



AYD

Ağ Yöneticileri Derneği



Siber Güvenlik Eğitimi

MALWARE

-Zararlı Yazılımlar-

Ozan BÜK - CCIE# 39061

Ağ Yöneticileri Derneği


CISCO

Networking
Academy

Malware nedir?

- *Malware, short for malicious software, is software used or created to disrupt computer operation, gather sensitive information, or gain access to private computer system.*

- Wikipedia

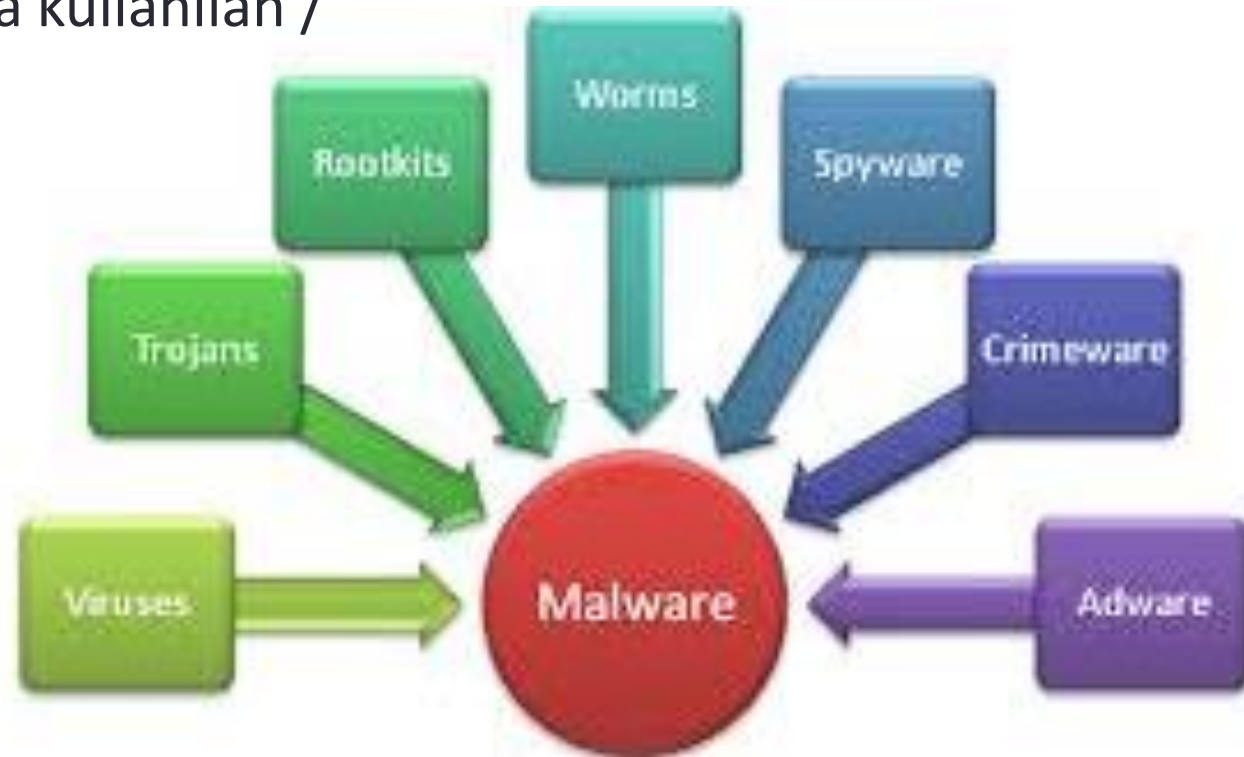
Zararlı yazılımlar;

bilgisayar operasyonunu bozmak, hassas verileri çalmak veya bir bilgisayar sistemine erişim sağlamak amacıyla kullanılan / geliştirilen yazılımlardır.

- Wikipedia

Exploit

An exploit is the term used to describe a program written to take advantage of a known vulnerability.



Malware nedir?



Malware (Zararlı Yazılım) tipleri:

ZARARLI YAZILIMLAR

- Virüsler (Virus)
- Solucanlar (Worms)
- Truva Atları (Trojan Horse)
- Rootkit'ler
- Casus Yazılımları (Spyware)
- Reklam Yazılımları (Adware)
- Botnet'ler
- Fidyeye Yazılımı (Ransomware)
- Scareware

