AYDIN BAYCAN
360109001
Meslek Matematiği

ICMP KEŞİF SALDIRILARI, GÜVENLİK RİSKLERİ VE SALDIRI YÖNTEMLERİ, SIR: SECURITY INTELLIGENCE REPORT

GÜNDEM

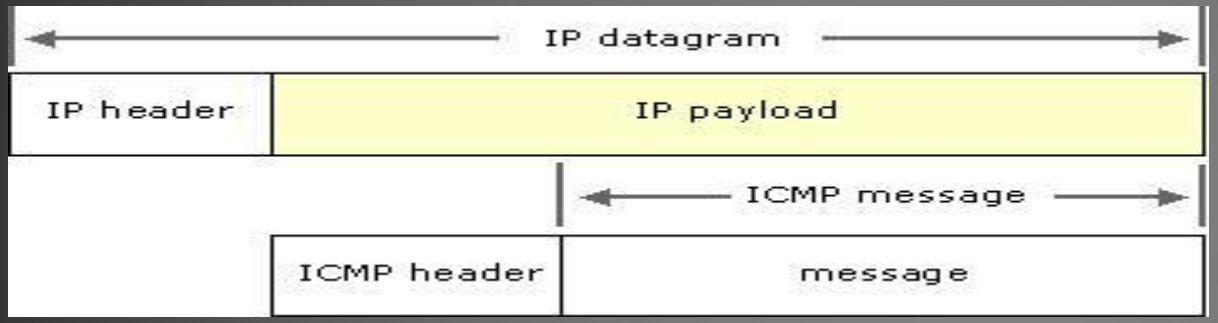
- •ICMP Nedir?
- •ICMP Keşif Saldırılarına Giriş
- •Sunucu Tespiti
- •Ağ Topolojisinin Tespiti
- •Güvenlik Duvarı Kurallarının Tespiti (“Firewalk”)
- •Ters Eşleme (“Inverse Mapping”)
- •Erişim Kontrol Listesi Tespiti
- •Protokol / Port Taraması
- •İşletim Sistemi Tanıma
- •ICMP Tüneli
- •Korunma Yolları ve Önlemler
- •Sonuç

1.BÖLÜM

ICMP Nedir? - I

- **ICMP (Internet Control Message Protocol)**

–IP protokol takımının bir parçası (RFC792)



- **İki Temel Görevi Bulunur:**

–Sürekli hata durumlarının bildirilmesi

–Ağ ile ilgili genel özellikleri saptamak üzere, istek ve cevap mesajlarıyla ağın araştırılması

ICMP Nedir? – II

ICMP Mesaj Çeşitleri:

–ICMP Hata Mesajları

- Destination Unreachable, Redirect, vs...

Table 1-3. Internet Control Message Protocol - Destination Unreachable Message

0										1										2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Type										Code										Checksum											
Unused																															
Internet header + 64 bits of original data datagram																															

–ICMP Sorgu Mesajları

- Echo Request-Reply, Timestamp Request-Reply

Table 1-5. Internet Control Message Protocol - Information Request/Information Reply Message

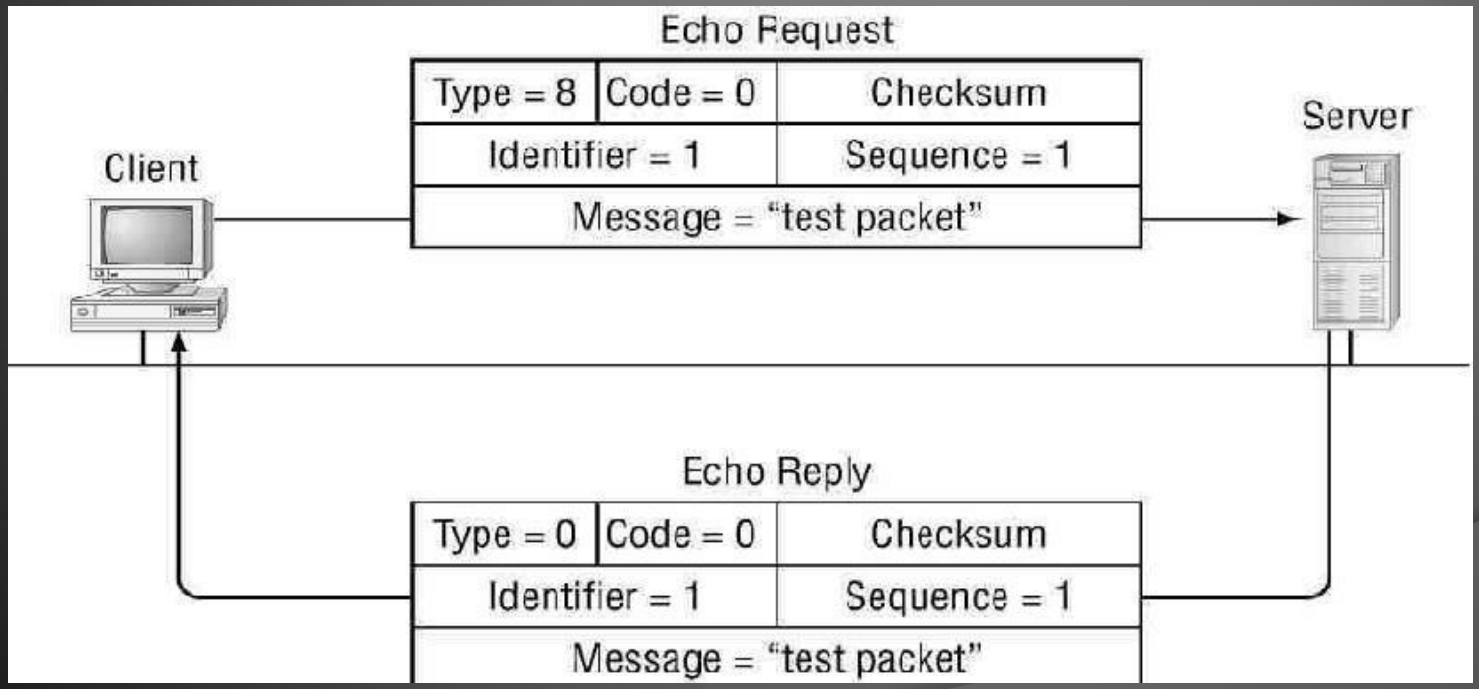
0										1										2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Type										Code										Checksum											
Identifier																				Sequence Number											

ICMP Keşif Saldırılarına Giriş

- **Keşif Saldırılarının Amacı:**
  - –Hedef sistemler hakkında bilgi elde etmek
  - –Bu bilgileri kullanarak hedef sistemlere etkin saldırılar düzenlemek
  - –Sistemde fark edilmeden dışarısı ile iletişimde bulunmak (ICMP Tunneli)
- **Keşif Saldırılarının Yöntemi:**
  - –Mesaj başlık kısımlarında değişiklik yapmak
  - –ICMP mesajlarını amaçları dışında kullanmak

Sunucu Tespiti - I

- **Tespit Yöntemi:**
  - –ICMP Echo Request mesajı gönderilir
  - –Karşılığında ICMP Echo Reply mesajı beklenir



Sunucu Tespiti - II

Sunucu tespit çeşitleri:

–ICMP/ Ping taraması (“ICMP/ Ping Sweep”)

- Tek tek sunucu IP adreslerine gönderilir.

–ICMP Yayınlama (“Broadcast ICMP”)

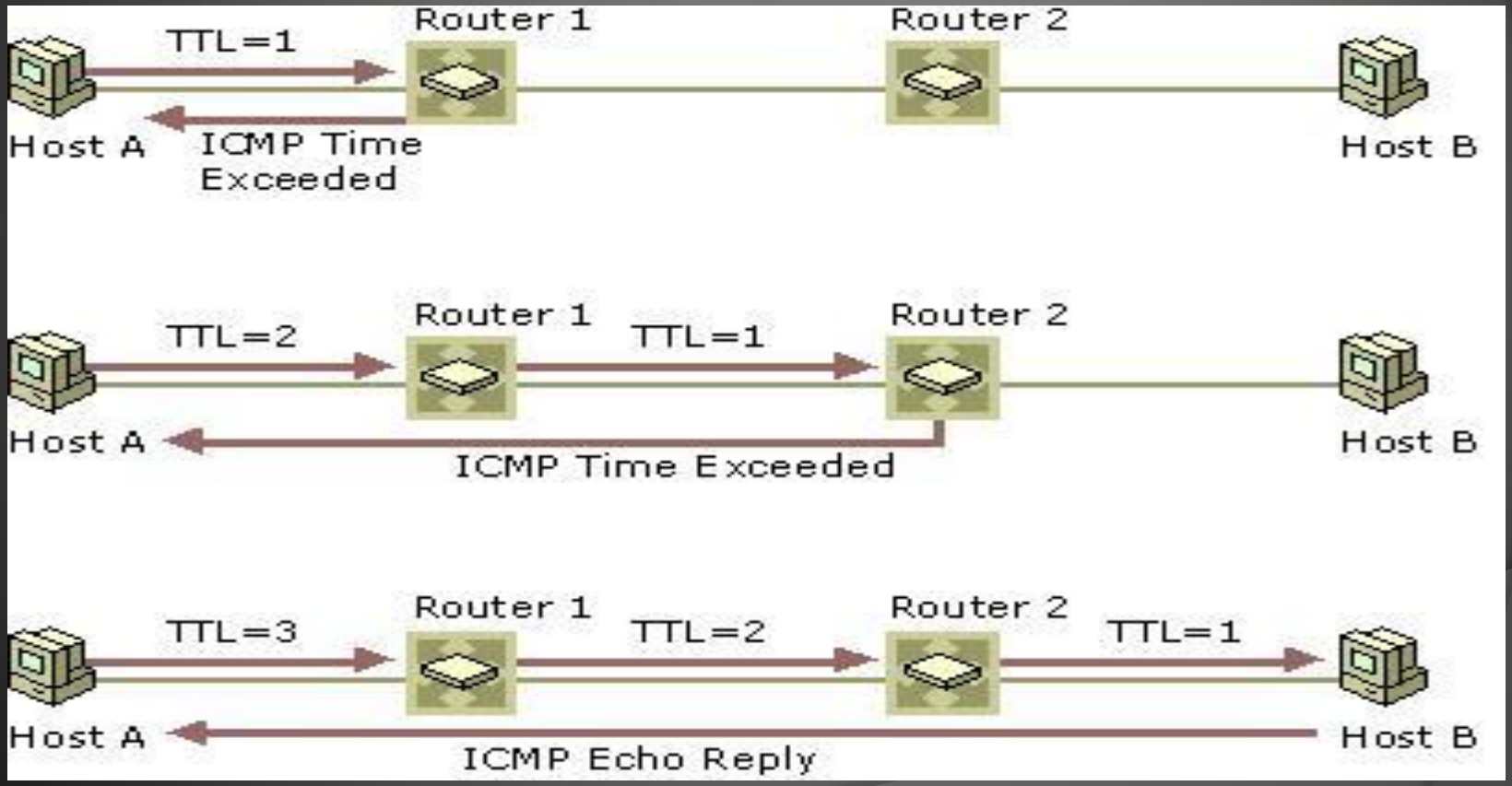
- Tüm ağın yayın (“broadcast”) adresine gönderilir.
- Not: Windows ve diğer bazı işletim sistemleri, yayın adresinden gelen ICMP mesajlarına cevap vermezler.

Ağ Topolojisinin Tespiti - I

- "Traceroute" komutu kullanılır (Windows için "tracert"), gerçekleştirimi şu şekildedir:
  - ICMP Echo Request mesajları (Windows için) gönderilir.
  - Her mesajda TTL ("Time-to-Live") değeri birden başlayarak birer birer arttırılır.
  - Yol boyunca ICMP Time Exceeded mesajı geri döndüren sunucu/ yönlendirici tespit edilir.

Ağ Topolojisinin Tespiti - II

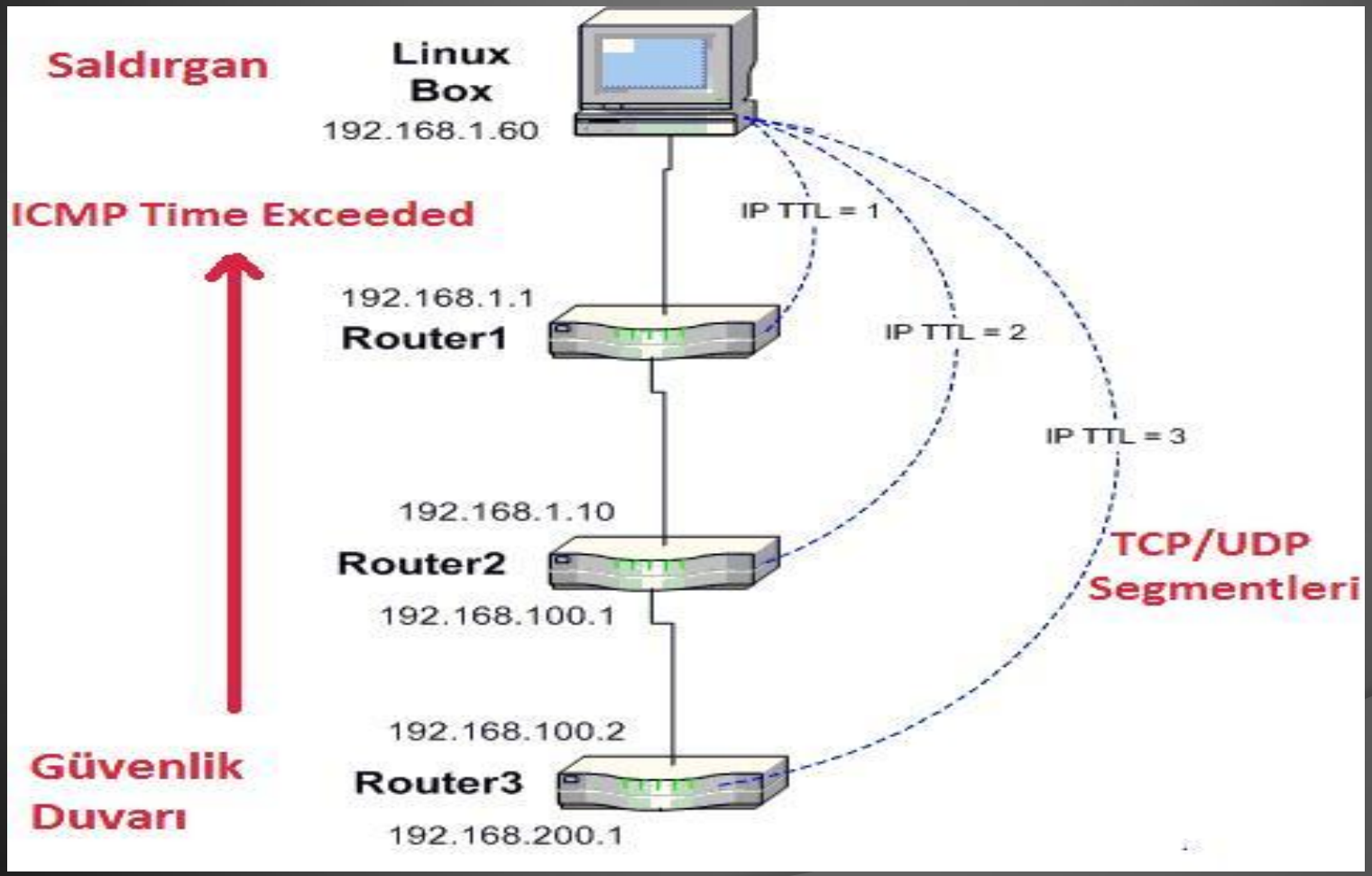
Örnek gösterim:



Güvenlik Duvarı Kurallarının Tespiti (“Firewalk”) - I

- **İki aşamada gerçekleştirilir:**
- –1. aşamada:
  - Saldırgan ile güvenlik duvarı arasındaki sunucu/yönlendirici (“hop”) sayısı tespit edilir (“traceroute”).
- –2. aşamada:
  - Arada yer alan sunucu/yönlendirici sayısından 1 büyük TTL değeri belirlenir.
  - Bu TTL değerine sahip farklı port kombinasyonlarında TCP/UDP segmentleri gönderilir
  - ICMP Time Exceeded mesajı geri döndüren segment portlarının açık olduğu anlaşılır.

Güvenlik Duvarı Kurallarının Tespiti (“Firewalk”) - II



Ters Eşleme

Güvenlik duvarının veya yönlendiricinin arkasındaki belirli bir IP aralığı için,

–ICMP Echo Request mesajları gönderilir

–ICMP Host Unreachable mesajı döndüren IP adresleri toplanır

–ICMP Host Unreachable mesajı döndürmeyen IP adreslerinde sunucu varlığı tespit edilir.

Not: Durum denetimli (“stateful”) güvenlik duvarları dışarıdan gelen ICMP Echo Request mesajlarını engeller, içeriden gidene izin verir.

Erişim Kontrol Listesi Tespiti - I

•Erişim kontrol listelerinin tespiti için:

–Uzunluk (“Total Length”) gerçek değerinden büyük bir değere sahip IP paketi oluşturulur.

–Bu IP paketi içinde belirli bir port numarasında TCP/UDP segmentleri sarmalanır.

