



AYD

Ağ Yöneticileri Derneği



Siber Güvenliğe Giriş

www.agyoneticileri.org

Gökhan AKIN- CCIE# 38627

Ağ Yöneticileri Derneği

Ben Kimim?

Gökhan AKIN,
CCIE #38627

Ağ Yöneticileri Derneği
Kurucu Başkanı

www.gokhanakin.net
gokhan@agyoneticileri.org
<http://www.linkedin.com/in/gakin>



Siber Güvenliğe Giriş

Ders 1 Gökhan AKIN (AYD)

Siber Güvenlik Nedir?

Saldırı Tipleri

Kişisel Güvenliğimizi Nasıl Sağlarız

Ders 2 Ozan BÜK (AYD) / Gökhan AKIN (AYD)

Zararlı Yazılımlar

Zararlı Yazılım Örnekleri

Bir Worm'un Anatomisi

Siber Güvenliğe Giriş

Ders 3 Hakan TAĞMAÇ (Cisco)

Güncel Global Siber Güvenlik Rapor
Açık Siber Güvenlik Mimarisi

Ders 4 Gökhan AKIN (AYD)

Ağ Güvenlik Cihazları
Siber Güvenlik Uzmanlığı
Siber güvenlik Üzerine Kariyer

Siber Nedir?



Siber sadece Internet DEĞİLDİR, çok daha fazlasıdır.

Ağlar Internet'e bağlı olabildiği gibi olmayabilir de,
(bu bir zorunluluk değildir!)

Örnekler:

- SCADA, GPS Uydu Hizmeti, Otoban, Metro ..vb

Siber Güvenlik Nedir?

- Gizlilik
- Bütünlük
- Erişilebilirlik



Amaç bunların sağlanması,
Yani bunları engellemek isteyenler var!

Kim bunlar?



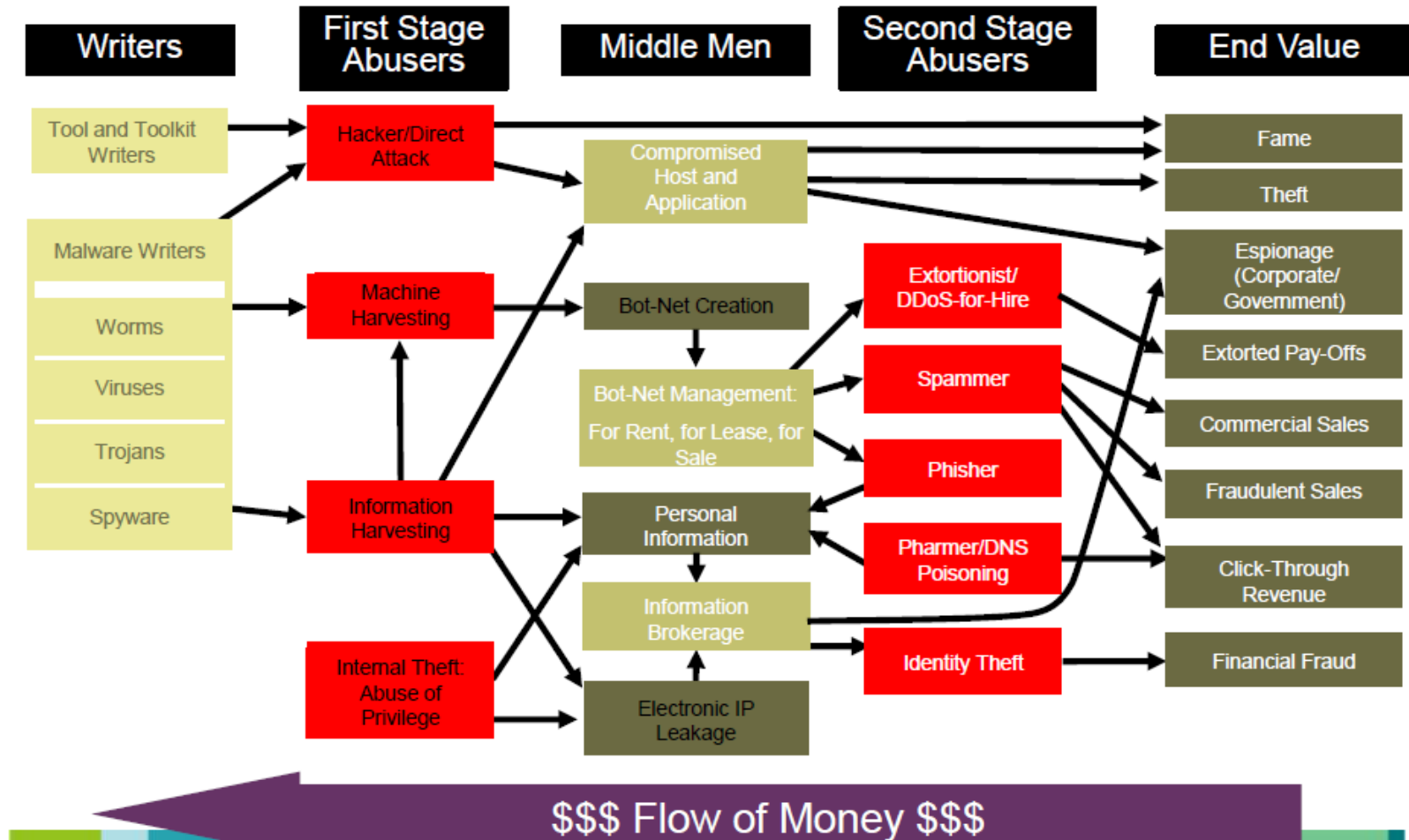
Kim bunlar?



Amaçları Ne?

- Devlet destekli - siber operasyonlar
- İdeolojik ve Politik - İfade Özgürlüğü Amaçlı
- Suç örgütleri – Gelir Amaçlı
- Düşük seviye veya bireysel -Kişisel Kazanç

Para Döngüsü



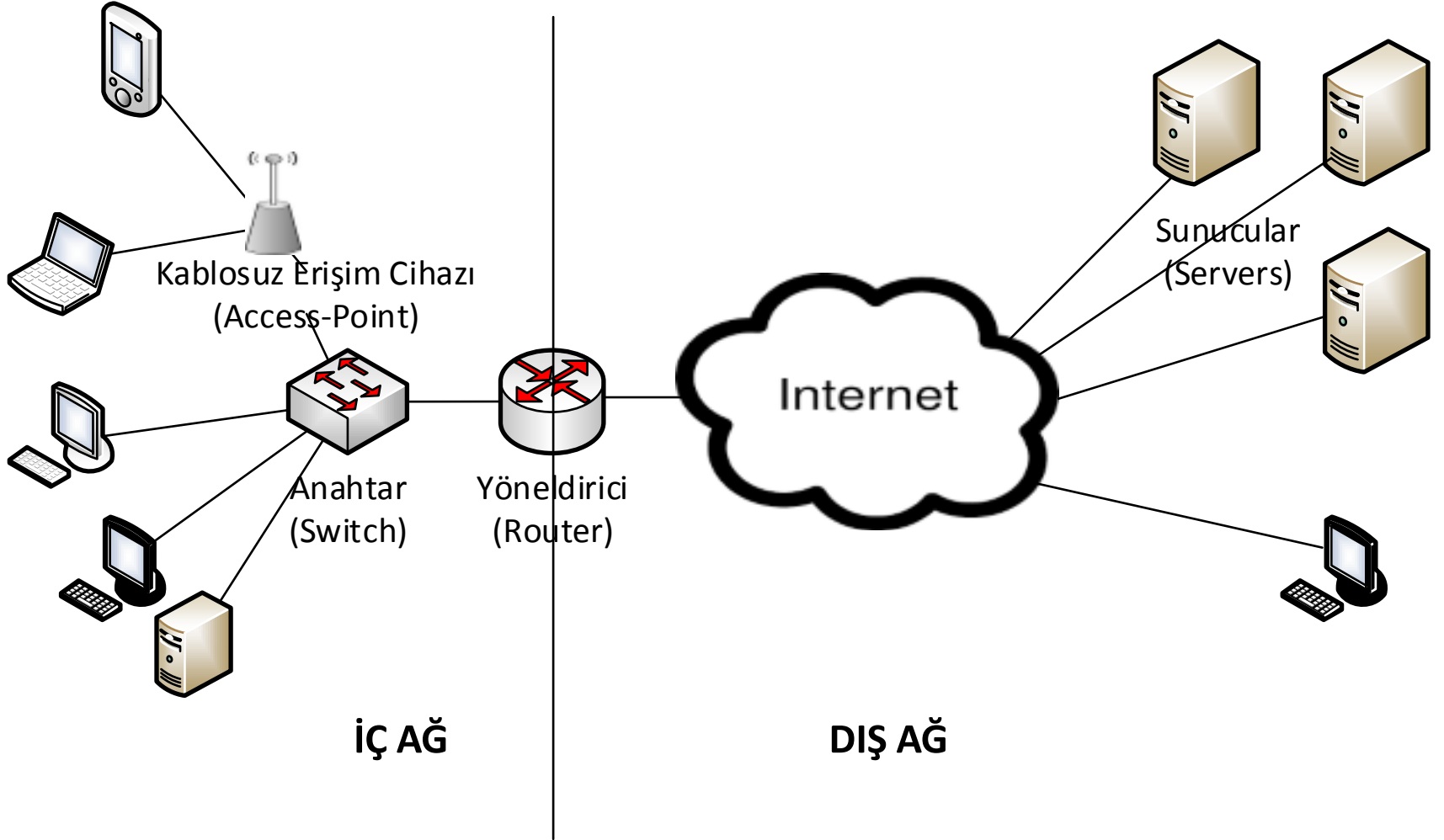
Nasıl Saldırıyorlar?



