KURUMSAL AGLARDA ZARARLI YAZILIMLARLA MÜCADELE YÖNTEMLERI

Gökhan AKIN, Enis KARAARSLAN

gokhan.akin@itu.edu.tr, enis.karaarslan@ege.edu.tr

UlakNet Computer Security Incident Response Team

Ulaknet Çalistayi 2008 / Konya

1. GIRIS (1)

ZARARLI YAZILIMLAR

Ingilizce "malicious software" in
kisaltilmis hali olan malwareler,
çesitli yollar ile bir bilgisayara bulasip,
bulastigi bilgisayar ve çevresine zarar vermesi
için yazilmis programlardir.

1. GIRIS (2)

BULASMA SEBEPLERI

-Yazilimlardaki güvenlik açiklari,

-Basit atanan sifreler,

-E-posta, sohbet yazilimlari..vs den gelen eklentiler,

-Kaçak yazilimlar,

-USB ve benzeri ara birimlerden baglanan otomatik çalistirma betigine gizlenen yazilimlar

1. GIRIS (3)

ALINABILECEK ÖNLEMLER

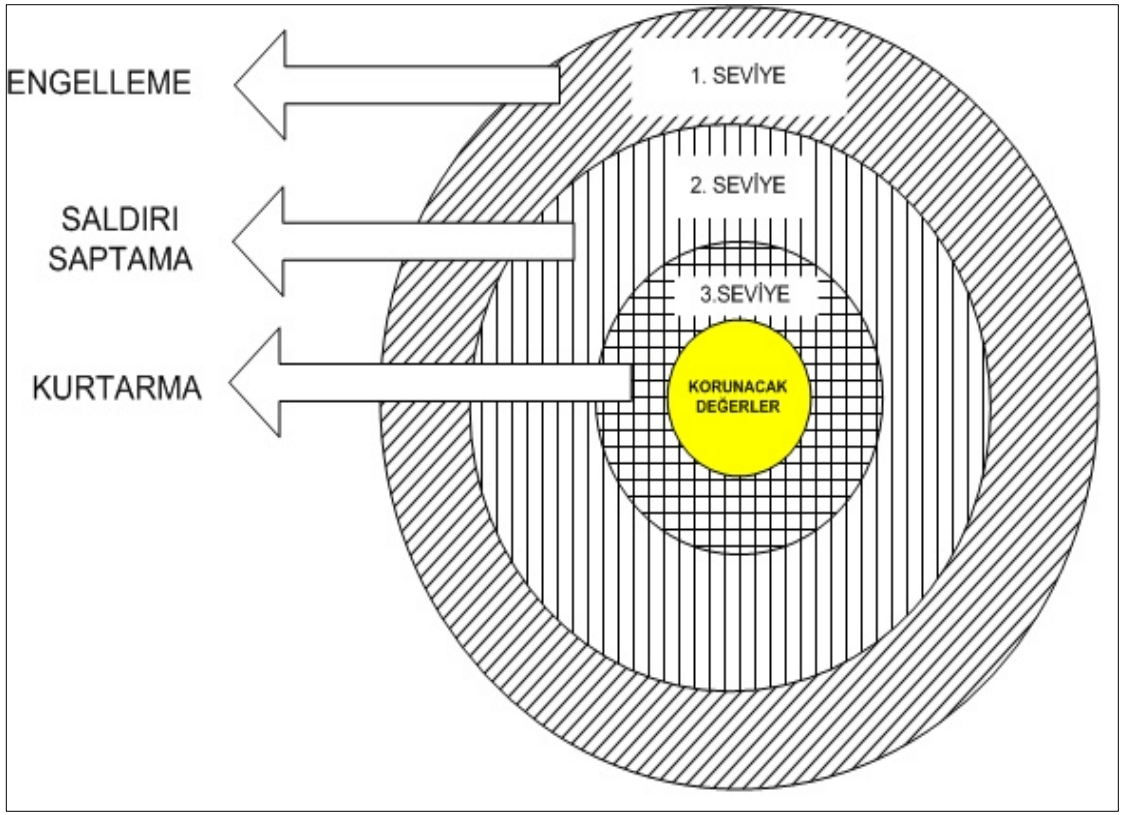
-Kurumsal politika ve bilinçlendirme çalismalari

-Makinelerde alinabilecek temel önlemler

-Agda alinabilecek temel önlemler

1. GIRIS (4)

ÖNLEMLERIN AMAÇLARI



2. KURUMSAL POLITIKA VE BILINÇLENDIRME ÇALISMALARI (1)

Kurumsal kullanim politikalari tüm yerel aglarda olmazsa olmaz bir gereksinimdir.

