



# **KURUM AĞLARINI ÖNEMLİ ZARARLI YAZILIM SALDIRILARINDAN KORUMA**

**Osman PAMUK**

- Giriş
- Örnek Zararlı Yazılımlar
  - Conficker
  - Stuxnet
- Önemli zararlı yazılım sızma noktaları ve korunma yöntemleri
  - Taşınabilir veri depolama sürücülerin kontrolü
  - İstemci tarafındaki uygulama zafiyetlerinin giderilmesi
  - Sunumcu servislerindeki zafiyetlerin giderilmesi
  - Yetkili kullanıcı hesaplarının kontrolü
- Sonuç

- **Bu yazılımlar niye zararlı?**
  - Botnet'ler aracılığı ile yapılan saldırılar
    - Spam gönderme
    - DDOS saldırıları
  - Banka hesap bilgilerinin veya oyun şifrelerinin ele geçirilmesi
  - Şirketlere veya ülkelere ait gizli bilgilere ulaşılması veya hassas bilgilerin değiştirilmesi
  - Siber savaş veya savunma

## • Conficker

- 2008 ekim ayında yayınlanan MS08-067 açıklığını kullanmakta
- Windows XP SP2 ve Windows 2003 SP1 makinalarında çok etkili
- 2009'un başında 3 milyondan fazla bilgisayara bulaştığı düşünülmekte

## • Stuxnet

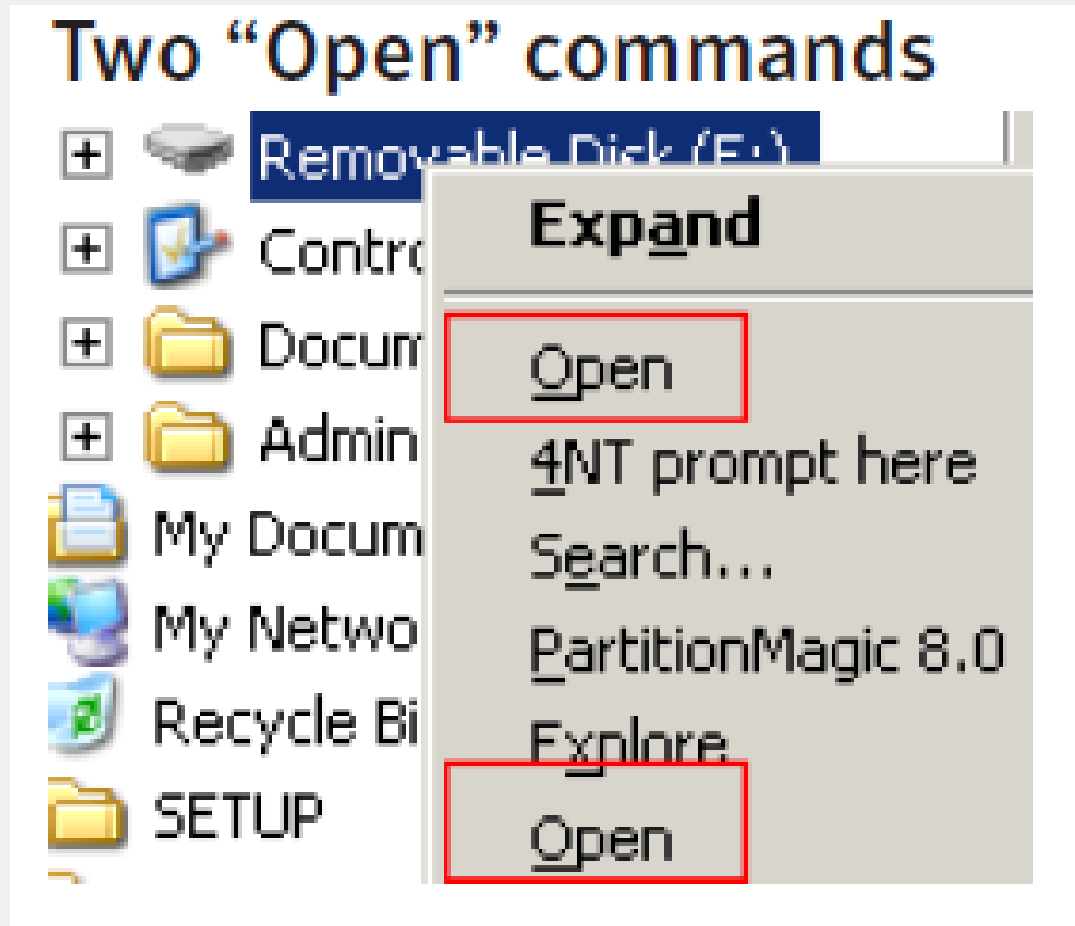
- İlk tespit edilme: 2009'un haziran ayı
- Şimdiye kadar tespit edilen en karmaşık zararlı yazılım örneği
- İçinde 4 farklı '0-day' açıklığı mevcut
- 2 yasal sertifika ile kendi dosyalarını gizlemeye çalışmakta
- Bilinen ilk PLC rootkit örneği

