



2008 Yılı Kritik Güvenlik Açıkları

Bahtiyar BİRCAN
Uzman Araştırmacı

bahtiyar @ uekae.tubitak.gov.tr
www.bilgiguvenligi.gov.tr

5Haziran 2009

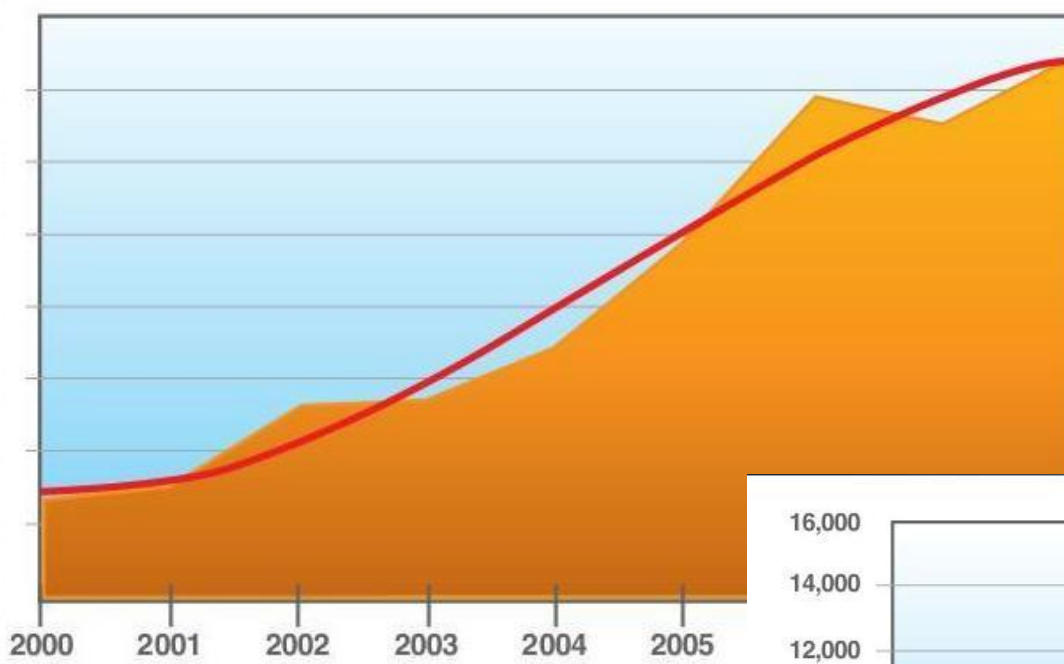
- 2008 Güvenlik Olayları Özeti
- Conficker virüsü
- Sahte SSL Sertifikaları
- DNS Önbellek Zehirlenmesi
 - Demo : İç DNS sunucu zehirlenme + Java update ile istemcilerin ele geçirilmesi
- Internet Explorer 7 XML açıklığı
 - Demo : Kötü niyetli web sitesi ile istemcilerin ele geçirilmesi

- Web Tabanlı saldırılar
- Spam
- Politik çatışmaların sanal yansımaları
 - Gürcistan – Rusya
 - Filistin – İsrail
 - Tibet – Çin
- Tarayıcı açıklıkları
- Antivirüs firmalarına saldırılar
- Conficker virüsü
- Sahte SSL Sertifikaları
- DNS Önbellek Zehirlenmesi
- Internet Explorer 7 (XML) açıklığı