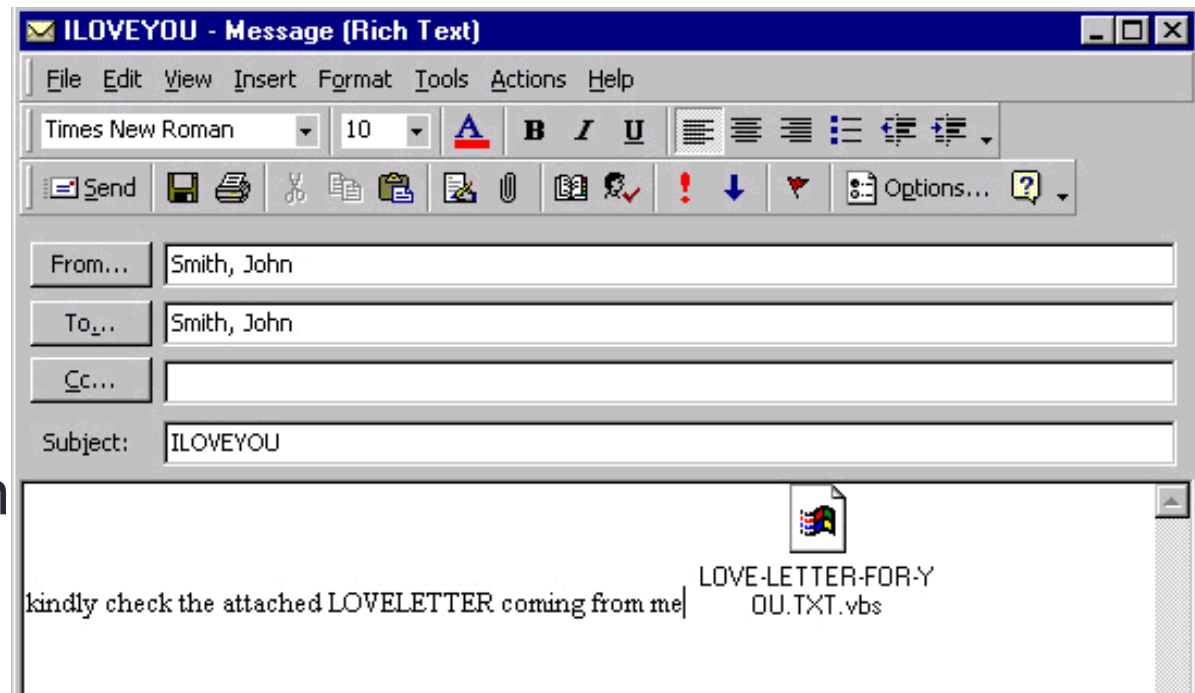


Virus nedir?



- Virüsler
(VIRUS)

- Çalıştırılabilir bir dosyaya eklenir,
- Yayılması için insan etkileşimi gerekir...



Worm nedir?



- Kendisini sistem üzerinde çoğaltabilir
- Yayılmak için insan müdahalesine ihtiyaç duymaz.

- Solucanlar
(WORMS)



Worm nedir?

Worms (Solucanlar)



Initial Code Red Worm Infection



Code Red Worm Infection 19 Hours Later

Trojan nedir?

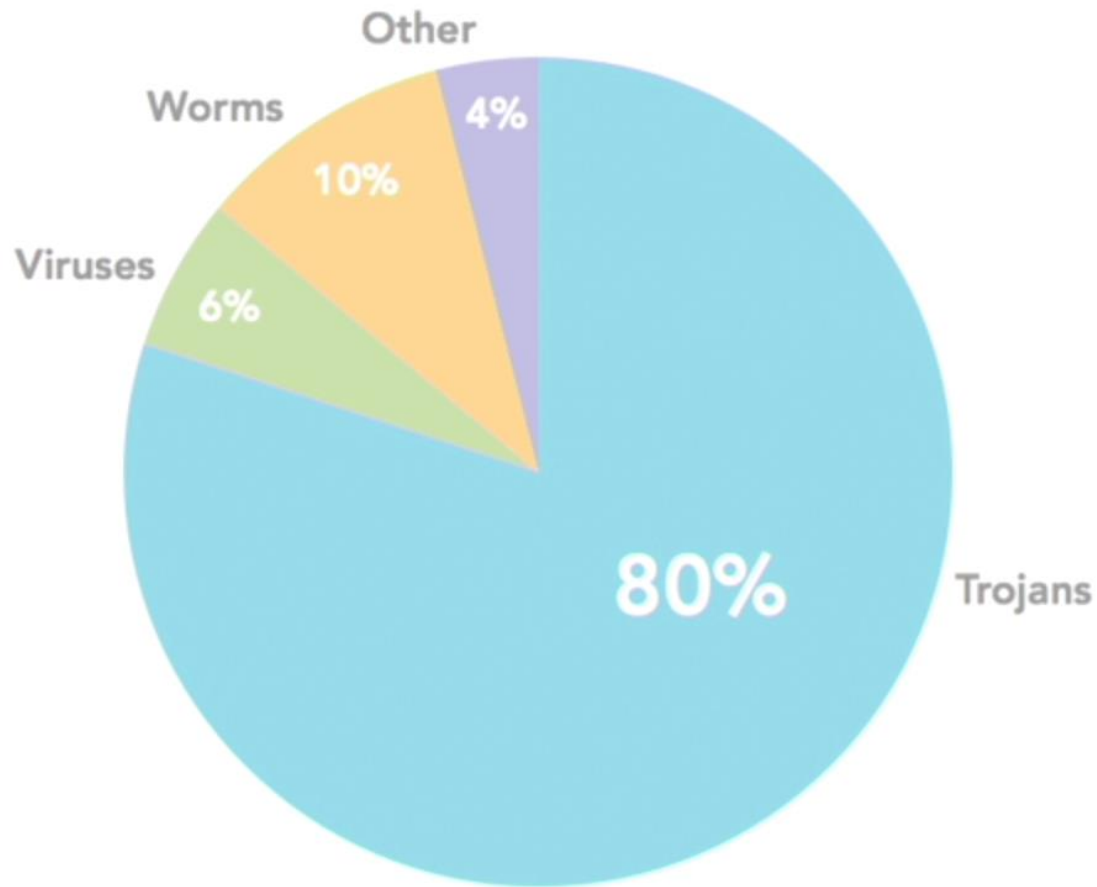
- Truva Atları
(TROJAN HORSE)



- Faydalı gibi görünür ama sisteme zarar verir
- Kendi kendine çoğalamaz,
- **Bulaşması için insan müdahalesine ihtiyaç duyar.**



Trojan nedir?



<https://www.file-extensions.org/filetype/extension/name/dangerous-malicious-files>

Blended Threat nedir?

Saldırıları başlatmak, iletmek ve yaymak için "virüsleri, solucanları, Truva Atlarını ve kötü amaçlı kodu sunucu ve Internet açıkları ile birleştiren bir saldırı" olarak tanımlanmaktadır. Karma tehditler, solucanlar gibi hızlı bir şekilde yayılmak üzere tasarlanmıştır, ancak tek bir saldırı vektörüne (e-posta gibi) güvenmek yerine, harmanlanmış tehditler hangi yayılma yolunu kullanmak için kullanılır.



Rootkit nedir?

- Rootkit'ler



- Backdoor (Arka kapı) bağlantısı yaratır.
- Root yetkisi ile kontrolü eline alır.



