



# Bulut Bilişim ve Güvenlik

Bahtiyar BİRCAN

Uzman Araştırmacı  
TÜBİTAK BİLGEM

8 Haziran 2011

- Bulut Bilişim nedir?
- Bulut Bilişim Güvenlik Riskleri
- Servis olarak Güvenlik
- Servis olarak Saldırı

- “Bulut bilişim, düşük yönetim çabası veya servis sağlayıcı etkileşimi ile, hızlı alınıp salıverilebilen ayarlanabilir bilişim kaynaklarının paylaşılır havuzuna, istendiğinde ve uygun bir şekilde ağ erişimi sağlayan bir modeldir.” (NIST)
- Cloud computing refers to the on-demand provision of computational resources (data, software) via a computer network, rather than from a local computer. ( Wikipedia )

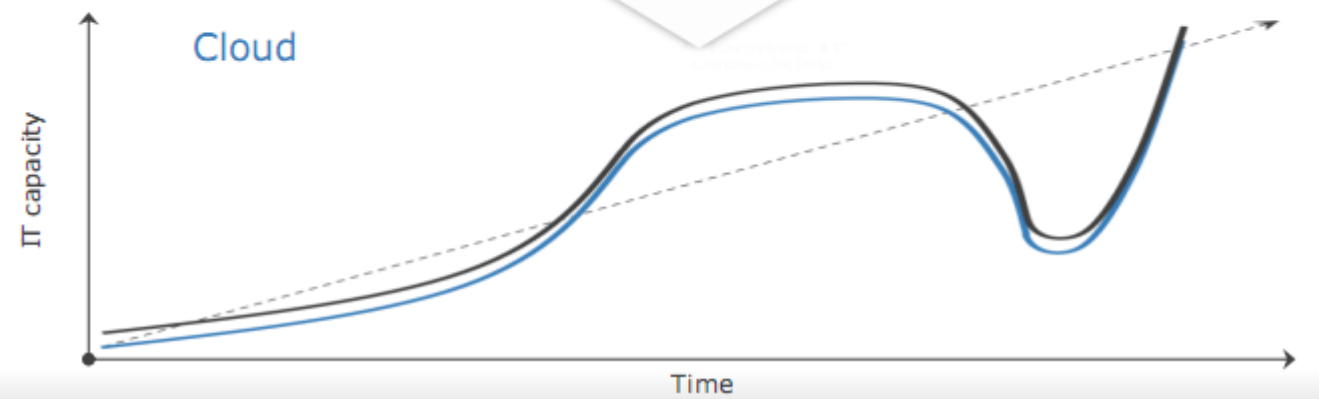
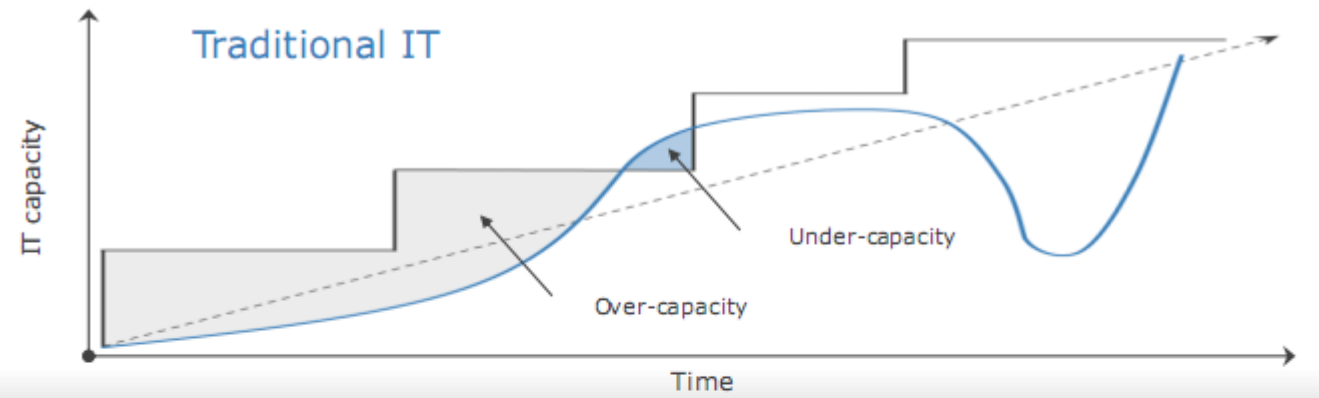
- Self-servis
- Çevrim içi - Her zaman erişilebilir
- Dinamik – İhtiyaca göre kapasite azaltma veya arttırabilme
- Kullandığın kadar öde
- Özel veya paylaşımlı olarak kullanabilme



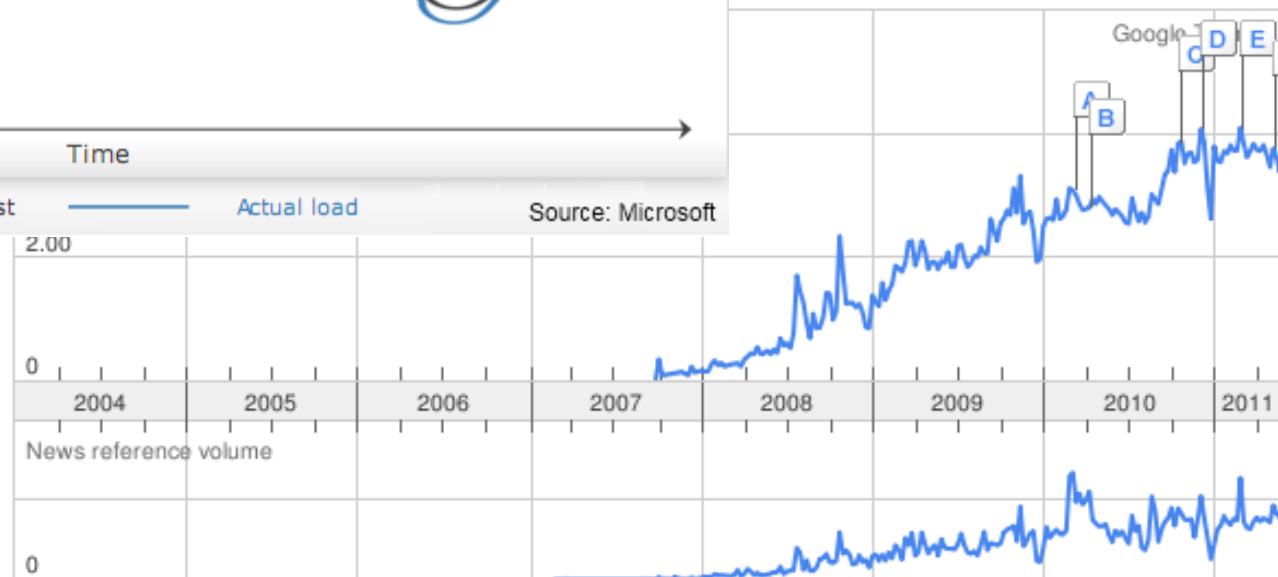
- Yüksek işlemci gücü
- Yüksek disk kapasitesi
- Yüksek bant genişliği
- Dağıtık mimari



# Neden Bulut Bilişim?



— Capacity    ..... Load forecast    — Actual load    Source: Microsoft



**AWS Management Console - Mozilla Firefox**

File Edit View History Bookmarks Tools Help

amazon.com https://console.aws.amazon.com/ec2/home?region=us-east-1#s=Instances

aws.amazon.com AWS | Products | Developers | Community | Support | Account **Welcome, Bahtiyar Bircan** | Settings | Sign Out

AWS Elastic Beanstalk S3 EC2 VPC CloudWatch Elastic MapReduce CloudFront CloudFormation RDS SNS IAM