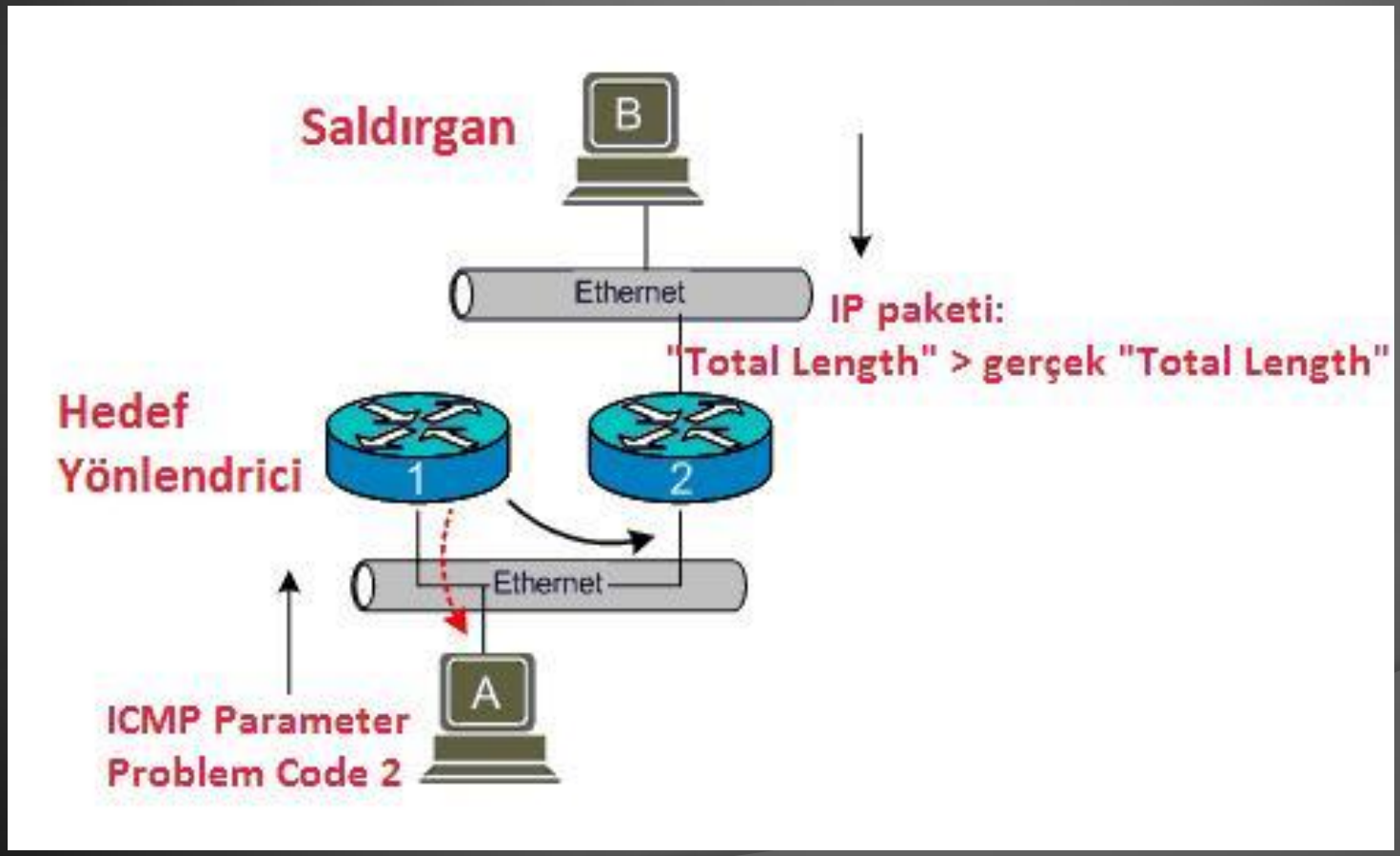
–Bu IP paketini alan hedef sunucu, paketi açarken uzunluk sorunu ile karşılaşır.

–Saldırgana “ICMP Parameter Problem Code 2” mesajı döndürülen port ve protokollerin açık olduğu tespit edilir.

–Tüm ağ ve port/servis kombinasyonları için tekrarlanması durumunda tüm liste elde edilir.

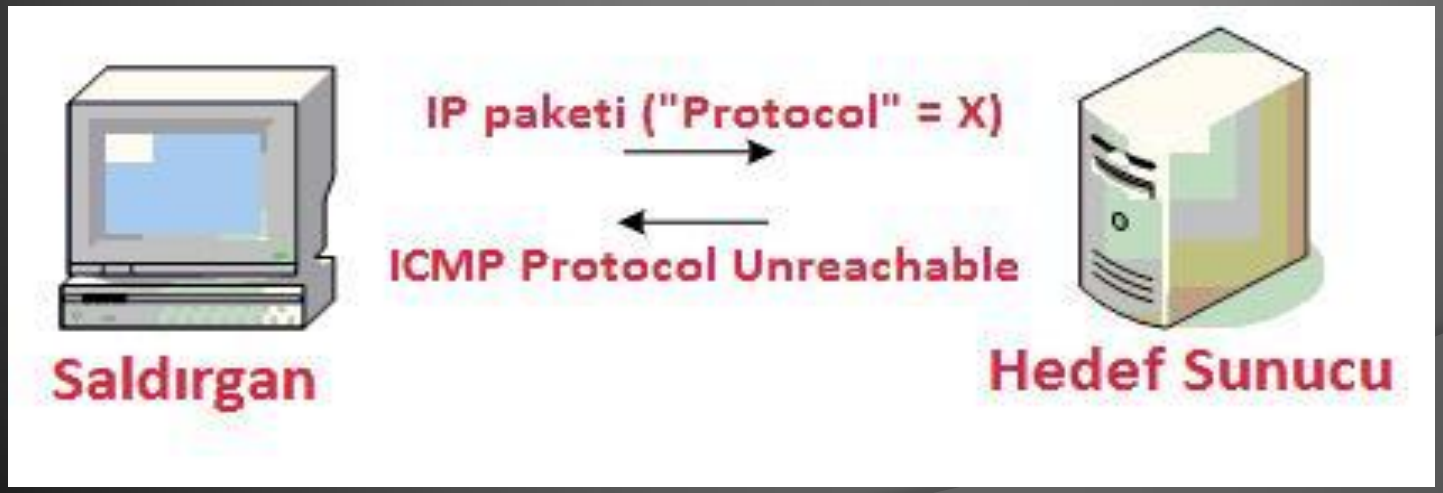
Erişim Kontrol Listesi Tespiti - II

Örnek Gösterim:



Protokol/Port Taraması

- **Hedef bir sunucuda çalışan servisler için:**
  - –IP paketi içindeki 8 bitlik protokol alanı seçilen protokol değeri ile gönderilir.
  - –ICMP Protocol/Port Unreachable mesajı geri dönülmemişse açık olduğu anlaşılır.



İşletim Sistemi Tanıma (“OS Fingerprinting”) - I

•İşletim sistemleri, ağ trafiğini yönetmede birbirlerinden farklılaşmışlardır.

– Bu sayede, hedef sunucunun işletim sistemi ve sürümü çıkartılabilir.

•İşletim sistemi tanım yöntemleri

–Aktif tanıma

•Hedef sunucuya aktif olarak mesaj gönderilip alınır

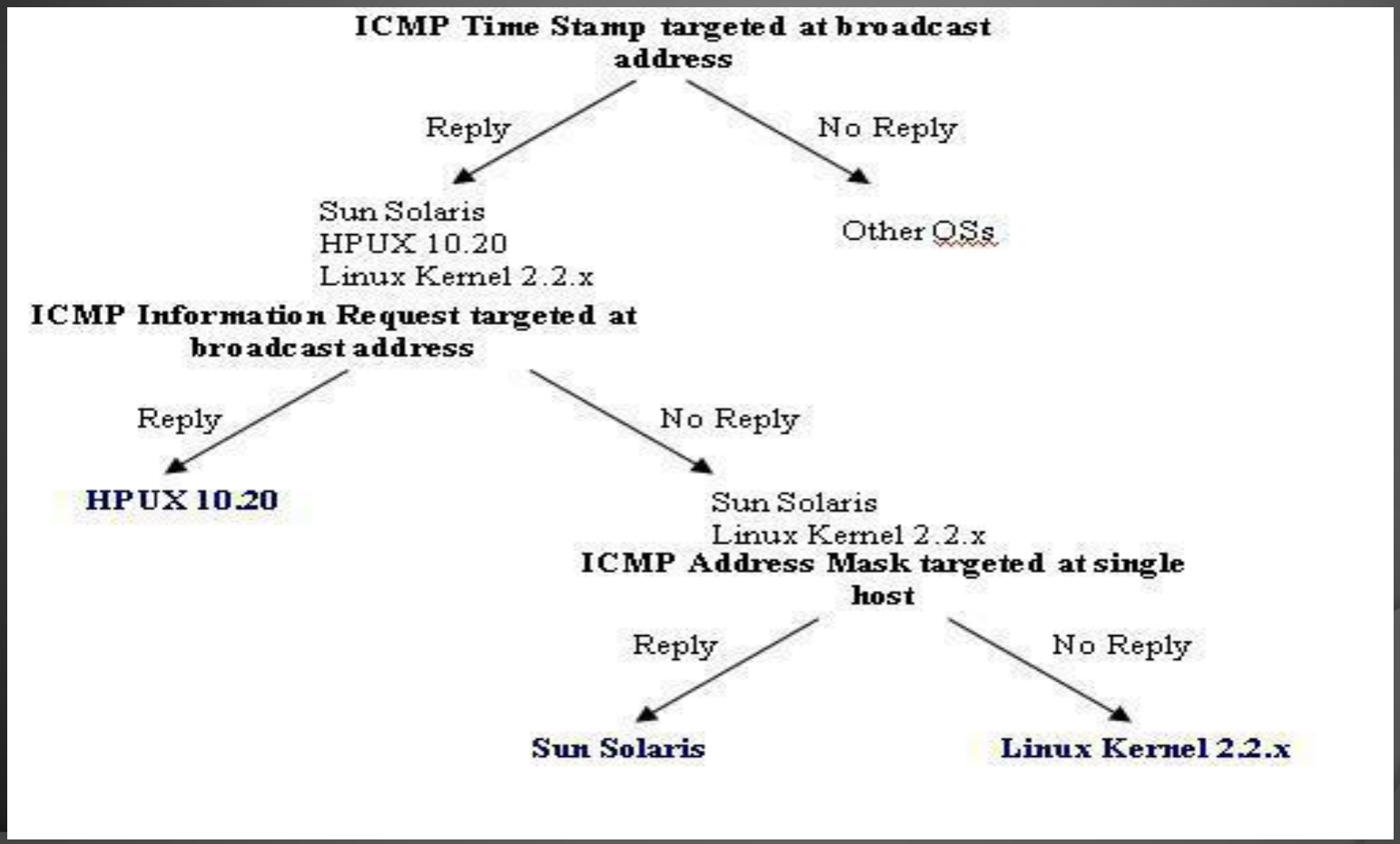
–Pasif tanıma

•Hedef sunucunun ağ iletişimi dinlenir, etkileşim yok

•Aktif tanımaya göre iz bırakmaz ama daha zor

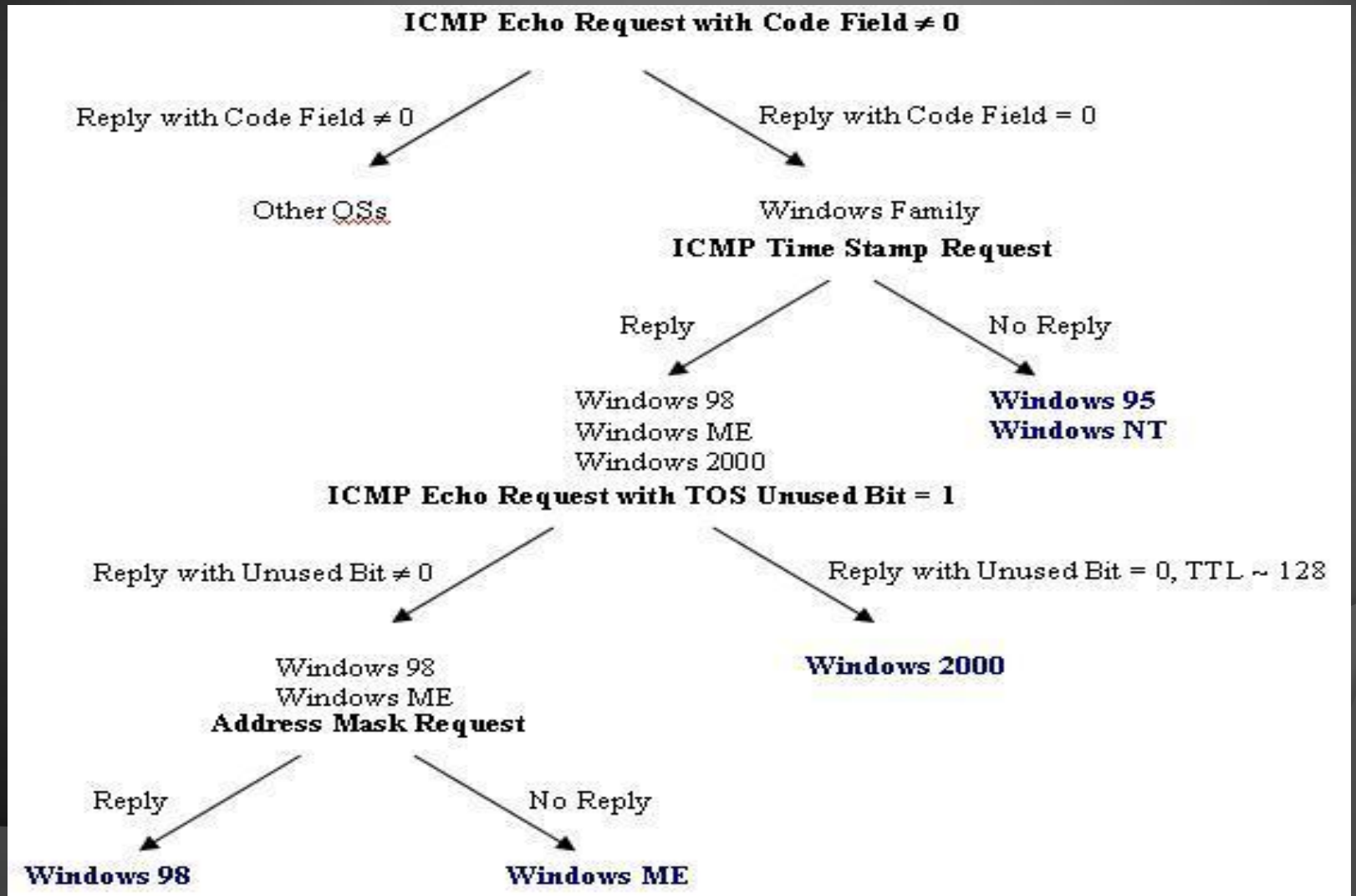
İşletim Sistemi Tanıma ("OS Fingerprinting") - II

- Linux işletim sistemi için örnek gösterim:



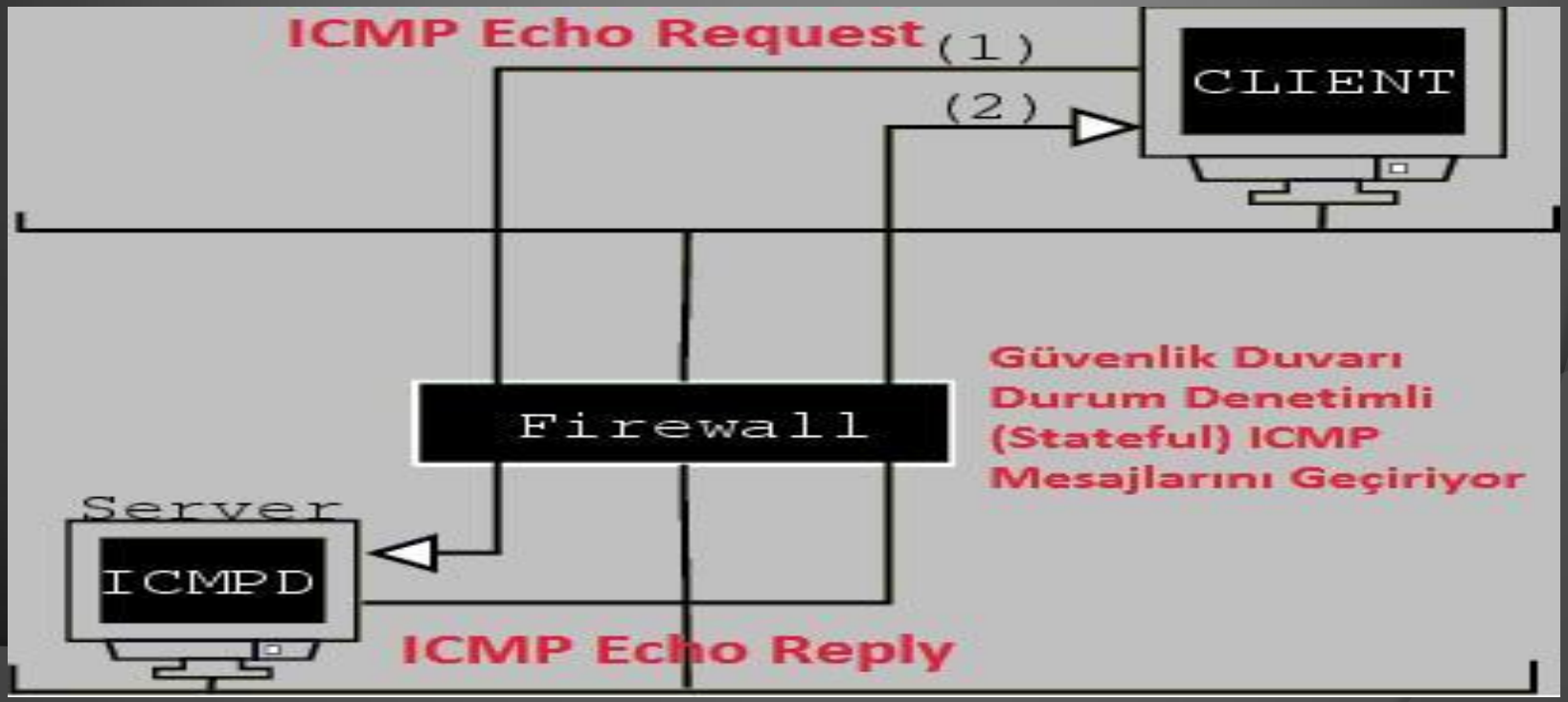
İşletim Sistemi Tanıma ("OS Fingerprinting") - III

- Windows işletim sistemi için gösterim:



ICMP Tüneli

•ICMP Echo Request mesajlarının veri alanı ("Payload") kısmına bilgi saklanarak gizli iletişim sağlanabilir.