Örnek Politikalar :http://csirt.ulakbim.gov.tr/politika/
(Reklam ☺)

2. KURUMSAL POLITIKA VE BILINÇLENDIRME ÇALISMALARI (2)

Isletim sistemi seçiminde kullanicilar destek verilebilecek isletim sistemlerine yönlendirmelidir.

Açik kaynak kodlu isletim sistemleri, örnegin Pardus'a kullanicilar yönlendirilebilir.

2. KURUMSAL POLITIKA VE BILINÇLENDIRME ÇALISMALARI (3)

- Anti-Virüs yazilimi kullanimi

- Sifre belirlenmesi politikasi

- Son kullanicilarinin egitim politikasi (Internet ücretsiz degil)

3. MAKINELERDE ALINABILECEK TEMEL ÖNLEMLER(1)

- Güvenlik yamalarinin güncel tutulmasi

- Mümkünse merkezi yama dagitim sisteminin olusturulmasi

- Isletim sistemlerinde gereksiz servislerin kapali tutulmasi

3. MAKINELERDE ALINABILECEK TEMEL ÖNLEMLER(2)

- Anti virüs yazilimi bulundurulmasi ve güncel tutulmasi

- Kisisel güvenlik duvari ve IDS/IPS yazilimlarinin kullanilmasi tesvik edilmesi. (Windows Firewall, Zonealarm, iptables, PF, vb.)

- Istemci bilgisayarlarda maksimum session sayisinin limitlenmesi

4. AGDA ALINABILECEK ÖNLEMLER

AĞDA ALINABİLECEK ÖNLEMLER	Birinci Katman *Bulaşmasını Engelleme*	Ikinci Katman *Bulaşmış Sistemi Saptama*	Üçüncü Katman *Kurtarma ve Etkileri Azaltma*	Kaynak No
4.1. L2 Cihazlar ile Alınabilecek Önlemler				
4.1.1. MAC Adresi Bazında Güvenlik		X	X	6
4.1.2. 802.1x Tabanlı Kimlik Tanımlama	X	X		7,8
4.1.3. Broadcast/Multicast Sınırlandırması		X	X	9
4.2. L3 Cihazlar ile Alınabilecek Önlemler				
4.2.1. VLAN Bazlı Güvenlik Çözümleri	X		X	10
4.2.2. Erisim Listeleri Alınabilecek Çözümler	X	X	X	11,12,13
4.2.3. QoS ile Bandgenişliği Sınırlaması			X	14,15
4.2.4. Yeni Nesil Güvenlik Çözümleri		X	X	16,17
4.3. Güvenlik Cihazları ile Alınabilecek Önlemler				
4.3.1. Firewall (Güvenlik Duvarları)	X	X	X	18
4.3.2. Antivirüs Geçitleri	X	X	X	19
4.3.3. IDS/IPS Sistemleri	X	X	X	20
4.4. Diğer Sistemler ile Alınabilecek Önlemler				
4.4.1. Saldırgan Tuzağı Ağları (Honeynet)		X		21,22
4.4.2. Merkezi Log Kontrolü		X		23,24,25
4.4.3. Trafik Analizi		X		4, 26
4.4.4. DNS Sunucu			X	13,27,28,29
4.4.5. Arp Saldırılarını Tespit Edebilen Uygulamalar		X		30

4.1. L2 CIHAZLAR ILE ALINABILECEK ÖNLEMLER (1)

4.1.1. MAC Adresi Bazinda Güvenlik

- Aga kontrolsüz bilgisayar (misafir) erisimini engellemek.

-Mac adresi ayni kalmak zorunda oldugu için kolayca bulasmis makinenin yeri tespit etmek.