**Navigation**

**Region:** US East (Virginia)

- > EC2 Dashboard
- INSTANCES
  - > Instances
  - > Spot Requests
  - > Reserved Instances
- IMAGES
  - > AMIs
  - > Bundle Tasks
- ELASTIC BLOCK STORE
  - > Volumes
  - > Snapshots
- NETWORKING & SECURITY
  - > Security Groups
  - > Elastic IPs
  - > Placement Groups
  - > Load Balancers
  - > Key Pairs

**My Instances**

Launch Instance Instance Actions Show/Hide Refresh Help

Viewing: All Instances All Instance Types

| Name                                | Instance | AMI ID     | Root         | Root Device I | Zone      | Type       | Status   | Lifecycle |        |
|-------------------------------------|----------|------------|--------------|---------------|-----------|------------|----------|-----------|--------|
| <input checked="" type="checkbox"/> | empty    | i-9948fdf7 | ami-8e1fece7 | ebs           | /dev/sda1 | us-east-1d | t1.micro | stopped   | normal |

1 EC2 Instance selected

**EC2 Instance: i-9948fdf7**

Description Monitoring Tags

|  |                                    |
|--|------------------------------------|
| <b>AMI:</b> amzn-ami-2011.02.1.x86_64-ebs (ami-8e1fece7) | <b>Zone:</b> us-east-1d            |
| <b>Security Groups:</b> quick-start-1                    | <b>Type:</b> t1.micro              |
| <b>Status:</b> stopped                                   | <b>Owner:</b> 466732463901         |
| <b>VPIC ID:</b> -  | <b>Subnet ID:</b> -                |
| <b>Source/Dest. Check:</b>                               | <b>Virtualization:</b> paravirtual |
| <b>Placement Group:</b>                                  | <b>Reservation:</b> r-0f9ef963     |
| <b>RAM Disk ID:</b> -                                    | <b>Platform:</b> -                 |
| <b>Key Pair Name:</b> key1                               | <b>Kernel ID:</b> aki-427d952b     |
| <b>Monitoring:</b> basic                                 | <b>AMI Launch Index:</b> 0         |
| <b>Elastic IP:</b> -                                     | <b>Root Device:</b> sda1           |
| <b>Root Device Type:</b> ebs                             | <b>Tenancy:</b> default            |
| <b>Lifecycle:</b> normal                                 |                                    |

© 2008 - 2011, Amazon Web Services LLC or its affiliates. All right reserved. | Feedback | Support | Privacy Policy | Terms of Use | An amazon.com company

Server FoxyProxy: 10kaplan

**Welcome, Bahtiyar Bircan** | Settings | Sign Out

Resources

are using the following Amazon resources in the US East (Virginia) Refresh

- 0 Running Instances
- 0 Elastic IPs
- 1 EBS Volume
- 0 EBS Snapshots
- 1 Key Pair
- 2 Security Groups
- 0 Load Balancers
- 0 Placement Groups

Related Links

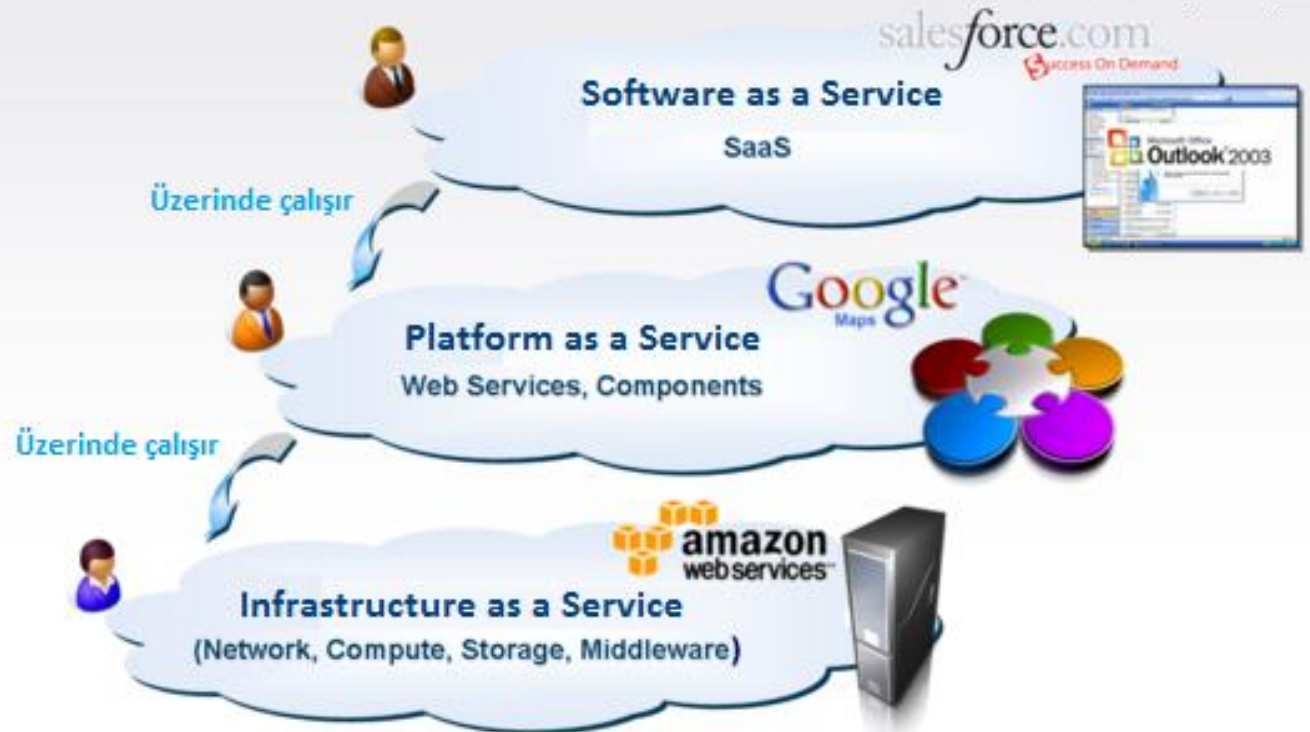
- Documentation
- EC2 Resources
- Help
- Feedback
- Report an Issue

© 2008 - 2011, Amazon Web Services LLC or its affiliates. All right reserved. | Feedback | Support | Privacy Policy | Terms of Use | An amazon.com company

Server FoxyProxy: 10kaplan

- Servis olarak Altyapı – SoA (IaaS)
- Servis olarak Platform – SoP (PaaS)
- Servis olarak Yazılım – SoY (SaaS)

## Bulut Hizmet Modelleri



# Bulut Bilişim Güvenlik Riskleri



- Hizmet devamlılığı
  - Amazon EC2 hizmet kesintisi
- Veri güvenliği ve gizliliği
- Güvenlik standartlarına uyumluluk
- Bulut bilişim servislerine saldırılar
- Ele geçirilmiş sunucu şablonları

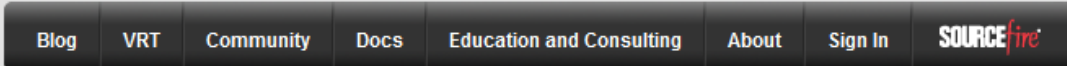

# Servis olarak Güvenlik (Security as a Service)



- Bulut bilişimin faydalarından güvenlik ürünleri de yararlanmaktadırlar.
- Bulut bilişim sayesinde güvenlik ürünleri daha hızlı, daha verimli ve daha etkin bir şekilde müşterilerine hizmet verebilmektedirler
- Alanlar
  - Antivirüs
  - Saldırı Tespit
  - Açıklık tarama
  - Güvenlik Testleri
  - Adli analiz



- Sourcefire popüler açık kaynaklı saldırı tespit sistemi olan Snort'un bulut üzerinden çalışan versiyonunu duyurdu.