Korunma Yolları ve Önlemler

- İnternetten iç ağa ICMP trafiği engellenmeli
- İç ağdan dışarıya, durum denetimli (“stateful”) olarak ICMP istek mesajlarına izin verilebilir.

–ICMP hata mesajlarının dışarı çıkışına izin verilmemeli

- İç ağ içinde ICMP istekleri (ping &traceroute) sınırlandırılmalı

–Sadece belirli bir yönetim sunucusu veya ağı içinden ağ araştırılabilmeli

Sonuç

•ICMP mesajları kötü amaçlarla kullanılması ve yeterli denetim uygulanmadığı durumlarda sistemler tehlike altındadır.

•Modern güvenlik duvarları, durum denetimli ve dinamik filtreleme ile İnternetten gelen trafiği engelleyebilir.

•En büyük tehlike iç ağda (LAN), güvenlik duvarı arkasında yapılacak keşiflerdir

–Trojan, virüs yüklü veya bot (“zombie”) bilgisayarlar yoluyla iç ağ ortaya çıkarılabilir.

2.BÖLÜM
Güvenlik Riskleri ve Saldırı Yöntemleri
Sunu İçeriği

Sunu İçeriği:

- Bilgi Güvenliği Kavramı ve Kapsamı
- Risk ve Tehditler
- Saldırı ve Saldırgan Kavramları / Gelişimleri
- Saldırgan Amaçları ve Ağdaki Hedefler
- Saldırı Yöntemleri ve Önlemler
- Görülebilecek Zararın Boyutu
- Genel Güvenlik Önlemleri

Bilgi Güvenliği Kavramı(IT Security)

Bilişim ürünleri/cihazları ile bu cihazlarda işlenmekte olan verilerin bütünlüğü ve sürekliliğini korumayı amaçlayan çalışma alanıdır.

Bilgi Güvenliğinin Amacı

- Veri Bütünlüğünün Korunması
- Erişim Denetimi
- Mahremiyet ve Gizliliğin Korunması
- Sistem Devamlılığının Sağlanması

Tehdit Türleri

Dahili Tehdit Unsurları

-Bilgisiz ve Bilinçsiz Kullanım

- Kötü Niyetli Hareketler

~ % 80

Harici Tehdit Unsurları

-Hedefe Yönelmiş Saldırılar

-Hedef Gözetmeyen Saldırılar

~ % 20

Dahili Tehdit Unsurları

- Bilgisiz ve Bilinçsiz Kullanım:

-Temizlik Görevlisinin Sunucunun Fişini Çekmesi

-Eğitilmemiş Çalışanın Veritabanını Silmesi

- Kötü Niyetli Hareketler:

-İşten Çıkarılan Çalışanın, Kuruma Ait Web Sitesini Değiştirmesi

-Bir Çalışanının, Ağda "Sniffer" Çalıştırarak E-postaları Okuması

-Bir Yöneticinin, Geliştirilen Ürünün Planını Rakip Kurumlara Satması

Harici Tehdit Unsurları

- **Hedefe Yönelmiş Saldırılar:**

-Bir Saldırganın Kurum Web Sitesini Değiştirmesi
-Bir Saldırganın Kurum Muhasebe Kayıtlarını Değiştirmesi
-Birçok Saldırganın Kurum Web Sunucusuna Hizmet
-Aksatma Saldırısı Yapması

- **Hedef Gözetmeyen Saldırılar:**

-Virüs Saldırıları (Melissa, CIH – Çernobil, Vote)
- Worm Saldırıları (Code Red, Nimda)
- Trojan Arka Kapıları (Netbus, Subseven, Black Orifice)

Saldırı Kavramı

- Kurum ve şahısların sahip oldukları tüm değer ve bilgilere izinsiz erişmek, zarar vermek,maddi/manevi kazanç sağlamak için bilişim sistemleri kullanılarak yapılan her türlü hareket dijital saldırı olarak tanımlanabilir.

Saldırgan Türleri

- Profesyonel Suçlular →
- Genç Kuşak Saldırganlar →
- Kurum Çalışanları →
- Endüstri ve Teknoloji Casusları →
- Dış Ülke yönetimleri →

Saldırgan Motivasyonu

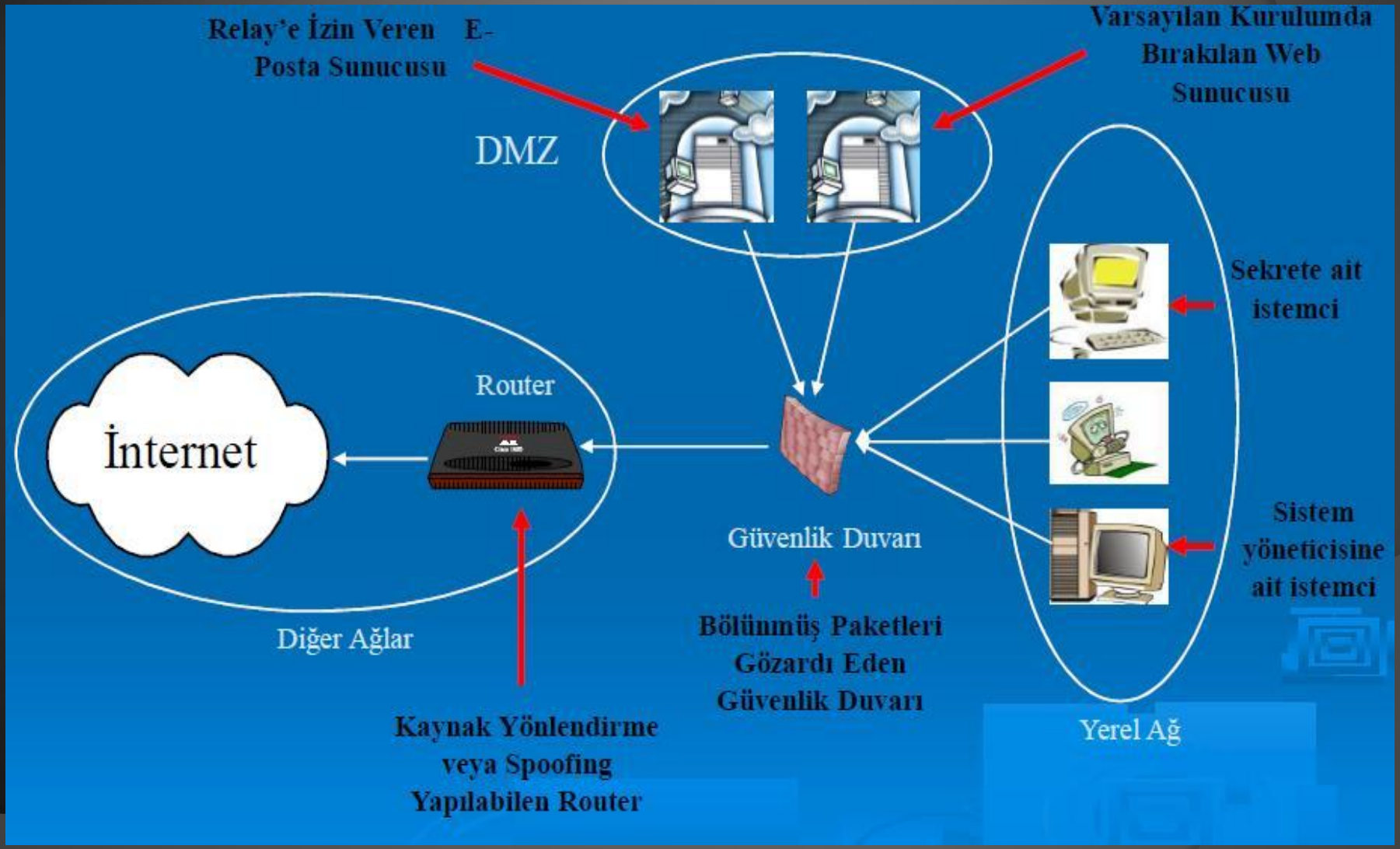
- Maddi Menfaatler
- Rekabet Avantajı

-Politik

-Ekonomik/Ticari

- Ek Kaynaklara Erişme İsteği
- Kişisel Öfke veya İntikam
- Merak veya Öğrenme İsteği
- Dikkatsiz Davranışlar

Ağda Bulunan ve Potansiyel Risk İçeren Sistemler



Saldırı Yöntemleri

- Hizmet Aksatma Saldırıları
- Dağıtık Hizmet Aksatma Saldırıları
- Ticari Bilgi ve Teknoloji Hırsızlıkları
- Web Sayfası İçeriği Değiştirme Saldırıları
- Kurum Üzerinden Farklı Bir Hedefe Saldırmak
- Virüs , Worm , Trojan Saldırıları
- İzinsiz Kaynak Kullanımı

Saldırılarda Sıkça Kullanılan Teknikler

- Sosyal Mühendislik
- Ağ Haritalama
- Uygulama Zayıflıkları
- Yerel Ağ Saldırıları
- Spoofing
- Hizmet Aksatma Saldırıları (Dos , DDos)
- Virüs, Worm , Trojan Kullanımı

Sosyal Mühendislik

- İnsan ilişkilerini veya insaların dikkatsizliklerini kullanarak kurum hakkında bilgi toplamak olarak tanımlanabilir.
- Amaç kurum yapısı, kurumsal ağın yapısı, çalışanların/yöneticilerin kişisel bilgileri,şifreler ve saldırıda kullanılabilecek her türlü materyalin toplanmasıdır.
- Kuruma çalışan olarak sızmak, çalışanlarla arkadaş olmak, teknik servis yada destek alınan bir kurumdan arıyormuş gibi görünerek bilgi toplamak, bilinen en iyi örnekleridir.

Sosyal Mühendislik – Önleme Yöntemleri

- Telefonda kuruma ait bilgiler, karşıdaki kişinin doğru kişi olduğuna emin olmadan verilmemelidir
- Çalışanları kuruma dahil ederken özgeçmişleri, alışkanlıkları ve eğilimleri mutlak incelenmelidir
- Kurum çöpleri (büro malzemeleri, not kağıtları, bordolar vs.) tamamen kullanılmaz hale getirilmeli daha sonra atılmalıdır
- Sistem yöneticilerinin, kurumsal bilgileri posta listelerinde, arkadaş ortamlarında ve benzeri yerlerde anması önlenmelidir
- Önemli sunuculara fiziksel erişimin olduğu noktalarda biometrik doğrulama sistemleri (retina testi, parmak izi testi vs.) ve akıllı kart gibi harici doğrulama sistemleri kullanılmalıdır

Ağ Haritalama

- Hedef ağda bulunan bileşenleri ve bu bileşenlere erişim haklarını saptamak için yapılmaktadır
- Aktif sistemlerin belirlenmesi, işletim sistemlerinin saptanması, aktif servislerin belirlenmesi ve bu bileşenlerin ağ üzerindeki konumlarının belirlenmesi gibi aşamalardan oluşur.
- Saldırgan, hedef ağın yöneticisi ile aynı bilgi seviyesine ulaşana kadar bu süreç devam etmektedir.
- Otomatize edilmiş yazılımlar ile yapılabilmektedir.

Ağ Haritalamada Ulaşılmak İstenen Bilgiler

- Hedef ağdaki tüm bileşenler.
- Hedef ağa ait olan alan adı, IP aralığı ve internet erişim hattının ait olduğu kurumlar, kişiler, bitiş süreleri.
- Hedef ağdaki aktif bileşenlerin işletim sistemleri, sürümleri,yama seviyesi.
- Sunucu sistemler üzerinde çalışan servisler,kullanılan uygulamalar ve yama seviyeleri.
- Hedef ağdaki tüm bileşenlere ve servislere erişim haklarının belirlenmesi.
- Hedef ağdaki tüm güvenlik uygulamaları, erişim listeleri, sürümleri, yama seviyeleri.
- Hedef ağdaki aktif bileşenlerin ağdaki yerleşimi.

Ağ Haritalamada Kullanılan Teknikler

- Sosyal Mühendislik
- Ping Taraması (Ping Sweep)
- Port Tarama (Port Scanning)
- İşletim Sistemi Saptama (Os Fingerprinting)
- Servis Açılış Mesajlarını Yakalama (Banner Grabing)
- Yol Haritası Belirleme (Tracerouting)
- Güvenlik Duvarı Kural Listesi Belirleme(Firewalking)
- Saldırı Tespit Sistemi Saptama/İnceleme

Ağ Haritalama – Önleme Yöntemleri

- Güvenlik Duvarı üzerinde, ağın devamlılığı için gerekli olmayan, internetten ağa yönelik her türlü IP paketini engelleyecek kurallar belirlemek.
- Güvenlik Duvarını uygulama seviyesinde kullanmak veya ağdaki işletim sistemlerini ele vermeyecek şekilde yapılandırmak.
- Güvenlik Duvarı üzerinde, ağdaki bileşenlerden, internetteki sistemlere ICMP hata mesajları gönderilmesini engellemek.
- Sunucu ve servis sunan uygulamalardaki tüm açılış/hata mesajlarını değiştirmek, yok etmek.
- Saldırı Tespit Sistemlerini gerekli olmadıkça tepki vermeyecek şekilde yapılandırmak.

Uygulama Zayıflıkları

- Servis sunan uygulamalardaki yapılandırma yada programlama hatası sebebiyle oluşur ve sistemde komut çalıştırmaya yada servisin durdurulmasına sebebiyet verir.
- Varsayılan yapılandırmayı kullanmak, zayıf şifreler belirlemek ve erişim hakları belirlememek en çok karşılaşılan yanlış yapılandırma örnekleridir.
- Klasör dışına geçebilmek, bellek taşırmak, yazılımda erişim sınırlaması bulundurmamak ve normal dışı isteklere karşı önlem almamak ise en sık karşılaşılan programlama hatalarıdır.

Uygulama Zayıflıkları – Önleme Yöntemleri

- Uygulamaların yeni sürümlerini kullanmak, yayınlanan tüm yamaları uygulamak
- Varsayılan yapılandırmayı değiştirmek ve kuruma/servise özel bir yapılandırma benimsemek
- Kolay tahmin edilemeyecek şifreler seçmek ve uygulamaya özel erişim haklarının belirlenmesini sağlamak.
- Uygun şekilde yapılandırmak şartıyla, uygulama seviyesinde güvenlik duvarları, uygulama geçitleri ve saldırı tespit sistemleri kullanmak

Yerel Ağ Saldırıları

- Yerel ağda bulunan kullanıcıların, sahip oldukları hakları kötü niyetli kullanması sonucu oluşmaktadır.
- Amaç genelde diğer çalışanların e-postalarını okumak, yöneticilerin şifrelerini yakalamak, kuruma veya farklı bir çalışana ait bilgilerinin incelenmesi olmaktadır.
- Paket yakalamak, oturum yakalamak, oturumlara müdahale etmek en sık kullanılan saldırılardır.

Yerel Ağ Saldırılarında Kullanılan Teknikler

- Sniffer kullanarak paket yakalamak
- Switch'li ağlarda ARP Spoofing yaparak paket yakalamak.
- Yakalanan paketlerin ait olduğu oturumları yakalamak ve müdahale etmek.
- SSH ve SSL oturumlarını yakalamak, güvenli sanılan oturumlardan veri çalmak.

Yerel Ağ Saldırıları – Önleme Yöntemleri

- Hub kullanılan ağlarda Switch kullanımına geçmek.
- Switch'leri her porta bir MAC adresi gelecek şekilde yapılandırmak, kaliteli Switch'ler kullanarak MAC adresi tablosunun taşmamasını sağlamak.
- Ağ üzerindeki tüm istemcilerde statik ARP tabloları oluşturmak ve değişiklikleri izlemek.
- SSH / SSL kullanılan oturumlarda en yeni sürümleri ve en yeni şifreleme algoritmalarını kullanmak.
- Gerekli görülen durumlarda harici doğrulama sistemleri kullanmak.