- MAC adreslerini degistirmeleri durumunda ag erisimleri durdurmak.

```
Interface <int adi> <int.no>
switchport port-security
switchport port-security maximum <toplam PC sayisi>
switchport port-security violation <protect | restrict | shutdown>
switchport port-security mac-address <PC'nin MAC adresi>
```

Birinci Katman	*Ikinci Katman*	*Üçüncü Katman*
Bulasmasini Engelleme	**Bulasmis Sistemi Saptama**	**Kurtarma ve Etkileri Azaltma**

4.1. L2 CIHAZLAR ILE ALINABILECEK ÖNLEMLER (2)

4.1.2. 802.1x Tabanli Kimlik Tanimlama

-Aga kontrolsüz bilgisayar (misafir) erisimini engellemek veya kisitlamak.

-NAC teknolojileri ile yamalarin ve anti virus programlarinin güncelligini saglamak.

-Kolayca bulasmis makinenin yeri tespit etmek.

Birinci Katman	*Ikinci Katman*	*Üçüncü Katman*
Bulasmasini Engelleme	**Bulasmis Sistemi Saptama**	**Kurtarma ve Etkileri Azaltma**

4.1. L2 CIHAZLAR ILE ALINABILECEK ÖNLEMLER (3)

4.1.3. Broadcast/Multicast Sinirlandirmasi

-Broadcast/Multicast ile yapilacak DoS saldirilarini engellemek.

-Loglama devreye alinirsa bulasmis makineyi tespit etmek.

```
interface <int adi> <int.no>
storm-control multicast level <Yüzde.Küsürati>
storm-control broadcast level <Yüzde.Küsürati>
storm-control unicast level <Yüzde.Küsürati>
storm-control action <shutdown | trap>
```

Birinci Katman	*Ikinci Katman*	*Üçüncü Katman*
Bulasmasini Engelleme	**Bulasmis Sistemi Saptama**	**Kurtarma ve Etkileri Azaltma**

4.2. L3 CIHAZLAR ILE ALINABILECEK ÖNLEMLER (1)

4.2.1. VLAN Bazli Güvenlik Çözümleri

- Baska kaynak IP adresi ile o VLAN'den trafik çikmasi engellenerek saldiri yapilmasi engellemek

- Raslansal hedef IPler seçerek DoS saldirisi yapan PClere ICMP unreachable paketlerinin yollanmasi engellemek ve yönlendirici yükünü azaltmak ve saldirgani timeout süresi kadar bekletmek

```
int Vlan Vlan_Numarasi
…
ip verify unicast source reachable-via rx allow-default
no ip unreachables
no ip redirects
no ip proxy-arp
```

Birinci Katman	*Ikinci Katman*	*Üçüncü Katman*
Bulasmasini Engelleme	**Bulasmis Sistemi Saptama**	**Kurtarma ve Etkileri Azaltma**

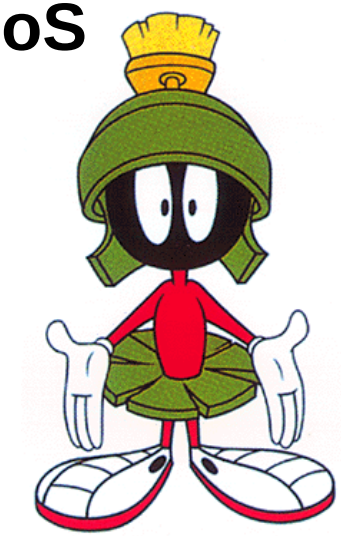
4.2. L3 CIHAZLAR ILE ALINABILECEK ÖNLEMLER (2)

4.2.2. Erisim Listeleri ile Alinabilecek Çözümler

-0.0.0.0/8, 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16, 127.0.0.0/8 ve 169.254.0.0/16 gibi kaynagi belli olmayan adresleri bloklayarak ve loglayarak DoS ataklarini engellemek ve belirlemek.

- Saldiri ve bulastirma ihtimali yüksek olan NETBIOS, SNMP, SMTP ..vs portlarini, ICMP kullanimi kontrol altina almak.

```
deny tcp any any eq 445 log
deny tcp any any range 135 139 log
…
deny ip 10.0.0.0 0.255.255.255 any log
…
deny icmp any any log
```



Marslilara HAYIR!

