

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

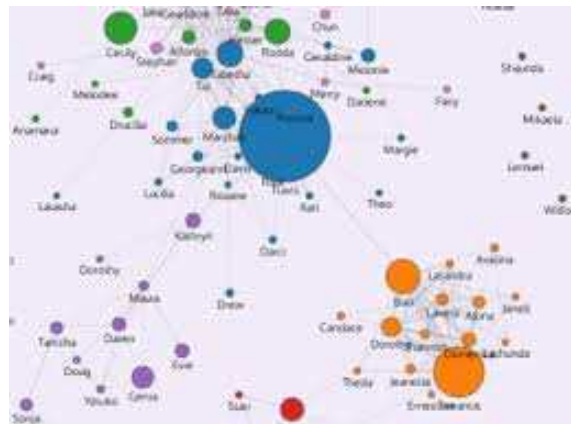
GELİŞMİŞ SİBER SİLAHLAR

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
Twitter'da Paylaş
A 12P 14P 16P 18P

10 yaşındaki kız hacker'ın iOS ve Android ceplerde bulunduğu 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 sıfırncı



ABD siber saldırıları 'savaş sebebi' sayacak

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

A+ A- 12P 14P 16P 18P

Yorum Yaz (7)

Yeni strateji, Washington'un 1950'lerde nükleer...



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: \$500,00

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 ağızınızı açık bırakacak.

19/06/2011 14:2

Ülkeler arasındaki mücadele ve savaşlar artık sadece gerçek dünyada değil **sanal dünyada** da yapılıyor. Hükümetler bilgisayar uzmanlarındaki 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**



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 istatistiksel 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 paylaşım 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

Maliye Bakanlığı'nın sitesine hack!

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

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



HABERTURK.COM EKONOMİ SERVİSİ

Hackerlar, bakanlığın internet sitesini çöktürtiler. 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 yanıltan dönmediğiniz sürece [hack](#) eylemleri devam edecektir" şeklinde not bıraktılar.

Maliye Bakanlığı duruma el koydu. Şimdilik siteye

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

821 YABANCI MİSYON ÇALIŞANININ KİMLİKLERİ AÇIĞA ÇIKTI



**DIŞİŞLERİ'NE
REDHACK
BOMBASI**



Tavsiye Et

Arkadaşların arasında bunu ilk tavsiye eden sen ol.

Daha önce İçişleri Bakanlığı, Emniyet Genel 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 şağı başvurularının yapıldığı bölümüne saldırdı.

Siteye Başbakan [Tayyip Erdoğan](#)'ın `target="_blank" class="keywords">Tayyip Erdoğan` in Libya'nın devrik lideri Muhammed

GELİŞMİŞ SİBER SİLAHLAR

TÜBİTAK Redhack kapışması - Türkiye Haberleri - Radikal - Mozilla Firefox

Dosya Düzen Görünüm Geçmiş Yer İmleri Araçlar Yardım

ECE-581 ÖDEV... ECE581 e-Devle... 10 Canlı online bahı... 10 Casino Oyunları... 10 Bets10 Yılbaşı K... Y redhack kurum... REDHACK Kuru... TÜBİTAK Re... x RedHack ve An... RedHack'tan Sib... 61 kuruma 17 g...

www.radikal.com.tr/turkiye/tubitak_redhack_kapismasi-1086903

Yandex 69 1

Beğen 314 Takip et

Arama Üye Girişi Blog Kitap Galeri WEBTV

Radikal TÜRKİYE EKONOMİ POLİTİKA DÜNYA SPOR HAYAT YAZARLAR TEKNOLOG ÖZEL

Internet alışverişinizi kart bilgisi girmeden yapın! 15 TL puan hediye

Anasayfa > Türkiye > TÜBİTAK Redhack kapışması

TÜBİTAK Redhack kapışması

04/05/2012 02:00 A+ A-

Kurumları geçen hafta uyararak TÜBİTAK dün kendisi Redhack'in 1 saatlik saldırısına uğradı. TÜBİTAK, "Saldırını püskürttük" dedi.

Haber: ZİYA ÖZİŞİK - ziya.ozisik@radikal.com.tr / Arşivi



TÜBİTAK'ın uyarısını Radikal cumartesi günü manşetten duyurmuştu.