- **Modern Ağlarda bizi dış dünyadan (internet'ten) koruyan neler var?**
  - Güvenlik duvarı, saldırı tespit ve engelleme sistemleri
  - Ağların internet ile bağlantısını fiziksel olarak kesmek
- **Peki bu yazılımlar nasıl oluyor da farklı ağlara ulaşabiliyor?**
  - Taşınabilir veri depolama cihazları ile

- Değiştirilmiş 'Autorun.inf' dosyası saldırısı
  - Conficker:



- **Stuxnet:**



## Peki ne yapabiliriz?

- Nisan 2007'de Windows 7'deki autorun özelliği değiştirildi
- Kasım 2009'da Windows 7'deki autoplay özelliği eski versiyonlara uygulanabilir hale getirildi
- Şubat 2011'de bu güncelleme WSUS'la dağıtılabilir 'Important, **non-security**' bir yama haline getirildi
- Microsoft: 'it's not a bug, it's a feature'

- **MS10-046: Windows Kabuğu Kısayol Açıklığı**
  - Kullanımı için zararlı içerikli bir 'LNK' uzantılı dosyanın bulunduğu klasörün açılması yeterli
  - 0-day açıklık
  - Windows 2000'den Windows 7'ye kadar etkili

- **Peki koruma için ne yapabiliriz?**
  - Farklı ağlar arasındaki veri akışı ihtiyaçları belirlenmeli ve ihtiyaç dışındaki veri akışına izin verilmemeli
  - Veri akışının sadece güvenliği sağlanmış noktalardan kontrollü bir şekilde yapılması
- **Örnek**
  - Windows güncellemelerinin internete bağlı olmayan ağlara aktarılması

## • İstemci Tarafındaki Uygulama Zafiyetleri

- Web tarayıcıları
  - IE, Mozilla Firefox, Chrome
- Diğer doküman görüntüleyici ve düzenleyicileri
  - Microsoft Ofis Uygulamaları, Adobe Acrobat Reader, Foxit, Flash Player, Multimedya Uygulamaları

## • Niye kritik?

- Çünkü çoğunlukla zararlı yazılımların ilk giriş noktası burası

- **RSA Şirketi Adobe Flash Player açıklığı saldırısı:**
  - **Elektronik posta** ile gönderilen içine **Flash Player**'daki açıklığını kullanan dosyası flash dosyası yerleştirilmiş **excel dosyasının** RSA çalışanları tarafından açılması
  - Ele geçirilen bilgisayarda hak yükseltmenin gerçekleştirilmesi
  - Hassas bilgilere erişim
  - Hassas bilgilerin dışarıya çıkarılması
- **Microsoft IE Açıklığı ve Oak Ridge Ulusal Laboratuvarına sızma saldırısı:**
  - **530** kurum çalışanına insan kaynaklarından geliyor süsü verilerek **elektronik posta** mail gönderilmiş ve **57** kullanıcı **maildeki linke** tıklamıştır

- **Peki nasıl korunacağız?**

- Güncellemeler hızlı bir şekilde uygulanmalı
- Güncelleme yoksa, önerilen güvenlik ayarları yapılmalı

- **Fakat ‘0-day’ açıklıklarına veya çok hızlı kullanılmaya başlanan açıklıklara karşı ne yapacağız?**

- Kullanıcılar bilinçlendirilmeli, güvenilir olmayan dokümanlar açılmamalı ve bağlantılara tıklanmamalı
- İnternet’e rahat ulaşımın olduğu ağlar ile kritik bilgilerin bulunduğu ağlar arası iletişimin kontrolü

- **Sunumcu Servislerindeki Zafiyetler**
  - Yayılmak için kullandıkları **uzaktan kod çalıştırma açıklıkları**:
    - Conficker: **MS08-067** (RPC)
    - Stuxnet: **MS08-067, MS10-061** (Print Spooler)
  - **Niye Kritik?**
    - Herhangi bir kullanıcı eylemine ihtiyacı yok