RFC 3704

Birinci Katman	*Ikinci Katman*	*Üçüncü Katman*
Bulasmasini Engelleme	**Bulasmis Sistemi Saptama**	**Kurtarma ve Etkileri Azaltma**

4.2. L3 CIHAZLAR ILE ALINABILECEK ÖNLEMLER (3)

4.2.3. QoS ile Kisi Basina Bant Genisligi Sinirlamasi

Birim kullanicinin disari veya içeri dogru trafik kullananim miktarinin kisitlanmasi,

Kötü bir yazilim bulasmis bilgisayarin ve P2P trafiginin ag kaynaklarini tüketmesi engellenir.

Bu sinirlama L3 anahtarlama cihazlarinin yani sira açik kaynak kodlu ipfw gibi yazilimlar ilede uygulanabilir.

Birinci Katman	*Ikinci Katman*	*Üçüncü Katman*
Bulasmasini Engelleme	Bulasmis Sistemi Saptama	Kurtarma ve Etkileri Azaltma

4.2. L3 CIHAZLAR ILE ALINABILECEK ÖNLEMLER (4)

4.2.4. Yeni Nesil Güvenlik Çözümleri

IP adreslerini degistirmelerini, DHCP ve ARP zehirleme saldirilari yapamalarini engellemek yeni nesil L3 anahtarlama cihazlarindaki örnek uygulamalar:

- **DHCP Snooping,**
- **Dynamic ARP Inspection,**
- **IP Source Guard**

Birinci Katman	*Ikinci Katman*	*Üçüncü Katman*
Bulasmasini Engelleme	Bulasmis Sistemi Saptama	Kurtarma ve Etkileri Azaltma

4.3. GÜVENLIK CIHALARI ILE ALINABILECEK ÖNLEMLER (1)

4.3.1. Güvenlik Duvarlari (Firewall)(1)

Güvenlik duvarlari, durum korumali (statefull) çalistiklari için, düzgün ayarlanmalari durumunda zararli yazilim aktivitesi içeren birçok baglantiyi engelleyebilecektir.

Servis saglayan sunucularin belirli portlari hariç, bütün portlar kurum disindan içeri dogru erisime kapatilmalidir.

Birinci Katman	*Ikinci Katman*	*Üçüncü Katman*
Bulasmasini Engelleme	**Bulasmis Sistemi Saptama**	**Kurtarma ve Etkileri Azaltma**

4.3. GÜVENLIK CIHALARI ILE ALINABILECEK ÖNLEMLER (1)

4.3.1. Güvenlik Duvarlari (Firewall)(2)

En Basit Kural Tablosu :

 # Kurum içinden disari trafik için
Bilinen zararli yazilim portlarini kapat
Diger bütün trafige izin ver

 # Kurum disindan içeri trafik için
Sunuculara sunucu portlarindan erisim izni
Geriye kalan bütün trafigi blokla

Birinci Katman	*Ikinci Katman*	*Üçüncü Katman*
Bulasmasini Engelleme	**Bulasmis Sistemi Saptama**	**Kurtarma ve Etkileri Azaltma**

4.3. GÜVENLIK CIHALARI ILE ALINABILECEK ÖNLEMLER (2)

4.3.2. Antivirüs Geçitleri

Ag trafigini zararli içerige ve daha çok eposta trafigini kontrol etmek amaçi ile kullanilan çözümlerdir.

Kötü amaçli yazilimlarin kendilerini bulastirmak için en sik kullandigi tekniklerden biri eposta oldugundan, kullanilmasi ciddi bir fayda saglamaktadir.

Ticari çözümlerin yani sira Clamav gibi GPL lisansina sahip çözümler de kullanilabilir.

