Dağıtık Zararlı Yazılım Toplama ve Analiz Modeli

[1]Bâkır EMRE ve [2]Doç.Dr.Hacı Ali MANTAR
*[1]Siber Güvenlik Enstitüsü, TÜBİTAK
[2]Bilgisayar Mühendisliği, Gebze Yüksek Teknoloji Enstitüsü

Özet

Bu makale dağıtık zararlı yazılım toplama ve analiz modelini anlatmaktadır. Tasarlanan model ile farklı kurumlarda konumlandırılan ve dağıtık halde bulunan sensörlere yapılan ağ saldırıları tuzak sitemlere yönlendirilmekte ve yönlendirilen ağ trafiği içerisinden zararlı yazılım toplanabilmektedir. Yakalanan zararlı yazılımlara karşı erken uyarı da oluşturulmaktadır. Oluşturulan model, dağıtık sensörler ve zararlı yazılım tespit merkezi olmak üzere iki ana kısımdan oluşmaktadır. Zararlı yazılım tespit merkezi, sanallaştırma sunucuları ve üzerinde barındırdığı tuzak sistemlerini, ağ trafiği izleme modülü, anti virüs tarayıcı modülü ve zararlı ağ trafiği kayıt veri tabanı gibi alt modülleri içermektedir. Dağıtık zararlı yazılım toplama ve analiz modeli ile yeni geliştirilen zararlı yazılımlar için anti-virüs imzası oluşturulabilmekte, ayrıca zararlı yazılımın oluşturduğu ağ trafiğinden IP ve DNS kara listeleri ve saldırı tespit sistemi imzası da oluşturulabilmektedir.

Anahtar Kelimeler: Zararlı Yazılım Tespiti, Tuzak sistemi, IDS, Sensor, Erken Uyarı Sistemi

1. Giriş

Zararlı yazılımlar günümüz siber dünyasının en büyük tehditlerinden biridir. Mobil cihazlardan, sunucu sistemlere, son kullanıcı bilgisayarlarından, pos cihazlarına kadar farklı tiplerdeki siber ortam araçlarını hedef almaktadır. Günlük olarak tespit edilen zararlı yazılımlar, 2010 yılında 50.000, 2011 yılında 70.000 ve 2012 yılında ise 100.000 sayısına ulaşmıştır [1],[2],[3]. Yeni çıkan zararlı yazılımları tespit etmek için kullanılan anti-virüsler gerek imza tabanlı olmalarından, gerekse sezgisel taramalarındaki false-pozitif oranlarının yüksek olmalarından dolayı etkin bir koruma sağlayamamaktadır. Zararlı yazılım analistleri yeni bir zararlı yazılım ile karşılaştıklarında, bu zararlı yazılımın karakteristiğini bularak, yazılıma ait anti-virüs imzasını oluşturmaktadır. Kurumları hedef alan zararlı yazılımların anında tespiti ve engellenmesi anti virüs imzalarının hızlı bir biçimde güncellenmesi ile mümkündür. Böylece zararlı yazılımın vereceği etki en aza indirilebilecektir. Anti-virüs tarayıcıları dışında zararlı yazılım tespit etmek için kullanılacak başka bir yöntem ise Honeypot'lardır (tuzak sistemler).

Tuzak sistemler yer aldığı ağlarda worm, virüs gibi zararlı yazılımlar tarafından yapılan saldırıları ya da bilgisayar korsanları (hacker) tarafından gerçekleştirilen atakları üzerine çekecek şekilde