Spyware (Casus Yazılım) nedir?

- Casus Yazılımlar
(SPYWARE)



Hedef sistemden bilgi toplayan yazılımlardır.



Adware (Reklam Yazılımı)Nedir?

- Reklam Yazılımları
(ADWARE)

izinli ya da izinsiz olarak reklam gösteren yazılımlardır.

Adware & Spyware



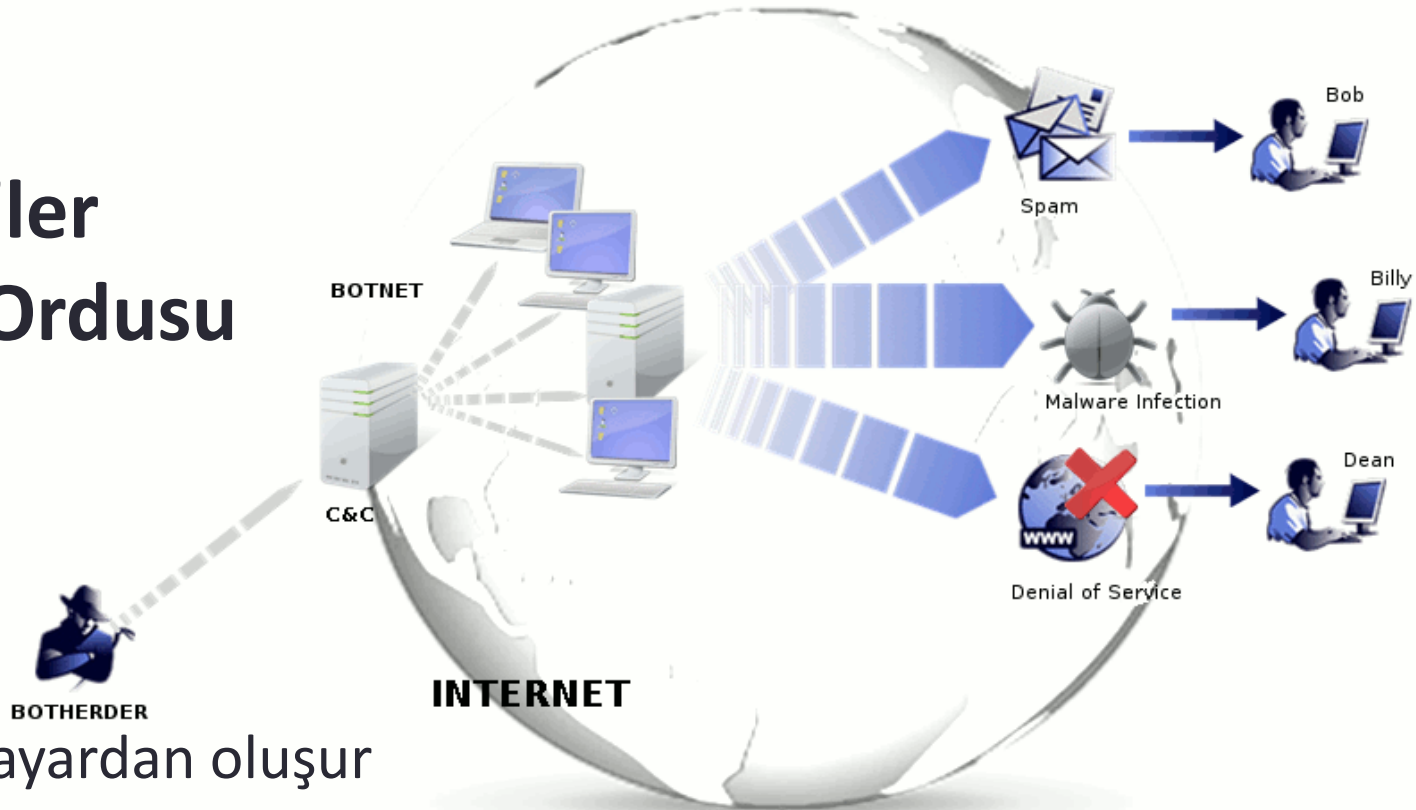
CHECKED



Adwares Detected

Botnet nedir?