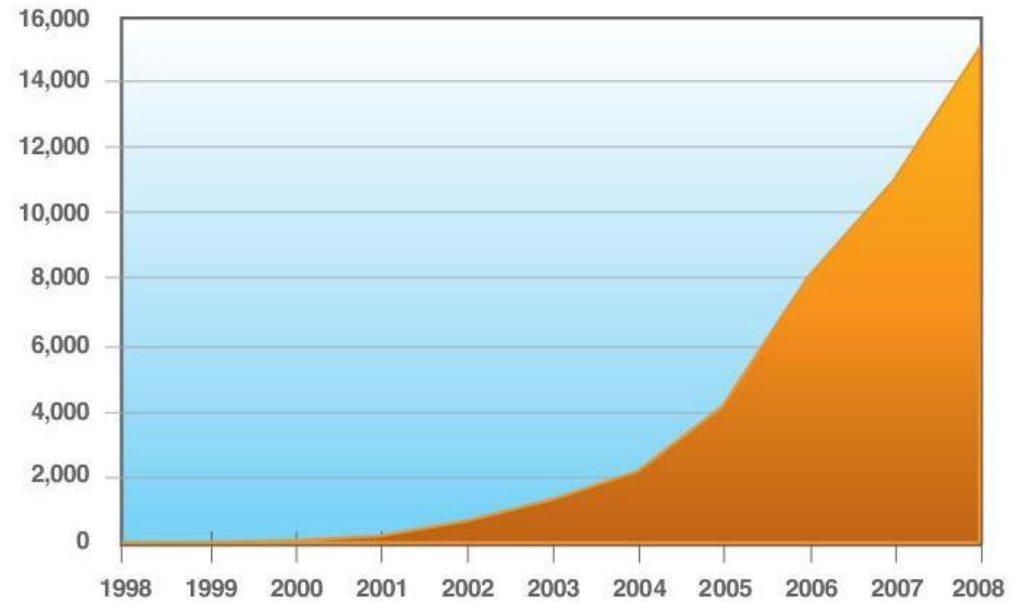
2008 güvenlik olayları özeti



UEKAE

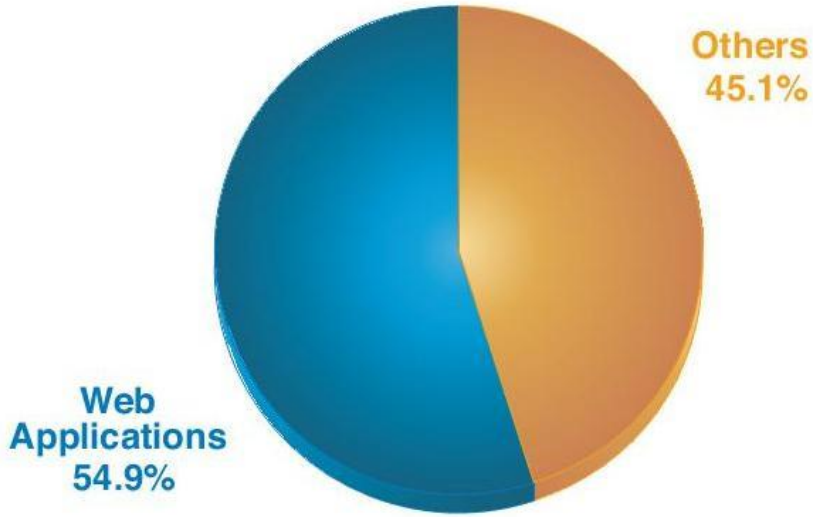


Vulnerability Disclosures, 2000 – 2008

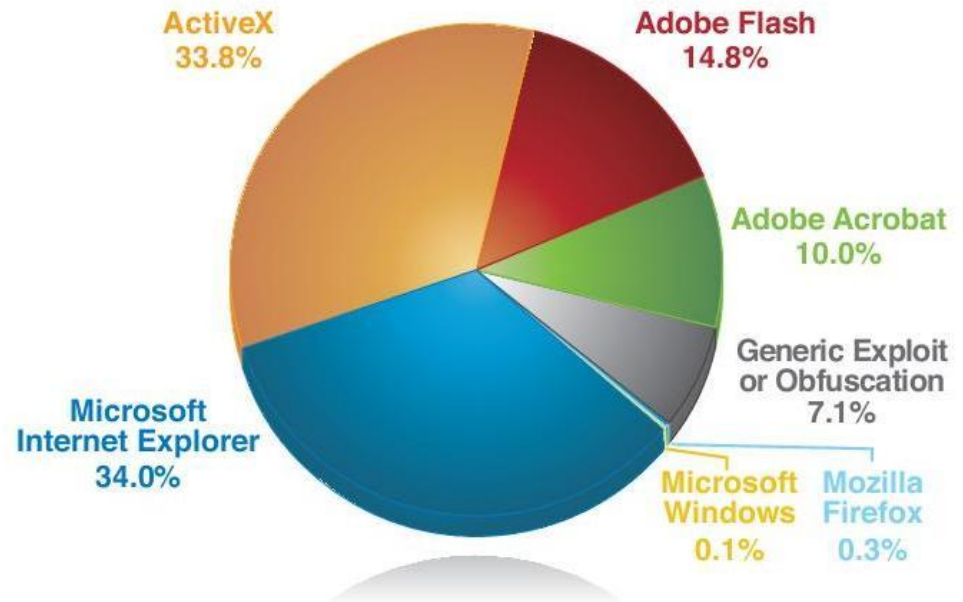


Cumulative Count of Web Application Vulnerabilities, 1998 – 2008

2008 güvenlik olayları özeti



Percentage of Disclosures that are Web Application Vulnerabilities, 2008