İlgili kişi: Bâkır EMRE: TÜBİTAK BİLGEM Siber Güvenlik Enstitüsü, PK71 41470 Gebze/KOCAELİ E-mail: bakir.emre@tubitak.gov.tr

tasarlanmaktadır. Temel görevleri bir uygulamayı, servisi, işletim sistemini ya da bir ağı tamamen taklit ederek saldırı kayıtlarının ve zararlı içeriğin toplanmasını sağlamaktır. Tuzak sistemler (TS) dış dünyaya bildirilmeyen IP adreslerini kullandığı için, bu yapılara yönelen her ağ hareketi şüpheli olarak kabul edilmektedir. TS'ler, üzerinde çalışan ya da çalışıyor gibi görünen servisleri veya işletim sistemleri sunmaktadır. Sunulan servisler veya işletim sistemleri çeşitli zafiyetler içerebilmektedir. TS'ler bu zafiyeti istismar etmek isteyen saldırganların ve kullandıkları saldırı yönteminin tespitine yardımcı olmaktadır. Tuzak sistemler kabiliyetlerine göre düşük etkileşimli ve yüksek etkileşimli olarak ikiye ayrılır [4]. Düşük etkileşimli TS'ler bir ağı ya da ağ servisini taklit edebilmektedir. Honeyd [5] düşük etkileşimli TS'ler için ilk ve en bilindik örnektir. Yönetilmesi, bakımı oldukça kolaydır. Düşük etkileşimli TS'ler ile saldırı istatistiği toplanabilmesine rağmen saldırının içeriği hakkında doyurucu bilgi sağlamamaktadır. Yüksek etkileşimli TS'lerde ise sunulan ağ servisleri gerçek işletim sistemleri üzerinde çalıştırılır veya gerçek servisler olarak çalışır. Sunulan servisler açıklık barındırır. Yüksek etkileşimli TS'ler daha fazla ve derinlemesine saldırı analizi yapılmasına da imkân sunar. Fakat yüksek etkileşimli TS'lerin bakımı ve yönetilmesi düşük etkileşimli TS'ler göre daha zordur.

Bu makalede tuzak sistemler kullanarak oluşturulan model ile zararlı yazılım tespiti ve analizi anlatılmıştır. Makalenin devamındaki bölümler ise şu şekildedir. 2. Bölümde daha önce yapılmış benzer çalışmalar anlatılmış, 3. Bölümde gerçekleştirilen model anlatılıp, daha önceki çalışmalardan farkı anlatılmış, 4. Bölümde ise elde edilen bulgular paylaşıldıktan sonra 5. Bölümde ise sonuç ve ileriki safhada gerçekleştirilecek iyileştirmelerden bahsedilmiştir.

2. İlgili Çalışmalar

Zararlı yazılım toplamak için oluşturulmuş bir çok araştırma mevcuttur. Song ve diğerleri Darknet'i temel alan zararlı yazılım tespit modeli önermiştir [6]. Buna göre bir kurumda kullanılmayan bir IP bloğundan Darknet [7] oluşturulur. Darknet, kurum için ayrılan ve kuruma yönlendirilmiş IP bloğunun, içinde aktif sunucu ve servislerin yer almadığı bir bölümüdür. Bir saldırgan ya da zararlı yazılım tarafından, hem kurumda yer alan bilgisayarlara hem de Darknet'de yer alan IP adreslerine aynı anda saldırıda bulunursa, saldırının kaynak IP adresinden gelen ağ hareketleri gözetim altına alınmaktadır. Sekiz aşama olarak tasarlanan sistem: "izleme, sınıflandırma, keşfetme, güncelleme, süzme, yönlendirme, analiz etme ve geri besleme" adımlarından oluşmaktadır. Bu adımlar doğrultusunda bir TAP cihazı ile kuruma gelen ağ trafiğinin kopyası çıkarılmaktadır. TAP cihazı ile oluşturulan ağ trafiği analiz sistemi adı verilen sisteme yönlendirilmektedir. Analiz sistemine yönlendirilen bu ağ trafiği ile zararlı yazılım elde etmek için çalışmalar yapılmaktadır. Sistemden zararlı yazılım elde etmek için bütün kurumlarda Darknet bloğu oluşturulması ve zararlı yazılım tespit ağı kurulması gerekmektedir. Ayrıca zararlı yazılım ağı içerisinde saldırı tespit sistemi (STS), veri tabanı ve analiz sunucusu gibi yapıları da barındırmak zorundadır. Böylesine büyük bir sistemin farklı kurumlara konumlandırıp uzaktan yönetmek ve bakımını yapmak etkin olmayabilmektedir.

