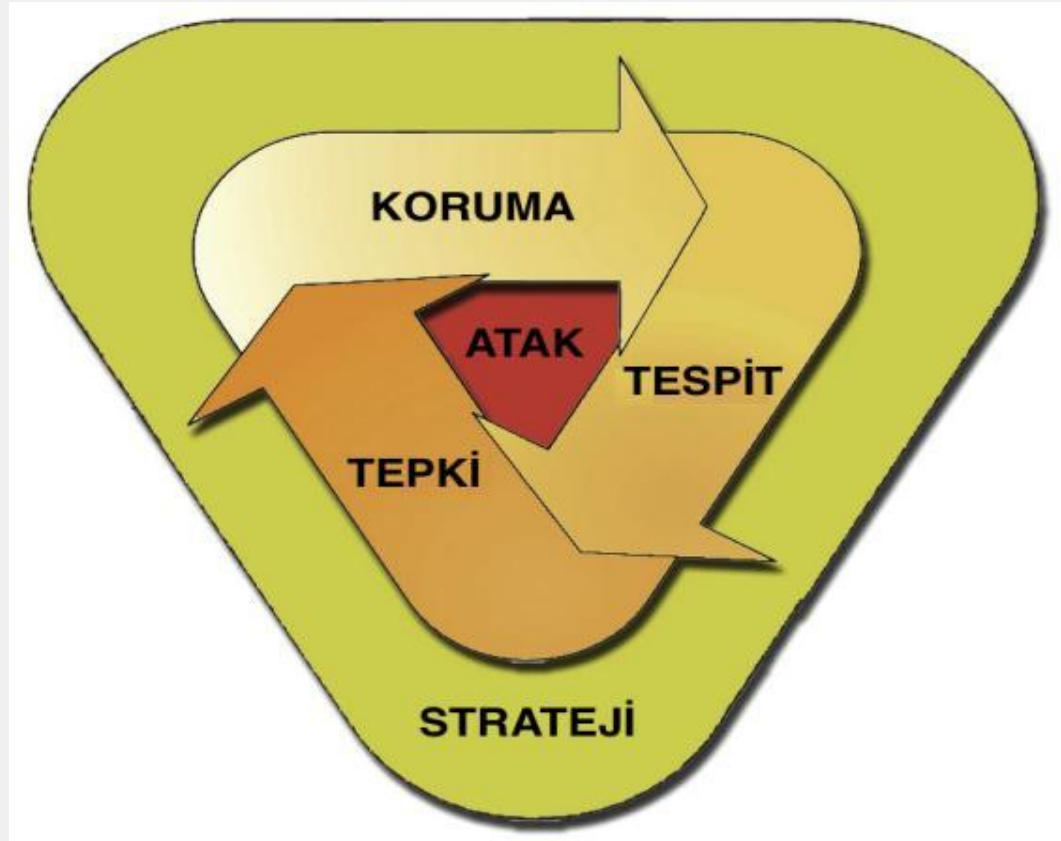
www.abuse.ch

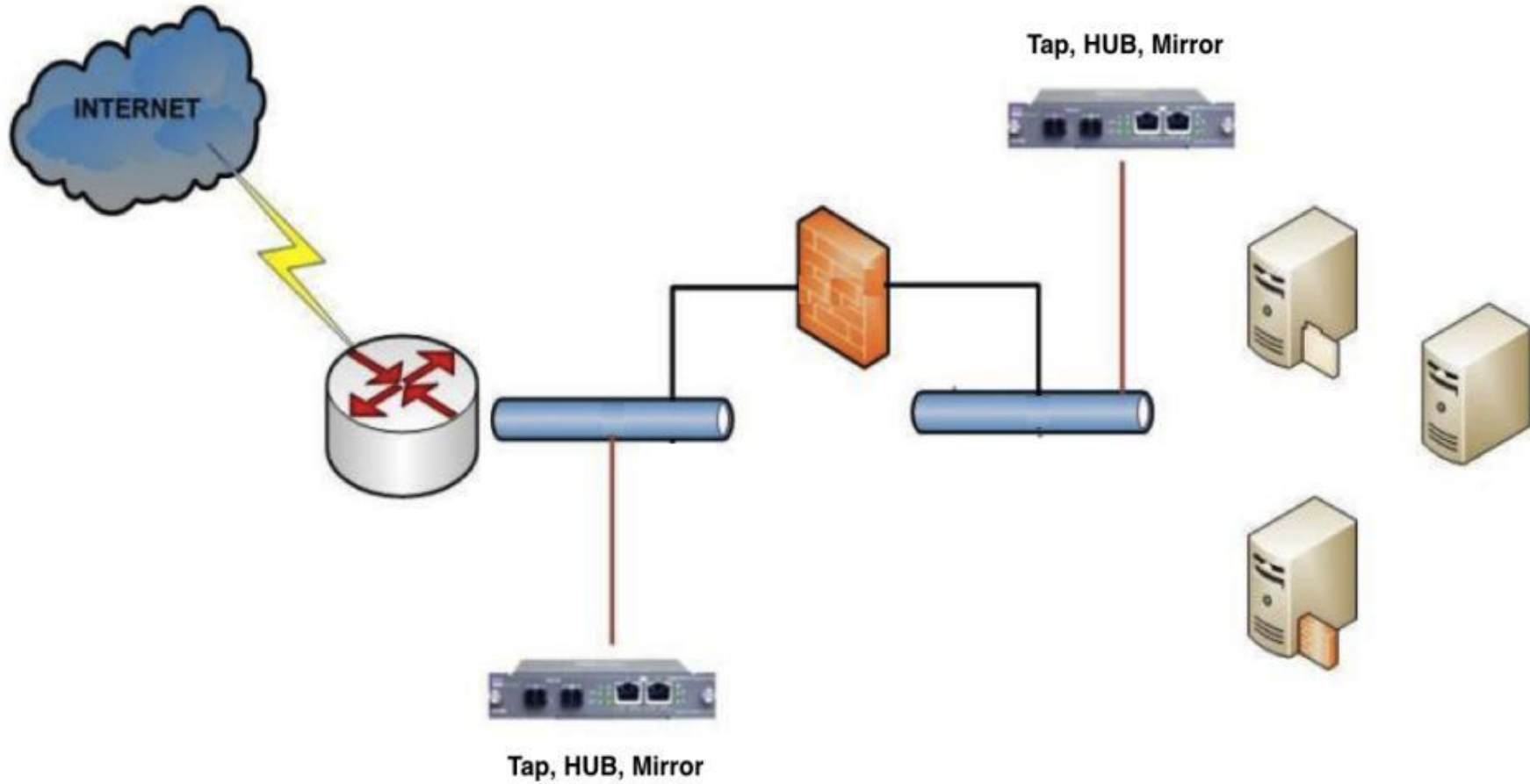
Botnet'e üye bilg. IP adresleri

Country: TURKEY
ISO Code: TR
Total Networks: 383
Total Subnets: 12,510,912
31.3.0.0/21
31.6.80.0/20
31.25.168.0/21
31.44.192.0/20
31.140.0.0/14
31.145.0.0/16
31.155.0.0/16
31.169.64.0/19
31.176.0.0/17
31.177.128.0/17
31.186.0.0/19
31.192.208.0/21
31.200.0.0/17
31.206.0.0/16
31.207.80.0/21
....

DDoS'tan Korunma Metodolojisi

- Hazırlanma aşaması
- Prosedürlerin belirlenmesi
- Gerekli araçların, yazılımların elde edilmesi
- Analiz Aşaması
- Koruma aşaması
- Raporlama





- Asıl Problem Botnet'lerdir. DDoS sadece belirtidir!
- Başkası sisteminizi test etmeden kendiniz test edin.
 - Network cihazları
 - Sunucuları
 - Çalışan Servisleri (Apache, IIS, bind, Oracle vs)
 - Uygulamalar
- Saldırı anında ve sonrasında yapılan işlemler, daha sonra yapılabilecek saldırılara karşı raporlanmalı.
- ISP'lerle işbirliği yapılmalı



TÜBİTAK-BİLGEM-UEKAE Bilişim Sistemleri Güvenliği Bölümü

emre@uekae.tubitak.gov.tr

0 262 648 15 71

www.uekae.tubitak.gov.tr

www.bilgiguvenligi.gov.tr