Beğen 0 Facebook'ta Paylaş Tweetle 0 +1 4

İSTANBUL - Türkiye'nin "hack" günlüğü bitecek gibi görünmüyor. Çeşitli illerde ilköğretim okulu öğrencilerinin bozuk süt ile zehirlenmesi nedeniyle ihaleyi kazanan süt üreticilerinin internet sitelerinin dün sabah hack'lenmesinin ardından akşamüstü hedef bizzat TÜBİTAK oldu. Geçen hafta devlet kurumlarını saldırılara karşı uyararak, siber saldırılara karşı tathikatlardan içe 'hacan' ile çıkan TÜBİTAK bu sefer kendisi



Baslat TÜBİTAK Redhack ka... Kargıdan Yüklenerler Gelişmiş Siber Silahlar ADVANCED PERSISTENT ... Sunum(2) - Microsoft Word

16 00:58

Radikal. devam edin

Politika ABD: Ricciardone'nin hedef alınmasından rahatsız

Dünya Kürtlerden ortak katılım için rest

Ekonomi Zencani'nin

GELİŞMİŞ SİBER SİLAHLAR

RedHack'tan Siber Saldırı - Mozilla Firefox

Dogya Düzen Görünüm Geçmiş Yer İmleri Araçlar Yardım

ECE-581 ÖDEV-1 - oz... ECE581 e-Devlet ve ... 10 Canlı online bahis, ca... 10 Casino Oyunları Onlin... 10 Bets10 Yılbaşı Kampa... redhack kurum saldırı... REDHACK Kurum ve ... RedHack'tan Siber... 61 kuruma 17 günlük ...

www.on5yirmi5.com/haber/bilim-teknoloji/internet/89308/redhacktan-siber-saldiri.html

Yandex En çok ziyaret edilenler İlk Adım

Aile Eğitim Spor Yaşam Kültür Sanat Teknoloji Sağlık Sinema Müzik Güncel Kariyer Arama

RedHack'tan Siber Saldırı



RedHack internet üzerinden, birçok kurumun web sitesine siber saldırı düzenledi...

Hızlı Paylaş 1 sayfaı tweetle 1 facebookda paylaş Sayfaı Yazdır

RedHack internet üzerinden, birçok kurumun web sitesine siber saldırı düzenledi... Dün,yüzlerce öğrencinin rahatsızlanmasına yol açan, süt firmalarının sitelerini hackleyen Redhack, şimdi de Anonymous işbirliği sonucunda, AKP'li Belediye Başkanı Melih Gökçek'in internet sitesi çöktürdü.

RedHack, Twitter'dan yaptığı açıklamada, Melih Gökçek'in kişisel internet sitesini "Türkiye

BENZER HABERLER

- Redhack incelemesi Hürriyete ulaştı
- Devlet hacker yetiştirecek!
- Şafak Sezer'den Redhack oyunu!..
- Ulusal Kanal yine hacklendi
- Redhack İstanbul İl Özel İdaresini hack!...
- İstanbul Emniyeti'ni "Redhack" vurdu!
- MOSSAD'a Redhack şoku!
- Melih Gökçek RedHack'e öyle bir cevap ...

Türkiye Gençlik Araştırması

ATEİSTİM- NAMAZ KILIYORUM GÖKÇEK'E İZ İLE ESSEK AYNI GÜNE YASAYANLAR. COŞUK YAPMAK İSTİYORUZ. SAĞAMA SİLE GÜVENİM!

ÇOK OKUNANLAR

Bu sorular cevap bekliyor: Suç yeri, suç tarihi, şüphelileri farklı 3 ayrı soruşturma dosyasının operasyon düğmesine niçin aynı gün basılıyor?

Başlat RedHack'tan Siber Sa... Karşından Yüklenenler Gelmiş Siber Silahlar ADVANCED PERSISTENT ... Sunum(2) - Microsoft Word

01:01

GELİŞMİŞ SİBER SİLAHLAR

61 kuruma 17 günlük siber saldırı - Hürriyet EKONOMİ - Mozilla Firefox

Dogya Düzen Görünüm Geçmiş Yer İmleri Araçlar Yardım

ECE-581 ÖDEV-1 - oz... ECE581 e-Devlet ve ... 10 Canlı online bahis, ca... 10 Casino Oyunları Onlin... 10 Bets10 Yılbaşı Kampa... redhack kurum saldırı... REDHACK Kurum ve K... 61 kuruma 17 günlük ...

www.hurriyet.com.tr/ekonomi/22337428.asp

Yandex En çok ziyaret edilenler İlk Adım

Ana Sayfa Arşiv hurriyet emlak.com hurriyetoto.com yenibiris DAILY NEWS yalala.co Üye Girişi Üye Ol Benim Sayfam