Sahgel ve diğerleri, botnet tespiti için zararlı yazılım yakalama ve analiz altyapısı önermiştir [8]. Buna göre farklı kurumlara honeynet (tuzak sistem ağı) kurulmaktadır. Kurulan tuzak sistem ağlarından elde edilen zararlı yazılımlar ve ağ saldırı verileri zararlı yazılım toplama merkezinde bulunan bir ilişkisel veri tabanında saklanacaktır. Bu veri tabanı zararlı yazılımın hash (özet

değeri) çıktısı ve tuzak sistem kaynak IP adresini saklayacaktır. Ayrıca merkezde bulunan analiz sunucusu üzerinde bu zararlı yazılım analiz edilip, bir web sunucusu vasıtası ile bu veriler gösterilebilmektedir. Bahsedilen altyapıda da, sistemin veri kaynağı olan tuzak sistem ağı, kurum ağına kurulacaktır. Bu tuzak sistem ağında tuzak sistem bilgisayarları, tuzak sistem ağ geçidi ve sanal anahtarlama cihazları gibi yapıları bulunduracaktır. Bu yapıların da uzaktan bakımının yapılması ve yönetilmesi zararlı yazılım yakalama işleminin otomatikleştirilmesinin önüne geçebilmektedir.

Bahsedilen çalışmalar dışında Takeda ve diğerlerinin sunduğu sürekli zararlı yazılım toplama ve analiz çatısı [9], Moore ve diğerlerinin sunduğu Network telescope [10], NoAH [11] ve The Honeynet Project [12] gibi birçok araştırma da dağıtık ortamda ağ saldırı analizi ve zararlı yazılım toplama üzerine yoğunlaşmıştır.

Bu makalede önerilen zararlı yazılım tespit ve analiz modeli ise diğer çalışmaların aksine farklı kurumlara kurulacak olan sistemin olabildiğince az cihazla çalışmasını sağlamaktadır. Farklı kurumlara konumlandırılacak cihazların azalması ile olası yazılım ve donanım hatasında sistemin işleyişine devam edebilmesi, tuzak sistemler zararlı yazılımlarca ele geçirildiğinde bu tuzak sistem üzerinden başka yerlere saldırmalarının kontrol altına alınabilmesi ve merkezi olarak tutulacak tuzak sistemlerin bakımının, yönetilmesinin kolaylaştırılması sağlanacaktır. Kurumlarda yer alacak sensor cihazlar bir yönlendirici gibi kendilerine gelen ağ trafiğini merkezdeki sunuculara gönderecek, gelen cevapları kendi üzerinden geçirip saldırgana iletecektir.