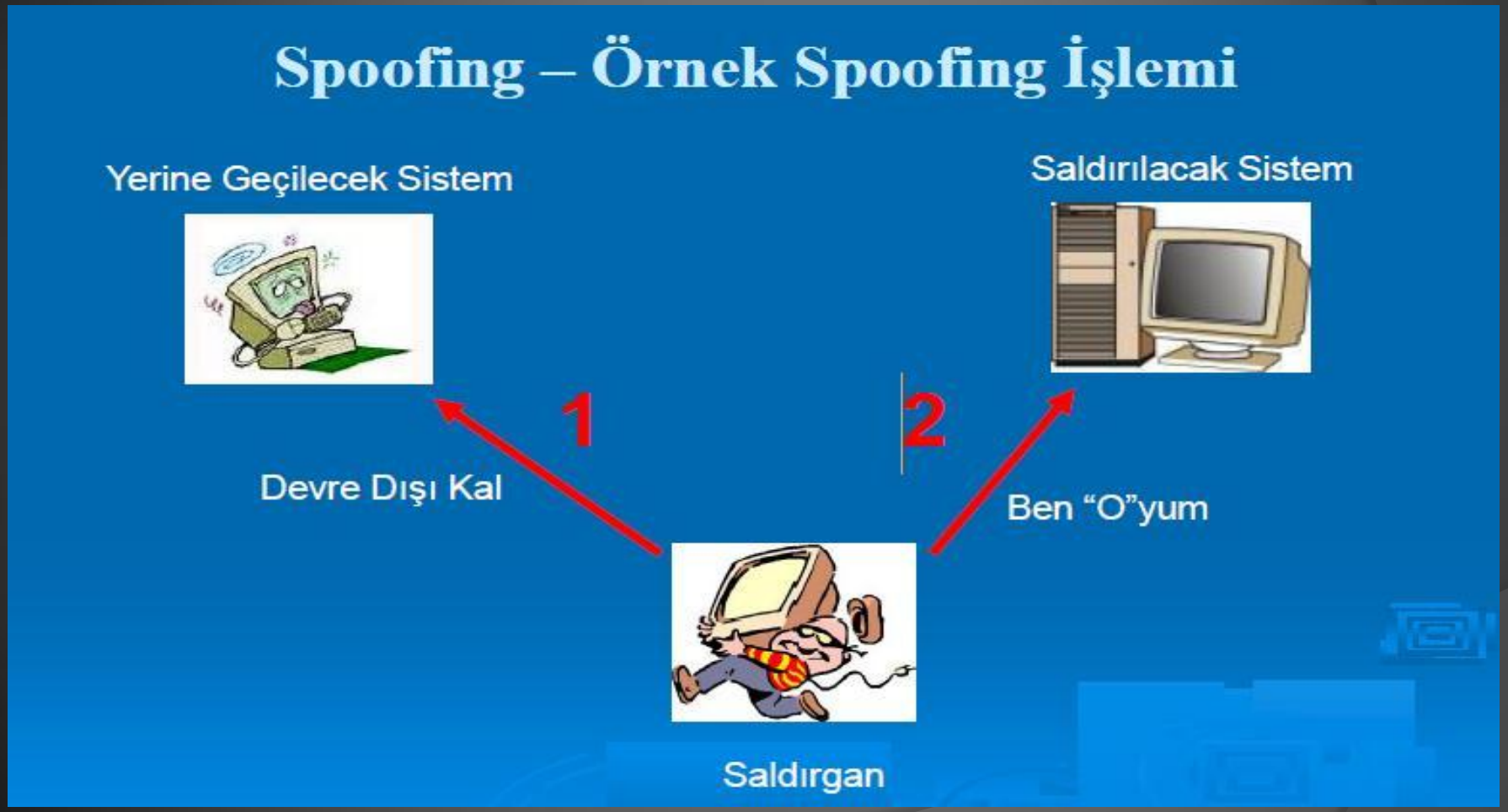
Spoofing

- Basitçe kaynak yanıltma olarak tanımlanabilir
- Genelde hedeften ek haklar kazanmak, saldırı suçundan farklı kişilerin/kurumların sorumlu olmasını sağlamak, kendini gizlemek veya dağıtık saldırılar düzenlemek için kullanılmaktadır.
- Çeşitli protokollerde, doğrulama sistemlerinde ve uygulamaya özel işlemlerde uygulanabilmektedir.

Spoofing Teknikleri

- MAC adreslerinin fiziki olarak değiştirilmesi veya ethernet paketlerindeki değişiklikler ile MAC Spoofing yapılabilir.
- ARP protokolündeki paketlerde IP/MAC adresleri eşleşmesini yanıltarak ARP Spoofing yapılabilir.
- IP Paketlerindeki kaynak IP adresini değiştirerek IP Spoofing yapılabilir.
- DNS sunucularını ele geçirerek veya sorgulara sahte cevaplar
- vererek DNS spoofing yapılabilir
- Web sunucudan alınmış cookie'nin kopyalanması suretiyle kimlik yanıltması yapılabilir.
- Parmak izi sistemlerinde, daha önce alınmış parmak izi örneği kullanılarak yapılabilir.

Spoofing – Örnek:



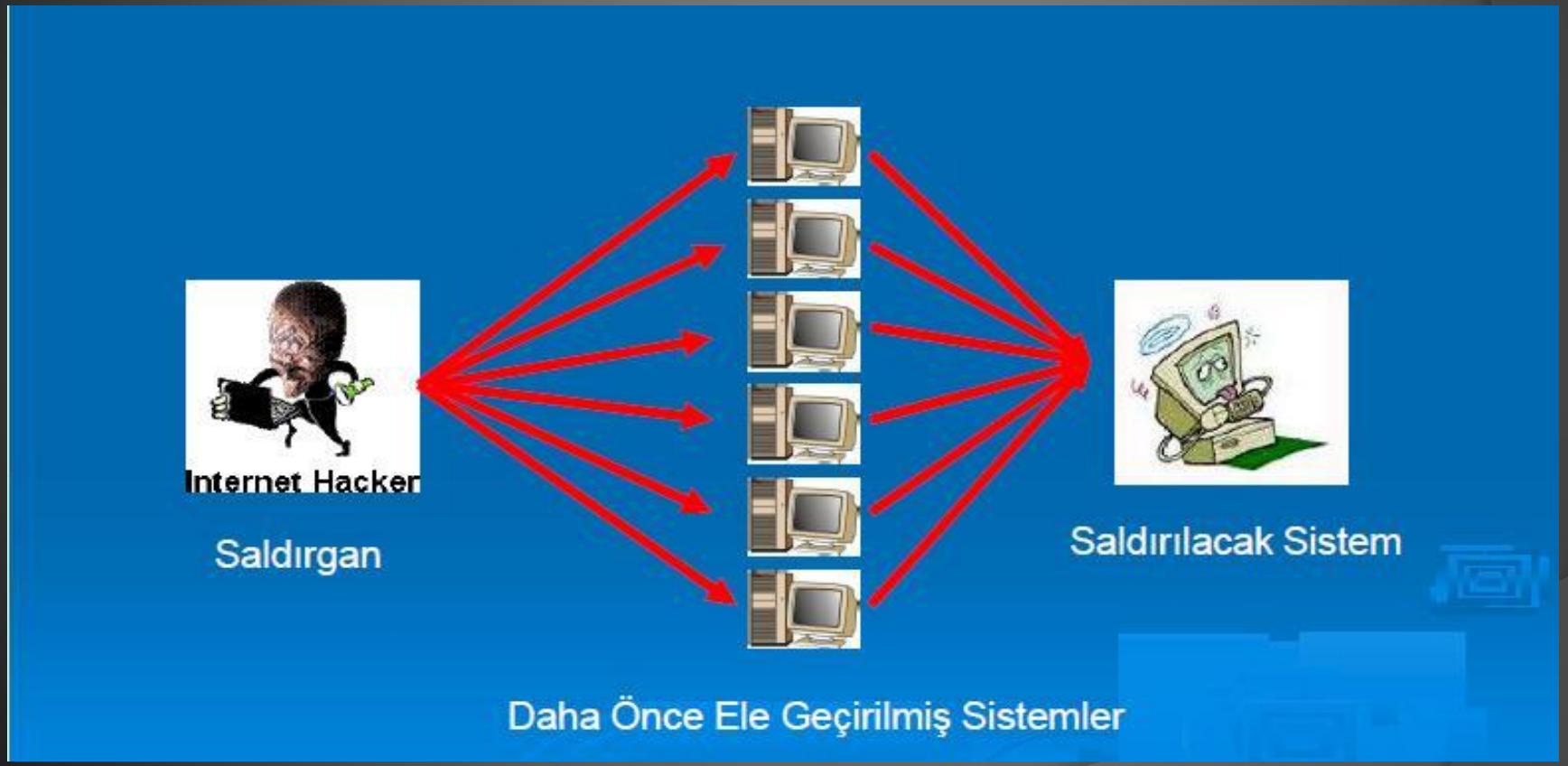
Spoofing – Önleme Yöntemleri

- Harici doğrulama sistemleri kullanmak
- IP, DNS, ARP, MAC adresleriyle doğrulama kullanan servisleri devre dışı bırakmak
- Statik ARP tabloları kullanmak, Switch'lerde her porta bir MAC adresi eşleşmesini sağlamak ve Swtich'leri tablo taşmalarından korumak.
- Ters sorguları aktif hale getirmek (RDNS, RARP vb.)
- Doğrulama bilgilerinin (şifre, dosyalar vb.) istemci sisteminde tutulmasını engellemek.

Hizmet Aksatma Saldırıları

- Protokol, işletim sistemi veya uygulamada bulunan zayıflıkların sonucunda,sunucunun servis veremez hale getirilmesidir.
- Hedef bir sunucu, servis, uygulama veya ağın devre dışı bırakılması olabilir.
- Tek merkezli yada çok merkezli olarak yapılabilir.

Dağıtık Hizmet Aksatma Saldırıları



Hizmet Aksatma Saldırıları – Önleme Yöntemleri

- Uygulama ve işletim sistemlerinin yayınlanmış tüm güncelleme/yamaları uygulanmalı, yeni sürümlerle hizmet verilmelidir.
- Uygulama seviyesinde güvenlik duvarları kullanılmalı ve uygulamalara yönelik tek merkezli saldırılar takip edilmelidir.
- Güvenlik Duvarı üzerinde, ağın devamlılığı için gerekli olmayan, internetten ağa yönelik her türlü IP paketini engelleyecek kurallar belirlenmelidir.
- Dağıtık saldırılardan korunmak için, internet servis sağlayıcısına iki yönlendirici ile bağlanılmalı ve biri devre dışı kaldığında diğeri devreye sokulmalıdır (Kısmi olarak çözüm sağlamaktadır).

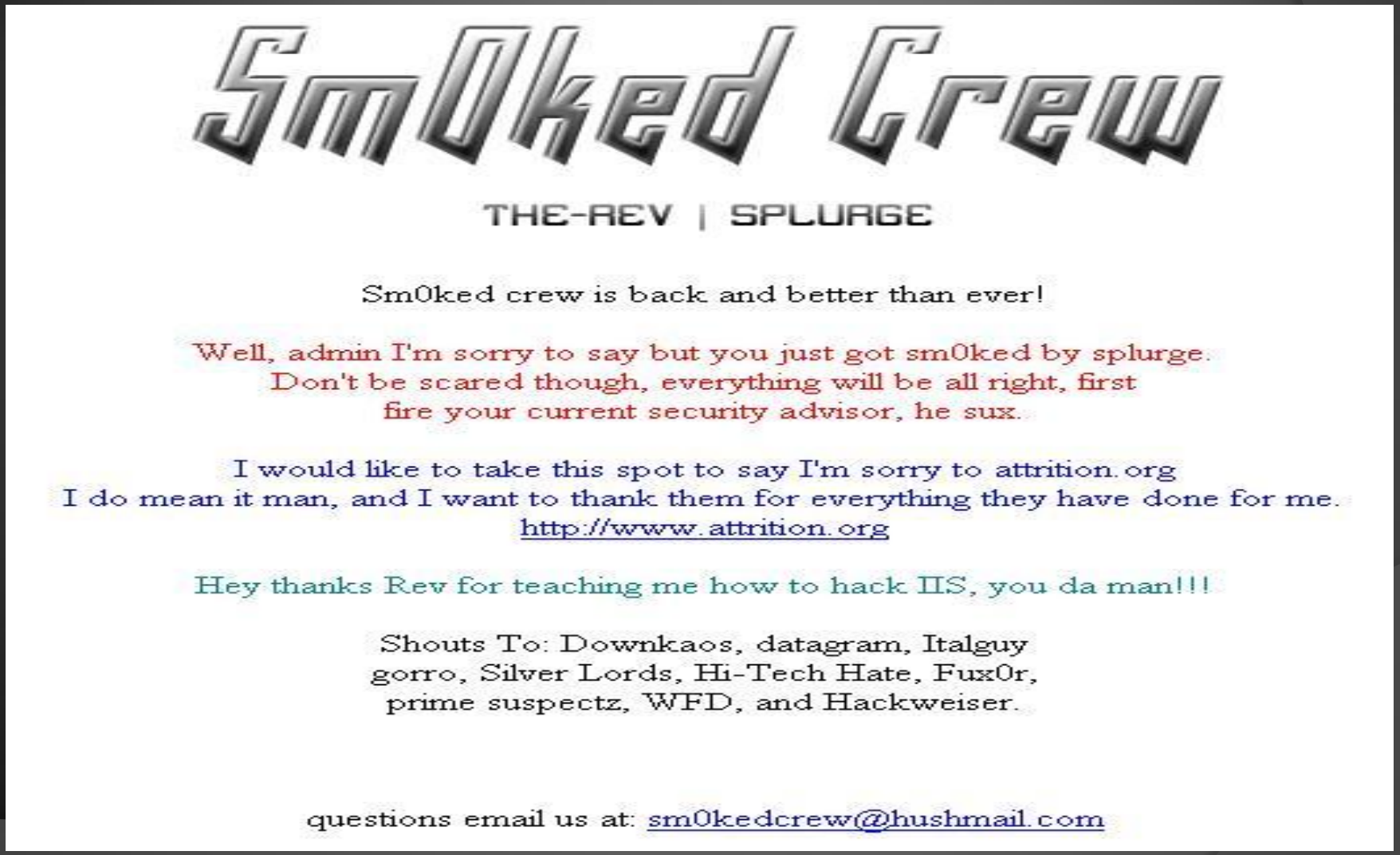
Virüs, Worm ve Trojan Tehlikeleri

- Virüs, Worm ve Trojan'lar hedef gözetmeksizin bulaşan ve genelde sistemin işleyişini durdurmaya çalışan küçük yazılımlardır.
- Virüs'ler e-posta, veri taşıma ortamları (disket, cd, dvd vb.) ve web sayfaları ile yayılabilir (Melisa, CIH).
- Worm'lar, Virüs'lerin kullandıkları yöntemlere ek olarak, uygulama/işletim sistemi zayıflıkları ile saldırılar düzenleyebilir ve bu şekilde de yayılabilir (Code Red, Nimda).
- Trojan'lar ancak ilgili uygulama çalıştırıldığında etkili olmaktadır (Netbus, Subseven)

Virüs, Worm ve Trojan'ları Önleme Yöntemleri

- Anti-Virüs sistemleri, tüm istemci ve sunucuları koruyacak şekilde kullanılmalıdır.
- Worm saldırılarını engelleyebilmek için Saldırı Tespit Sistemleri (eğer mümkün ise Güvenlik Duvarı)üzerinde önlemler alınmalıdır.
- İnternet üzerinden kurumsal ağa gelen FTP, HTTP, SMTP, POP3, IMAP gibi protokollere ait paketler Anti Virüs sistemleri tarafından incelenmeli,mümkün ise Anti Virüs ağ geçidi kullanılmalıdır.

Web Sayfası Değişimleri – NY Times 15/2/2001



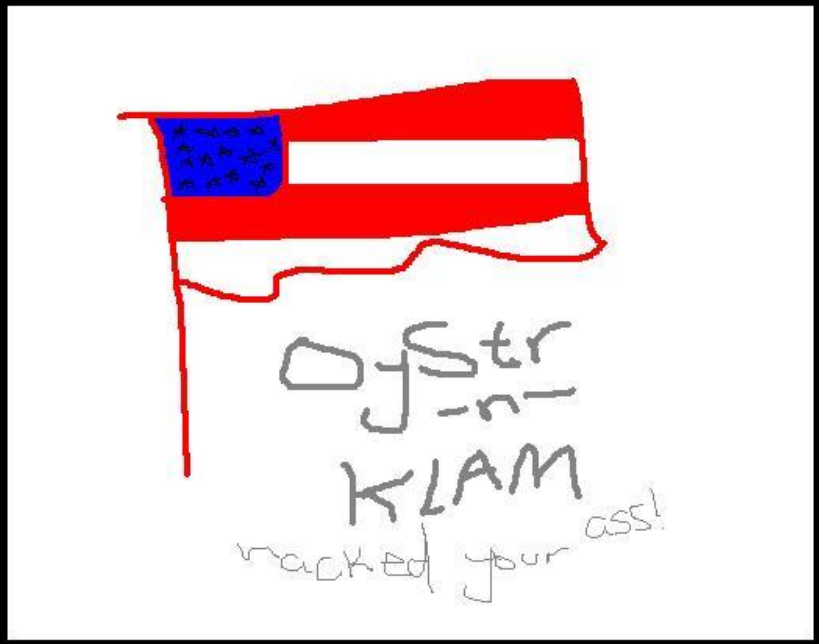
Web Sayfası Değişimleri – Yahoo 7/2/2000

Web Sayfası Değişimleri – healt.gov.tr 11.27.1999

WE BROKE INTO TURKEY'S NUCLEAR LAB (www.nukleer.gov.tr) BUT WE DECIDED TO GO FOR TURKEY'S HEALTH PAGE TOO!

OySTr n KLaM hacking the health of TURKEY

GOBBLE GOBBLE, j00 g0t h4ck3d



WATCH OUT YOUR COUNTRY IS NEXT!

