

Bilişim Terörü ve Bilişim Savaşları

Can ALPTEKİN
ca@dikey8.com

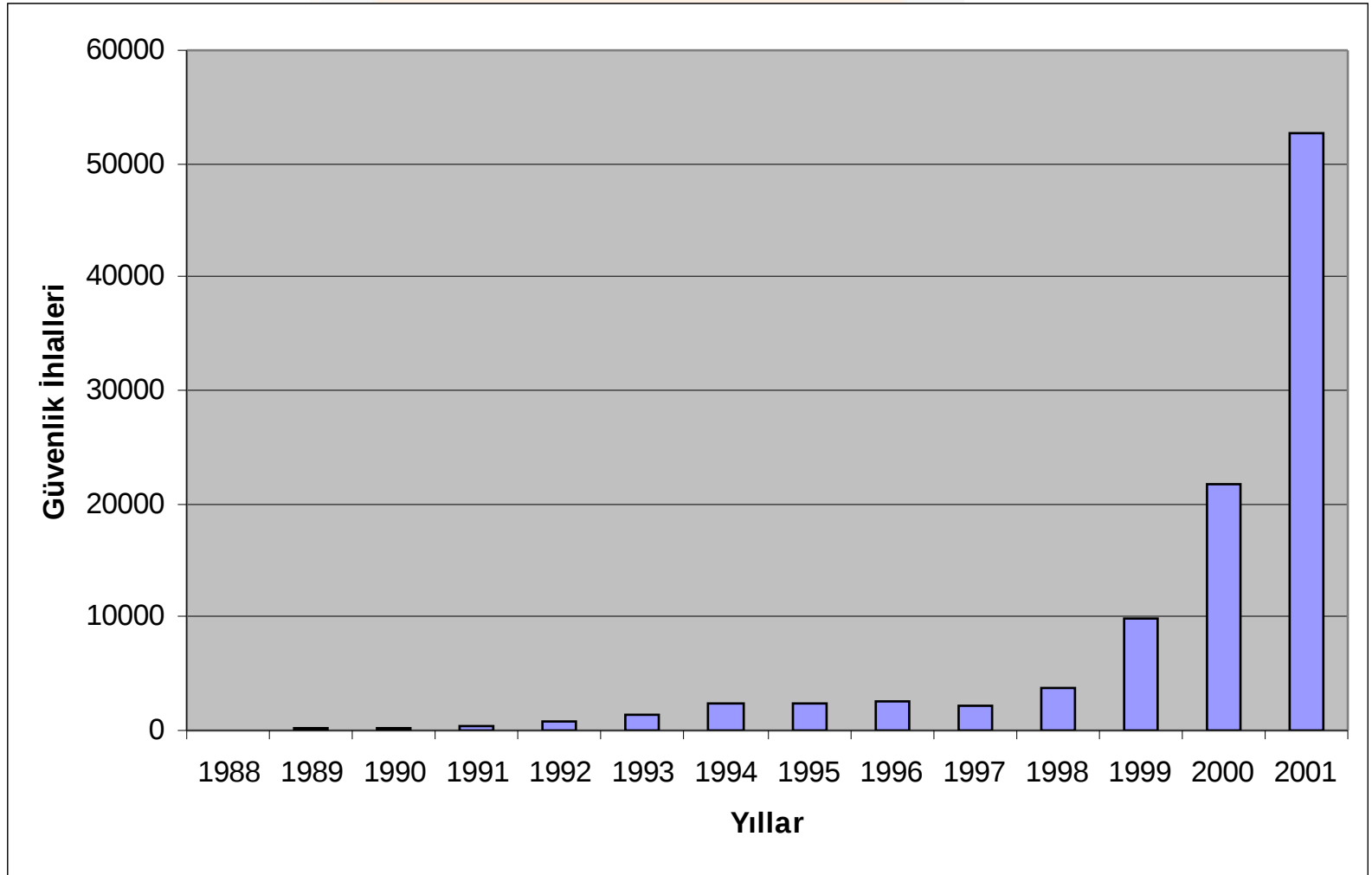
- Teknolojinin gelişmesi ile beraber artış gösteren bilişim suçları, “teknolojinin yardımı ile genellikle sanal bir ortamda kişi veya kurumlara maddi veya manevi zarar vermek” olarak tanımlanabilir.

