



T.C. İÇİŞLERİ BAKANLIĞI
EMNİYET GENEL MÜDÜRLÜĞÜ
KCM
KAÇAKÇILIK VE ORGANİZE
SUÇLARLA MÜCADELE
DAİRE BAŞKANLIĞI

Bilişim Suçlarında Yeni Trendler

Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı

Bilişim Suçları ile Mücadele Şube Müdürlüğü

Adli Bilişim Büro Amirliği

1. Teknoloji ve Bilişim Dünyası
2. Bilişim Suçları Sınıflandırması
3. Sosyal Medya ve İletişim
4. Siber Saldırıları
5. Bilgisayar Korsanlığı
6. Bilişim Suçlarında Trendler
7. Bilişim Suçlarıyla Mücadele Nasıl Yapılıyor?
8. Proaktif Faaliyetler

Teknoloji ve Bilişim Dünyanın Cazibesi

3

- Teknoloji
- İnternet
- E-Devlet
- Finans

Siber suçların hızla arttığı Türkiye'de kimce

Skandal! 687 bin öğretmenin bilgileri çalındı


12/02/2009 13:52

Binlerce öğretmenin okul ile T.C. Kimlik numaralarının da yer aldığı bilgilerin, çalınarak ünlü paylaşım sitesi rapidshare'e yüklendiğini ortaya çıktı

 Tavsiye et  Arkadaşlarının tavsiyelerini görmek için Kaydol.

[Önceki Haber](#) | [Sonraki Haber](#)

Haberleri Paylaş

-  Facebook
-  Delicious
-  Google
-  Yahoo
-  myspace
-  Stumble Upon
-  Mixx
-  Twitter
-  Digg
-  Reddit
-  Friend Feed

Haberler

er savaşta zayıf halkayız
eş müziğe ceza 'ağır ağır'
iyor!
ımızdan ağır ağır
yorlar
nsa'da sınıf savaşları ve
maire Sarkozy
nsa'da sınıf savaşları ve
maire Sarkozy



ANKARA - Yüzbinlerce öğretmenin okul ile T.C. Kimlik numaralarının da yer aldığı bilgilerin çalınarak ünlü paylaşım sitesi rapidshare'e yüklendiği ortaya çıktı.

Milli Eğitim Bakanlığı'nın MEBBİS kapsamında uygulamaya koyduğu ve eğitim alanındaki birçok hizmetin sanal ortama taşınmasını sağlayan İl ve İlçe Milli Eğitim Müdürlükleri Yönetim Bilgi Sistemi'ndeki (İLSİS) tüm verilerin; ünlü paylaşım sitesi Rapidshare'de paylaşımına açıldığı ortaya çıktı. SQL veritabanında yayımlanan verilerde, 687 bin öğretmenin

yaşanıyor. 2008'de 830 olan olay sayısı 2009'da 1.511'e yükseldi. Toplam siber suç sayısı ise 2.871 oldu.

Bilgi Teknolojileri ve İletişim Kurumu (BTK), yeni hazırladığı Bilgi Güvenliği: Riskler ve Öneriler başlıklı raporda vatandaşları uyardı. İnternette kötü niyetli yazılımlar ile hackerların kişilere

Haberleri Paylaş

-  Facebook
-  Delicious
-  Mixx
-  Twitter

Merkez Bankası'nın

EFT
SİSTEMİ
ÇÖKTÜ!



Bilişim Suçları

4



İnternet ve Bilgisayar Sadece Bir Araç

5

Bilişim Sistemleri Kullanılarak İşlenen Suçlar

Müstehcenlik ve Çocuk İstismar Suçları

Kumar Oynatmak için Yer ve İmkan Sağlamak

Hakaret – Tehdit - Şantaj

Devlet ve Devlet Büyükleri Aleyhine İşlenebilecek Suçlar

Siber Terör

Korsan CD ve Yazılım Çoğaltılması


İntihara Yönlendirmek

Sağlık İçin Tehlikeli Madde Temin Etmek

Uyuşturucu ve Uyarıcı Madde Kullanımını Kolaylaştırmak

Sosyal Medya&İletişim


6



GÜVENLİĞİNİZ TEHDİT ALTINDA!