- BOTNET'ler
- Zombie Ordusu

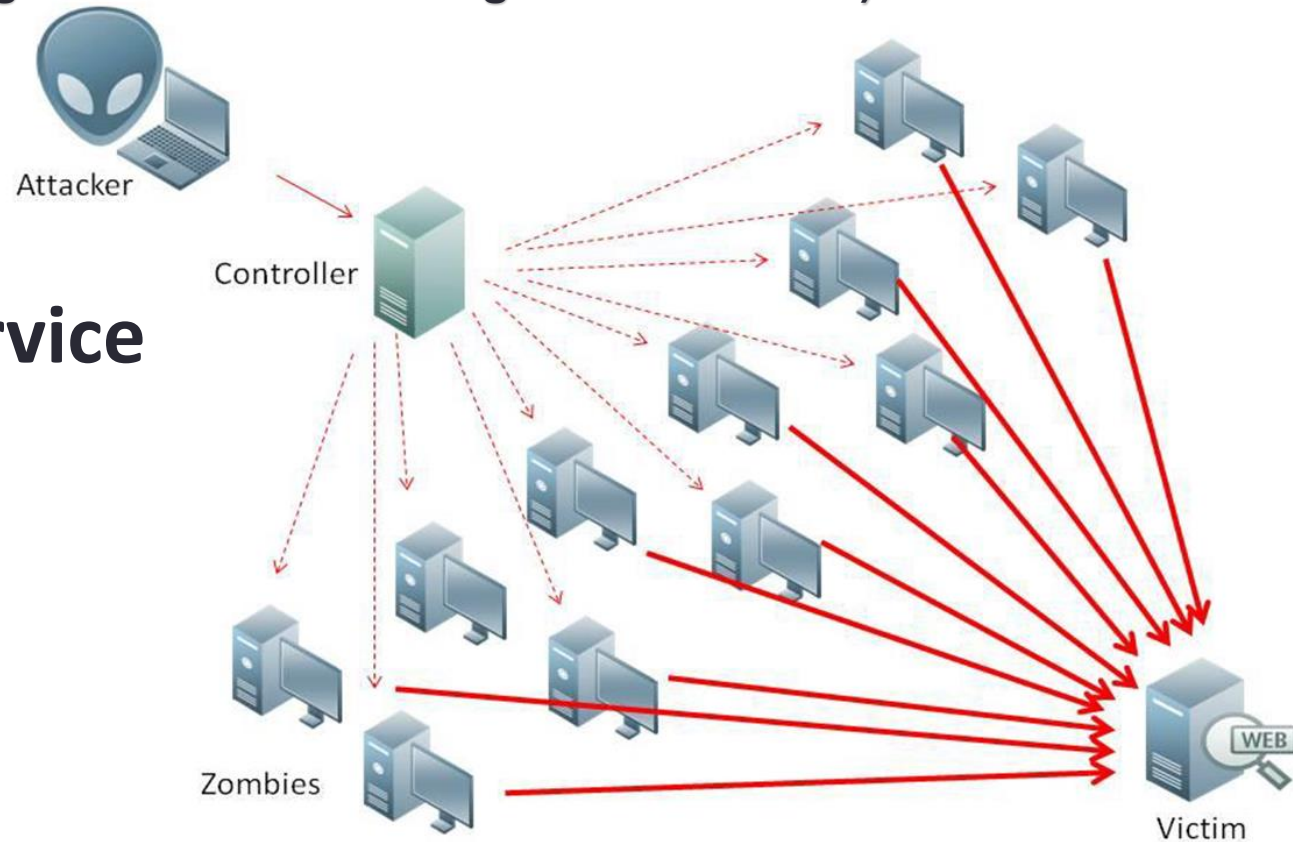


- Binlerce bilgisayardan oluşur
- Hedef;
 - Zararlı yazılımları yaymak
 - Bir saldırı düzenlemek

DDoS Attack nedir?

(Dağıtık Hizmet Reddi/Engelleme Saldırısı)

- **Distributed Denial of Service saldırısı.**



Ransomware (Fidye Virüsü)



APT nedir?

Advanced Persistent Threat Kişiyeye Özel Ataklar

- Ciddi hazırlık süreci
- Çok detaylı bilgi toplama aşaması
- Saldırı adımlarının sosyal bileşenleri konusunda bilgi
- Yaratıcı düşünme yeteneği
- Asıl saldırı vektörünü gizlemeye yönelik dikkat dağıtma çabası
- Henüz yaygınlaşmamış/duyulmamış istismar kodlarının kullanılması
- Fiziksel sızma eyleminden çekinmemeleri

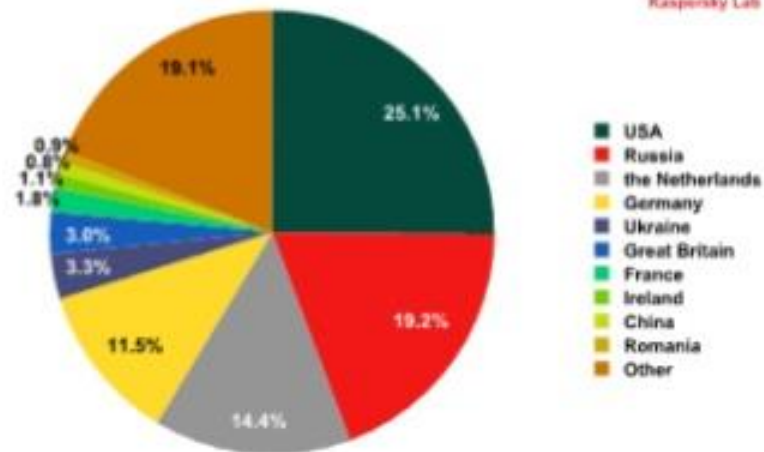


APT nedir?



The Popular “APT”s 2013

- Red October
- APT1
- MiniDuke
- TeamSpy
- Flame
- ➔ • Duqu
- StuxNet
- [.... Lot more ..]



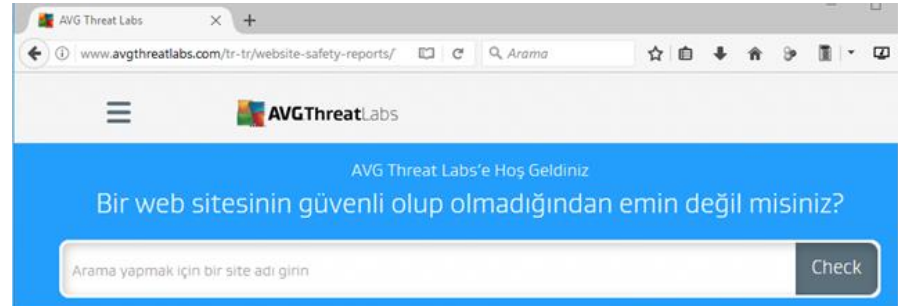
Top countries with Online Resources seeded with Malware

Sandboxing nedir?