Birinci Katman	*Ikinci Katman*	*Üçüncü Katman*
Bulasmasini Engelleme	**Bulasmis Sistemi Saptama**	**Kurtarma ve Etkileri Azaltma**

4.3. GÜVENLIK CIHALARI ILE ALINABILECEK ÖNLEMLER (3)

4.3.3. IDS/IPS Sistemleri

Saldiri saptama tespit ve engelleme sistemleri

- **Güvenlik duvarlari ile bütünlesik,**
- **Ayri sistemler olabilir.**

<u>Iyi yapilandirilmis</u> ve düzenli takip edilen IDS/IPS sistemi; agi pek çok kötü yazilimdan izole edebilecegi gibi, sorunun kaynagini tespitini de hizlandirmaktadir.

Ticari çözümlerin yani sira Snort gibi GPL lisansina sahip çözümler de kullanilabilir.

Birinci Katman	*Ikinci Katman*	*Üçüncü Katman*
Bulasmasini Engelleme	**Bulasmis Sistemi Saptama**	**Kurtarma ve Etkileri Azaltma**

4. DIGER SISTEMLER ILE ALINABILECEK ÖNLEMLER (1)

4.4.1. Saldirgan Tuzagi Aglari (Honeynet)

Çesitli bilinen zayifliklari simüle eden, virüs ve worm etkinligini yakalama amaçli kurulan sistemlerdir.

Tuzak agi yazilimlari ile bir makine üzerinde farkli isletim sistemlerini simüle eden sanal makineler, sanal yönlendiriciler ve sanal aglar olusturulabilir.

Örnek yazilimlar: Honeyd, Honeywall, Nepenthes, Amun

Birinci Katman	*Ikinci Katman*	*Üçüncü Katman*
Bulasmasini Engelleme	Bulasmis Sistemi Saptama	Kurtarma ve Etkileri Azaltma

4. DIGER SISTEMLER ILE ALINABILECEK ÖNLEMLER (2)

4.4.2. Merkezi Log Sunucu Sistemi

Ag cihazlarinda gelecek loglari sürekli ve kesintisiz tutacak bir log sunucusu mutlaka bulundurulmali, Bu sunucudaki kayitlar düzenli olarak incelenmelidir.

Log tutulmasi için syslog sunucusu ve incelemden kolaylik için swatch veya log watch kullanilabilir.

Birinci Katman	*Ikinci Katman*	*Üçüncü Katman*
Bulasmasini Engelleme	Bulasmis Sistemi Saptama	Kurtarma ve Etkileri Azaltma

4. DIGER SISTEMLER ILE ALINABILECEK ÖNLEMLER (3)

4.4.3. Trafik Akis Analizi Sunuculari(1)

Ag cihazlari, üzerlerinden geçen trafik akis (netflow) bilgisi, incelemek ve normal disi davranislar belirliyebilmek için harici bir sunucuya yollayabilir. Bu sekilde fazla paket ve fazla trafik yaratan makineler takip edilebilir.

Ayrica yine ag cihazlarinin bize sagladigi monitor port özellikleri ile trafik bir bilgisayara yönlendirebilir ve trafik bu sekilde de analiz edilebilir.
(Örnek: Wireshark, tcpdump, tcpdstat)

Birinci Katman	*Ikinci Katman*	*Üçüncü Katman*
Bulasmasini Engelleme	Bulasmis Sistemi Saptama	Kurtarma ve Etkileri Azaltma

4. DIGER SISTEMLER ILE ALINABILECEK ÖNLEMLER (3)

4.4.3. Trafik Akis Analizi Sunuculari(2)

Cisco cihazlarda devreye almak için kullanilacak komutlar su sekildedir.

```
router(Config)# ip flow-export version  <netflow VersiyonNumarasi>
router(Config)# ip flow-export destination <Flow sunucusunu IP adresi>
<Sunucun flow dinlemek icin kullandigi UDP port numarasi>
router(Config-if)# ip flow ingress
router(Config-if)# ip flow egress
```

Flow bilgisinin iletildigi sunucuda, bu veriyi isleyecek açik kaynak kodlu da olabilecek(nfsen,fprobe..gibi) bir yazilim kullanilabilir.