Saldırı Tipler

- Keşif Atakları - Reconnaissance Attacks
- Erişim Atakları - Access Attacks
- Servis Dışı Bırakma Atakları
 - Denial of Service (DoS) Attacks

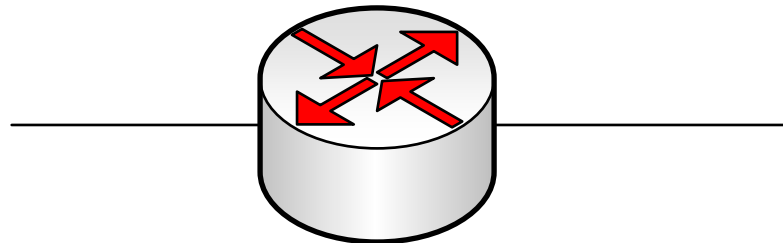
Tipik Bir Ağ



Yönlendirici (Router)



AĞ 1

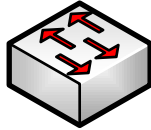


Yönlendirici
(Router)

AĞ 2

Anahtar (Switch)

Kablosuz Eriřim Cihazı (Access Point)

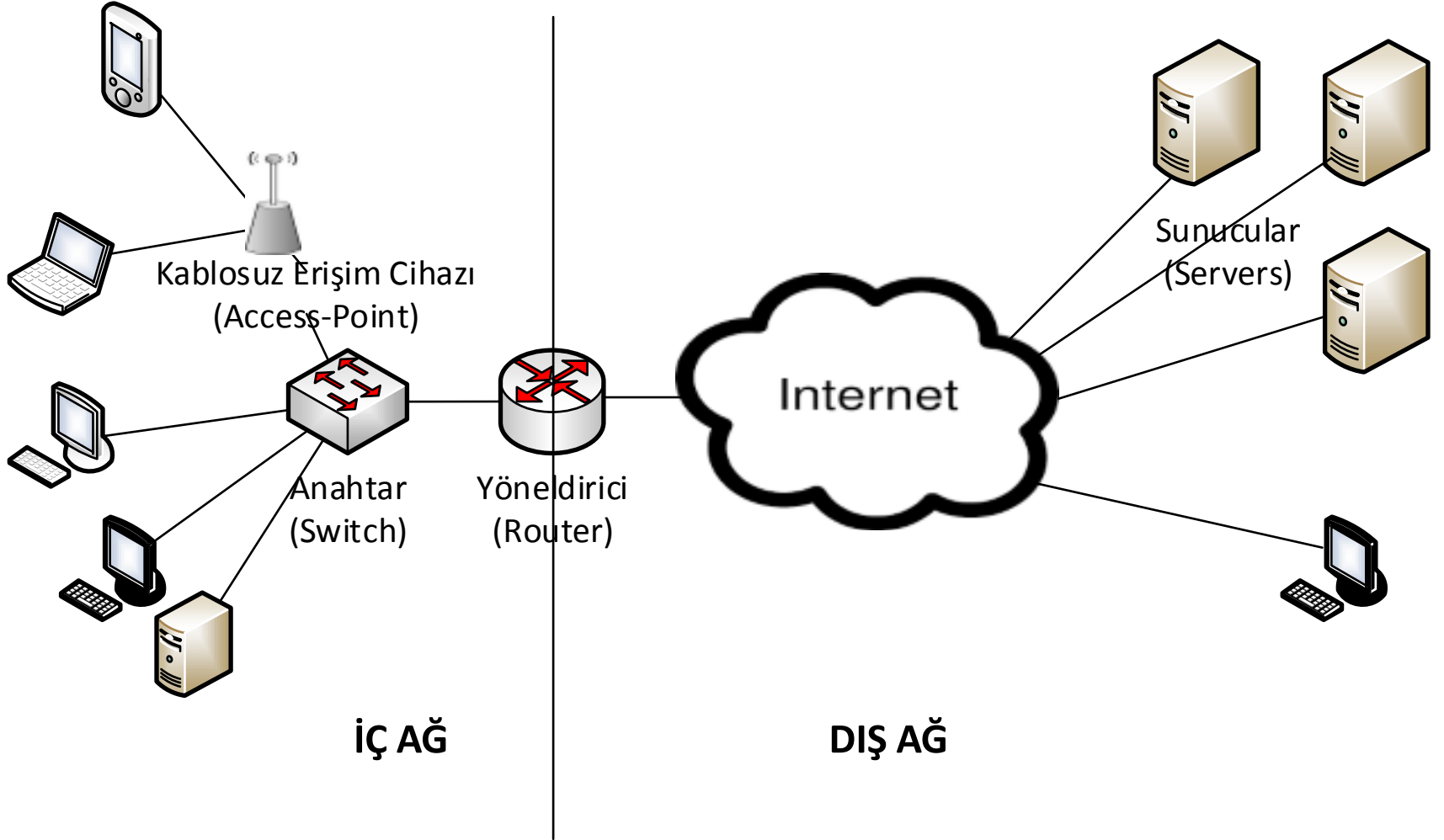


Anahtar
(Switch)



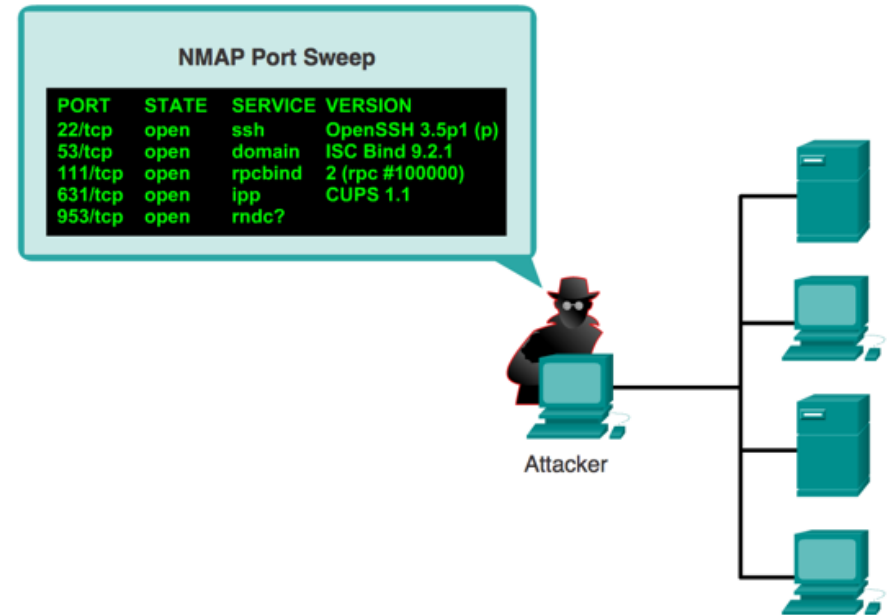
Kablosuz Eriřim Cihazı
(Access-Point)

Tipik Bir Ağ



Keşif Atakları

- Internet bilgi araştırması
- Ping taraması
- Port taraması
- Paketleri dinlemek



Keşif Atakları

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Ozan>ping www.trakya.edu.tr

Pinging www.trakya.edu.tr [193.255.140.50] with 32 bytes of data:
64 bytes from 193.255.140.50: icmp: 193.255.140.50 ttl=64 time=10.12 ms
64 bytes from 193.255.140.50: icmp: 193.255.140.50 ttl=64 time=10.12 ms
64 bytes from 193.255.140.50: icmp: 193.255.140.50 ttl=64 time=10.12 ms
64 bytes from 193.255.140.50: icmp: 193.255.140.50 ttl=64 time=10.12 ms

