

ULAKNET Balküpu Servisi



Murat SOYSAL
msoysal@ulakbim.gov.tr
Onur BEKTAŞ
onur@ulakbim.gov.tr
TÜBİTAK ULAKBİM

3. ULAKNET ÇALIŞTAY ve EĞİTİMİ - 02.06.2009 Didim



UlaNet Computer Security Incident Response Team

İçerik

- Ulak-CSIRT Balküğü Ç.G.
- Karadelik Uygulamaları
- Balküğü Uygulamaları
- ULAKNET “Karadelik Saldırı Tespit Sistemi”
- Saldırı Analiz Sonuçları

Ulak-CSIRT Balküpu ve Karadelik Çalışma Grubu



2007 Yılı Ocak ayında çalışmalarına başlayan Ulak-CSIRT Balküpu ve Karadelik Çalışma Grubu 20.01.2009 itibariyle çalışmalarını başarıyla tamamlamış ve faaliyetlerine son vermiştir. Grubun çalışması sürecinde oluşturulan çıktılar şu şekildedir:

- ULAKNET Balküpu Sistemi
- Balküpu İstatistikleri Servisi
- Balküpu & OLTA entegrasyonu
- AB 2007, AB 2008 Çalışma Grubu sunumları
- I.ULAKNET Eğitim ve Çalıştayı "Balküpu Test Yatağı Sunumu"
- I.ULAKNET Eğitim ve Çalıştayı "Honeyd Kurulumu Sunumu"
- II.ULAKNET Eğitim ve Çalıştayı "ULAKNET Balküpu Sistemi Sunumu"
- Ulak-CSIRT "Honeyd Kurulumu Belgesi"
- Ulak-CSIRT "Honeywall Kurulumu Belgesi"
- Soysal,M., Bektas O., Analysis of Attacks Towards Turkish Academic Network, ISCTURKEY'08, pp. 126-131, 25-27 December 2008, Ankara, Turkey

Sunum ve belgelere <http://www.ulakbim.gov.tr/ulaknet/dokuman> sayfasından ulaşabilirsiniz.

Karadelik Uygulamaları (Blackholes, DarkNet)

- Karadelikler istenmeyen trafiğin yönlendirildiği hedeflerdir. Ağ üzerinde kullanılmayan IP bloklarına gelen trafiğin incelenmesine dayanır.
- Karadeliğe yönlendirilen trafik çöpe atılabilir, anında incelenebilir ya da incelemek için saklanabilir
- Tanımlama hataları, yönlendirme sorunları, BOTNET ve DDoS saldırıları, solucan aktiviteleri

Balküpu Uygulamaları (Honeypots)



Balküpleri bilgi ve ađ güvenliđini tehdit eden saldırıların farkına varmak, saldırganların yöntemlerini izlemek, metodlarını belirlemek, yeni geliřtirilen saldırı sistemlerinden önceden haberdar olmak için özel olarak tasarlanmış yazılım veya sistemlerdir.

Yaygın servislerin (SMTP, HTTP, DNS vb) sunucuların işlevlerini öykünerek (benzemeye çalışarak) saldırganları üzerlerine çekerler.