- Şüpheli dosyayı korumalı bir ortamda tutar
- Davranışını analiz eder
- Sistemde ne tür değişikliklere yol açtığını gözlemler

İzole bir ortam oluşturan birçok yazılım vardır,

- Sandboxie
- Cuckoo Sandbox



- <https://transparencyreport.google.com/safe-browsing/search>
- <http://www.threatexpert.com/filescan.aspx>

Sibersular;

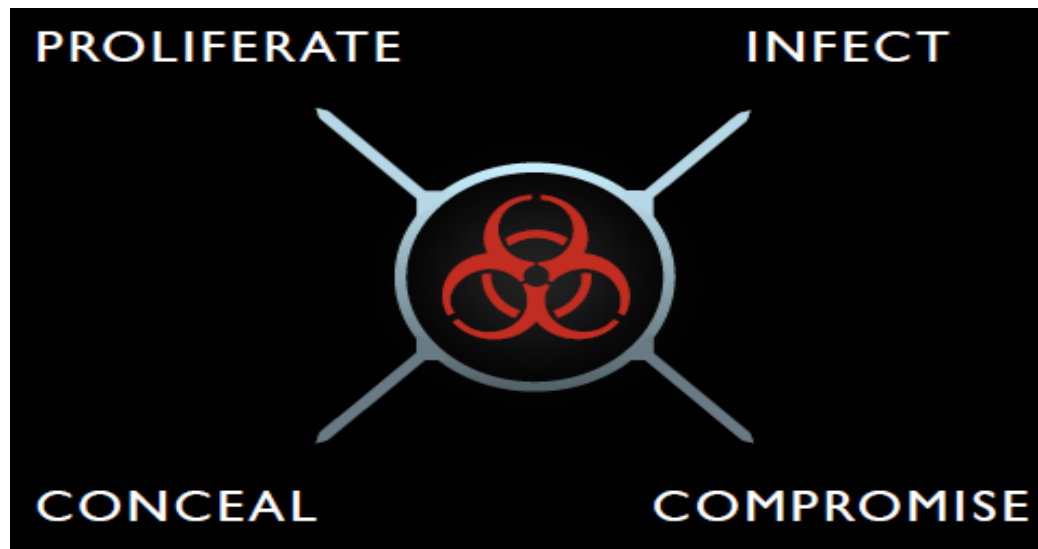


Overall Rank		Item	Percentage		2010 Price Ranges
2010	2009		2010	2009	
1	1	Credit card information	22%	19%	\$0.07–\$100
2	2	Bank account credentials	16%	19%	\$10–\$900
3	3	Email accounts	10%	7%	\$1–\$18
4	13	Attack tools	7%	2%	\$5–\$650
5	4	Email addresses	5%	7%	\$1/MB–\$20/MB
6	7	Credit card dumps	5%	5%	\$0.50–\$120
7	6	Full identities	5%	5%	\$0.50–\$20
8	14	Scam hosting	4%	2%	\$10–\$150
9	5	Shell scripts	4%	6%	\$2–\$7
10	9	Cash-out services	3%	4%	\$200–\$500 or 50%–70% of total value

Symantec gvenlik raporu:

Zararlı Yazılım karakteristikleri:

- İçeri Sızma (Infect)
- Yayılma (Proliferate)
- Kendini Gizleme (Conceal)
- Zarar Verme, Dışarı Veri Kaçırma (Compromise)

