ECE-581
E-Devlet ve e-Dönüşüm

Türk Hava Kurumu Üniversitesi

27 12 2013

Mehmet TUTUŞ
mehmettutus7@gmail.com

Özgür ULUSAN
ozgurulusan@gmail.com

E-DEVLET VE SİBER GÜVENLİK

GELİŞMİŞ SİBER SİLAHLAR

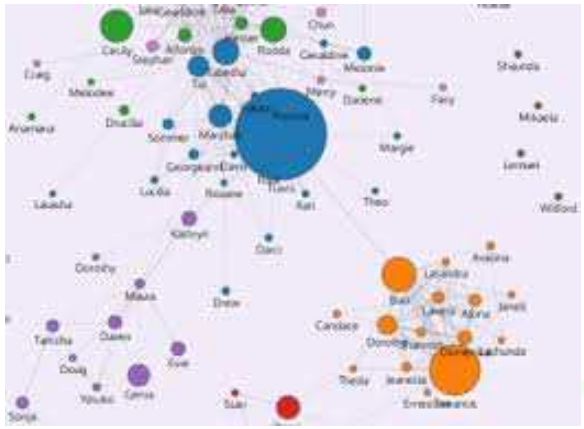
GELİŞMİŞ SİBER SİLAHLAR

Gelişmiş Kalıcı Tehdit Nedir? (APT - Advanced Persistent Threat)

- Yeni nesil bir siber tehdit çeşididir:
  - Gelişmiş ve karmaşık tekniklerle tasarlanmış
  - Kendini gizleyebilen
  - Amacı bilgi sızdırma, casusluk, sisteme zarar verme olan
  - Hedefi net olan

GELİŞMİŞ SİBER SİLAHLAR

APT – Gelişmiş Kalıcı Tehdit



GELİŞMİŞ SİBER SİLAHLAR

“Yakın gelecekte çıkabilecek büyük bir savaşta ilk mermi internette atılacaktır”

Rex Hughes

NATO Güvenlik Danışmanı

GELİŞMİŞ SİBER SİLAHLAR

Günümüz savaşları...

iPhone'daki Açığı 10 Yaşındaki Kız Buldu

10.08.2011 Çarşamba 08:00

Web Gündem

Bu Habere 25 Yorum Yapıldı

Bu Haber 87373 Defa Okunmuştur

Paylaş

12P 14P 16P 18P

10 yaşındaki kız hacker'ın iOS ve Android ceplerde bulduğu bu açık, ağızları açık bıraktı.

ABD'nin Las Vegas eyaletinde gerçekleştirilen hacker etkinliği DefCon, Defcon Kids adında yeni bir bölümün açılışını yaptı. News.com'un raporuna göre DefCom Kids, ortaya ilginç bir hikaye çıkardı bile. Zira "CyFi" takma adına sahip 10 yaşındaki bir kız hacker, iOS ve Android mobil oyunlarında bulunan bir sıfırıncı

WikiLeaks: **382** days of banking blockade - no process
Assange: **379** days detainment - no charge
Manning: **576** days in jail - no trial

We are forced to put all our efforts into raising funds to ensure our economic survival. For almost a year we have been fighting an unlawful financial blockade. We cannot allow giant US finance companies to decide how the whole world votes with its pocket. Our battles are costly. We need your

DONATE ›

Technical Information: $500,0(

ABD siber saldırıları 'savaş sebebi' sayacak

ABD ordusu, bilgisayar sistemlerine yönelik siber saldırılara askeri olarak misillemede bulunmaya hazırlanıyor.

A+ A- Yorum Yaz (7)

Yeni strateji, Washington'un 1950'lerde nüklee.

Sadece Kodlardan Oluşan İlk Silah: Stuxnet

Gelmiş geçmiş en tehlikeli ve karmaşık virüs olan Stuxnet'in anatomisini ve ardında yatan gerçekleri öğrenmek ister misiniz? Belgesel tadındaki bu video ağzınızı açık bırakacak.

19/06/2011 14:2

Ülkeler arasındaki mücadele ve savaşlar artık sadece gerçek dünyad değil **sanal dünyada** da yapılıyor. Hükümetler bilgisayar uzmanlarında oluşan ekiplerle kendilerini hacker saldırılarına karşı korumaya çalışıyorlar.

GELİŞMİŞ SİBER SİLAHLAR

Siber Saldırıların Amaçları

- SİYASİ
- EKONOMİK
- TEKNİK
- ASKERİ

GELİŞMİŞ SİBER SİLAHLAR

Siber Saldırıların Etkileri

- Teknoloji Casusluğu
- Maddi Finansal Kayıplar
- İnternet kaynaklarını ve sistemlerini devre dışı bırakmak
- Sahte belgeler, belgelemeler
- Prestij kayıpları

GELİŞMİŞ SİBER SİLAHLAR

APT Özellikleri

- Gelişmiş yapıya sahiptir.
- Kalıcı uzun sürelidir.
- Hedef odaklıdır.
- Arkasında genelde yetkin bir grup veya ülke bulunmaktadır.
- Sonuçları çok maliyetlidir.

GELİŞMİŞ SİBER SİLAHLAR

APT – Gelişmiş Kalıcı Tehdit

	Geleneksel Saldırgan	APT- Gelişmiş Kalıcı Tehdit
Sömürü Aracı	Yazılım açıklıkları	
Amaç	SPAM, DOS Saldırısı, Kimlik Hırsızlığı	Casusluk, Vasıflı Kimlik Hırsızlığı
Neden	Ün, Finansal kazanç	Askeri, Politik, Teknik
Hedef	Belli konfigürasyondaki cihazlar	Kullanıcılar
Etki Alanı	Karışık, Rasgele	Spesifik, Belirli
Süre	Hızlı	Yavaş
Kontrol	Otomatik Kötü Amaçlı Yazılım	Manuel Yönetim

GELİŞMİŞ SİBER SİLAHLAR

APT Aşamaları

GELİŞMİŞ SİBER SİLAHLAR

APT Ana Hedefleri

- **- Devlet Kuruluşları ve E-Devlet Platformu**
- **- Askeri Kuruluşlar**
- **- Savunma Sanayii**
- **- Kritik Altyapılar**
- **- Ticari İşletmeler**
- **- Bankacılık ve Finans Sektörü**
- **- Sivil Toplum Kuruluşları**