Blog VRT Community Docs Education and Consulting About Sign In SOURCEfire

## Snort News & Events

[Home Page](#) > [News](#) > Snort Now Available on the Amazon Cloud

### Snort Now Available on the Amazon Cloud

Hi everyone,

Snort and Sourcefire VRT Rules are now available as an Amazon Machine Image (AMI). Amazon EC2 customers can now deploy Snort with the latest VRT Rules as an AMI. Those interested in using Snort on EC2 should start by reviewing the Snort on EC2 Quick Start Guide we've posted to Snort.org [here](#). You can also read the press release [here](#).

To download the AMI:

- 1: <https://console.aws.amazon.com/ec2/home#c=EC2&s=LaunchInstanceWizard>
- 2: Log in to your EC2 Account
- 3: Select "Launch Instance"
- 4: Go to Community AMI's - Do a find on Sourcefire

- Açıklık tarama yazılımlarını da artık bulut üzerinden servis olarak almak mümkün.

## TENABLE SERVICES

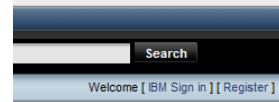


### Nessus Perimeter Service

The Tenable Nessus Perimeter Service is an enterprise-class remote vulnerability scanning service that may be used to audit Internet facing IP addresses for both network and web application vulnerabilities "from the cloud". Subscribers, who log in to Nessus scanners hosted in Tenable's secure datacenter, may employ Tenable Nessus Perimeter Service to scan any number of Internet facing sites covering a wide variety of devices - desktop computers, mobile laptops, iPhones - wherever is convenient and as often as needed, all for one low flat fee.

- > Product Overview
- > Key Benefits
- > Subscribe Today

The Tenable Nessus Perimeter Service portal provides secure access to detailed vulnerability audits and remediation information on Tenable's



and



- Services by industry
- Services A-Z
- Institute for Business Value
- Studies, papers, briefs

**Service detail**

Continuous vulnerability assessment of your IT assets, including web applications and databases, is essential to effectively securing your infrastructure and avoiding policy violations. You need a simple, cost-effective way to limit potential threats.

IBM Managed Security Services (Cloud Computing) - hosted vulnerability management provides cloud-based internal and external infrastructure scanning through a single portal, helps you more easily manage compliance requirements and specifies steps you can take to remediate vulnerabilities.

**Highlights**

- Helps manage compliance with security initiatives by scanning for and classifying vulnerabilities
- Provides remediation steps and data to assess and manage security risks to help reduce threat exposure
- Helps reduce cost and complexity of security maintenance through IBM cloud security services

**Innovate with Cloud Computing**

Rethink IT and reinvent your business with a new model for consuming and delivering IT and business services

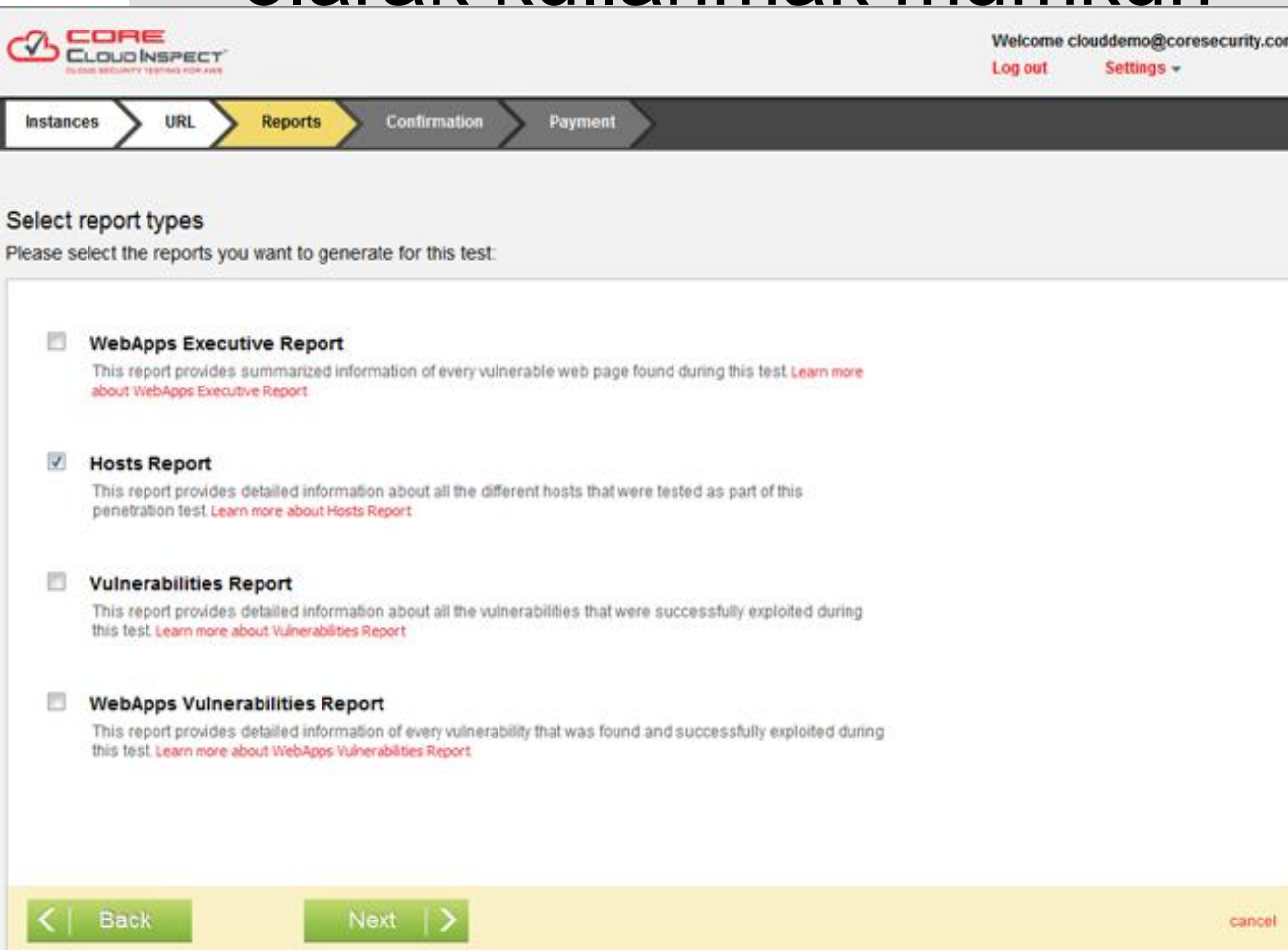
→ Cloud computing from IBM

**Web Seminar**

"Sasser," "Blaster" and "MyDoom": Why Your Network and AV Providers Can't Stop Them. Watch this educational



- Güvenlik testlerini bulut tabanlı servis olarak kullanmak mümkün



**CORE CLOUD INSPECT**  
CLOUD SECURITY TESTING FOR AWS

Welcome clouddemo@coresecurity.com  
Log out Settings

Instances URL **Reports** Confirmation Payment

Select report types  
Please select the reports you want to generate for this test:

- WebApps Executive Report**  
This report provides summarized information of every vulnerable web page found during this test. [Learn more about WebApps Executive Report](#)
- Hosts Report**  
This report provides detailed information about all the different hosts that were tested as part of this penetration test. [Learn more about Hosts Report](#)
- Vulnerabilities Report**  
This report provides detailed information about all the vulnerabilities that were successfully exploited during this test. [Learn more about Vulnerabilities Report](#)
- WebApps Vulnerabilities Report**  
This report provides detailed information of every vulnerability that was found and successfully exploited during this test. [Learn more about WebApps Vulnerabilities Report](#)

Back Next cancel

+1.800.610.2833

Search

Subscribe via RSS

Type here to search...

...gnation for existing security frameworks  
...etration test of your installation. And as any  
...ternet doubtlessly knows, this is a complex,  
...issues, has introduced an on-demand service  
...lined and cost-effective avenue available.

