

T.C.
GEBZE YÜKSEK TEKNOLOJİ ENSTİTÜSÜ
MÜHENDİSLİK ve FEN BİLİMLERİ ENSTİTÜSÜ

DAĞITIK ZARARLI YAZILIM TOPLAMA
VE ANALİZ MODELİ

BÂKIR EMRE
YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

GEBZE
2013

T.C.
GEBZE YÜKSEK TEKNOLOJİ ENSTİTÜSÜ
MÜHENDİSLİK ve FEN BİLİMLERİ ENSTİTÜSÜ

DAĞITIK ZARARLI YAZILIM TOPLAMA
VE ANALİZ MODELİ

BÂKIR EMRE
YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

DANIŞMANI
DOÇ. DR. HACI ALİ MANTAR

GEBZE
2013



**GEBZE YÜKSEK TEKNOLOJİ
ENSTİTÜSÜ**

YÜKSEK LİSANS JÜRİ ONAY FORMU

GYTE Mühendislik ve Fen Bilimleri Enstitüsü Yönetim Kurulu'nun 17/06/2013 tarih ve 2013/32 sayılı kararıyla oluşturulan jüri tarafından 27/06/2013 tarihinde tez savunma sınavı yapılan Bakır EMRE'nin tez çalışması Bilgisayar Mühendisliği Anabilim Dalında YÜKSEK LİSANS tezi olarak kabul edilmiştir.

JÜRİ

ÜYE

(TEZ DANIŞMANI) : Doç. Dr. Hacı Ali MANTAR

ÜYE

: Yrd. Doç. Dr. Hasari ÇELEBİ

ÜYE

: Yrd. Doç. Dr. Serdar Süer ERDEM

ONAY

GYTE Mühendislik ve Fen Bilimleri Enstitüsü Yönetim Kurulu'nun tarih ve/..... sayılı kararı.

İMZA/MÜHÜR

ÖZET

Siber tehditlerin en başında gelen zararlı yazılımların tehdit alanları genişlediği için her geçen gün sayısı da artmaktadır. Artan zararlı yazılımlar karşısında anti virüs tarayıcılar yeterli olmamaktadır. Zararlı yazılımların vermiş olduğu ekonomik zarar, itibar kaybı ve çalışan verimliliği azalması gibi nedenlerden dolayı zararlı yazılım tespiti için yeni yöntemlere ihtiyaç duyulmaktadır.

Bu çalışmada ağ üzerinden yayılmaya çalışan zararlı yazılımların tespiti için tuzak sistemleri temel alan dağıtık zararlı yazılım toplama ve analiz modeli önerilmiştir. Önerilen zararlı yazılım toplama ve analiz modeli ile farklı kurumlarda konumlandırılan ve dağıtık halde bulunan sensörlere yapılan ağ saldırıları tuzak sistemlere yönlendirilmektedir. Tuzak sistemlere yönlendirilen ağ trafiği içerisinden zararlı yazılım toplanabilmektedir. Yakalanan zararlı yazılımlara karşı erken uyarı 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, zararlı yazılımın oluşturduğu ağ trafiğinden IP ve DNS kara listeleri ve saldırı tespit sistemi imzası oluşturulabilmektedir.

Anahtar Kelimeler: Zararlı Yazılım Tespiti; Tuzak Sistem; Saldırı tespit sistemi; Kara liste; Tuzak Ağı.

SUMMARY

Being one of the leading threats to cyber security, the number of malwares are increasing rapidly as the threat landscape extend. However, the antivirus software is not capable of handling that number of new malwares. Considering the economic damages, loss of reputation decrease in employee productivity caused by malwares, in addition to antivirus software, new methods needs to be implemented to detect malwares.

In this thesis we propose a distributed model to analyze and collect malwares that spread over the Internet. The proposed model depicts the forwarding of network attacks coming from internet to distributed sensors located in enterprise networks to honeypots. The honeypots capture the traffic in order to identify malwares whereas various early notifications are generated to help analyze the flow.

The model comprises to two main parts; distributed sensors and malware detection center. Malware detection center is composed of sub modules like virtualization servers which are hosted low and high interaction honeypots, network traffic monitoring systems, anti-virus scanners and malware hash and strings database. Anti-virus signature for recently developed malware, IP and DNS black lists from the traffic generated by malware and intrusion detection system signature can be derived with the proposed distributed malware collection and analysis framework.