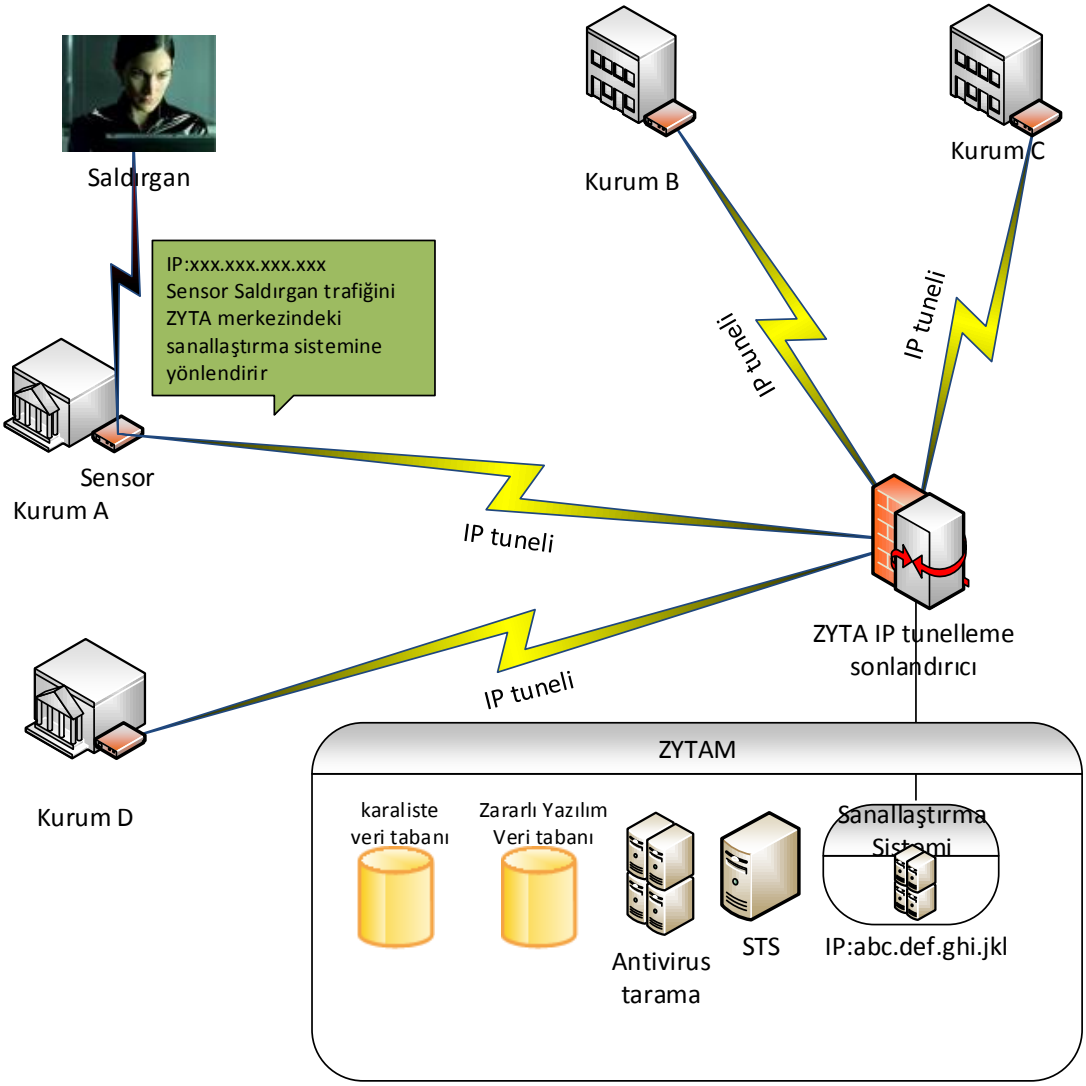
3. Dağıtık Zararlı Yazılım Toplama ve Analiz Modeli

Dağıtık zararlı yazılım toplama ve analiz modeli temel olarak iki ana bileşenden oluşmaktadır. Zararlı yazılım yakalama bileşeni ve analiz bileşeni. Önerilen model diğer çalışmaların aksine dağıtık olarak konumlandırılan sensörler'e gelen ağ trafiği ortak bir merkeze IP tünelleme ile göndererek, merkezde bulunan ve ilgili sensöre karşılık kurulan tuzak sistemlerince çalıştırılarak analiz edilebilmeyi sağlamaktadır. Sensörler kurumun kullanılmayan IP adresleri içerisinden seçilmektedir. Merkez ise tespit ve analiz sunucularını barındırmaktadır.

