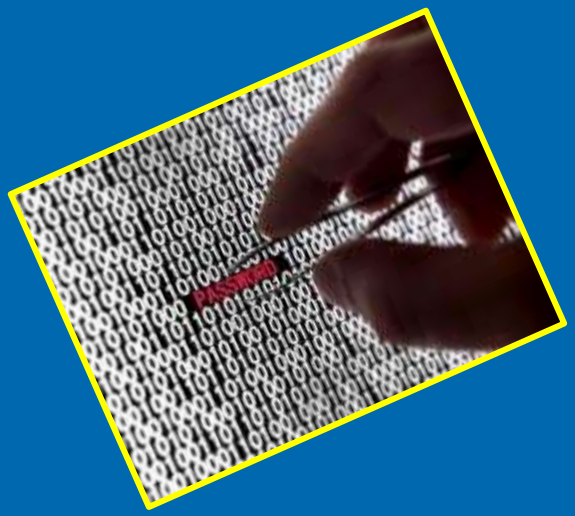


eTURİZM
&
BİLGİ GÜVENLİĞİ

Dr. Güntekin Şimşek
gsimsek@adu.edu.tr

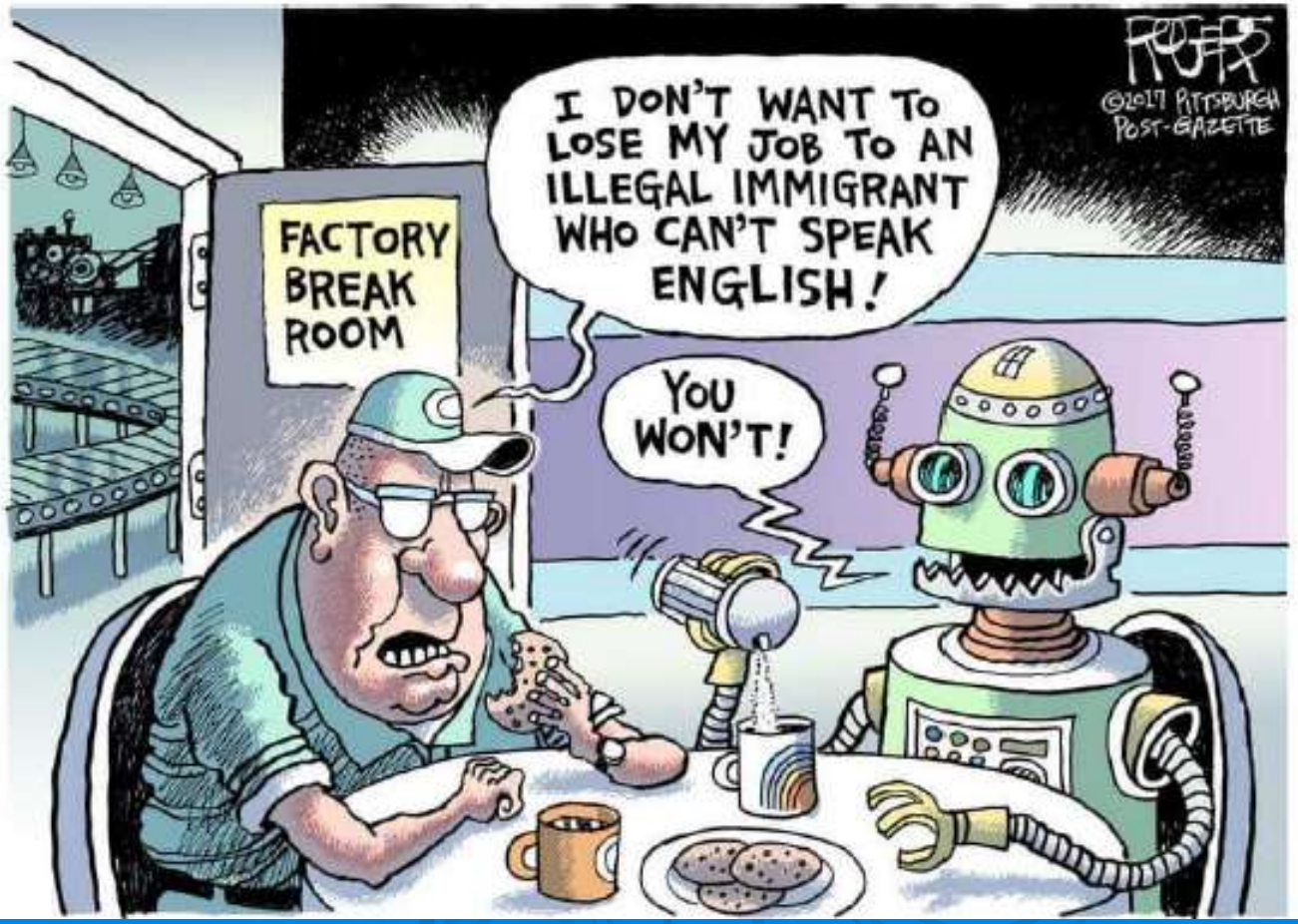

LISTEN!
THE ENEMY MAY BE TALKING
DON'T TALK!
THE ENEMY MAY BE LISTENING

Application of robots, AI and automation technologies:

- *Manufacturing*

Application of robots, AI and automation technologies:

- *Manufacturing*



Application of robots, AI and automation technologies:

- *Warehousing, supply and logistics*

Application of robots, AI and automation technologies:

- *Warehousing, supply and logistics*

Application of robots, AI and automation technologies:

- *Agriculture*

Application of robots, AI and automation technologies:

- *Transportation / Autonomous cars*

Application of robots, AI and automation technologies:

- *Medicine*

Application of robots, AI and automation technologies:

- *Warfare*

Application of robots, AI and automation technologies:

- *Legal services*

Application of robots, AI and automation technologies:

- *Households*

Application of robots, AI and automation technologies:

- *Households*

Application of robots, AI and automation technologies:

- *Swimming pools*
- *Gardens*

Application of robots, AI and automation technologies:

- *Guards*

- *Parcel delivery*

Application of robots, AI and automation technologies:

- *Education*

- *Entertainment*

Application of robots, AI and automation technologies:

- *Information provision in service industries*

Application of robots, AI and automation technologies:

- *Cucumbers cutting robots*

Application of robots, AI and automation technologies:

- *Sex services*

18
+

https://surgefs.imgix.net/quality=v:80/K25JiHV0QUKIXCo9usln?auto=format&ixlib=imgixjs-3.3.2&w=1000

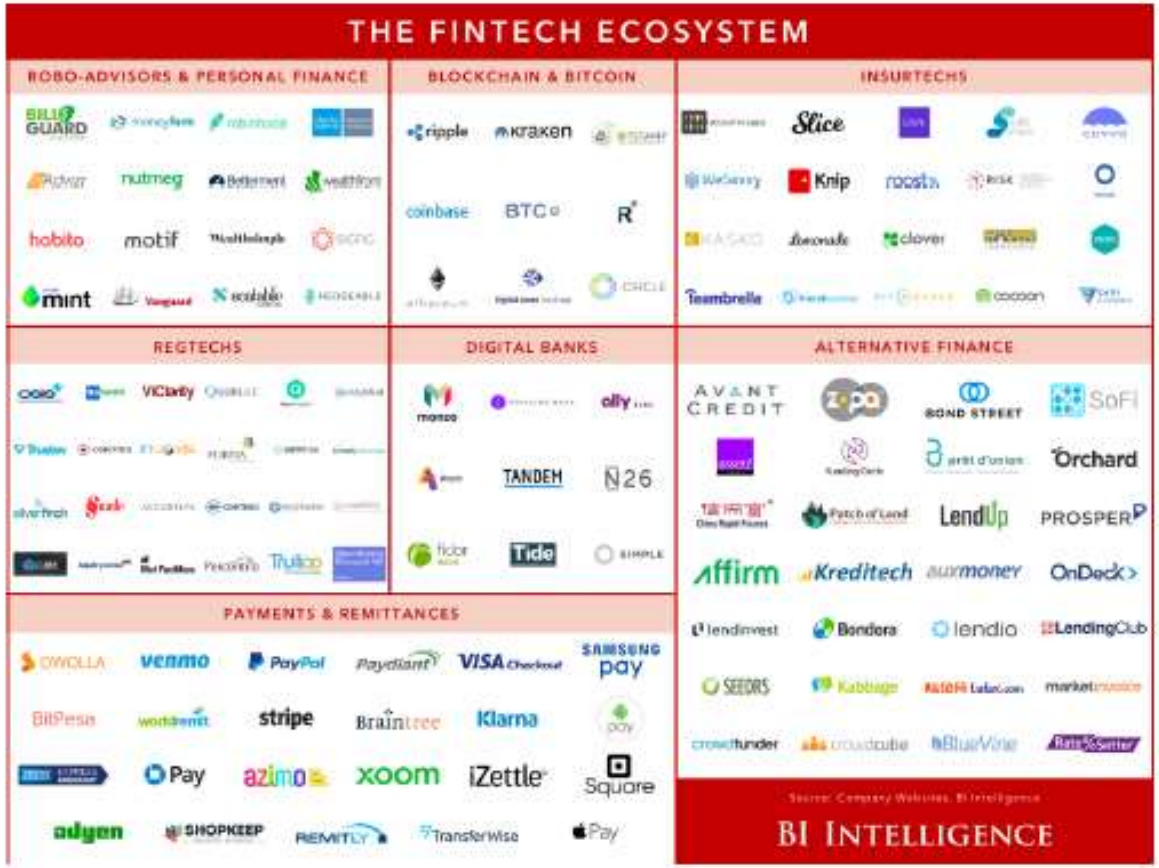
https://www.vanguardngr.com/wp-content/uploads/2018/02/Sex-robot-2.png

Application of robots, AI and automation technologies:

- *Search engines*
- *E-commerce*

Application of robots, AI and automation technologies:

- *Finance*

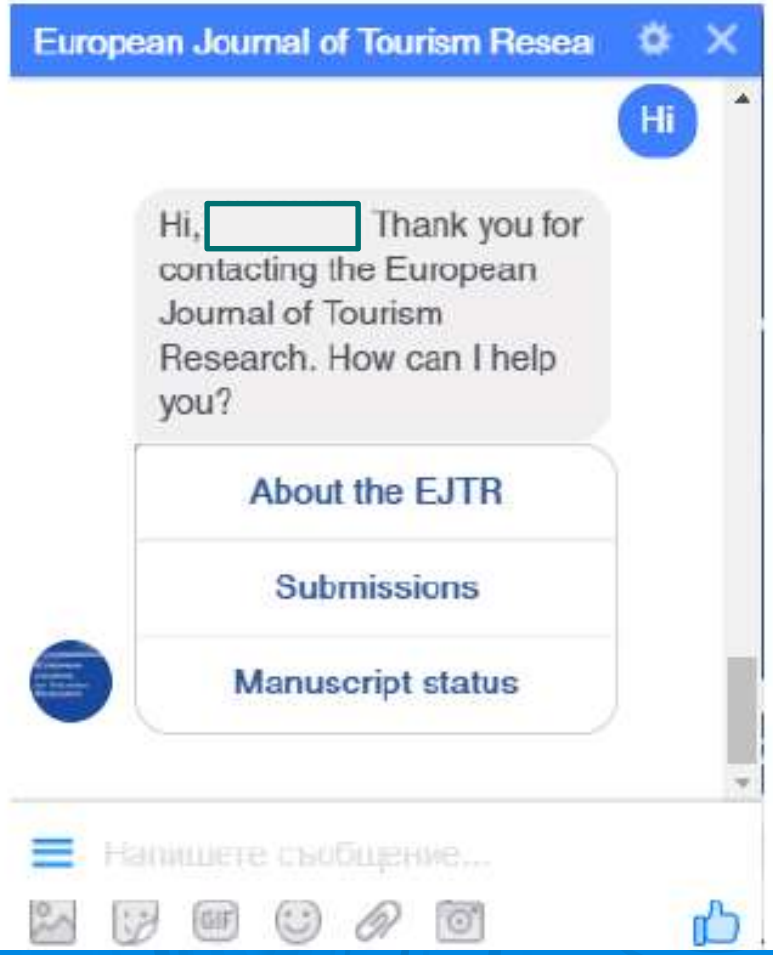


Application of robots, AI and automation technologies:

- *Digital assistants*

Application of robots, AI and automation technologies:

- *Social media chatbots*

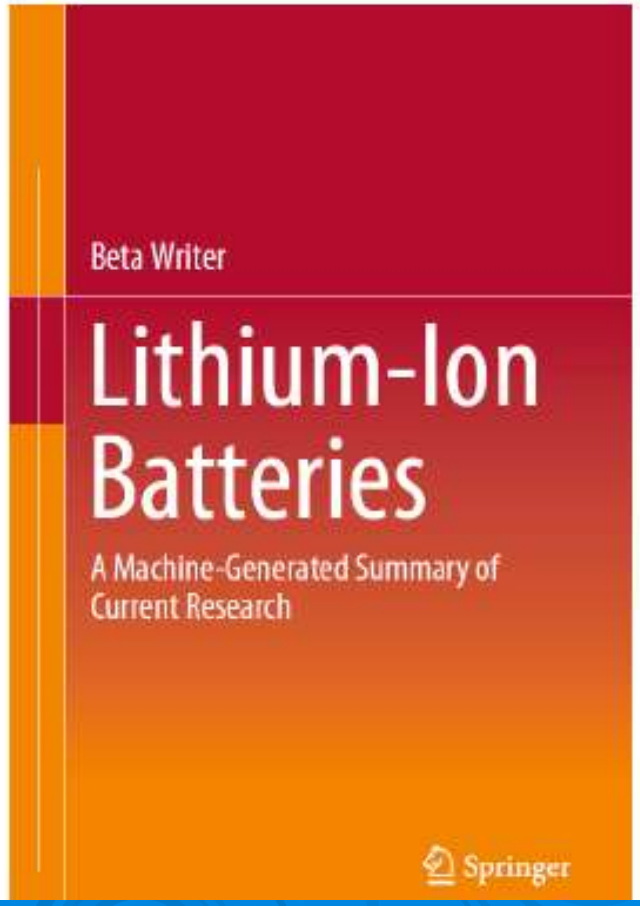


Application of robots, AI and automation technologies:

- *Journalism*

Application of robots, AI and automation technologies:

- *Academic research*



Application of robots, AI and automation technologies:

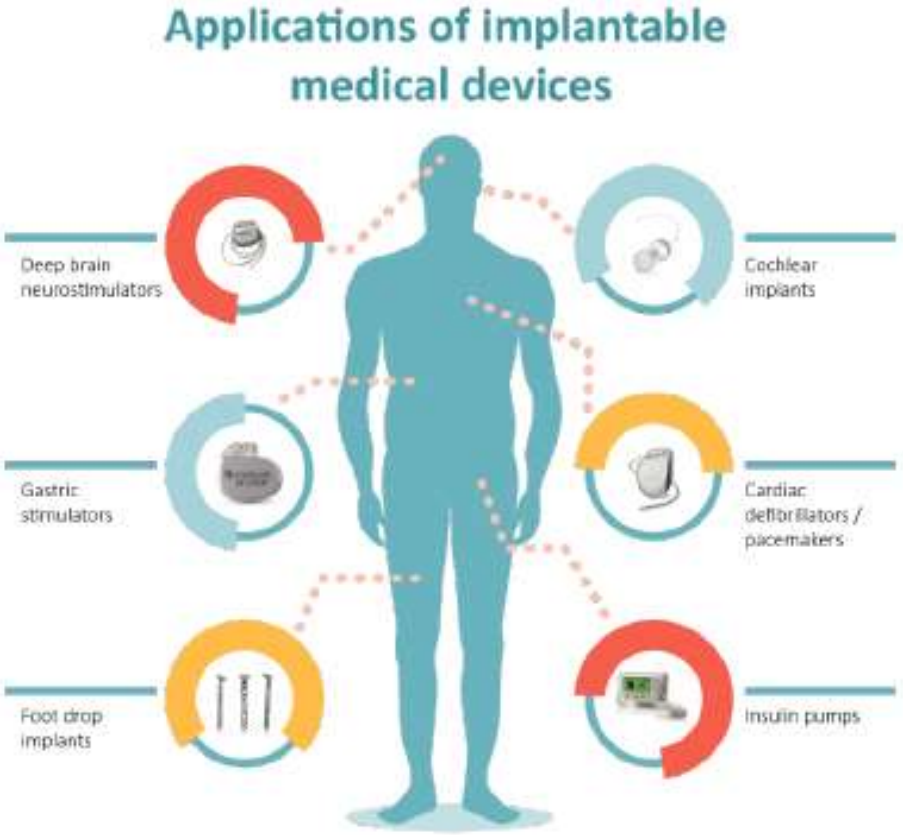
- *Retail*

Application of robots, AI and automation technologies:

- *Wearable technology*

Application of robots, AI and automation technologies:

- *Implantable technology*

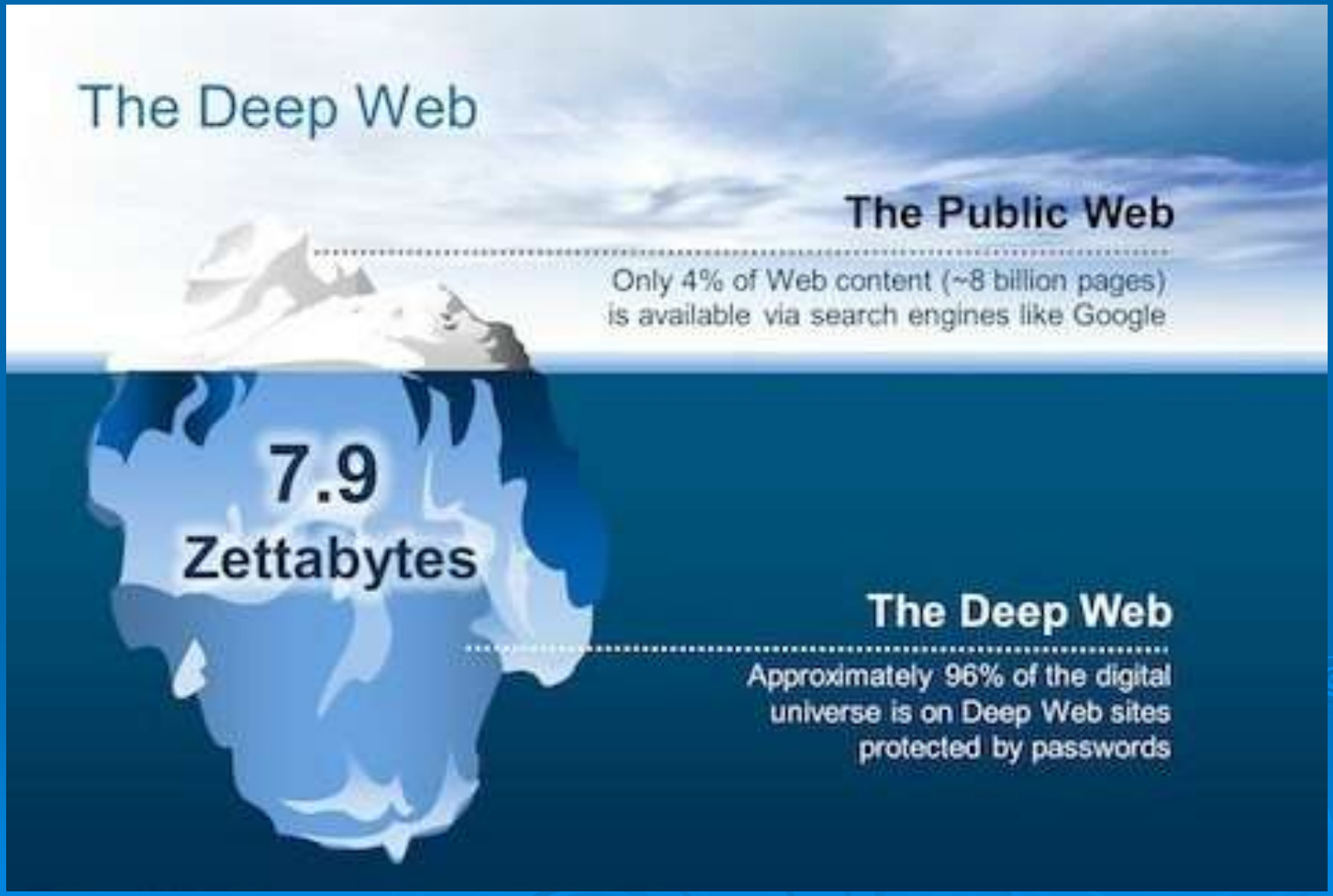


Application of robots, AI and automation technologies:

- *Human microchip implants*


Surface Web
Deep Web
Dark Web

Bir diğer adı Deep Web olan, gizemli, derin internet, sınırsız erişim sağlanabilen, yasal olmayan birçok konuda farklı insanlar tanıyabileceğiniz internet kullanımı Dark Web olarak ifade ediliyor. Son günlerde kulaktan kulağa dolaşmaya başlayan, hem korkutucu hem de ilgi çekici olan bir sistem herkes tarafından merak edilmeye devam ediyor.


The Deep Web
The Public Web
Only 4% of Web content (~8 billion pages) is available via search engines like Google
7.9
Zettabytes
The Deep Web
Approximately 96% of the digital universe is on Deep Web sites protected by passwords

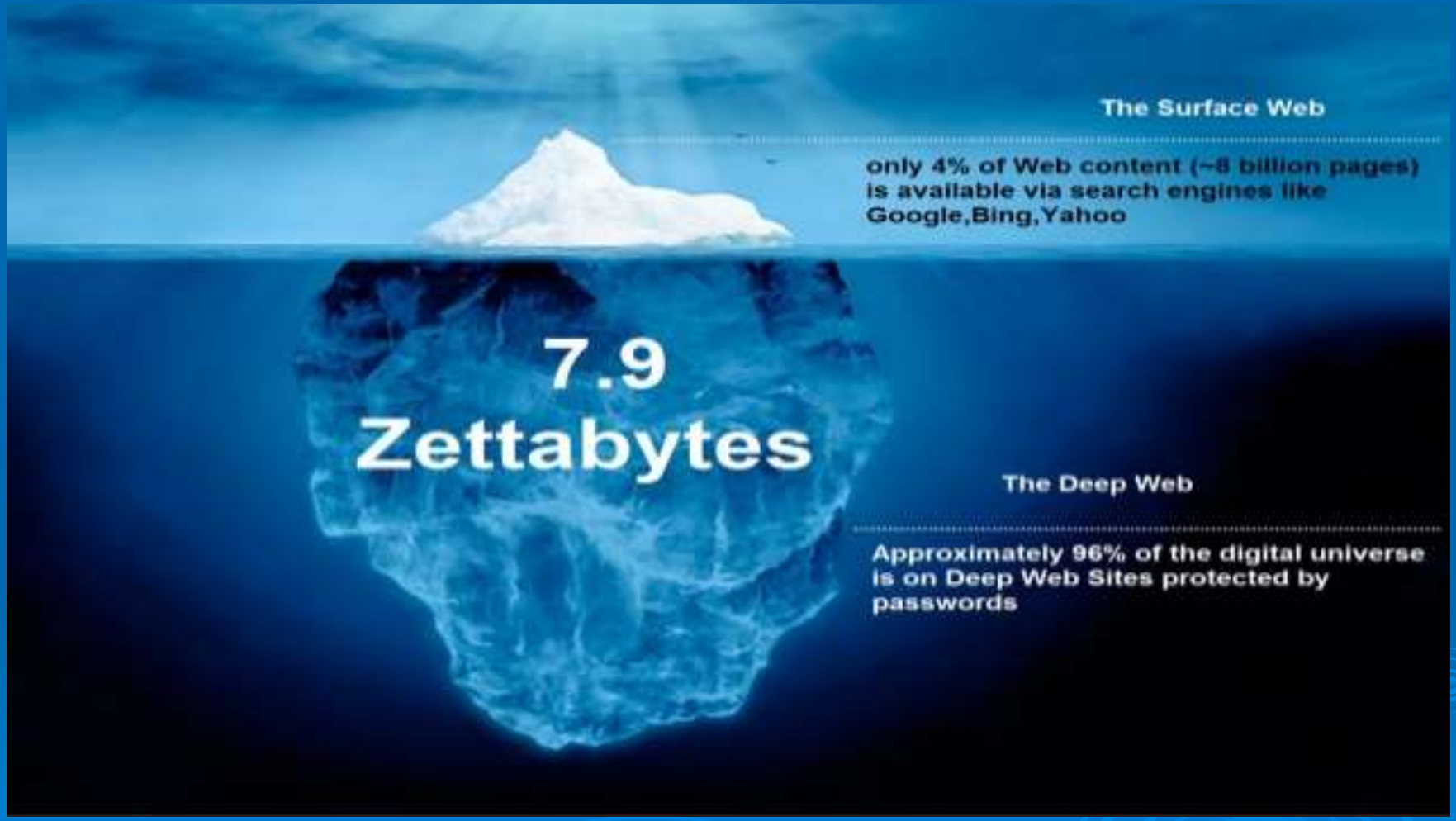

jodacame.com
WordPress
Drupal
Joomla!
Google+
facebook
YouTube
twitter
Nivel 2
MEGA
TARINGA!
Nivel 3
The Pirate Bay
Nivel 4
The Hidden Wiki
Nivel 5
Nivel 6

Surface Web

- The surface Web is that portion of the World Wide Web that is indexable by conventional search engines.
- It is also known as the Clearnet, the visible Web or Indexable Web.
- Eighty-five percent of Web users use search engines to find needed information, but nearly as high a percentage cite the inability to find desired information as one of their biggest frustrations.
- A traditional search engine sees only a small amount of the information that's available -- a measly 0.03 % [source: OEDB].

Deep Web - Introduction

- The Deep Web is World Wide Web content that is not part of the Surface Web, which is indexed by standard search engines.
- It is also called the Deepnet, Invisible Web or Hidden Web.
- Largest growing category of new information on the Internet.
- 400-550X more public information than the Surface Web.
- Total quality 1000-2000X greater than the quality of the Surface Web.