■ Belli başlı Bilişim Suçları

- Telekomünikasyon hizmetleri hırsızlığı
- Bilgisayar Sistemlerinin başka suç işlemek için kullanılması
- Bilgi Korsanlığı, Sahtecilik ve Kalpazanlık
- Kötü,Çirkin görüntü ve kayıtların yayılması
- Tehdit ve Gasp
- Siber Terör

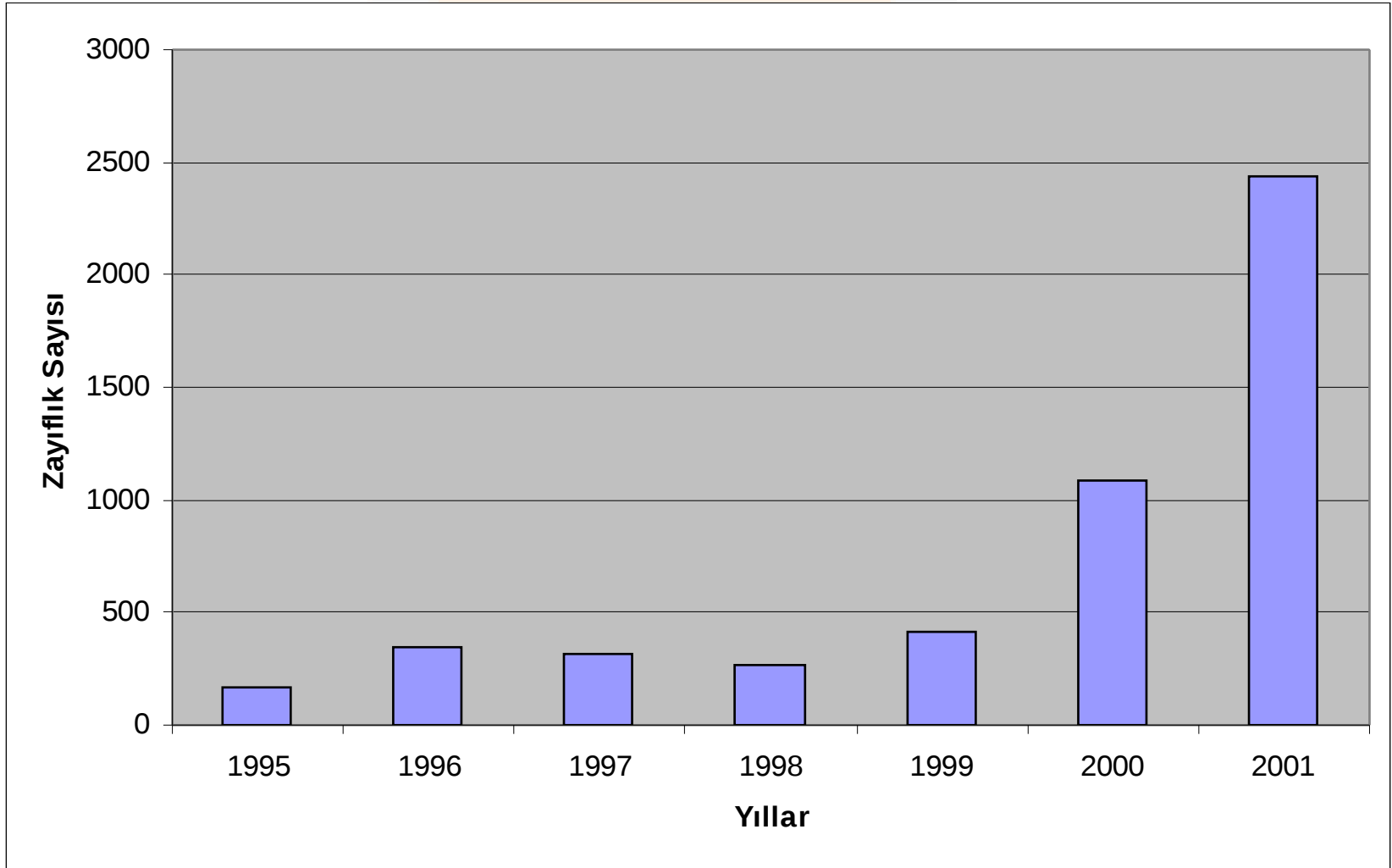
Kaynak : Siber Terörizm ve Ulusal Güvenliğe Tehdit Oluşturma Boyutu
Yrd.Doç.Dr. Mehmet Özcan