Hürriyet EKONOMİ

GÜNDEM PLANET EKONOMİ SPOR KELEBEK KÜLTÜR - SANAT YAZARLAR HURRIYET tv SAĞLIK - YAŞAM TEKNOLOJİ

Hava Durumu Sinema Astroloji Tv Rehberi Piyasalar E- Gazete Canlı Skor En İyi On PASAJ Foto Galerisi Okur Temsilcisi Eğitim Ekler - Bölgeler

EKONOMİ ANA SAYFA ÖZEL RÖPORTAJLAR EKO - ANALİZ ENERJİ

61 kuruma 17 günlük siber saldırı

Esra KAYA 11 Ocak 2013

Tavsiye Et 4 Tweetle 19 8+1 0 e-posta



Redhack isimli hacker grubunun YÖK'ün internet sitesine saldırısıyla tekrar gündeme gelen, kurum ve kuruluşların internet sitesine yönelik 'siber saldırılara' karşı 2'nci Ulusal Siber Güvenlik Tatbikatı yapıldı.

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı koordinasyonunda, Bilgi Teknolojileri ve İletişim Kurumu (BTK) ile TÜBİTAK tarafından yürütülen tatbikatta 61 kuruma gerçek siber saldırı yapıldı. 25 Aralık'ta başlayan tatbikat yaklaşık 17 gün sürdü. Siber Güvenlik Tatbikatında, 42 kişi Tatbikat Merkezinde görevlendirilen personel, 152 kişi de oyuncu kurumlardan olmak üzere toplam 194 personel görev aldı.

ULUSLARARASI TATBİKAT

TİB'de kurulan merkezde yapılan tatbikatın sonuçları önümüzdeki günlerde açıklanacak. Ulaştırma, Denizcilik ve Haberleşme Bakanı Binali Yıldırım, Türkiye'nin riskli ülkeler sıralamasında 6'ncı sırada olduğunu belirterek şunları söyledi: "Türkiye, askeri alanda NATO içinde siber tehdit riskini gören üyeler arasında ilk 12 arasında yerini alıyor. Bu önemli bir adım. Hem askeri anlamda hem sivil anlamda bu tehditle ilgili gerekli adımlar atılmaya başlandı. 2014 yılında ilk defa uluslararası düzeyde bu tatbikatları yapmayı hedefliyoruz. Uluslararası bir rapora göre; güvenlik kötücül yazılım bulaşan bilgisayar sıralamasında Türkiye 6. sırada. Demek ki sistemlerimizi güvenli bir bölgeye taşımamız gerekiyor. Kötücül yazılımların bulaştığı bu bilgisayarları tespit eden tedbirleri almamız

Merhaba
Hürriyet Facebook deneyiminden yararlanmak için Facebook ile giriş yapın. Giriş Yapın

Hürriyet'i Takip Et
f Beğen 614b t Takip et

Piyasalarda Bugün

GELİŞMİŞ SİBER SİLAHLAR



RedHack ve Anonymous, Emniyet ve MİT'in fişini çekti

Anonymous, RedHack'e destek için Emniyet Genel Müdürlüğü'nün resmi web sayfasını hackledi. RedHack de MİT'e saldırdığını açıkladı.

19 Temmuz 2012 Perşembe 12:26



Tavsiye Et

51 kişi tavsiye etti. Arkadaşlarının neler tavsiye ettiğini görmek için [Kaydol](#).

Emniyet Genel Müdürlüğü internet sitesine sabah saatlerinde ulaşılamadı.

YAZARLAR

Tümü



Hikmet Çiçek

Ergenekon'un 'gerekçeli karar'ı neden yazılmıyor?



Levent Kırca

Uzun lafın kısası



Rafet Ballı

İHL çıkmazı 3 / İslamcıların başörtülü fakat eğitimli kadın sorunu



Halil Nebiler

Hasdal'ın dağlarında çiçekler açar

ÖZEL HABER

- 'Unutmazsak değiştirebiliriz'
- Üsküdar'da sabah oldu, emniyet farkında mı?
- Kardan adama soru çözümler

GELİŞMİŞ SİBER SİLAHLAR

Anonymous'tan bakanlıklara saldırı-Sabah - 28 Nisan 2012 - Mozilla Firefox

Doğya Düzen Görünüm Geçmiş Yer İmleri Araçlar Yardım

ECE-581 ÖDEV-1 - özgür... ECE581 e-Devlet ve e-Dö... Canlı online bahis, canlı sp... Casino Oyunları Online, Bl... Bets10 Yılbacı Kampanyala... anonymous kurum saldırı... Anonymous'tan bakanlık...

www.sabah.com.tr/Teknoloji/Haber/2012/04/28/anonymous-tan-bakanliklara-saldiri

Yandex En çok ziyaret edilenler İlk Adım

Sony Xperia Z1'e Ayda **₺40**'ye sahip olmak işte bu kadar kolay

Vodafone Red

Detaylı Bilgi >

Vodafone

GCMFOREX

DÜNYA PİYASALARINA AÇILAN KAPINIZ!