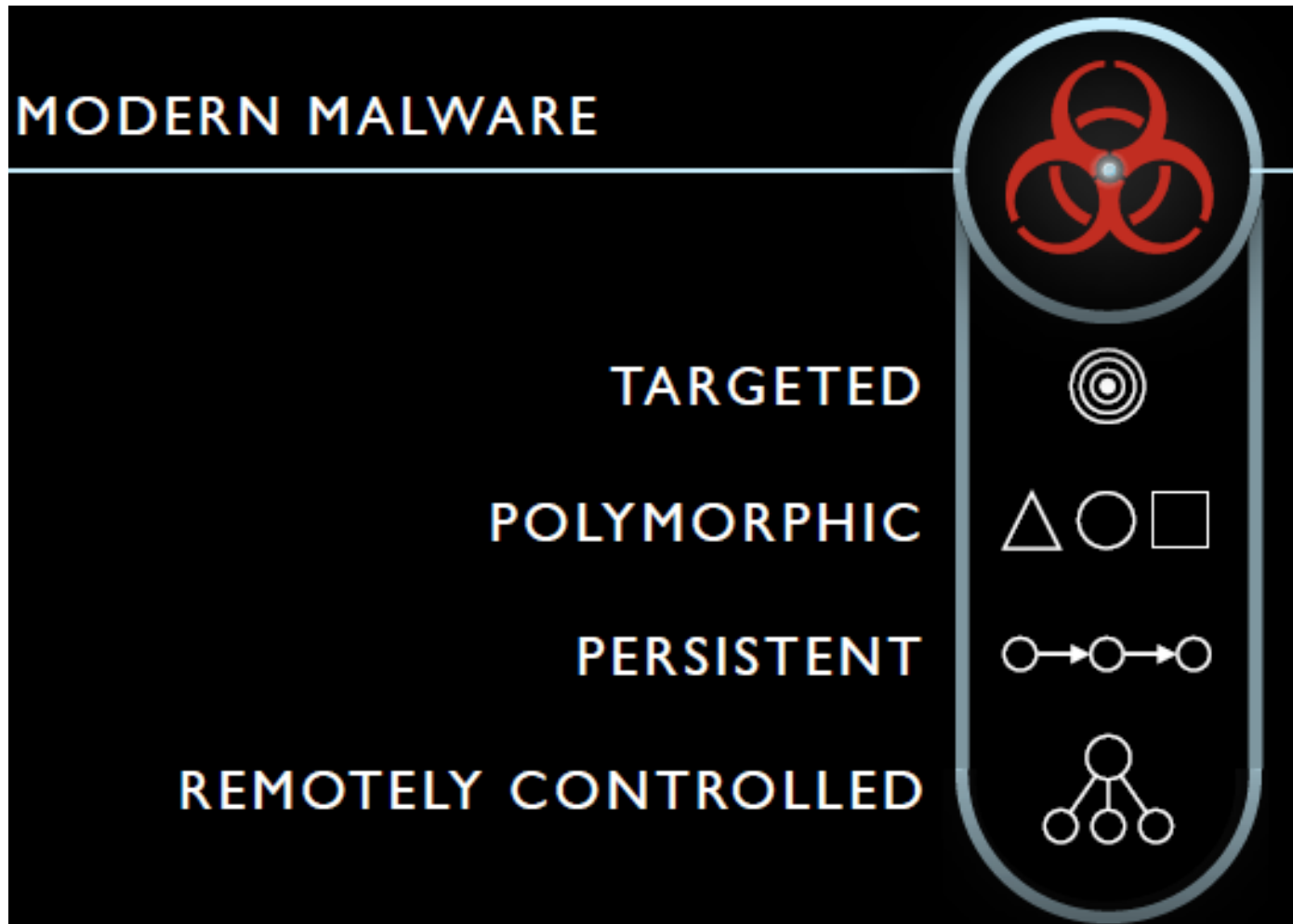


Malware Geliştirme Amaçları

- GOVERNMENT (Ülkeler arası Siber Savaşlar)
- ORGANİZE SUÇLAR
- TERORİST AKTİVİTELER
- AKTİVİSTLER (HACKTİVİZM)

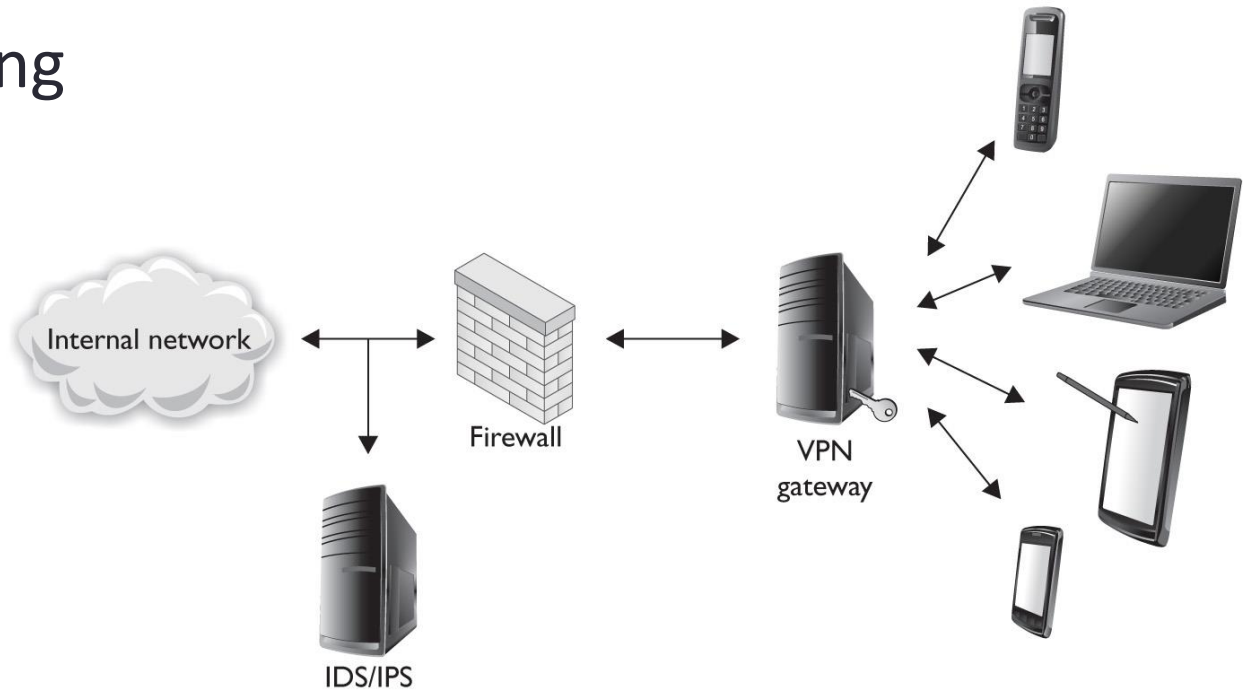


Modern Zararlı Yazılımlar



Geleneksel savunma metotları:

- Anti virüs (imza veri tabanı kontrolü)
- Güvenlik Duvarı (filtreleme, port açma/kapama)
- Saldırı Tespit (IDS) / Saldırı Önleme Sistemleri (IPS)
- Sandboxing



Son Kullanıcılar için

Basit Güvenlik Önerileri

- Harici sürücüleri kullanmadan önce virüs taraması yapın
- İşletim Sistemi güncellemelerini yapın.
- Şüpheli epostaları açmayın
- Anti virüs yazılımı kullanın
- Güvenlik Duvarı kullanın
- Lisanssız yazılım kullanmayın
- Düzenli yedek alın
- Güvenli bağlantı kullanın (SSL etc)
- Ekleri dikkatli açın (.zip, .exe dosyalarını açmayın)
- Güçlü şifreler kullanın, kişisel bilgilerinizi gerekmedikçe paylaşmayın

Son Kullanıcılar için

Basit Güvenlik Önerileri

- Harici sürücüleri kullanmadan önce virüs taraması yapın
- İşletim Sistemi güncellemelerini yapın.
- Şüpheli epostaları açmayın
- Anti virüs yazılımı kullanın
- Güvenlik Duvarı kullanın
- Lisanssız yazılım kullanmayın
- Düzenli yedek alın
- Güvenli bağlantı kullanın (SSL etc)
- Ekleri dikkatli açın (.zip, .exe dosyalarını açmayın)
- Güçlü şifreler kullanın, kişisel bilgilerinizi gerekmedikçe paylaşmayın

Günümüzde MALWARE trendleri



STUXNET Solucanı – 2010 İRAN NÜKLEER TESİSLERİNE SALDIRI (APT)