Artan Ağ Güvenliği İhlalleri



Kaynak : CERT

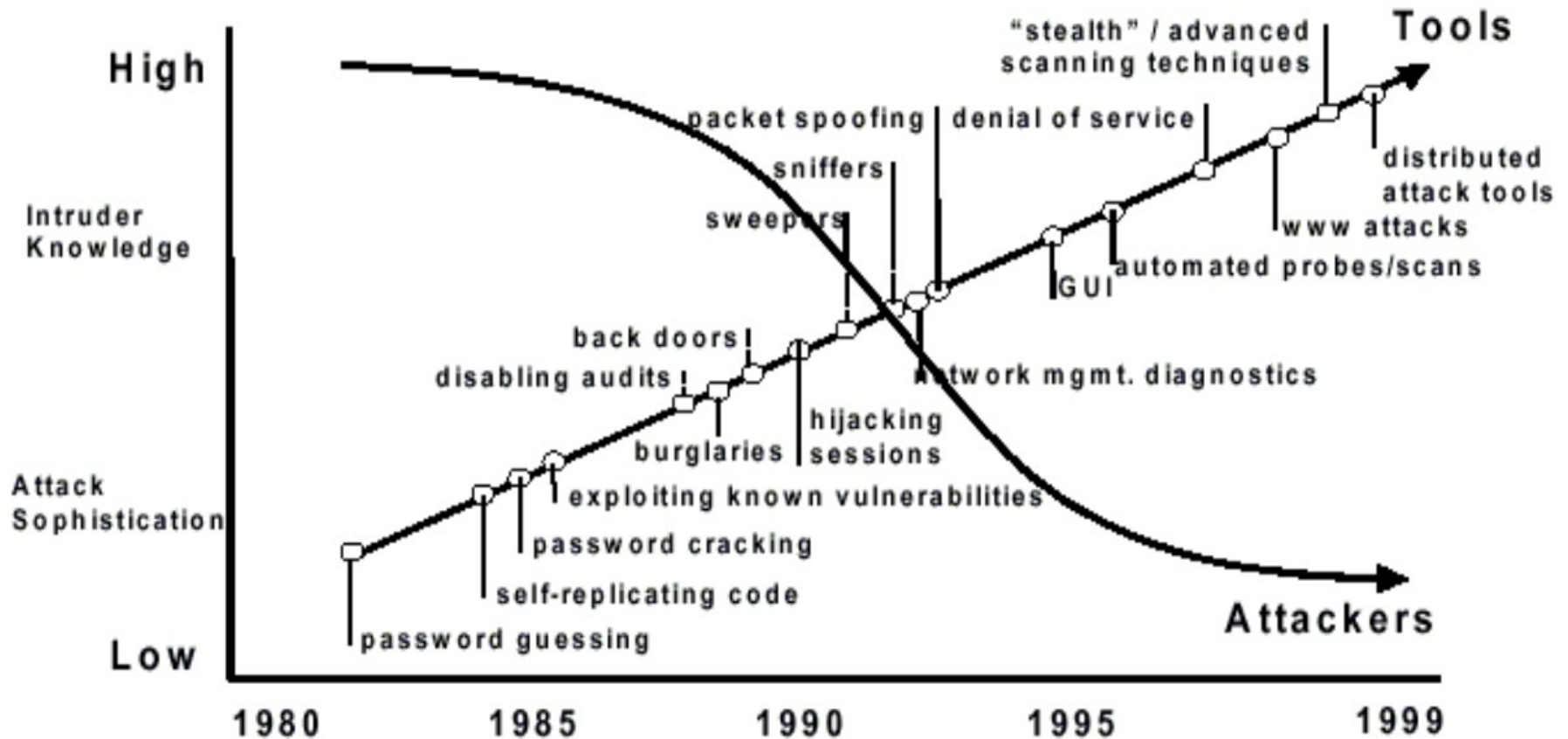
Zayıflık Sayısındaki Artış



Kaynak : CERT

Gerekli Etkenler :

- Fırsat
- İrade ve Motivasyon



- Saldırı sayısı artıyor
- Saldırgan sayısı artıyor
- Saldırgan'ın bilgi düzeyi **düşüyor !!**

- Hedefli ve Bilinçli Saldırgan
- Hedefsiz ama Bilinçli Saldırgan
- Hedefli ama Bilinçsiz Saldırgan
- Hedefsiz ve Bilinçsiz Saldırgan

- Hedefli ve Bilinçli Saldırgan,
 - Belli bir amacı var
 - Sistematik çalışıyor
 - Bilgi seviyesi yüksek
 - Kendini saklamaya özen gösteriyor
 - Kendine özel araçlar kullanıyor
 - Tehlikeli ve Gerçek Kötü

- Hedefsiz ama Bilinçli Saldırgan
 - Amacı yok
 - Internet'te rastlantısal hedefler seçiyor
 - Belli bir sistematığı yok
 - Kendini saklamayı çoğunlukla başarıyor
 - Bilgi düzeyi yüksek ama bu işi kişisel eğlence amaçlı yapıyor
 - Yakalanma kaygısı var

- Hedefli ama Bilinçsiz Saldırgan
 - Belli bir amacı var
 - Bilgi seviyesi az düzeyde
 - Kendini ispatlama endişesinde
 - Kulaktan dolma bilgileri var
 - Büyük ölçüde zararsız
 - Genellikle otomatik araçları kullanıyor