GELİŞMİŞ SİBER SİLAHLAR

APT Ana Hedefleri

Kritik E-Devlet Altyapıları

24

GELİŞMİŞ SİBER SİLAHLAR

SANAL DÜNYADA BİLGİ MİKTARI

- 2.27 milyar internet kullanıcısı
- Günlük 247 milyar e-posta
- 240 milyon internet adresi
- 19.2 milyar internet sayfası
- 1.6 milyar resim
- 50 milyon ses-görüntü dosyası

GELİŞMİŞ SİBER SİLAHLAR

SANAL DÜNYADA BİLGİ MİKTARI

2010 yılı, OECD ülkeleri yapılan istatiksel verilerde;

- **e-posta gönderme : % 67**
- **İnternet yoluyla Sipariş Verme : % 43**
- **İnternet Bankacılığı : % 40**

GELİŞMİŞ SİBER SİLAHLAR

APT Saldırı Sonuçları

- **Britanya'da geçen yıl siber saldırıların ülke ekonomisine maliyeti 27 milyar pound.**
- **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.**

GELİŞMİŞ SİBER SİLAHLAR

APT Saldırı Sonuçları

- **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 zarara yol açmıştır.**

GELİŞMİŞ SİBER SİLAHLAR

Ülkemizde Yapılan APT Saldırıları ve Sonuçları

- **Cumhurbaşkanlığı**
- **TBMM**
- **Başbakanlık**
- **İçişleri/Dışişleri/Ulaştırma vb. Bakanlıklar**
- **Genel Kurmay Başkanlığı/MIT/Emniyet/BTK/TİB vb. Kurum ve Kuruluşlar**

GELİŞMİŞ SİBER SİLAHLAR

Ülkemizde Yapılan APT Saldırıları ve Sonuçları

- **Bilgi Teknolojileri ve İletişim Kurumu hack'lendi. Ele geçirilen tüm bilgiler internette yayınlandı.**
- **MERNİS (70 Milyon Kişinin Kimlik Bilgileri ele geçirildi)**
- **UYAP (Bir şebekenin, Türkiye genelinde tüm adli kayıtların tutulduğu UYAP'a defalarca giriş yaptığı belirlendi.)**

GELİŞMİŞ SİBER SİLAHLAR

Ülkemizde Yapılan APT Saldırıları ve Sonuçları

- **İLSİS (Milli Eğitim Bakanlığı'nın 687 bin öğretmene ait kayıtların tutulduğu İl ve İlçe Milli Eğitim Müdürlükleri Yönetim Bilgi Sistemi'nin 2009 yılında 'hacker'ların saldırısına uğradığı ortaya çıktı. Öğretmenlerin isim, soyisim, T.C. kimlik no ve okul isimlerinin bulunduğu bilgileri ünlü paylaşım sitesi Rapidshare'de paylaşıma açıldı. MEB, bakanlık çalışanlarında bir güvenlik zaafiyeti olup olmadığı ile ilgili soruşturma başlattı.)**

GELİŞMİŞ SİBER SİLAHLAR

Ülkemizde E-devlet ve APT

RedHack Emniyet'ten Bildiriyor

RedHack, POLNET ve Ankara Emniyet Müdürlüğü sunucularına girerek, ele geçirdikleri ihbar, şikayet dilekçeleri ve yazışmaları internette yayınladı. Belgeler endişeli vatandaşın hassasiyetlerini ortaya koyuyor.

Ankara - BİA Haber Merkezi 27 Şubat 2012, Pazartesi

Redhack, bu kez Dışişleri'ni hack'ledi!

Kızıl Hackerlar olarak da bilinen bilgisayar korsanları grubu Redhack, bu kez Dışişleri Bakanlığı'nın internet sitesini hack'ledi. Korsanlar eylemlerine kanıt olarak Türkiye'deki yabancı misyonlarda çalışanların kimlik kopyalarını internette yayınladı.

03 Temmuz 2012 Salı 12:52

Daha önce İçişleri Bakanlığı, Emniyet Gene Müdürlüğü, çok sayıda AK Partili belediye ve Türk Silahlı Kuvvetleri'nin internet sitelerini hack'leyen Redhack, sabah 8.25 sularında Dışişleri Bakanlığı'nın internet sitesinde staj başvurularının yapıldığı bölümüne saldırdı.

Siteye Başbakan Tayyip Erdoğan' target="_blank" class="keywords">Tayyip Erdoğan'ın Libya'nın devrik lideri Muammer

Maliye Bakanlığı'nın sitesine hack!

Maliye Bakanlığı'nın resmi internet sitesine girenler ilginç bir görüntüyle karşılaştılar. Siteye şimdilik ulaşılamıyor...

09 Kasım 2011 Çarşamba, 02:34:37 **Güncelleme:** 11 Kasım 2011 Cuma, 23:36:54

HABERTURK.COM EKONOMİ SERVİSİ

Hackerlar, bakanlığın internet sitesini çökerttiler. Sitede terörist başı Abdullah Öcalan'ın posterleri görünürken, terör yanlısı bir video da ekli görünüyordu.

Ana sayfada PKK lehine propaganda yazılan sitede, hackerlar "Tecrite son verilmesini istiyoruz. Bu yanlıştan dönmediğiniz sürece hack eylemleri devam edecektir" şeklinde not bıraktılar.