Birinci Katman	*Ikinci Katman*	*Üçüncü Katman*
Bulasmasini Engelleme	Bulasmis Sistemi Saptama	Kurtarma ve Etkileri Azaltma

4. DIGER SISTEMLER ILE ALINABILECEK ÖNLEMLER (4)

4.4.4. DNS Sunucuda Alinabilecek Önlemler(1)

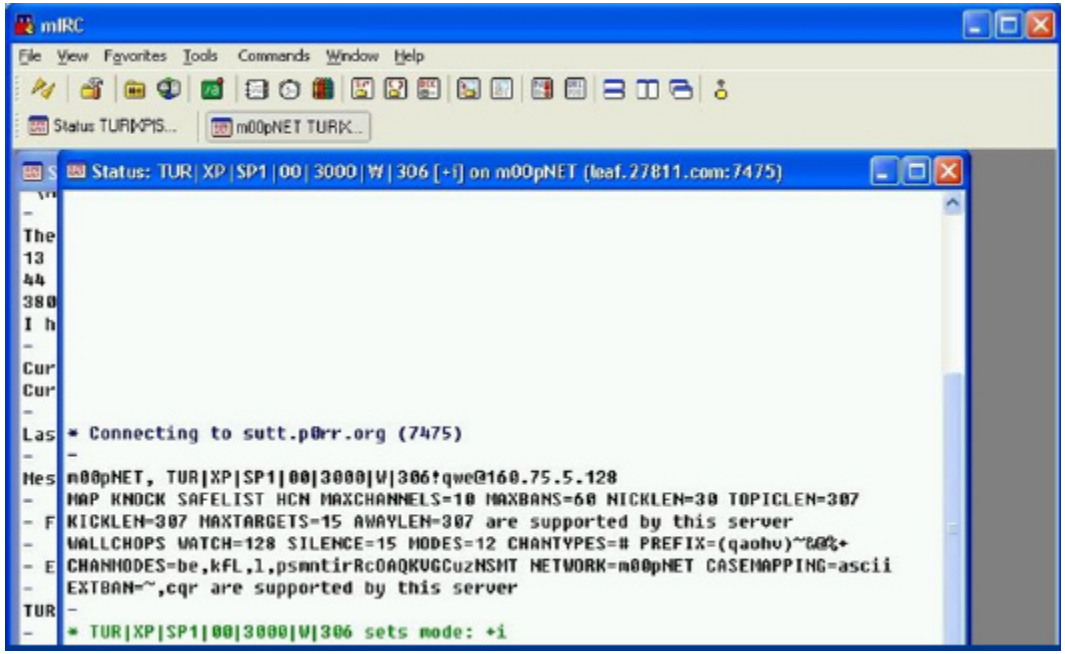
DNS sunucularini, zararli yazilimlardan dolayi üzerlerine gelebilecek gereksiz trafik yükünü azaltmak için yine kaynagi olmayan 0.0.0.0/8, 10.0.0.0/8, 172.16.0.0/12 192.168.0.0/16, 127.0.0.0/8 ve 169.254.0.0/16 adresleri bloklanmalidir.

Birinci Katman	*Ikinci Katman*	*Üçüncü Katman*
Bulasmasini Engelleme	Bulasmis Sistemi Saptama	Kurtarma ve Etkileri Azaltma

4. DIGER SISTEMLER ILE ALINABILECEK ÖNLEMLER (4)

4.4.4. DNS Sunucuda Alinabilecek Önlemler(2)

Zararli yazilimlar önceden belirlenmis domain adi ile belirli bir IRC sunucusuna baglanir ve istenen komutlari alir. Bu adresler bloklanabilir.



Birinci Katman	*Ikinci Katman*	*Üçüncü Katman*
Bulasmasini Engelleme	Bulasmis Sistemi Saptama	Kurtarma ve Etkileri Azaltma