Zararlı yazılım sayısının 50 milyona çıkmasının beklendiğini 2011'de, virüsler en çok kurumsal şirketleri tehdit ediyor...

2011 yılı BT güvenliği açısından neler getiriyor? Kendimizi hazırlamamız gereken tehditler neler olacak? ESET'in kıdemli araştırma uzmanı David Harley ve ESET Sanal Tehdit Analiz Merkezi (CTAC) uzmanları, 2011 tehdit eğilimlerini açıkladı. Buna göre Facebook, Twitter gibi sosyal platformların yanı sıra Google, Yahoo, Bing gibi popüler arama motorlarına yönelik sosyal mühendislik saldırıları artacak. Taşınabilir cihazlara yani internet bağlantılı akıllı telefonlara yönelik tehditlerde de yoğunlaşma olacak. ESET uzmanlarına göre, Botnetler yani virüslü çok sayıda bilgisayarın uzaktan yönetilmesi tehditinin, 2011 yılında da büyümeye devam edeceğini öngörüyor. Öte yandan 2010 yılında "bilinen" bulaşıcı



Siber Saldırıları Savaş Sebebi

7

21. Yüzyılın Yeni Savaş Tekniği: Siber Savaş

15.10.2010 - 09:57

Bilişimin büyük bir silah haline dönüştüğü günümüzde, geride hemen hemen hiç iz bırakmayan, fail ve azmettiricisinin dünyanın derinliklerinde kaybolmasını sağlayan ve sanal âlemden kullanılan siber savaşlar büyük bir hızla yaygınlaşıyor.

20. yüzyılın sonunda ve 21. başında yepyeni bir savaş ile karşı karşıyayız. Kimi buna "siber savaş" (cyber war), kimi de buna "enformasyon savaş" veya "Post modern savaş" diyor. Bu savaş tekniğinin ortaya çıkmasında ana unsur insan yaşamının iletişim ağının vazgeçilmez haline gelen bilgisayarlardır.

Bilgisayar, uzay çağını geride bırakarak, bilgi toplumunu oluşturmadaki önemi yadsınamayacak kadar büyümüş ve bugün bankalardan marketlere, evlerden karakollara, polisten suç örgütlerine kadar, yaşamımızın her alanına girmiştir. Bu bilgisayarlar içerisinde devletler bile çok özel bilgilerini ve projelerini saklamaya başlamışlardır. Tabii bu saklı bilgiler ülkelerin kurdukları gizli birimlerde görevlendirdikleri usta 'hacker'larla birbirlerinin sistemlerine girerek elde edilmeye başlanmıştır. Bu savaş taktiği sadece bilgi edinme amaçlı olarak kullanılmıyor, bunun yanında herhangi bir web sayfasını hizmet dışı bırakma (DOS) saldırısı, bilgileri değiştirilerek aldatma veya internet üzerinden karşı propaganda oluşturma şeklinde de yapılıyor. Kısaca bu savaşta bilgisayar teknolojisi ile çalışan makinelerin hedefi saptırılabilir, karşı cephenin savaş stratejileri değiştirilebilir ve ülkenin sahip olduğu gizli yazılımları çöktürülüyor.

Estonya Ve Gürcistan Örneği

26 Nisan 2007 tarihinde Estonya, başkentindeki meşhur Rus askerini sembolize eden "Bronz Asker Heykeli"ni yerinden kaldırmış ve bu olaydan dolayı Rusya'dan sert konuma gelmişti. Rusya'nın bazı eyaletlerinde ise gösteriler yapılmıştı. Hemen akabinde ise Rusya Estonya'ya karşı tarihte ilk olan siber savaşını başlatmıştı. Rusya bu savaş ile Estonya'daki devlete ait bazı web sayfaları ele geçirmiş ve devlet haberleşme ve bankacılık sistemleri felce uğratılmıştı. Bunun yanında Estonya devlet başkanlığı, parlamentosu, bütün bakanlıklar, altı büyük haberleşme



Bilgisayar Korsanlığı

8

RSA hacked, SecurID users possible

Posted on 18 March 2011.



In an open letter, Art Coviello, the executive chairman of EMC's security division (EMC), made public the fact that the company has suffered a breach and data loss following a sophisticated cyber attack."