Ping statistics for 193.255.140.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milliseconds:
        Minimum = 10, Maximum = 10, Average = 10
    Control-C (Ctrl+C)
C:\Users\Ozan>
```

Database Query — Welcome t... X +

https://apps.db.ripe.net/search/query.html?searchtext Search

Search results

This is the RIPE Database search service. The objects are in RPSL format. The RIPE Database is subject to [Terms and Conditions](#).

Abuse contact info: `abuse@ulakbim.gov.tr`

inetnum:	193.255.140.0 - 193.255.140.255
netname:	TRAKYA-NET
descr:	Trakya Universitesi Bilisayar Uyg. Arast. Merk.
country:	TR
admin-c:	EB1351-RIPE
tech-c:	FA783-RIPE
tech-c:	SS2358-RIPE
status:	ASSIGNED PA

Eriřim Atakları

Eriřip ne yapacak?

Siber Güvenlik Nedir?

- Gizlilik
- Bütünlük
- Erişilebilirlik



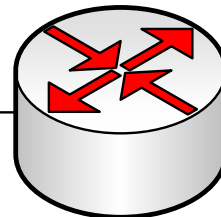
Nasıl Erişebilirler?

- Basit Parolalar...
- Yazılımsal hatlar,
 - Buffer overflow(İşletim sistemleri vs)
 - SQL injection, vb (Web Sayfaları)
- Aradaki Adam Atakları
- Malware'ler ile (Virus,Worm,Trojen...)

Günlük Bir Log

May 29 13:50:48: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: **ts**] [localport: 22]
May 29 14:10:25: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: **minecraft**] [localport: 22]
May 29 14:10:28: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: **admin**] [localport: 22]
May 29 14:10:31: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: **root**] [localport: 22]
May 29 14:10:34: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: **root**] [localport: 22]
May 29 14:10:37: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: **lp**] [localport: 22]
May 29 14:10:40: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: **wordpress**] [localport: 22]
May 29 14:10:44: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: **root**] [localport: 22]
May 29 14:10:47: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: **admin**] [localport: 22]
May 29 14:15:49: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: **alias**] [localport: 22]
May 29 14:15:52: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: **alias**] [localport: 22]
May 29 14:17:28: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: **app**] [localport: 22]
May 29 14:21:27: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: **wp**] [localport: 22]

AĞ 1



Yönelirici
(Router)

AĞ 2

En Çok Kullanılan 10 Parola

rockyou.com'un 32 milyon hesabında

1. 123456
2. 12345
3. 123456789
4. password
5. iloveyou
6. princess
7. 1234567
8. rockyou
9. 12345678
10. abc123



Parolanı paylaşmak

“Parola diř fırçanız gibidir. Başkasının kullanmasına izin vermeyin, ve altı ayda bir yenileyin.”

“Treat your password like your toothbrush.
Don’t let anybody else use it, and get
a new one every six months.”

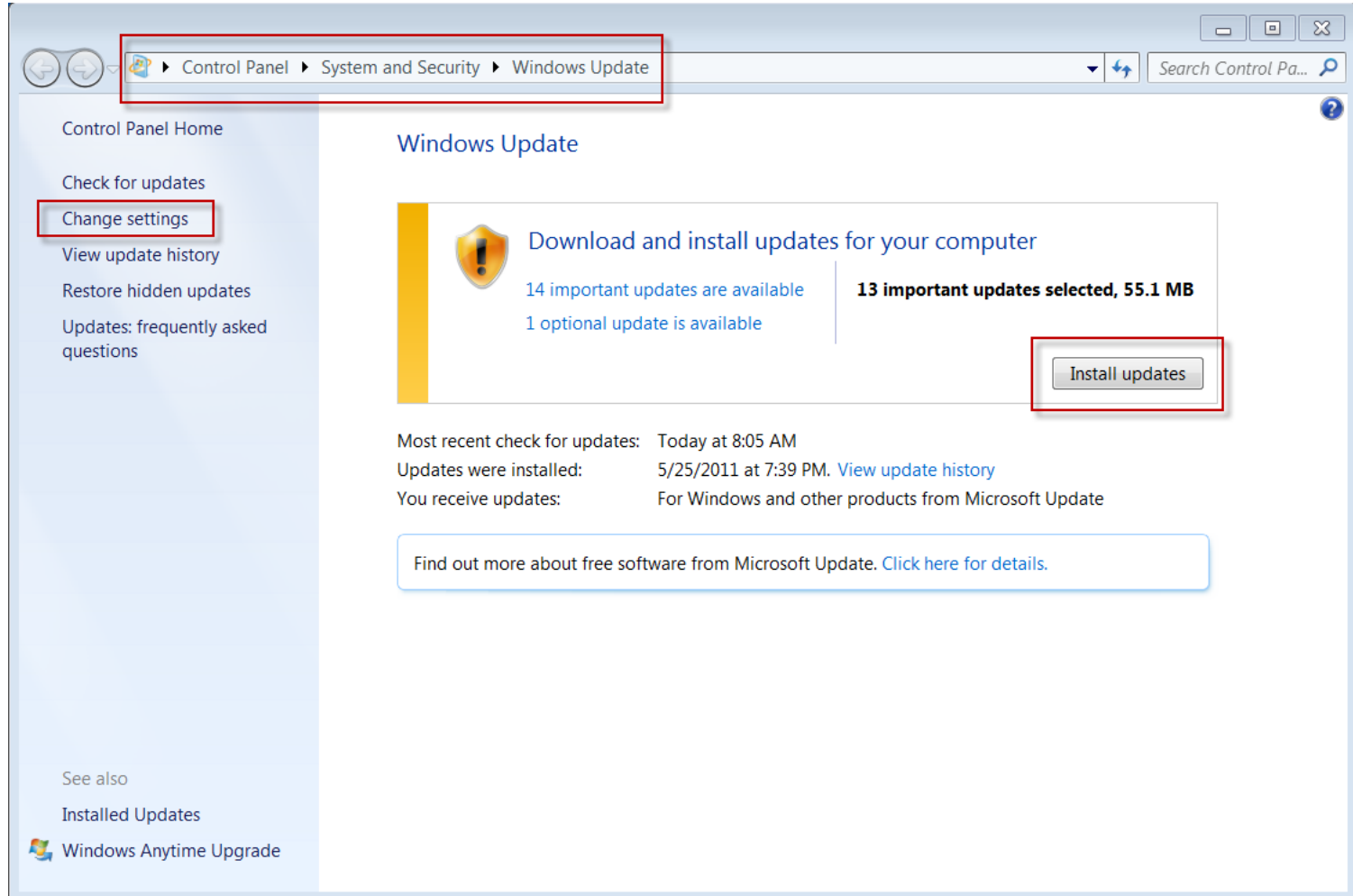
Clifford Stoll
Author



Nasıl Erişebilirler?

- Basit Parolalar...
- Yazılımsal hatlar,
 - Buffer overflow(İşletim sistemleri vs)
 - SQL injection, vb (Web Sayfaları)
- Aradaki Adam Atakları
- Malware'ler ile (Virus,Worm,Trojen...)

Yazılımsal Hatalar



Nasıl Erişebilirler?

- Basit Parolalar...
- Yazılımsal hatlar
(Buffer overflow, SQL injection..)
- Aradaki Adam Atakları
- Malware'ler ile (Virus, Worm, Trojan...)

http://isube.garanti.com.tr/isube/login/login/passwordentrypersonal-tr



Kurumsal İnternet Şubesi | English

Bu site güvenlidir.



Güvenli Bankacılığa Hoş Geldiniz

Lütfen giriş yönteminizi seçin.

Müşteri / T.C. Kimlik Numarası

Kart Numarası

Müşteri / T.C. Kimlik Numarası

Parola

Müşteri numaramı ya da parolamı unuttum.

İnternet Şubesi Giriş



İnternet Şubesi parola al

İnternet Şubesi parolanız yoksa
veya unuttuysanız buradan parola
alabilirsiniz.

Parola Al



Yardım ve Güvenlik

Güvenliğiniz için lütfen
aşağıdaki bilgilere dikkat edin.Güvenli bir İnternet deneyimi
ve güncel virüsler hakkında
bilgi almak için lütfen tıklayın.
[Detaylı bilgi](#)[Başkası adına mı işlem
yapıyorsunuz?](#)[Tasarruf Mevduatı Güvencesi](#)[Diğer Yardım ve Güvenlik](#)



Güvenli Bankacılığa Hoş Geldiniz

Lütfen giriş yönteminizi seçin.

Müşteri / T.C. Kimlik Numarası

Kart Numarası

Müşteri / T.C. Kimlik Numarası

Parola

Müşteri numaramı ya da parolamı unuttum.

İnternet Şubesi parola al

İnternet Şubesi parolanız yoksa
veya unuttuysanız buradan parola
alabilirsiniz.

Parola Al



Yardım ve Güvenlik



Güvenliğiniz için lütfen
aşağıdaki bilgilere dikkat edin.



Güvenli bir İnternet deneyimi
ve güncel virüsler hakkında
bilgi almak için lütfen tıklayın.
[Detaylı bilgi](#)



Başkası adına mı işlem
yapıyorsunuz?



Tasarruf Mevduatı Güvencesi

[Diğer Yardım ve Güvenlik](#)

İnternet Şubesi Giriş



DHCP'den IP aldıkta ne aldık??

Wi-Fi

eduroam

gok6

KAHVEZAMANI

Little Pilot

cafemarmaris

Delta-Park

HANIME

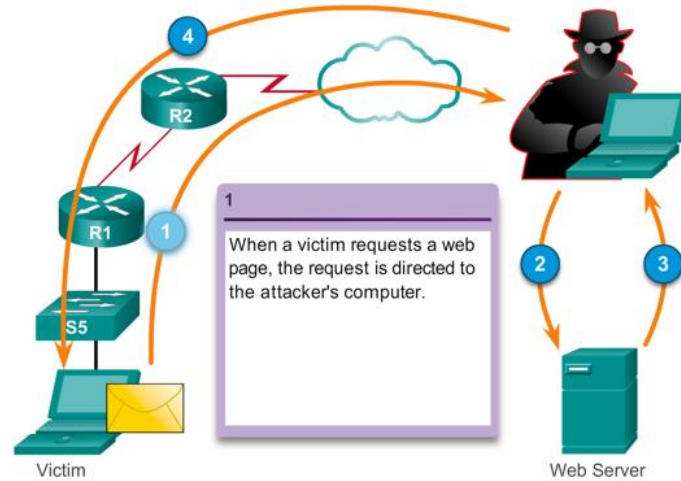
SUPERO

Ziyafet

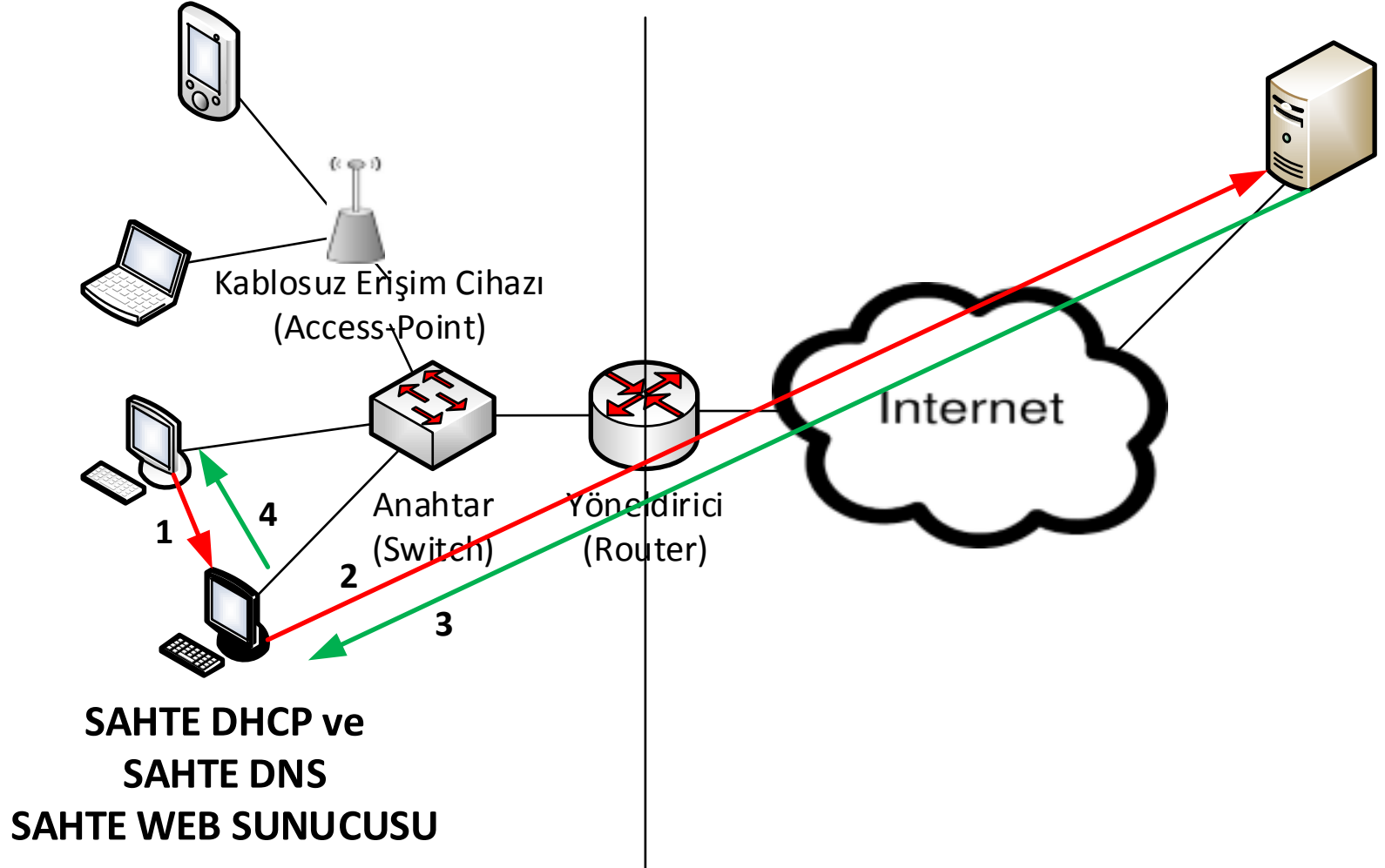
Saglik_K