Maliye Bakanlığı duruma el koydu. Şimdilik siteye

GELİŞMİŞ SİBER SİLAHLAR

GELİŞMİŞ SİBER SİLAHLAR

GELİŞMİŞ SİBER SİLAHLAR

GELİŞMİŞ SİBER SİLAHLAR

GELİŞMİŞ SİBER SİLAHLAR

GELİŞMİŞ SİBER SİLAHLAR

Bilinen Siber Saldırı Tehditleri

Stuxnet / Flame

Zeus (Zitmo)

Night Dragon

Buckshot Yankee

Nitro

Citadel

DuQu

SpyEye (Spitmo)

WARP

Red October

Aurora

Shady Rat

GELİŞMİŞ SİBER SİLAHLAR

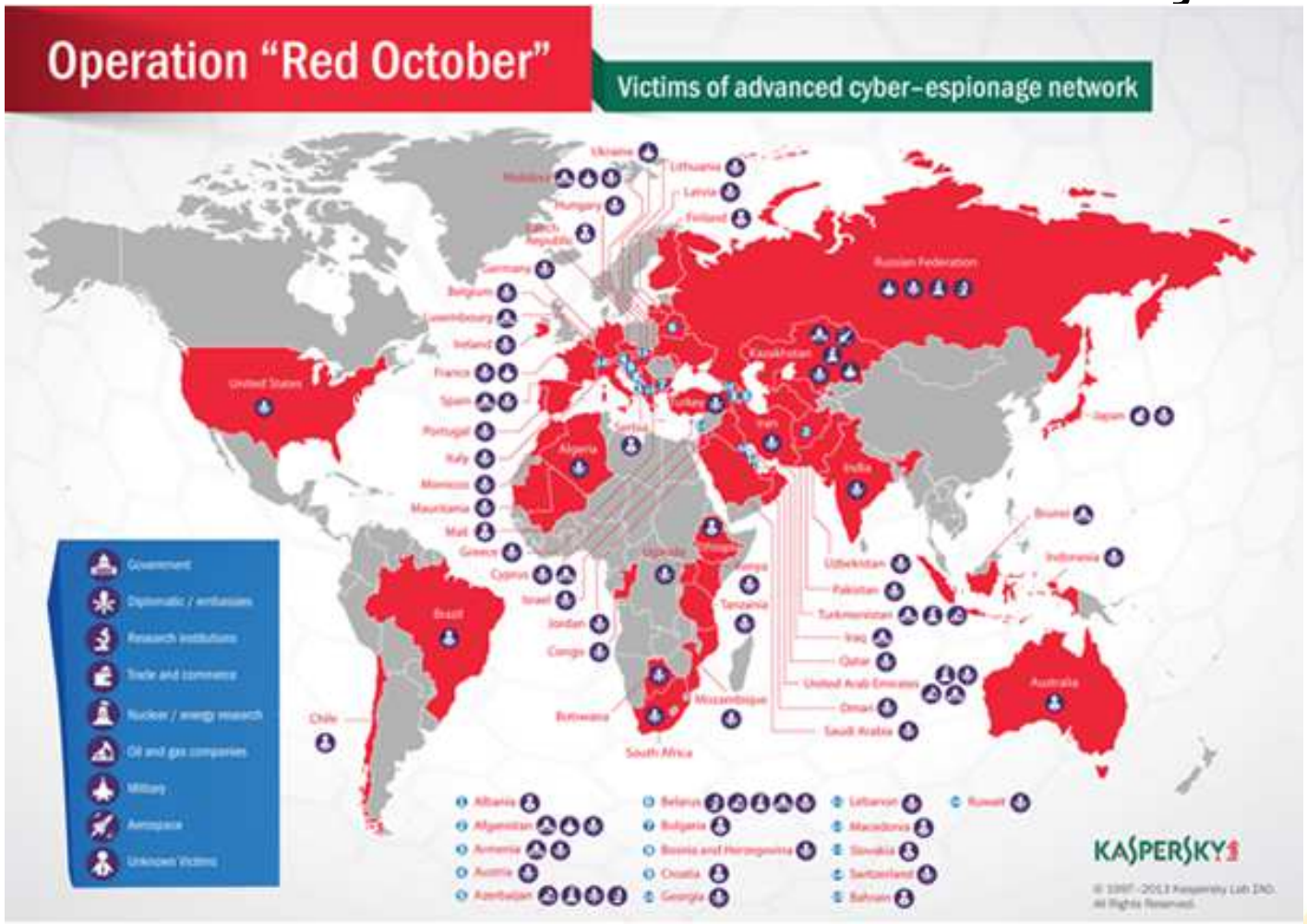
Stuxnet virüsünü analiz eden Symantec firmasının uzmanlarına göre Virüs en çok İran' daki nükleer santrallere bulaştırılmıştır.

GELİŞMİŞ SİBER SİLAHLAR

- Stuxnet virüsü sistemin bir çok açığını buldu ve İran'ın nükleer tesislerini yok etti. Bu İran'ın nükleer santralini 6-7 yıl geriye gönderdi. Tüm bunlar sosyo ekonomik bir kargaşa olmaksızın yapıldı. Savaş ve can kaybı olmadı.

GELİŞMİŞ SİBER SİLAHLAR

RED-OCTOBER NERELERE ULAŞMIŞ



GELİŞMİŞ SİBER SİLAHLAR

Red-October Saldırıları

RUSSIAN FEDERATION	35
KAZAKHSTAN	21
AZERBAIJAN	15
BELGIUM	15
INDIA	15
AFGHANISTAN	10
ARMENIA	10
IRAN	7
TURKMENISTAN	7
UKRAINE	6
UNITED STATES	6
VIETNAM	6
BELARUS	5
GREECE	5
ITALY	5
MOROCCO	5
PAKISTAN	5
SWITZERLAND	5
UGANDA	5
UNITED ARAB EMIRATES	5
BRAZIL	4
FRANCE	4
GEORGIA	4
GERMANY	4
JORDAN	4
MOLDOVA	4
SOUTH AFRICA	4
TAJIKISTAN	4
TURKEY	4
UZBEKISTAN	4
AUSTRIA	3
CYPRUS	3
KYRGYZSTAN	3
LEBANON	3
MALAYSIA	3
QATAR	3
SAUDI ARABIA	3
CONGO	2
INDONESIA	2
KENYA	2
LITHUANIA	2
OMAN	2
TANZANIA	2