Categorizing the attack as an Advanced Persistent Threat (APT) that is often associated with corporate espionage and state-sponsored attacks - he said that their investigation revealed that the information extracted from the company systems is related to its SecurID two-factor authentication products, which are widely used by government agencies, private companies and other large organizations to add an additional layer of security for when employees log into their companies' networks.

RSA Hacked & Confidential Information Identified

RSA's security systems identified the attack

BY MAUREEN O'GARA

MARCH 21, 2011 11:45 PM EDT

RELATED PRINT EMAIL FEEDBACK



EMC's RSA security unit identified extremely sophisticated information being extracted from the company's two-factor authentication systems. RSA executive chairman Art Coviello is confident that the information extracted from the company's SecurID systems is not a direct attack on any of our RSA SecurID customers, but it potentially could be used to reduce the effectiveness of our authentication implementation as part of a larger attack.

He wasn't more specific, leaving users uncertain about the extent of the breach.

03.06.2011 10:23:32

Dijital terör artıyor: Sony yine hacklendi

HABER

Yazı boyutu



Google'ın Gmail hesaplarını hedef alan saldırının ardından Sony de saldırıya uğradı. Daha önce 77 milyon playstation kullanıcısının hesabını ele geçiren hackerlar bu kez 1 milyondan fazla kişinin şifresini, e-mail adresini ve diğer kişisel bilgilerini çaldıklarını duyurdu.

Saldırını Lulz Security isimli grup üstlendi ve küçük bir müdahaleyle SonyPictures.com kullanıcılarının tüm bilgilerini ele geçirdiklerini açıkladılar.

Ayrıca kullanıcılara, "Bu tarz saldırılara açık olan bir şirkete nasıl güvenirsiniz" sorusunu sordular.

Paylaş: f G t e m

Beğen Arkadaşlarının neleri beğendiğini görmek için Kaydol.

İlgili Haberler

- Sony'ye yeni hacker saldırısı
- Bahçelî'nin Diyarbakır mitingine siber saldırı
- İngilizler müstehcenliğe karşı bakın ne yapıyor...
- CHP interneti ucuzlatmayı vaad etti
- Çin "Google'ı hackledi" iddiasını reddetti

Nisan ayında yine başka bir saldırının hedefindeki Sony ise, olayı araştırdıklarını belirtti.

Bir önceki saldırıda Playstation kullanıcısı 77 milyon kişinin hesapları çalınmış, Sony, Playstation ağını 1 ay süreyle kapatmak zorunda kalmıştı.

Lulz Security daha önce de Amerikan PBS televizyonunun internet sitesinde protesto amaçlı asılsız bir haber yayımlanmıştı.