...st web portal for seven days. During that time,  
...tinue the service for a second week, we will

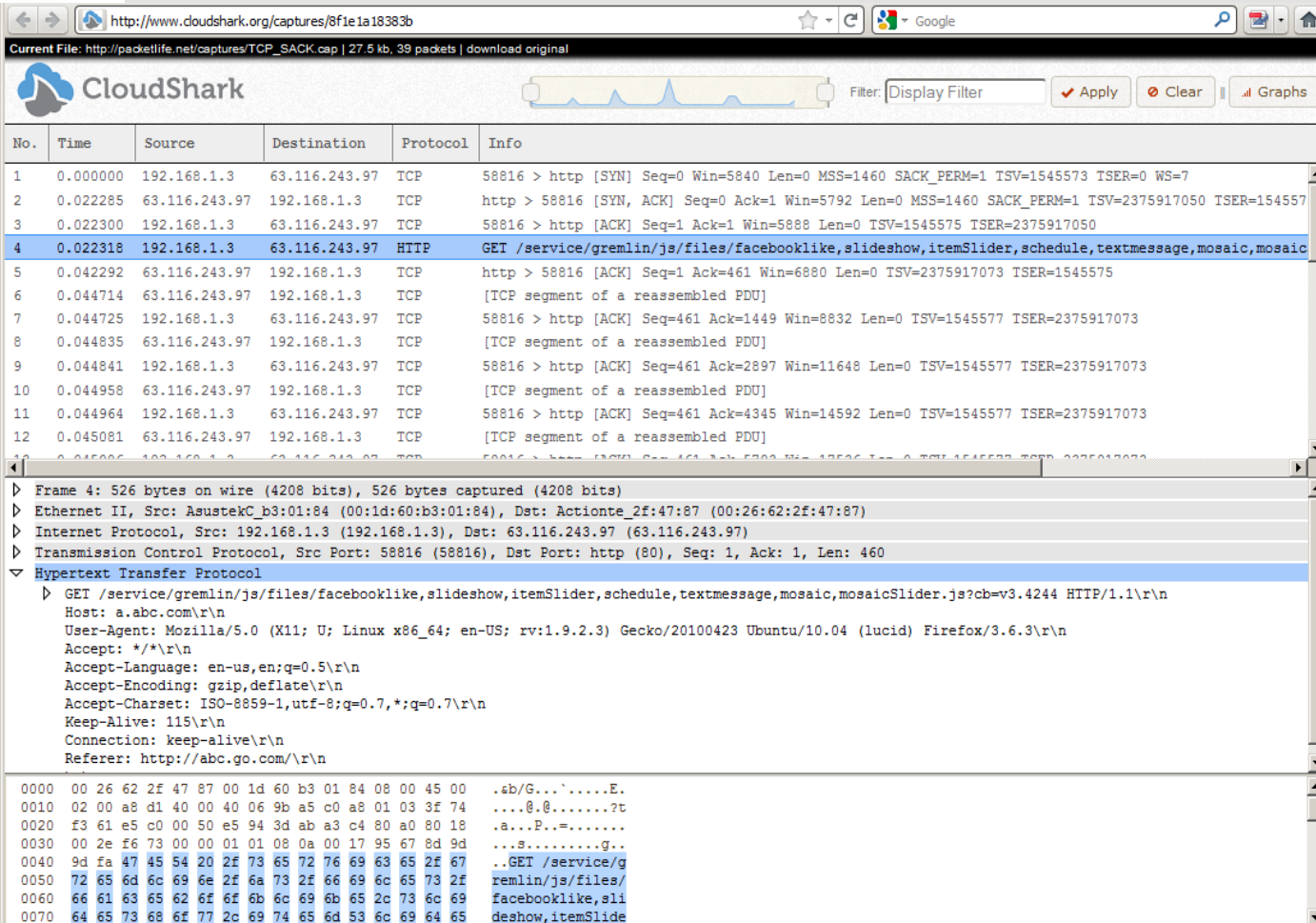
...etration testing resources, from  
...mote solutions using our security console,  
...d our pricing is notably competitive.

...nular. No point in your network that was  
...security management benchmarks are  
...into the following analysis and performance

...dentify and evaluate your network topology,  
...active hosts, IP addresses, installed operating systems, open network ports, and all installed security devices.

...Analysis entails performing application mapping, network scanning/fuzzing, and vulnerability analysis. It effectively identifies

- Ağ tabanlı adli analizleri artık doğrudan bulut üzerinden yapmak mümkün



Current File: http://packetlife.net/captures/TCP\_SACK.cap | 27.5 kb, 39 packets | download original

| No. | Time     | Source        | Destination   | Protocol | Info  |
|-----|----------|---------------|---------------|----------|---|
| 1   | 0.000000 | 192.168.1.3   | 63.116.243.97 | TCP      | 58816 > http [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSV=1545573 TSER=0 WS=7  |
| 2   | 0.022285 | 63.116.243.97 | 192.168.1.3   | TCP      | http > 58816 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSV=2375917050 TSER=154557                                  |
| 3   | 0.022300 | 192.168.1.3   | 63.116.243.97 | TCP      | 58816 > http [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSV=1545575 TSER=2375917050   |
| 4   | 0.022318 | 192.168.1.3   | 63.116.243.97 | HTTP     | GET /service/gremlin/js/files/facebooklike,slideshow,itemSlider,schedule,textmessage,mosaic,mosaicSlider.js?cb=v3.4244 HTTP/1.1\r\n |
| 5   | 0.042292 | 63.116.243.97 | 192.168.1.3   | TCP      | http > 58816 [ACK] Seq=1 Ack=461 Win=6880 Len=0 TSV=2375917073 TSER=1545575   |
| 6   | 0.044714 | 63.116.243.97 | 192.168.1.3   | TCP      | [TCP segment of a reassembled PDU]  |
| 7   | 0.044725 | 192.168.1.3   | 63.116.243.97 | TCP      | 58816 > http [ACK] Seq=461 Ack=1449 Win=8832 Len=0 TSV=1545577 TSER=2375917073  |
| 8   | 0.044835 | 63.116.243.97 | 192.168.1.3   | TCP      | [TCP segment of a reassembled PDU]  |
| 9   | 0.044841 | 192.168.1.3   | 63.116.243.97 | TCP      | 58816 > http [ACK] Seq=461 Ack=2897 Win=11648 Len=0 TSV=1545577 TSER=2375917073   |
| 10  | 0.044958 | 63.116.243.97 | 192.168.1.3   | TCP      | [TCP segment of a reassembled PDU]  |
| 11  | 0.044964 | 192.168.1.3   | 63.116.243.97 | TCP      | 58816 > http [ACK] Seq=461 Ack=4345 Win=14592 Len=0 TSV=1545577 TSER=2375917073   |
| 12  | 0.045081 | 63.116.243.97 | 192.168.1.3   | TCP      | [TCP segment of a reassembled PDU]  |

Frame 4: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits)

Ethernet II, Src: AsustekC\_b3:01:84 (00:1d:60:b3:01:84), Dst: Actionte\_2f:47:87 (00:26:62:2f:47:87)

Internet Protocol, Src: 192.168.1.3 (192.168.1.3), Dst: 63.116.243.97 (63.116.243.97)

Transmission Control Protocol, Src Port: 58816 (58816), Dst Port: http (80), Seq: 1, Ack: 1, Len: 460

Hypertext Transfer Protocol

```

GET /service/gremlin/js/files/facebooklike,slideshow,itemSlider,schedule,textmessage,mosaic,mosaicSlider.js?cb=v3.4244 HTTP/1.1\r\n
Host: a.abc.com\r\n
User-Agent: Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.2.3) Gecko/20100423 Ubuntu/10.04 (lucid) Firefox/3.6.3\r\n
Accept: */*\r\n
Accept-Language: en-us,en;q=0.5\r\n
Accept-Encoding: gzip,deflate\r\n
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
Keep-Alive: 115\r\n
Connection: keep-alive\r\n
Referer: http://abc.go.com/\r\n

```

0000 00 26 62 2f 47 87 00 1d 60 b3 01 84 08 00 45 00 .sb/G...E.