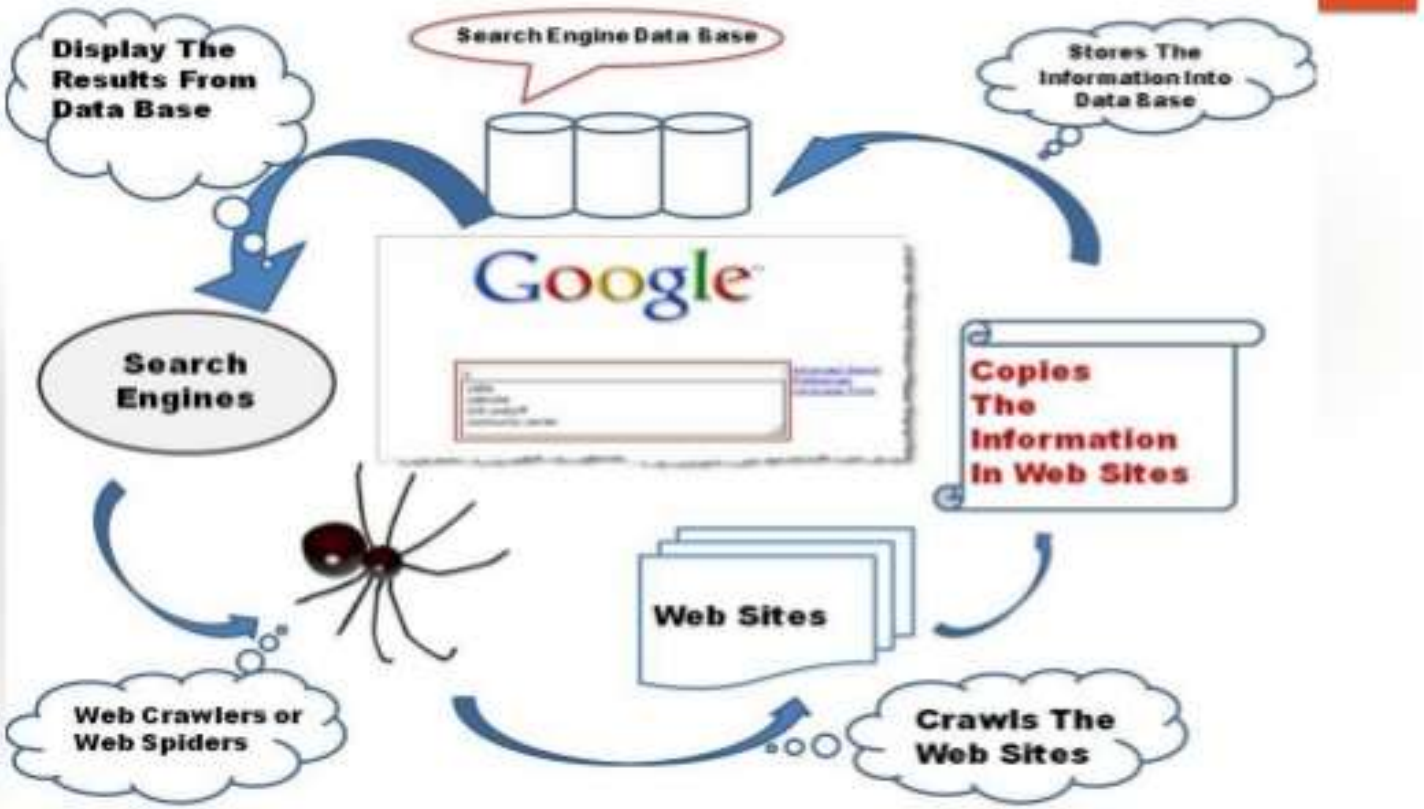

The Surface Web
only 4% of Web content (~8 billion pages) is available via search engines like Google,Bing,Yahoo
7.9
Zettabytes
The Deep Web
Approximately 96% of the digital universe is on Deep Web Sites protected by passwords

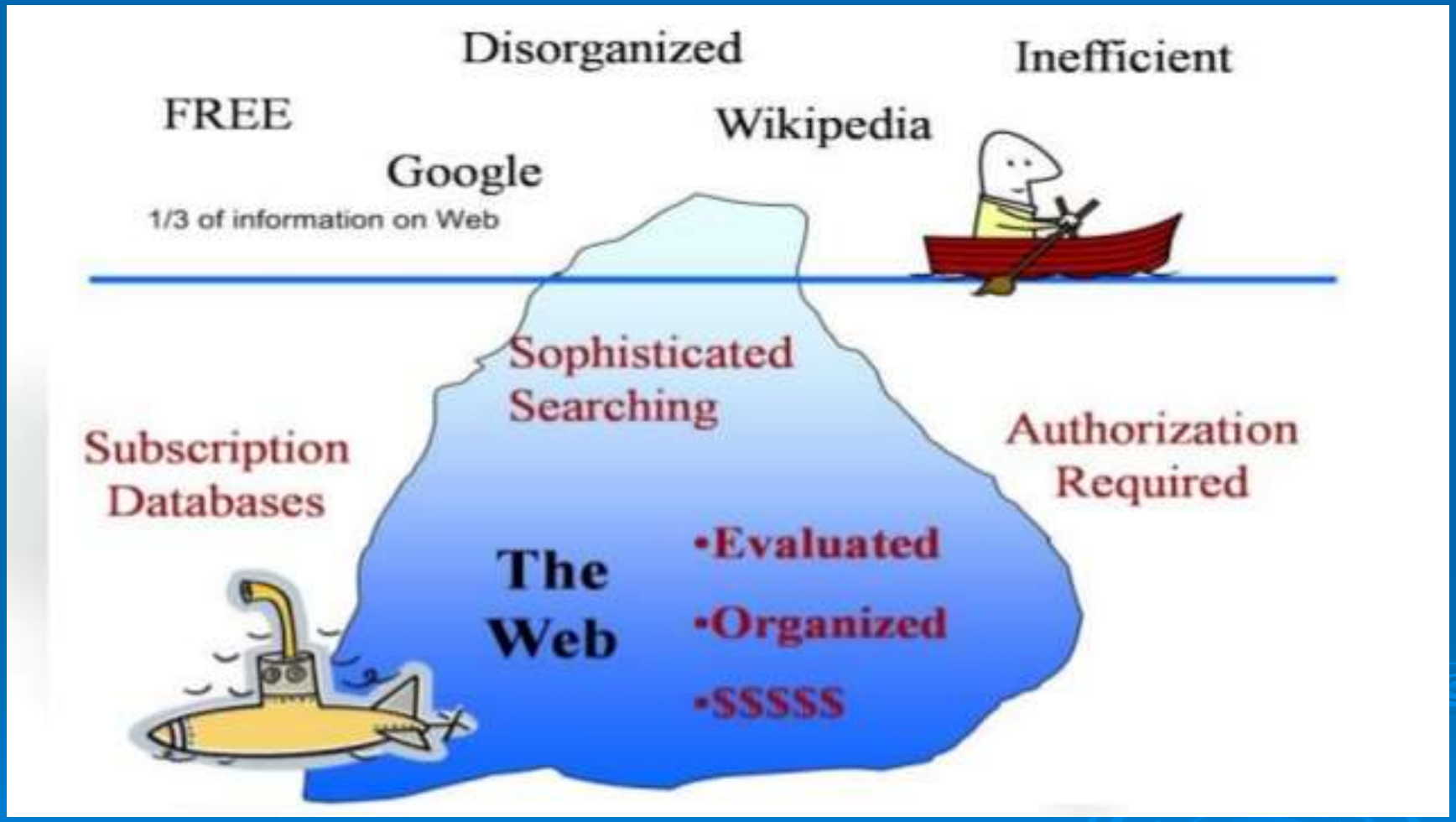
History

- Jill Ellsworth used the term invisible Web in 1994 to refer to websites that were not registered with any search engine.
- Mike Bergman cited a January 1996 article by Frank Garcia:

  "It would be a site that's possibly reasonably designed, but they didn't bother to register it with any of the search engines. So, no one can find them! You're hidden. I call that the invisible Web".
- Another early use of the term Invisible Web was by Bruce Mount and Matthew B. Koll of Personal Library Software in 1996.
- The first use of the specific term Deep Web, now generally accepted, occurred in the aforementioned 2001 Bergman study.

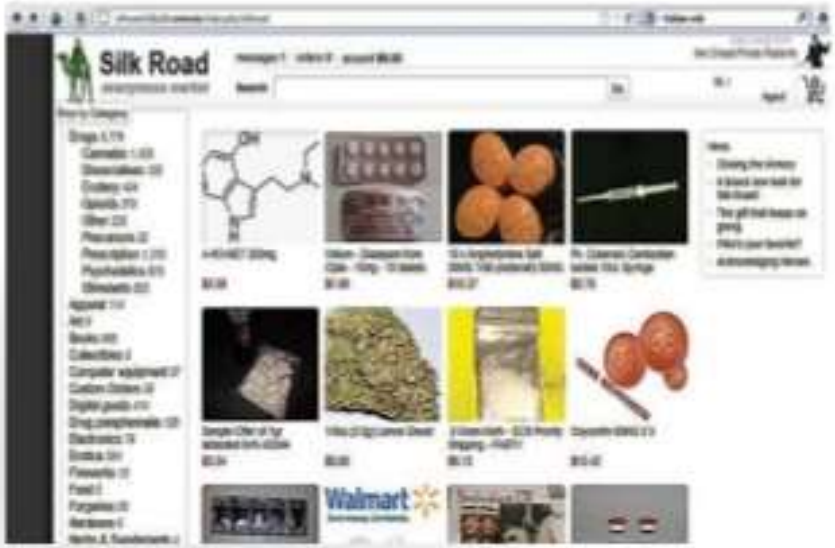
How search engines work




Disorganized
Inefficient
FREE
Wikipedia
Google
1/3 of information on Web
Sophisticated
Searching
Subscription
Databases
Authorization
Required
The
Web
•Evaluated
•Organized
•SSSSS

The Onion Router (TOR)

- Tor is software that installs into your browser and sets up the specific connections you need to access dark Web sites.
- Critically it is free software for enabling online anonymity and censorship resistance.
- Onion routing refers to the process of removing encryption layers from Internet communications, similar to peeling back the layers of an onion.
- Using Tor makes it more difficult to trace Internet activity, including "visits to Web sites, online posts, instant messages, and other communication forms", back to the user.
- It is intended to protect the personal privacy of users, as well as their freedom and ability to conduct confidential business by keeping their internet activities from being monitored.



Silk Road Website

U.S. authorities shut down Silk after the alleged owner of the site Ross William Ulbricht was arrested.

hidden wiki at Duck | Hidden Wiki Links | ffi5v46ttwgx3fby.onion/ | Euro Guns - Numbe | Hidden Wiki | mmgh3rqeswrlgzdr | Imperial Library of T

wywg65dio2lhe76z.onion

EuroGuns

Products FAQs Register Login

Walther PPK, Kal.7,65

New and unused and unregistered!
Ammo can only be purchased if you also buy the gun.

Product	Price	Quantity
Walther PPK, Kal.7,65	600 EUR = 0.07046 ฿	1 X Buy now
Ammo, 50 Rounds	40 EUR = 0.00470 ฿	1 X Buy now

Sunum | Bilgi Güvenliği Ba... | Gelen Kutusu (12)... | Euro Guns - Num... | TUR 14:04

hidden wiki at DuckDuck | Hidden Wiki Links - Com | ffi5v46ttwgx3fby.onion/ | Rent-A-Hacker - Hire a h | UK Passports - Buy real U | Hidden Wiki

njs4tmqjy64rpyji.onion

Products | Login | Register | FAQs

UK Passports

Your UK Passport - Name of your choice!

We are selling original UK Passports made with your info/picture.
Your info will get entered into the official passport database.
So it's possible to travel with our passports.
How we do it? Trade secret!
Information on how to send us your information and pictures will be given after purchase!

You can even enter the UK/EU with our passports, we will add a stamp for the country you are in before we send you your passport to any country!
Ideal for people who want to work in the EU/UK.

Product	Price	Quantity
Your original UK passport with your info/pictures This is 50% of the final price, you pay the other 50% once we show you pictures of your new passport	1000 GBP = 0.13903 ฿	1 X Buy now
NEW: UK bank account with online banking and card. Great for cashing out bitcoin. Accounts are created in a secure way to make sure they don't get banned.	700 GBP = 0.09732 ฿	1 X Buy now

Temp | Gelen Kutusu (12) - g... | UK Passports - Buy re... | TUR 14:02

hidden wiki at Duck | Hidden Wiki | Tor | Hidden Wiki Deep Web | owriezc726nuc3fv | penisvqibeqxdo2s | HOME | ELECTRONION

creditclap4h3w6b.onion

80%

CreditCard and PayPal vendor

Home | EU cards | US cards | PayPal | How to buy | Contact us

We are a vendor for credit cards (both eu and us) and paypal accounts.

You can purchase the cards and the paypal accounts by sending a mail to us. Browse through the cards and accounts and feel free to ask any questions you have.

We ship with UPS or to Germany with DHL. All shippings are provided with a tracking number so you can follow your order.

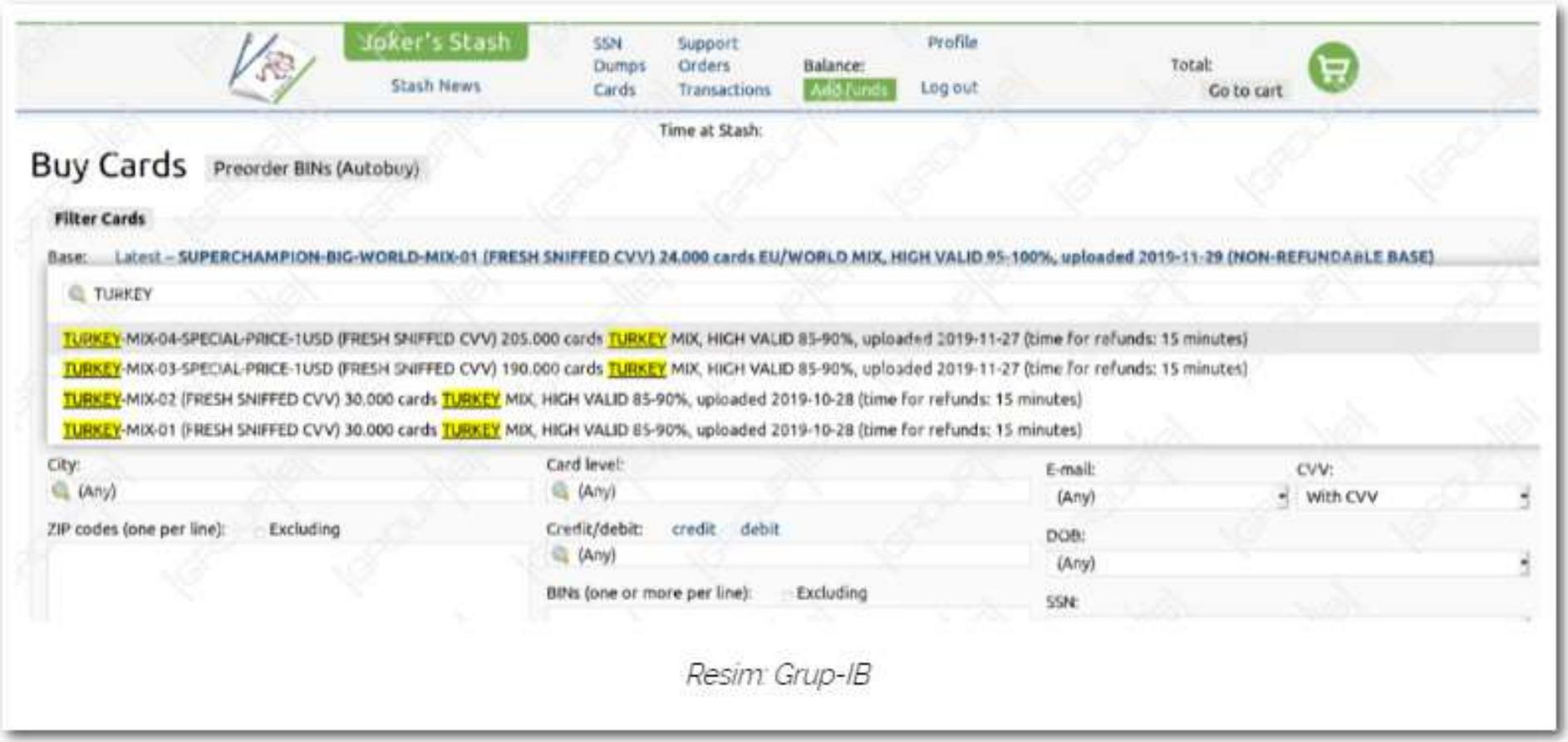
EU cards
Cards with up to 5000€ to withdraw worldwide!

US cards
Cards with up to 5000$ to withdraw worldwide!

PayPal

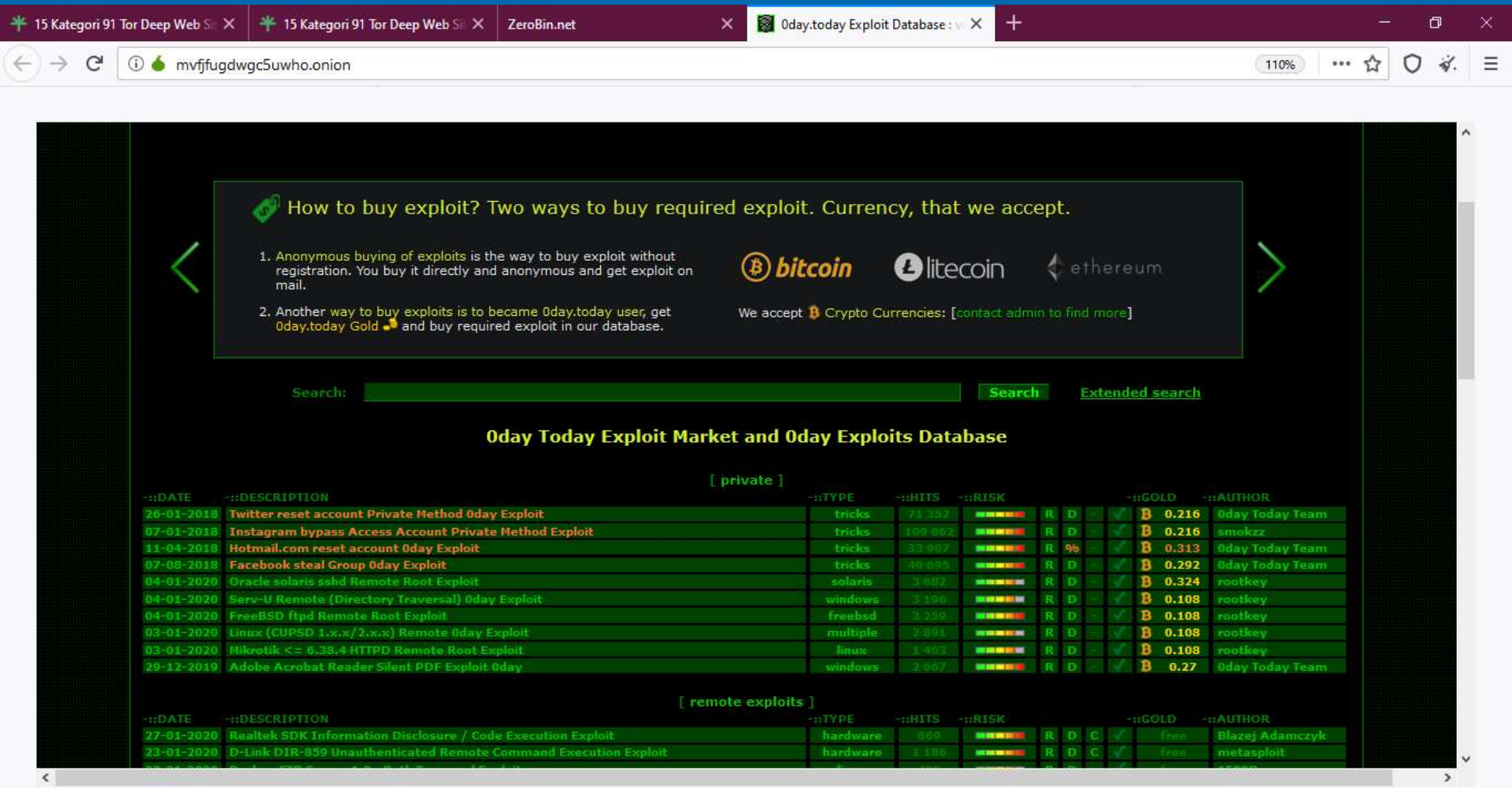
PayPal Accounts
Fresh PayPal accounts with up to 3500$ to cash out!

Sunum | Bilgi Güvenliği Ba... | Gelen Kutusu (12)... | HOME - Tor Brow... | TUR | 14:22



Resim: Grup-IB


hidden wiki at DuckDuck
Hidden Wiki Links - Com
ffi5v46ttwgx3fby.onion/
Rent-A-Hacker - Hire a h
UK Passports - Buy real U
Hidden Wiki
5eme2auqilcux2wq.onion
Rent-A-Hacker
Products
FAQs
Register
Login
Rent-A-Hacker
Experienced hacker offering his services!
(Illegal) Hacking and social engineering is my business since i was 16 years old. I never had a real job, so i had the time to get really good at hacking and i made a good amount of money last +-20 years.
I have worked for other people before, now i am also offering my services for everyone with enough cash here.
Prices:
I am not doing this to make a few bucks here and there, i am not from some crappy eastern europe country and happy to scam people for 50 EUR.
I am a professional computer expert who could earn 50-100 EUR an hour with a legal job.
So stop reading if you don't have a serious problem worth spending some cash at.
Prices depend a lot on the problem you want me to solve, but minimum amount for smaller jobs is 250 EUR.
You can pay me anonymously using Bitcoin.
Technical skills:
- Web (HTML, PHP, SQL, APACHE)
- C/C++, Assembler, Delphi
- 0day Exploits, Highly personalized trojans, Bots, DDOS
- Spear Phishing Attacks to get accounts from selected targets
- Basically anything a hacker needs to be successful, if i don't know it, i'll learn it very fast
- Anonymity: no one will ever find out who i am or anything about my clients.
Social Engineering skills:
- Very good written and spoken (phone calls) english, spanish and german.
- If i can't hack something technically i'll make phone calls or write emails to the target to get the needed information, i have had people make things you wouldn't believe really often.
- A lot of experience with security practices inside big corporations.
Sunum
Bilgi Güvenliği Ba...
Gelen Kutusu (12)...
Rent-A-Hacker - ...
TUR
14:03


15 Kategori 91 Tor Deep Web
15 Kategori 91 Tor Deep Web
ZeroBin.net
0day.today Exploit Database
mvfjfugdwgc5uwho.onion
110%
How to buy exploit? Two ways to buy required exploit. Currency, that we accept.
1. Anonymous buying of exploits is the way to buy exploit without registration. You buy it directly and anonymous and get exploit on mail.
2. Another way to buy exploits is to became 0day.today user, get 0day.today Gold and buy required exploit in our database.
bitcoin
litecoin
ethereum
We accept Crypto Currencies: [contact admin to find more]
Search:
Search
Extended search
0day Today Exploit Market and 0day Exploits Database
[private]
-::DATE -::DESCRIPTION -::TYPE -::HITS -::RISK -::GOLD -::AUTHOR
26-01-2018 Twitter reset account Private Method 0day Exploit tricks 71 352 R D - 0.216 0day Today Team
07-01-2018 Instagram bypass Access Account Private Method Exploit tricks 109 862 R D - 0.216 smokzz
11-04-2018 Hotmail.com reset account 0day Exploit tricks 33 907 R % - 0.313 0day Today Team
07-08-2018 Facebook steal Group 0day Exploit tricks 40 695 R D - 0.292 0day Today Team
04-01-2020 Oracle solaris sshd Remote Root Exploit solaris 3 682 R D - 0.324 rootkey
04-01-2020 Serv-U Remote (Directory Traversal) 0day Exploit windows 3 196 R D - 0.108 rootkey
04-01-2020 FreeBSD ftpd Remote Root Exploit freebsd 3 259 R D - 0.108 rootkey
03-01-2020 Linux (CUPSD 1.x.x/2.x.x) Remote 0day Exploit multiple 2 891 R D - 0.108 rootkey
03-01-2020 Mikrotik <= 6.38.4 HTTPD Remote Root Exploit linux 1 403 R D - 0.108 rootkey
29-12-2019 Adobe Acrobat Reader Silent PDF Exploit 0day windows 2 667 R D - 0.27 0day Today Team
[remote exploits]
-::DATE -::DESCRIPTION -::TYPE -::HITS -::RISK -::GOLD -::AUTHOR
27-01-2020 Realtek SDK Information Disclosure / Code Execution Exploit hardware 669 R D C free Blazej Adamczyk
23-01-2020 D-Link DIR-859 Unauthenticated Remote Command Execution Exploit hardware 1 186 R D C free metasploit
3.2 Million "Right to B...
0day.today Exploit Da...
TUR
10:18

ego sum qui sum

CNN

Live TV

'Internet of things' or 'vulnerability of everything'? Japan will hack its own citizens to find out

By James Griffiths, CNN

Updated 9:59 PM EST, Fri February 01, 2019

(CNN) — Children playing in a middle school gym in Indonesia; a man getting ready for bed in a Moscow apartment; an Australian family coming and going from their garage; and a woman feeding her cat in

ÖNCE BAŞLIKLAR?

GÜNDEM

DİKKAT!! Televizyonunuz Sizi Dinliyor!!

Sesli kumanda fonksiyonu bizi dinliyor mu?

Samsung, müşterilerini akıllı televizyonların sesli kumanda fonksiyonu devredeyken şahsi konularda konuşmamaları için uyardı. Söz konusu kurulumun televizyon sahiplerini dinlediği de eklendi.Ortamdaki tüm konuşmaları kaydeden televizyonun bu kayıtları Samsung ya da üçüncü kişilerle paylaşabildiği de belirtiliyor.

Aktivistler buna şiddetle karşı çıkarken ,bu teknolojinin George Orwell'in herkesin izlendiği otoriter bir geleceğin kurgulandığı 1984 adındaki romanını anımsattığını söylüyorlar.