Dağıtık zararlı yazılım toplama ve analiz modelini oluşturan bileşenler ayrıntılı olarak şu şekildedir;

- Saldırgan Ağ Trafiğini sanallaştırma ortamına yönlendiren, farklı kurumlarda konumlandırılan yönlendirici cihazları (sensör).
- Yüksek etkileşimli tuzak sistemlerini içinde barındıran sanallaştırma ortamı.
- Yüksek etkileşimli tuzak sistemlere gelen saldırgan ağ trafiğinden alarmlar üreten STS (Snort)
- Yüksek etkileşimli tuzak sistemlere gelen zararlı ikili dosyaları ağ üzerinden ayıklama modülü (Suricata)
- Zararlı yazılım veri tabanı
- Zararlı yazılım tarama sistemi
- Kara liste veri tabanı

Şekil 1'de modelin genel mimarisi görünmektedir. Farklı kurumlardaki sensör olarak kullanılabilecek bilgisayarların görevi ağ trafiğini yönlendirmedir. Buradaki yönlendirme klasik bağlamda kullanılan yönlendirici cihaz gibi değildir. İki yönlü bir yönlendirme yapmaktadır. Sensör cihaz kendisine gelen ağ trafiğini zararlı yazılım tespit ve analiz merkezine göndermekte, buradan dönen cevapları yine sensör cihaz üzerinden geçirerek saldırgana iletmektedir. Ayrıca sensör cihaz, üzerinde hiçbir servis sunmamaktadır. Bu sebeple işlemci ve bellek kullanımı çok az olmaktadır. Dolayısıyla bu cihaz için donanım seçerken maliyeti az olan Raspberry-pi [13] gibi mikro-pc'ler seçilebilmektedir. Sensör cihazların işleyebileceği bant genişliğinden fazla ağ trafiği geldiği ya da cihazlara DoS/DDoS saldırıları yapıldığı durumlarda cihaz çalışamayacaktır. Aksi her durumda çalışmasına devam edecektir.



Şekil 1Dağıtık Zararlı Yazılım Tarama ve Analiz Modeli

Zararlı yazılım tespit merkezi ise sensör trafiğinin sonlandırma sunucusu (OpenVPN açık kaynak IP tünelleme çözümü kullanılmaktadır), üzerinde yüksek etkileşimli tuzak sistemlerini barındıran sanallaştırma sistemi, ağ trafiği incelenmesi ve ağ trafiğinden zararlı içeriğin çıkarılması için Saldırı Tespit Sistemi (STS), zararlı yazılımların özet değerlerinin bulunduğu veri tabanı, anti virüs tarama sistemi ve zararlı yazılımların depolandığı dosya sunucu gibi yapıları barındırmaktadır.

Zararlı bir yazılımın analiz süreci şu şekilde sürdürülmektedir.

- Zararlı ağ trafiği sensor bilgisayarları tarar.
- Tarama trafiği sensor vasıtası ile zararlı yazılım tespit merkezindeki OpenVPN sonlandırma sunucusuna iletilir.
- OpenVPN sonlandırma sunucusundan, bu sensor için atanmış sanallaştırma sistemi (Oracle VirtualBox [15]) üzerindeki sanal tuzak sistemine iletilir.
- Zararlı yazılım, sanal tuzak sistemdeki açık servisi bulup bu servisteki açıklığı istismar etmeye çalışır.
- İstismar edilen açıklık anında ağ trafiği STS [16] tarafından analiz edilir ve ilgili alarm oluşturulur.
- Eğer ikili dosya sanal tuzak sistemine eklenmeye çalışılırsa bu dosya ayıklama sunucusu olarak kullanılan STS [17] tarafından ayıklanır.
- Ayıklanan dosyanın özet bilgisi çıkarılıp, bu dosyanın daha önceden tespit edilen bir zararlı yazılım olup olmadığı zararlı yazılım özet değerlerinin tutulduğu veri tabanından sorgulanır.
- Eğer dosya özeti veri tabanında var ise dosya ile ilgili işlem yapılmaz, bulunan dosyaların sayısı bir arttırılır.
- Eğer dosya özeti veri tabanında yok ise dosya anti-virüs tarama sisteminde farklı anti virüsler ile taratılmaya çalışılır.
- Anti-virüs tarama sisteminde dosyanın hangi zararlı yazılım ailesinde olduğu tespit edilir.
- Eğer anti-virüs tarama sisteminde dosya ile ilgili herhangi bir imza yok ise bu dosya yine sanallaştırma sistemi üzerinde bulunan yüksek etkileşimli tuzak sistemleri içerisinde (Microsoft Windows XP SP1, SP2 ve SP3) çalıştırılır.
- Bu zararlı dosya kapalı kutu testine (black-box test) tabi tutulur.
- Black-box test sonucu zararlı yazılımın yapmış olduğu ağ trafiği incelenir.
- Ağ trafiğinden bağlantı kurulmaya çalışılan IP ve DNS adresleri kaydedilir.
- IP ve DNS adresleri kara liste veri tabanı ile karşılaştırılır.
- IP ve DNS adresleri, bilinen bir zararlı yazılımın daha önceden bağlandığı IP ve DNS adresleri ile aynı ise bu zararlı yazılım da aynı aileye dahil edilir.