Günümüzde MALWARE trendleri



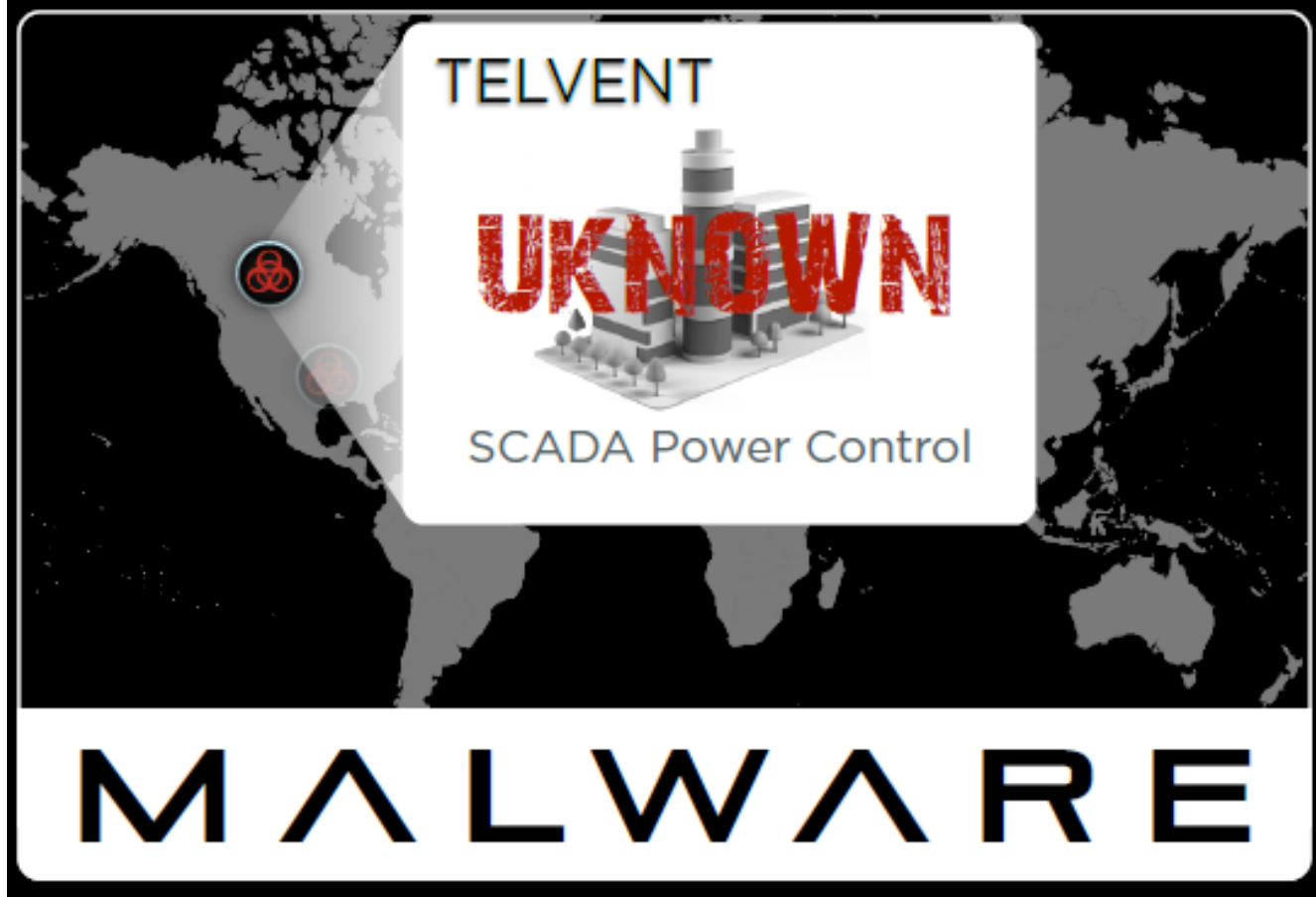
2011 - RSA FİRMASININ KRİPTO ALGORİTMASI ÇALINDI

Günümüzde MALWARE trendleri



SHAMMOON Virüsü – 2012 ARAMCO FİRMASINA SALDIRI

Günümüzde MALWARE trendleri



2012 – TELVENT FİRMASININ SCADA KODLARI ÇALINDI

Ransomware (Fidye Virüsü) nedir?



Günümüzde MALWARE trendleri



HESAP NUMARASI :

FATURA DÖNEMİ : **Kasım 2014**

SON ÖDEME TARİHİ : **14 Kasım 2014**

ÖDENECEK TUTAR : **251,36 TL**



E-Faturamı Görüntüle

URL: <http://efatura.ttnet-fatura.info/>

görmek için tıklayınız

Faturanızı hesap numarası ile ödeyebilir, otomatik ödeme talimatı ve diğer tüm ödeme işlemlerinizi bu numara üzerinden takip edebilirsiniz.

Kredi kartınızla hemen ödemek veya otomatik ödeme talimatı vermek için [tıklayınız](#) ya da 444 0375 TTNET Müşteri Hizmetlerini arayınız.

Faturanızın arka sayfasını görmek için [tıklayınız](#).



















URL: <http://efatura.ttnet-fatura.com/>

2014 – CRYPTOLOCKER SALDIRISI



Günümüzde MALWARE trendleri



Ad	Değişirme tarihi
 0D01 068.JPG.encrypted	24.03.2015 10:55
 0D01 069.JPG.encrypted	24.03.2015 10:55
 0D01 071.JPG.encrypted	24.03.2015 10:55
 0D01 072.JPG.encrypted	24.03.2015 10:55
 0D01 073.JPG.encrypted	24.03.2015 10:55
 0D01 074.JPG.encrypted	24.03.2015 10:55
 0D01 075.JPG.encrypted	24.03.2015 10:55
 0R.70.57-000060.00.jpg.encrypted	24.03.2015 10:55
 0R.72.57-000000.00.jpg.encrypted	24.03.2015 10:55
 0R.74.00-000000.00.JPG.encrypted	24.03.2015 10:55
 001.29.jpg.encrypted	24.03.2015 10:54
 1YTU140025T5509.JPG.encrypted	24.03.2015 10:57
 02.101.013.JPG.encrypted	24.03.2015 10:54
 02.980.021.JPG.encrypted	24.03.2015 10:54
 2TU012510-0205.JPG.encrypted	24.03.2015 10:58
 2TU012550-0081.jpg.encrypted	24.03.2015 10:58
 2TU012610-0067.jpg.encrypted	24.03.2015 10:58
 2TU012610-0078.JPG.encrypted	24.03.2015 10:58