WEBDEN CEPTEN TABLETTE

HESAP AÇ >

sabah.com.tr

Üye Girişi Üye Ol E-Gazete English Arşiv

28 Nisan 2012, Cumartesi

İstanbul 13/3°C

Takip et: @sabah Beğen 3096 +1 10 b

VIDEO HABER PLUS

Haberler > Teknoloji Haberleri > Anonymous'tan bakanlıklara saldırı

Anonymous'tan bakanlıklara saldırı

Uluslararası hacker grubu "Anonymous"un bazı bakanlıklar ve kamu kurumlarının internet sitelerine yönelik siber saldırı düzenlediği bildirildi.

AA Giriş Tarihi: 28.04.2012, 11:39 Güncelleme Tarihi: 28.04.2012, 11:40

Gönder Yazdır A+ A- Beğen 22 Tweet 13 +1 0



Bir süre önce Türkiye'deki kamu kurumlarının internet sitelerine siber saldırı düzenleyeceğini duyuran Anonymous bünyesinde hareket eden hackerlar, saat 20.00 sıralarında Adalet, İçişleri ve Dışişleri bakanlıklarıyla Emniyet Genel Müdürlüğü bünyesindeki web sitelerine "DDOS" adı verilen internet erişimini engellemek için hakerete geçti.

Siber saldırıyla birlikte Bilgi Teknolojileri ve İletişim Kurumu Başkanlığı bünyesindeki Telekomünikasyon İletişim Başkanlığında (TİB) görev yapan uzman ekip, kamu kurumlarıyla organize hareket ederek savunma görevini üstlendi. Bir süre önce TİB bünyesinde siber tehditlere karşı kurulan Teknik İşletme Daire Başkanlığı da siber savunmada aktif rol üstlendi.

Saldırdan internet siteleri etkilenmedi

TİB Teknik İşletme Daire Başkanı Dr. Barış Yaslan, AA muhabirine yaptığı açıklamada, siber saldırının hedefinde aralarında, TBMM'ye ait www.meclis.gov.tr, Adalet Bakanlığı'na ait www.adalet.gov.tr, İçişleri Bakanlığı'na ait www.icisleri.gov.tr, Dışişleri Bakanlığı'na ait www.mfa.gov.tr, Emniyet Genel Müdürlüğü'ne ait www.egm.gov.tr ile Telekomünikasyon Kurumu Başkanlığı bünyesindeki web siteleri de siber saldırıya uğramadığını belirtti.

ETİKETLER

fotoğraf facebook credits htc Kaniş Tepesi sosyal paylaşım sitesi incelemek için egzersizler sony Twitter iPhone uygulamaları apple NASA son haber kullanımı son dakika idc Twitter Gartner AveaBIZ Iphone 4 teknokullis

SOSYAL MEDYA

Başlat Anonymous'tan baka... Karşından Yüklenenler Gelmiş Siber Silahlar ADVANCED PERSISTENT ... Sunum(2) - Microsoft Word

01:03

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.