Bilgisayar Korsanlığı

9

En büyük motivasyon **P A R A**

İnsanlar nerede

Güç Gösterisi

Kişiler Şifreler

Kişisel Bilgiler

Ticari sırlar

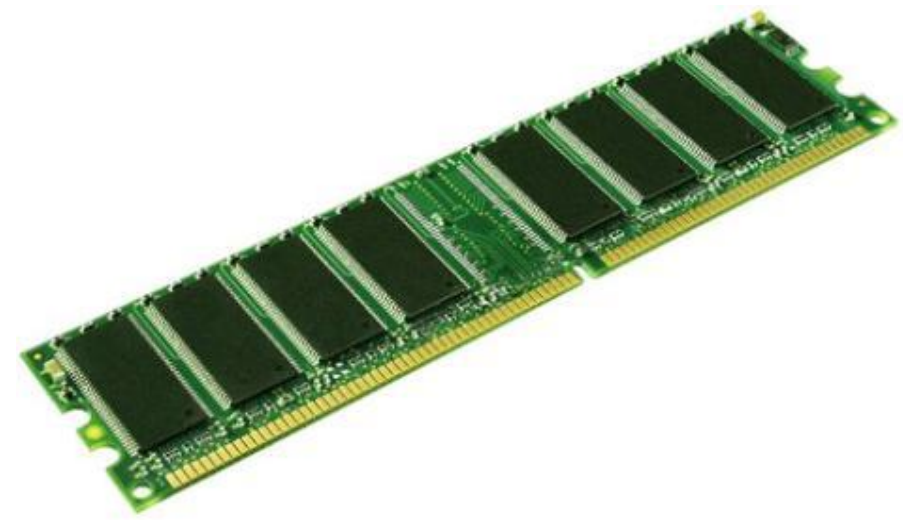
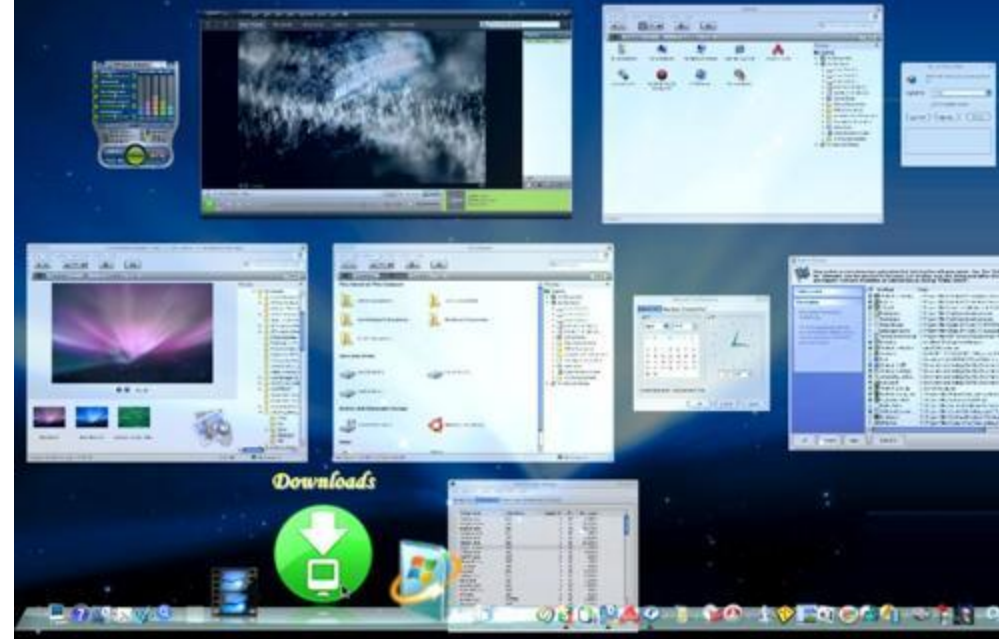
Devlet güvenliğini ilgilendiren bilgiler

BİLGİ EN BÜYÜK GÜÇTÜR

Trendler

10

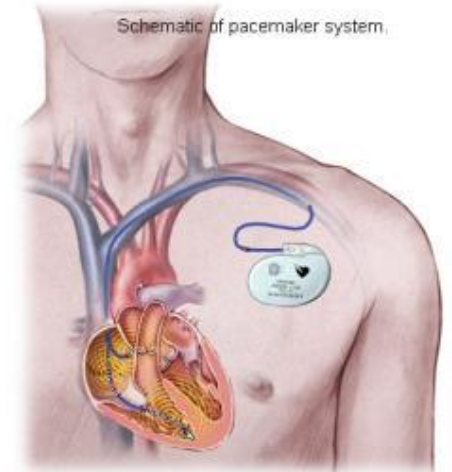
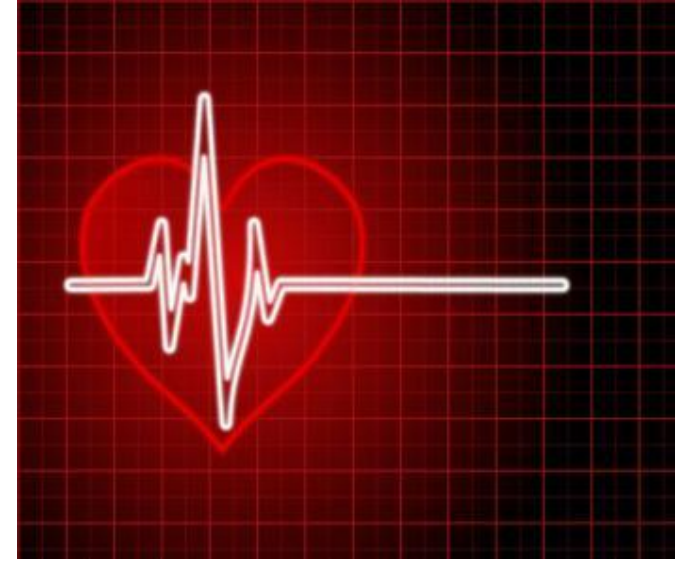
Spyware casus yazılımlar
Mobil uygulamalar
Ram belleğe yönelik zararlı yazılımlar
Ortak platform