Keywords: Malware detection; Honeypot; IDS; Blacklist; Honeynet.

TEŞEKKÜR

Tez çalışmamda bana sürekli yol gösteren ve yardımlarını esirgemeyen saygıdeğer hocam Sayın Doç. Dr. Hacı Ali MANTAR'a, tez çalışmam sırasında bana gösterdikleri anlayış ve sabırdan ötürü tüm çalışma arkadaşlarıma ve son olarak beni bu günlere getiren aileme sonsuz teşekkürlerimi sunarım.

İÇİNDEKİLER

	<u>Sayfa</u>
ÖZET	iv
SUMMARY	v
TEŞEKKÜR	vi
İÇİNDEKİLER	vii
SİMGELER VE KISALTMALAR DİZİNİ	viii
ŞEKİLLER DİZİNİ	ix
TABLolar DİZİNİ	x
1. GİRİŞ	1
2. YÖNTEM	3
2.1. KONU İLE İLGİLİ ÇALIŞMALAR	3
2.2. ÖNERİLEN YÖNTEM	12
2.3. Dağıtık Zararlı Yazılım Toplama ve Analiz Modeli Bileşenleri	13
2.3.1. Sensör	14
2.3.2. Sanallaştırma Sistemi	17
2.3.3. Saldırı Tespit Sistemi	19
2.4. Test Sonuçları ve Analiz	23
3. SONUÇLAR VE ÖNERİLER	29
KAYNAKLAR	31
ÖZGEÇMİŞ	33
EKLER	34

SİMGELER VE KISALTMALAR DİZİNİ

<u>Simgeler ve</u>	<u>Açıklamalar</u>
<u>Kısaltmalar</u>	
AV	: Anti virüs
Bot	: Köle Bilgisayar
Botnet	: Köle Bilgisayar Ağı
CERT	: Bilgisayar Olaylarına Müdahale Ekibi (Computer Emergency Response Team)
DETS	: Düşük Etkileşimli Tuzak Sistemi
DDoS	: Dağıtık Servis Dışı Bırakma (Distributed Denial of Service)
IDP	: Saldırı Tespit Önleme (Intrusion Detection Prevention)
IP	: İnternet Protokolü (Internet Protocol)
MD5	: Mesaj Özet Algoritması 5 (Message-Digest Algorithm 5)
MZ	: DOS MZ Yürütülebilir Dosya (DOS MZ Executable)
OpenVPN	: Açık Kaynak VPN çözümü
PE	: Taşınabilir Yürütülebilir Dosya (Portable Executable)
STS	: Saldırı tespit sistemi (IDS - Intrusion Detection System)
TCP	: İletim Kontrol Protokolü (Transmission Control Protocol)
TS	: Tuzak Sistemi (Honeypot)
VLAN	: Sanal Yerel Alan Ağı (Virtual Local Area Network)
VPN	: Sanal Özel Ağ (Virtual Private Network)
YETS	: Yüksek Etkileşimli Tuzak Sistemi
ZYTAM	: Zararlı Yazılım Toplama ve Analiz Merkezi

ŞEKİLLER DİZİNİ

<u>Sekil No:</u>	<u>Sayfa</u>
2.1: Sehgal tarafından önerilen dağıtık tuzak ağı topolojisi.	5
2.2: Song et al. tarafından önerilen Darknet temelli zararlı yazılım toplama modeli.	6
2.3: Darknet temelli zararlı yazılım toplama modeli akış diyagramı.	7
2.4: Birinci nesil tuzak sistem ağı.	8
2.5: İkinci nesil tuzak sistem ağı.	9
2.6: Üçüncü nesil tuzak sistem ağı.	10
2.7: HoneyBow GENIII tuzak ağı topolojisi.	11
2.8: Dağıtık zararlı yazılım toplama ve analiz modeli topolojisi.	14
2.9: Zararlı yazılım toplama akış diyagramı.	16
2.10: Suricata ağ üzerinden dosya çıkarma için yapılandırma dosyası değişiklikleri.	20
2.11: Ağ üzerinden bütün dosyaları diske kaydetme için STS imzası.	20
2.12: Zararlı yazılım analiz sistemi akış diyagramı.	22
2.13: Yakalanan tekil dosyaların günlere göre dağılımı.	24