2014'ün en çok kullanılan şifreleri listesi ise şu şekilde:

1- 123456 (yerini korudu)
2- password (yerini korudu)
3- 12345 (17 sıra yükseldi)
4- 12345678 (1 sıra düştü)
5- qwerty (1 basamak düştü)
6- 1234567890 (yerini korudu)
7- 1234 (9 basamak yükseldi)
8- baseball (listeye yeni girdi)
9- dragon (listeye yeni girdi)
10- football (listeye yeni girdi)
11- 1234567 (4 basamak düştü)
12- monkey (5 basamak yükseldi)
13- letmein (1 basamak yükseldi)
14- abc123 (9 basamak düştü)
15- 111111 (8 basamak düştü)
16- mustang (listeye yeni girdi)
17- access (listeye yeni girdi)
18- shadow (yerini korudu)
19- master (listeye yeni girdi)
20- michael (listeye yeni girdi)

https://www.sabah.com.tr/teknoloji/2015/01/21/iste-en-cok-kullanilan-sifreler

Listeye göre en kötü 10 şifre;

12345678
qwerty
12345
123456789
letmein
1234567
football
iloveyou

https://www.sabah.com.tr/teknoloji/2017/12/20/sakin-bu-sifreleri-kullanmayin

23 HAZİRAN 2015
YAZAR: YAVUZ YENER

‘Gelmiş geçmiş en geniş çaplı siber saldırı: Shady RAT’

İlk defa 2011 yılında McAfee’nin hazırladığı bir raporla kamuoyunun haberdar olduğu Shady RAT (*Remote Access Tool*) saldırıları, gelmiş geçmiş en geniş çaplı siber saldırı olma ünvanını rahatlıkla hak ediyor. Bu çapta bir saldırıda dahi saldırganların kimlikleri tespit edilememiş olsa da McAfee’nin hazırladığı rapor, ekonominin her sektöründe faaliyet gösteren herhangi bir şirketin, benzer siber saldırılara maruz kalabileceğini vurguluyor.

McAfee, Shady RAT’in ilk izlerinin 2009 senesinde, bir savunma şirketinin uğradığı saldırıların forenzik analizinin yapıldığı dönemde keşfedildiğini belirtiyor. McAfee, saldırganların komuta-kontrol serverlarından birisine erişim edindiğini ve saldırı loglarını bu serverlar üzerinden analiz ettiğini belirtiyor.

Rapora göre hedef alınan bir firmada saldırıların fark edilip gerekli önlemlerin alınması hâlinde dahi sızmanın, ilk başladığı andan itibaren yaklaşık bir ay boyunca devam ettiği belirtiliyor. Sızmanın kısa sürdüğü kurbanlar arasında Uluslararası Olimpiyat Komitesi, Vietnamlı bir teknoloji şirketi, Asyalı bir ülkenin ticaret örgütü, Kanadalı bir devlet kurumu, Amerikalı bir savunma şirketi ile Amerikalı bir muhasebe firması bulunuyor. Ancak rapor, bu sızmaların kısa sürmesini sadece kurbanların siber savunmadaki başarısıyla değil, saldırganların bazı örneklerde zaten kısa bir saldırı amaçlamasıyla da açıklıyor. Diğer taraftan sızmaların 20-28 ay boyunca tespit edilemediği pek çok örnek de var.

Örgütlü bir şekilde saldırdığı anlaşılan hackerların temel hedefleri devletler, örgütler, büyük firmalar, savunma şirketleri ve hatta uluslararası Olimpiyat komiteleri. ABD, Japonya, Tayvan, Birleşik Krallık, Hindistan, Güney Kore, Vietnam ve Kanada büyük zarara uğrayan devletler arasında yer alıyor. Bunun dışında Birleşmiş Milletler ve Uluslararası Olimpiyat Komitesi gibi uluslararası örgütler de saldırıların kurbanı.

19 EYLÜL 2016

Fransız ajan itiraf etti: NSA Başkanlık Sarayı'nın bilgisayarlarına girdi

Bernard Babier

Amerika Ulusal Güvenlik Ajansı NSA'nın marifetlerini bilmeyen pek az. Almanya Başbakanı Angela Merkel'i bile dinlemeye aldıklarının tüm dünyanın öğrendiği, NSA'nın bir şekilde Fransız sarayı Elysee'nin de bilgisayarlarına girdiği ortaya çıktı.

2006 ila 2013 yılları arasında Fransa'nın elektronik istihbaratından sorumlu Bernard Barbier'in itiraf ile bu gerçek gün yüzüne çıktı. İtiraf da Barbier'in 1976 yılında mezun olduğu üniversitede öğrencilere yaptığı konuşmanın görüntülerinin YouTube'de yayımlanması ve bu görüntüyü bir gazetecinin fark etmesi ile kamuoyuna mal oldu.

6 MART 2016

Siber saldırı hastaneyi çalışamaz hale getirdi

ABD'nin Güney Kaliforniya bölgesinde bulunan bir hastaneye yapılan siber saldırı sonucu, kurumun günlük işlemlerinde ciddi aksamalar meydana geldi ve hastalar tahliye edilmek zorunda kaldı.

Hollywood Presbyterian Hastanesi'nin sistemini hackleyen siber saldırganların hastane yönetiminden sisteme tekrar giriş izni için fidye istediği öğrenildi. Çalışan ya da hasta bilgilerinin çalınıp çalınmadığı bilinmese de, olayın ardından FBI soruşturmaya el koydu. Hastanenin acil servisinin saldırıdan ciddi anlamda etkilendiği duyuruldu.

6 EYLÜL 2016

St Jude olayı: Hackerlar yatırım şirketlerinin yeni partnerleri mi oluyor?

ABD geçtiğimiz iki haftadır bir yatırım firması, bir siber güvenlik şirketi ve bir de sağlık cihazı üreticisinin karıştığı daha önce örneği olmayan bir siber güvenlik olayını tartışıyor.

Kalp ile ilgili cihazlar üreten St. Jude Medical, medikal cihazların siber güvenliğine yoğunlaşan MedSec ve Muddy Waters adlı bir yatırım firmasını aynı hikayenin kahramanları haline getiren olay MedSec için çalışan hackerların St Jude'un ürettiği medikal cihazlarda çok ciddi güvenlik açıklarını bulduğunu iddia etmesiyle başladı.

Birçok 'meslektaşının' aksine St Jude'a siber saldırı düzenleyen hackerlar, şirkete mail atıp kriptoladığı veriler karşılığında fidye istemedi; ya da sistemlerde bulduğu sıfırıncı gün açıklıklarını şirkete satmaya çalışmadı. Bu alternatiflerin yerine farklı bir yol seçen MedSec hackerları bir yatırım şirketinin kapısını çalmayı tercih etti.

Mayıs ayında Muddy Waters Capital yatırım şirketinde yönetici olarak çalışan Carson Block'a ulaşan siber saldırganlar, yatırım uzmanını ellerinde St Jude'u piyasada çok ciddi sıkıntıya sokacak bilgilerin bulunduğuna ikna etti. Buna göre St Jude'un ürettiği kalp temposunu ayarlayan ve kalbin normal dışı atımını tekrar normal ritmine dönmesini sağlayan cihazlarda (defibrillator) hastaların hayatını tehdit eden güvenlik açıkları bulunuyor. MedSec'in bu durumu fark ettiği halde, müşterilerinin hayatının tehlikede olduğunu St Jude yerine bir yatırım şirketi olan Muddy Waters'a bildirmesinin bir etik skandal doğurmasına rağmen şaşırtıcı bilgiler bu kadarla sınırlı kalmıyor.

7 EYLÜL 2016

‘Sinsi yazılım Sauron’un arkasında bir devlet var’

Sauron Projesi olarak adlandırılan siber casusluk yazılımının geçtiğimiz beş yılda 30’a yakın kurum ve kuruluşun ağlarında faaliyet gösterdiği tespit edildi. Uzunca bir süredir ortalıkta olmasına rağmen daha geçtiğimiz eylül ayında farkedilen yazılım araştırmacıların korkulu rüyası haline geldi.

Yüzüklerin Efendisi hikayesindeki her şeyi görebilen karakterin ismi verilen kötü amaçlı yazılım sisteme giriş bilgileri, şifreleme anahtarları, yapılandırma dosyalarını ele geçirmek için kullanılabildiği gibi aynı zamanda klavye hareketlerini kaydederek sistemlerde arka kapı oluşturarak siber saldırganlara davetiye çıkarıyor.

Comodo’un iddiasına göre, bu kötü amaçlı yazılımın ardında devlet destekli bir hacker grubunun bulunma ihtimali var. Ordu, finansal ve telekomünikasyon kurumlarının ağlarında da tespit edilen yazılım Çin’den Belçika’ya ve İsveç’e kadar bir çok ülkedeki çeşitli kurumların sistemlerinde saptandı.

26 ŞUBAT 2016
YAZAR: REYHAN GÜNER

Siber Dünyanın Çete Lideri: Ehud Tenenbaum

Ehud Tenenbaum, nam-ı diğer "The Analyzer" ya da "Udi", ABD Hava Kuvvetleri'nin bilgisayarlarından Hamas'ın resmi web sayfasına kadar, siber alanda hacklenmedik platform bırakmayan bir İsrailli hacker. İsmi son olarak ABD ve Kanada'daki çeşitli bankaların hesaplarından milyonlarca doları kendi hesabına aktarmasıyla yeniden gündeme gelen Tenenbaum, 17 yıllık bilgisayar korsanlığı macerasının neredeyse tamamını hakkında verilen tutuklama kararlarından kaçarak geçirmesine rağmen bir türlü iflah olmuyor.

Tüm zamanların siber suç çeşitliliği bakımından "en zengin" eylemlerini gerçekleştiren Ehud Tenenbaum, 1979 yılında İsrail'in Hod HaŞaron kentinde dünyaya geldi. Diğer hacker hikayelerinin aksine, Tenenbaum'un çocukluğu ve siber dünyaya merak salışıyla ilgili detaylar net olarak bilinmiyor. Fakat efsane hackerın ismine ilk kez Pink Pony (Pembe Midilli) adlı hacker grubunun üyeleri arasında rastlıyoruz. Pink Pony'de kendi gibi bilgisayar korsanlarıyla iletişime geçip siber kabiliyetlerini geliştiren ve farklı siber saldırı taktikleri öğrenen Tenenbaum, kısa zamanda etrafında toplanan yetenekli ve bir o kadar da tehlikeli bilgisayar korsanlarından oluşan bir siber grubun liderliğini yapmaya başladı.

25 Ekim 2017

Ukrayna Bitcoin'i yasallaştırıyor, madencilik faaliyetleri artıyor

Ukrayna Parlamentosu'na 6 Ekim'de sunulan ilk yasa tasarısının hemen ardından, kripto para birimleriyle ilgili ikinci yasa tasarısı Ukrayna Parlamentosu'na sunuldu. Yeni tasarılar ülkede bu para birimlerinin mali varlık olarak tanınmasını sağlarken aynı zamanda madencilik faaliyetleri için sadeleştirilmiş vergilendirme ve düşük fatura gibi kolaylıklar sağlıyor.

Yeni yasa tasarısında, parlamentonun mali politikalarıyla ilgilenen komitesinin başındaki Serhiy Rybalka kripto para birimlerinin "mali varlık" olarak tanınmasını önerdi. Bitcoin.com'un haberine göre Rybalka, kripto para birimleriyle ilgili yeni kurallar çıkarıp süreci uzatmaktansa bu para birimlerini mevcut yasalara uyarlamanın daha iyi bir çözüm olacağını düşünüyor.

16 Şubat 2018

Japonya'nın en büyük bankası kripto para çıkarmaya hazırlanıyor

Japonya'nın en büyük bankası Mitsubishi UFJ, gelecek aya kendi kripto parasını piyasaya sürmeyi planlıyor. MUFG Coin'i Japon Yeni partisinde olacak ve öncelikle finansal hizmetlerde çalışanlara sunulacak. Kredi kartıyla karşılaştırıldığında, bu adımla birlikte, bireyler arasındaki para transferi veya alışveriş gibi işlemler daha düşük maliyetlerle gerçekleştirilecek.

Kullanıcıların kripto parayı kullanabilmesi için bir hesap oluşturması gerekecek ve MUFG, işlemlerin dahili olarak yürütülmesini üstlenecek. Mitsubishi UFJ Financial, 2016 yılında paraları sunmak için bir takım testler yaptı ve geçen sene Coinbase tarafından işletilen kripto para değişimi GDAX ile anlaştılar.

11 Aralık 2017

Bitcoin, enerji tüketiminde Danimarka'yla yarışıyor

Bitcoin'in hızla yükselen değeri rekor seviyede enerji tüketimini beraberinde getiriyor. Ars Technica adlı internet sitesinin haberine göre, Bitcoin yıllık enerji tüketimi Danimarka'nın yıllık enerji tüketimiyle aynı seviyede.

Yıllık enerji tüketiminin 32 TWh civarında olması beraberinde sürdürülebilirlikle ilgili soruları da getiriyor. Grist adlı derginin yazarı Eric Holthaus bugünkü oranlara bakarak Bitcoin'in 2020 yılına kadar bütün dünyanın tükettiği miktarda elektrik enerjisi tüketeceğini tahmin ediyor. Holthaus'a göre bu sürdürülebilirlik açısından sorunları beraberinde getiriyor.

12 Şubat 2018

Kaspersky'deki iç savaşı Rus istihbaratı mı kazandı?

Müşterilerinin özel -ve hatta gizli- bilgilerini Rus istihbaratına aktardığına yönelik iddialarla zor günler yaşayan siber güvenlik şirketi Kaspersky Lab hakkında bu iddiaları destekleyen bir yazı yayınlandı. BuzzFeed'in Rusya merkezli Medusa sitesinden aktardığı habere göre, şirketin kontrolü için Batılı yatırımcılar, işine odaklanmış mühendisler ve Rus istihbarat servisine yakın odaklar arasındaki mücadele sonuçlandı. Ancak şirketin, Rusya dışında 1998'den bu yana inşa ettiği her şeyi mahvetmek pahasına...

Habere göre, söz konusu 3 grup arasındaki mücadele 2010 yılında başladı. Şirketin CEO'su Eugene Kaspersky'nin 20 yaşındaki oğlu Ivan'ın Moskova'da kaçırıldığı 19 Nisan 2011'de gün yüzüne çıktı. O sırada Londra'da olan Eugene, olaydan bir telefonla haberdar oldu. Oğlunu kaçıranlar, 3 milyon Euro fidye istiyordu. Eugene Kaspersky hemen şirketin avukatı - ve eski bir KGB çalışanı olduğu iddia edilen - Igor Chekunov'u arayarak yardım istedi. Ivan dört gün sonra kurtarılsa da bu olaydan sonra Kaspersky Lab şirketindeki mücadelede Rus istihbaratı ağır basmaya başladı.

13 Şubat 2018

Ülke şokta: 10 İsviçreliden birinin kişisel bilgileri ele geçirilmiş

İsviçreli telekomünikasyon şirketi Swisscom, geçtiğimiz yıl bir güvenlik açığından dolayı yaklaşık 800 bin müşterisinin kişisel bilgilerinin yetkili olmayan kişilerin eline geçtiğini itiraf etti. Info security'nin haberine göre büyük kısmı devlete ait olan şirket, söz konusu bilgileri ele geçiren kişilerin geçtiğimiz sonbaharda şirketin satış ortaklarından biri aracılığıyla sisteme sızdığını açıkladı.

Mağdur olan kişilerin çoğunu cep telefonu müşterileri oluştururken az sayıda internet abonesinin de durumdan etkilendiği belirtildi. Bilgileri ele geçirilen müşterilerin sayısı, İsviçre nüfusunun yüzde 10'una tekabül ediyor.

Gizliliği ifşa edilen bilgileri arasında müşterilerin adları, adresleri, telefon numaraları ve doğum tarihleri bulunuyor. Swisscom, bu bilgileri 'hassas olmayan bilgi' kategorisinde değerlendirse de, söz konusu veriler kötü niyetli kişilere e-dolandırıcılık yapma noktasında bir başlangıç alanı sağlıyor. Şirket şimdiye kadar böyle bir şey olmadığını açıkladı.

19 Şubat 2018

İnternet kullanıcıları en çok parasal mevzularda 'oltaya geliyor'

Phishing, İngilizce password (parola) ile fishing (avlama) kelimelerinin birleşiminden oluşan bir siber güvenlik terimi. Yemleme olarak Türkçeye çevrilen saldırı yöntemi ile yasadışı yollarla bir kişinin şifresini veya kredi kartı ayrıntılarını öğrenmek amaçlanıyor. Scmagazineuk.com sitesinin haberine göre, son yapılan bir araştırma internet kullanıcılarının en çok parasal konularda oltaya geldiğini ortaya koydu.

KnowBe4 araştırması kapsamında yaklaşık 6 milyon kişiye yemleme e-postası gönderildi. Çıkan sonuç ise insanların en çok para vaat eden ya da para kaybı ile tehdit edilen yemleme e-postalarının peşinden gittiğini gösterdi.

27 Ocak 2018

Japonya'da 500 milyon dolarlık kripto para vurgunu

Bilgisayar korsanları, Japonya'nın en büyük dijital döviz piyasalarından biri olan Coincheck'in sistemlerini hackleyerek, yaklaşık 500 milyon dolar değerindeki kripto parayı kendi hesaplarına geçirdi.

Coincheck, Cuma günü yaşanan olayın ardından Bitcoin haricindeki tüm kripto para birimlerine ait işlemleri durdurduklarını açıkladı.

Bilgisayar korsanlarının NEM adlı kripto parayı nasıl çaldıklarının incelendiği belirtildi. Coincheck'ten yapılan açıklamada "Müşterilerimizin varlıklarının koruma altında olduğunu garantilemeye çalışıyoruz" denildi.

2014'te de bir diğer Japon dijital döviz piyasası sistemlerinden 480 milyon dolardan fazla kripto paranın çalındığını açıklamıştı. Başta Bitcoin olmak üzere, birçok ditijal para birimi geçen Aralık ayında büyük değer kazanmış, Ocak ayı ortasında ise ciddi düşüş yaşamıştı.

Bir ara 19 bin 800 dolara kadar yükselen Bitcoin, Ocak ayı ortasında 10 bin doların altına indi.

16 Şubat 2018

Hackerlar, Rusya Merkez Bankası'ndan 6 milyon dolar çaldı

Rusya Merkez Bankası, uluslararası para transfer sistemi SWIFT'e gerçekleştirilen bir saldırı ile geçen sene sisteminden 6 milyon dolar (339,5 milyon ruble) çalındığını açıkladı.

Reuters'ın haberine göre Rusya Merkez Bankası, saldırıyı Rus bankalarına karşı gerçekleştirilen dijital hırsızlıklar adlı raporunun sonunda belirtti. Saldırının kimler tarafından gerçekleştirildiği ise aktarılmadı.

Rusya Merkez Bankası, "SWIFT sistemi operatörüne gerçekleştirilen başarılı bir saldırı ile 339,5 milyon ruble'nin çalındığına" dair bilgi edindiklerini belirtti. Banka, Reuters'a konuyla ilgili detaylı bilgi vermedi.

Saldırılar yaygınlaştı

Her gün trilyonlarca dolar paranın transfer edildiği SWIFT sisteminin sözcüsü ise olay bazında açıklama yapmadıklarını belirtti. SWIFT sözcüsü Natasha de Teran, herhangi bir olası dolandırıcılığın bildirilmesi takdirinde güvenliğin sağlanması için yardımcı olduklarını söyledi.

19 Şubat 2018

‘Beyaz şapkalı hackerlar’ mühendislerden 3 kat fazla kazanıyor

‘Bug bounty hunter’ Türkçeye ödül avcısı olarak çevirebileceğimiz bir hacker terimi. Bu kişileri, teknoloji firmalarının sistemlerinin daha güvenli olmasını sağlamak adına düzenledikleri yarışmalara katılan ve sistemlerdeki açıkları siber saldırganlardan önce bulan ‘iyi niyetli hacker’ olarak tanımlamak mümkün.

Son yapılan bir araştırmaya göre ise bu ‘ödül avcıları’ ortalamanın epeyce üzerinde bir gelire sahipler. 195’ten fazla ülkede 1700 ödül avcısı arasında yapılan bir araştırmaya göre ‘iyi niyetli hacker’ ya da ‘beyaz şapkalı hacker’ olarak bilinen ödül avcılarının standart bir yazılım mühendisi maaşının 2,7 katı büyüklüğünde yıllık gelirleri bulunuyor.

Araştırma, teknoloji şirketlerinin güvenlik açığını bulabilen kişilere binlerce dolar kazandıran HackerOne adlı şirket tarafından gerçekleştirildi. Şirketin kendi düzenlediği ödül avı yarışmasından elde edilen bilgilere dayandırdığı araştırmaya göre bazı yerlerde hackerler ile mühendislerin geliri arasındaki uçurum daha da derin. Örneğin Hindistan’da hackerlerin geliri mühendislerin gelirinin 16 katına çıkabiliyor. ABD’de ise ödül avcıları ortalamanın 2,4 katı gelire sahip.

19 Şubat 2018

Riyad yönetiminden biyometrik güvenliğe büyük yatırım

Riyad'da bulunan Kral Saud Üniversitesi (KSU), Kral Abdüllaziz Şehri Bilim ve Teknoloji Ofisi'nden dijital güvenliğe katkı sağlayacak biyometrik şifreleme sistemleri araştırmasında kullanılmak üzere hibe aldı. Parmak izi, yüz tanıma, avuç içi izi, iris ve ses yoluyla kimlik belirleme yöntemlerini içeren biyometrik tabanlı kimlik belirleme teknolojileri kişiye özgü biyolojik ya da davranışsal karakteristik özellikleri belirlemede kullanılıyor.

Krallık da dahil bir çok ülke, ulusal güvenlik ve kimlik hırsızlığını önlemek için biyometrik sistemlere yatırım yapıyor. KSU'da görev yapan Prof. Muhammed Khurram Han, hibe kapsamında oluşturulan araştırma ekibinin lideri oldu. Khan, Arab News'a yaptığı açıklamada hibenin, 'El Tabanlı Biyometrik Birleşme ve Biyo-Şifreleme Ölçümü' (Hand-based Biometrics Fusion and Bio-Cryptosystem Computation) adlı projede kullanılacağını söyledi. Han ayrıca projenin, 'Ulusal Dönüştürme 2020 İnisiyatifi' adı altında üniversite ve araştırma merkezlerine sağlanan hibe programı kapsamında kabul edildiğini ifade etti.

13 Aralık 2017

Almanya hack-back istiyor

Almanya, diğer ülkelerin kendisine yönelik gerçekleştirdiği siber saldırılara karşı ‘hack back’ yapmak istiyor. Cyberdb’nin haberine göre iç istihbarat servisi yetkilileri geçtiğimiz ekim ayında kanun yapıcılardan, ülkeye yönelik gerçekleştirilen siber saldırılara ‘karşı saldırı’ yapmasına izin verecek yetkinin çıkartılmasını istiyor.

İç istihbarat birimi yönetimi, özellikle Alman server’larından çalınarak yurtdışında konuşlu olan serverlara taşınan bilginin silinmesini mümkün kılacak yetkiye sahip olmak istiyor. Almanya’nın dış istihbarat birimlerinin buna yetkin olduğu halde böyle operasyonları yürütme hakkı bulunmuyor.

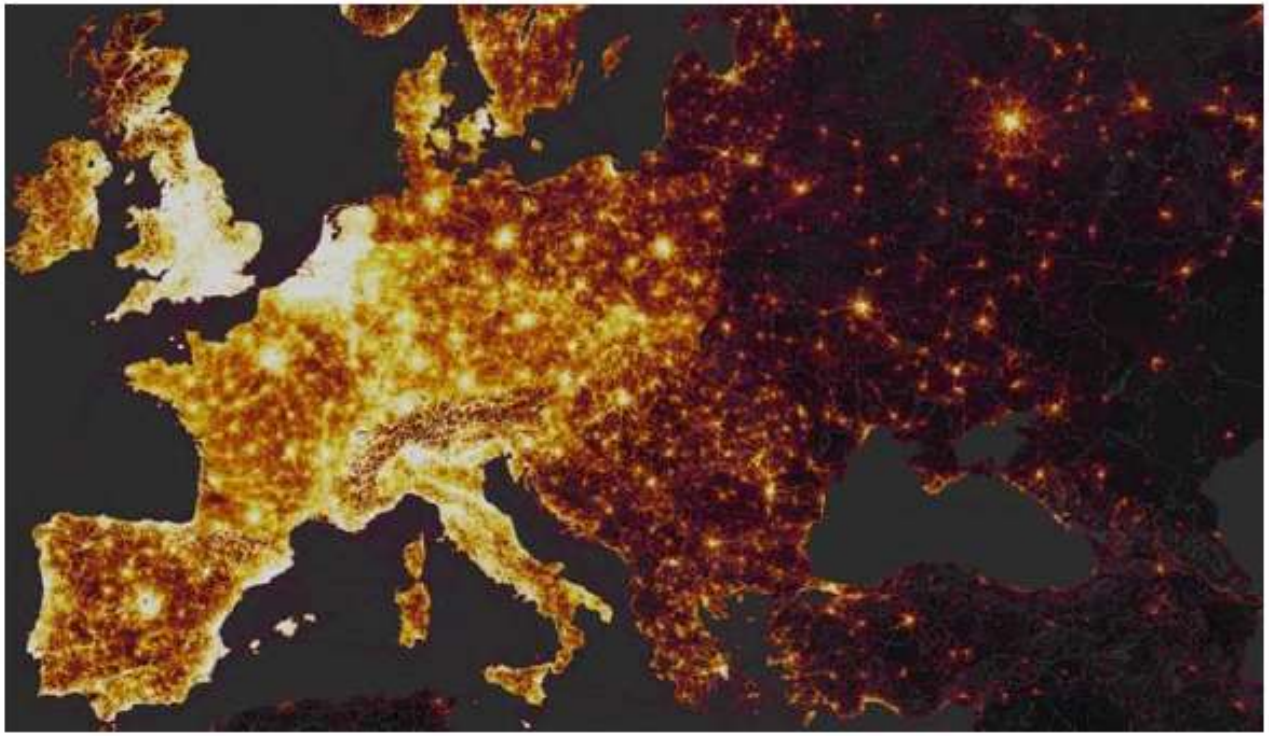
İlgili haber>> Almanya, WhatsApp mesajlarını hacklemeye hazır

Diğer bir çok ülke gibi Almanya da uzun süredir APT olarak adlandırılan ve yabancı hükümetler tarafından yürütüldüğünden şüphelenilen ‘gelişmiş kalıcı tehditler’in kurbanı durumunda. APT genel olarak saldırganların sistemlere yetkisiz erişim sağlayarak orada uzun süre kalması anlamına geliyor.

ABD endişeli: Fitness uygulaması Strava gizli askeri üsleri açığa çıkardı

Günlük Haber Onur Seven **29 Ocak 2018, Pazartesi 11:25** 14370 10

Fitness takip uygulaması Strava'nın kamuya açık ısı haritası Suriye ve Irak gibi savaş bölgelerindeki gizli askeri üstleri açığa çıkardı. Peki ısı haritasında güvenliği tehdit eden başka neler var?



Birçok koşu, jogging ve **fitness uygulaması** kullanıcıların spor aktivitelerini takip etmesini sağlayan **GPS özelliğiyle** birlikte gelir. Bunlardan biri olan **Strava**'nın Amerika'ya ait gizli **askeri üslerin** ve tesislerin yerlerini dünyaya açmış olması büyük yankı uyandırdı.