Biyoloji Bilgi Teknolojisiyle Buluşuyor

11

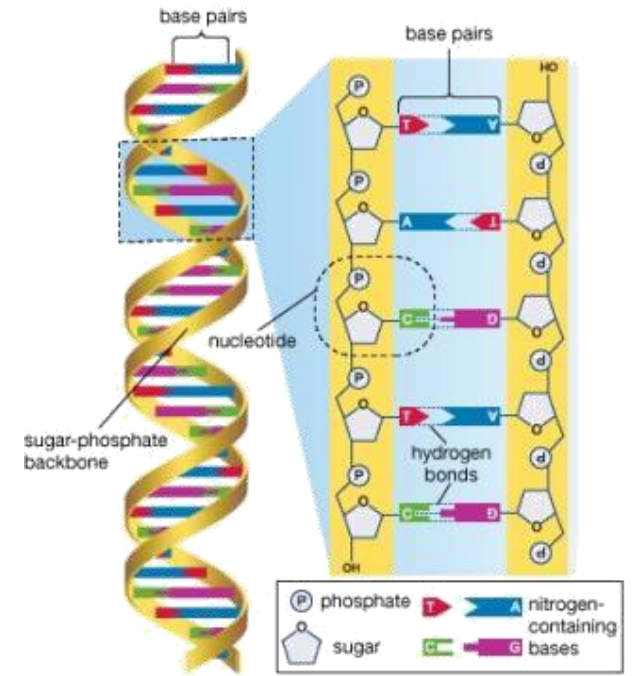
- ✓ Yapay Organlar ve birçoğu artık nete bağlı
- ✓ University of Massachusetts Mart 2008'de bir araştırma yaptı ve Medtronic pacemaker saldırısının teknik olarak mümkün olduğunu saptadı
- ✓ İnsan Kalbini Hacklemeye Çalışanlar Var
- ✓ Yapay ellerle Ameliyat.
- ✓ Nanomedicine.



İnsan Genetiği

12

- İnsan Genetiği tarihte ilk defa çözüldü.
- Bilgisayar 1 ve 0'lar ile temel dilini oluştururken, insan vücudunun kod bilgisi (A-T) (C-G) den oluşmaktadır.
- İnsan bedeni hacklenmeyi bekleyen bir başka işletim sistemi
- Sinetic (synthetic) biyoloji konusunda üniversite ve exploit yarışmaları başladı.
- "Hackerlar"ın insan vücudunda ölüm hücreleri oluşturmak için çalıştığı biliniyor.



Sevimli Robotlar

13



Bilişim Suçlarıyla Mücadele

14

- İstanbul Bilişim Suçları ve Sistemleri Şube Müdürlüğü
- 80 İl Kaçakçılık ve Organize Suçlarla Mücadele Şube Müdürlüğü bünyesinde Bilişim Suçları Büro Amirlikleri
- 15 İl Kaçakçılık ve Organize Suçlarla Mücadele Şube Müdürlüğü bünyesinde Adli Bilişim Büro Amirlikleri

Proaktif Uygulamalar

15

İnternet Servis Sağlayıcılar yetkilendirme konusunda ICANN tarafından belirlenen tavsiyeleri uygulamaktadır ve uygulanmalıdır.

- Botnet task force (Uluslar arası Çalışma Grupları)
- Bilişim Endüstrisi
- Kanun Uygulayıcılar
- Üniversiteler
- Farkındalık (Medya)

Kamu ve Özel Kurumlar İşbirliği

Teşekkürler



Özgür SAYAR
Emniyet Amiri
Adli Bilişim Büro Amiri

Emniyet Genel Müdürlüğü
Kaçakçılık Ve Organize Suçlarla Mücadele Daire Başkanlığı
Bilişim Suçlarıyla Mücadele Şube Müdürlüğü

Tel : 312 412 74 70
Faks : 312 412 74 59

e-posta: osayar@kom.gov.tr