Saldırıya Uğrayabilecek Değerler

- Kurum İsmi, Güvenilirliği ve Markaları
- Kuruma Ait Özel / Mahrem / Gizli Bilgiler
- İşin Devamlılığını Sağlayan Bilgi ve Süreçler
- Üçüncü Şahıslar Tarafından Emanet Edilen Bilgiler
- Kuruma Ait Adli, Ticari Teknolojik Bilgiler

Genel Güvenlik Önlemleri

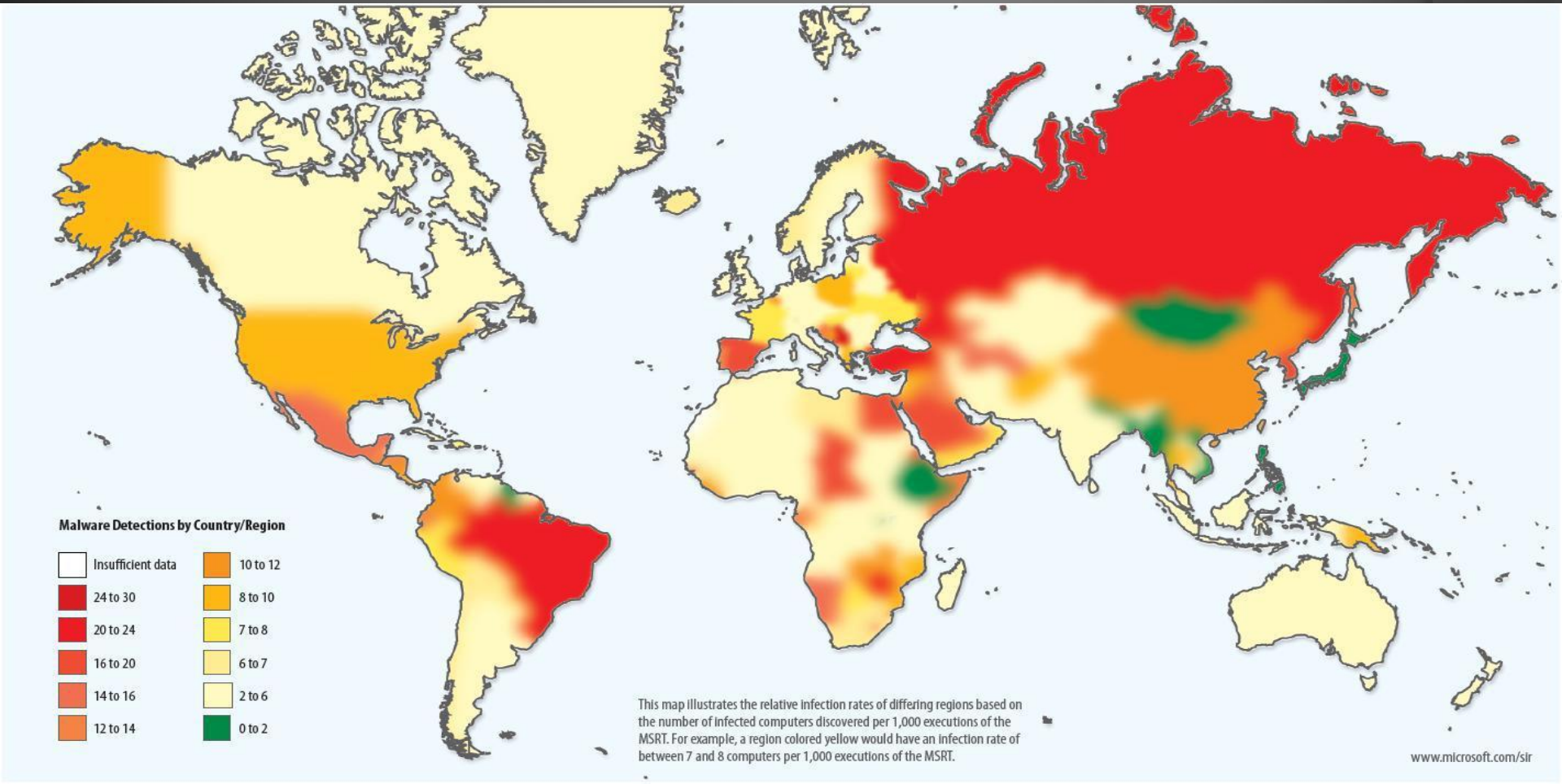
- Bir Güvenlik Politikası Oluşturulmalı
- Tüm Ağ Sorun Kaldırabilecek Şekilde ve Politikada Belirlendiği Gibi Yapılandırılmalı
- Düzenli Olarak Yedekleme Yapılmalı ve Yedekler Kontrol Edilmeli.
- Gerek Duyulan Güvenlik Uygulamaları Kullanılmalı
  - Güvenlik Duvarı
  - Saldırı Tespit Sistemi
  - Anti-Virüs Sistemi
- Ağ Düzenli Olarak Denetlenmeli ve İzlenmeli
- Çalışanlar Politikalar ve Uygulamalar Konusunda Eğitilmeli

3.BÖLÜM SIR *V6* SIR RAPORLARI HAKKINDA

- SIR: Security Intelligence Report – Güvenlik İstihbarat Raporu
- Yılda iki kez yayınlanır.
- Volume 9, 2010‟un ilk yarısında toplanan veriler doğrultusunda hazırlanmıştır.
- http://www.microsoft.com/sir

adresinden en güncel rapora ve daha önceki raporlara ulaşılabilir .

ZARARLI VE İSTENMEYEN YAZILIMLARIN DÜNYA HARİTASI-2008'in 2.YARISI



ÜLKELERDEKİ ZARARLI YAZILIM ORANLARI

En Düşük Oranlar

Location	1H08
Vietnam	1.3
Philippines	1.4
Macao S.A.R.	1.5
Japan	1.7
Morocco	2.1
Pakistan	2.2
Austria	2.3
Luxembourg	2.5
Algeria	2.6
Finland	2.6
Puerto Rico	2.7

En Yüksek Oranlar

Location	1H08
Serbia and Montenegro	77.0
Russia	21.1
Brazil	20.9
Türkiye	20.5
Spain	19.2
Saudi Arabia	18.5
Korea	18.3
Egypt	16.5
Mexico	15.9
Guatemala	13.9
Portugal	13.4

Türkiye‟de zararlı yazılım bulaşma oranı 20.5

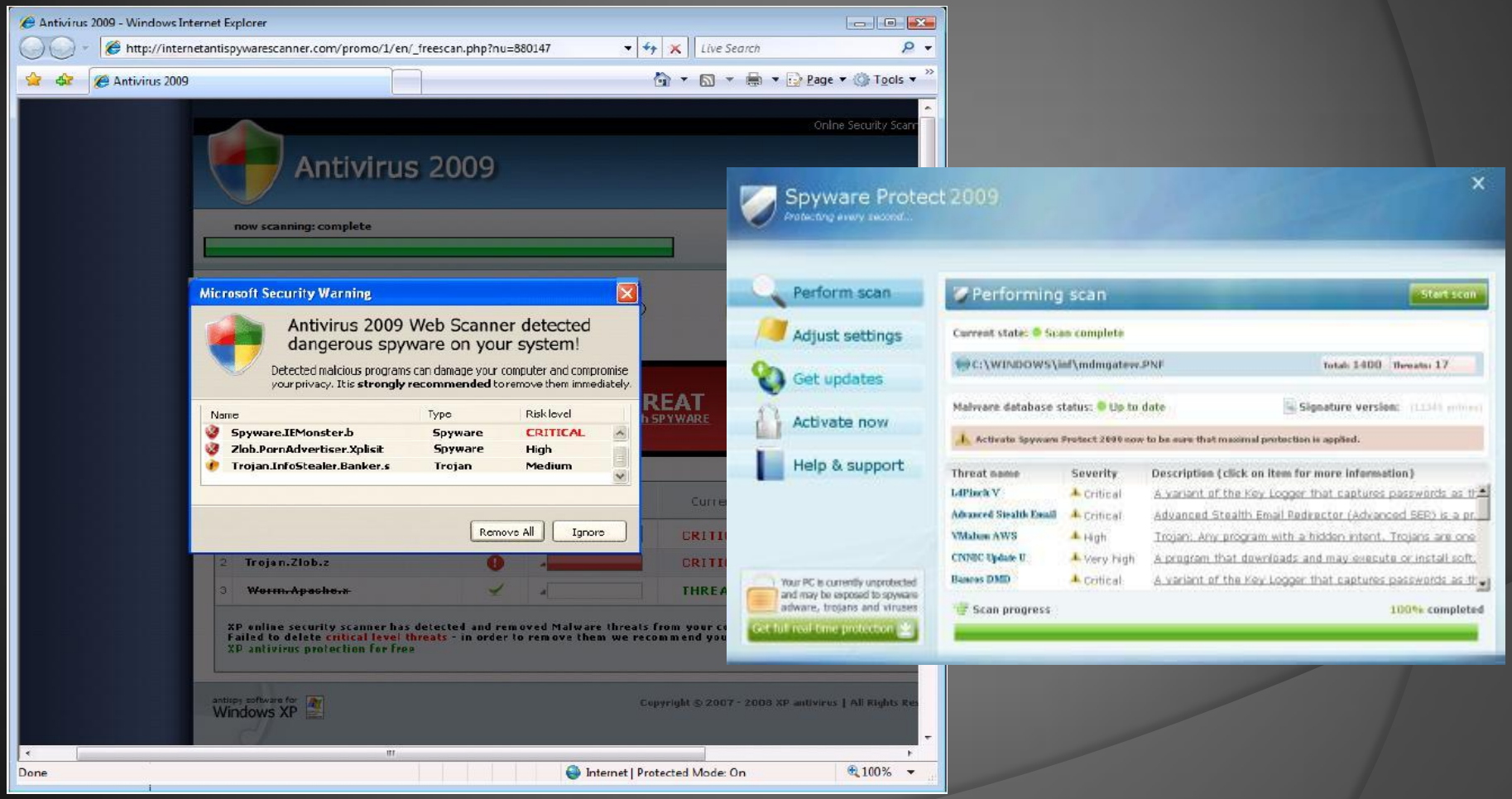
MSRT‟nin çalıştığı her 1000 bilgisayardan 20.5‟de zararlı kod var.

2008‟in 2. yarısı dünya ortalaması 8.6

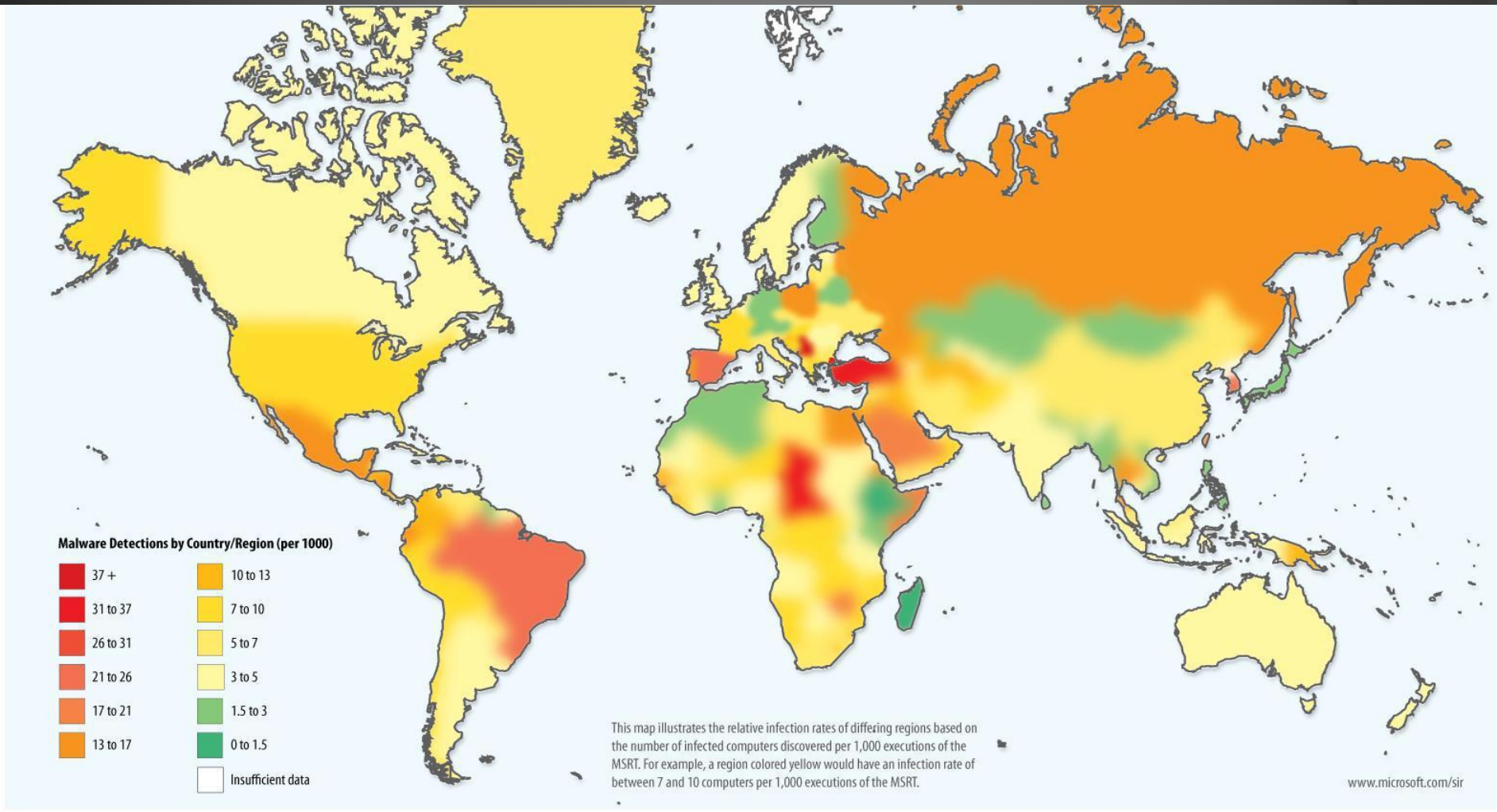
SIR V6'da Özel Odak: SAHTE GÜVENLİK YAZILIMLARI

- Genellikle kullanıcıları korkutma yöntemini kullanırlar.
- Kullanıcının bilgisayarında zararlı kodlar varmış gibi gösterip bu kodları temizlemek için kullanıcının bu uygulamanın "tam sürümü"nü alması gerektiği söylerler.
- Tuzağa düşen kullanıcılar korunmayı beklerken çoğu zaman aslında başka bir tehditin parçası olurlar.

SAHTE GÜVENLİK YAZILIMLARI



SIR V7
Zararlı ve İstenmeyen Yazılımların Dünya Haritası-2009'UN 1. YARISI



ÜLKELERDEKİ ZARARLI YAZILIM ORANLARI

En Düşük Oranlar

Location	1H09
Finland	1.9
Austria	2.1
Puerto Rico	2.1
Philippines	2.3
Vietnam	2.4
Macao S.A.R	2.2
Tunisia	2.5
Morocco	2.6
Algeria	2.8
Kenya	2.9
Kazakhstan	2.9

En Yüksek Oranlar

Location	1H09
Serbia and Montenegro	97.2
Türkiye	32.2
Brazil	25.4
Spain	21.6
Korea	21.3
Saudi Arabia	20.8
Taiwan	20.4
Guatemala	17.0
Russia	15.0
Mexico	14.5
Thailand	14.0

Türkiye‟de zararlı yazılım bulaşma oranı 32.2

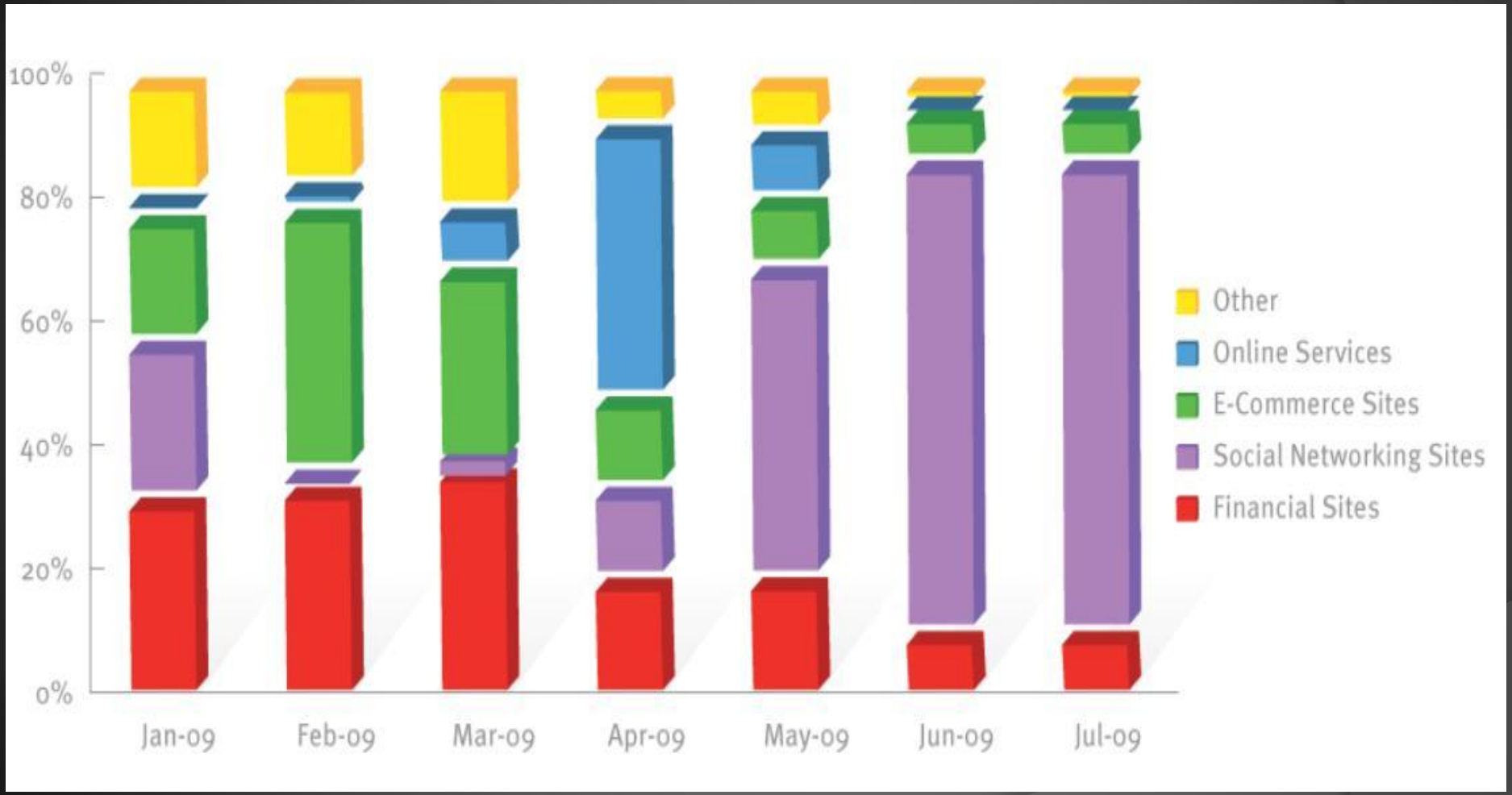
MSRT‟nin çalıştığı her 1000 bilgisayardan 32.2‟de zararlı kod var.