19 ŞUBAT 2019

İnsan gibi metin üreten yapay zekayı rafa kaldırdılar

OpenAI adlı yapay zeka çalışmaları yürüten kuruluş, insan gibi metinler üretebilen yapay zekayı tehlikeli bularak rafa kaldırdı.

Yazılım basit olarak kendisine verilen bir metinde sırada kullanılacak kelimeleri seçiyor ve metnin tutarlı şekilde devamını getiriyor. Tıpkı bir insan gibi yazabildiği görülen algoritma üzerindeki çalışmalar kötü amaçlarla kullanımı ve yol açabileceği zararlar düşünülerek şimdilik durduruldu.

Bir insandan farksız şekilde her konuda mükemmel metin yazarlığı yapabilen bir yazılımın özellikle 'yalan haber' üretimi ve sosyal medyada trendler oluşturmak veya siyasi, ekonomik saldırı amaçlarıyla robot hesaplarca kullanılabileceği öngörülüyor.

Kısıtlı bir sürümü yayınlanacak

Kendi kendini sürebilen Tesla otomobilleri ve kendi kendine iniş yapan roketler üreten SpaceX firmasının sahibi Elon Musk'ın en büyük finansörü olduğu OpenAI kar amacı gütmeyen ve pek çok alanda yapay zeka geliştiren bir organizasyon.

Musk yapay zekanın insanoğlunun varlığına bir numaralı tehdit olduğunu düşünüyor ve bu konuda yetkilileri her fırsatta uyarıyor. OpenAI'ın kurucularından olan Musk, bu organizasyonda yöneticilk yapmıyor ve yapılan araştırmalara müdahale etmiyor ancak içeriğini herkesten önce öğrenebiliyor

18 ŞUBAT 2019

İngiliz meclisinden Facebook'a ağır suçlama: Dijital Gangster

İngiliz meclisi raporunda, Facebook, gizilik ve rekabet kurallarını kasıtlı olarak çiğnemekle suçlanarak "dijital gangster gibi davranmakla" suçlandı.

İngiltere Parlamentosu Dijital, Kültür, Medya ve Spor Komitesi'nin dezenformasyon ve sahte haber ile ilgili hazırladığı 108 sayfalık raporda, Facebook'un kullanıcıların verilerini kâr amaçlı sattığı, sosyal medya platformunun çok daha katı bir düzenlemeye tabi tutulması gerektiği vurgulandı.

Komite'nin bir yıldan uzun süren çalışması sonucu ortaya çıkan raporda, şirkete ağır eleştiriler getirildi:

"Facebook, kârı veri güvenliğine tercih etmeyi sürdürüyor. Kullanıcı bilgilerinden kazanç elde etmek için risk alıyor. Bizce çok açık ki Facebook sadece ciddi güvenlik açıkları kamuoyunda duyulunca önlem alıyor" denildi.

Geçen yıl Facebook'un 50 milyon kullanıcı profiline ait verileri Cambridge Analytica şirketi ile paylaştığı ve bu bilgilerin şirket tarafından usulsüz kullanıldığı ortaya çıkmıştı. İngiliz şirket, kişisel verileri 2016 ABD başkanlık seçimlerini etkilemek için kullanmakla suçlanmıştı.

'Demokrasiyi riske atıyor'

20 MART 2018

Cambridge Skandalı, Facebook'a pahalıya mal oluyor: Soruşturmalar başladı

İngiliz şirket Cambridge Analytica'nın Facebook'ta 50 milyon kullanıcının kişisel verilerini usulsüz bir şekilde kullandığının ortaya çıkmasıyla başlayan skandal kar topu gibi büyüyor.

İngiltere ve Avrupa Birliği parlamentoları, Facebook'un kurucusu ve CEO'su Mark Zuckerberg'i ifade vermeye çağırdı.

ABD Federal Ticaret Komisyonu, Facebook'un kullanıcıların verilerini üçüncü parti kurumlarla paylaşarak kullanıcı sözleşmesini ihlal ettiğine dair haberlerin ortaya çıkmasının ardından soruşturma başlatıldığını duyurdu.

Facebook hisseleri çakılırken, şirket piyasa değerinden 20 milyar dolar kaybetti.

Soruşturmaların hedefinde olan sadece Facebook değil. İngiltere Bilgi Komisyonu, Cambridge Analytica hakkında soruşturma başlatılmasını istedi.

Skandal, Channel 4 televizyon kanalının Cambridge Analytica ile haberi ile ortaya çıktı. Televizyon kanalının yaptığı gizli kamera çekimlerinde şirketin yöneticileri, siyasetçilerin itibarını sarsmak için 'aşk tuzakları' hazırlanabileceğini ve rüşvet verilebileceğini söylerken görülüyordu. Şirket usulsüzlük yapıldığı iddialarını reddediyor.

Channel 4 News'un Pazartesi günü yayınlanan programında, zengin bir Sri Lankalı müşteri kılığında şirketle iletişime geçen muhabirleri Cambridge Analytica Yöneticisi Alexander Nix ile buluşuyor. Gizli kamerayla kaydedilen görüşmede Nix, internette siyasetçilerin nasıl itibarsızlaştırılabileceğine dair taktiklerini anlatıyor. Nix, hedef alınan bireye 'gerçek olamayacak kadar iyi bir anlaşma sunulabileceğini ve bu görüntülerin kayıt altına alınabileceğini' söylüyor.

19 ŞUBAT 2019

Telefon görüşmelerini izinsiz kaydeden Triout 50 milyon kez indirilmiş

Ağustos 2018'de keşfedilen ve telefon görüşmelerini izinsiz kaydeden **Triout** casus yazılımı yeniden ortaya çıktı. Dünyada 500 milyondan fazla kullanıcıyı koruyan Bitdefender Antivirüs, Google Play'de ve üçüncü parti mağazalarda bulunan Psiphon uygulamasıyla cihaza kullanıcının bilgisi dışında yüklenen Triout yazılımının 50 milyon kez indirildiğini tespit etti.

Popüler uygulamaları kullanarak cihazlara sızan ve hedefli casusluk saldırıları düzenlemek amacıyla üretildiği düşünülen Triout, telefon görüşmeleri, mesajlar, fotoğraflar, videolar ve lokasyonlar gibi bilgileri ele geçirerek siber saldırganların yönettiği bir sunucuya yönlendiriyor.

En son 7 Aralık 2018'de aktif gözüken yazılımın varlığını tekrar tespit eden araştırmacılar, yazılımın artık (Psiphon) "com.psiphon3" isimli proxy uygulamasıyla yayıldığını belirterek gizlenme kabiliyeti oldukça yüksek olan Triout'a karşı uyarıyor.

Gizliliği Yem Olarak Kullanıyor

Engelli bazı websitelerine giriş sağlayan popüler bir uygulama olan ve bir öncekiyle aynı kötü niyetli yazılım kökünü barındıran Psiphon uygulamasının şimdiye kadar 50 milyondan fazla indirildiği ve çoğu pozitif olmak üzere 1 milyondan fazla yoruma sahip olduğu biliniyor.

15 ŞUBAT 2019

Bu Trojan cep telefonu hareket edince bulaşıyor!

Google Play'de bulunan bazı aplikasyonlar üzerinden cep telefonuna bulaşan ve harekete duyarlı olan bir Trojan ortaya çıktı.

Son dönemde özellikle mobil cihazlara yönelik zararlı yazılımların sayısında artış gözleniyor. Trend Micro araştırmacıları Google Play'de geniş kullanıcı kitlelerine yayılma olasılığı bulunan iki adet zararlı bankacılık yazılımı keşfettiler.

Görünüşte online bankacılık kullananlar için birçok avantaj sağlayan Currency Converter ve BatterySaverMobi olarak adlandırılan bu iki uygulama kısa sürede Google Play'den kaldırıldı.

Pil kullanımında tasarruf sağlamaya yardımcı olacağı belirtilen BatterySaverMobi isimli uygulama kaldırılmadan önce 5 bin defa indirilmişti. 73 kullanıcıdan 4,5 gibi yüksek bir puan alan uygulama hakkında yapılan yorumların ise çoğunun anonim ve gerçeği yansıtmadığı görüldü.

Para birimlerini çevirmeye yardımcı olan Currency Converter ve BatterySaverMobi uygulamaları üzerinden saldırganlar kullanıcının cihazına ve sensörlerine erişerek burada saklanıyor. Kullanıcılar cihazlarını hareket ettirdiğinde, hareket sensöründen gelen veriyle birlikte trojan aktive oluyor.

2 EKİM 2018

Kim Kardashian internette aranması en tehlikeli ünlü isim!

Kim Kardashian

İnternette Kim Kardashian-West'in kızkardeşleriyle tartışmaları ya da eşi Kanye West'in Twitter'daki çıkışlarına verdiği yanıtları merak ediyor ve internette arıyorsanız daha dikkatli olmanız gerekiyor.

Siber güvenlik şirketi McAfee'ye göre Kim Kardashian 2018 yılında internette aranması en tehlikeli ünlü isim.

Şirket, ünlülerin isimleri aranınca çıkan sonuçların kaçında zararlı sitelere linkler bulunduğunu ölçerek sıralama yapıyor.

Geçen yılki listede ilk sırada Craig David bulunuyordu.

Bu yılki sıralamada Naomi Campbell ikinci olurken, Kim Kardashian'ın kızkardeşi Kourtney Kardashian üçüncü sırayı aldı. Şarkıcı Adele ve Love Island programının sunucusu Caroline Flack de dördüncü ve beşinci sıradalar.

30 MART 2018

Hackerlar, Scarlett Johansson'ın fotoğrafının içine kötü amaçlı yazılım sakladı

Siber saldırganlar, bu kez de Monero madenciliği yapan kötü amaçlı yazılımı yaymak için ünlü oyuncu Scarlett Johansson'ın fotoğrafını kullandı. Hackread'in haberine göre, Imperva adlı şirketteki araştırmacılar madencilik yapan kötü amaçlı yazılımın kurulması için saldırganların PostgreSQL sunucusunu ele geçirdiğini fark etti.

Kötü amaçlı yazılım ünlü Hollywood yıldızı Scarlett Johansson'un fotoğrafının içine gizlenmişti. Yazılımın ana amacıysa Monero madenciliği yapmaktı. PostgreSQL, araştırmacıların MySQL'den daha karmaşık olduğunu düşündüğü ve yaygın olarak kullanılan açık kaynak veritabanı olarak biliniyor.

Imperva'daki araştırmacıları ortak veritabanı saldırılarını, bilgisayar korsanları tarafından kullanılan araçları ve yöntemleri, veritabanına nasıl eriştiklerini ve ne yaptıklarını öğrenmek için bu veritabanını kullandı. Standart bilgi toplama adımlarını takip ederken olağandışı bir olay gözlemlendi. Saldırganlar, bir web sitesinden Scarlett Johansson'a ait bir görüntü indirmişti ve dosyanın içinde gizlenmiş ikili veri yükü söz konusuydu.

Imperva'daki araştırmacılar ayrıca saldırganların sunucuda komutlarını yürütmek üzere PostgreSQL ile etkileşime geçebilmek için gelişmiş veya değiştirilmiş bir Metasploit modülü kullandıklarını gözlemledi. Araştırmacılar, saldırganın sistem komutlarını yürütme yetkisini kazandığı an, belirli bir cihazda kripto para birimi madenciliği planı için sunucunun CPU'sunu ve GPU'sunu belirlemek üzere çalıştıklarını belirtti. Son olarak, cihaza Monero madenciliği programı kurulduğu gözlemlendi. Şu ana kadar saldırganların 312 Monero topladığı biliniyor. Bu da saldırganların birden fazla sunucuyu ele geçirdiğini

https://medium.com/@Eurasianews/monero-xmr-madencili%C4%9Fi-ile-g%C3%BCnl%C3%BCk-10usd-kazanabilirsiniz-53c147f7e4c3

9 ŞUBAT 2020

İnanılmaz ama gerçek: Bilgisiyarınızdan ekran parlaklık ayarları değiştirilerek veri çalınabilir

Mordechai Guri

Uzun yıllardır siber güvenlik uzmanları, internet bağlantısı olmayan güvenliksiz yerel ağlardan fiziksel olarak izole edilmiş hava boşluğuna alınmış (air-gapped) cihazlardan veri almak için çeşitli çalışmalar yürütüyor.

Air-gapped cihaz hackleme denince akla gelen isimlerin başında İsrail ben Gurion Üniversitesi Siber Güvenlik Araştırma Merkezinde çalışan Mordechai Guri geliyor.

Guri ve arkadaşlarının yaptığı son araştırma, hava boşluğundaki bilgisayarlardan herhangi bir network bağlantısına gerek kalmadan ve cihazla fiziksel bir temas sağlamadan hassas bilgi alınabileceğini gösterdi. Araştırmacıların yaptığı açıklamaya göre, cihazdan veri almayı sağlayan örtülü kanal tespit edilemiyor ve kullanıcı cihazda işlem yaparken bile fark ettirmeden veri çekmeyi başarıyor.

19 KASIM 2019

ABD devlet kurumları ağlarındaki 7 cihazın 4'ünden haberi yok(muş)

RPA Robotic progress automatisation concept illustration.

ABD'de Anayurt Güvenliği Bakanlığının uyguladığı CDM (Continuos Diagnostic and Mitigation) programı kamu kurumlarında siber güvenlikle ilgili ilginç bulguların çıkmasına neden oldu.

2013 yılında başlayan CDM programının amacı Amerikan devlet kurumlarına dijital ekosistemlerini görmeleri için kuş bakışı bir değerlendirme imkanı sunmak. Siber Güvenlik ve Altyapı Güvenliği Ajansı'nın yürüttüğü program, 'kullanıcılar, cihazlar, sistem ve kurumların ağındaki trafik ile ilgili net bilgi ve görüşe hakim olunursa, saldırılara karşı daha iyi savunma sağlanır' fikrine

17 EYLÜL 2019

Küçük şirketlerin neredeyse yarısı 2019'da veri sızıntısı yaşadı

Medyada büyük şirketlerin yaşadığı veri sızıntıları manşetlerde yerini alsa da, küçük işletmelerin bilgi güvenliği konusunda yaşadığı problemler hiç de küçümsenecek seviyede değil.

Bilgi güvenliği için yeterli kaynak ayıramamaları nedeniyle siber saldırganların öncelikli hedefleri arasında yer alan küçük şirketlerin üçte birinin veri sızıntısı tehlikesiyle karşı karşıya olduğu ortaya çıktı.

4 EYLÜL 2019

Stuxnet hakkındaki efsaneler son buldu: Nasıl bulaştırıldığı ortaya çıktı

İran'ın nükleer programını hedef alan Stuxnet saldırısı uzun yıllardır gizemini koruyordu. Bunca yıl karanlıkta kalan soru ise şu idi: ABD ve İsrail, zararlı yazılımlarını yüksek güvenlikli uranyum zenginleştirme tesisindeki bilgisayar sistemlerine yerleştirmeyi nasıl başardı?

Bu gizem geçtiğimiz günlerde Yahoo News'de Kim Zetter imzasıyla yayınlanan haberle çözülmüş oldu. Habere göre Hollanda istihbaratı için çalışan İranlı bir köstebek, ABD ve İsrail'in Stuxnet virüsünü İran'ın Natantz'daki nükleer tesisindeki santrifüjlere bulaştırılmasını sağladı. Santrifüj, uranyum zenginleştirmede kritik öneme sahip bir laboratuvar cihazı.

17 EYLÜL 2018

Hedef: 10 bin üniversite öğrencisine siber güvenlik dersi

SysSec adlı konsoryumun girişimi ve üniversitelerin katkısı ile on bin üniversite öğrencisine siber güvenlikle ilgili ders verilmeye başlandı.

Bu program ile on bin üniversite öğrencisine yazılım zafiyetleri ve güvenli programlamanın temel kavramlarını anlatılması ile siber güvenliği geliştirilmesi hedefleniyor.

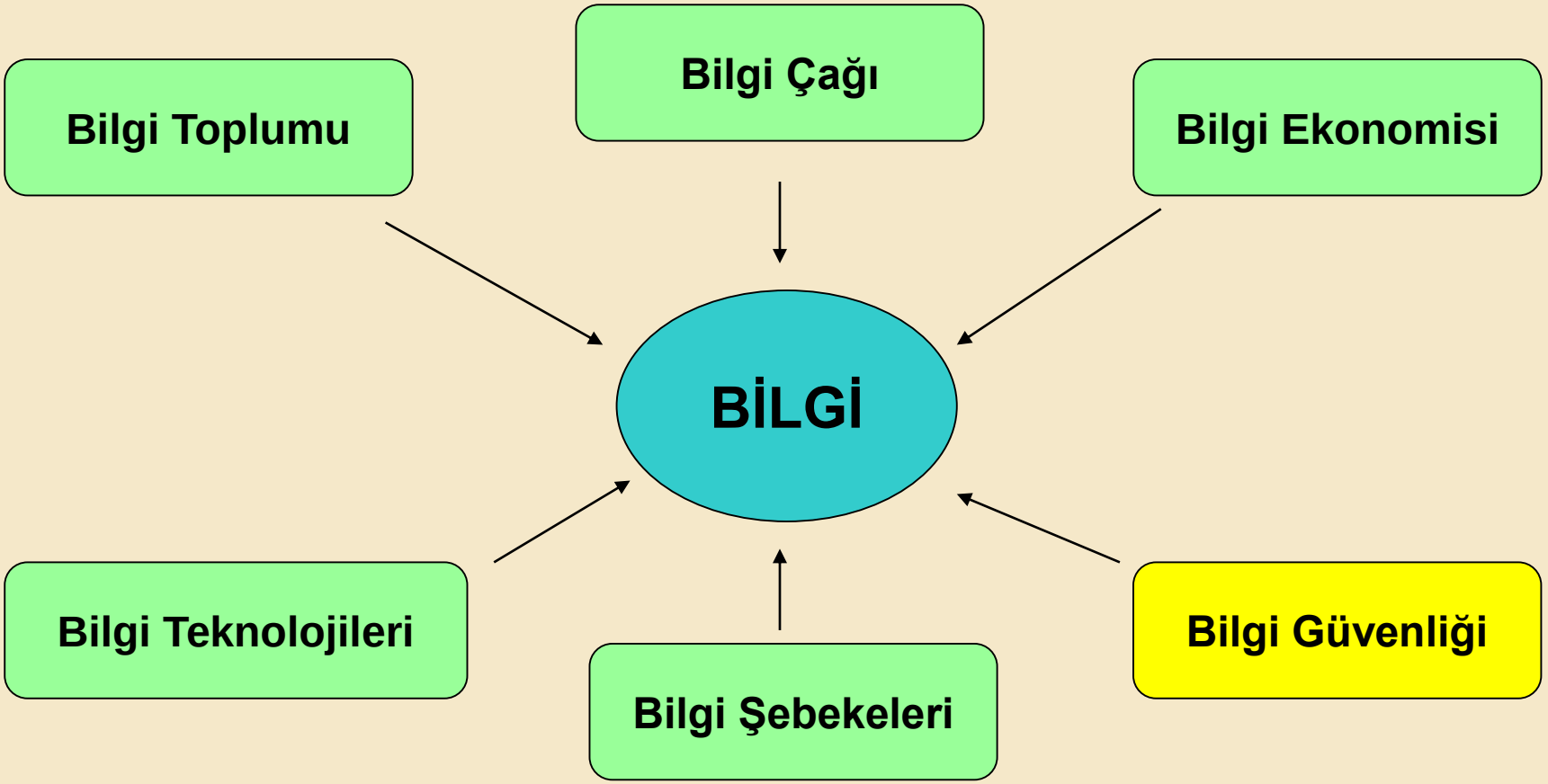
Konsoryumun internet sitesindeki açıklamada, "Bu program öğrenciler, güvenliğin bir bilişim sisteminin kurulmasındaki her aşamada gerekli olduğu, geliştirmenin son halkasında ekleyecekleri bir şey olmadığını öğrenmektir," denildi.

Şimdiye kadar dört binden fazla öğrenci bu derslerden yararlanmış durumda. Programa Pakistan'dan Amerika'ya kadar çeşitli üniversiteler ders programları ile katkı veriyor. Türkiye'den katılan üniversite ile bulunmuyor.

Proje kapsamında verilen dersler arasında bilgisayar güvenliği, donanım güvenliği, güvenli sistemler, kriptografik ve iletişim güvenliği, gelişmiş internet güvenliği gibi çeşitli dersler var.

Dersin Çerçevesi?

BİLGİ


Bilgi Çağı
Bilgi Toplumu
Bilgi Ekonomisi
BİLGİ
Bilgi Teknolojileri
Bilgi Şebekeleri
Bilgi Güvenliği

Bilgi nedir ?

Bilgi, kurumun en değerli varlığıdır. Korunması ve verimli kullanılması sağlanmalıdır.

Bulunduğu yerler;

- İnsanda (Sözlü)
- Kağıt üzerinde
- Bilgisayar sistemlerinde
- Fiziksel ortamlarda
- ...

Siber Uzay: Küresel Bir Alan

TÜRKİYEDE İNTERNET KULLANIMI

İnternette geçirilen günlük ortalama süre; Bilgisayarlarda **4,9 saat**, Mobil cihazlarda **1,9 saat.**

İnternet Kullanıcı Sayısı:

- **Dünyada→ 3 milyar 79 milyon**
- **Türkiye'de→ 46,2 milyon(18.)**

İnternet Kullanım Oranı:

- **Dünyada→ %42,4**
- **Türkiye'de→ %56,7**

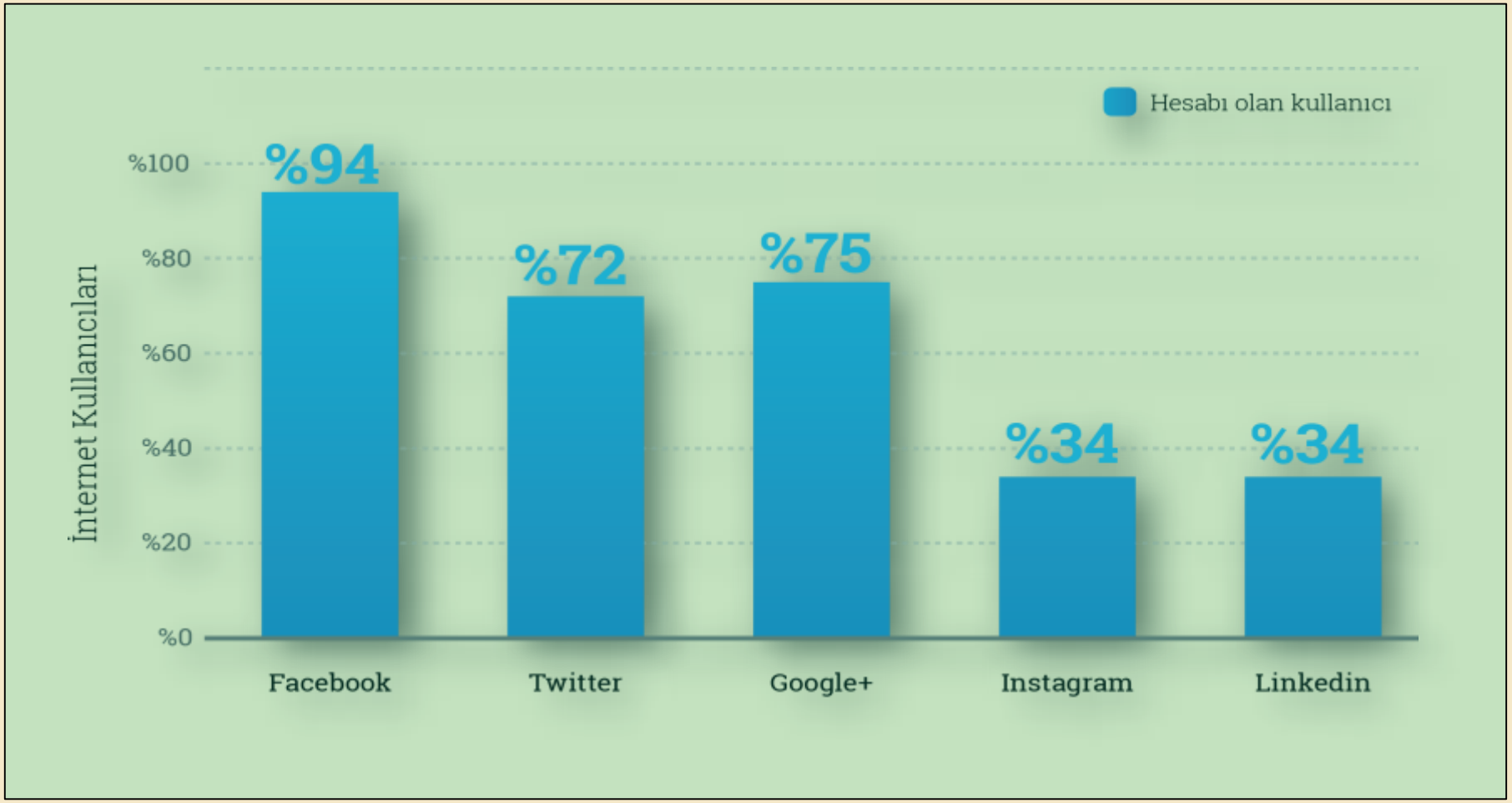
İnternet kullanım amaçları:

- **Sosyal Paylaşım→ %80,9**
- **Online haber→ %70,2**
- **Oyun, film, müzik→ %62,1**

Kaynak: TÜİK, Hanehalkı Bilişim Bilişim Tek. Kullanım Anketi

TÜRKİYEDE İNTERNET KULLANIMI

Türkiye'de Sosyal Medyada geçirilen **günlük ortalama** süre **2,5 saat**.



Kaynak: Global Digital Statistics

Yeni Eğilim: Sosyal Şebekeleşme

İnternet Faaliyetleri

* *Postalama,*
* *Bilgi Paylaşımı*
* *Tartışma Platformları*
* *Telefon açma,*
* *Alışveriş yapma,*
* *Pazarlama*
* *Bankacılık,*
* *Müzik ve Oyun*

Sosyal Medya

* *Youtube*
* *Facebook*
* *Twitter*
* *Skype*
* *RSS*
* *Google*
* *Talk*
* *Blog*
* *Linkedin*

Siber Uzaya Artan Bağımlılık

- Ülkelerin altyapı sistemlerinin siber uzaya bağımlı hale gelmesi ile;
  - -bireyler
  - -kurumlar
  - -devletler

  siber tehditlere açık hale gelmektedir.