 - Çok fazla iz bırakıyor

- Hedefsiz ve Bilinçsiz Saldırgan
 - Amacı yok
 - Rastlantısal hedefler seçiyor
 - Kulaktan dolma bilgileri var
 - Kolaylıkla takip edilebiliyor
 - Daha çok DoS saldırıları gerçekleştiriyor
 - Saldırgan profilinde en büyük yüzdeyi oluşturuyor

Türkiyede Internet tehdidi: ÖSYM örnek çalışması
B. Dayıoğlu, O. Şehitoğlu, A. Özgit

Inet-Tr 2001

<http://www.dikey8.com/docs/inettr2001-osym.pps>

Solucan (Worm) Kavramı

- Siber savaşta kendi başlarına çalışan saldırganlar
- Morris Worm
- Hedef ayırımı yapmıyorlar
- Genellikle kişisel zevk için üretiliyorlar
- Çok hızlı ve etkili yayılıyorlar
- En büyük zararları veriyorlar
 - Nimda dünya üzerinde IT güvenliğine ayrılan bütçeden daha fazla zarar verdi.
- Giderek Gelişiyorlar

- Yeni Nesil Worm (1999 HNN)
 - Dağıtım
 - FTP, Mail, Web, DCC, ...
 - Çalıştırma
 - Bulaşma
 - Kayıtlı ve Sistemantik Çalışma
 - Yayılma
 - Yeniden Paketleme, Web, FTP, Mail, Network, DCC, ...
 - Güncelleme
 - Hedef ve program güncelleme
 - Kendini gizleme güncellemesi
 - Vurucu Darbe





Teşekkürler

Teşekkürler