0010 02 00 a8 d1 40 00 40 06 9b a5 c0 a8 01 03 3f 74 ....@.....?t

0020 f3 61 e5 c0 00 50 e5 94 3d ab a3 c4 80 a0 80 18 .a...P.....

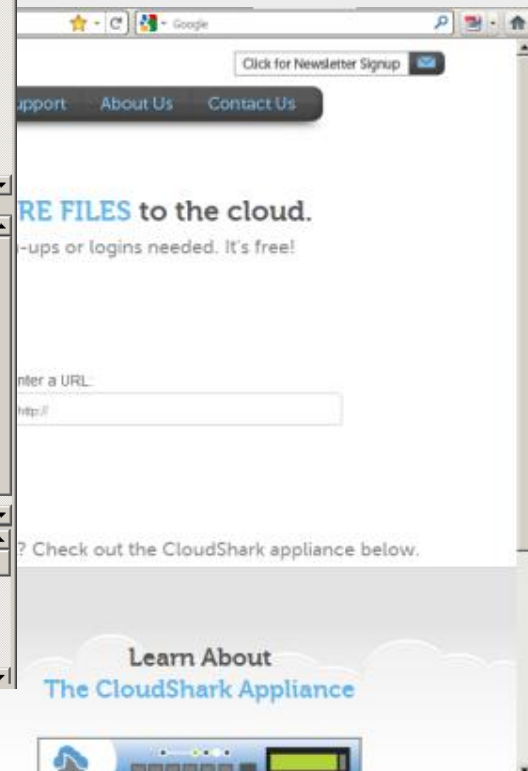
0030 00 2e f6 73 00 00 01 01 08 0a 00 17 95 67 8d 9d ...s.....g..

0040 9d fa 47 45 54 20 2f 73 65 72 76 69 63 65 2f 67 ..GET /service/g

0050 72 65 6d 6c 69 6e 2f 6a 73 2f 66 69 6c 65 73 2f remlin/js/files/

0060 66 61 63 65 62 6f 6f 6b 6c 69 6b 65 2c 73 6c 69 facebooklike,li

0070 64 65 73 68 6f 77 2c 69 74 65 6d 53 6c 69 64 65 deshow,itemSlide



Click for Newsletter Signup

Support About Us Contact Us

RE FILES to the cloud.

-ups or logins needed. It's free!

Enter a URL:

http://

? Check out the CloudShark appliance below.

Learn About The CloudShark Appliance

# Servis olarak Saldırı (Hacking as a Service)



- Bulut bilişim siber suçlular için de cazip bir alan haline gelmiştir.
- Bulut servisleri kullanan bir çok şirket saldırganların hedefi haline gelmiştir.
- Suçlular çeşitli saldırıları yönetmek ve gerçekleştirmek için bulut bilişim servislerini kullanmaktadırlar
  - DDoS
  - Şifre kırma
  - Spam gönderme
  - Botnet kontrolü
  - Zararlı kodların (malware) dağıtılması
  - Lisanslı yazılımların ve filmlerin izinsiz dağıtımı

bahtiyar@ip-10-105-100-122

```

_ | _ | _ )
_ | ( /
_ | \ | _ |

```

Amazon Linux AMI  
Beta

See /usr/share/doc/system-release-2011.02 for latest release notes. :-)

[ec2-user@ip-10-105-100-122 ~]\$ sudo su -

[root@ip-10-105-100-122 ~]# nmap -V

Nmap version 5.21 ( <http://nmap.org> )

[root@ip-10-105-100-122 ~]# nmap localhost

Starting Nmap 5.21 ( <http://nmap.org> ) at 2011-06-06 12:06 UTC

Nmap scan report for localhost (127.0.0.1)

Host is up (0.0000070s latency).

Not shown: 998 closed ports

| PORT | STATE | SERVICE |
|------|-------|---------|
|------|-------|---------|

|        |      |     |
|--------|------|-----|
| 22/tcp | open | ssh |
|--------|------|-----|

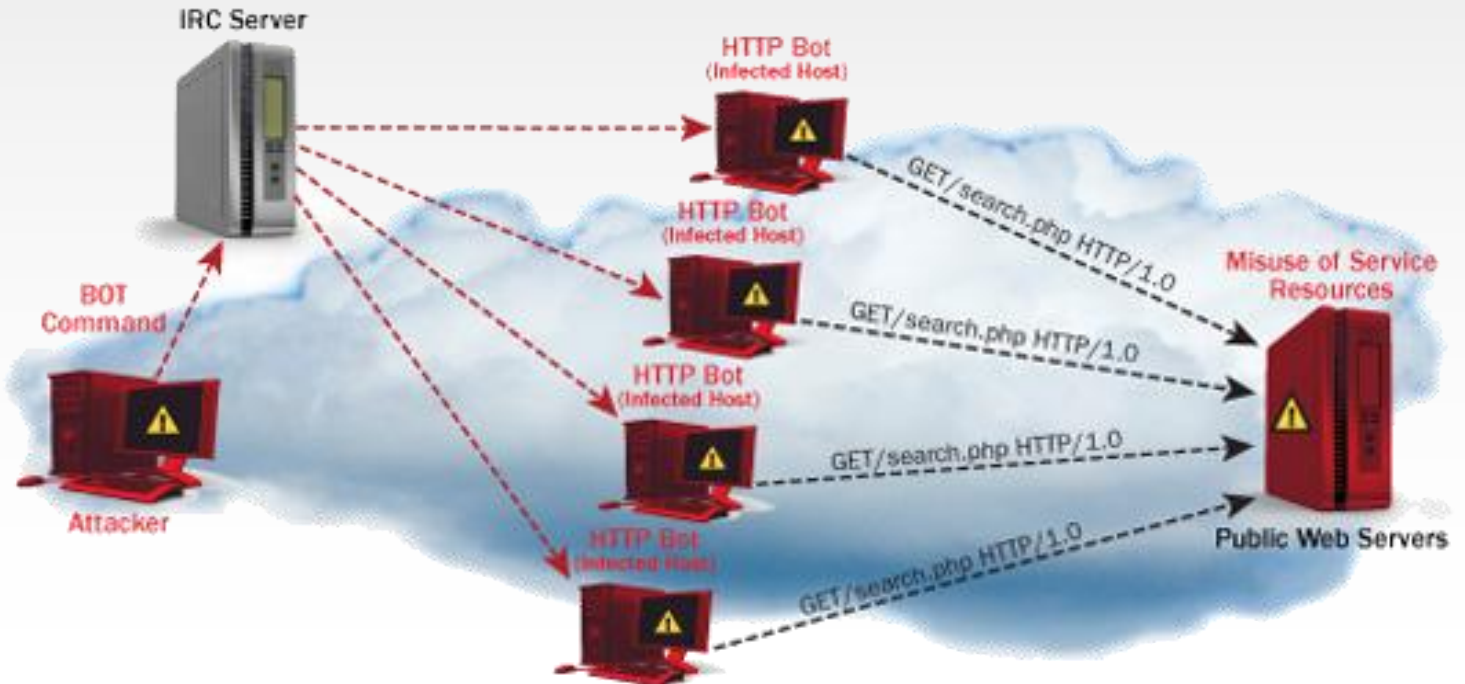
|        |      |      |
|--------|------|------|
| 25/tcp | open | smtp |
|--------|------|------|

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds



# Servis olarak DDoS (DDoS as a Service)

- Bulut bilişimde bulunun güçlü kaynaklar dağıtık servis dışı saldırıları için oldukça uygun bir zemin hazırlayabilmektedir.
  - Yüksek Bant Genişliği
  - Dağıtık Mimari



# Servis olarak Zararlı Kod (Exploit as a Service)

- Bulut bilişim servisleri zararlı kodların kullanımında da etkin olarak kullanılmaktadır.
  - Zararlı kod üretilmesi
  - Zararlı kod dağıtımı



The screenshot shows the ROBO FAT control panel. On the left, there are several menu items: STATS, LINK TRAPP, SELLERS, FILE, SETTINGS, and CLEAR. Below these is a 3D rendering of a robot. The main area contains a dropdown menu set to 'All' and a 'Statistic' table.