Siber Tehditler

- **Siber Suçlar**
- **Siber Terörizm**
- **Devlet Destekli Siber Saldırılar**

1. e-li ve m-li ortamlar yaygınlaşıyor..
2. Uygulamalar artıyor..
3. Tehdit, tehlikeler, saldırılar artıyor..
4. Yeni çözümler geliştiriliyor..
5. Bilinmesi gerekenler çoğalıyor..
6. Yapılacak ve kontrol edilecek parametreler sürekli artıyor.

- ***Saldıran Taraf***
- *Saldırılar artmakta saldırı bilgi seviyesi hızla azalmakta*
- *Kötücül kodlar gelişerek ve değişerek hızla yayılmakta*
- *Organize olarak sanal suç örgütlerini kurma*
- *İyilerden hep bir adım önde*

- ***Savunan Taraf***
- *Güvenliğiniz en zayıf halkanız kadardır.*
- *%99,9 Korunma + %0,1 Korunmasızlık = %100 güvensizlik*
- *Bilgisizlik, ilgisizlik, hafife alma*
- *Korunma maliyetleri (Yatırım, Eğitim)*
- *Kişilere güven duygusu*
- *E-dünyanın doğasında olan güvensizlik*

SALDIRILAR

- *Saldırılar artık kapsamlı*
- *Çoklu saldırılar popüler*
- *Senaryoları yazılmış ve denenmiş,*
- *Karma yapıları içeriyor..*
- *Bilinmeyenler /düşünülmeyenler..*
- *Sürekli yenilikler içeriyor..*
- *Takip gerektiriyor..*
- *Yüksek bilgi birikimi gerektiriyor..*

SALDIRILAR

- *Casus yazılım sayısı artıyor.*
- *Farklılaşıyorlar.*
- *Kendilerini saklayabiliyorlar, görünmez olabiliyorlar.*
- *Silseniz bile tekrar kopyalayabiliyorlar*
- *Belirli bir süre var olup sonra kendilerini yok edebiliyorlar.*
- *38 grupta sınıflandırılıyorlar.*

GELİŞMELER NE YÖNDE?

- *Standartlar daha da spesifik.*
- *Kritik yapıların güvenliği mercek altında..*
- *Yeni çözümler kullanılıyor (Diyot Yaklaşımı)*
- *Kısıtlı kullanım sunan işletim sistemleri (JeOS)*
- *"Şifre (password)" yerini "Deyim veya Cümle Şifre (Pass-sentence)"..*
- *Sıfır gün / saat yaklaşımı*
- *360 derece güvenlik.*
- *"Bilgi Güçtür!" yerine "Bilgi Güvenliği Sağlandığı Ölçüde Güçtür!" "Bilgi üretmeden korunulamaz."*

WIKILEAKS

- *Dünyanın güvenlik açısından çok iyi dersler çıkaracağı en iyi örnek*
- *ABD'nin sanal savaş denemesi*
- *Kendisini/diğer ülkeleri nasıl etkileyecek*
- *Geliştirilen teknolojileri test etme*
- *Facebook ve Google gibi teknolojilerini ne kadar iyi kullanabiliyor testi*
- *İnternet ne kadar kontrol edebilir / edilemez..*

GOOGLE

- *Mükemmel bir arama motoru*
- *En çok tercih edilen arama motoru*
- *Mükemmel hizmetler veriyor*
- *Academics, books, translation, blogs, gmail, documents, mobil, talk, maps, IPv6, Google+, ……*
- *Değeri Milyar Dolarlarla ifade ediliyor*
- *FAKAT…*

GOOGLE devam

- *Dünyanın en iyi casus yazılım sistemi*
- *Dünyanın bilgisini topluyor..*
- *Ülkesine hizmet eden en iyi yazılımlardan birisi..*
- *Bizi bizden (ülkeleri, ülkelerden) daha iyi analiz edebiliyor..*
- *Kelime/Cümle/Resim/Ses araması yapabiliyor..*
- *İstihbarat için vazgeçilmez bir ortam..*
- *Tabii ki bu sistemi iyi kullananlar için..*
- *encrypted.google.com hizmette/idi???*
- *Güvenlik açığı oluşturabilecek hususları kapatıyor..*

SOSYAL AĞLAR

- *Kimlikleri Taklit Etme*
- *İstenmeyen E-postalar (Spam) ve Bot Saldırıları*
- *Kötü Amaçlı Sosyal Ağ Uygulamaları*
- *Siteler Arası Kod Çalıştırma (XSS) ve Siteler Arası İstek Sahteciliği (CSRF) Saldırıları*
- *Kimlik Hırsızlığı*
- *Casusluk*
- *Sahte Linkler/Bağlantılar*
- *Bilgi Toplama Saldırıları*

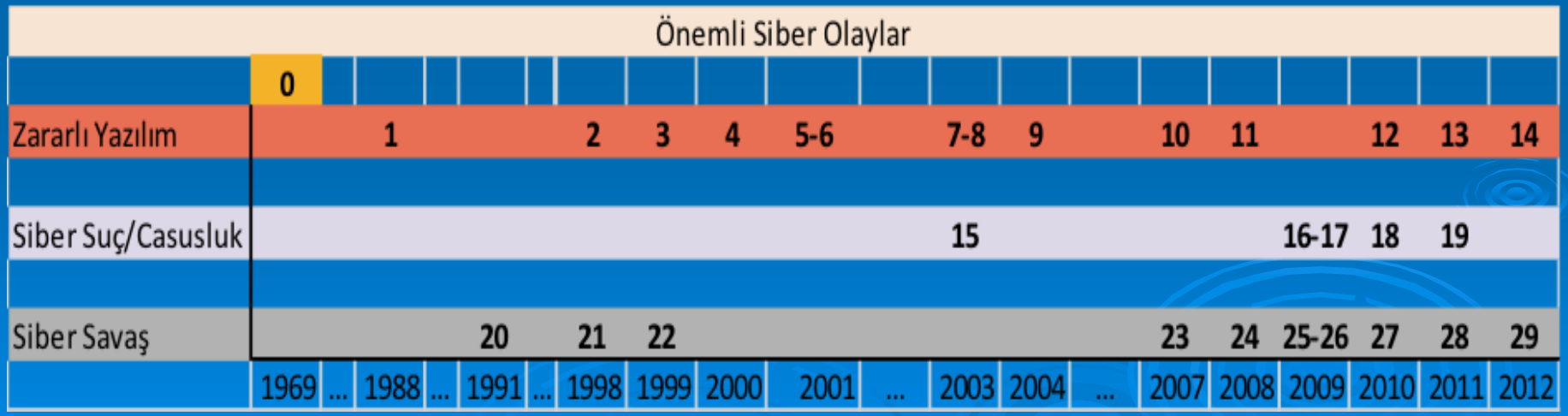
GÜNDEM KARIŞIK DEDİK

- ***Savaşlar internete kaydı..***
- *Ayyıldız TİM, Cyber Warrior, RedHack, Coldhacker*
- *Anonymous*
- ***LulzSec (ABD Senatosu),***
- *Estonya*
- *Gürcistan*
- ***Wikileaks***
- ***İyilerin ve Kötülerin amansız savaşı***
- *Saldıran Taraf*
- *Savunan Taraf*

Ne Saldırıyor ?

Siber Olay Çizelgesi

- **Zararlı Yazılımlar:** İnternet'in doğuşundan (**1 Ekim 1969**) beri milyarlarca yazılım geliştirilmiştir. Geliştirilen bu yazılımlar bir yarar sağlasın diye geliştirilirken bazıları da amaçları dışında kullanılarak var oldukları sistemlere/kullanıcılara zarar vermek için oluşturulmuştur. Bu yazılımlarından bazıları aşağıdaki gibidir:
- Morris Solucanı, Back Orifice, Melissa, I.love.You, Code Red, Nimda
- Blaster, Slammer, Sasser, Zeus, Conficker, stuxnet, duqu, flame

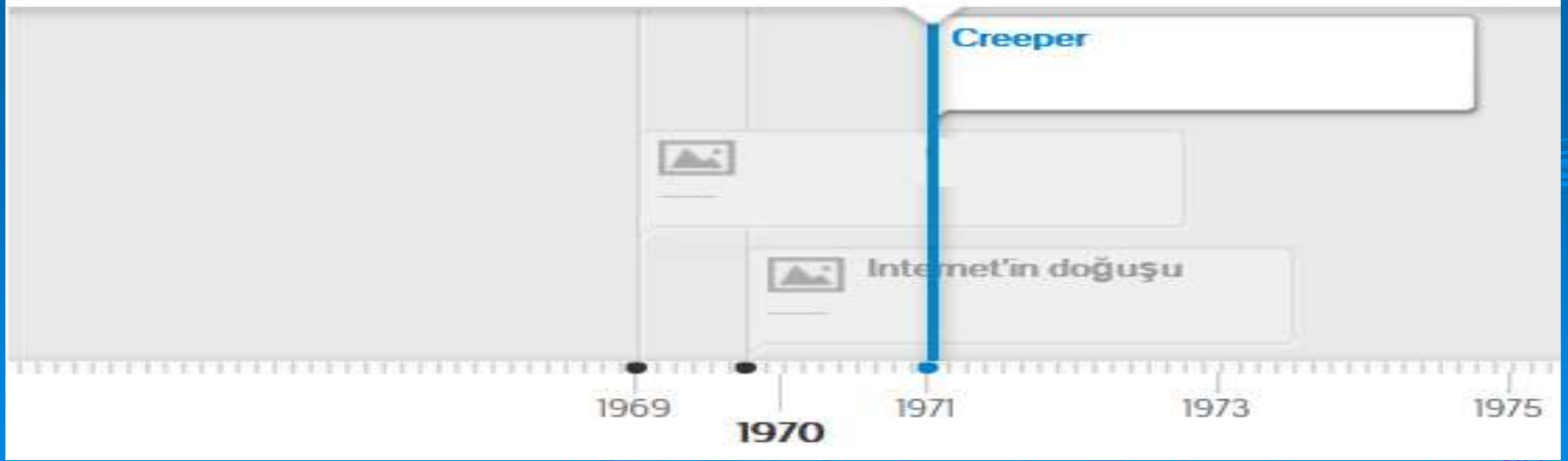


1 Ocak, 1971 — 1 Şubat, 1971

Creeper

İlk virus ortaya çıktı

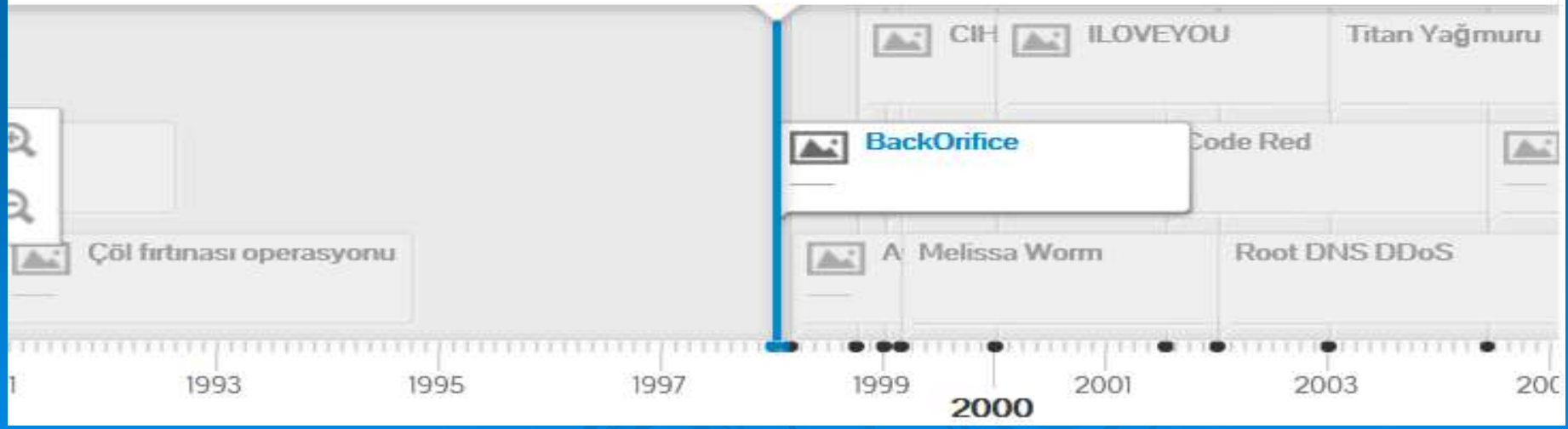
Kayıtlara ilk bilgisayar virüsü olarak geçen Creeper ARPANET'deki bilgisayarlara bulaşmıştır. Bulaştığı bilgisayara aslında pek de bir zararı olmayan Creeper; asıl zararı, programcıları virüs mantığıyla tanıştırarak vermiştir.
"I am Creeper catch me if you can"



1 Ocak, 1998 — 1 Mart, 1998

BackOrifice

Back Orifice (ya da kısaca BO) bilgisayarları uzaktan izinsiz bir şekilde yöneten zararlı yazılım yayınlandı



1 Ekim, 1998 — 1 Kasım, 1998

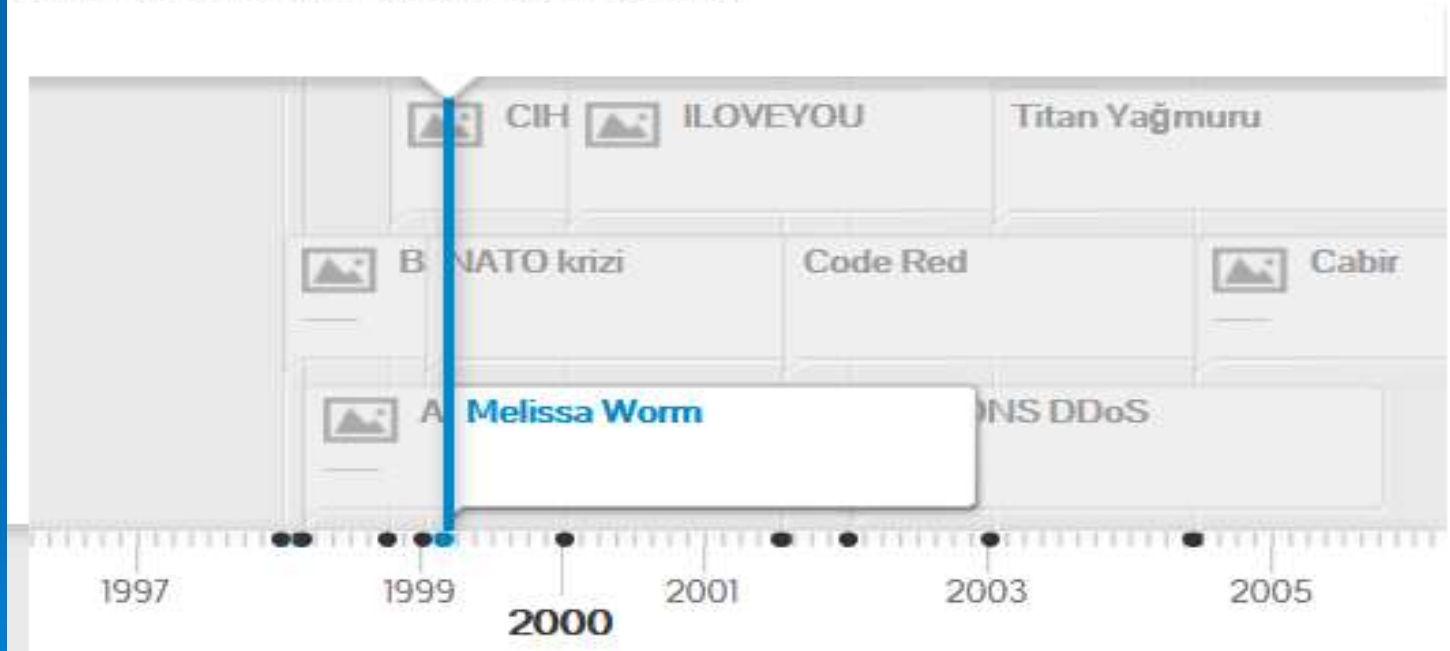
CIH - Cernobil virusu

Cernobil virusu ortaya çıktı 60 milyon bilgisayar etkilendi ve 1 milyar dolara yakın maddi zarara yol açtı

1 Mart, 1999 — 2 Mart, 1999

Melissa Worm

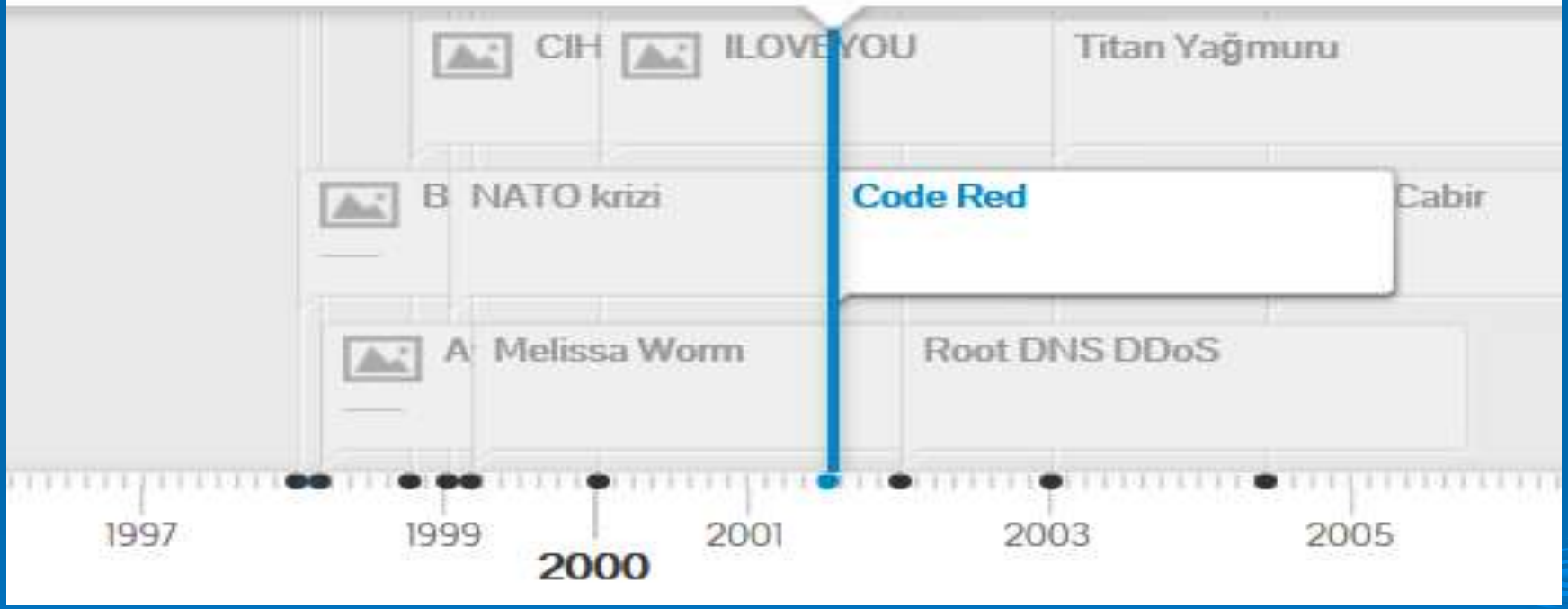
Microsoft Word makrolarını kullanan virüs sayesinde, sistemdeki dosyalar siliner-ek, bu dosyalar MS Outlook eposta istemcisindeki 50 kişiye gönderilip virüsün daha fazla yayılması sağlanıyordu



13 Temmuz, 2001 — 2 Şubat, 2001

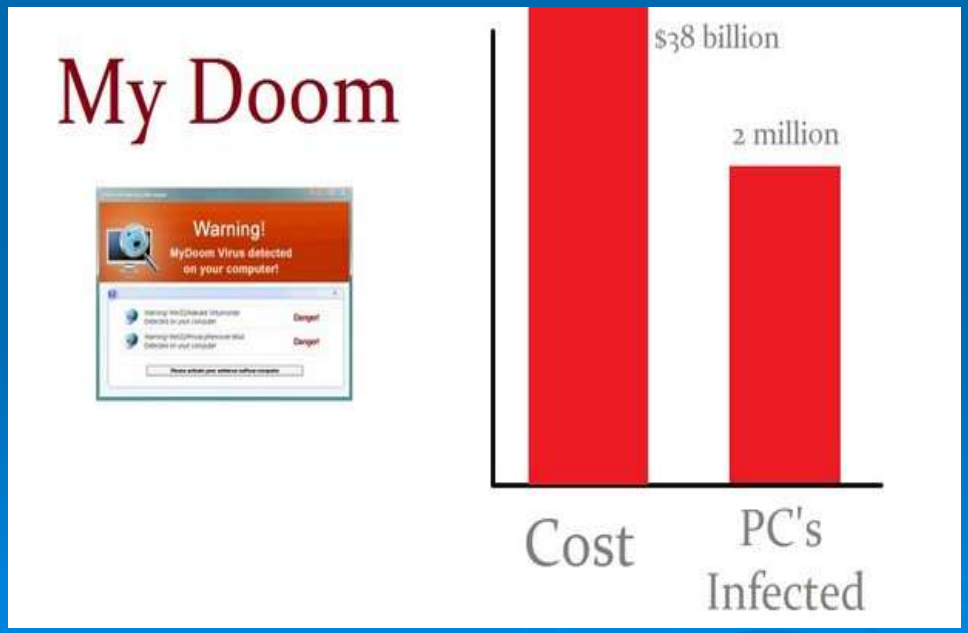
Code Red

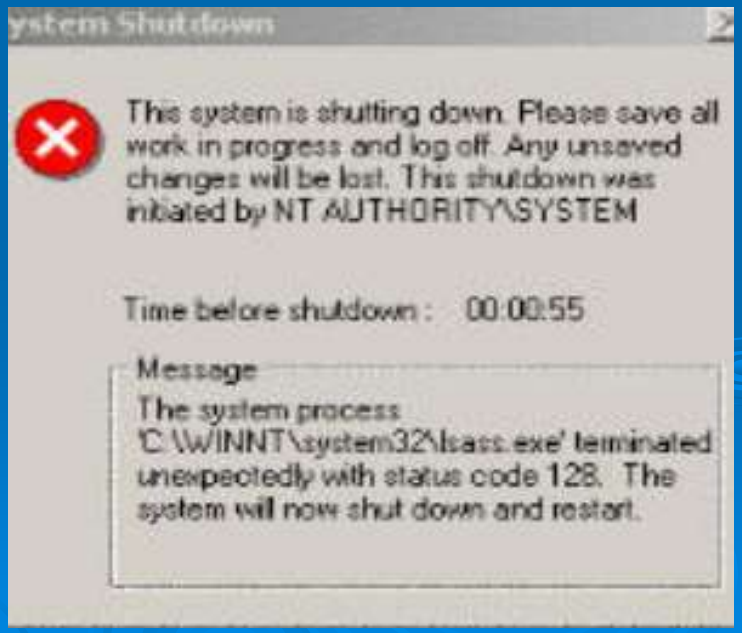
Microsoft IIS sunucuları hedef alan worm ortaya çıktı.



Yaklaşık 2.6 milyar dolar zarara neden olduğu sanılan ve aynı zamanda Bady ismiyle de bilinen Code Red, sistemlere maksimum seviyede zarar verilebilmesi için geliştirilmişti. Bu virüsün gazabına uğrayan sunucunun etkisinde kalan web sayfalarında ise şu mesaj görüntüleniyordu: "HELLO! Welcome to http://www.worm.com! Hacked by Chinese!".

Mydoom tarihin gördüğü **en tehlikeli** zararlı yazılımlardan biriydi. 2004 yılında ortaya çıkan Mydoom bulaştığı bilgisayardan özür dileyen ilginç bir yapıya sahipti. Kimin tarafından yazıldığı asla belirlenmeyen **virüs** çıktığı dönemdeki dünya e-posta trafiğini felç etmişti

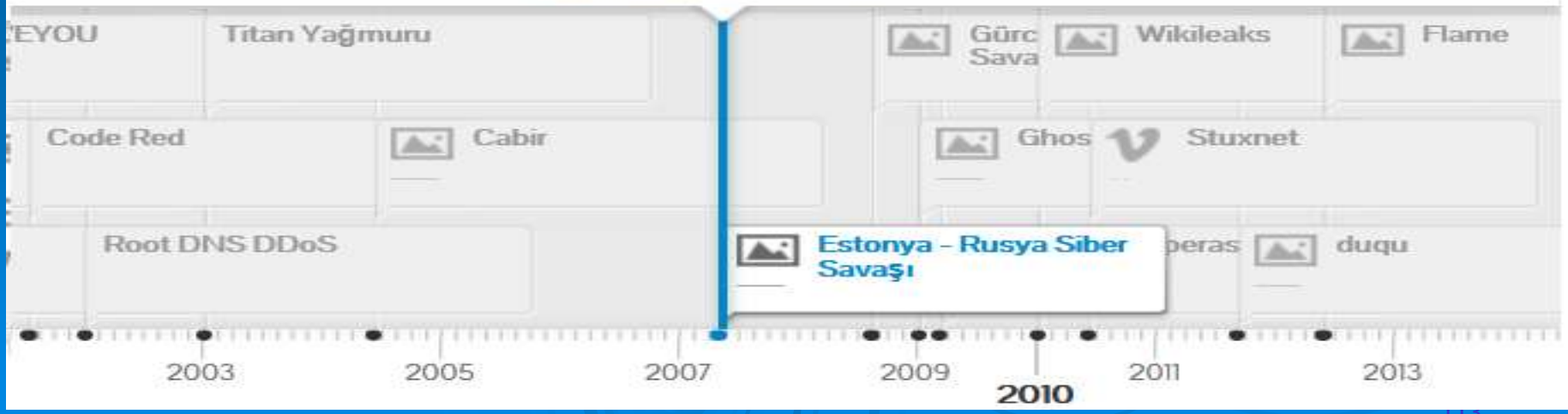




27 Nisan, 2007 — 18 Mayıs, 2007

Estonya - Rusya Siber Savaşı

İkinci Dünya Savaşı sonrasında Sovyetler Birliği tarafından Estonya'nın Nazi istilasından korunmasının temsili için dikilen Bronz Asker Anıtı'nın 26 Nisan 2007'de Estonya tarafından kaldırılması Rusya tarafından kınandı. Daha sonra Rusya kaynaklı siber saldırılar başlamış oldu. Devlet sitelerini Hedef alan çeşitli siber saldırılar düzenlendi.