```
Link-Local IPv6 Address . . . . . : fe80::3821:a5a8:49a3:80a0%68 (Preferred)
IPv4 Address . . . . . : 192.168.10.78 (Tentative)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.10.1
DHCPv6 IAID . . . . . : 1677742166
DHCPv6 Client DUID. . . . . : 00-01-00-01-19-14-B7-21-00-24-E8-9D-D4-E2

DNS Servers . . . . . : 88.10.2.5
Primary WINS Server . . . . . : 192.168.116.2
NetBIOS over Tcpip. . . . . : Enabled
```



Yanlış DNS Sunucusu neye sebep olur?



Nasıl Erişebilirler?

- Basit Parolalar...
- Yazılımsal hatlar
(Buffer overflow, SQL injection..)
- Aradaki Adam Atakları
- Malware'ler ile (Virus, Worm, Trojan...)

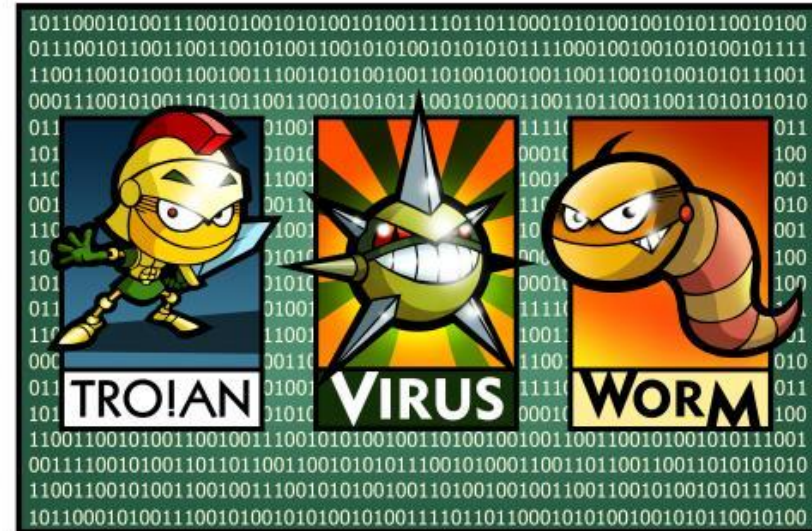
Malware nedir?

- *Malware, short for malicious software, is software used or created to disrupt computer operation, gather sensitive information, or gain access to private computer system.*

- Wikipedia

Zararlı yazılımlar;
bilgisayar operasyonunu bozmak,
hassas verileri toplamak veya bir
bilgisayar sistemine erişim sağlamak
amacıyla kullanılan / yaratılan
yazılımlardır.

- Wikipedia



Malware'ler nasıl bulaşıyor?

- Basit Parolalar...
- Yazılımsal hatlar (Buffer overflow, SQL injection..)

+

- Bilinçsiz kullanım : Email, USB bellekler, Warez...

Bir Worm'un Anatomisi

← ⓘ www.gokhanakin.net ↻ 🔍 Search


Most Visited Getting Started Save to Mendeley OpenDaylight Dlux_1 OpenDaylight Dlux_2 ODL1 - RestConf Doc...

GÖKHAN AKIN
CCIE #38627

Hakkımda Etkinlikler Dökümanlarım Bana Ulaşın [ENG]

Ağ Güvenliği Dökümanlarım

1. Kampüs Ağlarında Aranan Kullanıcıların Tespiti V1.1 - *Metin:* [PDF] *Sunum:* [PDF]
2. DHCP Servisine Yeni Bir Bakış - *Metin:* [PDF] *Sunum:* [PDF]
3. Kurumsal Ağlarda Zararlı Yazılımı Mücadele Klavuzu - *Metin:* [PDF] *Sunum:* [PDF] [PPS]
4. Bir Worm'un Anatomisi - *Metin:* [PDF] *Sunum:* [PPS]
5. P2P Trafik Tespiti için Cisco NBAR Kullanımı - *Metin:* [PDF] *Sunum:* [PPT]



2. Ders

Sunumun Linki:

www.gokhanakin.net

Malware'de Uç Örneklerden biri



STUXNET Solucanı – 2010 İRAN NÜKLEER TESİSLERİNE SALDIRI (APT)

Günümüzde MALWARE trendleri