4. DIGER SISTEMLER ILE ALINABILECEK ÖNLEMLER (5)

4.4.5. Arp Saldirilarini Tespit Edebilen Uygulamalar

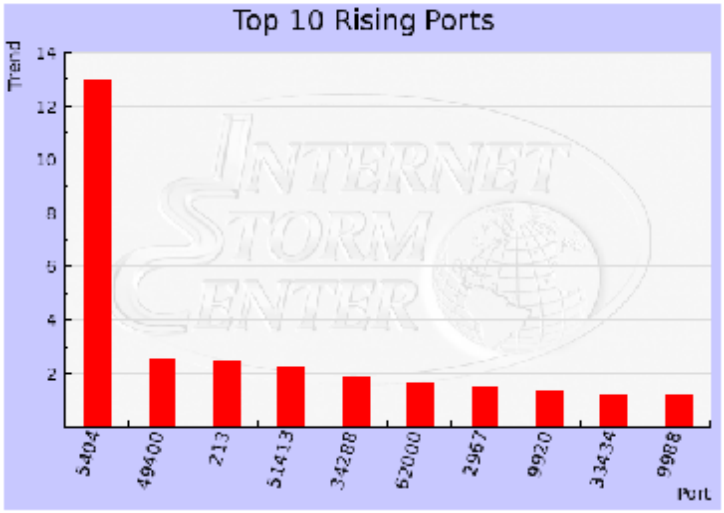
Son dönemde arp zehirlemesi teknigi malware ile de kullanilmaya baslamistir.

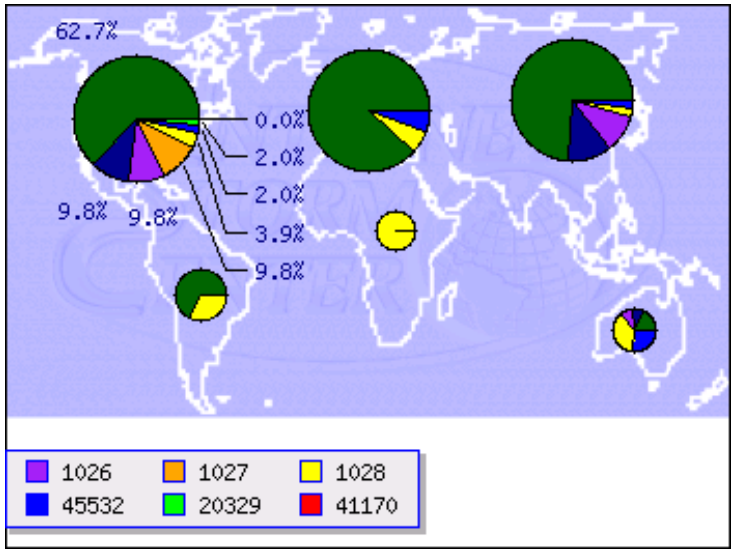
Örnegin aradaki adam saldirisi ile(man in the middle attack) hedef bilgisayarin bütün veri akisi dinlenebilmektedir.
(Örnek: Arpwatch, Arpsnmp)

Birinci Katman	*Ikinci Katman*	*Üçüncü Katman*
Bulasmasini Engelleme	Bulasmis Sistemi Saptama	Kurtarma ve Etkileri Azaltma

DIS BILGI KAYNAKLARI - dshield.org

Trends





by Reports

Port	Reports
1434	286297
1433	245471
445	202252
139	169201
135	87215
2967	81258
1026	65930
1027	60017
45532	52778
25	44046

by Targets

Port	Targets
1434	76679
1433	76502
2967	68679
445	38514
135	36294
22	15189
137	15032
139	14694
21	13103
80	7806

by Sources

Port	Sources
1026	28330
1027	28071
1028	28014
45532	9501
25	5721
20329	5609
4672	4989
445	4865
43737	4201
6881	4003

port report

Top 10 Source IPs

IP Address	Reports	Attacks	First Seen	Last Seen
121.162.129.138	175,577	98,863	2008-04-16	2008-04-30
081.209.145.131	247,573	92,461	2008-03-08	2008-05-01
218.106.091.025	1,122,193	92,171	2008-02-01	2008-05-01
202.099.011.099	906,578	90,201	2007-11-01	2008-05-01
058.020.222.030	836,598	88,420	2008-04-03	2008-05-01
067.059.063.252	155,976	88,017	2008-04-20	2008-04-30
061.178.181.005	593,233	87,618	2008-03-06	2008-05-01
202.103.011.041	558,814	86,551	2007-12-26	2008-05-01
061.153.050.237	457,413	85,375	2008-04-01	2008-05-01
059.063.025.161	389,011	84,419	2008-01-27	2008-05-01