1 Ocak, 2010 — 2 Şubat, 2010

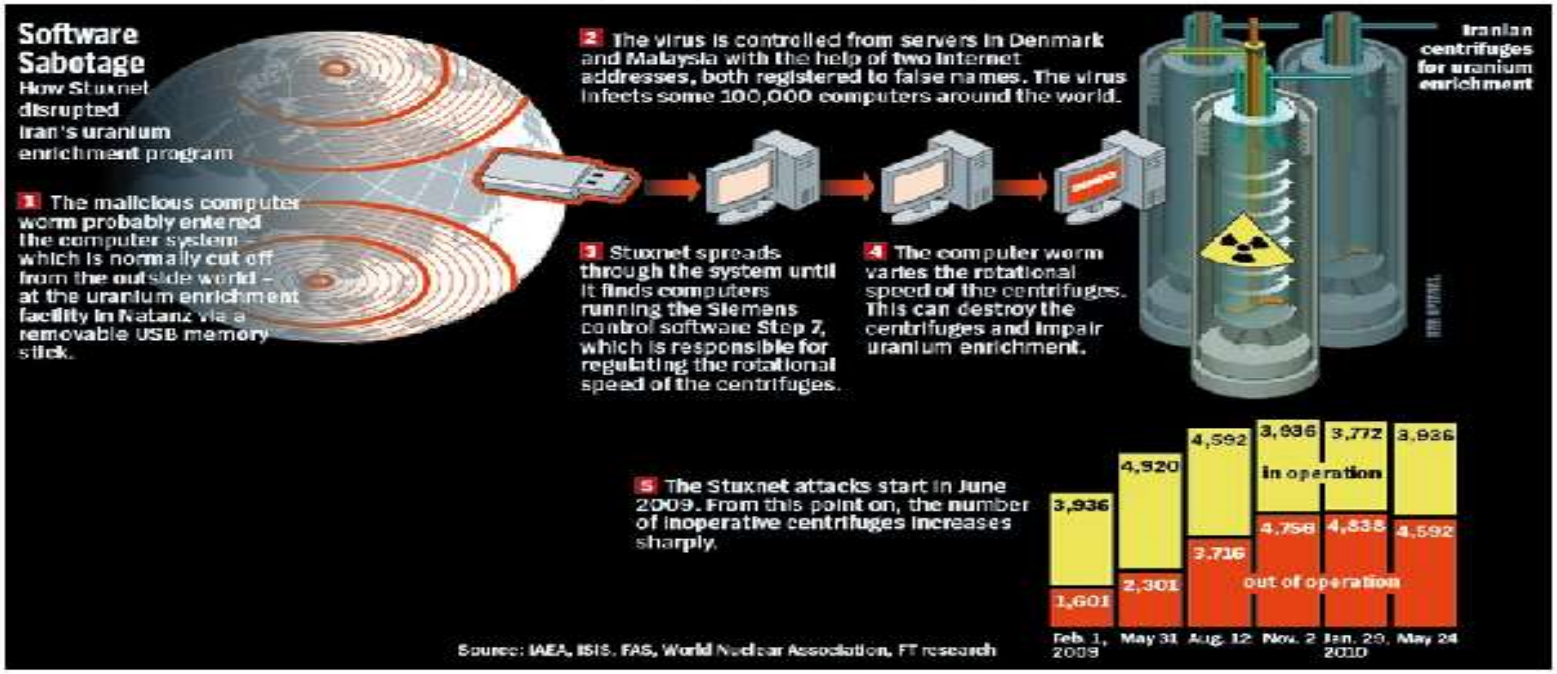
Wikileaks

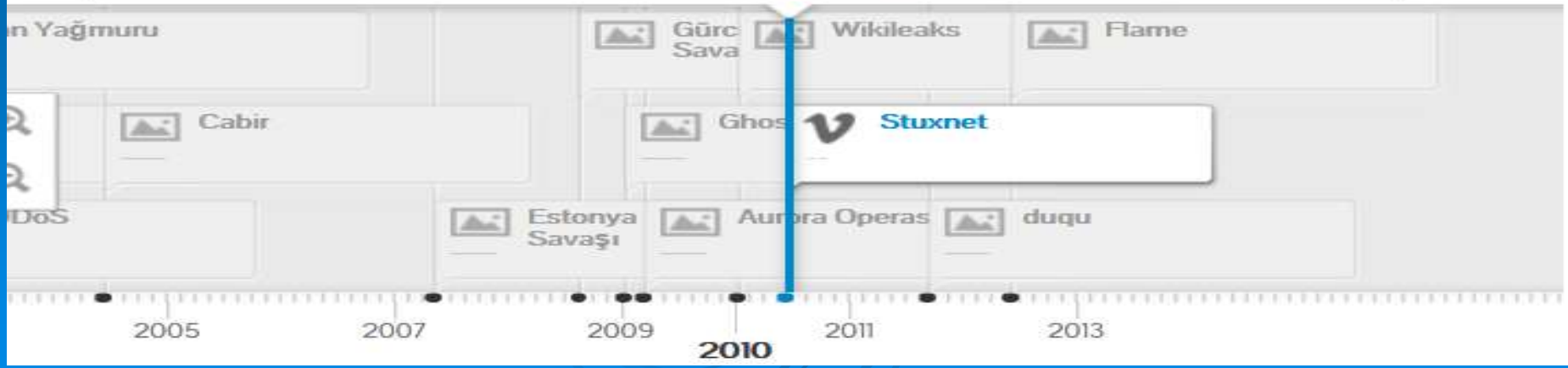
Amerikan büyükelçiliklerince 1968-2010 yılları arasında yapılan yaklaşık 250.000 yazışmanın internete sızdırılması ve bunun duyurulmasını engellemek için Wikileaks sitesine karşı DoS (servis dışı bırakma) saldırıları ile gündem bir anda değişmiştir. Anonymous adlı haktivist grup ise Wikileaks'e destek verme amaçlı olarak Mastercard, Paypal, Visa ve çeşitli devlet kurumlarının sitelerini hedef alan karşı bir saldırı başlattığını duyurmuş ve gönüllü olarak herkesin bu saldırıları desteklemesini istemiştir.

1 Haziran, 2010

Stuxnet

İran'ın Uranyum zenginleştirme faaliyetlerini sekteye uğratmak için oluşturulmuş Natanz nükleer santralindeki SCADA sistemleri hedef alan siber sabotaj faaliyetlerini gerçekleştiren zararlı yazılım





Araştırmalar & Veri

- *Britanya'da siber saldırıların ülke ekonomisine maliyeti 27 milyar pound'u buldu.*
- *Yılda 100 binden fazla siber saldırının yaşandığı ABD'de ise bu rakam tahmini olarak 100 milyar dolar civarında.*
- ***I Love You** virüsü dünya çapında yaklaşık 45 milyon bilgisayara bulaşmış ve yaklaşık **10 milyar USD'lik** maddi kayba yol açmıştır.*
- ***Nimda** kurtçuğunun dünya çapında yaklaşık **3 milyar USD' lik,***
- ***Love Bug**'ın ise **10 milyar USD' lik** kayba yol açmıştır*
- ***MyDoom** adlı truva atının yol açtığı maddi zarar **4,8 milyar USD** civarında*

Kaynak: Schjølberg, S., Hubbard, Lemos, R., Hahn, R.W

YA HACKERLER !

1-Kevin Mitnick

Kevin Mitnick, "Tüm Hackerların Kralı" olarak biliniyor ve sıklıkla Darth Vader'a benzetiliyor. 80'lerin sonuna doğru ilk hacklerini gerçekleştiren Mitnick; zamanla Nokia, IBM ve sonunda ABD'nin askeri merkezi Pentagon'u hackledi. Elinden milyonlarca dolar geçti. 1995'te tutuklanana kadar FBI tarafından en uzun süre aranan hacker oldu. 4 yıl hapse çarptırıldı. Şu anda ABD için danışmanlık hizmeti veriyor.

2-Matthew Bevan & Richard Price

Bu iki İngiliz hacker, 1994'e Pentagon'un savaş simülasyonunu hackledi. ABD adına Kuzey Kore'ye mesajlar gönderen hackerlar, bu ülkenin de bazı çok gizli belgelerine ulaştılar. Bu, ABD hükümeti için çok büyük şoktu. Sonunda yakalandılar, ancak neredeyse bir nükleer savaş çıkartıyorlardı.

3-Anonymous

Anonymous, kim olduğu bilinmeyen ve anonim olduğu düşünülen bir hacker grubu. Vatikan'dan Çin'e, CIA'den FBI'a kadar birçok ülkeyi ve kurumu hackleyerek, hükümetlerin çevirdiği dolapları ve çok gizli bilgileri halka açıklıyorlar. Bu işi para karşılığı yapmasalar da, yaptıkları işlerin doğurduğu sonuçlar belki de parayla oynamaktan doğacak sonuçlardan daha etkili.

4-Astra

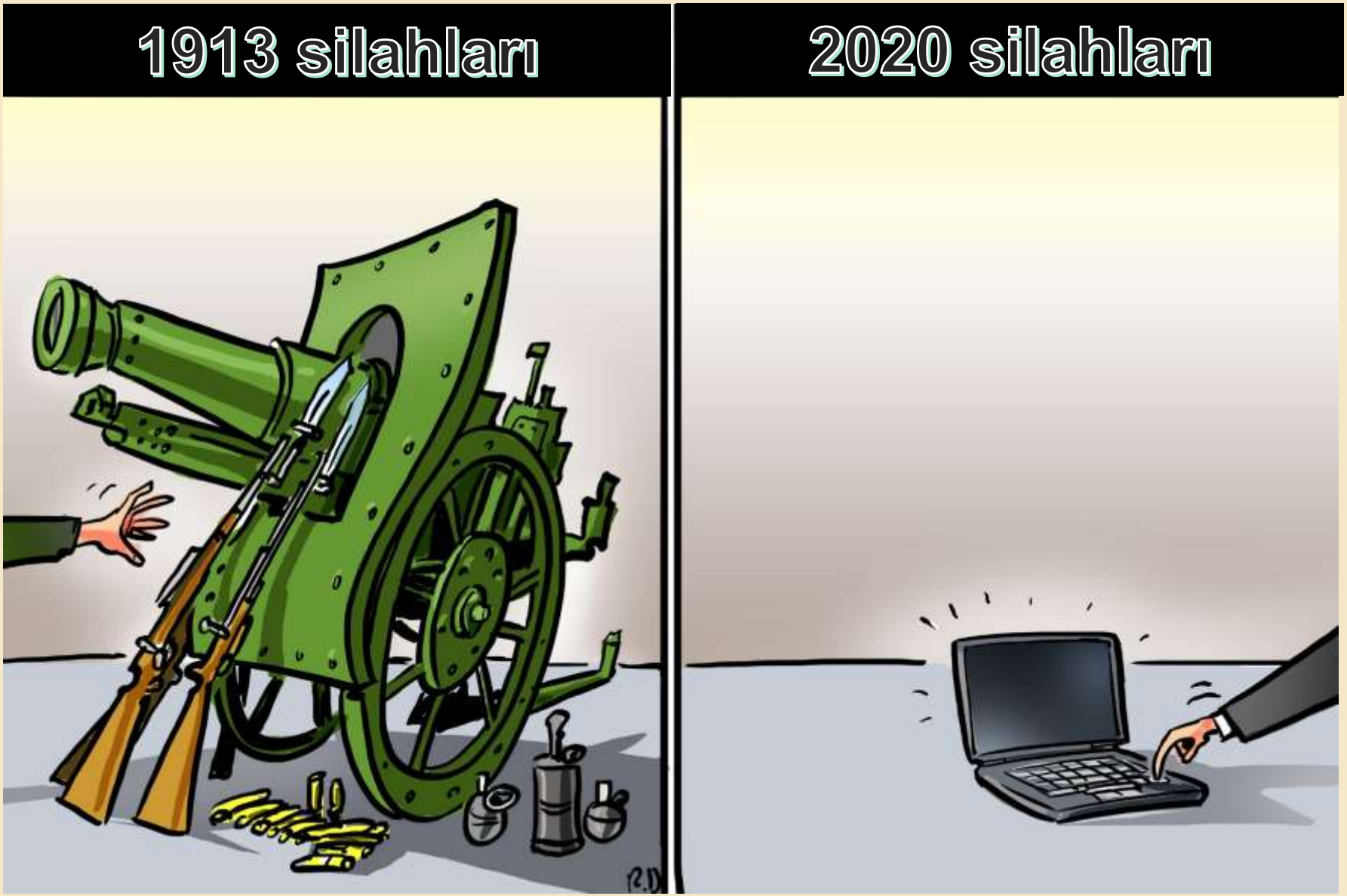
Astra, ismi açıklanmayan bir hacker. 2000'lerin başından sonuna dek yüksek silah teknolojisi bilgilerinden ileri yazılım projelerine dek birçok hackte bulundu ve bu değerli bilgileri diğer gizli servislere ve çıkar gruplarına sattı. 2008'de Yunan hükümeti tarafından tutuklandı, ancak ismi açıklanmadı. 58 yaşında bir matematikçi olduğu ve 8 yıl hapis yattığı söylentiler arasında. Verdiği zararın 360.000.000 dolar olduğu tahmin ediliyor.

5-Gary McKinnon

SOLO takma adıyla hacklemelerde bulunan Gary McKinnon, ABD ordusunu ve NASA'yı defalarca hackledi. Verdiği zarar 700.000 dolarlık bir harcama ile ancak kapatılabildi. Birçok önemli belgeyi kopyalayıp sildi. Yakalandıktan sonra soruşturmada McKinnon'un esas amacının para çalmak olmadığı ortaya çıktı. O, aslında uzaylıların varlığı hakkındaki bilgileri araştırıyordu. McKinnon, NASA ve ABD ordusunun serverlarında uzaylılarla ilgili binlerce dosya olduğunu ve uzaylıların gerçekten var olduklarını ileri sürüyor.

Uzayı keşfetmenin kaderi at arabasında

Çünkü roketlerin geleceği iki atın poposuna bağlı…


1913 silahları
2020 silahları

Nükleer Silah Tesisi

Siber Silah Tesisi


We have a responsibility to protect your information. If we can't, we don't deserve it.
The inside story of the revelations that shook the world
The Observer
Brexit insider claims Vote Leave team may have broken law

Sokaktan çevirdiğiniz herhangi birine Google'ın, Twitter'ın, Facebook'un ya da Instagram'ın neden ücretsiz olduğunu sorun. Çoğu kişi cevabı tam bilemese de reklam için diyecektir. Cevap doğru olsa da, olay boş bir alanda reklam göstermek kadar basit değil, keşke öyle olsaydı.

Noah Hariri bunun adına Dataizm diyor... Bilgiye sahip olanlar yönetecek dünyayı... Dijital imparatorluklar oluşacak.

Hayatta en pahalı şey bedavadır…

Artık çok geç. Facebook yaklaşık 10 beğeni veya paylaşımdan sonra sizi çevrenizde ki insanlardan daha iyi tanıyor.

Bu sosyal ağlar, hiç biri bize sunulan hikayelerde ki gibi masum değil.

- ***EN TEMEL AMACLARI İSTİHBARAT***
- ***TOPLUMUN EĞİLİMİNİ ÖĞRENME***
- ***BU EĞİLİM İLE YÖNLENDİRME YAPMA***
- ***YENİ DEĞERLER VE YAŞAM BİÇİMİ OLUŞTURMA.***

ROBOTLAŞMIŞ BİREYLER

Biyometrik verilerle birlikte, "davranışsal biyometri" verileri kullanılıyor. Mesela klavyede her bir tuşa vuruş arasında geçen süre, vuruş kuvveti, ekranın hangi noktadan kaydırıldığı, nasıl zoom yapıldığı, telefonu tutuş açısı gibi parametreler kişiyi tanımlamak için kullanılıyor.

Hareket sensörü ile de, o kişinin kendisine özel yürüyüş ritmi ve karakteristiği saptanabiliyor. O kişi güvenlik gerekçesi ile bir başkasının telefonunu kullansa, telefonda yine bir başkasının hesabı yüklü olsa bile birkaç adım sonra telefonu gerçekte kimin kullandığı biliniyor

Acxiom, Epsilon, RapLeaf, Flurry, BlueKai...

Bunlar muhtemelen çoğunuzun ismini duymadığı şirketler. Yüz milyarlarca dolarlık gözetleme sektörünün arkasındaki bu veri simsarlarının yaptığı iş, verilerimizi toplamak, analiz etmek ve reklamcılara ya da pazarlamacılara satmak

Hangi veriyi topluyorlar derseniz, bir kişiye dair ulaşabildikleri ne kadar veri varsa hepsini.

Bu veriyi kişilerin online aktivitelerinden bankalara, kredi kartı hareketlerinden kullandıkları mobil operatörlere ya da üye oldukları yerlere kadar pek çok yerden topluyorlar.

Bu firmalardan mesela Axxxx'un arşivinde, tüm dünyadan 700 milyondan fazla kişinin bilgisi var ve her kişiye 13 haneli bir kod atanmış durumda. Bu kodlar, her biri farklı bir profil içeren 70 kümeden birine atanıyor ve kişi o profille tanımlanıyor.

Mesela 56 nolu kümedekiler;

“30-35 yaş aralığında, üniversite mezunu, boşanmış, 1 ya da 2 çocuğu olan, orta düzey geliri olan, kirada oturan erkekler” gibi. Firma bu bilgileri olduğu gibi satabiliyor ya da kategoriyi daha da daraltmak için başka bir firmaya verebiliyor.

Bu durumda diğer firma, aldığı bilgilere ek olarak;

“kamuda çalışanlar”, “babası sağ olanlar”, “şu lokasyonda oturanlar” ya da “alkole düşkün olanlar” gibi daha da detaya inebiliyor. Bazı firmalarsa bu kümelerle ilgili çok daha derin detaylara ve özel bilgilere inebiliyor

Bir başka örnek;

Mesela “kanser hastası olanlar”, “HIV virüsü taşıyanlar”, “X ameliyatı olanlar” ya da “cinsel saldırıya uğrayanlar” gibi. Büyük veri simsarlarından MxxxxE200 isimli şirket, bu bilgileri çok ucuz bir fiyata (1000 kişi için 79$) isteyen ilaç firmalarına satıyor.

Facebook-Cambridge Analytica (CA) skandalı.

CA da veri simsarlarından veriyi alıp işleyen şirketlerden biri…

Veri simsarlarının topladığı verinin önemli bir kısmı, bedava diye düşünüp telefona kurduğumuz uygulamalardan geliyor. Mesela Angry Birds, Candy Crush, Fruit Ninja gibi ücretsiz popüler oyunlar neden sizden lokasyona ve temel bilgilere erişim izni ister?

Milyonlarca kişinin oynadığı bu oyunları yazan firmalar, nasıl para kazanıyor? Ya da neden Google, yıllarca üzerinde çalıştığı onlarca uygulamayı hiç para almadan herkese bedava dağıtıyor? Peki ya Twitter, Facebook, Instagram, Snapchat ve diğer uygulamalar?

Girdiğiniz bir sitede, Facebook'un o meşhur "beğen" tuşunun olması yeterli, hesabınızın olup olmaması, o tuşa basıp basmamanız önemli değil, kayıt altındasınız. Hatta o sitede "beğen" tuşu da olmayabilir, veri simsarları vasıtasıyla ne yaptığınızı yine takip ediyor.

Benzer şekilde Google'ın Gmail'ini de kullanmıyorum diyebilirsiniz, ancak yine bir şey fark etmiyor. Eğer Gmail hesabı olan birine mail attıysanız, bu Google'ın sizin hesabınızı mercek altına alması için yeterli, çünkü Gmail lisans anlaşmasına göre Google'ın buna hakkı var.

Google, hem kendi ürünleri (Gmail, Google Docs, Google Drive, Haritalar), hem satın aldığı firmalar (Youtube gibi), hem de veri simsarları vasıtasıyla bizi bizden daha iyi tanıyor. Google'ın CEO'su şöyle demişti: "Şu an nerede olduğunuzu ve az çok ne düşündüğünüzü biliyoruz"

1997/8 yılında Echolon kuruldu CIA tarafından daha Google yoktu ortada yine aynı CIA 1970'lerin sonu 1980'lerin başında herhangi bir ofis bahçesine bakır bir çubuk saplayarak uzaktaki bir odada bulunan bilgisayar monitördeki görüntüyü filtreleyebiliyordu şuan 2019…

BİRAZ AYRINTI

Siber Suçlar

- Siber suçlar:

-bilgisayarın konusunu, vasıtasını, simgesini oluşturduğu suç olgusu içeren fiiller

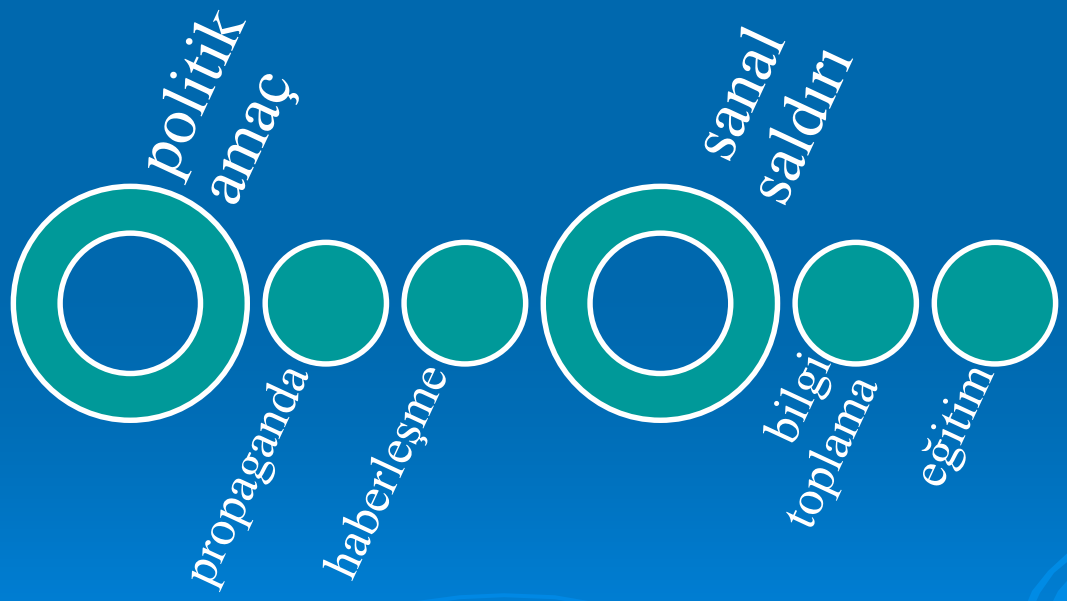
-bilişim sistemleri aracılığıyla işlenen suçlar

Siber Suçlar

- Avrupa Konseyi Siber Suçlar Sözleşmesi'ne göre siber suçlar:
  - -bilgisayar veri sistemlerinin gizliliğinin ihlali
  - -bilgisayar üzerinden sahtekarlık ve dolandırıcılık
  - -çocuk pornografisi
  - -telif hakları ile ilgili suçlar

Siber Terörizm

- Siber terörizm, belirli bir politik amaca ulaşabilmek için bilgisayar sistemleri aracılığıyla gerçekleştirilen eylemlerdir.



Siber Terörizm

- Olası siber terör saldırıları:

-haberleşme, ulaşım, su, elektrik, ve doğalgaz sistemlerini çökertme

-baraj kapaklarını açma

-emniyetin, hastanelerim ve itfaiyelerin çalışmasını engelleme

-hükümet kurumlarını çalışamaz hale getirme

Siber Saldırı/Siber Savaş

- *Hedef seçilen şahıs, şirket, kurum, örgüt, gibi yapıların **bilgi sistemlerine** veya iletişim altyapılarına yapılan planlı ve koordineli saldırılara **'siber saldırı'** deniyor. Bunlar, ticari, politik veya askerî amaçlı olabiliyor.*

- *Aynı saldırıların ülke veya ülkelere yönelik yapılmasına ise **'siber savaş'** deniyor.*

- *Bu tanımlara göre, Anonymous isimli grubun Türkiye'deki bazı kurumlara yönelik eylemine siber saldırı, Wikileakes'in yaptığına ise siber savaş demek mümkün.*

Devlet Destekli Siber Saldırılar

- 2010'da İran'ın nükleer programına yönelik Stuxnet virüsü ile bir saldırı gerçekleştirilmiştir.

- 2007'de Estonya hükümetine ve medyasına yönelik, 2008'de Gürcistan'a yönelik siber saldırı yapılmıştır.

Devlet Destekli Siber Saldırılar

- Siber savaşlar, ülkelerin güvenlik stratejilerinde yer almaya başlamıştır.
- Devletler, siber kuvvetler tesis etmeye yönelmiştir.
- ABD, 2009'da Siber Savaş Komutanlığı'nı kurmuştur.
- Çin, 2050 yılına kadar elektronik egemenliği hedeflemektedir ve bu kapsamda bir *siber doktrin* geliştirmiştir.

Devlet Destekli Siber Saldırılar

- Yakın gelecekte devletlerarası mücadele siber alanda yoğunlaşacaktır.
- Bilgi ve bilişim sistemlerinin güvenliği ulusal ve uluslararası güvenliğin bir parçası haline gelmektedir.

Siber Savaş

Siber savaşın temelleri Soğuk Savaş döneminde atılmıştır.

* Teknoloji bu süreci hızlandırmıştır.
* ABD, Rusya, Çin, İsrail ve İngiltere gibi ülkeler;
  - Savunma ve Saldırı timlerini oluşturuyor.
  - Ayrıca **taşeron hacker**lar da kullanıyorlar.

21. yüzyıl teknolojileri dünyanın geleceğine şekil veriyor;

Teknolojinin ulaştığı nokta artık onun doğrudan bir silah olarak da kullanabileceğini göstermekte.

Siber Savaş

CIA Başkanı Leon Panetta,

"İnternet üzerinden, hükümet birimlerimize saldıranlara karşı en ufak bir tahammül göstermeyeceğiz. Savunmamız da karşı saldırılarımız da en sert biçimde gerçekleşecek. ***Soğuk Savaş bitti ama teknoloji savaşları başladı."***

Eski ABD Savunma Bakanı Albright;

"Siber saldırılar NATO ya karşı 3 tehditten biri olarak kabul edilecektir."