GELİŞMİŞ SİBER SİLAHLAR

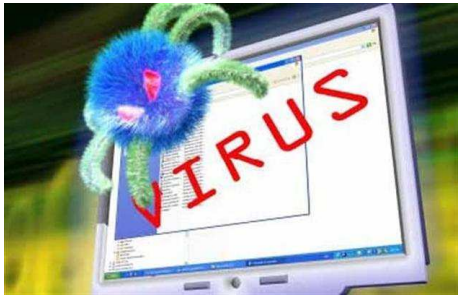


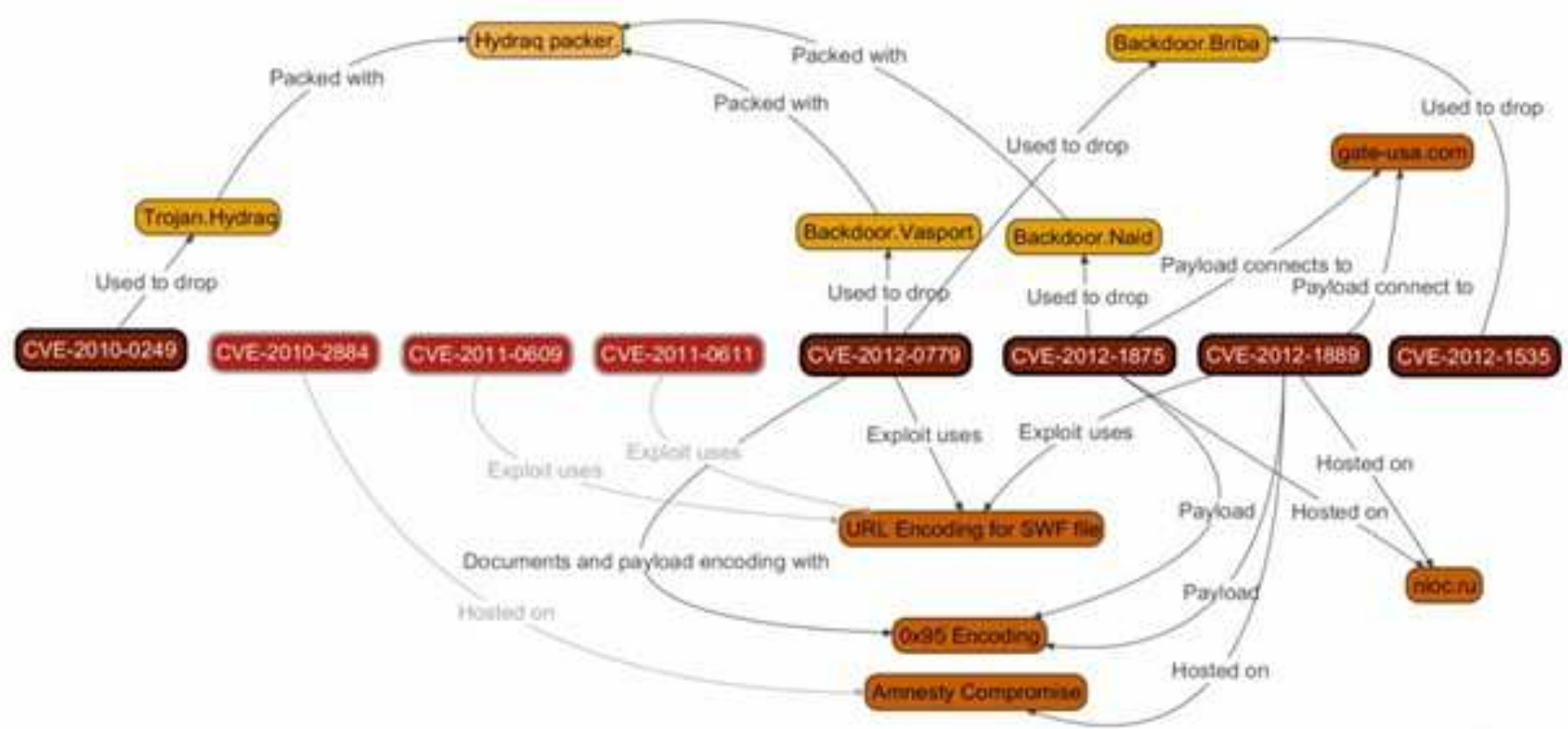
Figure 13 – Heat map of all known victims after 2012-09-01

GELİŞMİŞ SİBER SİLAHLAR

"Teamspy" KSN detections (unique PCs) - March 2013

GELİŞMİŞ SİBER SİLAHLAR

Elderwood Projesi İlişki Şeması



GELİŞMİŞ SİBER SİLAHLAR

Elderwood Saldırganlarının Kullandıkları Açıklıklar

CVE	BID	Tanım	Uygulama
2012-0779	53395	Nesne Türü Karışıklığı Uzaktan Kod Çalıştırma Açıklığı	Adobe Flash Player
2012-1875	53847	Aynı ID Özelliklerine Sahip Uzaktan Kod Çalıştırma Açıklığı	Microsoft Internet Explorer
2012-1889	53934	Uzaktan Kod Çalıştırma Açıklığı	Microsoft XML Core Services
2012-1535	55009	Uzaktan Kod Çalıştırma Açıklığı	Adobe Flash Player
2011-0609	46860	SWF Dosyası Uzaktan Bellek Bozulması Açıklığı	Adobe Flash Player
2011-0611	47314	SWF Dosyası Uzaktan Bellek Bozulması Açıklığı	Adobe Flash Player
2011-2110	48268	Adobe Flash Player Uzaktan Bellek Bozulması Açıklığı	Adobe Flash Player
2010-0249	37815	srcElement()' Uzaktan Kod Çalıştırma Açıklığı	Internet Explorer

Acaba Siz de mi ;)

GELİŞMİŞ SİBER SİLAHLAR

TARİHTEKİ ÖNEMLİ ON HACKER SALDIRISI

1983

- Adını her dönem güvenlik uzmanlarına hatırlatacak Kevin Poulsen adlı korsanın sıralamaya girecek boyuttaki ilk icraatı daha öğrenciyken ABD'nin bütün güvenlik ve savunma ağının bağlı olduğu (ve internetin doğumunda model olarak rol oynayan) bilgisayar ağına sızar. Bir güvenlik açığını keşfederek başardığı bu sızma sonunda geçici de olsa ülkenin bütün savunma sisteminin kontrolünü elinde tutmayı başarır.