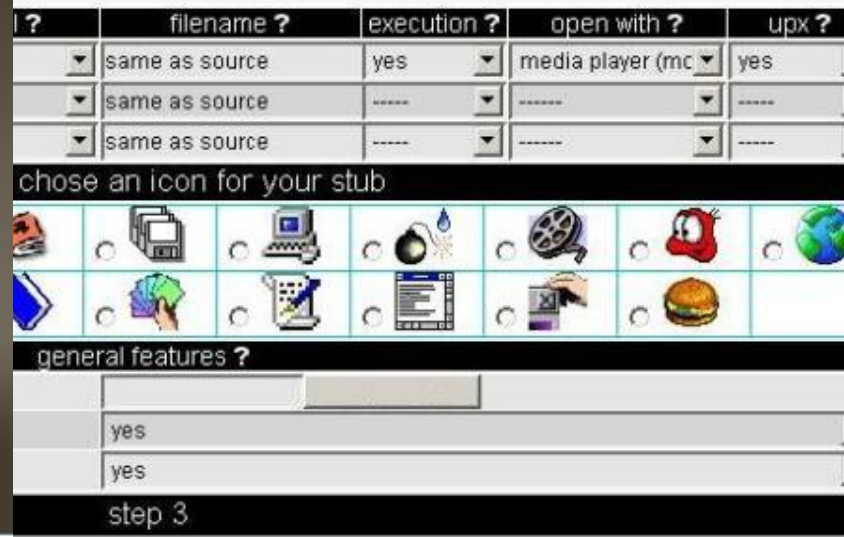
| Statistic | Traff | Loads | Efficiency |
|-----------|-------|-------|------------|
|           | 57    | 7     | 12.28%     |

Below the statistic table is a 'Browsers' table:

| Browser | Traff | Loads | Efficiency |
|---------|-------|-------|------------|
| Safari  | 20    | 1     | 5%         |
| Chrome  | 9     | 1     | 11.11%     |
| Firefox | 9     | 2     | 22.22%     |
| MSIE 6  | 2     | 1     | 50%        |
| MSIE 7  | 3     | 0     | 0%         |
| MSIE 8  | 14    | 2     | 14.29%     |

At the bottom, there is a 'TOP5 countries' table:

| Country | Traff | Loads | Efficiency |
|---------|-------|-------|------------|
|         | 33    | 1     | 3.03%      |
|         | 5     | 1     | 20%        |
|         | 3     | 0     | 0%         |
|         | 3     | 0     | 0%         |
|         | 2     | 1     | 50%        |



The screenshot shows a file manager interface with a table of file entries and a selection area for icons.

| ?                        | filename ?     | execution ? | open with ?      | upx ? |
|--------------------------|----------------|-------------|------------------|-------|
| <input type="checkbox"/> | same as source | yes         | media player (mc | yes   |
| <input type="checkbox"/> | same as source | ----        | -----            | ----  |
| <input type="checkbox"/> | same as source | ----        | -----            | ----  |

Below the table is a section titled 'choose an icon for your stub' with a grid of various icons.

At the bottom, there is a 'general features ?' section with a dropdown menu set to 'yes' and another dropdown menu set to 'yes'.

The bottom of the screenshot shows 'step 3'.

# Servis olarak Botnet (Botnet as a Service)

- Botnet yönetimi
- Botnet üyesi sunucular



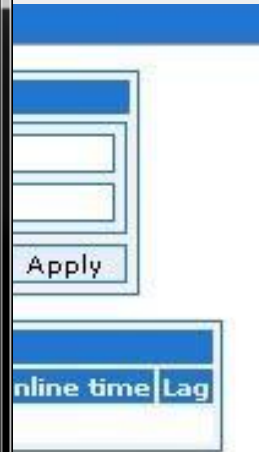
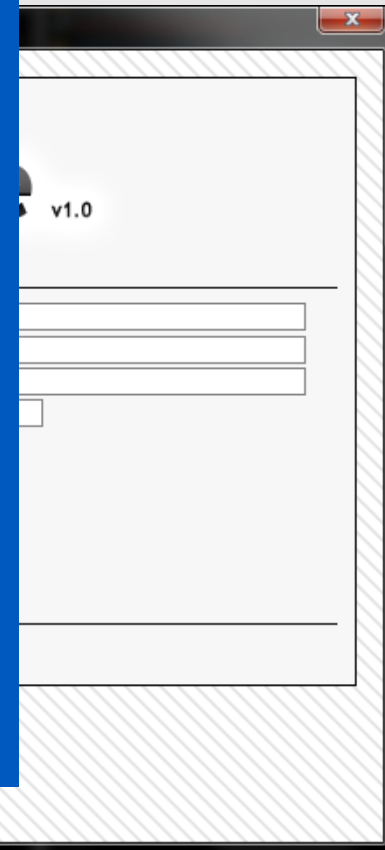
|                           |                                  |                                |                                    |
|---------------------------|----------------------------------|--------------------------------|------------------------------------|
| Время сервера:            | 29.04.2009 21:09:16              | exe=http://host.com/exe.exe    | Команда на загрузку и запуск файла |
| Всего ботов:              | 743                              | dd1=http://host.com/script.php | Команда к началу http атаки хоста  |
| Онлайн ботов:             | 743                              | dd2=http://host.com/           | Команда к началу icmp атаки хоста  |
| Свободных ботов:          | 742                              | upd=http://host.com/loader.exe | Обновление, своего же лоадера      |
| Последняя команда:        | dd1=http://test.com/index.php... | vote=http://host.com/vote.php  | Голосование в опросах на сайтах    |
| Выполняют:                | 1                                | wtf                            | Остановка выполнения всех команд   |
| Трафик:                   | 0 MB                             |                                |                                    |
| Версия панели управления: | 2.1.0 Optima                     |                                |                                    |
| Версия бота:              | 1.12                             |                                |                                    |

[Главная](#)
[Расписание](#)
[Неактивные](#)
[Все активные](#)
[Выйти](#)