## MS08-067 ile yayılım:

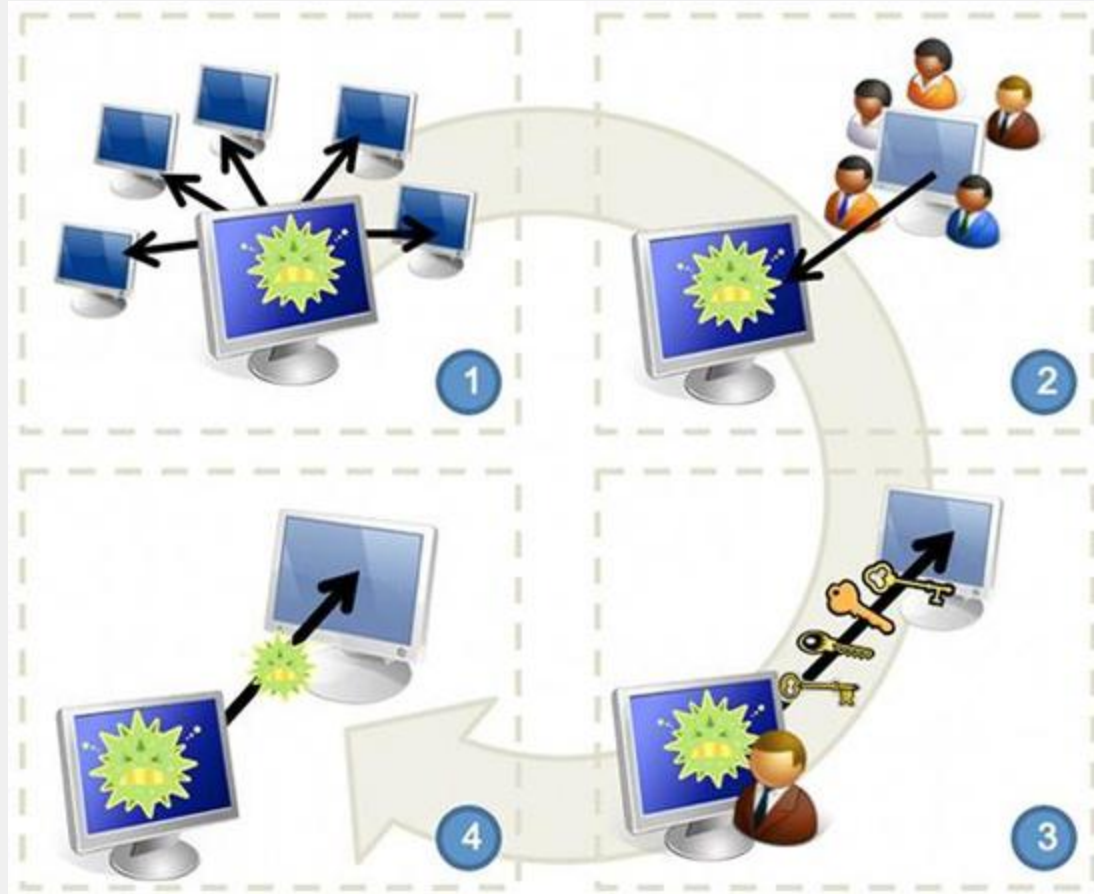


1. MS08-67 Açıklığı ile kabuk kodun enjekte edilmesi,
2. Geri bağlanmanın gerçekleştirilmesi
3. Solucan dosyasının gönderilmesi

- Peki korunma için neler yapmamız lazım?
  - Kritik güncellemelerin acilen yapılması
  - Güncelleme hazır değilse gerekli güvenlik sıkılaştırmalarının yapılması
- ‘0-day’ açıklıklara karşı ne yapacağız?
  - Saldırı yüzeyinin azaltılması
    - Gereksiz servislerin kapatılması
    - Farklı bilgisayar ağların oluşturulması
    - Ağlar arasındaki iletişimin kısıtlanması

- Yetkili Kullanıcı Hesaplarının Kullanımı
  - Conficker:
    - Oturum açmış kullanıcıların hakları ve ağ paylaşımları
    - Kullanıcı isimlerinin bulunması ve zayıf şifrelerin sözlük saldırısı ile kırılması
  - Stuxnet:
    - Oturum açmış kullanıcıların hakları ve ağ paylaşımları

# Kullanıcı Hesaplarının Saldırı



1. Ağdaki bütün makinelerin bulunması
2. Her makinadan kullanıcı hesabı isimlerinin toplanması
3. Her kullanıcı ismi için şifre tahmin etmenin gerçekleştirilmesi
4. Eğer kimlik doğrulama gerçekleşirse solucanın kopyalanması

## • Önlem

- Sistem yöneticilerine sadece ihtiyaçları olan hakların verilmesi
- Yerel yönetici hakkına sahip hesapların dikkatli kullanımı
- Bu hakların sadece gerekli olduğu zaman kullanılması (run as)

- Güncel güvenlik açıklıklarını ve saldırı yöntemlerini takip etme
- Gerekli önlemleri hızlı bir şekilde alma
- Veri akışının kontrolünün sağlanması
- Saldırı yüzeyinin azaltılması
- Yetkilik kullanıcı hesaplarının dikkatli kullanımı
- Kullanıcıların bilinçlendirmesi



## TÜBİTAK-BİLGEM-UEKAE Bilişim Sistemleri Güvenliği Bölümü

pamuk@uekae.tubitak.gov.tr

0 262 468 1568

[www.uekae.tubitak.gov.tr](http://www.uekae.tubitak.gov.tr)

[www.bilgiguvenligi.gov.tr](http://www.bilgiguvenligi.gov.tr)