The screenshot shows the TTNET E-Fatura portal. At the top is the TTNET logo. Below it, there are four rows of information: HESAP NUMARASI (blank), FATURA DÖNEMİ (Kasım 2014), SON ÖDEME TARİHİ (14 Kasım 2014), and ÖDENECEK TUTAR (251,36 TL). To the right of this information is a blue button labeled 'Rehber Fatura videosu için tıklayınız.' and an orange button labeled 'E-Faturamı Görüntüle'. Below the orange button is a text box containing the URL: <http://efatura.ttnet-fatura.info/>. Below the text box is a paragraph of text: 'Faturanızı hesap numarası ile ödeyebilir, otomatik ödeme talimatı ve diğer tüm ödeme işlemlerinizi bu numara üzerinden takip edebilirsiniz.' followed by 'Kredi kartınızla hemen ödemek veya otomatik ödeme talimatı vermek için [tıklayınız](#) ya da 444 0375 TTNET Müşteri Hizmetlerini arayınız.' and 'Faturanızın arka sayfasını görmek için [tıklayınız](#).' A mouse cursor is pointing at the 'tıklayınız' link in the second paragraph. Below the text box is another text box containing the URL: <http://efatura.ttnet-fatura.com/>.

HESAP NUMARASI :

FATURA DÖNEMİ : **Kasım 2014**

SON ÖDEME TARİHİ : **14 Kasım 2014**

ÖDENECEK TUTAR : **251,36 TL**

Rehber Fatura videosu için tıklayınız.

E-Faturamı Görüntüle

URL: <http://efatura.ttnet-fatura.info/>

Faturanızı hesap numarası ile ödeyebilir, otomatik ödeme talimatı ve diğer tüm ödeme işlemlerinizi bu numara üzerinden takip edebilirsiniz.

Kredi kartınızla hemen ödemek veya otomatik ödeme talimatı vermek için [tıklayınız](#) ya da 444 0375 TTNET Müşteri Hizmetlerini arayınız.

Faturanızın arka sayfasını görmek için [tıklayınız](#).

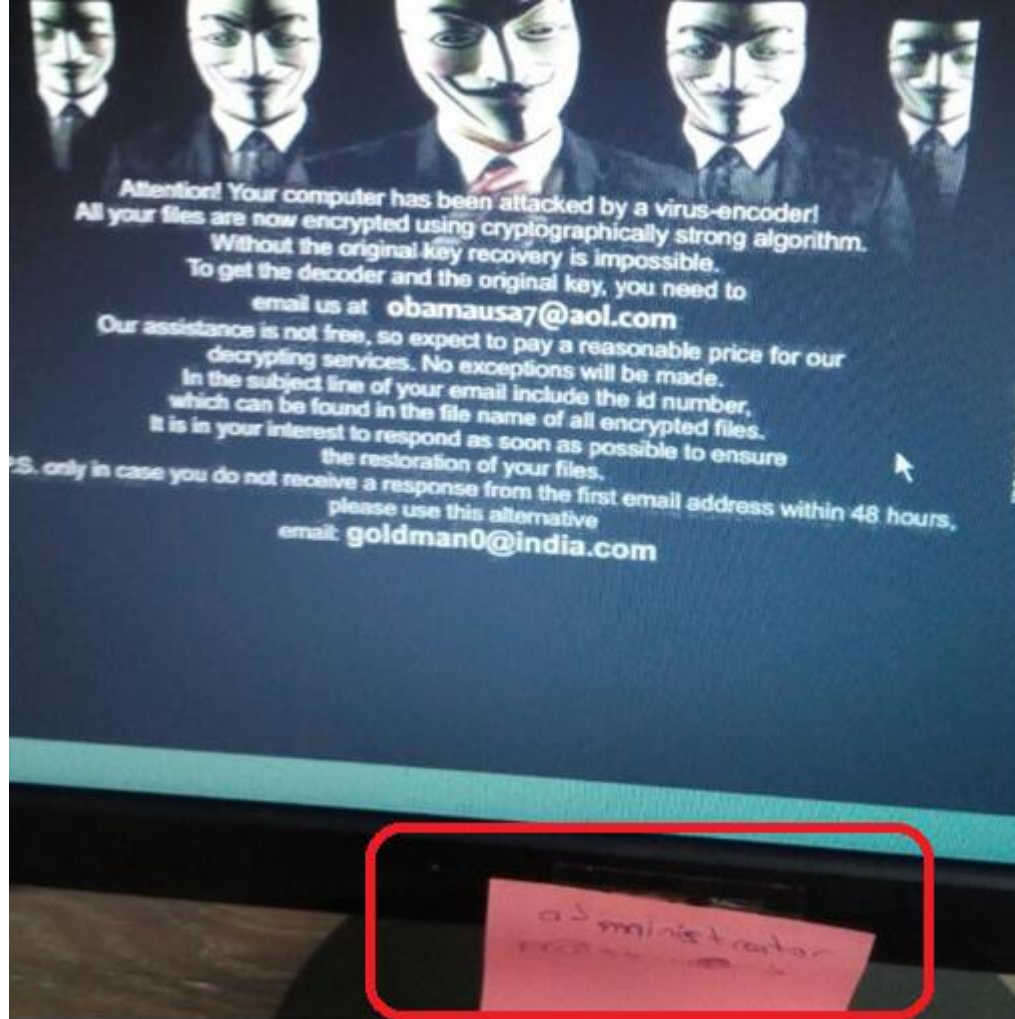
URL: <http://efatura.ttnet-fatura.com/>

2014 – CRYPTOLOCKER SALDIRISI

Günümüzde MALWARE trendleri



Günümüzde MALWARE trendleri



Günümüzde MALWARE trendleri



Ad	Değişirme tarihi
<input type="checkbox"/> 0D01 068.JPG.encrypted	24.03.2015 10:55
<input type="checkbox"/> 0D01 069.JPG.encrypted	24.03.2015 10:55
<input type="checkbox"/> 0D01 071.JPG.encrypted	24.03.2015 10:55
<input type="checkbox"/> 0D01 072.JPG.encrypted	24.03.2015 10:55
<input type="checkbox"/> 0D01 073.JPG.encrypted	24.03.2015 10:55
<input type="checkbox"/> 0D01 074.JPG.encrypted	24.03.2015 10:55
<input type="checkbox"/> 0D01 075.JPG.encrypted	24.03.2015 10:55
<input type="checkbox"/> 0R.70.57-000060.00.jpg.encrypted	24.03.2015 10:55
<input type="checkbox"/> 0R.72.57-000000.00.jpg.encrypted	24.03.2015 10:55
<input type="checkbox"/> 0R.74.00-000000.00.JPG.encrypted	24.03.2015 10:55
<input type="checkbox"/> 001.29.jpg.encrypted	24.03.2015 10:54