Modele aşağıdaki işlevleri görecek yeni modüller de eklenebilir:

- IP ve DNS adresleri veri tabanında yok ise bu dosyanın eriştiği sistem çağrıları tespit edilir.
- Elde edilen sistem çağrıları var olan zararlı yazılımların sistem çağrıları ile benzerlikleri karşılaştırılır ve hangi zararlı yazılım ailesinden olduğu istatistiksel olarak gösterilir.

4. Tespit edilen Zararlı yazılım istatistikleri

Zararlı yazılım tespit ve analiz modeli tarafından iki sensör cihazı ile bir hafta süren analiz çalışmaları sonucu tespit edilen zararlı yazılımların istatistiki bilgileri **Tablo *1*** 'de gösterilmiştir.

Tip	**Sayı**
Toplam zararlı yazılım	849
Tekil zararlı yazılım	43
Anti-virüs tarayıcıların tespit edemediği zararlı yazılım	21

Tablo 1. Zararlı Yazılım Tespit ve Analiz Sistemi tarafından yakalanan dosyalar

Toplanan zararlı yazılım sayısı 849 olarak tekil zararlı yazılım sayısı ise 43 olarak tespit edilmiştir. Bu zararlı yazılımlardan 21 tanesi ise daha önce hiçbir anti-virüs tarayıcıda imzası bulunmayan zararlı yazılım olarak öne çıkmaktadır. Bu zararlı yazılımlar var olan bir zararlı yazılımın yeni varyantı olabileceği gibi daha önce keşfedilmeyen bir zararlı da olabilmektedir. Zararlı yazılım tespit ve analiz modeli daha fazla sensor ile daha uzun süreli çalıştığında toplanacak tekil zararlı yazılım sayısı da artacaktır.

Sistem tarafından yakalanan farklı tipteki zararlı yazılımların bazılarının özet değerleri ve aileleri **Tablo *2***'deki gibi gösterilmiştir. Aile isimleri Microsoft zararlı yazılım koruma merkezi isimlendirme standardına [18] göre yapılmıştır. Buna göre Zeus Botneti [19] olarak bilinen zararlı yazılım ailesine ait Zbot, Sdbot varyantı ve Rbot gibi çeşitli Botnet dropper'larının yeni sürümleri tespit edilebilmektedir. Ayrıca Microsoft sistemleri hedef alana Conficker kurtçuğu da yakalanan zararlı yazılımlar arasındadır.