TABLÖLAR DİZİNİ

<u>Tablo No:</u>	<u>Sayfa</u>
2.1: Dionaëa tarafından dinlenen portlar ve verilen servisler.	19
2.2: Dağıtık zararlı yazılım toplama ve analiz modeli tarafından toplanan dosyalar.	23
2.3: Tespit edilen zararlı yazılım aileleri ve adetleri.	25
2.4: Zararlı dosya tarafından indirilen autorun.inf dosyası içeriğı.	26
2.5: Zararlı yazılımın güncellenmesi sırasında web sunucudan alınan hatalar.	26
2.6: 870f5f36745f3c0b90ab391f6f383f41 MD5 özetli zararlı yazılım içeriğı.	27
2.7: Virut zararlısı STS imzası.	28

1. GİRİŞ

Zararlı yazılımlar günümüz siber dünyasının en büyük tehditlerinden biridir. Zararlı yazılım siber ortamdaki varlıklara zarar vermek, çalışmasını engellemek bu varlıklardan veri çalmak gibi çeşitli görevleri edinmiş yazılımlara verilen isimdir. Tehdit alanı genişleyen zararlı yazılımlar artık son kullanıcı bilgisayarlarından, sunucu sistemlere, mobil cihazlardan, pos cihazlarına, gömülü sistemlerden, tıbbi sistemlere kadar farklı tiplerdeki siber ortam araçlarını hedef almaktadır. Tehdit alanlarının genişlemesinden dolayı her gün oluşturulan zararlı yazılımlar da artmaktadır. Günlük olarak tespit edilen zararlı yazılımların son üç yıldaki değişimlerine bakacak olursak; 2010 yılında 50.000 [Web 1], 2011 yılında 70.000 [Web 2] ve 2012 yılında ise 100.000 [Web 3] sayısına ulaşmıştır. Zararlı yazılımları tespit etmek için defakto standart olarak bilinen anti virüs tarayıcılar veya antimalware tarayıcılar kullanılmaktadır. Bu yazılımlar gerek imza tabanlı tespit yapmaları ve imza veri tabanlarında olmayan dosyaları tespit edememeleri, gerekse sezgisel taramalarındaki yanlış pozitif (false-pozitive) oranlarının yüksek olmalarından dolayı etkin bir koruma sağlayamamaktadır. Zararlı yazılım geliştiricileri, anti virüs tarayıcıların belirli bir sürüm zararlı yazılımı engellemeye başladıktan sonra bu zararlı yazılımın kodunu değiştirip geliştirerek yeni sürüm zararlı yazılım ile sistemlere zarar vermeyi sürdürmeyi amaçlar. Zararlı yazılım analistleri de yeni bir zararlı yazılım ile karşılaştıklarında, bu zararlı yazılımı analiz ederek karakteristiğini bulmakta ve yazılıma ait anti-virüs imzasını oluşturmaktadır. Kurumları hedef alan yeni zararlı yazılımların anında tespiti ve engellenmesi anti virüs imzalarının hızlı bir biçimde güncellenmesi ile mümkündür. Bu işlemlerin otomatik olarak yapılması zararlı yazılımın vereceği etkiyi 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 bilgisayar solucanı, virüs gibi zararlı yazılımlar tarafından yapılan saldırıları ya da bilgisayar korsanları (hacker) tarafından gerçekleştirilen atakları üzerine çekecek şekilde tasarlanmaktadır. Temel görevleri bir uygulamayı, servisi, işletim sistemini ya da bilgisayar ağını taklit ederek saldırı kayıtlarının ve zararlı içeriğin toplanmasını sağlamak, saldırganların atak yöntemlerini izlemek, metotlarını belirlemek, yeni geliştirilen saldırı tekniklerinden önceden haberdar olmak için özel olarak tasarlanmış yazılım veya sistemlerdir. Tuzak sistemler

(TS) dış dünyaya bildirilmeyen IP adreslerini kullanır. Dolayısıyla 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 tespitinde büyük rol oynamaktadır.

Bu tez çalışmasında tuzak sistemler kullanılarak oluşturulan model ile yayılma vektörü olarak bilgisayar ağlarını kullanan zararlı yazılımların toplanması, tespiti ve analizi anlatılmıştır. Erken uyarı sistemi olarak da kullanılabilecek sistem ile ağ üzerinde yayılmaya çalışan yeni zararlı yazılımların ya da var olan zararlı yazılımların yeni varyantlarının tespiti mümkün olmaktadır.