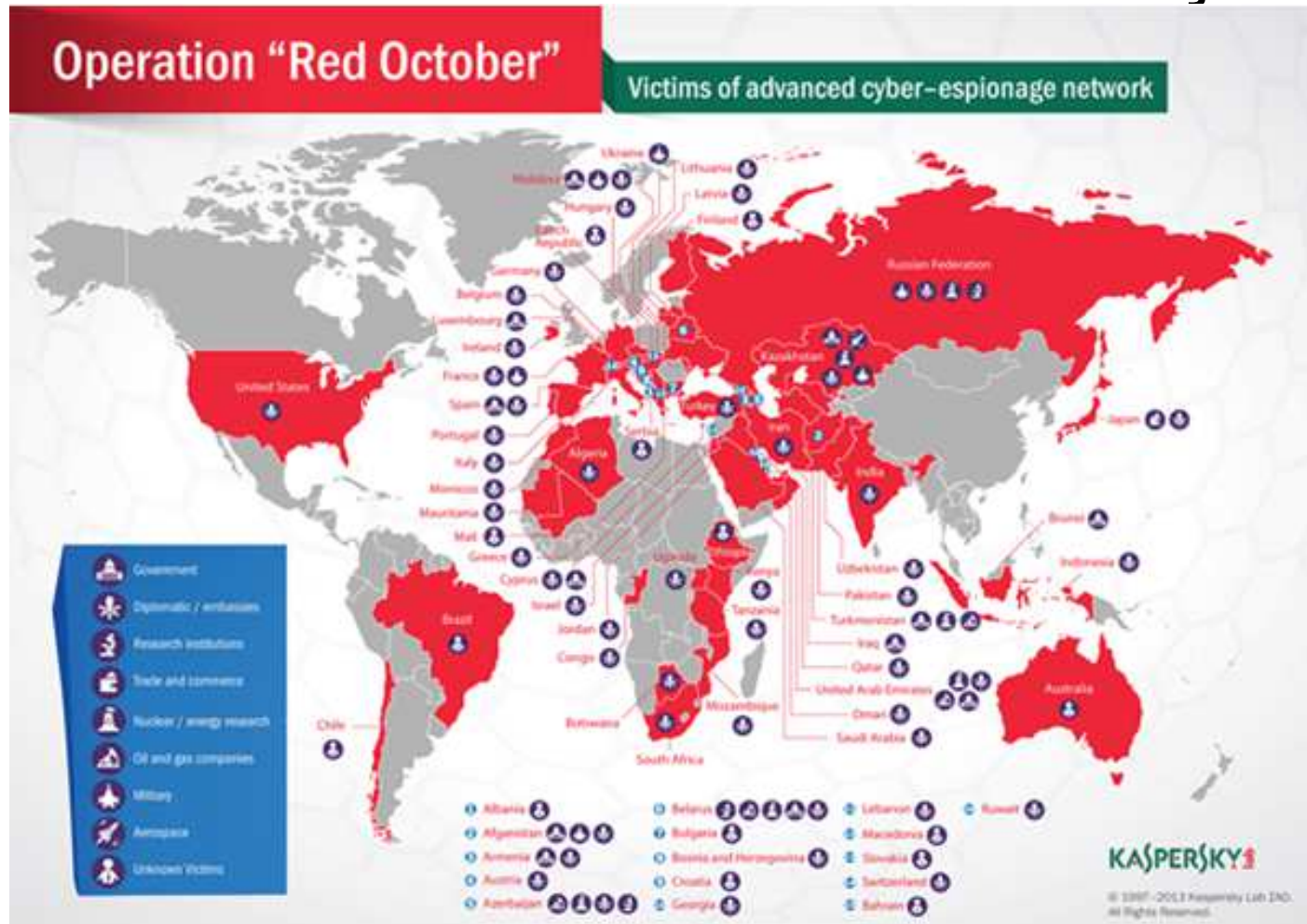


GELİŞMİŞ SİBER SİLAHLAR

- ❑ 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

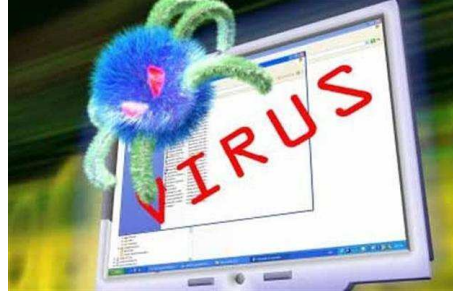


Figure 13 – Heat map of all known victims after 2012-09-01

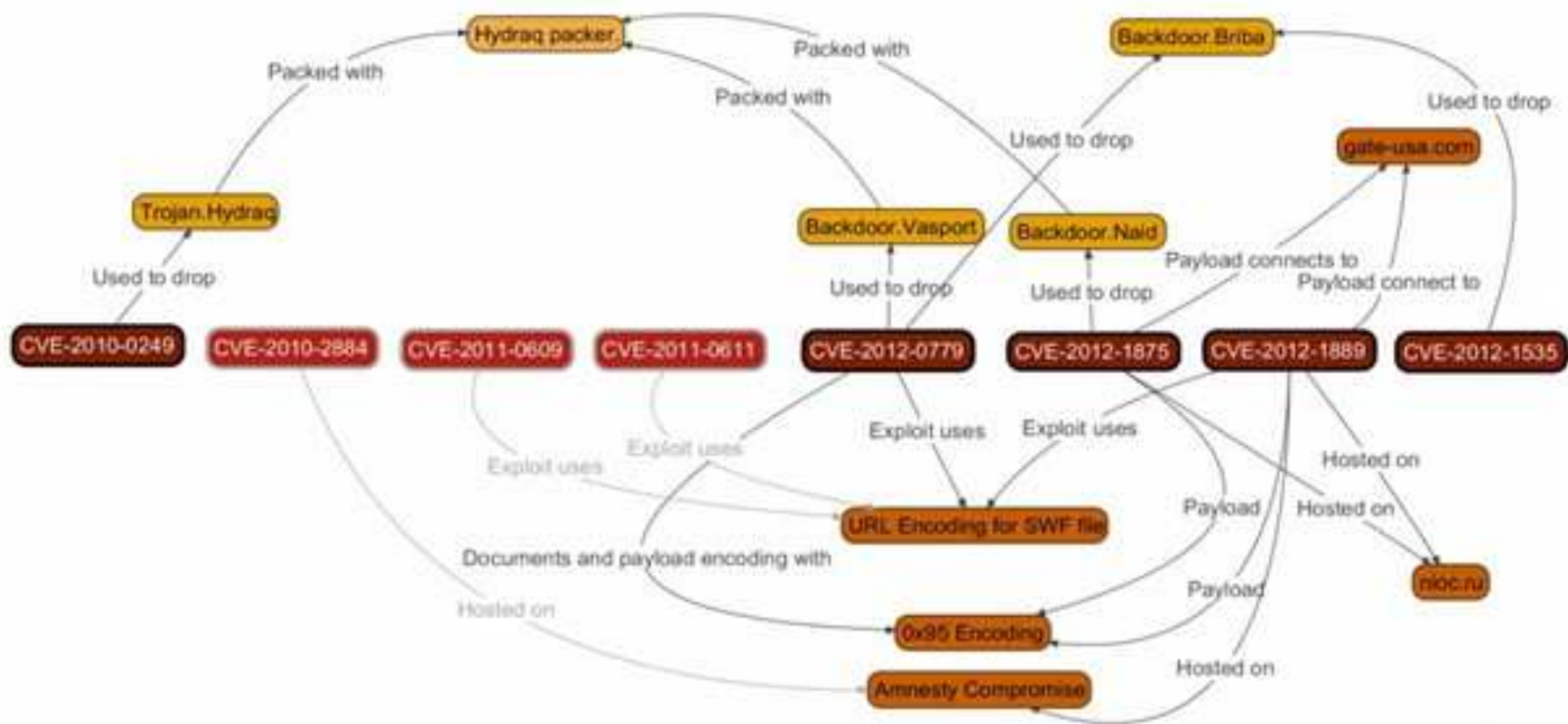
GELİŞMİŞ SİBER SİLAHLAR



"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 karşılaşılıyor hatta belki mağduru oluyorsunuz. Morris, internetin ilk solucan (worm) virüsünün yazarı. 99 satırlık bir deneme projesi olarak 'ortaya saldırdığı' 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 çıtaı 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