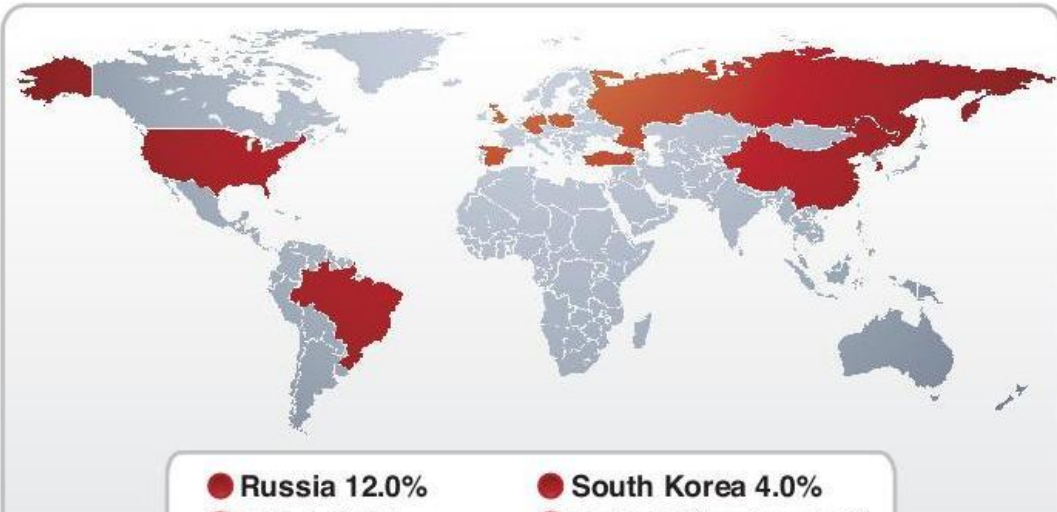


Malicious Website Exploits by Affected Application, ISS Cobion Crawler, 2008 Q4

2008 güvenlik olayları özeti

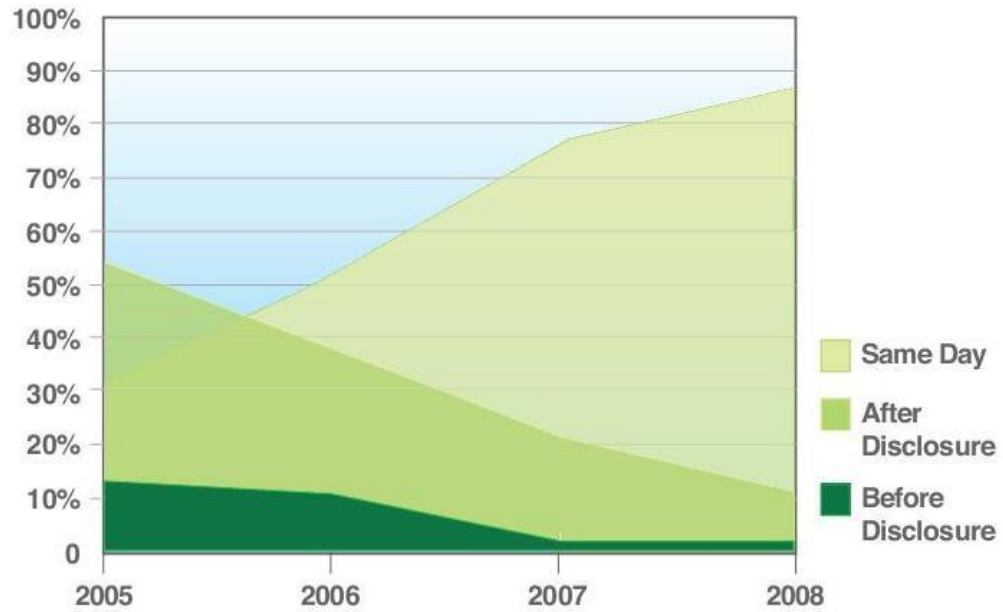


UEKAE



- Russia 12.0%
- U.S.A. 9.6%
- Turkey 7.8%
- Brazil 5.6%
- China 4.4%
- South Korea 4.0%
- United Kingdom 3.3%
- Spain 3.2%
- Poland 3.2%
- Germany 3.2%