Bölüm 2.1 ağ üzerinden zararlı yazılım toplamaya ilişkin literatürde önerilmiş, yaklaşımlardan bahsedilmiş ve bu çalışmalara temel olan tuzak sistem çeşitleri anlatılmıştır. Bölüm 2.2'te bu yüksek lisans çalışmasına konu olmuş model anlatılmış bu modelin bileşenleri ayrıntılı olarak incelenmiştir. Bölüm 2.4'de bu model ile yakalanan zararlı yazılımların istatistikî verileri ve analizleri tartışılmış. Sonuç ise Bölüm 3'de yer almıştır.

2. YÖNTEM

Bu bölümde, zararlı yazılım toplama ve analiz modellerine yönelik önerilen yönteme temel oluşturacak bilgiler verilmiş ve zararlı yazılım toplamaya ilişkin literatürde önerilmiş yaklaşımlardan bahsedilmiştir.

2.1. KONU İLE İLGİLİ ÇALIŞMALAR

Zararlı yazılım toplamak için oluşturulmuş birçok araştırma mevcuttur. Yapılan çalışmaların büyük bir çoğunluğu tuzak sistemleri/ağları kullanarak yapılmış çalışmalardır. Tuzak sistemler:

- Yetkisiz girişler hakkında bilgi toplamak,
- Gelen saldırıları tespit etmek,
- Saldırı kayıtlarını kaydetmek
- Hedef şaşırtmak

gibi amaçlar için kullanılan bilişim sistemi araçlarıdır.

Tuzak sistemler kabiliyetlerine göre düşük etkileşimli ve yüksek etkileşimli olarak ikiye ayrılır [Provos and Holz, 2007]. Düşük etkileşimli TS'ler bir ağı ya da ağ servisini taklit edebilmektedir. Honeyd [Web 4] düşük etkileşimli TS'ler için ilk ve en bilindik örnektir. Honeyd, bir bilgisayar üzerinde 65535'e kadar sanal ağ ve sunucu barındırıyor gibi gösteren bir yazılımdır. Honeyd verilen yapılandırmaya göre bir bilgisayar üzerinde sanal ağlar oluşturabilmekte ve bu ağlar içinde çalışan Cisco IOS, Microsoft Windows 2000, Linux 2.4 vb. işletim sistemlerine ait sunucuları taklit edecek şekilde tasarlanmıştır [Spitzner, 2003]. Ayrıca bu işletim sistemleri üzerinde çalışan FTP, HTTP, SNMP gibi çeşitli hizmetlerinde servis edildiğini bildirmektedir. Fakat bu simülasyon yeteri kadar gerçekçi değildir. Düşük etkileşimli TS'lerin yönetilmesi, bakımı oldukça kolaydır. DETS'ler ile saldırı istatistiği toplanabilmesine rağmen saldırının içeriği hakkında doyurucu bilgi sağlamamaktadır.

Yüksek etkileşimli TS'lerde ise sunulan ağ servisleri, işletim sistemleri gerçek cihazlar ya da sanallaştırma sistemleri üzerinde çalıştırılmaktadır. Sunulan servisler açıklık barındırır ve saldırganın ya da zararlı yazılımın servislerdeki açıklık vasıtasıyla sisteme sızdırılması sağlanmaktadır. Yüksek etkileşimli TS'ler daha fazla ve derinlemesine saldırı analizi yapılmasına da imkân sunar. Fakat bakımı ve yönetilmesi düşük etkileşimli TS'ler göre daha zor olmaktadır.