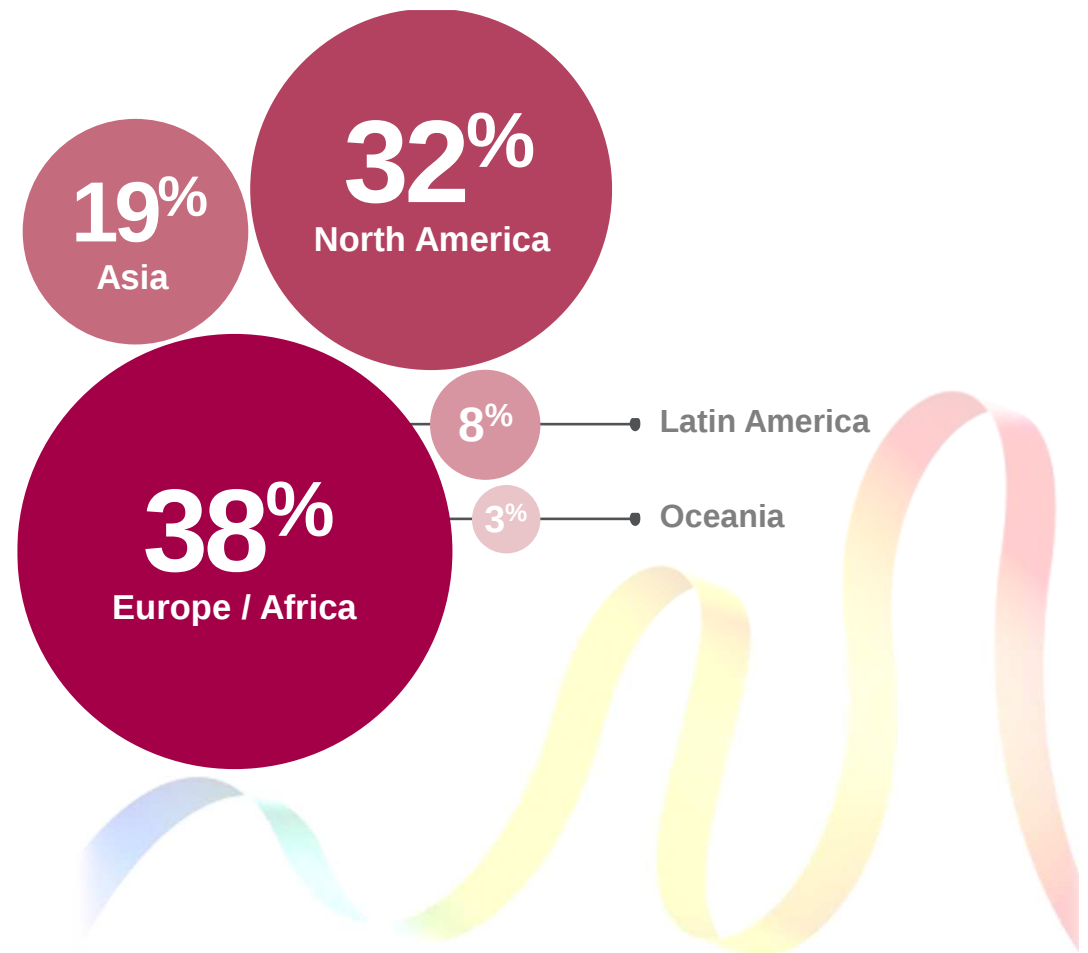
ÖNLEMLER



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 güvenlik ve ekonomik anlamda çok ciddi bir tehdit olduğunu anlamış.

25%

Çok Farkında

42%

Farkında

29%

Biraz Farkında

4%

Farkında Değil

GELİŞMİŞ SİBER SİLAHLAR

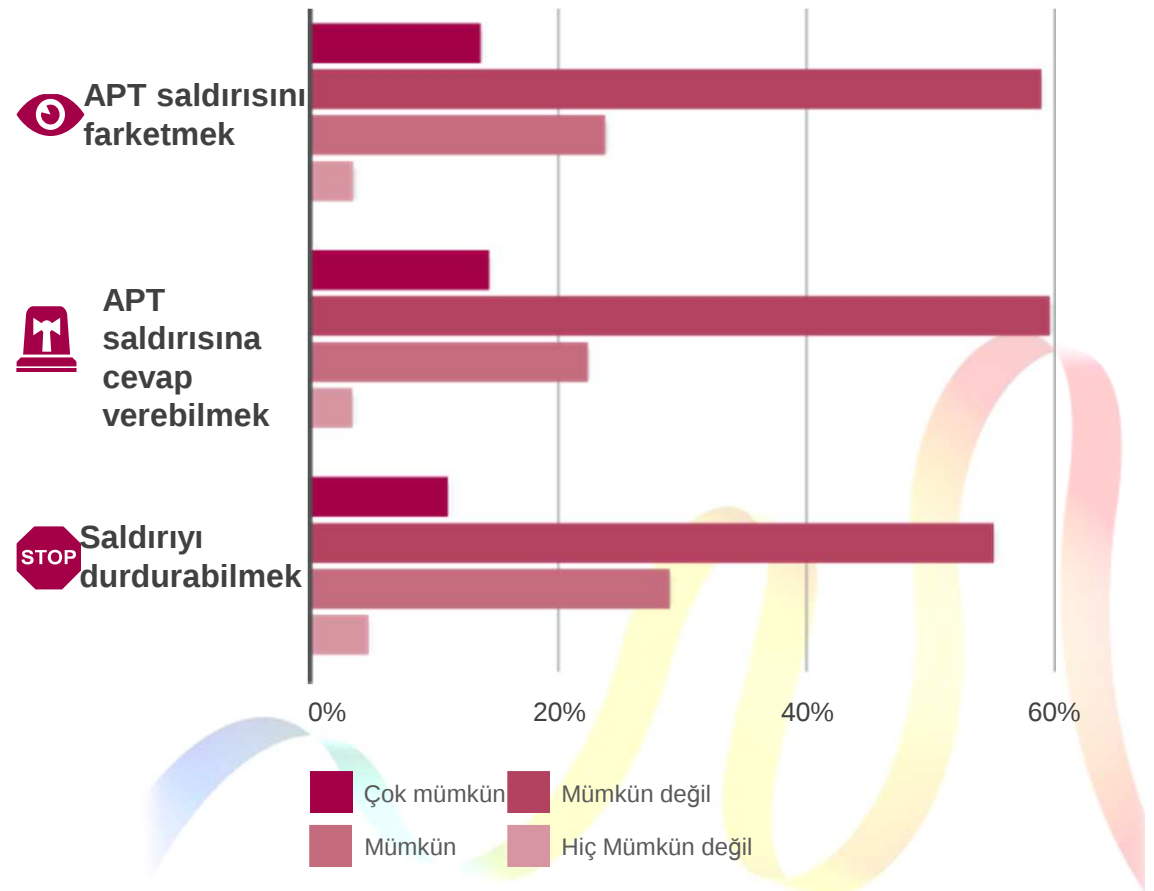
ISACA APT ANKETİ

60% a kadar katılımcıların 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 savaşılabılır?