Siber Savaş

* Casusluk
* Manipülasyon
* Propaganda
* İletişim
* Virüs
* Truva atları
* Sistem bozma
* Siber bombalarla sabotaj
* Bilgi kirliliği
* Sistem kilitleme
* Dolandırıcılık

Siber Savaşın Hedefleri

Dünyada ilk defa enformasyon savaşları deyimini kullanan insan olan **John Arquilla,** günümüz teknolojisiyle kitlesel ölçekte yıkıcı eylemlerin gerçekleştirilebileceğinin bilindiğini, ancak Stuxnetle birlikte sadece enformatik değil fiziki tahribatın da verilebileceğinin anlaşıldığını söylemektedir.

Siber saldırılarla bir ülkenin trafik ışıklarından güç şebekelerine kara deniz hava yollarına kadar her şeyini felç etmek mümkündür.

AB'nin Siber Güvenlik Politikaları

- Avrupa Komisyonu, 2010'da Dijital Gündem'i uygulamaya koymuştur.
- Avrupa Siber Suçlar Merkezi 2013'te faaliyete geçmiştir.
- Avrupa Ağ ve Bilgi Güvenliği Ajansı'nın (ENISA) yetkileri artırılmıştır.
- 2011'de AB'nin ilk Bilgisayar Acil Müdahale Ekibi (CERT) kurulmuştur.

NATO'nunSiber Güvenlik Politikaları

NATO Güvenlik Ofisi'ne bağlı olarak Siber Saldırılarla Mücadele Birimi (CIPC) tesis edilmiştir.

Bükreş Zirvesi'nin (2008) ardından Siber Savunma Mükemmeliyet Merkezi kurulmuştur.

NATO'nun Siber Güvenlik Politikaları

- 2011'de İttifak'ın Savunma Bakanları, NATO Siber Savunma Politikası'nı onaylamıştır.
- Ancak, NATO'nun siber savunma politikasının İttifak'ın toplu savunma görevine uyarlanması (5. madde) konusundaki belirsizlik devam etmektedir.

Türkiye'de Siber Güvenlik

Türkiye Avrupa, Orta Doğu ve Afrika bölgelerinde kötü amaçlı yazılım saldırılarına maruz kalan 10 ülke arasında ???. sıradadır.

Bilim, Sanayi ve Teknoloji Bakanlığı, TÜBİTAK ve Bilgi Teknolojileri ve İletişim Kurumu siber güvenlik alanında faaliyetlerini artırmaktadır.

Türkiye'de Siber Güvenlik

e-Dönüşüm Türkiye Projesi kapsamında, TÜBİTAK'a Bilgisayar Olaylarına Müdahale Merkezi kurma görevi verilmiştir.

TÜBİTAK BİLGEM ve Bilgi Teknolojileri ve İletişim Kurumu koordinasyonunda Ocak 2011'de siber tatbikat gerçekleştirilmiştir.

2011'de Ulusal Siber Güvenlik Strateji Belgesi Çalıştayı düzenlenmiştir.

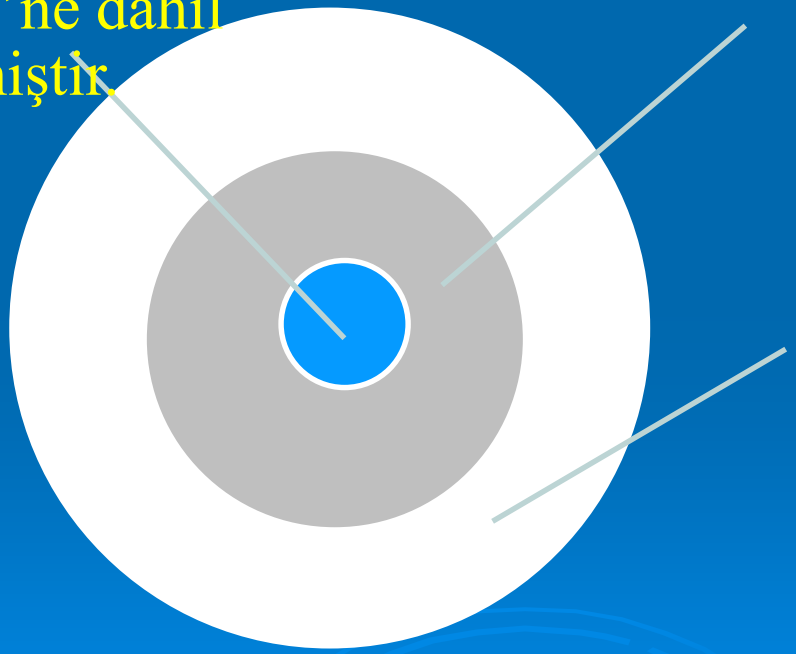
Türkiye'de Siber Güvenlik

- Bilişim suçları ile ilgili yasal mevzuat değiştirilmiştir.
- 5237 sayılı Türk Ceza Kanunu, 5651 sayılı internet ortamındaki yayınları düzenleyen kanun ve 5070 sayılı Elektronik İmza Kanunu'yla Türkiye'nin siber güvenlik hukukunun altyapısı oluşturulmuştur.

KVKK

Türkiye'de Siber Güvenlik

Siber terörizm Milli Güvenlik Siyaset Belgesi'ne dahil etmiştir.



Ancak henüz Türkiye, ulusal siber güvenlik strateji belgesini hazırlayamamıştır. Bu önemli bir eksikliktir.

Bir diğer eksiklik, siber güvenlikten sorumlu kurumları koordine edecek otoritenin olmayışıdır.

Kritik Altyapılar

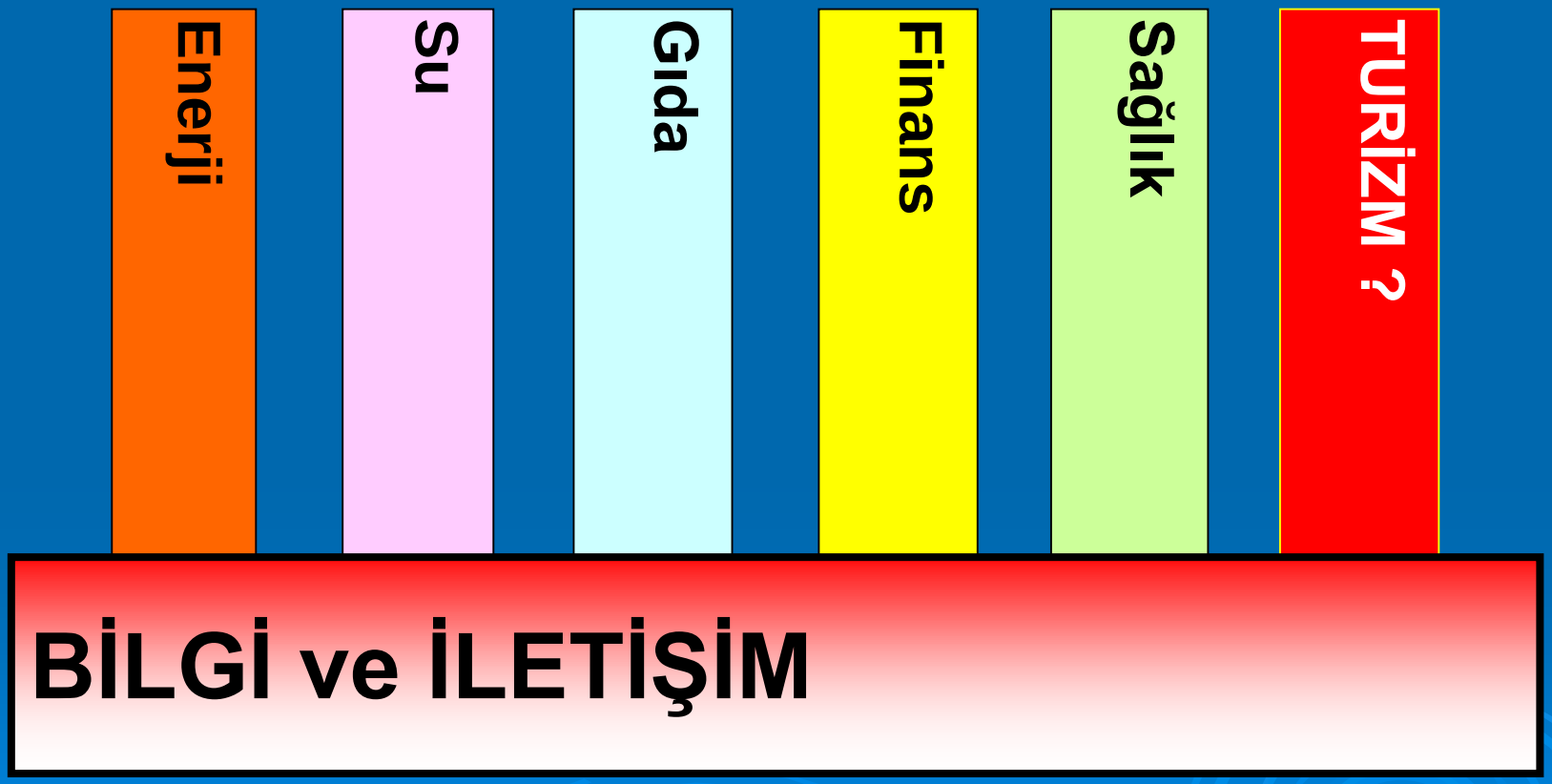
* Zarar görmesi veya yok olması halinde,

* Vatandaşların sağlığına, emniyetine, güvenliğine ve ekonomik refahına veya hükümetin etkin ve verimli işleyişine ciddi olumsuz etki edecek

* Fiziki ve bilgi teknolojileri tesisleri, şebekeler, hizmetler ve varlıklar

Kaynak: AB Komisyonu

Kritik Altyapılar



Kaynak: Canbay, C., Kritik Altyapıların Korunması, CEBIT

Siber Tehdit Araçları

- Hizmetin engellenmesi saldırıları (DoS, DDoS)
- Bilgisayar virüsleri
- Kurtçuk (worm)
- Truva atı (trojan)
- Klavye izleme (key logger) yazılımları
- İstem dışı ticari tanıtım (adware) yazılımları
- Casus / köstebek (spyware) yazılımlar
- Yemleme (phishing)
- İstem dışı elektronik posta (spam)
- Şebeke trafiğinin dinlenmesi (sniffing ve monitoring)

Siber Tehditlerin Amaçları

- Sisteme yetkisiz erişim
- Sistemin bozulması
- Hizmetlerin engellenmesi
- Bilgilerin değiştirilmesi
- Bilgilerin yok edilmesi
- Bilgilerin ifşa edilmesi
- Bilgilerin çalınması

TEHLİKE ORTADA PEKİ ÇÖZÜM NEDİR?

Bilgi Güvenliği?

"*Kurum, kuruluş ve kullanıcıların bilgi varlıklarını korumak amacıyla kullanılan yöntemler, politikalar, kavramlar, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulama deneyimleri ve kullanılan teknolojiler bütünü*" olarak tanımlanıyor.

Bilgi güvenliği nedir ?

Kurum un en değerli varlığı olan **Bilgi** nin kaybolmasını, zarara uğramasını, yok olmasını, yetkisiz ve kötü niyetli kişilerin eline geçmesini engellemektir.

- **Gizlilik** (Kim ?)
- **Bütünlük** (Ne ?, Hangi ?)
- **Erişilebilirlik** (Ne zaman?, Nasıl ?)

Bilgi güvenliği nedir ?

Gizlilik; Bilgi ye erişime izni olan yetkili kişiler yada sistemlerin erişmesini sağlamaktır.

Bütünlük; Bilgi nin yetkisiz kişi yada işlemler tarafından değiştirilmemesini sağlamaktır. Böylece Bilgi nin tutarlılığı sağlanmış olur.

Erişilebilirlik ; Bilgi ye doğru zamanda erişimin ve erişim sürekliliğinin sağlanmasıdır.

Bilgi Güvenliğinin Temel Hedefi?

Kurum ve kuruluşların bilgi varlıkları ve kaynaklarını hedeflenen amaçlar doğrultusunda organizasyon, insan, finans, teknik ve bilgi değerlerini dikkate alarak, varlıkların ve kaynakların başlarına **KÖTÜ BİR ŞEYLER GELMEDEN** korumaktır.

Bilgi güvenliği politikası ne işe yarar ?

- Personele, yaptıkları iş kadar, iş yapış yöntemlerinin ve işledikleri bilginin değerini farkettirir.
- Kurumu, bilgi kaybı nedeni ile uğrayacağı zarardan korur. Rekabetçi bir avantaj sağlar.
- Riskleri yönetilebilir kılar.
- Toplam kalitenin artmasına neden olur.

Bilgi Güvenliği Tanımı (ABD Başkanı Obama)

- **“Ülke olarak karşılaşılan çok ciddi ekonomik ve ulusal güvenlik sağlama hedeflerinden birisi olup hükümet veya ülke olarak henüz tam anlamıyla önlem alamadığımız bir hususdur.”**
- **“Amerika’nın sayısal altyapısını kapsamlı olarak güven altına alma yaklaşımlarının geliştirilmesi ve bilgi ile haberleşme altyapısının savunulmasına yönelik olarak federal çözümlerin gözden geçirilmesi” emrini verir.**
- ***"America's economic prosperity in the 21st century will depend on cyber security." May 2009***

Türkiye'de Tanımlar..

- *Ulaştırma Eski Bakanı Sn. Binali* Yıldırım
- "Bilgi güvenliğinde ortak akıl ve ortak hareketle hattı müdafaa yerine sathı müdafaanın başarılı bir şekilde gerçekleştirilme girişimi",
- "Devletin birinci dereceden ilgilenmesi gereken bir mesele olarak görüyoruz.'' "siber savaş tehdidine karşı hazırlıklı olmanın, kurumların bilgi güvenliği olaylarına müdahale yeteneği ile kurumlar arası koordinasyon yeteneğini tespit ederek, alınacak önlemler ve bilincinin arttırılmasını amaçlamak"

Bilgi Güvenliği Stratejisi (ABD)

- *Kamu kurumları ağlarını tek bir ağ altında güvenli internet bağlantıları ile yönetme*
- *Kamu kurumları genelinde saldırıları tespit eden sensörler kurma*
- *Kamu kurumları genelinde saldırı önleme sistemleri kurulumunun sürdürülmesi.*
- *Ar-Ge çabalarının arttırılmasını koordine etmek ve yönlendirme*
- *Güvenilen internet bağlantıları ile tek bir ağ kuruluş olarak kamu kurumları hizmetlerinin yönetilmesi.*
- *Durumsal farkındalığı geliştirmek için mevcut siber merkezleri birbirine bağlama.*
- *Hükümet çapında karşı siber casusluk planı geliştirilmesi ve uygulanması.*
- *Sınıflandırılmış ağların güvenliğini arttırma.*
- *Siber eğitim çalışmalarını genişletme.*
- *Kalıcı bir "sıçrama-ilerleme" teknolojisi, stratejiler ve programlar tanımlayınız ve geliştiriniz.*
- *Kalıcı ve caydırıcılık stratejileri ve programları tanımlama ve geliştirme.*
- *Küresel tedarik zinciri ve risk yönetimi için çok yönlü yaklaşımlar geliştirme.*
- *Kritik altyapı alanları içine alan ve devletin sorumluluklarını tanımlayan genişletilmiş siber güvenlik çalışmaları yapma*

PENTAGON: **Sinop'taki kuleye ihtiyaç yok**

RICHARD CLARKE (Beyaz Saray Siber Güvenlik Uzmanı)

"Casusluk artık çok kolaylaştı. Eskiden Washington'daki Rus Elçiliği'nde çalışan bir KGB ajanının bir FBI ajanı ayartması çok zordu. Ama şimdi Moskova'da oturuyorsun. Ve hiçbir risk olmadan binlerce sayfa çalabiliyorsun. Eskinin casuslarına artık gerek yok."

Hem İstihbarat örgütlerindeki insan kaynağı, hem de Altyapı farklılaştı:

"Eskiden Sinop'ta büyük bir kulemiz vardı. Rusya'daki konuşmaları dinliyorduk. Ama şimdi buna ihtiyaç yok. Kimse radyo frekansı kullanmıyor. Ulusal Güvenlik Ajansı'nın (NSA) Maryland'deki kampüsünden bütün dünyadaki internet trafiğini izliyoruz.

Bu konudaki bütçe Pentagon'a ait olduğundan, NSA ve Pentagon neredeyse tek bir kuruluş gibi çalışıyor. Amerikalı asker Sinop'a gitmesine gerek kalmadan her işini masasından halledebiliyor."

Siber Savaş Hazırlığı (ABD)

ABD Hükümetinin, sanal güvenlik harcamaları;

* 2002 yılında **2.7 milyar dolar**,
* 2003' yılında ise **4.2 milyar dolar**'dır.

İyi bir orduya sahip olmak güvenlik için yeterli değil.

* Bilgisayarın ve enformasyon, artık devletleri içine alabilecek kadar güçlüdür.

ABD Hükümeti siber savaşlarda mücadele etmek için

* Günlük **12 milyon dolar** harcamaktadır.

> Gelecek siber ordular üzerine kurulacaktır.

Yapılan tahminlere göre Siber tehditlerden korunmak için 2010 yılında dünya çapında 16.5 milyar dolarlık güvenlik yazılımı harcaması yapılmış olup bunun her yıl yaklaşık %10 artması beklenmektedir.

Bilgi Güvenliği Stratejisi (DE)

- *Kritik Bilgi Altyapılarını Koruma*
- *Almanya BT Sistemleri Güvenliğini Sağlama*
- *Kamu Yönetiminde BT Güvenliğin Güçlendirilmesi*
- *Ulusal Siber Müdahale Merkezi*
- *Ulusal Siber Güvenlik Konseyi*
- *Siber Güvenlik İçin Etkili Suç Kontrolü*
- *Avrupa Ve Dünya Çapında Siber Güvenliği Sağlamak İçin Etkin Koordinasyon*
- *Güvenilir Ve Sağlam Bilgi Teknolojisi Kullanımı*
- *Federal Kurumlardaki Personellerin Eğitimi Ve Gelişimi*
- *Siber Saldırılara Müdahale Araçları*

Bilgi Güvenliği Stratejisi (NL)

- *Bağlama ve güçlendirme girişimleri*
- *Kamu-Özel Ortaklığı*
- *Bireysel sorumluluk*
- *Departmanlar arasındaki sorumluluk Bölümü*
- *Aktif uluslararası işbirliği*
- *Alınması gereken önlemler orantılı olmalıdır*
- *Öz-denetim*

DÜNYADA SİBER GÜVENLİK

- *Genel durum pek iç açıcı değil..*
- *Bilgi varlıklarına değer veren ülkeler ülke stratejilerini geliştiriyorlar..*
- *Tehditleri belirleme ve durdurmaya yönelik çözümler üzerinde çalışılıyor..*
- *Politika ve stratejileri belirleme ve bunları yürürlüğe koyma..*
- *Farkındalık oluşturma çabaları..*
- *Uluslararası işbirliklerini geliştirme..*

Bilgi Güvenliği ihlalleri nelere mal olur ?

- Para
- İş kaybı
- İmaj
- Güven
- Zaman
- ...

En Zayıf Halka

- *İnsan,*
- *USB bellekler !!!*

Top 10 Strategic Technology Trends for 2020

People-centric

Hyperautomation

Multiexperience

Democratization

Human Augmentation

Transparency and Traceability

Smart spaces

Empowered Edge

Distributed Cloud

Autonomous Things

Practical Blockchain

AI Security

gartner.com/SmarterWithGartner

Gartner.

Personel den beklenenler

Fiziksel güvenlik :

- Binanın korunması
- Kilitler
- BT bileşenlerinin korunması
- Fiziksel saldırı tesbit sistemleri
- Güvenlik görevlisi
- Kapı giriş sistemleri
- Kameralar

Personel den beklenenler

Çalışma ortamı temizliği (Temiz Masa İlkesi)

Personel den beklenenler

Sistem güvenliği:

- Donanım ve Yazılım kurulması
  - İlgili ekipman güvenlik açığına sebep olabilir
  - İlgili ekipman mevcut sistemin çalışmamasına sebep olabilir
  - Kopya ve lisanssız ise hukuki problem oluşturabilir
  - İnternetten indirilmiş ise virüs taşıyor olabilir
  - Mevcut sistemle uyuşmuyor olabilir

Personel den beklenenler

Sistem güvenliği:

- Parola belirleme
  - En az 8 karakterden oluşmalı
  - Büyük harf, küçük harf, rakam ve özel karakterler içermeli
  - Harflerle oluşmuş kısmı anlamlı sözcükler içermemeli
  - Düzenli olarak değişmeli
  - Başkaları ile paylaşılmamalı
  - Rahat erişebilir yerde saklanmamalı
  - Kolay tahmin edilir olmamalı

Personel den beklenenler

Sistem güvenliği:

- Virüsler
  - Bilgi Güvenliği için gerçek ve kesin bir tehdit oluştururlar
  - Bilgi ye zarar verebilir, yok edebilir, yetkisiz kişilerin eline geçmesini sağlayabilir

Personel den beklenenler

Sistem güvenliği:

- Virüsler nasıl bulaşır ?
  - İnternet yada ağ üzerinden
  - USB bellek yada harici disklerden
  - Korsan \ Lisanssız yazılım CD lerinden
  - E-Posta yoluyla

Personel den beklenenler

Sistem güvenliği: Phishing saldırısı

Sayın müşterimiz,
Ağustos ayından itibaren T.C Merkez Bankası'nın aldığı karara dayanarak tüm internet bankacılığı sistemlerinde TCMB'ye bağlı tüm bankaların (AKBANK, ANADOLU BANK, ASYA BANK, GARANTİ BANKASI, FORTIS BANK, FINANSBANK, HSBC BANK, ŞEKERBANK, T.C İŞ BANKASI, TURKEYFINANS, TEB, TEKFENBANK, TEKSTILBANK, KOÇBANK, KUVEYTTÜRK, YAPI VE KREDİ BANKASI, VAKIFBANK) SSL yanlımları ve internet bankacılığına hizmet eden bilgisayarlar güncellenmektedir. Bu güncelleme nedeniyle sistemler yenileneceğinden, hem aktif internet bankacılığı kullanıcılarını tespit etmek, hem de güvenlik açısından sizlere daha iyi bir hizmet verebilmek için bilgilerinizi teyit etmeniz gerekecek ve yeni veritabanımıza kaydedilecektir. Bilgilerinizin teyidi ve yeni veritabanına eklenmesi zorunludur. Teyit işlemi yapılmadığı takdirde Ağustos ayından sonra internet bankacılığını kullanabilmeniz için TCMB Ankara Şubesi'nden bilgilerinizi teyit edip yeni veritabanına kaydettirmeniz gerekecektir. Aşağıdaki linkten bilgilerinizi internet üzerinden teyit edebilir, ya da TCMB Ankara Şubesi'nden bilgilerinizi teyit edebilirsiniz.

İnternet üzerinden teyit işlemini yapmak için aşağıdaki linke tıklayın;
http://tcmb.gov.tr.teyit.merkezbanka.org/guncelleme.php?nid=d3fd99df91df76df

DİKKAT: Lütfen TCMB üzerinden gelmeyen mailleri dikkate almayınız. TCMB üzerinden gelmeyen mailleri güvenliğiniz için bize bildirin. Teyit işlemleriyle hiçbir banka doğrudan ilgilenmemektedir. Bütün teyit işlemleri TCMB tarafından organize edilmektedir. Teşekkürler.

Adres: İstiklal Cad. 10 Ulus, 06100 Ankara, Türkiye
Telefon : (312) 310 3546
©TCMB 2006

Personel den beklenenler

Sistem güvenliği: Virüslerin yayılma süreleri

Kod	Zaman	OS	Etkilenen Sistemler	Yayılma Zamanı
Lion			10,000	3 gün
Code Red			400,000	5 gün
Nimda			100-200k	21 saat
Slammer			100-200k	87 dakika
MSBlaster			900k+	11 saat

Personel den beklenenler

Sosyal Mühendislik:

Sistem ve bilgiler üzerinde izinsiz erişim sağlayabilmek için insanların aldatılma yada hilekarlıkla kullanılmasıdır.

Yardımcı olmaya istekli olma, başkalarına güvenme ve zpr durumda kalmak istemem gibi zaaflarımızdan yararlanırlar.

Amaç > Dolandırıcılık, sistemlere erişmek, endüstriyel casusluk, kimlik hırsızlığı, sistemleri bozmak için gereken bilgiyi elde etmek.

Bilgi güvenliği yanıbaşımızda…

Siz ya da yakınlarınız bilgi güvenliği konusunda hiç problem yaşadınız mı? Yaşanmış olaylar saymakla bitmez.

ÖNCELİKLE…

- *Bilgi güvenliği **ciddi olarak ele alınması** gerekiyor.*
- ***Neyin korunacağını bilmek** en önemli adım.*
- ***Nasıl korunacağını** veya korunamayacağını bilmek (risk yönetimi) **işin özü**.*
- *Uygulama safhası doğru yolda olunduğunun, **gözlem, izleme ve denetim** de etkinlik ve **başarının anahtarıdır**.*
- ***İnsan-Eğitim-Teknoloji** birlikteliğini sağlamada işin **püf noktasıdır**.*

DAHA SONRA…

- *Bu işlemleri koordine edecek bir birimin kurulması,*
- *Siber suçlarla mücadele biriminin kurulması*
- *Ulusal stratejilerin belirlenmesi ve kısa sürede hayata geçirilmesi*
- *Farkındalık-eğitim çalışmalarının arttırılması*
- *Uluslararası BG standartlarının BT hizmeti veren devlet kurumlarında zorunlu hale getirilmesi*
- *Uluslararası işbirliğinin artırılması*
- *Bu konuda yapılacak olan ar-ge çalışmaları desteklenmeli*
- *Güncel tehditleri takip edip, duyuracak ve giderecek ekiplerin güçlendirilmesi veya bir yapı altında toplanması*

KISACA…

- *Konunun sahibinin bilinmesi*
- *Standartların takip edilmesi ve uygulanması*
- *Farkındalık eğitimlerin arttırılması*
- *Sızma testlerine önem verilmesi*
- *Güncel tehditlerin takip edilmesi ve mevcut sistemlerdeki açıkların giderilmesi*
- *Tüm kurumları mümkün olduğunca siber güvenlik tatbikatlarına katılması*
- *Güvenli yazılım geliştirme teknikleri kullanılarak yazılımların geliştirilmesi*
- *Saldırı tespitlerinin yapılması ve engellenmesi*
- *Veri kurtarma yaklaşımlarının bilinmesi*
- *Ulusal ve uluslar arası işbirliğinin arttırılması*

Güncel örnekler

- Bir kurumda çalışanlarla ilgili kişisel bilgilerin internetten yayınlanması.
- İnteraktif bankacılık sistemi kullanıcısının hesabındaki paraların çalınması.
- Öğrencilerin notlarının sistemde değiştirilmesi.
- Bir turizm tesisinde kalan müşterilerin bilgilerin ele geçirilmesi.
- Kendilerini gizlemek için başka kişilere ait bilgisayarların ele geçirilip oradan saldırı yapılması.
- Ele geçirilen bilgisayarlar üzerinden topluca istenmeyen mesajlar gönderilmesi.