Dünya ortalaması 8.7

Phishing

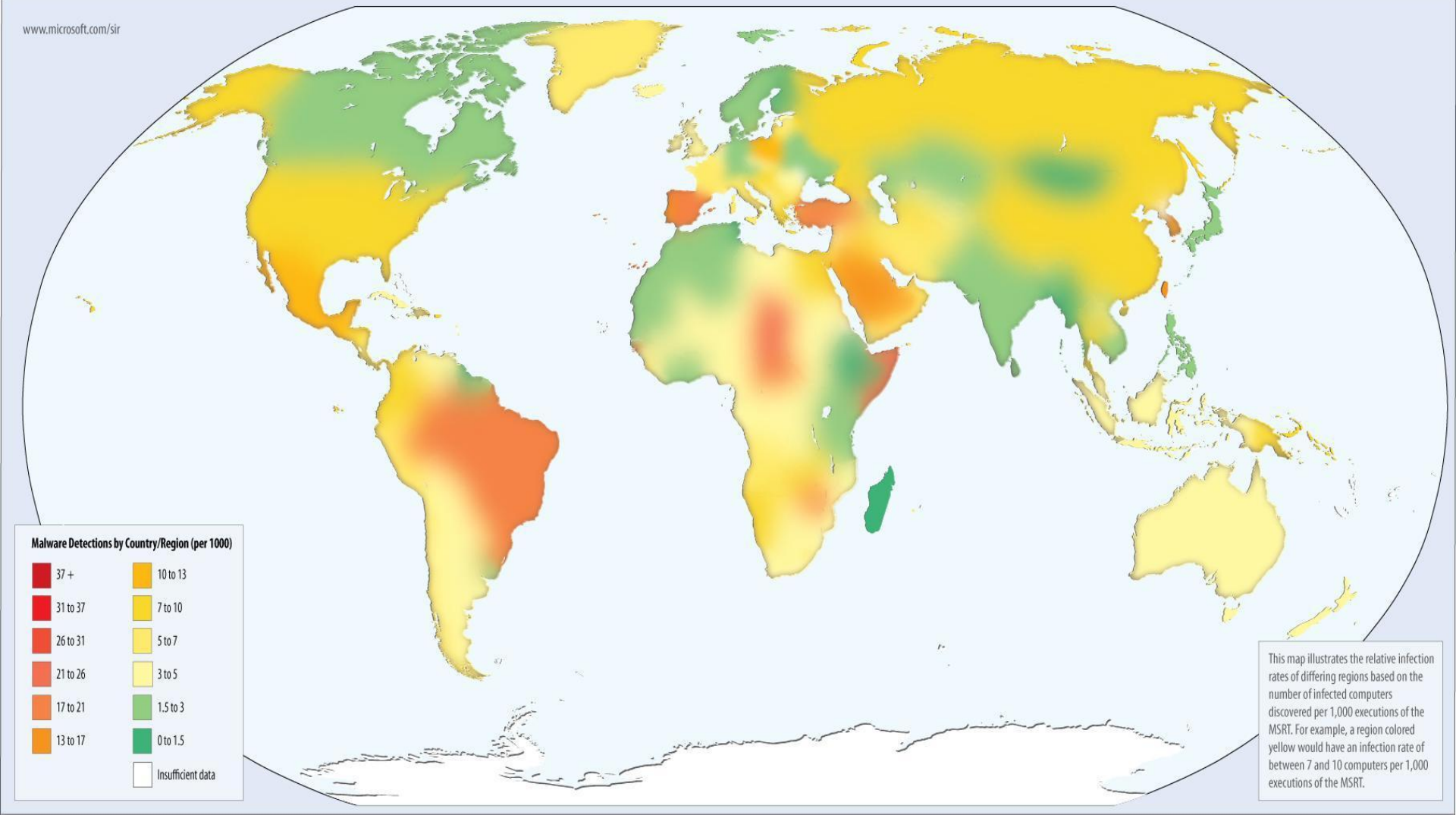
- 2009‟un ilk yarısında phishing görüntülemesi ciddi bir şekilde arttı. Bunun en büyük sebebi phishing saldırılarının sosyal paylaşım sitelerine yönelmesiydi.
- Oyun siteleri, portallar , paylaşım siteleri hedef alınan siteler arasındaydı.
- Phishing oranı, Nisan 2009‟a kadar aynı seviyede giderken yazın sosyal sitelere saldırılarla birlikte 4 katına çıktı.

Phishing: Hedef Seçilen Sektörler



- Sosyal Ağların hedef alınması giderek artıyor
- Finans sektörünün hedef alınması azalıyor

SIR V8
Zararlı ve İstenmeyen Yazılımların Dünya Haritası-2009'UN 2. YARISI



ÜLKELERDEKİ ZARARLI YAZILIM ORANLARI

En Düşük Oranlar

Location	2H09
Réunion	1.3
Finland	1.4
Tunisia	1.4
Algeria	1.5
Belarus	1.5
Austria	1.7
Senegal	1.7
Philippines	1.7
Morocco	1.8
Vietnam	1.8

En Yüksek Oranlar

Location	2H09
Türkiye	**20.0**
Brazil	18.0
Spain	17.1
Taiwan	16.7
Korea	16.0
Portugal	13.6
Saudi Arabia	13.0
Guatemala	12.5
Poland	11.0
Mexico	10.0

Türkiye‟de zararlı yazılım bulaşma oranı 20.0

MSRT‟nin çalıştığı her 1000 bilgisayardan 20‟sinde zararlı kod var.

Dünya ortalaması 7.0

Security Intelligence Report Volume 9

- SIR 9 geçmiş dönemlerden gelen verileri de kullanır ama asıl olarak 2010'un ilk yarısı odaklıdır.
- Bütün Rapor İçinde:
  - --Zararlı Yazılım Trendleri
    - -Coğrafi Trendler
    - -İşletim Sistemi Trendleri
    - -Ev ve Kurumsal Tehditler
- Sahte Güvenlik Yazılımları
- E-Mail Tehditleri
  - --Spam Trendleri ve istatistikleri
- Yazılım Hassasiyetleri ile ilgili detaylı bilgi mevcuttur.

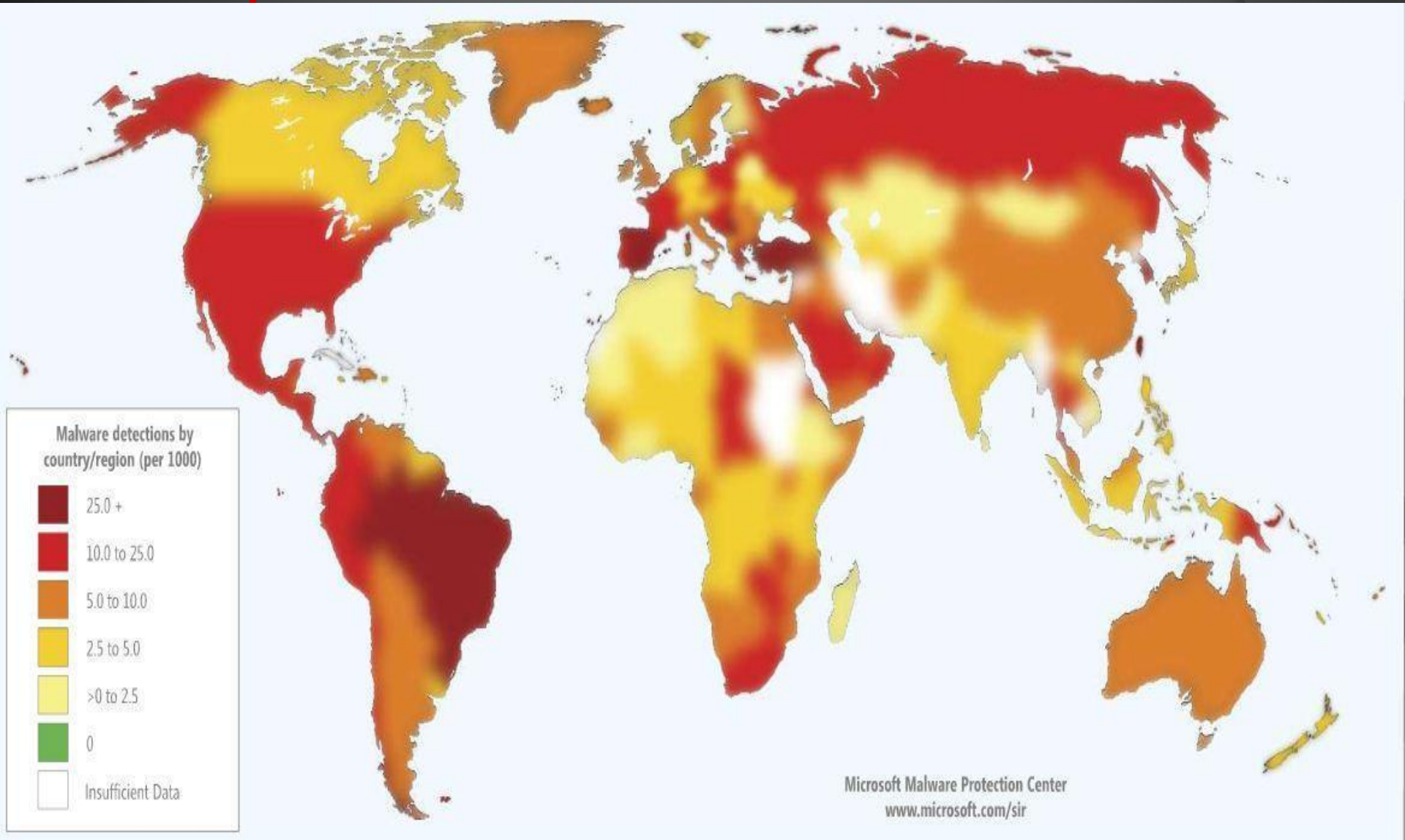
SIR V9 VERİ KAYNAKLARI

- Microsoft‟un anti-malware lab‟ları
- Microsoft Security Essentials, çoklu dil desteğiyle, milyonlarca bilgisayarda koruma sağlar.
- Internet Explorer SmartScreen Filter, Phishing Filter web sayfalarıyla gelebilecek tehditlere karşı koruma sağlar.
- Forefront Client Security ile dünya çapında tüm kurumlar için daha güvenli çalışma ortamı sağlanır.
- Forefront Online Protection for Exchange binlerce kurumsal müşteriyi korur ve milyarlarca e-postayı tarar.

SIR V9 VERİ KAYNAKLARI

- Windows Defender, tüm dünya çapında 100 milyondan fazla kullanıcıya sahiptir.
- Windows Live Hotmail, 30 ülkede 280 milyondan fazla aktif kullanıcı tarafından kullanılmaktadır.
- MSRT (Malicious Software Removal Tool), 2010‟un ilk yarısında aylık ortalama 550 milyon, toplamda ise 3.2 milyarı aşkın sayıda indirildi.
- Bing arama motoru yılda milyarlarca web sayfasını tarayarak zararlı içerik tespit eder.
- Windows Live OneCare, gerçek zamanlı koruma sağlar.

Zararlı ve İstenmeyen Yazılımların Dünya Haritası-2010'UN 1. YARISI



ÜLKELERDEKİ ZARARLI YAZILIM ORANLARI

Coğrafik Trendler

Rank	Country	2Q10
1	Belarus	1.3
2	Bangladesh	1.5
3	Sri Lanka	1.8
4	Tunisia	1.8
5	Morocco	1.9
6	Pakistan	2.1
7	Algeria	2.1
8	Vietnam	2.1
9	Finland	2.1
10	Kazakhstan	2.2

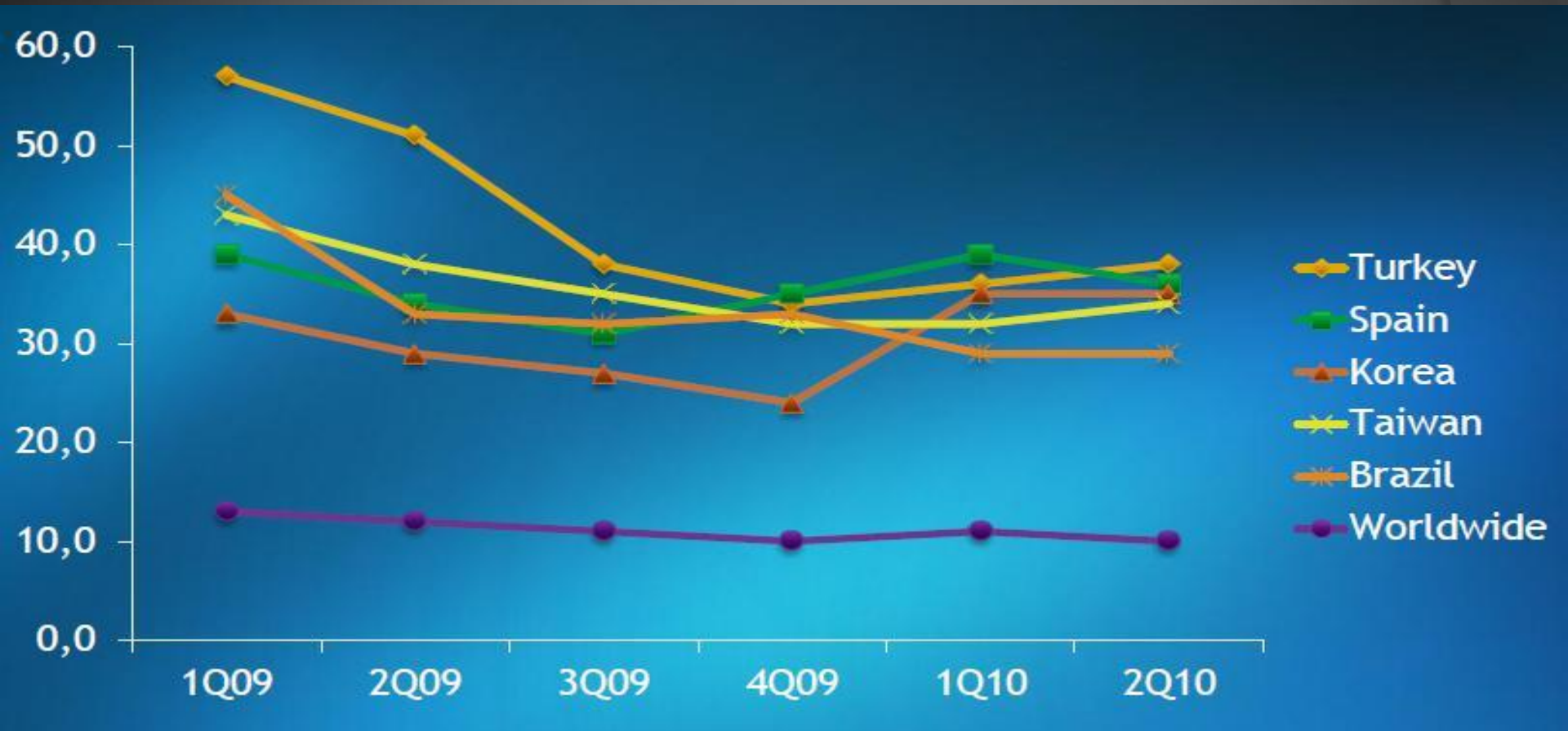
Locations with the **lowest** infection rates, by CCM, in Q2 2010 (200,000 quarterly MSRT executions or more)

Rank	Country	2Q10
1	Turkey	36.6
2	Spain	35.7
3	Korea	34.4
4	Taiwan	33.5
5	Brazil	25.8
6	Poland	21.8
7	Mexico	21.4
8	El Salvador	20.5
9	Peru	19.2
10	Portugal	18.1

Locations with the **highest** infection rates, by CCM, in Q2 2010 (200,000 quarterly MSRT executions or more)

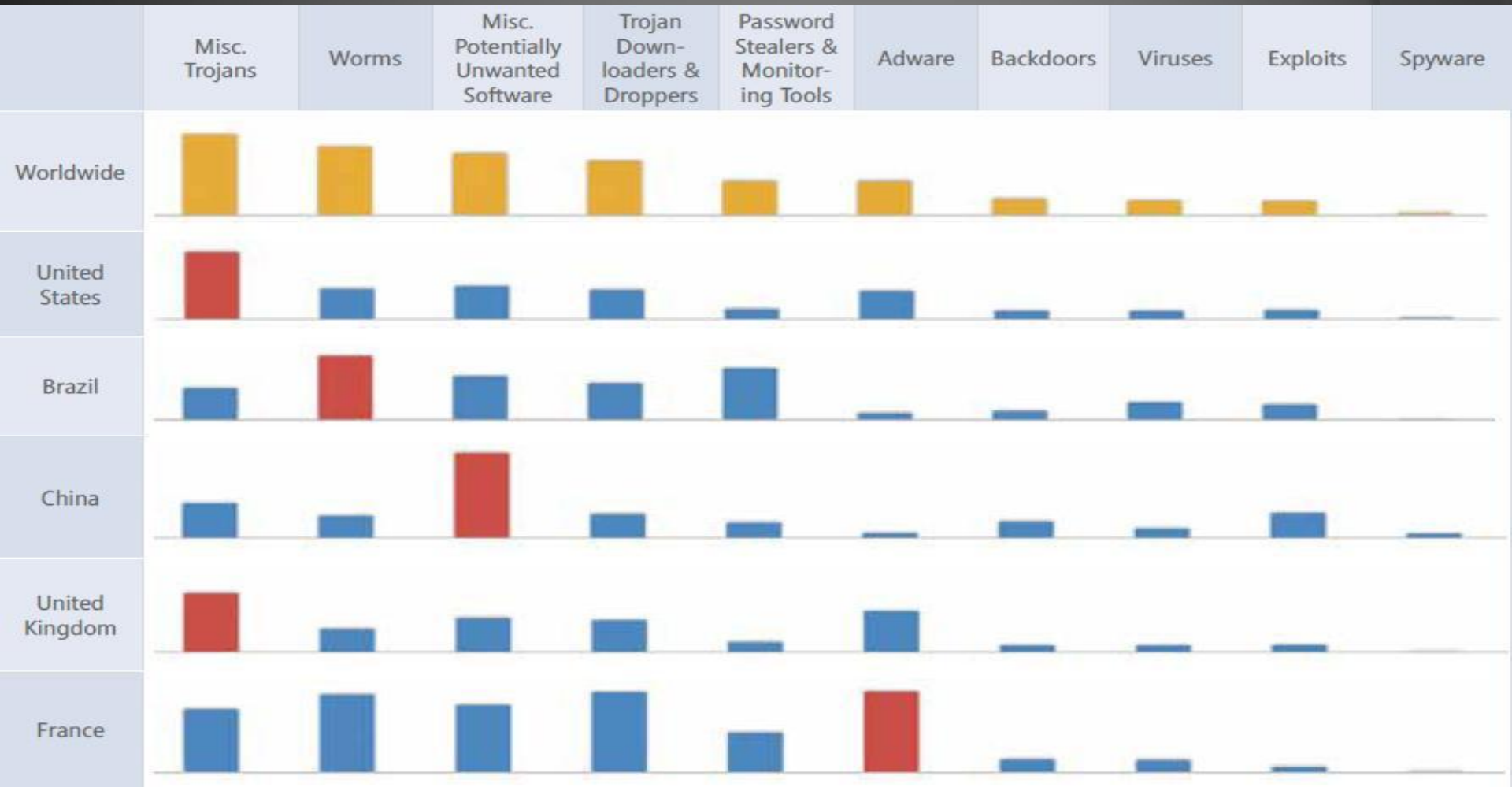
ÜLKELERDEKİ ZARARLI YAZILIM ORANLARI

- Türkiye, İspanya, Kore, Tayvan ve Brezilya en az 100.000 MSRT bildirimiyle üst sıralarda.