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

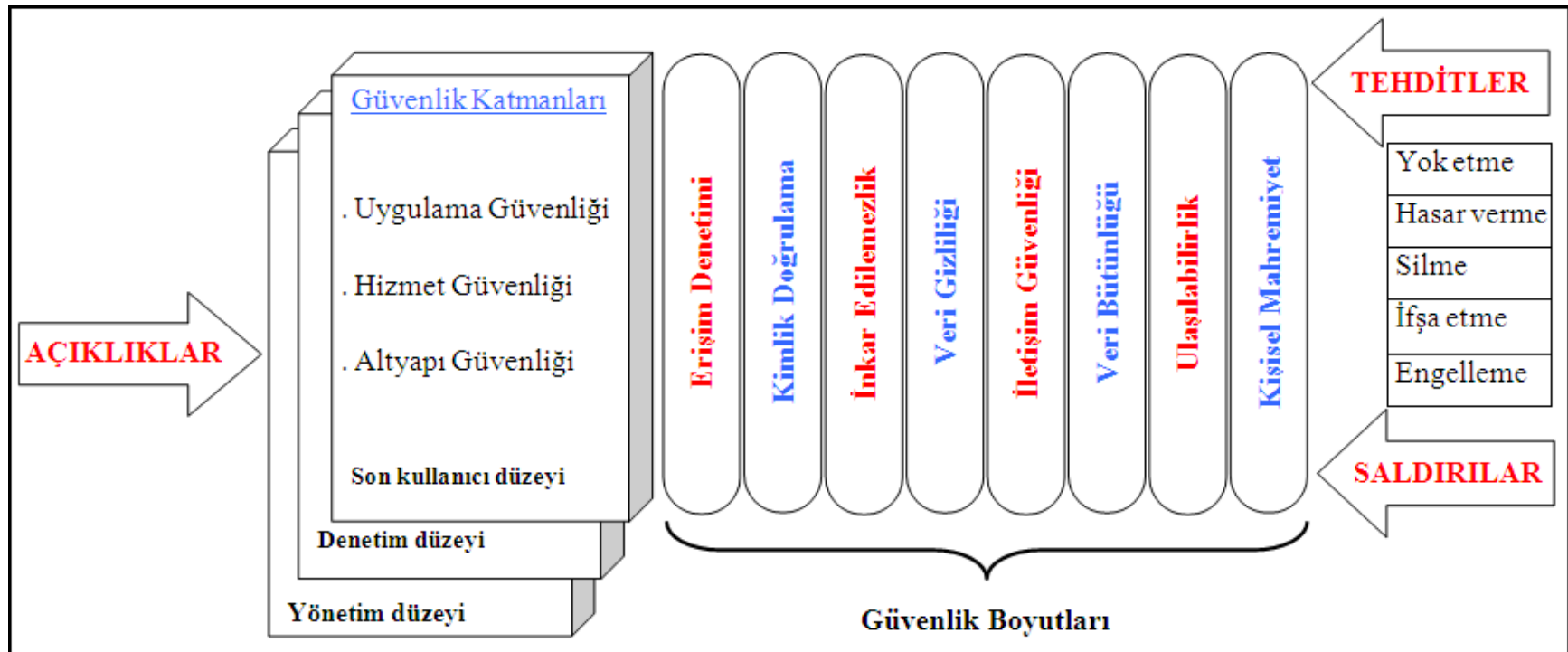
ÖNLEMLER

- ❑ **Avrupa Birliği ve Siber Güvenlik Koruma Birliği tarafından desteklenen projeye 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

*“3. Dünya Savaşının nasıl olacağını
bilmiyorum ama 4. Dünya Savaşının taş
ve sopalarla olacağını biliyorum.”*

Albert Einstein

REVOLUTION

GELİŞMİŞ SİBER SİLAHLAR

Kaynaklar ve Referanslar

- ❑ Cisco Systems, *Cybersecurity*, Peter Romness Gary Osland Cisco Systems Inc. Business Development Cybersecurity - U.S. Public Sector 2013
- ❑ Ozan UÇAR, *Bilgi Güvenliği Akademisi*, *Advanced Persistent 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