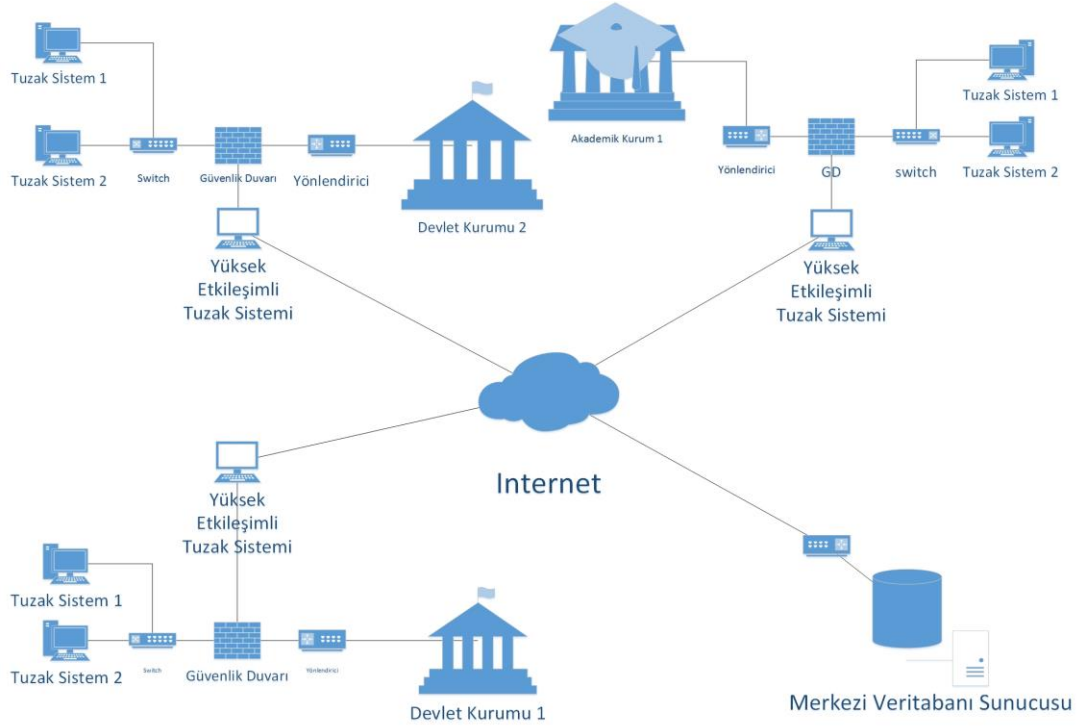
[Sehgal, 2012]'de Botnet tespiti için zararlı yazılım yakalama ve analiz altyapısı önerilmiştir. Botnet, 'Robot Network' kavramından türetilmiştir. Botnet; dağıtık halde çalışan bir ağı, ağ içindeki binlerce köle bilgisayar ve bu köle bilgisayarları yöneten BotMaster'dan oluşmaktadır. Köle bilgisayar ya da bot'lar uygulamalarda ya da işletim sistemlerindeki açıklıktan faydalanılarak ele geçirilerek robot ağı dahil edilen sistemlerdir. Robot ağı dahil olan köle bilgisayarlar, BotMaster'ın gönderdiği komutlar doğrultusunda DDoS saldırıları, istenmeyen e-posta gönderileri gibi çeşitli saldırı amaçları için kullanılmaktadır. Bu sistem mimarisi sayesinde binlerce bilgisayar tek bilgisayar gibi davranabilmektedir.

[Sehgal, 2012] tarafından önerilen model, üç katmandan oluşan ve Şekil 2.1'de gösterildiği üzere dağıtık honeynet'in (tuzak sistem ağı) kendi başına yayılmaya çalışan zararlı yazılımları toplamasını amaçlamaktadır.

İlk katman tuzak sistem ağı sensörlerini ki bu sensörler zararlı yazılım yakalamak için kullanılmaktadır. Bu sensörler düşük etkileşimli ve yüksek etkileşimli tuzak sistemlerinin her ikisini de içermektedir.

İkinci katman tuzak sistem ağı sunucularını betimler. Tuzak sistem ağı sunucuları sensörler tarafından gönderilen verileri işleyip ilişkisel veri tabanına çevirmek için kullanılmaktadır.