<input type="checkbox"/> 1YTU140025T5509.JPG.encrypted	24.03.2015 10:57
<input type="checkbox"/> 02.101.013.JPG.encrypted	24.03.2015 10:54
<input type="checkbox"/> 02.980.021.JPG.encrypted	24.03.2015 10:54
<input type="checkbox"/> 2TU012510-0205.JPG.encrypted	24.03.2015 10:58
<input type="checkbox"/> 2TU012550-0081.jpg.encrypted	24.03.2015 10:58
<input type="checkbox"/> 2TU012610-0067.jpg.encrypted	24.03.2015 10:58
<input type="checkbox"/> 2TU012610-0078.JPG.encrypted	24.03.2015 10:58

2014 – CRYPTOLOCKER SALDIRISI

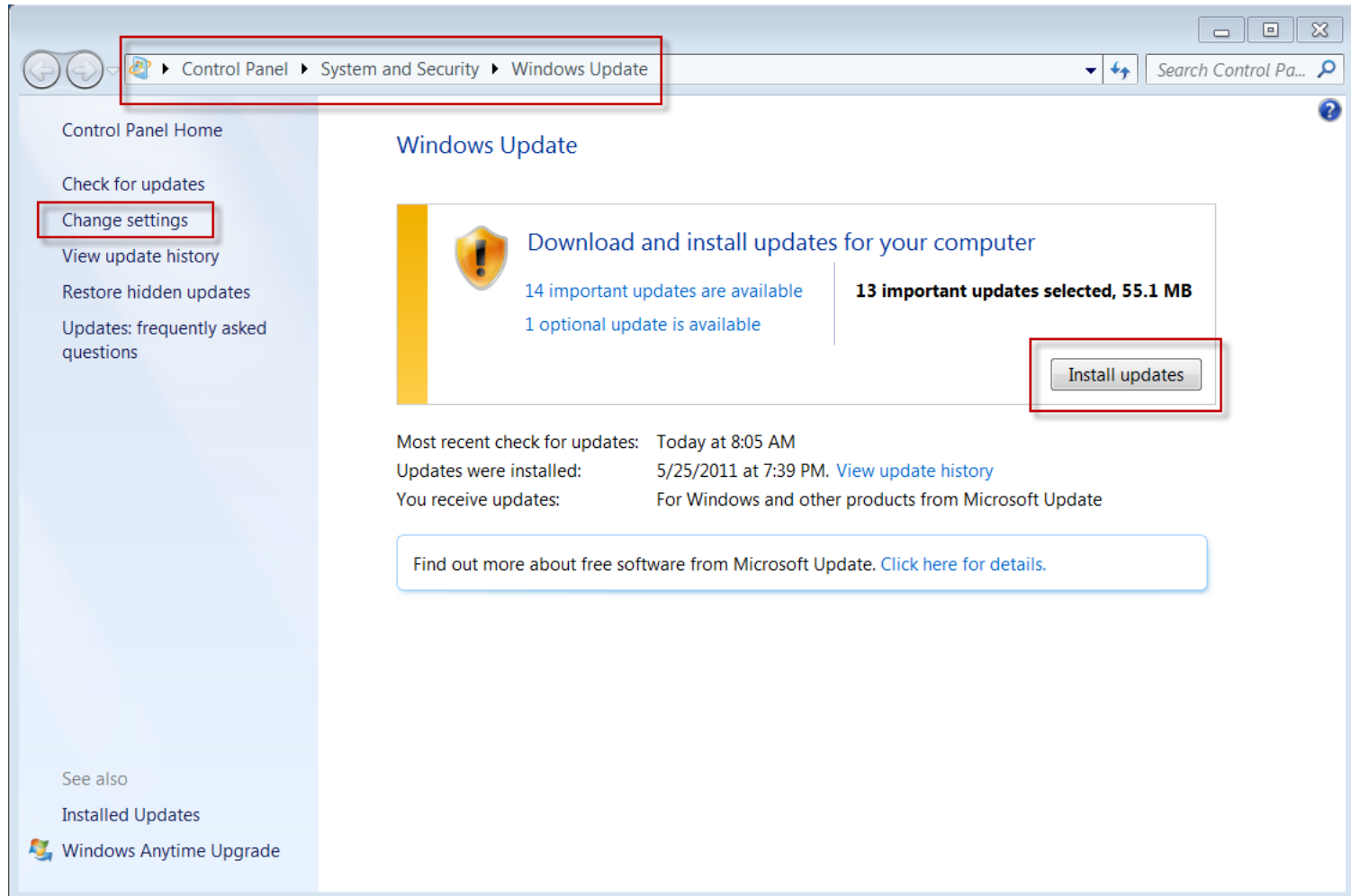
WannaCry Ransomware (Fidye Zararlı Yazılımı)



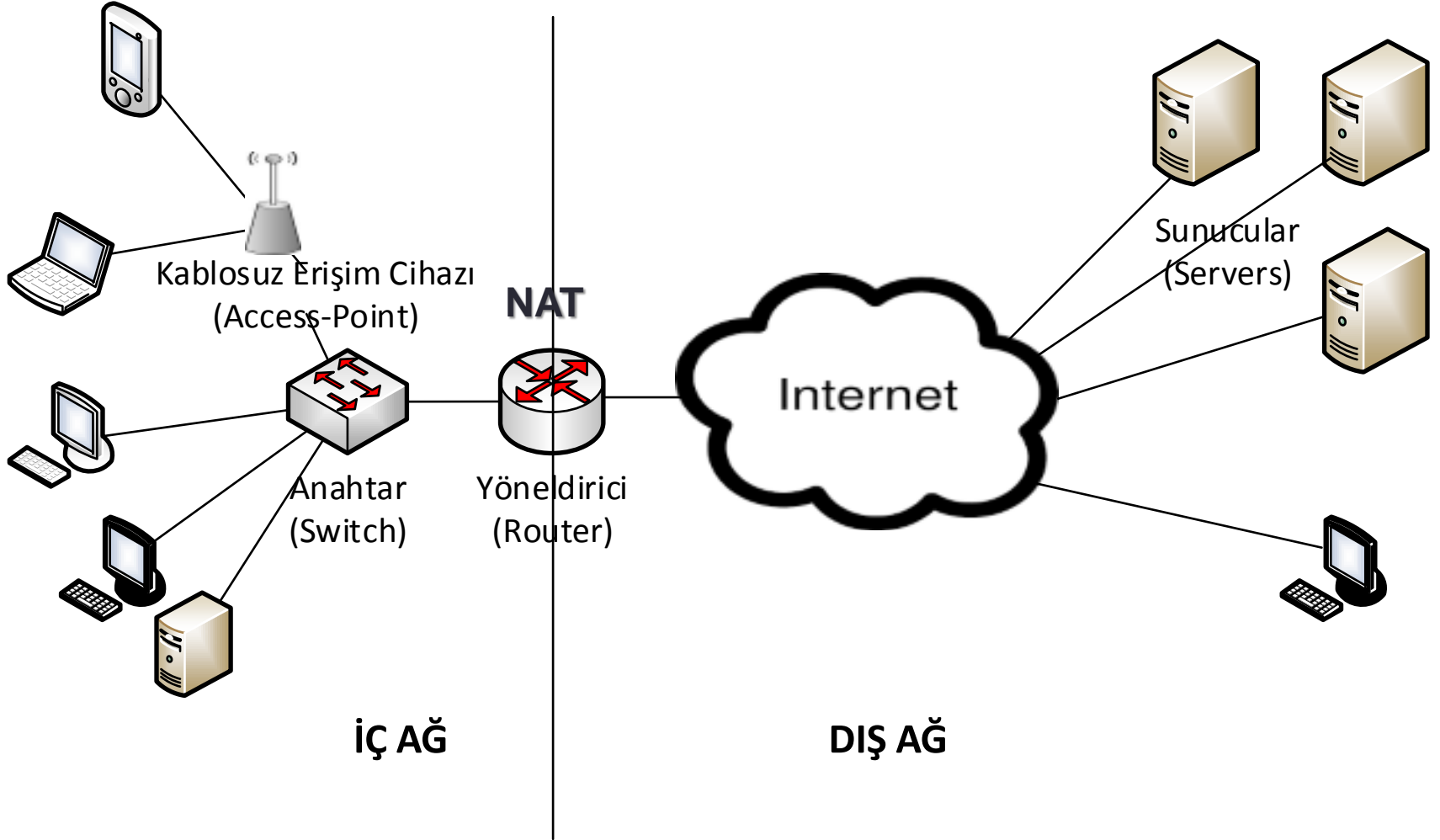
The attack started on Friday, 12 May 2017, and within a day was reported to have infected more than 230,000 computers in over 150 countries.

(Wikipedia)

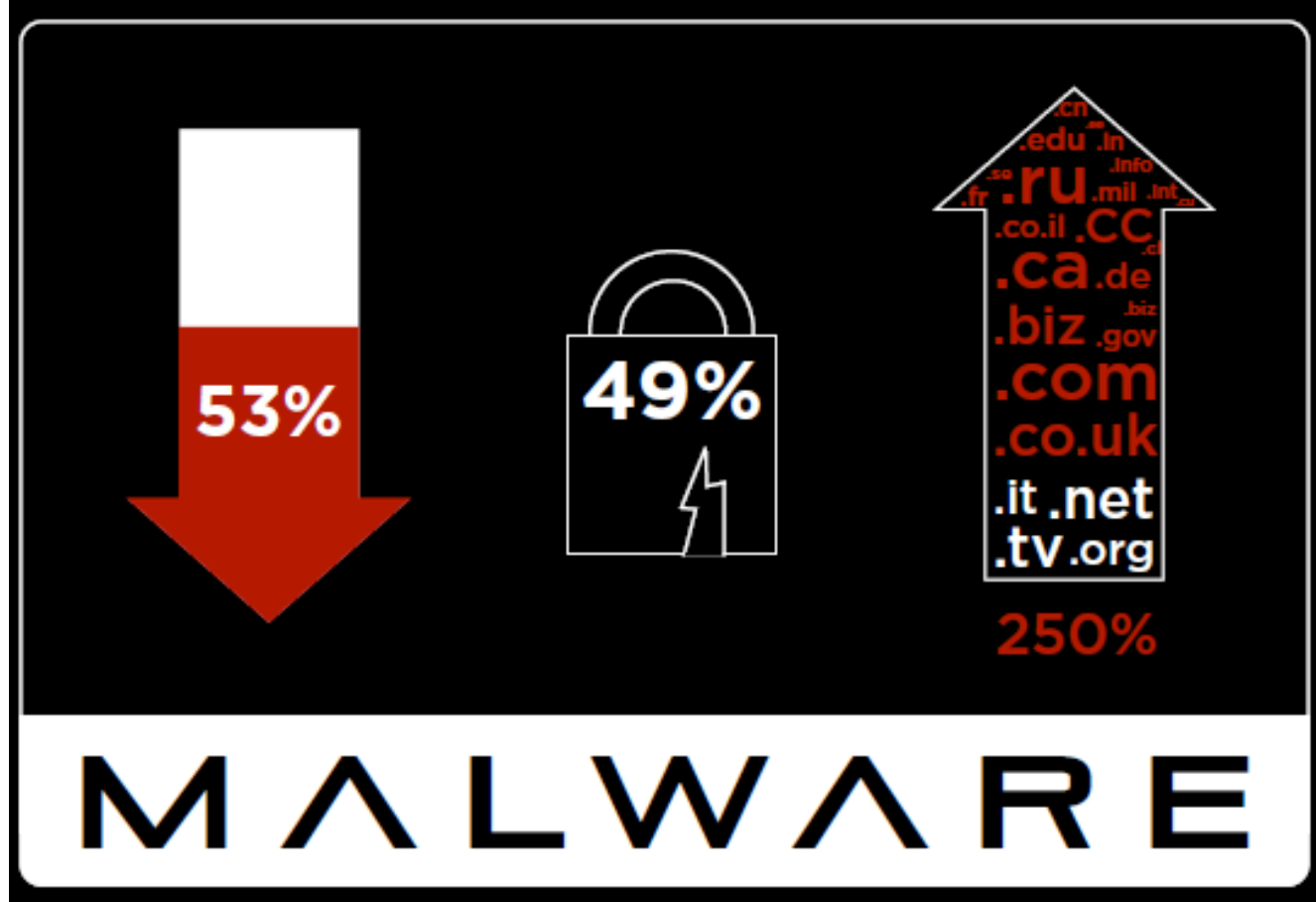
Yazılımsal Hatalar



Neden Bana Bulaşmadı?



Günümüzde MALWARE trendleri



Her gün ortalama 2 farklı tip Malware ortaya çıkıyor.

Güvenlik Açıklarının sadece %49'u için Zararlı Yazılım'lar geliştirilmiş.

Malware Geliştirme Amaçları

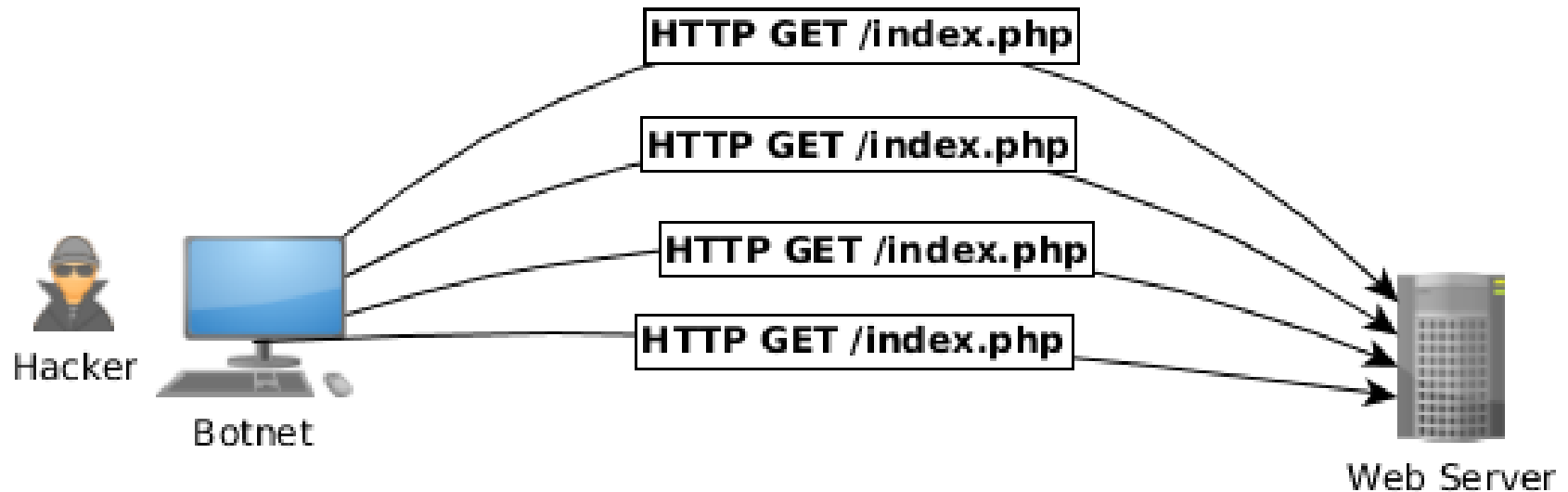
- GOVERNMENT (Ülkeler arası Siber Savaşlar)
- ORGANİZE SUÇLAR
- TERORİST AKTİVİTELER
- AKTİVİSTLER (HACKTİVİZM)



DoS veya DDoS Servis Dışı Bırakma Atakları

Servis Dışı Bırakma Atakları

Denial of Service (DoS) Attacks



İlk Ciddi DoS Saldırısı

- MafiaBoy 15 yaşında bir Öğrenci Montreal, Canada.
- Şubat 2000'de Yahoo!, Amazon.com, Dell, Inc., E*TRADE, eBay ve CNN.

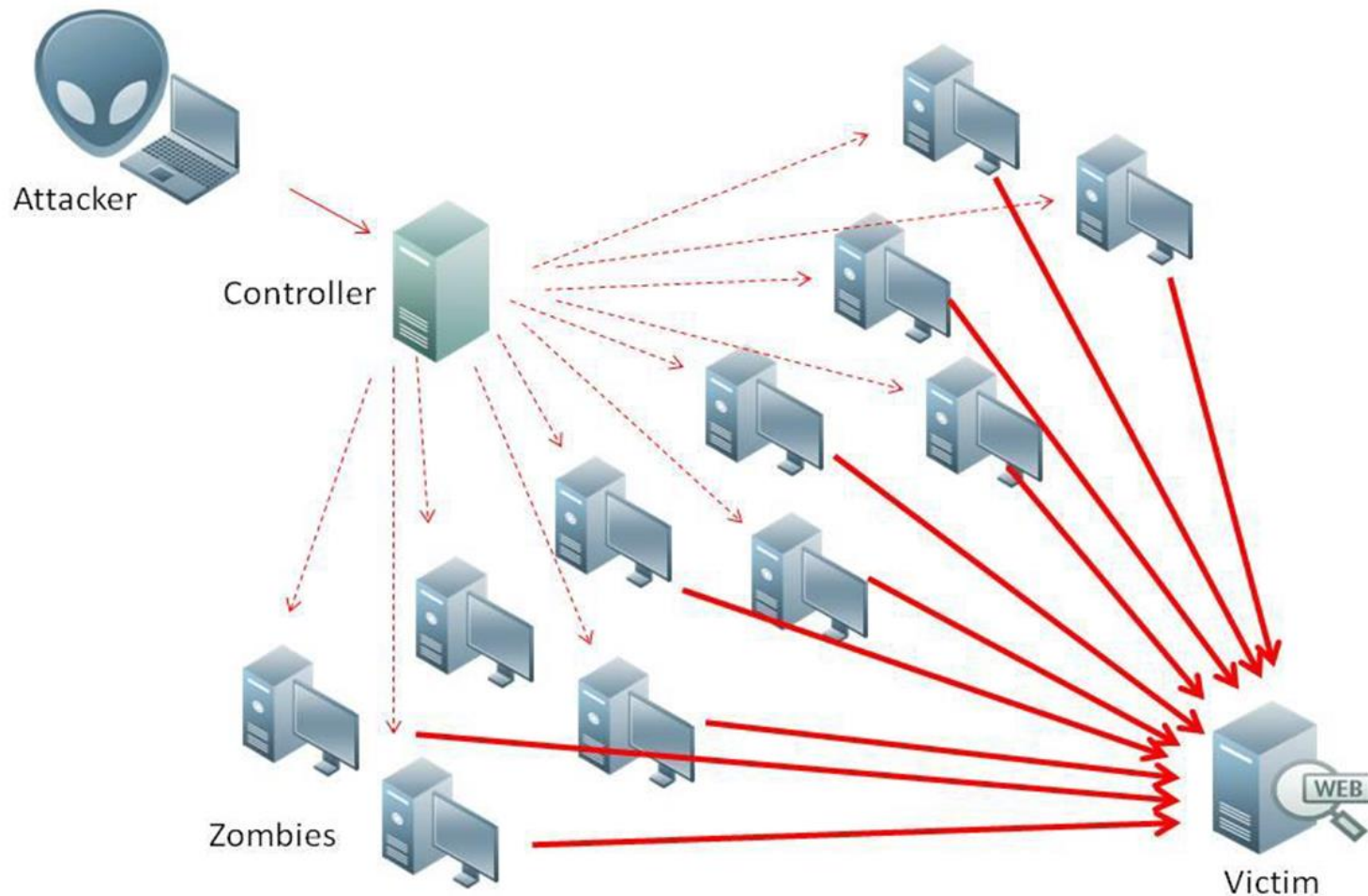
2001'de 8 aylık kamu cezası ve
internet kullanım kısıtlaması

2008 Kitap "Mafiaboy: How I Cracked
the Internet and Why It's Still Broken".

Ve bolca TV Programı 😊



DDoS (Distributed Denial of Service)



delete.net/tr-alan-adlarinda-erisim-problemi-yasaniyor-66774

Search

★

📁

🔒

⬇

🏠

🔍

.tr Alan Adlarında Erişim Problemi Yaşanıyor!

Paylaşın



İnternet

Dün öğle saatlerinde başlayan .tr alan adlarına sahip sitelerde yaşanan problemler henüz kesin olarak çözülmedi. Peki, .tr alan adı probleminin kaynağı ne?

15.12.2015 / 12:45



**Siemens**
Yetkili Satıcılarında!



Türkiye'ye özgü .tr alan adlarında dün öğle saatlerinde problem meydana geldi. .tr uzantılı alan adlarında meydana gelen erişim problemlerinin kaynağı ilk araştırmalarda DNS sunucularının taleplere cevap vermemesi