Zararlı ve İstenmeyen Yazılımlar Ülke Kırılımı

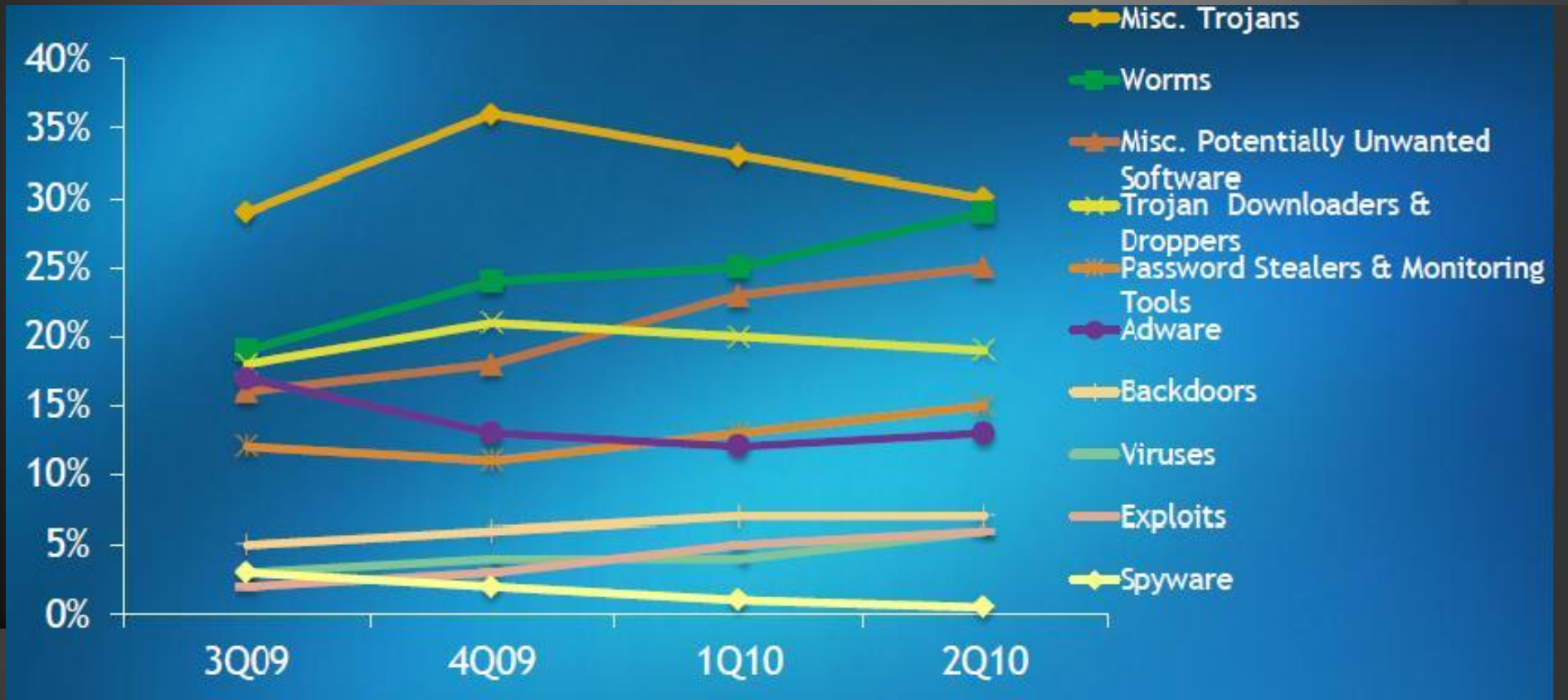
- 2010'un ilk yarısı için 5 farklı ülkeden tehdit çeşitleri



Zararlı ve İstenmeyen Yazılımlar Kategori Kırılımı

- Çeşitli Trojanler (Sahte Güvenlik Yazılımları) En Yüksek
- Worm bulaşma sayısı artış gösteriyor

3Q09-2Q10 arasında temizlenen tüm bilgisayarların kategori bazında dağılımı



1Q10 ve 2Q10'da En Çok Algılanan Malware Ailesi

Rank	Family	Most Significant Category	1Q10	2Q10	1 Year Trend
1	Win32/Taterf	Worms	1,495,286	2,320,953	
2	Win32/Frethog	Password Stealers & Monitoring Tools	2,010,989	1,997,669	
3	Win32/Renos	Trojan Downloaders & Droppers	2,691,987	1,888,339	
4	Win32/Rimecud	Worms	1,807,773	1,748,260	
5	Win32/Conficker	Worms	1,496,877	1,663,349	
6	Win32/Autorun	Worms	1,256,356	1,645,851	
7	Win32/Hotbar	Adware	1,015,055	1,482,681	
8	Win32/FakeSpypro	Miscellaneous Trojans	1,244,353	1,423,528	
9	Win32/Alureon	Miscellaneous Trojans	1,463,885	1,035,079	
10	Win32/Zwangi	Misc. Potentially Unwanted Software	542,011	859,801	

SIR V9
BOTNET ÖZEL RAPORU

Bilgisayarınızın Kontrolü Kimde?

Botnet Nedir?

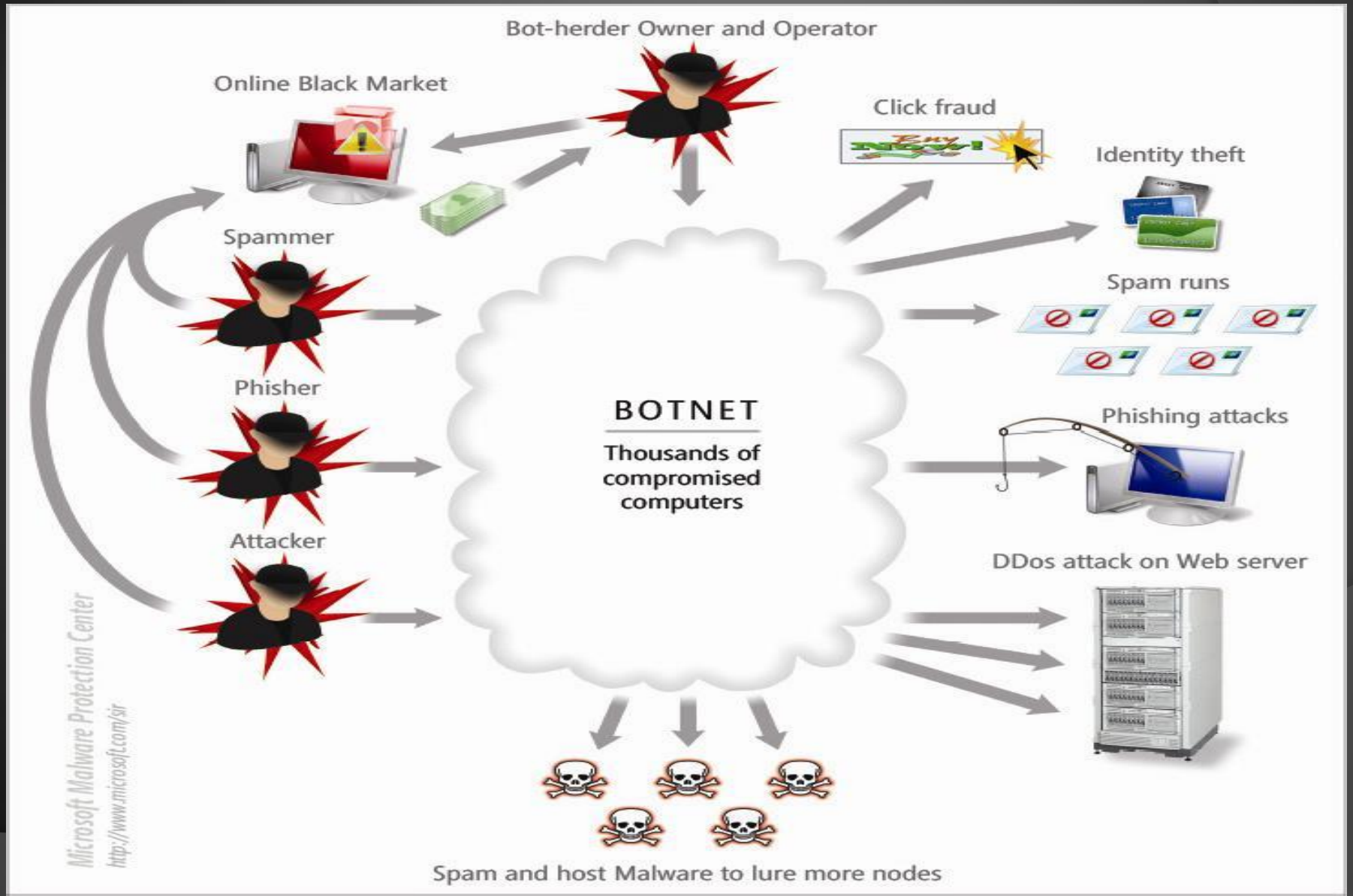
- Botnetler, belirli bir insiyatif çerçevesinde bir ağda kendilerinden istenen görevleri yerine getiren akıllı yazılımlardır.
- Botlar, çok faydalı amaçlar için kullanılabilirler; dahası önem arzeden görevleri yerine getirebilirler.
- Ne yazık ki, botlar aynı zamanda kötü amaçlar için de kullanılabilirler.
- Botlar, diğer kötü amaçlı yazılımlar gibi, birkaç farklı yolla yayılabilirler:

--Zayıf veya kullanılmayan güvenlik politikalarını aşarak

--Güvenlik hassasiyetlerini aşarak

--Çeşitli yollarla (örneğin sosyal içeriklerle) kullanıcıları kandırıp, onların kötü amaçlı yazılımları yüklemeye ikna ederek

İş Başında Bir BOTNET



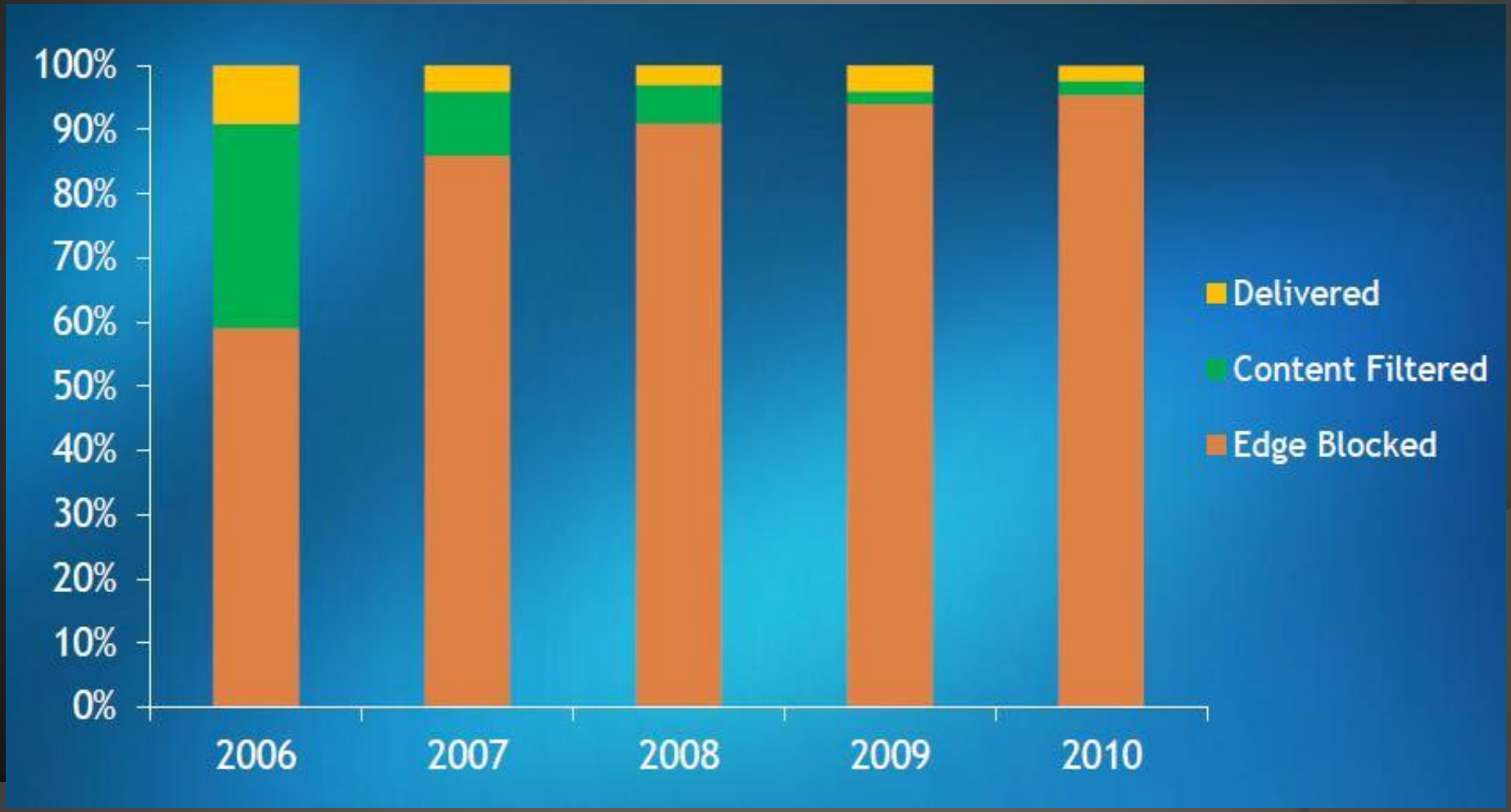
BOTNETLER NE AMAÇLA KULLANILIR

- Günümüzde **spam iletilerinin büyük çoğunluğu, botnetler tarafından gönderilmektedir.**
- Kullanıcıları, kişisel bilgilerini paylaşmaya yönlendirmeyi hedefleyen **phishing mesajları çoğunlukla botnetler tarafından oluşturulup gönderilir.**
- Pek çok bot, yayıldığı makinelerdeki kişisel bilgileri arayıp, **hassas bilgiyi çalmaya komutanmıştır.**
- **DoS (Denial-of-Service) saldırısı, bir bilgisayar kaynağı tarafından sunulan servisi kullanılamaz duruma getirmek için gerçekleştirilen saldırılardır. (Örneğin, Wikileaks destekçilerinin MasterCard, PayPal, Visa vb sitelere yaptıkları saldırılar). Bu saldırılarda botnetler kullanılır.**

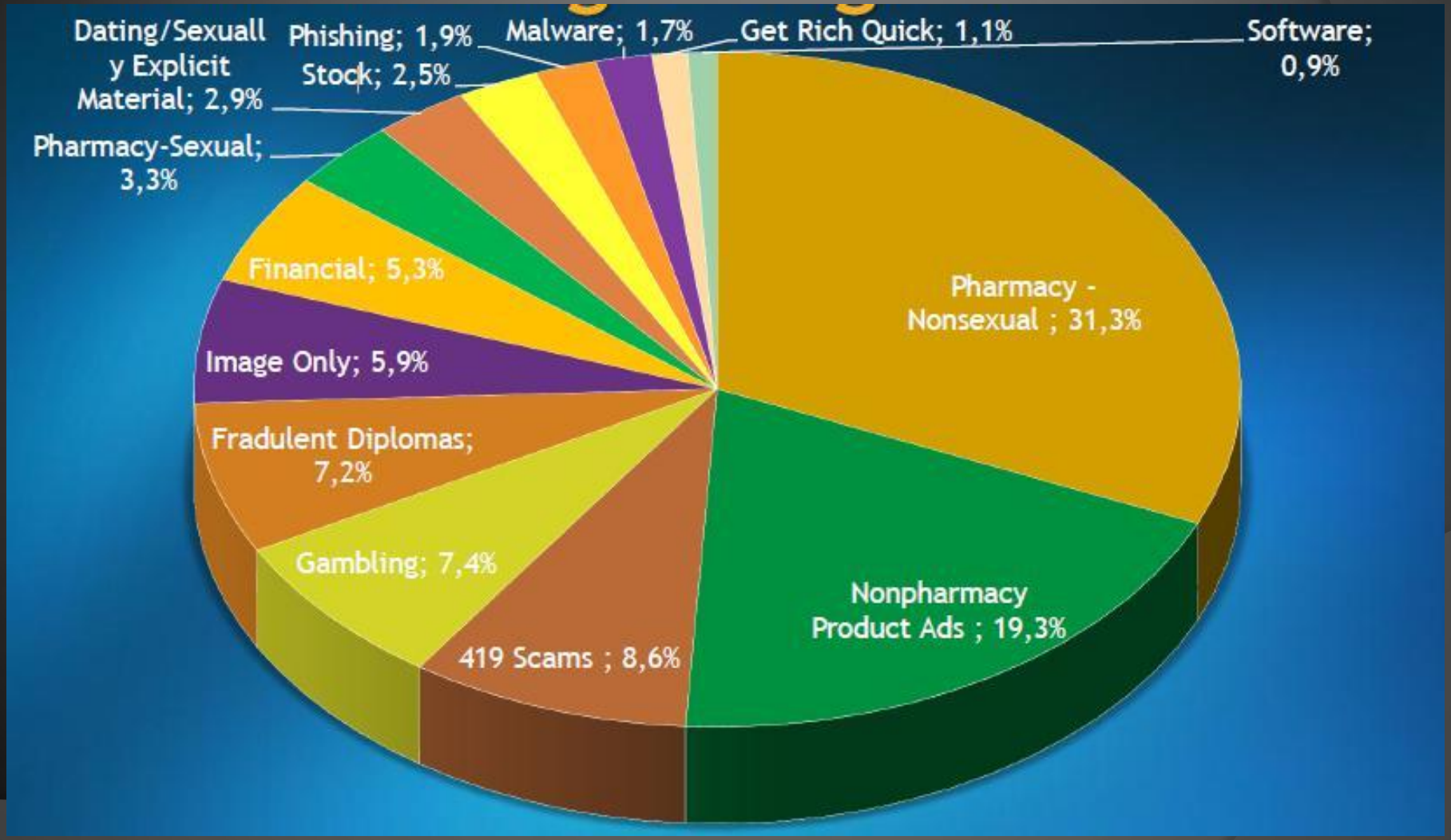
BOTNETLER NE AMAÇLA KULLANILIR

- Botnetler, kötü amaçlı ve istenmeyen yazılımları yükletme amaçlı kullanılabilir. Bu şekilde yüklenen yazılımlar, çoğu zaman kendilerini kullanıcıdan gizleyerek çalışırlar.
- Botnetler, kötü amaçlı yazılımların yayılmasında önemli rol oynar.
- Botlar zaman zaman, tıklama başına ödeme yapan (pay-per-click) reklam amaçlı içerekleri hedef alabilir. Sahte tıklamalar gerçekleştirerek, kendi sahibine para kazandırabilir.