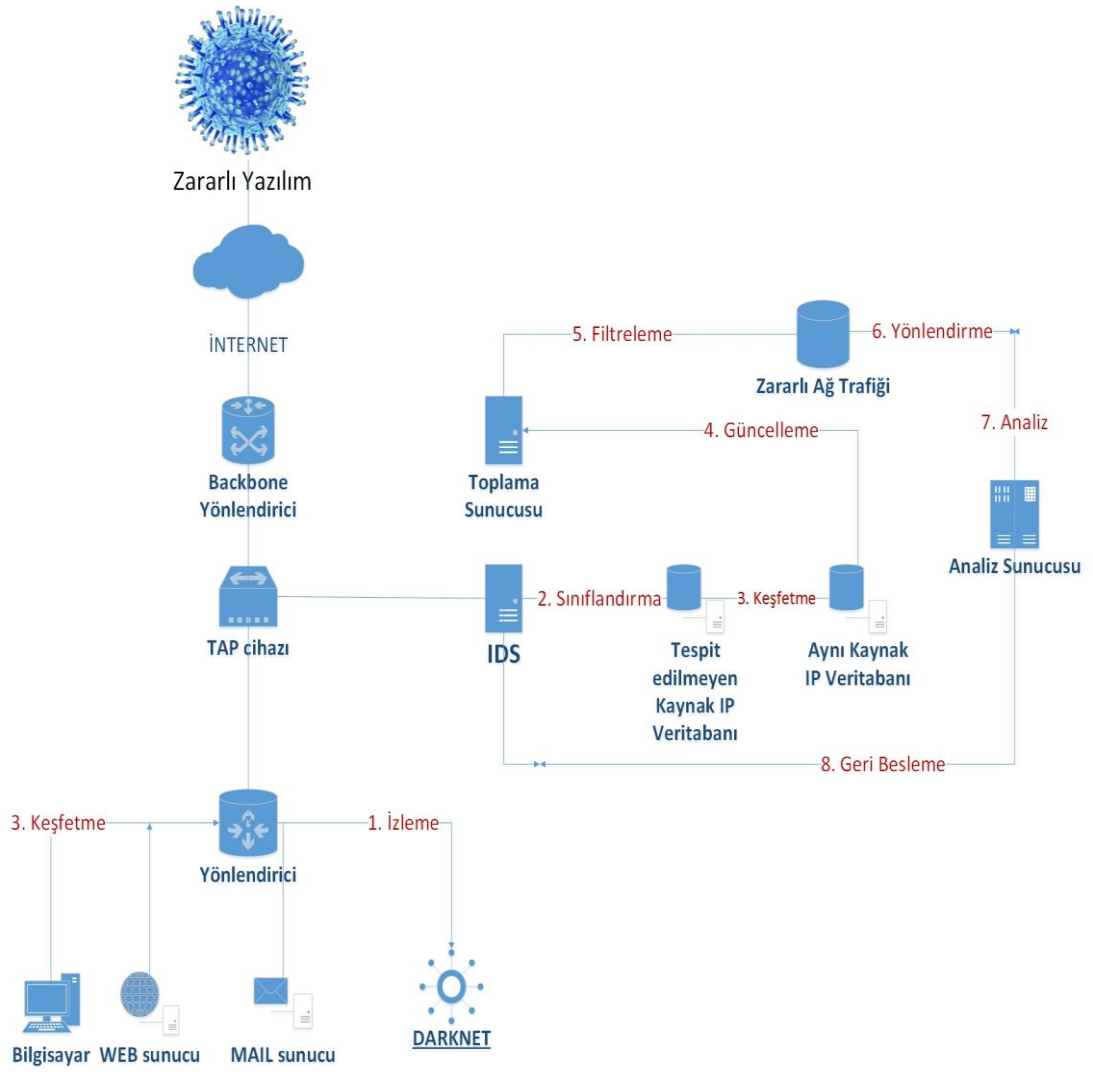
Üçüncü katman ise analizin kaynağı olan veri tabanını tanımlamaktadır.



Şekil 2.1: Sehgal tarafından önerilen dağıtık tuzak ağı topolojisi.

Kurulan tuzak sistem ağlarından elde edilen zararlı yazılımlar ve ağ saldırı verileri zararlı yazılım toplama merkezinde bulunan bir ilişkisel veri tabanında saklanmaktadır. Bu veri tabanı zararlı yazılımın MD5 hash (özet değeri) çıktısı ve tuzak sistem kaynak IP adresini saklamaktadır. Ayrıca merkezde bulunan analiz sunucusu üzerinde bu zararlı yazılım dinamik analiz sürecine tabi tutulmaktadır. Analizin sonucu bir web sunucusu vasıtası ile gösterilebilmektedir. Bahsedilen altyapıda, sistemin veri kaynağı olan tuzak sistem ağı, kurum ağına kurulacaktır. Tuzak sistem ağında tuzak sistem bilgisayarları, tuzak sistem ağ geçidi ve sanal anahtarlama cihazları gibi yapıları bulundurulmaktadır. Bu yapıların da uzaktan bakımının yapılması ve yönetilmesi zararlı yazılım yakalama işleminin otomatikleştirilmesinin önüne geçebilmektedir.