1988

- 23 yaşındaki üniversite öğrencisi Robert Morris'i tanımıyor olsanız da hâlâ hemen her gün onun attığı tohumun zehriyle karşılaşıyor hatta belki mağduru oluyorsunuz. Morris, internetin ilk solucan (worm) virüsünün yazarı. 99 satırlık bir deneme projesi olarak 'ortaya saldığı' solucan virüsü bilgisayardan bilgisayara bulaşma özelliğiyle o dönemde bile büyük sorun yaratmış ve iki yıl hapse mahkûm olmuştu.

GELİŞMİŞ SİBER SİLAHLAR

1990

- 27 yaşındaki Amerikalı bilgisayar tutkunu Kevin Mitnick, bilgisayar sistemlerine sızma denemelerinde çıtayı iyice yükselterek başta Nokia, Fujitsu, Motorola ve Sun Microsystems firmaları olmak üzere önüne gelen her yere girmeye ve bilgileri kopyalamaya başlar. Uzun süreli bir takip sonucu Mitnick'i yakalamayı gurur meselesi yapan FBI için çalışan rakip meslektaşı tarafından yakalandığında birçok kişi rahat bir nefes alır. Beş yıl hapis yatan Mitnick hiçbir elektronik cihaza yaklaşmama ve kullanmama şartıyla serbest bırakılır. Şu an pek çok eski hacker gibi bir siber güvenlik danışmanı…

1990

- Adını yeniden anacağımız Kevin Poulsen'in bu seferki hedefi lüks bir spor arabaydı. Los Angeles'taki bir radyo istasyonu kendilerini arayacak 102. dinleyici için son model bir Porsche vereceğini duyurunca Poulsen telefon sistemini eline geçirerek kendisi dışındakilerin telefonu kullanmasını engelledi. Aracı kazandı ancak iki yıl hapis cezasından kurtulamadı.

GELİŞMİŞ SİBER SİLAHLAR

1993

- Kendilerine Masters of Deception adını veren bir hacker grubu hedef olarak Amerikan iletişim sistemini belirler. Üstelik bunda hayli başarılı da olur. Ülkenin en gizli ve karanlık kurumu NSA da dahil olmak üzere bankalar, telekom şirketleri gibi önlerine gelen bütün sistemlere girerler. Yaptıklarıysa daha çok uluslararası aramaları bedavaya getirmektir.

1995

- Rus hacker Vladimir Levin, siber tarih yapraklarında banka soyan ilk insan oldu. Citibank'ın Amerika'daki ağına Rusya'daki evinden girmeyi başaran Levin, bankanın hesabından 10 milyon doları buhar etti. Sefahat içindeki yaşamı Londra'da İnterpol tarafından yakalanmasıyla son buldu. Yapılan araştırmada paraları Amerika, Finlandiya, Hollanda ve İsrail'deki hesaplarına aktardığı ortaya çıktı.

GELİŞMİŞ SİBER SİLAHLAR

1996

- NASA ve ABD donanması için bileşenler üreten O**** Engineering adlı firmanın sistemine altı satırlık bir kod ekleyen Timothy Lloyd kurumsal ölçekteki en büyük hasarı verdi. Zamana ayarlı bir mantık bombası içeren yazılım çalıştığı anda kurumun bütün üretim verilerini silmeye başladı. Zarar 10 milyon dolar olarak belirlendi.

1999

- O yıllarda 30 yaşında olan David Smith, Las Vegas'ta strip dansı yapan sevgilisi Melissa'nın adını verdiği virüsüyle dünyanın her yerinde adından söz ettirdi. Dünya çapında 300 firmanın bilgilerinin tamamen silinmesine yol açan bu virüs toplamda 400 milyon dolarlık hasara yol açtı. Yakalanan Smith beş yıl hapse mahkûm oldu.

GELİŞMİŞ SİBER SİLAHLAR

2000

- Yaşı küçük olduğu için gerçek ismi açıklanmayan ancak internette MafiaBoy adıyla ‘çalışan’ hacker, aralarında Yahoo, eBay ve Amazon gibi dev sitelerin de bulunduğu 52 ağ üstündeki 75 sunucuya sızarak terör estirdi. 2000 yılında yakayı ele verip tutuklanıncaya kadar da faaliyetlerine devam etti.

2002

- İngiliz Gary McKinnon, evinde geçirdiği uykusuz saatleri bilgisayar sistemlerine sızarak değerlendirmeye karar veren başka bir hacker. ABD savunma ağına girerek 90′ın üstünde sisteme girmeyi başaran McKinnon anavatanında yakalanarak hapse konuldu ve yargılanmasına devam ediyor. Ancak ABD onu kendi ülkesinde yargılamak istiyor.