Geographical Distribution of Spam Senders



Rise in 0-day Exploits

Conficker virüsü

- **Açıklığın yapısı:**

- 23 ekim 2008 tarihinde MS08-67 yaması Microsoft tarafından yayınlandı
- 27 ekim 2008 tarihinde Ulusal Bilgi Güvenliği Kapısında (www.bilgiguvenligi.gov.tr) açıklık ile ilgili duyuru yayınlandı.
- Microsoft normal açıklık yayınlama periyodunun dışına çıkarak açıklığı duyurmak zorunda kaldı
- Açıklık tüm Windows İşletim Sistemlerini etkilemektedir.
- Açıklık Windows Server RPC servisinde ve *netapi32.dll* kütüphanesindeki hatalardan kaynaklanmaktadır.
- Koddaki hatadan dolayı yetkisiz bir kullanıcı özel tasarlanmış bir RPC istemiyle uzaktan kod çalıştırabilmektedir
- Açık duyurusundan bir gün sonra açıklığı kullanan virüsler (Conficker, Downadup, Kido) yayılmaya başladı.
- Ocak 2009'da virüsün yayılmasında patlama oldu ve internete bağlı virüs bulaşan bilgisayar sayısının 9 ile 15 milyonu arasında olduğu tahmin ediliyor. (Kaynak: F-Secure)
- Microsoft , virüsün yazarını yakalamada yardımcı olanlar için ödül vereceğini duyurdu

- **Etkileri :**
 - Dünyada ve Türkiyede birçok kamu ve özel kurum virüsten etkilendi
 - Atatürk Havalimanı
 - İngiltere Savunma Bakanlığı
 - Fransa Deniz Kuvvetleri
 - Norveç polisi
 - Alman Silahlı Kuvvetleri

- **Çalışma Şekli :**

- Açıklığı kullanan vürüsler çeşitli yollarla (USB autorun, zararlı web sayfası, dosya/e-posta eklentisi..) bilgisayara bulaşiyor
- Bulaştığı bilgisayardaki yönetici hesaplarını kırmaya çalışıyor
- Yerel ağı tarayarak ağdaki diğer bilgisayarlara sıçramaya çalışıyor
- Antivirüs yazılımları ve Windows güncelleme sitelerine erişimi engelliyor
- P2P uygulamaları ile diğer bilgisayarlara sıçramaya çalışıyor

- **Önlemler :**

- Microsoft tarafından yayınlanan yamanın (ms08-67, KB958644) uygulanması
- Antivirüs üreticileri tarafından sağlanan temizleme araçlarının kullanılması
- Antivirüs yazılımlarının güncellenmesi
- USB bellekler için otomatik çalıştırma seçeneklerinin devre dışı bırakılması
- Dosya paylaşımlarının kontrol altına alınması

Sahte SSL Sertifikaları

- **Açıklığın yapısı**

- 30 Aralık 2008 tarihinde 25. Chaos konferansında açıklık duyurusu ve demosu yapıldı
- 31 Aralık 2008 tarihinde Ulusal Bilgi Güvenliği Kapısında (www.bilgiguvenligi.gov.tr) açıklık ile ilgili duyuru yayınlandı
- Açıklık temelde SSL Sertifikaları veren sertifikasyon makamlarının (CA) tahmin edilebilir seri numaraları ve sertifika imzalama için MD5 algoritmasını kullanmalarından kaynaklanmaktadır
- Açıklığa dair teknik ayrıntılar [http:// www.win.tue.nl/hashclash/rogue-ca/](http://www.win.tue.nl/hashclash/rogue-ca/) adresinden edinilebilir

- **Etkileri**

- Açıklığın demosu

<https://i.broke.the.internet.and.all.i.got.was.this.t-shirt.phreedom.org/> adresinden görülebilir.