googleads.g.doubleclick.net... ş ve konuyla ilgili çözüm çalışmaları başlamıştı.



KARANLIK TARAFIN GÜCÜNÜ
HENÜZ GÖRMEDİNİZ

250 TL HEDİYE ÇEKİ



Sadece Teknosa'da! >>



TL1949 Hemen Satın Al!

gruppai.com

Kar edebilmeyi öğrenin.
Ücretsiz eğitiminizi hemen alın!

PrimeTrade



TL159 Hemen Satın Al!

gruppai.com



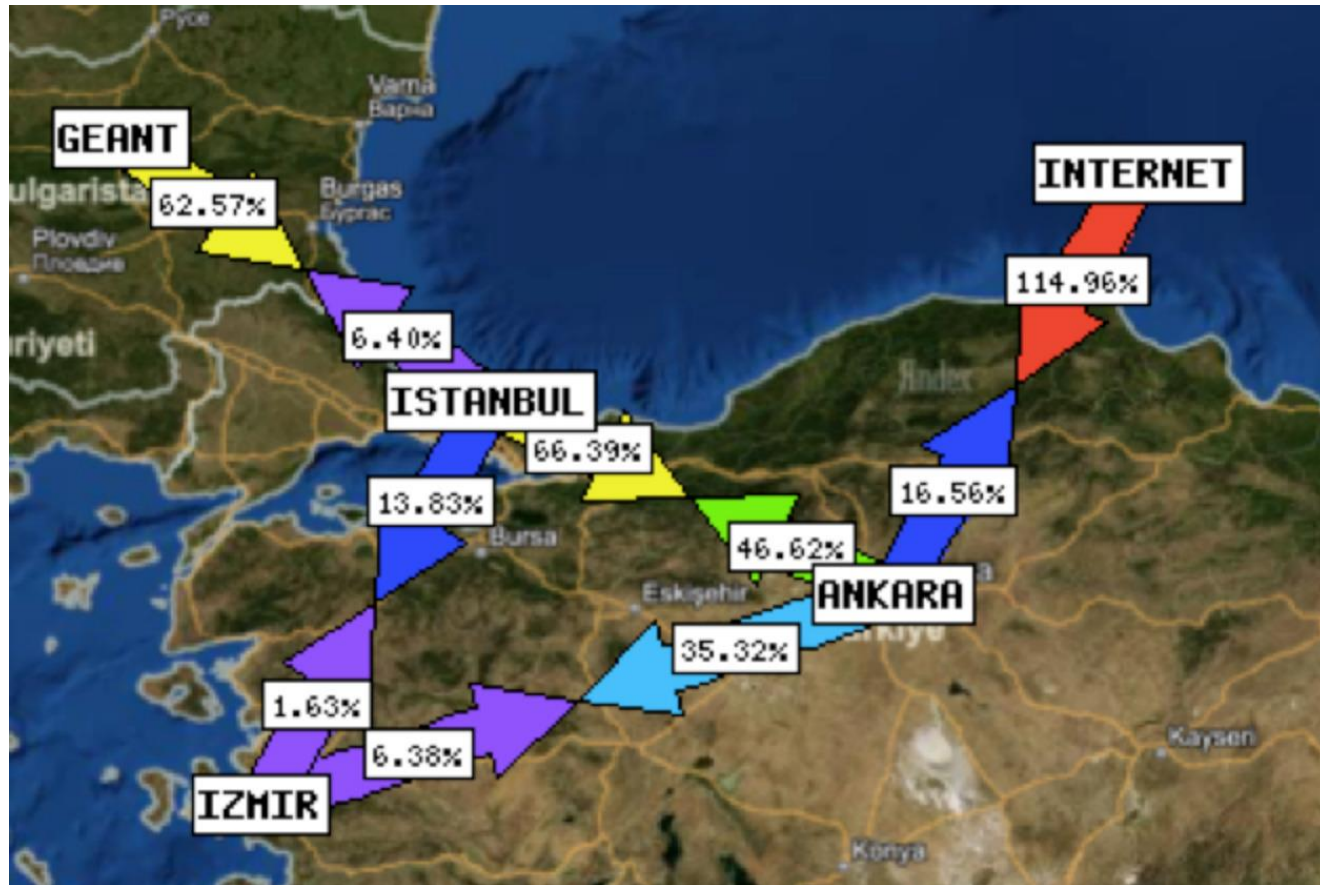
SINIRLARI ZORLAYANLARA SINIRSIZ PAKET!

turknet.net

TürkNet ile sınırsız internetin keyfini çıkartın.

www.ag.org.tr

.TR Adreslerine DDoS Saldırısı



SGK ya Asılsız Siber Saldırı Haberi

Haberin Tarihi: Aralık 18, 2015 Bu Haberi Sosyal Medyada Paylaş: [Twitter](#) [Facebook](#) [LinkedIn](#)



SGK yetkililerinden siber saldırının asılsız olduğu sistemdeki sorunun tamamen taşınma sürecine bağlı olduğu bu konuda duyurunun kurumumuz tarafından yayınlandığı bilgisini aldık.Bu tür haberlere itibar edilmemesi rica olunup en kısa süre içerisinde hizmet vermeye başlanacaktır.

Sonraki Haber



Bölümün en çok okunan haberleri



Yaşanan Hizmet Kesintileri Hakkında Basın Duyurusu



Veri Merkezi Taşınması



Bedeli Ödenecek İlaçlar Listesinde

Yapılan Düzenlemeler Hakkında Duyuru 2015/50 (Ek) (Genel Sağlık Sigortası Genel Müdürlüğü)



Medula Eczane Reçete ve Rapor Web

Servisleri Kullanım Kılavuzu



Tıbbi Malzeme Listeleri Tıbbi Malzeme Alan

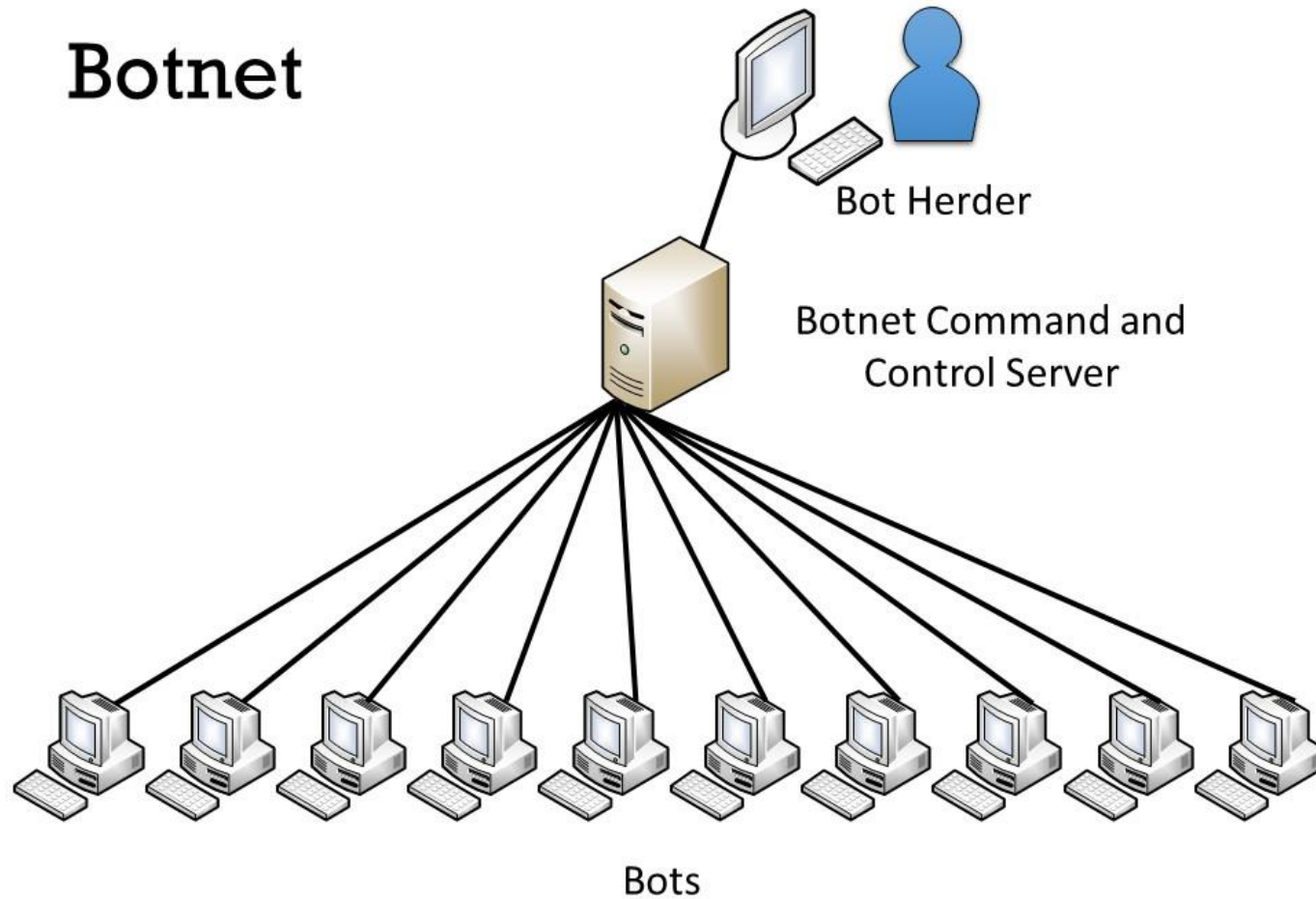
Tanımlarına Ürünlerin Eşleştirilmesi İle İlgili Önemli Duyuru-18 (Genel Sağlık Sigortası Genel Müdürlüğü)

Kim, nasıl yapıyor ??



Botnet

Botnet



Zeus Botnet

rigim P... X Zeus Tracker :: Monitor X +

ker.abuse.ch/monitor.php

Zeus Tracker :: Monitor

Below is a list of all Zeus C&Cs as well as Fake URLs which are currently known to Zeus Tracker. You can browse the Zeus Tracker to get a list of Zeus C&Cs and FakeURLs for a specified country or AS. Additionally, Zeus Tracker provides a feature which allows to filter the Zeus C&Cs for specified nameservers, level, status and many more.

Each Zeus C&C or FakeURL is tagged with a *level*. The level indicates which kind of IP the Host is hosted on. Here is an overview about the levels and its meaning:

Level	Description
Level 1	Bulletproof hosted
Level 2	Hacked webservice
Level 3	Free hosting service
Level 4	Unknown
Level 5	Hosted on a FastFlux botnet

Additionally, every host is at least in one of the following category:

- Hosts which are tagged as **CC** are Zeus Command&Control servers
- Hosts which are tagged as **FU** are referenced by Zeus as FakeURLs

You can also search the Zeus Tracker for domains, IPs, urls, MD5 hashes or FakeURLs:

Browse: [Zeus BinaryURLs](#) | [Zeus ConfigURLs](#) | [Zeus Dropzones](#)
Malware family filter: [Zeus](#) | [Ice IX](#) | [Citadel](#) | [KINS](#)
Set a filter for the list below: [Remove filter \(Show all\)](#) | [online Zeus hosts](#) | [offline Zeus hosts](#) | [Zeus hosts with files online](#) | [order by lastupdated](#)
Filter C&C server tagged with level: [Level 1 \(Bulletproof\)](#) | [Level 2 \(Hijacked sites\)](#) | [Level 3 \(Free webhosting\)](#) | [Level 4 \(Unknown\)](#) | [Level 5 \(FastFlux hosted\)](#)
[Subscribe this list via RSS feed](#)

Dateadded	Malware	Host	IP address	Level	Status	Files Online	SBL	Country	AS number	Uptime
2015-12-19	VMZeus	superclasp.com	107.180.49.252	2	online	2	SBL 201414		AS26496	23:50:10
2015-12-18	VMZeus	thetankshop.com.au	27.121.66.4	2	online	1	SBL 280004		AS24446	49:23:21
2015-12-09	VMZeus	emreerdem.com.tr	85.95.237.78	2	online	2	SBL 728988		AS42926	270:18:46
2015-12-08	Zeus	beautifulmindsinc.com	184.168.56.1	4	online	1	Not listed		AS26496	293:01:31
2015-10-09	VMZeus	balcaolocal.com	131.72.52.210	2	online	2	Not listed		AS61718	338:59:59
2015-09-13	VMZeus	wavufilm.com	119.59.120.8	2	online	2	SBL 274234		AS56067	338:59:59
2014-11-15	Zeus	championbft.com	104.207.130.93	4	online	1	Not listed		AS20473	338:59:59
2014-05-29	Citadel	www.loongweed.com	202.142.215.16	2	online	1	SBL 222707		AS7654	338:59:59

of Zeus C&Cs displayed: 8
of Zeus C&Cs in Zeus Tracker: 568 [\[Remove all filters\]](#)

<https://zeustracker.abuse.ch/>

Son Kullanıcılar için

Basit Güvenlik Önerileri

- İşletim Sistemi güncellemeleri yapın
- Anti virüs yazılımı kullanın
- Güvenlik Duvarı kullanın
- Lisanssız yazılım kullanmayın
- Düzenli yedek alın
- Güvenli bağlantı kullanın (SSL etc)
- Ekleri dikkatli açın (.zip, .exe dosyalarını açmayın)
- Güçlü şifreler kullanın, kişisel bilgilerinizi gerekmedikçe paylaşmayın

Teşekkürler



AYD

Ağ Yöneticileri Derneği

Dernek Sitesi: www.agyoneticileri.org

Eğitim Portalı: www.ag.org.tr

Email: [egitim @ agyoneticileri.org](mailto:egitim@agyoneticileri.org)

<http://www.facebook.com/AgYoneticileriDerneği>