[Song et al., 2012]'de Darknet'i temel alan zararlı yazılım tespit modeli önerilmiştir. Darknet [Web 5], kurum için ayrılan ve kuruma yönlendirilmiş IP bloğunun, içinde aktif cihaz, sunucu ve servislerin yer almadığı bir bölümüdür. Buna göre bir kurumda kullanılmayan bir IP bloğundan Darknet oluşturulur. 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.



Şekil 2.2: Song et al. tarafından önerilen Darknet temelli zararlı yazılım toplama modeli.

Sekiz aşama olarak tasarlanan sistem aşağıdaki adımlardan oluşmaktadır.

- İzleme,
- Sınıflandırma,
- Keşfetme,
- Güncelleme,
- Süzme,
- Yönlendirme,
- Analiz etme,
- Geri besleme

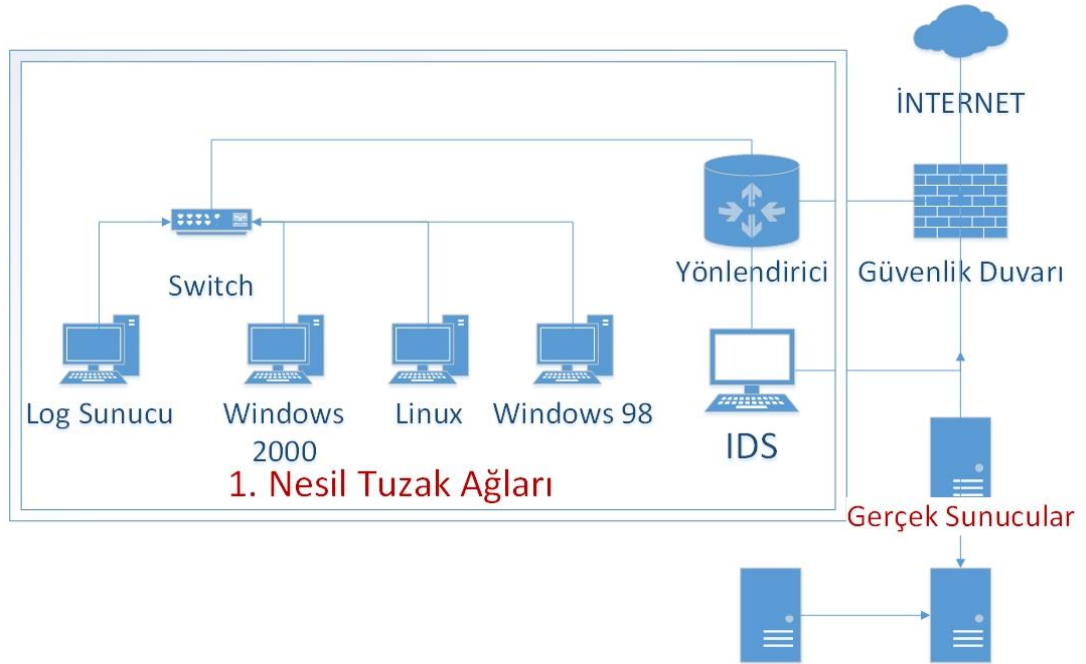
Bu adımlar doğrultusunda bir TAP cihazı ile kuruma gelen ağ trafiğinin kopyası çıkarılmaktadır. TAP cihazı ile oluşturulan ağ trafiği analiz sistemi ağı adı verilen ağa yönlendirilmektedir. Analiz sistemine yönlendirilen bu ağ trafiği ile zararlı yazılım elde etmek için çalışmalar yapılmaktadır. Ağ trafiği saldırı tespit sistemi üzerinden geçirilerek bu ağ trafiğinin atak içerip içermediğine bakılmaktadır. Eğer STS bu ağ trafiğinden bir alarm oluşturmuyorsa saldırgan IP adresinin gerçek sistemlere paket gönderip göndermediği kontrol edilmektedir. Gönderilen paketler spoof (sahte) IP değil ise zararlı ağ trafiği veri tabanına kaydedilmekte ve analiz sunucusu üzerinden geçirilmektedir. Analiz sunucusu üzerinde STS imzası oluşturup STS'ye geri bildirim olarak girilmekte ve gelecekte bu saldırıyla karşı karşıya kalındığında saldırıya bağışıklık kazanılmaktadır.

Şekil 2.3: Darknet temelli zararlı yazılım toplama modeli akış diyagramı.