Peki ya siz ?

Toplumdaki imajın zedelenebilir.

Maddi kayıpların ZAMAN VE EFOR KAYBIN **olabilir!**

Bilgisayarın, programların veya dosyaların zarar görebilir!

Bilgilerin başka kişilerin eline geçebilir.

Başka kişilerin suçlarından dolayı ceza alabilirsin.

Dikkat Düşünce Tuzağı

Bilgi güvenliği konusunda birçok kişi hatalar yapabiliyor.

Ne yazık ki bu konuda "**yalnız olmamak**", "**yalnız olmadığını bilmek**" bir teselli vermiyor.

Dikkat Düşünce Tuzağı

Aksine kapımızda bekleyen tehditler artırıyor. Kolaylıkla düşebileceğiniz düşünce tuzakları, yanlış çıkarımlar, riskli düşünceler nelerdir?

Güncel Düşünce Tuzakları

- Anti virüs (virüsten korunma) yazılımımız var, dolayısıyla güvendeyim! (*güncel ise*)
- Güvenlik duvarı (firewall) kullanıyoruz, dolayısıyla güvendeyiz! (*arada kontrol edilmeli*)
- Bilgisayarla pek işim olmuyor. Bu konu beni ilgilendirmez. (*Herkesle ilgili*)
- Bilgimin kopyasını alıyorum, güvenlikten bana ne! (*güncelliği – yedek değil*)
- Güvenlik saldırıları kurum dışından geliyor! (*Başarılı saldırı içeriden geliyor*)
- Aşırı şüpheci olmaya gerek yok. En fazla bir kaç önemsiz dosya gider. (*Mesele sadece dosya değil – sizin adınıza …*)
- Güvenlikten bilgi işlem sorumludur (*"ofiste o işlerle ilgilenen başka biri var. Benim öğrenmeme gerek yok"*) (*Herkes sorumlu*)
- Bir şey olmaz. Bugüne kadar bir şey olmadı sonra da olmaz. (*Çekirge*)

Siz nasıl hareket ederdiniz?

Yanınızda aileniz ya da çok sevdiğiniz arkadaşlarınız olduğunu ve beraber çıkmayı planladığınız kısa bir gezi olduğunu düşünün.

ARABANIZ…

Kullanacağınız araba

- son derece güçlü
- en son çıkan modellerden biri
- iç tasarımı tam hayal ettiğiniz gibi
- son teknoloji aksesuarlara sahip

fakat

- freni tutmayabiliyor
- hava yastıkları tutukluk yapabiliyor
- emniyet kemeri bazen yerinden çıkabiliyor

Yanınızdaki kişiler araba freninde bir problem olduğunu, bazen tam tutmayabildiğini bilmiyorlar. Nasıl davranırsınız?

- *Onları korkutmamak için hiç birşey söylemem.*
- *Onlara arabanın durumu açıklar, arabayı kullanamayacağımızı bildiririm.*
- *Onlara arabanın durumu açıklar, kullanıp kullanmama kararını onlara bırakırım.*
- *Önce tedirgin etmemek için birşey söylemem. Yolculuk bittikten sonra açıklarım.*

Cevabınız ne olursa olsun kendimize soralım.

Asıl mesele nedir?

Tedirgin etme / Tedirgin etmeme meselesi mi?

- risk alma veya almama meselesi mi?
- Unutmayın. **Alınmayacak riskler vardır**.

Bilgi güvenliği konusunda da durum çok farklı değil.

- *Freni bozuk bir arabada seyahat etmek ve bunu bilmemek hoşunuza gider mi?*
- *Peki ya güvenlik tedbirleri alınmadan bilgisayar kullanmak ve aldığınız riskleri bilmemek hoşunuza gider mi?*

Kim Sorumlu ?

- Bilgi güvenliğinin sağlanmasından **herkes sorumludur.**
- Bu sorumluluklar yasal olarak da ifade edilmiş ve **5651 sayılı kanun** (Türkiye) *"İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi"* amacı ile düzenlenmiştir.

Sizin yeriniz !

Herhangi bir bilgi sisteminde aşağıdaki konumlardan ***herhangi birisinde iseniz sorumluluğunuz var*** demektir.

- *Bilginin sahibi*
- *Bilgiyi kullanan*
- *Bilgi sistemini yöneten*

Bu durum çok geniş bir kitleyi içerdiğinden *"bilgi güvenliğinin sağlanmasından herkes sorumludur"* diye genelleme yapmakta bir sakınca yoktur.

Herkes sorumlu ise bilgi güvenliğinin seviyesi nasıl belirlenir?

Bilgi sistemlerini bir zincir gibi düşündüğümüzde bu zincirin en zayıf halkası çoğunlukla sistemin kullanıcılarıdır. Unutulmamalıdır ki "***bir zincir en zayıf halkası kadar sağlamdır.***"

Bilgi güvenliğinin seviyesi de bu durumda kullanıcılara bağlı olduğundan, **kullanıcı bilinci** bilgi güvenliğinin sağlanması için son derece hayati bir öneme sahiptir ve bilgi güvenliği seviyesini belirler.

Kullanıcı Bilincinin Önemi

Güvenlik açıklıklarının çoğu kullanıcı hatalarından kaynaklanmakta, bilinçli ya da bilinçsiz olarak yapılan yanlışlar bilgi kaybına neden olmaktadır.

Kötü niyetli olmanız şart değil. Belki de sadece deneme amacı ile *"paylaşımları kıran programları"*, *"port taraması yapan programları"* kullandınız. ***Farkında bile olmadan bilgi güvenliği açıklığı oluşturabiliyor olabilirsiniz.***

İçeriden gelebilecek hatalar/zararlar

Sistemi içeriden yani kullanıcıdan gelebilecek hatalara ve zararlara karşı koruyan bir mekanizma yoktur.

Hatta dışarıdan gelen saldırganın herhangi bir kullanıcı adı ve şifresi mevcut değilken, içerideki kullanıcının kullanıcı adı ve şifresiyle bazı haklara sahip olması, içerideki tehdidin önemini arttırır.

Bu nedenle bilinçli kullanıcılar olmamız şart olduğu gibi, çevremizdeki kişilerin de bilinçli kullanıcılar olması için üstümüze düşeni yapmalıyız.

Bir kullanıcının hatası tüm sistemi etkileyebilir.

Örneğin;

- Bir kullanıcı kendi kullandığı bilgisayar ile tüm ağa bağlı olduğundan kullanıcıya bulaşan bir tehdit tüm sisteme yayılabilir.

- E-posta ile gelen ".exe" uzantılı bir eklenti, resim dosyası ya da müzik dosyası beraberinde bir solucan ya da truva atı içerebilir. Kullanıcı ekteki dosyayı açtığında tüm sisteme zarar verebilecek bir yazılıma izin vermiş olabilir. Ekteki virüs ya da zararlı yazılım kullanıcının bilinçsizliği nedeniyle tüm sisteme bulaşmış olur.

Bilgi Güvenliği Standartları ?

- *Bilgi güvenliği yönetim standartları (ISO/IEC 270XX ailesi)*
- *Kriptografik standartlar (PKCS)*
- *Güvenlik Değerlendirme standartları*
- *Güvenlik Denetimleri ve Hizmetleri*
- *Kimlik yönetimi ve gizlilik*
- *IT hizmet yönetimi*

Konu Özeti

- *Bilgi güvenliğinin en önemli parçası kullanıcı güvenlik bilincidir.*
- *Oluşan güvenlik açıklıklarının önemli bir kısmı kullanıcı hatasından kaynaklanmaktadır.*
- *Saldırganlar (Hacker) çoğunlukla kullanıcı hatalarını kullanmaktadır.*
- *Bilgi güvenliğinin en zayıf halkası kullanıcılardır.*
- *Bir kullanıcının güvenlik ihlali tüm sistemi etkileyebilir.*
- *Teknik önlemler kullanıcı hatalarını önlemede yetersiz kalmaktadır.*
- *Kullanıcılar tarafından dikkat edilebilecek bazı kurallar sistemlerin güvenliğinin sağlanmasında kritik bir öneme sahiptir.*

AYRINTILI
DEVAM EDELİM

İnternetten İçerik Kaldırma veya Erişimin Engellenmesi Nedir?

İnternet sitesi veya web sayfasına erişimin engellenmesi;

internet üzerinden yayımlanan haber, video, fotoğraf, yorum vb. içeriklerle kişilik haklarının veya özel hayatın gizliliğinin ihlali, suç işlenmesi, kamu yararı bulunması gibi nedenlerle öncelikle hukuka aykırı içeriğin bulunduğu internet sitesindeki URL'ye, ihlal bu şekilde giderilemediği takdirde tüm internet sitesine erişimin engellenmesini ifade etmektedir.

İnternetten içerik kaldırma/silme; *internet üzerinden yayımlanan ve hukuka aykırılık teşkil eden haber, video, fotoğraf, yorum vb. içeriklerin kaldırılması veya silinmesidir. İçerik kaldırma/silme işlemi,* ***ancak yer veya içerik sağlayıcı tarafından yerine getirilebilir.***

İnternet üzerinden yapılan yayınların düzenlenmesi, hukuka aykırı içeriklerin kaldırılması ve internet sitelerine erişimin engellenmesine dair temel kurallar *5651 sayılı* "İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" ile düzenlenmiştir.

E-Tespit

Türkiye Noterler Birliği'nin 7 gün/24 saat esasına göre internette herhangi bir web sayfası veya sosyal medya hesabı üzerindeki veri veya bilgiyi ***URL bazlı tarama yaparak*** tespit etmesidir.

E-tespit talep eden kişi, içeriğini tespit etmek istediği URL'yi Noterler Birliği'nin veri tabanına gönderir, kendisine bir e-tespit başvuru numarası verilir, söz konusu başvuru numarasıyla mesai saatleri içinde herhangi bir notere başvurularak online yapılan tespit kağıda dökülerek noter tarafından onaylanır. E-tespit yöntemiyle internet üzerinden işlenen suçlar veya özel hukuk uyuşmazlıklarına neden olan fiiller kesin bir şekilde tespit edilmiş olur.

https://e-hizmet.tnb.org.tr/tespit/

İÇERİK SAĞLAYICI

Internet sitesine yazı yazmak, yorum yapmak, ses kaydı, fotoğraf, video veya başkaca bir şekilde ***internet ortamına bilgi veya içerik sağlayan herkestir***.

Örneğin, youtube sitesine video yükleyen herhangi bir kişi, haber sitesine yorum yapan okuyucu, gazetede makale yazarı, herhangi siteye entry giren üye vb. tüm internet kullanıcıları içerik sağlayıcı olarak nitelenir. İçerik sağlayıcı, bağlantı sağladığı başkasına ait içerikten sorumlu değildir. Ancak, sunuş biçiminden, bağlantı sağladığı içeriği benimsediği ve kullanıcının söz konusu içeriğe ulaşmasını amaçladığı açıkça belli ise genel hükümlere göre sorumludur (5651 sayılı kanun m.5/2).

TEMEL İNTERNET AKTÖRLERİ-İÇERİK SAĞLAYICILAR

İÇERİK SAĞLAYICI

İnternet ortamı üzerinden kullanıcılara içerik (metin, resim, video, müzik, oyun vb.) üreten kişidir.

5651 sayılı Kanun'da

"İçerik sağlayıcı: İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişiler" olarak tanımlanmaktadır.

Web X.0 teknolojisinin yaygınlaşması ve bunun bir sonucu olarak ortaya çıkan web siteleri sayesinde herhangi bir İnternet kullanıcısı kolayca içerik üretebilmektedir.

Bu durumdan dolayı günümüzde her kullanıcı aynı zamanda bir içerik sağlayıcısı konumundadır.

İnternet ortamında milyonlarca içerik sağlayıcı bulunmaktadır.

İnternette yaklaşık **950 milyon** alan adı ve 45 milyar web sayfası (URL) vardır. Bunların büyük bir çoğunluğu yurtdışı kaynaklıdır.

Ülkemizde **1 milyon 300 bin**in üzerinde aktif yerli web sitesi olduğu tahmin edilmektedir.

YER SAĞLAYICI

Internet kullanıcılarının (içerik sağlayıcıların) giriş yaptığı web sitesinin "mülkiyet hakkı sahibi", "işletmecisi" veya "hosting" (web sitesi içeriğinin barındırıldığı yer) hizmeti veren firma yer sağlayıcı olarak nitelendirilir. Yer sağlayıcı, internet kullanıcılarının içerik sağlamasına imkan sunar.

Örneğin, Hürriyet gazetesinin sahibi veya Hürriyet gazetesine hosting hizmeti (barındırma hizmeti) veren firma yer sağlayıcıdır. Gazetenin yazarları veya haberlerin altına yorum yapan kullanıcılar da içerik sağlayıcıdır. Yer sağlayıcı, yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olduğunda içeriği çıkarmakla yükümlüdür (5651 sayılı Kanun m.5).

TEMEL İNTERNET AKTÖRLERİ-YER SAĞLAYICILAR

İnternetteki herhangi bir içeriğin ulaşılabilir olması için bu içeriği barındıracak ve **7 gün 24 saat** yayınlayacak sistemlere ihtiyaç duyulmaktadır.

Sunduğu teknik altyapı ile İnternet içeriğine barındırma hizmeti (hosting) veren kişi ve şirketlere **yer sağlayıcı** denilmektedir.

5651 sayılı Kanunda "Yer sağlayıcı: Hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişiler" olarak tanımlanmaktadır

Yer sağlayıcılık için aranan teknik gereksinimler çok yüksek olmadığı için şirketler dışında gerçek kişiler de bu hizmeti sunabilmektedir. Örneğin gerçek kişiler evlerindeki bilgisayarda gerekli ayarları yaparak yer sağlayıcılık hizmeti verebilmektedir.

Türkiye'de yer sağlayıcılık hizmetinin sunulabilmesi için BTK'ya bildirimde bulunulması gerekmektedir. Hâlihazırda bildirimde bulunmuş 3.318 yer sağlayıcı bulunmaktadır. Bununla birlikte ülkemizde bulunup da bildirimde bulunmamış ya da yurt dışında hizmet sunan çok sayıda yer sağlayıcısı vardır.

Facebook, Youtube ve Twitter gibi sosyal ağlar hem **içerik** hem de **yer sağlayıcısıdır.**

ERİŞİM SAĞLAYICI

Kullanıcılarına internet ortamına kablolu veya kablosuz erişim imkanı sağlayan Turkcell, Superonline, TTNET, Kablonet vb. gibi isimlerle internete erişim hizmeti sunan her türlü gerçek veya tüzel kişileri ifade eder. Erişim sağlayıcı, belli bir ücret karşılığında kullanıcının internete bağlanmasını sağlayan firmadır. Erişim sağlayıcı gerçek veya tüzel kişileri ifade etmek üzere "internet servis sağlayıcı" (İSS) kavramı da kullanılmaktadır.

Örneğin, Turkcell'den 125 TL'ye internet paketi satın alınması halinde Turkcell firması "erişim sağlayıcı", diğer bir deyişle internet servis sağlayıcı olarak nitelendirilmektedir. Erişim sağlayıcı, kendisi aracılığıyla erişilen bilgilerin içeriklerinin hukuka aykırı olup olmadıklarını ve sorumluluğu gerektirip gerektirmediğini kontrol etmekle yükümlü değildir. Ancak, erişim sağlayıcı, herhangi bir kullanıcısının yayınladığı hukuka aykırı içerikten, haberdar edilmesi halinde içeriğe erişimi engellemekle yükümlüdür (5651 sayılı kanun m.6).

TEMEL İNTERNET AKTÖRLERİ-ERİŞİM SAĞLAYICILAR

İnternet Servis (Erişim) Sağlayıcı (İSS - ISP)

İSS; kullanıcıların belirli bir ücret karşılığında İnternet ortamına ulaşmasını sağlamaktadır.

5651 sayılı Kanunda "Erişim sağlayıcı: Kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişiler" olarak tanımlanmaktadır.

Türkiye'de şirketlerin İSS hizmeti verebilmesi için BTK'dan lisans alması gerekmektedir. Hâlihazırda İSS lisansına sahip 366 firma bulunmaktadır.

Örn: TürkTelekom, Turkcell, Vodafone, Türksat, Superonline vb.

Ticari amaçla internet toplu kullanım sağlayıcı (İnternet Kafeler)

İnternet salonu ve benzeri umuma açık yerlerde belirli bir ücret karşılığı internet toplu kullanım sağlayıcılığı hizmeti veren veya bununla beraber bilgisayarlarda bilgi ve beceri artırıcı veya zekâ geliştirici nitelikteki oyunların oynatılmasına imkân sağlayan işletmelerdir. Yönetmeliğe göre bu işletmelerin bağlı bulundukları mülki idare amirliklerinden "izin belgesi" almaları gerekmektedir.

İnternet toplu kullanım sağlayıcı

Kişilere belli bir yerde ve belli bir süre internet kullanım olanağı sağlayan gerçek ve tüzel kişilerdir.
Örneğin; Kamu kuruluşları, şirketler, oteller gibi çalışanlarına ve müşterilerine internet erişim olanağı sunan yerler internet toplu kullanım sağlayıcıdır.

IP Adresi (IP numarası);

kullanıcının ev, işyeri veya cep telefonu ile internet bağlandığında kendisine verilen numaradır. IP adresi, internet bağlanan her bilgisayara sistem tarafından ayrı ayrı verilen bir nevi kimliktir. IP adresleri sınırlı olduğundan internet servis sağlayıcıları (erişim sağlayıcılar, örneğin TTNET), internete bağlanan kullanıcıya her seferinde ayrı bir IP adresi verir, kullanıcının internet bağlantısı kesildiğinde aynı IP adresi internete bağlanan başka bir kullanıcıya verilir.

Alan Adı (Domain Name); internette bulunan tüm sayfalar bir alan adına bağlı olarak yayınlanır.

Örneğin,

“http://www.simsek.name.tr” bir alan adı olup bu alan adına bağlı ayrı içerikleri olan yüzlerce web sayfası vardır.

URL (Universal Resource Locator); internet kullanıcılarının internette dolaşırken adres çubuğunda gördüğü açık adrestir. Yukarıda “http://www.simsek.name.tr” sitesinin bir alan adı olduğunu belirtmiştik, URL ise bu alan adına bağlı sayfalardan herhangi birinin özel adresidir.

Örneğin, bir URL adresi şu şekildedir:
“http:// www.simsek.name.tr/ders.html”

Erişim Sağlayıcıları Birliği (ESB):

5651 sayılı kanunun suç işlenmesini düzenleyen 8. maddesi kapsamı dışındaki erişimin engellenmesi kararlarının uygulanmasını sağlamak üzere Erişim Sağlayıcıları Birliği kurulmuştur. Birlik özel hukuk tüzel kişiliğini haizdir (5651 sayılı Kanun m.6/A). Erişimin engellenmesi kararları uygulanmak üzere Birliğe gönderilir. Birliğe yapılan tebligat erişim sağlayıcının (turkcell, ttnet vb.) bizzat kendisine yapılmış sayılır. Erişim Sağlayıcıları Birliği

Bilgi Teknolojileri ve İletişim Başkanlığı (BTK):

Kamu tüzel kişiliğini haiz, idarî ve mali özerkliğe sahip özel bütçeli bir kamu kurumudur. BTK, özellikle internet üzerinden suç işlenmesi, özel hayatın gizliliğinin ihlal edilmesi ve gecikmesinde sakınca bulunan hallerde mahkeme kararına gerek olmadan erişimin engellenmesi kararını doğrudan verebilen özel yetkili bir kurumdur.

https://www.btk.gov.tr/

Bilgi Teknolojileri ve İletişim Başkanlığı (BTK) Nasıl Çalışır?

İnternetten İçerik (Video, Fotoğraf, Haber, Yorum vb.) Kaldırma ve Erişimi Engelleme Şartları

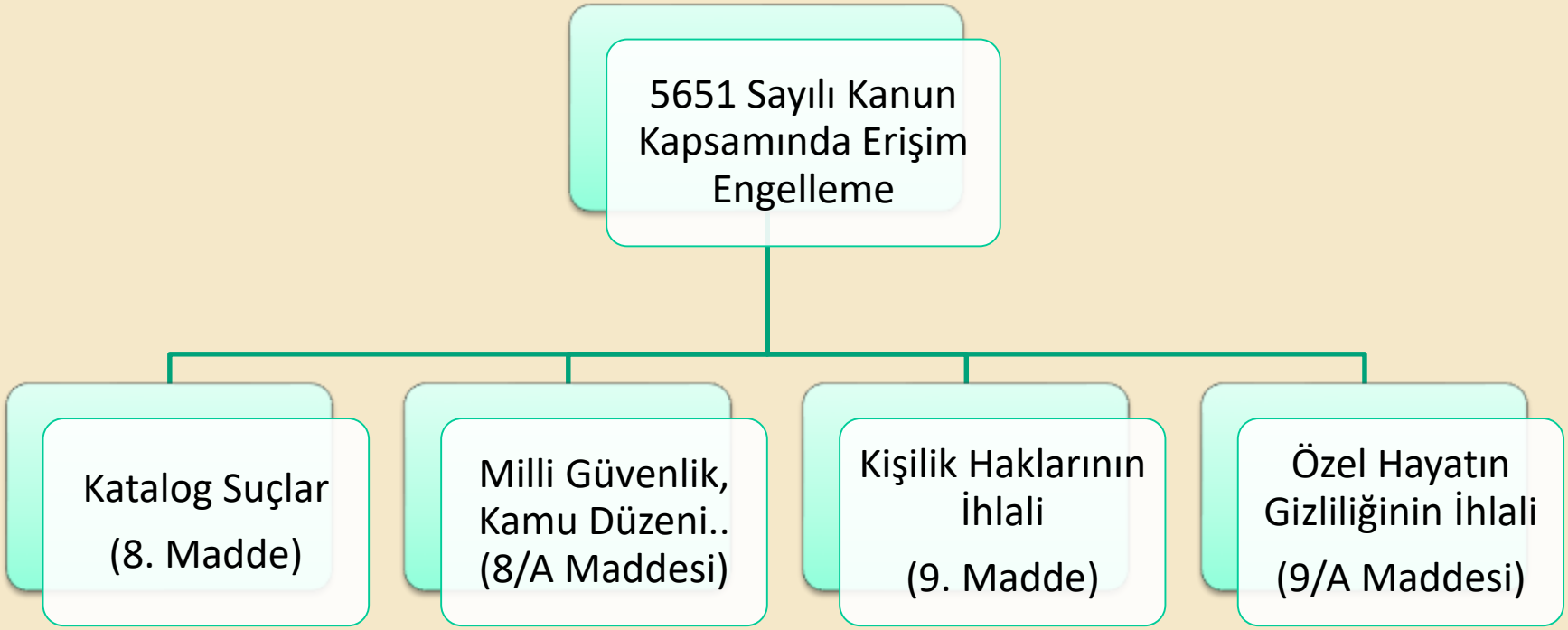
BAZI TANIMLAR-ERİŞİMİN ENGELLENMESİ

URL adresi (link): Herhangi bir içeriğin (metin, resim, video, müzik, oyun vb.) İnternette bulunduğu tam İnternet adresini ifade eder.

Bu çoğu zaman bir web sitesi içindeki herhangi bir web sayfasının adresidir.

Örneğin: http://www.adu.edu.tr

5651 SAYILI YASA KAPSAMINDA İÇERİK ÇIKARMA/ERİŞİM ENGELLEME



http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5651.pdf

5651 SAYILI YASA KAPSAMINDA İÇERİK ÇIKARMA/ERİŞİM ENGELLEME

8. Madde
(Katalog Suçları)

- İntihara Yönlendirme (TCK Madde 84)
- Çocukların Cinsel İstismarı (TCK Madde 103, birinci fıkra)
- Uyuşturucu veya Uyarıcı Madde Kullanılmasını Kolaylaştırma (TCK Madde 190)
- Sağlık İçin Tehlikeli Madde Temini (TCK Madde 194)
- Müstehcenlik (TCK Madde 226)
- Fuhuş (TCK Madde 227)
- Kumar Oynanması İçin Yer ve İmkan Sağlama (TCK Madde 228)

Adli mercilerin talepleri → Vatandaş ihbarları / www.ihbarweb.org.tr → Kamu kurum ve kuruluşlarından gelen ihbarlar / bim.org.tr

5651 SAYILI YASA KAPSAMINDA İÇERİK ÇIKARMA/ERİŞİM ENGELLEME

Katalog Suçları 8. Madde

Adli mercilerin talepleri (Soruşturma aşamasında hakim, kovuşturma aşamasında mahkeme, GSBH'de savcı)

Vatandaş ihbarları / www.ihbarweb.org.tr

Kamu kurum ve kuruluşlarından gelen ihbarlar / bim.org.tr

→ Adli İYM

→ İdari İhbarweb

→ HIS-Operatör → Operatör (Teknik Değerlendirme) → Hukuk (Hukuki Değerlendirme)

→ Erişim Sağlayıcılar Erişim Engelleme

YURTİÇİ

Resen veya Mahkeme Kararı

* Çocukların Cinsel İstismarı
* Müstehcenlik
* Fuhuş

Mahkeme Kararı

*Atatürk Aleyhine İşlenen Suçlar
* İntihara Yönlendirme
* Uyuşturucu veya Uyarıcı Madde Kullanılmasını Kolaylaştırma
* Sağlık İçin Tehlikeli Madde Temini
* Kumar Oynanması İçin Yer ve İmkan Sağlama

YURTDIŞI

(RESEN veya Mahkeme Kararı)

*Atatürk Aleyhine İşlenen Suçlar
* İntihara Yönlendirme
* Uyuşturucu veya Uyarıcı Madde Kullanılmasını Kolaylaştırma
* Sağlık İçin Tehlikeli Madde Temini
* Kumar Oynanması İçin Yer ve İmkan Sağlama
* Çocukların Cinsel İstismarı
* Müstehcenlik
* Fuhuş

Ara Sınav Konuları

- Bilişim Hukuku ve Turizm Bilişim Suçu

- Online Turizm Endüstrisinde Kişilik Haklarının İhlali ve Özel Hayat

- Online Turizm Endüstrisinde Fikir ve Sanat Eserleri Kanunun İhlali, Unutulma Hakkı ve Kamu Yararı Nedeniyle İçerik Çıkarma