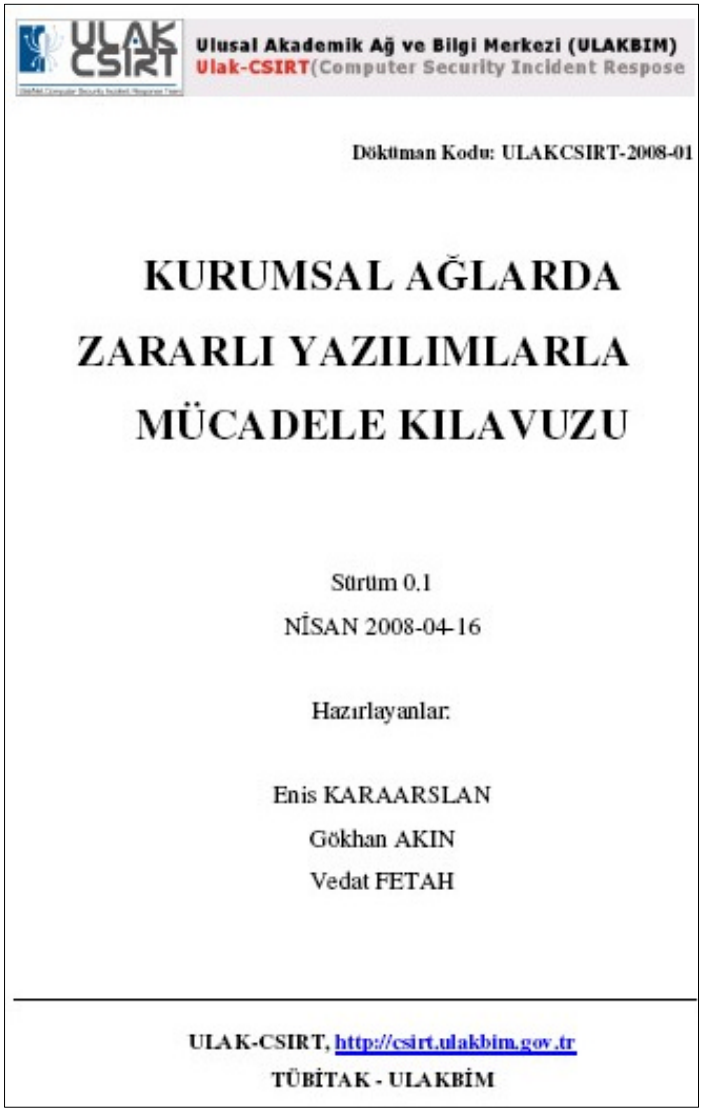
Top Sources

5. SONUÇ

“Güvenlik bir ürün degil, bir süreçtir.”
Bruce Schneier

Ciddi yatirimlarla yapilabilecek önlemler var oldugu gibi; açik kaynak kodlu çözümler ve kurumsal bilinçlendirme ile birçok güvenlik ihlalinin önüne geçmek mümkündür.

5. SONUÇ



Ulusal Akademik Ağ ve Bilgi Merkezi (ULAKBIM)
Ulak-CSIRT(Computer Security Incident Respose

Döküman Kodu: ULAKCSIRT-2008-01

KURUMSAL AĞLARDA
ZARARLI YAZILIMLARLA
MÜCADELE KILAVUZU

Sürüm 0.1
NİSAN 2008-04-16

Hazırlayanlar:

Enis KARAARSLAN
Gökhan AKIN
Vedat FETAH

ULAK-CSIRT, http://csirt.ulakbim.gov.tr
TÜBİTAK - ULAKBİM

Bu sunumun daha kapsamli içerigi için ULAK-CSIRT "Kurumsal Aglarda Zararli Yazilimlarla Mücadele Kilavuzu" dökümanini inceleyebilirsiniz.

Bu rapor sürekli gelistirme halindadir, bir sonraki versyonu için sizin de mutlaka katkilarinizi bekliyoruz.

SORULAR

Tesekkürler

csirt@ulakbim.gov.tr

http://csirt.ulakbim.gov.tr/dokumanlar