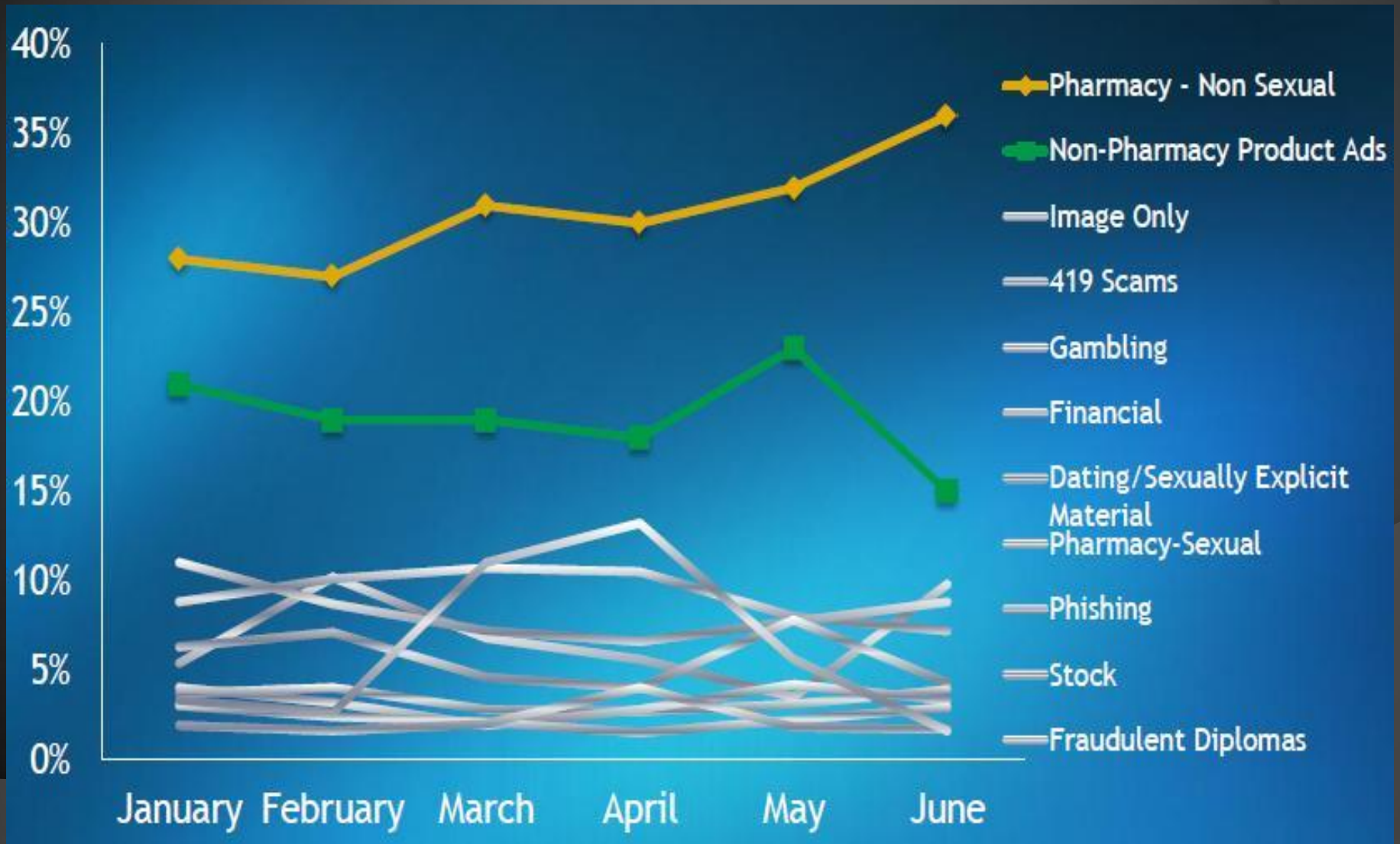
2006-2010 Yılları Arasında Edge - Blocking ve İçerik Filtreleme Yöntemiyle Engellenen İleti Yüzdesi



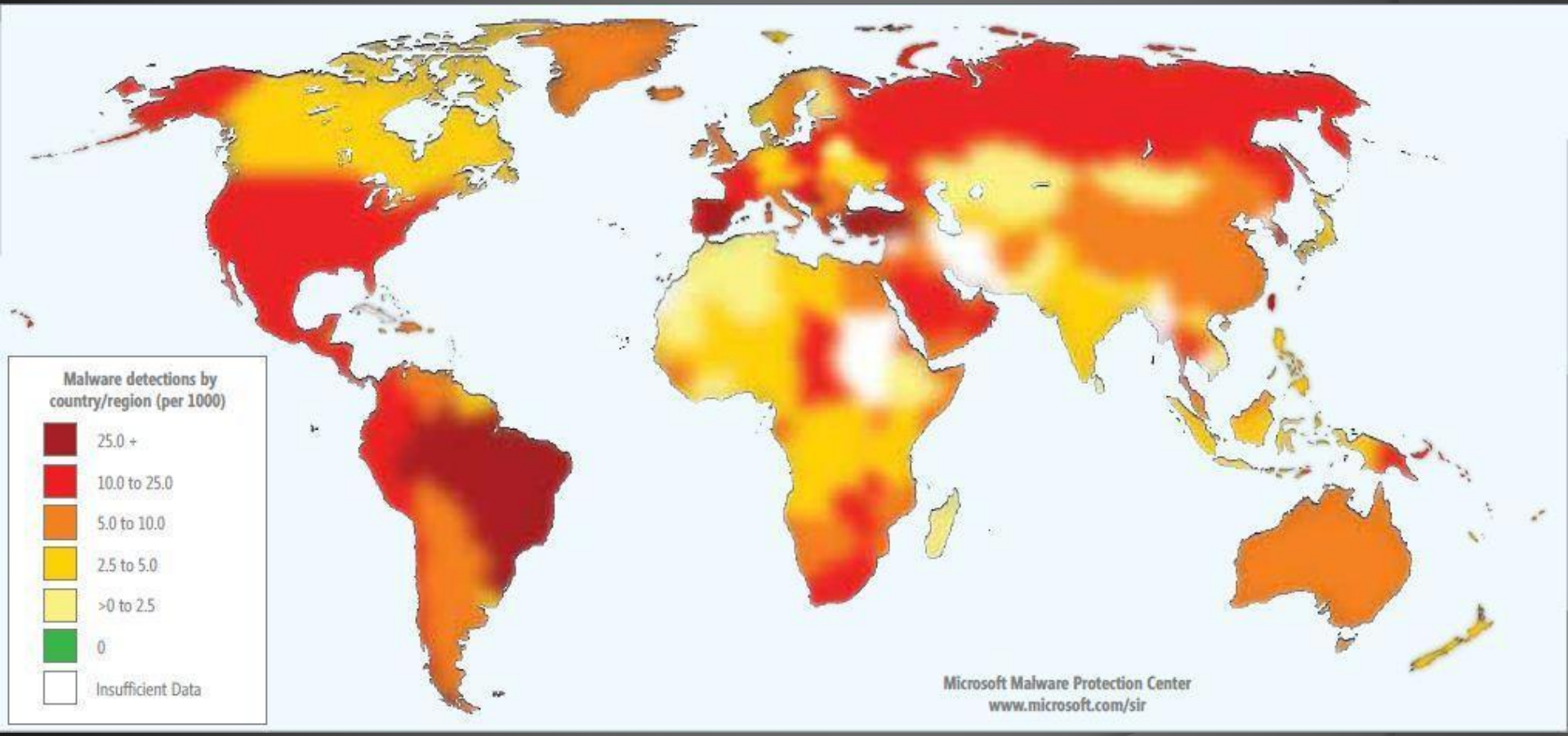
2Q10'da FOPE Tarafından Bloklanan İletilerin Kategori Dağılımı



1Q10 ve 2Q10'da İçerik Filtresine Takılan İleti Kategorileri



TÜRKİYE
ÜLKE BAZINDA ENFEKSİYON HIZI(CCM)

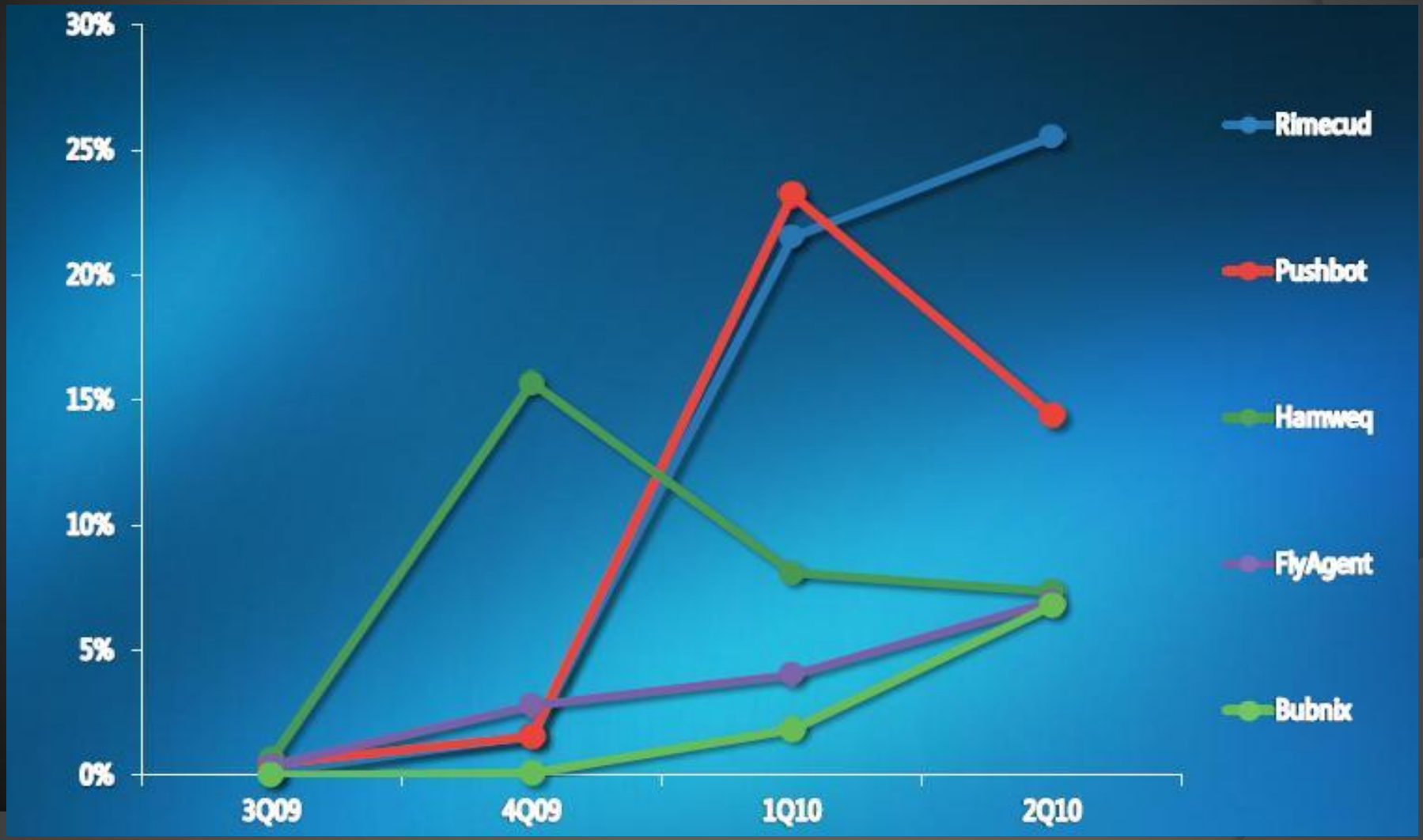


MSRT çalışan 200.000‟in üzerindeki lokasyonda, 2Q10‟da Türkiye %3.66 ile (CCM 36.6) ile en yüksek orana sahip. Türkiye‟nin ardından 35.7 (CCM) ile İspanya ve 34.4 (CCM) ile Kore geliyor.

2Q10'da En Çok BOT Temizlenen 25 Ülke- Türkiye 12. Sırada

Rank	Country/Region	Computers with Bot Cleanings (1Q10)	Computers with Bot Cleanings (2Q10)	Bot Cleanings Per 1000 MSRT Executions (Bot CCM)
1	United States	2,163,216	2,148,169	5.2
2	Brazil	511,002	550,426	5.2
3	Spain	485,603	381,948	12.4
4	Korea	422,663	354,906	14.6
5	Mexico	364,554	331,434	11.4
6	France	344,743	271,478	4.0
7	United Kingdom	251,406	243,817	2.7
8	China	227,470	230,037	1.0
9	Russia	181,341	199,229	4.3
10	Germany	200,016	156,975	1.4
11	Italy	191,588	130,888	2.6
12	Turkey	91,262	98,411	4.7
13	Canada	96,834	87,379	1.4
14	Netherlands	115,349	77,466	2.5
15	Colombia	76,610	71,493	5.8
16	Portugal	83,379	68,903	5.7
17	Australia	72,903	66,576	2.8
18	Poland	87,926	62,704	3.9
19	Taiwan	52,915	54,347	3.4
20	Japan	63,202	52,827	0.6
21	Argentina	38,229	43,162	3.8
22	Saudi Arabia	33,283	40,793	5.5
23	Belgium	51,689	39,508	3.4
24	Chile	37,705	39,245	5.1
25	India	37,895	38,954	1.0

Türkiye’deki En Yüksek BotNet Tehditleri



2Q10'da Türkiye'deki Toplam Tehditler Başlıca Botnet Aileleri - Özet

- Pushbot :

--Pushbot, 2Q10‟da Türkiye‟deki botnetler içinde 26%‟lık oranla en etkili botnet ailesi olmasıyla beraber bir önceki çeyreğe göre düşüş göstermiştir.

- Rimecud :

--Geçtiğimiz birkaç çeyrek içinde, pek çok yer Rimecud algılanmasında artış kaydetti, Türkiye‟de de son iki çeyreğe nazaran 24% ‟lük artış göstermiştir.

Rimecud, internet yoluyla satılan bir kit ailesidir, ki bu da artışta öenmli rol oynamaktadır.

- Rimecud, Hamweq, Pushbot :

--Hepsi de, USB bağlantılı diskler gibi taşınabilir sürücülerde kendilerini kopyalarak yayılmaları amacıyla dizayn edilmiştir.

Hamweq ve Pushbot, geleneksel IRC–tabanlı C&C mekanizması kullanırken, Rimecud özel ayarlı protokol kullanır.

Otomatik SQL Sızma Atakları

- «.tr» TLD‟si, tüm TLDler içerisinde SQL Sızmalarından en çok etkilenen alan adı olarak ilk sırada yer alıyor.

Rank	TLD	Associated with	Victimized pages
1	.tr	Turkey	88,378
2	.com	Commercial entities	43,144
3	.org	Nonprofit organizations	18,331
4	.net	Network infrastructure	5,206
5	.ru	Russia	5,179
6	.it	Italy	3,395
7	.ro	Romania	1,817
8	.uk	United Kingdom	1,812
9	.my	Malaysia	1,773
10	.nl	Netherlands	1,545

KAYNAKLAR:

- http://uekae.tubitak.gov.tr
- http://www.microsoft.com/security/portal
- http://www.microsoft.com/sir
- CERT – http://www.cert.org
- SANS – http://www.sans.org
- Security Focus – http://www.securityfocus.com
- Siyah Şapka – http://www.siyahsapka.com
- Dikey8 – http://www.dikey8.com
- Olympos – http://www.olympos.org
- Güvenlik Haber – http://www.guvenlikhaber.com
- Alldas.org – Defacement Archive – http://defaced.alldas.org/?tld=tr
- Attrition.org – Defacement Archive – http://www.attrition.org/mirror/attrition/tr.html
- Security Space – http://www.securityspace.com