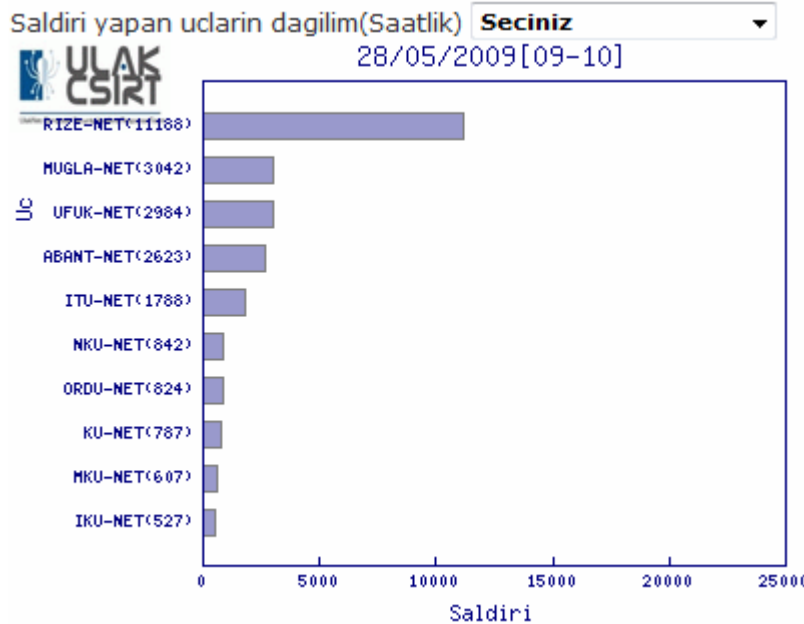
ULAKNET

Karadelik Saldırı Tespit Sistemi



- Kullanılmayan IP bloklarına gelen trafik-Genel yönlendirme
ip route 193.140.0.0 0.0.255.255 karadelik
ip route 194.27.0.0 0.0.255.255 karadelik
ip route 193.255.0.0 0.0.255.255 karadelik
ip route 79.123.128.0 0.0.254.255 karadelik
ip route 95.183.128.0 0.0.254.255 karadelik
- Bir ULAKNET ucuna gelen trafik-Özel yönlendirme
ip route 193.140.83.0 0.0.0.255 ULAKNET_UCU
- Geçerli bir hedef IPsi olan tüm trafik ilgili ULAKNET ucuna yönlendirken geri kalan trafik (şüpheli) Karadeliğe iletilmektedir.
- karadelik : Honeyd çalıştıran bir Balküpe sunucusu*
*Saldırı trafiğinden mümkün olan en fazla paketin yakalanması

Balküpu İstatistikleri



Günlük ve saatlik olmak üzere:

- Saldırı yapan ULAKNET uçları
- Saldırı yapan ülkeler
- Saldırı yapan IP'ler
- Saldırı yapan işletim sistemleri

Web sayfasından yayınlanmaktadır

<http://www.ulakbim.gov.tr/ulaknet/istatistik/balkupu/>

3. ULAKNET ÇALIŞTAY ve EĞİTİMİ - 02.06.2009 Didim

Balüpu Olay Kayıtları - I

- Toplanan kayıtlar günde iki kez işlenmekte, en çok trafik yaratan 10 IP için olay kayıtları oluşturulmaktadır.
- (09:00 ve 15:00 da)
- Amaç uç sorumlularına mesai saatleri içinde olay üzerinde çalışma fırsatı tanımak

Balküpu Olay Kayıtları -II



'2009-05-27 14:00:00' ve '2009-05-28 08:00:00' arasında, belirtilen İP'nizden, ULAKBİM balküpüne normalin dışında bir trafik gözlenmiştir.

Saldırıyı gerçekleştiren İP Adresi: 193.255.X.Y

Olayı yaratan kişinin eposta adresi: csirt@ulakbim.gov.tr

Tarih ve saat: 28 May 2009 9:5

Saldırının tipi veya şekli: Diğer

Ek bilgiler:

Gözlenen trafikle ilgili bilgiler ve -varsa- üretilen saldırı kayıtları aşağıda listelenmiştir.

Zaman	Protokol	Kaynak Ip	Kaynak Port	Hedef İP	Hedef Port
2009-05-27 23:50:14	tcp	193.255.X.Y	2131	10.1.151.159	445
2009-05-27 23:50:14	tcp	193.255.X.Y	2119	10.1.116.114	445
2009-05-27 23:50:02	tcp	193.255.X.Y	2709	10.1.253.148	445
2009-05-27 23:50:00	tcp	193.255.X.Y	2704	10.1.121.169	445
2009-05-27 23:50:00	tcp	193.255.X.Y	2712	10.1.148.200	445
2009-05-27 23:49:59	tcp	193.255.X.Y	2712	10.1.148.200	445
2009-05-27 23:49:59	tcp	193.255.X.Y	2698	10.1.139.241	445
2009-05-27 23:49:59	tcp	193.255.X.Y	2709	10.1.253.148	445
2009-05-27 23:49:59	tcp	193.255.X.Y	2694	10.1.88.38	445
2009-05-27 23:49:58	tcp	193.255.X.Y	2704	10.1.121.169	445

3. ULAKNET ÇALIŞTAY ve EĞİTİMİ - 02.06.2009 Didim



Sonuçlar



- ULAKNET Ağ yönetim merkezi ve ULAKNET uç yöneticileri ağa yönelik saldırılar hakkında genel görünüme sahip oldu.
- ULAKNET uçlarından kaynaklı saldırılardan olay kayıtları oluşturularak çözüm aşamaları Ulak-CSIRT tarafından takibe alındı.
- Bazı yönlendirme ve tanımlama hataları tespit edilerek düzeltildi.
- Ülkemizde ilk defa bu büyüklükte bir saldırı analizi yapıldı.
- Hazırlanan Türkçe belgeler ile bu alanda uygulama yapmak isteyen araştırmacılar için kaynak hazırlandı.

Sorular&Yorumlar



- İlginiz için teşekkürler...
- İletişim için:
 - msoysal@ulakbim.gov.tr
 - onur@ulakbim.gov.tr
 - csirt@ulakbim.gov.tr
 - <http://csirt.ulakbim.gov.tr>