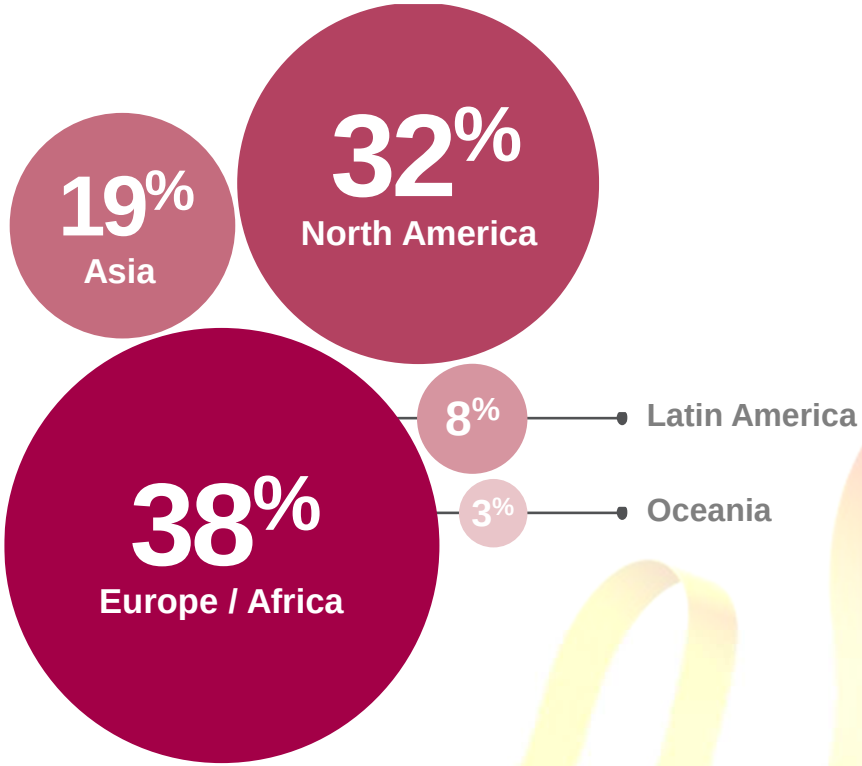
GELİŞMİŞ SİBER SİLAHLAR

ÖNLEMLER

GELİŞMİŞ SİBER SİLAHLAR

ISACA APT ANKETİ

- ISACA kurumu dünya çapında 1500 kişi üzerinde APT hakkında araştırma yapmış.



GELİŞMİŞ SİBER SİLAHLAR

ISACA APT ANKETİ

- Farkındalık

42.5% katılımcı farkında…

28.6%, biraz farkında…

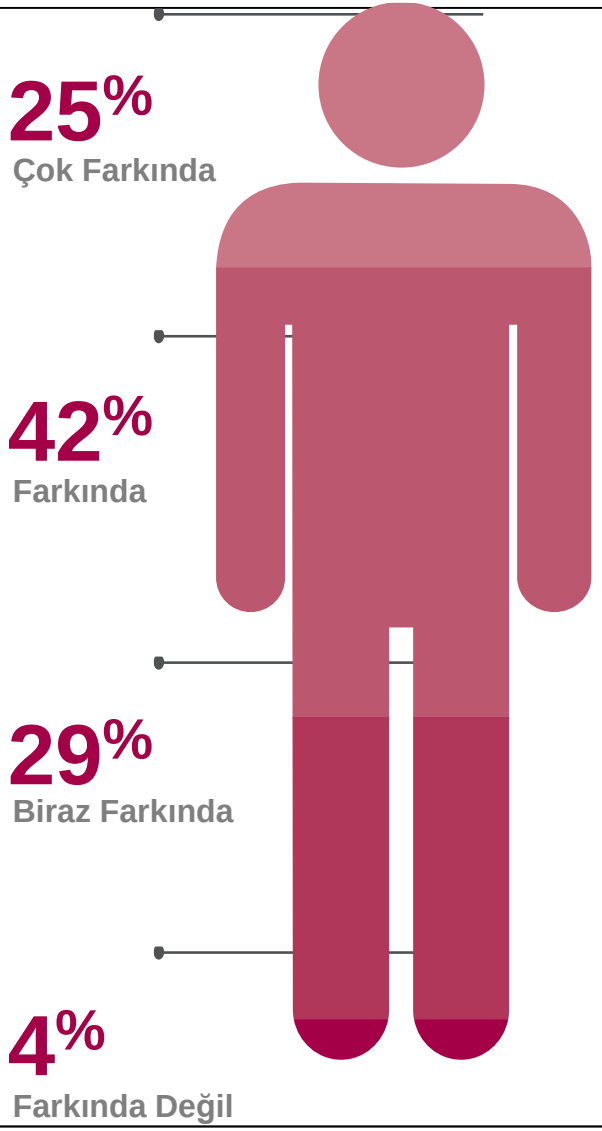
25.1% çok farkında APT hakkında.

Özetle, **96.2%** APT hakkında biraz farkında…

Ama en önemlisi::

93.6%

Katılımcı APT nin gğvenlik ve ekonomik anlamda çok ciddi bir tehdit olduğunu anlamış.