Zararlı yazılım MD5 özeti	Zararlı Yazılım Ailesi
154af659dd1cf366188f827bbb1edd1c	Trojan:Win32/Zbot
17978bf5c97eb9e3457dfffd903ca853	Backdoor:Win32/Rbot
62077132299c05fa1e9788f7d04778f6	Worm:Win32/IRCBot.variant
3284fad8a6238205829d812a26a608ff	Worm:Win32/Conficker.B
f29f008f6da3a4931f1e5774517882fe	VirTool:Win32/CeeInject.gen!ID

Tablo 2. Tespit edilen farklı zararlı yazılımlardan birkaçı

5. Sonuç

Bu çalışmada günümüz siber dünyasının en önemli problemlerinden olan zararlı yazılımların tespiti için yeni bir tespit ve analiz sistemi önerilmiştir. Oluşturulan model ile anti-virüslerin imza veri tabanlarında olmayan, yeni keşfedilen ya da var olan zararlı yazılımların yeni varyantlarının tespiti de mümkün olmaktadır. Sistemin merkezi analiz yapabilmesi, farklı ağlara gelebilecek saldırıların, zararlı yazılımların tespiti için düşük donanımlı bir bilgisayar kullanılabilmesine imkan vermesi, her kuruma her ağa farklı analiz sistemi kurma gereksinimi olmaması daha önce

yapılmış çalışmalara göre katma değer sağlamaktadır. Gelecekte sisteme eklenebilecek olan zararlı yazılım sistem çağrıları karşılaştırma modülü ile ailesi tespit edilemeyen zararlı yazılımlar da bulunabilecektir. Ayrıca istemci bilgisayarlar için oluşturulacak ajan yazılımı ile masaüstü kullanıcıların şüphelendikleri dosyaları zararlı yazılım tespiti ve analiz merkezinde analiz edilerek zararlı olmadıkları da tespit edilebilecektir.

Referanslar

[1] http://blogs.comodo.com/pc-security/computer-protection/50000-malware-created-daily/ (Nisan 2013)
[2] http://eugene.kaspersky.com/2011/10/28/number-of-the-month-70k-per-day/ (Nisan 2013)
[3] McAfee Threats Report: Fourth Quarter 2012 - http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2012.pdf (Nisan 2013)
[4] Spitzner, L.: Honeypots: Tracking Hackers. Addison-Wesley (2003)
[5] Honeyd: virtual honeypot, http://www.honeyd.org/
[6] J. Song, J. Choi, and S. Choi, "A Malware Collection and Analysis Framework Based on Darknet Traffic," pp. 624–631, 2012.
[7] http://www.team-cymru.org/Services/darknets.html (Nisan 2013)
[8] R. K. Sehgal, "An Integrated Framework for Malware Collection and Analysis for Botnet Tracking Integrated Botnet tracking System," no. 10, pp. 50–55, 2012
[9] K. Takeda and M. Mizutani, "Design and prototyping of framework for automated continuous malware collection and analysis," *Security Technology (ICCST), 2011*
[10] D. Moore, C. Shannon, G. M. Voelker, and S. Savage, "Network Telescopes : Technical Report," pp. 1–14. 2004
[11] J. Kohlrausch, "Experiences with the NoAH Honeynet Testbed to Detect new Internet Worms," *2009 Fifth International Conference on IT Security Incident Management and IT Forensics*, pp. 13–26, 2009.
[12] The Honeynet Project:, The Honeynet Project is a leading international security research organization, dedicated to investigating the latest attacks and developing open source security tools to improve Internet security, http://www.honeynet.org
[13] The Raspberry Pi is a credit card sized single-board computer, http://www.raspberrypi.org/
[14] OpenVPN, Open Source VPN, http://www.openvpn.net/
[15] Oracle VirtualBox: Powerful x86 and AMD64/Intel64 virtualization product, http://www.virtualbox.org
[16] Snort: The Open Source Network Intrusion detection systems. http://www.snort.org
[17] Suricata: Open Source IDS / IPS / NSM engine, http://www.suricata-ids.org/
[18] Microsoft Malware Protection Center Naming Standards www.microsoft.com/security/portal/shared/malwarenaming.aspx (Nisan 2013)
[19] http://en.wikipedia.org/wiki/Zeus_%28Trojan_horse%29 (Nisan 2013)