2014 – CRYPTOLOCKER SALDIRISI

Günümüzde MALWARE trendleri

8775563743 nolu hattınıza ait ARALIK-2014 Dönemi Türk Telekom Faturanız

Türk Telekom e-Fatura <haber@eturktelekom.org>

Tarih: 17.12.2014 Çar 15:10

Kime:

TÜRK TELEKOM

E-FATURA (ELEKTRONİK FATURA)



Sayın Müsterimiz,

Son ödeme tarihi **18/12/2014** olan **219,23 TL** tutarındaki güncel faturanıza buradan ulaşabilirsiniz.

[E-FATURA GÖRÜNTÜLE](#)

[E-FATURA ÖDEME](#)

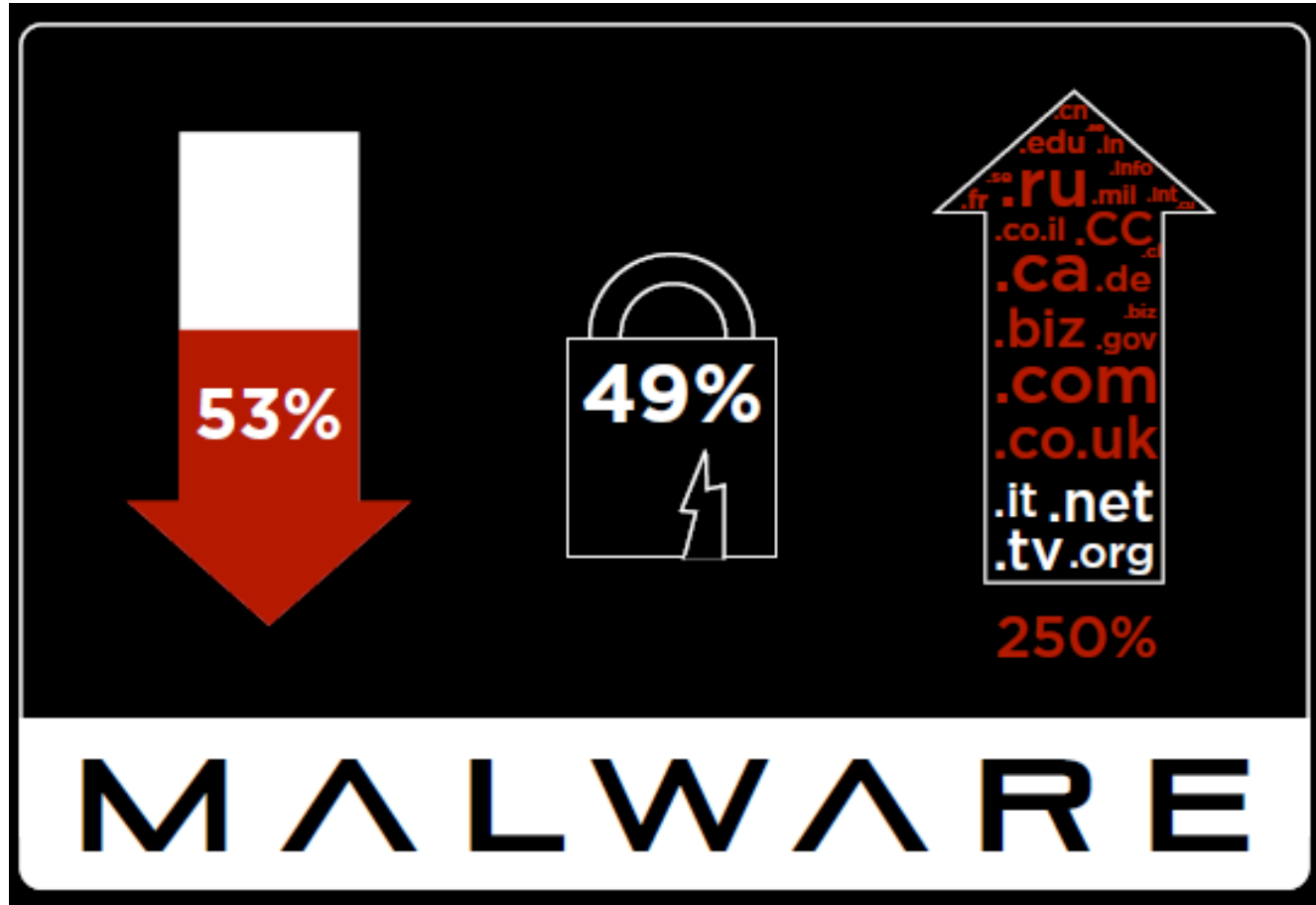
Kağıt tüketimini azaltmak ve çevreyi korumak için e-fatura kullanımı büyük önem taşıyor. Sizde e-fatura tercih ettiğiniz için teşekkür ederiz.

2014 – CRYPTOLOCKER SALDIRISI

WannaCry nedir?



Günümüzde MALWARE trendleri



Her gün ortalama 2 farklı tip Malware ortaya çıkıyor.

Güvenlik Açıklarının sadece %49'u için Zararlı Yazılım'lar geliştirilmiş.

Teşekkürler



Dernek Sitesi: www.agyoneticileri.org

Eğitim Portalı: www.ag.org.tr

Email: [egitim @ agyoneticileri.org](mailto:egitim@agyoneticileri.org)

www.facebook.com/AgYoneticileriDernegi