- Bu yöntemle üretilen SSL sertifikaları kullanılarak sahte e-ticaret ve internet bankacılığı siteleri oluşturulabilir

- **Önlemler**

- Sertifikasyon makamları :

- İmzalama işlemlerinde MD5 özet algoritması yerine SHA-1 gibi daha güçlü algoritmaların kullanılması
- Tahmin edilmesi zor, rastgele seri numarası kullanımı

- Son kullanıcılar :

- MD5 ile imzalanmış SSL sertifikaları kullanan web sitelere girilmemesi
- Firefox kullanan son kullanıcıların SSL Blacklist eklentisinin kullanılması

DNS Önbellek Zehirlenmesi

• Açıklığın yapısı

- 9 Temmuz 2008’de Dan Kaminsky tarafından duyuruldu
- 1 Ağustos 2008 tarihinde Ulusal Bilgi Güvenliği Kapısında (www.bilgiguvenligi.gov.tr) açıklık ile ilgili duyuru yayınlandı.
- DNS protokolünün temel uygulamasında olduğu için hemen hemen tüm yazılım üreticileri etkilendi (Cisco, Microsoft, Sun...)
- Dan Kaminsky birçok firma ile işbirliği yaparak aynı anda tüm sistemler için açıklık duyurusundan 2 gün önce yama çıkartılması sağlandı
- Açıklık sadece “**recursion**” özelliği açık olan sunucuları etkilemektedir.
- Recursion özelliği açık olan DNS sunucular kendi üzerinde olmayan domainlere ait bilgileri o domainin yetkili DNS sunucusuna sorup istemciye aldıkları cevabı iletirler
- Bu sorgulama sırasında DNS mesajının “header” bölümünün ilk 16 biti **TXID** olarak isimlendirilmiş bir “nonce” olarak tanımlıdır ve sorguyu düzenleyen program tarafından doldurulan bir alandır. Bu alan, sorguya verilen yanıtta da birebir kopyalanır ve böylece soru-yanıt eşleştirmesi sağlanabilir.
- Araya girilerek yapılan önbellek zehirlenmesi saldırıları, bu sayının tahmin edilmesine dayanır.

- Etkileri
 - Olta (phishing) sitelerinin kolayca kurulup işletilmesi
 - Araya girme saldırıları ile kullanıcı ismi ve parola gibi hassas bilgilerin elde edilmesi
 - Başka saldırılarla birleştirilerek saldırıların gerçekleştirilmesi
 - Sahte SSL Sertifikaları
 - Internet Explorer 7 XML açıklığı

DEMO!

- Önlemler
 - DNS sunucuların yamanması
 - DNSSEC kullanımı
 - Yamanamayan sunuculara erişimin engellenmesi
 - Sahte IP adreslerinden gelen trafiğin filtrelenmesi
 - Yerel DNS önbelleği kullanılması
 - Yamanamayan sunucuların önüne güvenlik duvarının konulması
 - Trafiğin başka sunucuya yönlendirilmesi

Internet Explorer 7 XML açıklığı

• Açıklığın yapısı

- 9 Aralık 2008 tarihinde McAfee , 12 Aralık 2008 tarihinde Microsoft firmaları tarafından duyuruldu .
- Microsoft 8 gün sonra , 17 Aralık 2008 tarihinde açıklıkla ilgili yama yayınladı (ms08-78)
- 10 Aralık 2008 tarihinde Ulusal Bilgi Güvenliği Kapısında (www.bilgiguvenligi.gov.tr) açıklık ile ilgili duyuru yayınlandı.
- Açıklık, Internet Explorer 7 yazılımının veri kaynaklarına bağlanma (databinding) fonksiyonunda bulunmaktadır.
- Bu fonksiyonda uzaktan kod çalıştırılmasına izin veren geçersiz işaretçi referansı (invalid object pointer reference) açıklığı vardır.
- Yaygın olarak kullanılan saldırı metodlarında bir web sayfası içindeki XML etiketleri (tag) ile *databinding* fonksiyonu çağırılmakta ve bu etiketlerin IE7 tarafından işlenmesi sırasında yukarıda bahsedilen açıklık ortaya çıkmaktadır.

- Etkileri
 - Kötü niyetli web sitelerini ziyaret eden istemcilerin tamamen ele geçirilmesi ve hassas bilgilerin elde edilmesi
- Önlemler
 - Microsoft tarafından yayınlanan yamanın uygulanması (MS08-78 ,KB960714)
 - Alternatif web tarayıcıların kullanılması
 - Zaafiyeti sömüren sitelere erişimin kısıtlanması

DEMO!

Teşekkürler

Bahtiyar BİRCAN

www.bilgiguvenligi.gov.tr
bahtiyar @ uekae.tubitak.gov.tr