GELİŞMİŞ SİBER SİLAHLAR

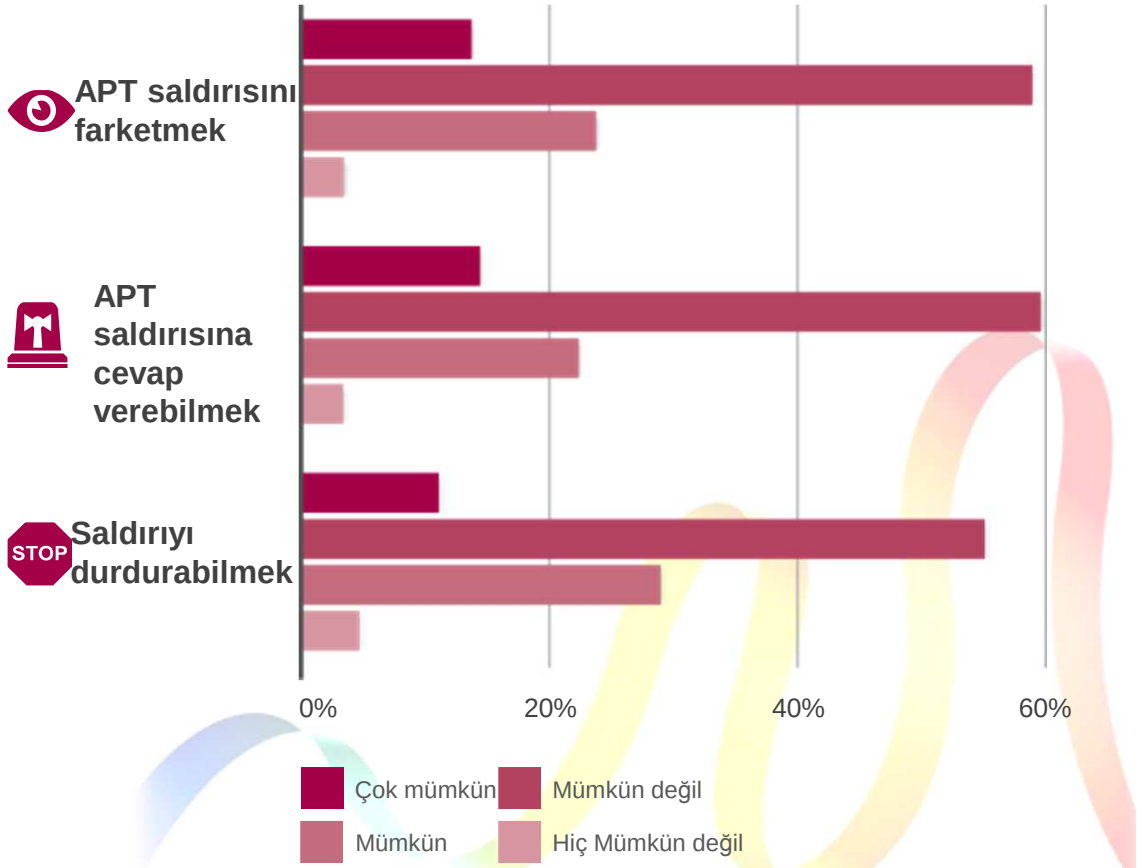
ISACA APT ANKETİ

60% a kadar katılıcıların büyük çoğunluğu, APT saldırısını farkedip, karşı cevap verip ve durdurabileceğine inanıyor.

31.1% APT ye karşı koymak için olay yönetimi planına sahip.

49.5% hazır durumda bekliyor ama elle tutulur bir çözüme sahip değiller.

Bir APT saldırısının üstesinden nasıl gelineceğini bilme?



GELİŞMİŞ SİBER SİLAHLAR

ISACA APT ANKETİ

- İnsanlar APT den nasıl korunabilir ve savaşabilir?

94.9%	**Anti-Virus / Anti-Malware kullanarak**
92.8%	**Network Tech** (Firewalls, etc.) **kullanarak**
71.2%	**IPS kullanarak**

GELİŞMİŞ SİBER SİLAHLAR

ÖNLEMLER

Siber Savunma Tatbikatı
26-28 Kasım 2013
Estonya
33 Ülke Katıldı

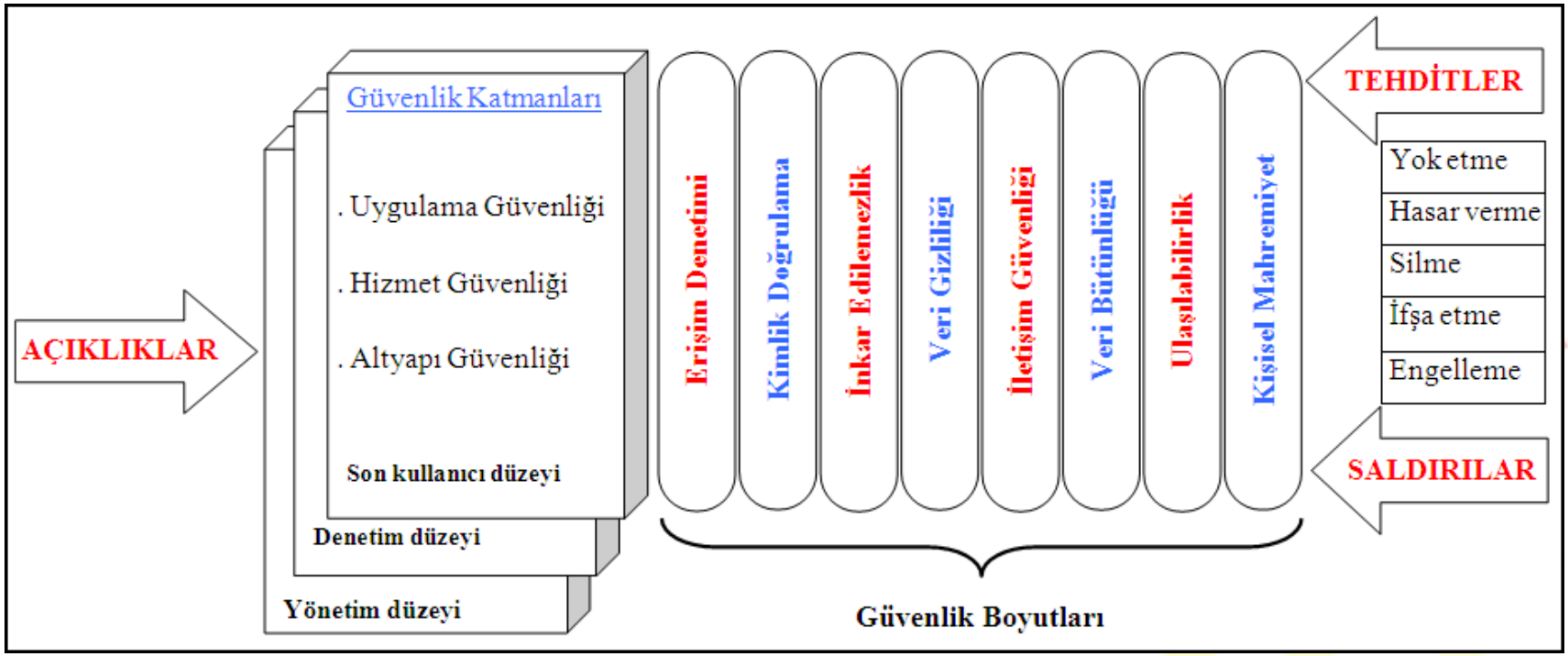
GELİŞMİŞ SİBER SİLAHLAR

ÖNLEMLER

- **Avrupa Birliği ve Siber Güvenlik Koruma Birliği tarafından desteklenen projeyle Trend Micro, 2020'de karşımıza çıkacak dünya ve olası tehditleri işleyen özel bir kısa film serisi hazırladı.**

GELİŞMİŞ SİBER SİLAHLAR

ÖNLEMLER



GELİŞMİŞ SİBER SİLAHLAR

SONUÇ

- Siber saldırılar yoluyla gelebilecek tehditlerin önüne geçilebilmesi için üç ana önlem alınması gerekiyor.