Изменение общей команды




| Последний адрес + | Регистрация +       | Номер + | Версия + | Синхронизация + | Команда + | Трафик + | Команда + |
|-------------------|---------------------|---------|----------|-----------------|-----------|----------|-----------|
| 118.67.229.2      | 2009-03-28 00:30:00 | 531340  | 1.12b    | 32 дней назад   | wtf       | 0 MB     | Команда   |
| 82.73.92.89       | 2009-03-28 00:30:00 | 488396  | 1.12b    | 30 дней назад   | wtf       | 0 MB     | Команда   |
| 86.21.47.251      | 2009-03-28 00:30:00 | 671252  | 1.12b    | 30 дней назад   | wtf       | 0 MB     | Команда   |
| 62.117.46.65      | 2009-03-28 00:30:00 | 547537  | 1.12b    | 31 дней назад   | wtf       | 0 MB     | Команда   |
| 124.123.7.106     | 2009-03-28 00:30:00 | 181564  | 1.12b    | 30 дней назад   | wtf       | 0 MB     | Команда   |
| 189.75.10.86      | 2009-03-28 00:30:00 | 553356  | 1.12b    | 32 дней назад   | wtf       | 0 MB     | Команда   |
| 190.176.44.229    | 2009-03-28 00:30:00 | 198484  | 1.12b    | 30 дней назад   | wtf       | 0 MB     | Команда   |
| 190.13.11.98      | 2009-03-28 00:30:00 | 756183  | 1.12b    | 32 дней назад   | wtf       | 0 MB     | Команда   |
| 117.192.167.60    | 2009-03-28 00:30:00 | 116012  | 1.12b    | 32 дней назад   | wtf       | 0 MB     | Команда   |
| 88.70.6.4         | 2009-03-28 00:30:00 | 745086  | 1.12b    | 30 дней назад   | wtf       | 0 MB     | Команда   |
| 82.91.8.157       | 2009-03-28 00:30:00 | 369975  | 1.12b    | 30 дней назад   | wtf       | 0 MB     | Команда   |
| 87.217.129.96     | 2009-03-28 00:30:00 | 290000  | 1.12b    | 30 дней назад   | wtf       | 0 MB     | Команда   |
| 94.99.68.14       | 2009-03-28 00:30:00 | 111955  | 1.12b    | 31 дней назад   | wtf       | 0 MB     | Команда   |
| 186.12.127.206    | 2009-03-28 00:30:00 | 458950  | 1.12b    | 32 дней назад   | wtf       | 0 MB     | Команда   |
| 201.28.66.155     | 2009-03-28 00:30:00 | 569245  | 1.12b    | 31 дней назад   | wtf       | 0 MB     | Команда   |
| 189.156.16.188    | 2009-03-28 00:30:00 | 830464  | 1.12b    | 30 дней назад   | wtf       | 0 MB     | Команда   |
| 94.142.38.159     | 2009-03-28 00:30:00 | 331817  | 1.12b    | 32 дней назад   | wtf       | 0 MB     | Команда   |
| 59.94.129.211     | 2009-03-28 00:30:00 | 608682  | 1.12b    | 31 дней назад   | wtf       | 0 MB     | Команда   |
| 189.26.193.8      | 2009-03-28 00:30:00 | 886468  | 1.12b    | 32 дней назад   | wtf       | 0 MB     | Команда   |
| 94.211.69.181     | 2009-03-28 00:30:00 | 014911  | 1.12b    | 32 дней назад   | wtf       | 0 MB     | Команда   |



Logout

- Bulut bilişimin güçlü işlem gücü saldırganlar tarafından dağıtık olarak şifre kırma işlemleri için kullanılmaktadır.
- Bu altyapı sayesinde bir çok şifre kırma servisi geliştirilmiştir.
- Şifre kırma servisleri
  - Kablosuz ağ şifrelerinin kırılması WPA kırma
  - İşletim sistemi şifrelerinin kırılması (SHA1)
  - Ağ cihazlarının şifrelerinin kırılması (MD5)

Kablosuz ağların şifrelemesinde kullanılan WPA/WPA2 protokollerine ait şifreler bulut bilişim kaynakları kullanılarak kırılabilmektedir.



WPA  
CRACKER

about run faq

Step 1, upload your network capture.

First select the pcap file that contains the WPA-PSK handshake you'd like to crack. We only accept pcap files which are less than 10MB in size, so you might need to use Wireshark to pull out just the handshake (and a beacon for your ssid) if your capture is larger than that. Be patient when you click next, your pcap is uploading.

- pcap file:  Browse...
- ssid of target network:

**NEXT** →

A Thoughtcrime Labs Production  
In Association With The Institute For Disruptive Studies

- Senaryo: 1-6 karakter uzunluğunda şifrelerin kırılması
- Algoritma: SHA1
- Yöntem: Kaba kuvvet saldırısı (brute-force)
- Maliyet : 2100\$
- Kırma süresi : 49 Dakika
- Kullanılan donanım
  - 22 GB of memory
  - 33.5 EC2 Compute Units (2 x Intel Xeon X5570, quad-core “Nehalem” architecture)
  - 2 x NVIDIA Tesla “Fermi” M2050 GPUs
  - 1690 GB of instance storage
  - 64-bit platform
  - I/O Performance: Very High (10 Gigabit Ethernet)
  - API name: cg1.4xlarge

- Bir çok kriptografik işlemde kullanılan MD5 özetleri ve şifreler de bulut tabanlı servisler ile kırılabilmektedir.

## ONLINE MD5 CRACKER

Welcome to HashHack, The online md5 cracker that sets a new precedent in online MD5 hash cracking.

HashHack's online md5 cracker uses a large database of precomputed hashes to crack your hashes quickly and efficiently, our online hash database currently stores 21,152,093 unique precomputed md5 hashes for your cracking pleasure.

MD5 Hash:  3+2=

Statistics : : Total: 24896 - Cracked: 4029 - Not Cracked: 20867 - Success(%): 16.183322622108 %

### The Last 10 Md5 Hashes Cracked Online:

| ID    | HASH                             | PASSWORD | METHOD   |
|-------|----------------------------------|----------|----------|
| 26468 | e10adc3949ba59abbe56e057f20f883e | 123456   | DATABASE |
| 26462 | 098f6bcd4621d373cade4e832627b4f6 | test     | DATABASE |
| 26449 | 9818e2287e76d37753313e255e2428a2 | melody   | DATABASE |

# md5crack

## Recently Cracked md5 Hashs

Original:

5158951716b440c3d165e0 meta

5158951716b440c3d165e0 meta

e9a23cbc455158951716b440c3d165e0 meta

e9a23cbc455158951716b440c3d165e0 meta

e9a23cbc455158951716b440c3d165e0 meta

- Bulut tabanlı şifre kırma yazılımları
  - CloudCrack
  - MOSCRACK

```
File Edit View Search Terminal Tabs Help
rbabchis@haze: /haze
[26517] Got node 192.168.1.70
[26517] Got chunk moscrackdict.343
[26517] Copying files to node 192.168.1.70
[26517] Estimated completion time: 366 seconds
Generated 11x chunk for node slappy; moscrackdict.354
Spawned pid 26519. Now 15 active processes
[26519] Got node slappy
[26519] Got chunk moscrackdict.354
[26519] Estimated completion time: 370 seconds
[26509] Copying files to node ec2-50-16-156-83.compute-1.amazonaws.com
Generated 1x chunk for node iphone; moscrackdict.365
Spawned pid 26523. Now 16 active processes
[26523] Estimated completion time: 360 seconds
[26523] Got node iphone
[26523] Got chunk moscrackdict.365
[26508] Copying files to node ec2-50-16-69-153.compute-1.amazonaws.com
[26502] Launching aircrack-ng on node ec2-50-16-67-66.compute-1.amazonaws.com
[26514] Launching aircrack-ng on node ec2-75-101-255-31.compute-1.amazonaws.com
[26487] Launching aircrack-ng on node ec2-50-17-107-112.compute-1.amazonaws.com
[26483] Launching aircrack-ng on node ec2-184-73-30-7.compute-1.amazonaws.com
[26484] Launching aircrack-ng on node ec2-184-73-123-98.compute-1.amazonaws.com
[26508] Launching aircrack-ng on node ec2-50-16-69-153.compute-1.amazonaws.com
```

## NVIDIA GPU-Accelerated Suite!

...ous posts such as - [MOSCRACK](#) and [WPA](#) [open source](#) offering that is NOT a cracker, but written in CUDA - a parallel computing architecture.



...cryptanalysis suite for cloud computing on Amazon EC2 Cluster Compute cloud. It is a NVIDIA GPU-Accelerated Suite written in CUDA, NVIDIA's massively parallel programming language. CloudCrack contains custom CUDA code for storing a large target RSA modulus  $n$  in shared GPU memory, with each GPU core working as a parallel factoring process to break the target modulus.