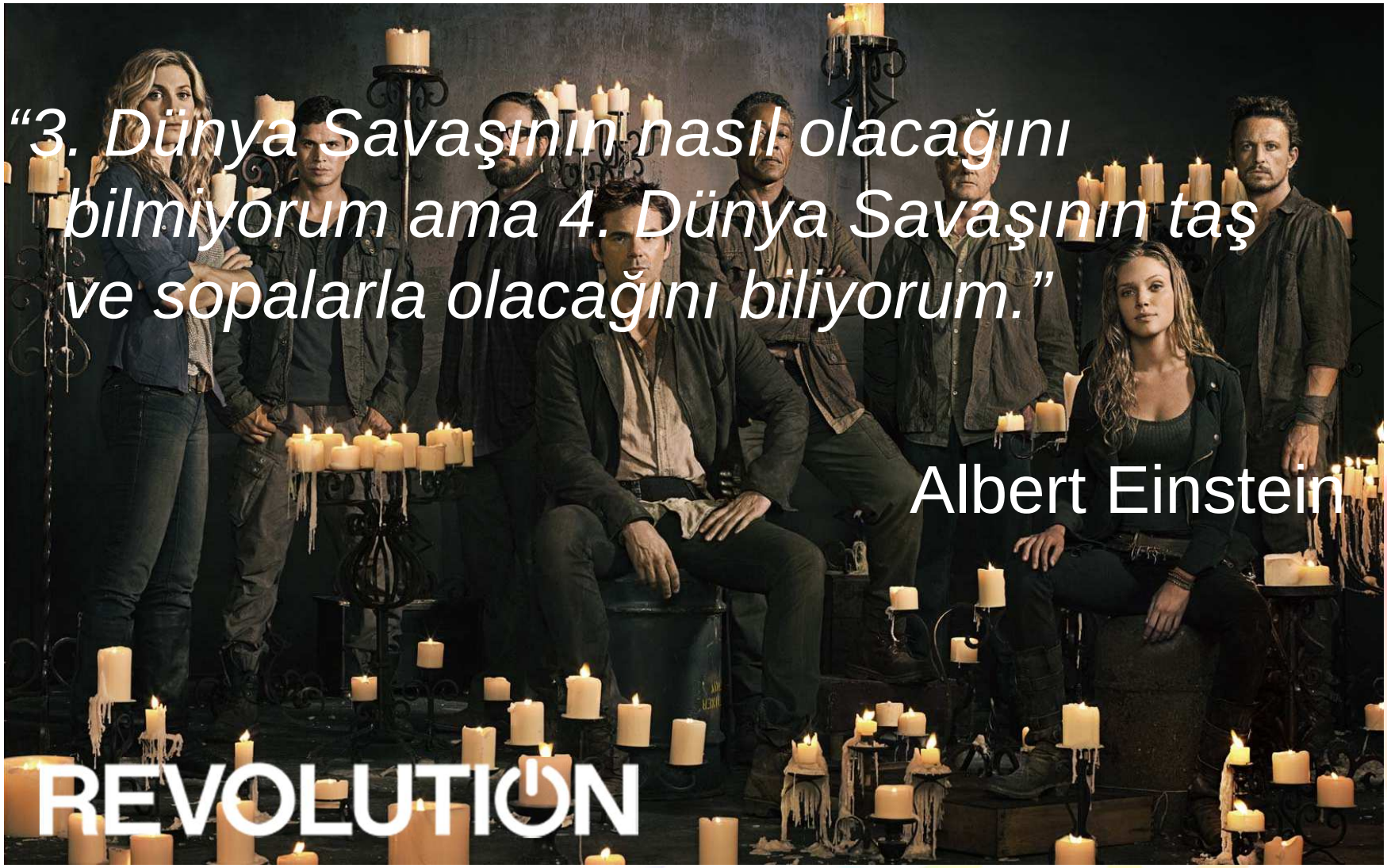
  - Uluslararası savaş hukukunun bir an önce güncellenerek, savunma amaçlı olmayan siber saldırıların kesin olarak yasaklanması.

  - Ükelerin beşinci kuvvet olarak savunma amaçlı siber ordular kurması.

  - Günümüz internetinin bir an önce bilgisayar odaklı internete dönüştürülmeye başlanması.

- İngiltere'nin eski başbakanlarından Gordon Brown'unda da belirttiği gibi devletlerin büyük bir güç olabilmek için artık sadece açık denizlere değil, aynı zamanda internete de hâkim olması gerekiyor.

GELİŞMİŞ SİBER SİLAHLAR



GELİŞMİŞ SİBER SİLAHLAR

Kaynaklar ve Referasnlar

- **Cisco Systems**, *Cybersecurity, Peter Romness Gary Osland Cisco Systems Inc. Business Development Cybersecurity - U.S. Public Sector 2013*
- **Ozan UÇAR**, *Bilgi Güvenliği Akademisi, Advanced Persisten Threat*
- **Huzeyfe ÖNAL**, *Bilgi Güvenliği Akademisi, Hedef Odaklı Sızma Testleri*
- **Bahtiyar BİRCAN**, *Tübitak, GELİŞMİŞ SİBER SİLAHLAR VE TESPİT ÖNTEMLERİ*
- **Ari Juels ve Ting-Fang Yen**, *RSA Laboratories, Sherlock Holmes and the Case of the Advanced Persistent Threat*
- **Symantec**, *Preparing the Right Defense for the New Threat Landscape Advanced Persistent Threats: A Symantec Perspective*
- **Websense**, *ADVANCED PERSISTENT THREATS AND OTHER ADVANCED ATTACKS: THREAT ANALYSIS AND DEFENSE STRATEGIES FOR SMB, MID-SIZE, AND ENTERPRISE ORGANIZATIONS*
- **ISACA**, *Advanced Persistent Threat Awareness*
- **Börteçin EGE,** Bilişimin Karanlık Yüze-Kasım 2012 Bilim ve Teknik Dergisi
- **www.turkiye.gov.tr**

E-DEVLET VE SİBER GÜVENLİK GELİŞMİŞ SİBER SİLAHLAR

TEŞEKKÜRLER

Mehmet TUTUŞ
mehmettutus7@gmail.com

Özgür ULUSAN
ozgurulusan@gmail.com