# Servis olarak Spam (Spam as a Service)



## EMAIL RESPONSES Scenario (1): New Laptop



| Email                       | Group          | Time Viewed                    |
|-----------------------------|----------------|--------------------------------|
| bob.smith@yourcompany.com   | Marketing Dept | Sun Sep 09 21:09:10 -0400 2007 |
| jane.doe@yourcompany.com    | Front Office   | Sun Sep 09 21:11:01 -0400 2007 |
| kevin.smith@yourcompany.com | Front Office   | Sun Sep 09 21:13:03 -0400 2007 |
| jack.loe@yourcompany.com    | Front Office   | Sun Sep 09 21:14:23 -0400 2007 |
| jason.smith@yourcompany.com | Front Office   | Sun Sep 09 21:14:44 -0400 2007 |
| jack.smith@yourcompany.com  | Marketing Dept | Sun Sep 09 21:15:10 -0400 2007 |
| mike.doe@yourcompany.com    | Front Office   | Sun Sep 09 21:16:01 -0400 2007 |
| ron.smith@yourcompany.com   | Front Office   | Sun Sep 09 21:16:03 -0400 2007 |
| aaron.loe@yourcompany.com   | Front Office   | Sun Sep 09 21:16:23 -0400 2007 |
| jaime.smith@yourcompany.com | Front Office   | Sun Sep 09 21:17:44 -0400 2007 |
| sam.smith@yourcompany.com   | Marketing Dept | Sun Sep 09 21:18:13 -0400 2007 |
| bob.doe@yourcompany.com     | Marketing Dept | Sun Sep 09 21:19:21 -0400 2007 |
| hiana.smith@yourcompany.com | Marketing Dept | Sun Sep 09 21:19:42 -0400 2007 |

| Mail to            | Summary   |
|--------------------|---|
| byahoo.co.uk       | Given up SMTP (firewalled or blacklisted)             |
| ioe@ukonline.co.uk | Given up SMTP (firewalled or blacklisted)             |
| lukonline.co.uk    | Given up SMTP (firewalled or blacklisted)             |
| ioe@yahoo.co.uk    | Given up SMTP (firewalled or blacklisted)             |
| lyahoo.co.uk       | Given up SMTP (firewalled or blacklisted)             |
| @ukonline.co.uk    | Given up SMTP (firewalled or blacklisted)             |
| ukonline.co.uk     | Connection failed: 8180815; firewalled or blacklisted |
| @yahoo.co.uk       | Given up SMTP (firewalled or blacklisted)             |
| yahoo.co.uk        | Given up SMTP (firewalled or blacklisted)             |
| ng@ukonline.co.uk  | Given up SMTP (firewalled or blacklisted)             |
| it@ukonline.co.uk  | Given up SMTP (firewalled or blacklisted)             |
| ng@yahoo.co.uk     | Given up SMTP (firewalled or blacklisted)             |
| it@yahoo.co.uk     | Given up SMTP (firewalled or blacklisted)             |
| s@vmail.com        | Given up SMTP (firewalled or blacklisted)             |
| jp@ukonline.co.uk  | Connection failed: 8180815; firewalled or blacklisted |
| lukonline.co.uk    | Given up SMTP (firewalled or blacklisted)             |
| jp@yahoo.co.uk     | Given up SMTP (firewalled or blacklisted)             |
| lyahoo.co.uk       | Given up SMTP (firewalled or blacklisted)             |
| @yahoo.com         | Given up SMTP (firewalled or blacklisted)             |
| ir@yahoo.com       | Given up SMTP (firewalled or blacklisted)             |
| uff@vmail.com      | Given up SMTP (firewalled or blacklisted)             |
| ub@ukonline.co.uk  | Given up SMTP (firewalled or blacklisted)             |
| mann78@vmail.com   | Given up SMTP (firewalled or blacklisted)             |
| @yahoo.co.uk       | Given up SMTP (firewalled or blacklisted)             |
| ukonline.co.uk     | Given up SMTP (firewalled or blacklisted)             |
| ukonline.co.uk     | Given up SMTP (firewalled or blacklisted)             |
| ukonline.co.uk     | Given up SMTP (firewalled or blacklisted)             |
| s@yahoo.co.uk      | Given up SMTP (firewalled or blacklisted)             |
| lyahoo.co.uk       | Given up SMTP (firewalled or blacklisted)             |
| lukonline.co.uk    | Given up SMTP (firewalled or blacklisted)             |
| her@ukonline.co.uk | Given up SMTP (firewalled or blacklisted)             |
| ur@freeuk.com      | Given up SMTP (firewalled or blacklisted)             |
| lyahoo.com         | Given up SMTP (firewalled or blacklisted)             |
| nan@ukonline.co.uk | Given up SMTP (firewalled or blacklisted)             |
| yahoo.co.uk        | Connection failed: 8180815; firewalled or blacklisted |
| yahoo.co.uk        | Given up SMTP (firewalled or blacklisted)             |
| all@yahoo.com      | Given up SMTP (firewalled or blacklisted)             |
| nan@yahoo.co.uk    | Given up SMTP (firewalled or blacklisted)             |
| lukonline.co.uk    | Given up SMTP (firewalled or blacklisted)             |
| ler1@yahoo.com     | Given up SMTP (firewalled or blacklisted)             |
| i@ukonline.co.uk   | Given up SMTP (firewalled or blacklisted)             |
| @ukonline.co.uk    | Connection failed: 8180815; firewalled or blacklisted |
| i@yahoo.co.uk      | Given up SMTP (firewalled or blacklisted)             |
| yahoo.co.uk        | Given up SMTP (firewalled or blacklisted)             |
| cu@ukonline.co.uk  | Given up SMTP (firewalled or blacklisted)             |
| er@yahoo.co.uk     | Given up SMTP (firewalled or blacklisted)             |
| xeve24@yahoo.com   | Connection failed: 8180815; firewalled or blacklisted |
| j@yahoo.co.uk      | Given up SMTP (firewalled or blacklisted)             |
| s@yahoo.co.uk      | Given up SMTP (firewalled or blacklisted)             |
| lyahoo.co.uk       | Given up SMTP (firewalled or blacklisted)             |
| he@yahoo.com       | Given up SMTP (firewalled or blacklisted)             |
| id@yahoo.com       | Given up SMTP (firewalled or blacklisted)             |
| lyahoo.com         | Given up SMTP (firewalled or blacklisted)             |
| @ukonline.co.uk    | Connection failed: 8180815; firewalled or blacklisted |
| cu@yahoo.co.uk     | Connection failed: 8180815; firewalled or blacklisted |
| er@yahoo.com       | Connection failed: 8180815; firewalled or blacklisted |
| rcu@ukonline.co.uk |   |
| jer@yahoo.co.uk    |   |
| iteve24@yahoo.com  |   |
| lj@yahoo.co.uk     |   |
| se@yahoo.co.uk     |   |
| @yahoo.co.uk       |   |
| be@yahoo.com       |   |
| 00@yahoo.com       |   |
| lyahoo.com         |   |
| @ukonline.co.uk    |   |
| rcu@yahoo.co.uk    |   |
| ter@yahoo.com      |   |

# Servis olarak Korsan Yazılım (Warez as a Service)

- Korsan yazılım, film ve müzik albümü dağıtımları da bulut bilişim kaynakları sayesinde daha yaygın hale gelmiştir.
  - Geniş disk kapasitesi
  - Yüksek bant genişliği
  - Dünyanın farklı bölgelerine dağılmış veri merkezleri



The Pirate Bay



- Bulut bilişim servislerinin kullanımı giderek artan bir trend göstermektedir.
- Bulut bilişim de diğer teknolojiler gibi iyi veya kötü amaçlar için kullanılabilir.
- Bulut bilişime geçmek isteyen kurumlar mevcut riskleri göz önünde bulundurarak geçiş stratejilerini oluşturmaları gerekmektedir.





# Sorular?

# Teşekkürler

**Bahtiyar BİRCAN**  
bahtiyar@uekae.tubitak.gov.tr