Sistemden zararlı yazılım elde etmek için bütün kurumlarda Darknet bloğu oluşturulması ve zararlı yazılım tespit ağı kurulması gerekmektedir. Ayrıca zararlı yazılım ağı içerisinde STS, veri tabanı ve analiz sunucusu gibi yapıları da barındırmak zorundadır. Böylesine büyük bir sistemin farklı kurumlara konumlandırmak, uzaktan yönetmek ve bakımını yapmak etkin olmayabilmektedir.

[Zhuge et al., 2007]’de kendi kendine yayılan bilgisayar solucanları ve bot gibi zararlı yazılımlar için HoneyBow araç seti modelini önermişlerdir. Yüksek etkileşimli TS kullanılarak MwWatcher, MwSubmitter, MwFetcher ve MWHunter gibi alt bileşenlerden oluşan bu yapı The HoneyNet Project [Web 6] tarafından önerilen GENIII tuzak sistem ağını kullanmaktadır.

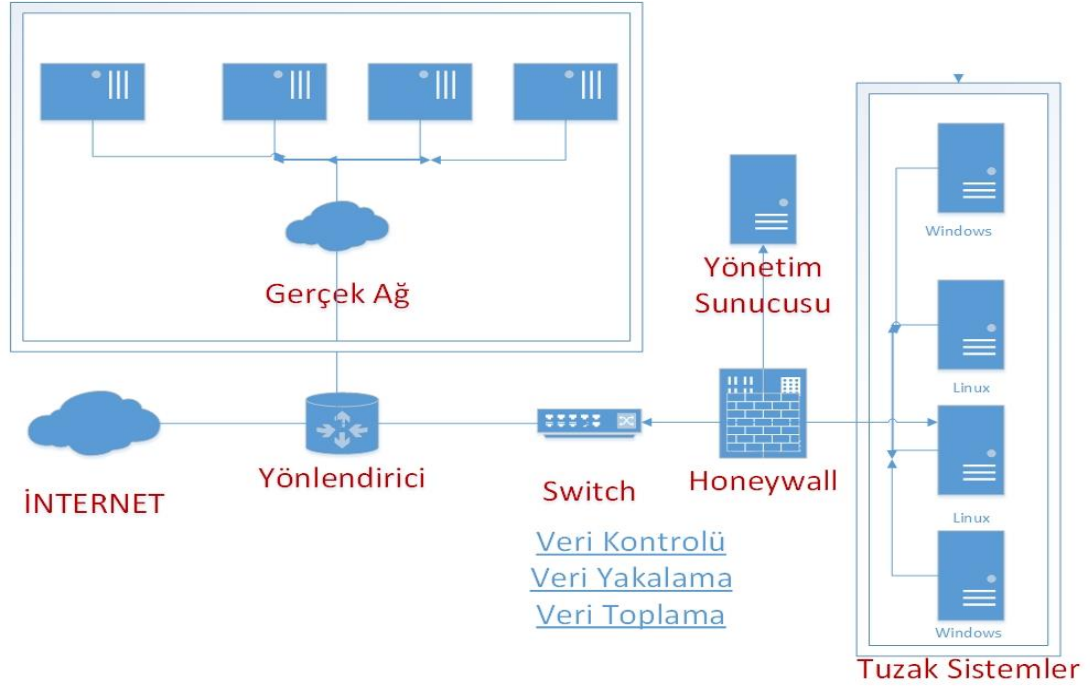
Birinci nesil tuzak ağı (GENI HoneyNet) kavramı 1999 yılında çıkmıştır [Spitzner, 2003]. Bir saldırı tespit sistemi ile ağ geçidi olarak kullanılmakta olan güvenlik duvarı ve bu ağ geçidinin arkasında gerçek cihazlar üzerine kurulu tuzak sistemlerinden oluşmaktaydı. Ağ geçidi üzerinde iki ağ kartı bulunmakta, bir tanesi İnternet’e diğeri ise tuzak sistemi bloğuna bağlanmaktaydı.



Şekil 2.4: Birinci nesil tuzak sistem ağı.

İkinci nesil tuzak ağı (GENII HoneyNet) kavramı 2001 yılında çıkmıştır [Spitzner, 2003]. Ağ geçidi artık STS ve güvenlik duvarının her ikisini barındırmakta, bu ağ geçidinin arkasında tuzak sistemleri vardır. Fakat bu ağ geçidi üzerinde 3 ağ

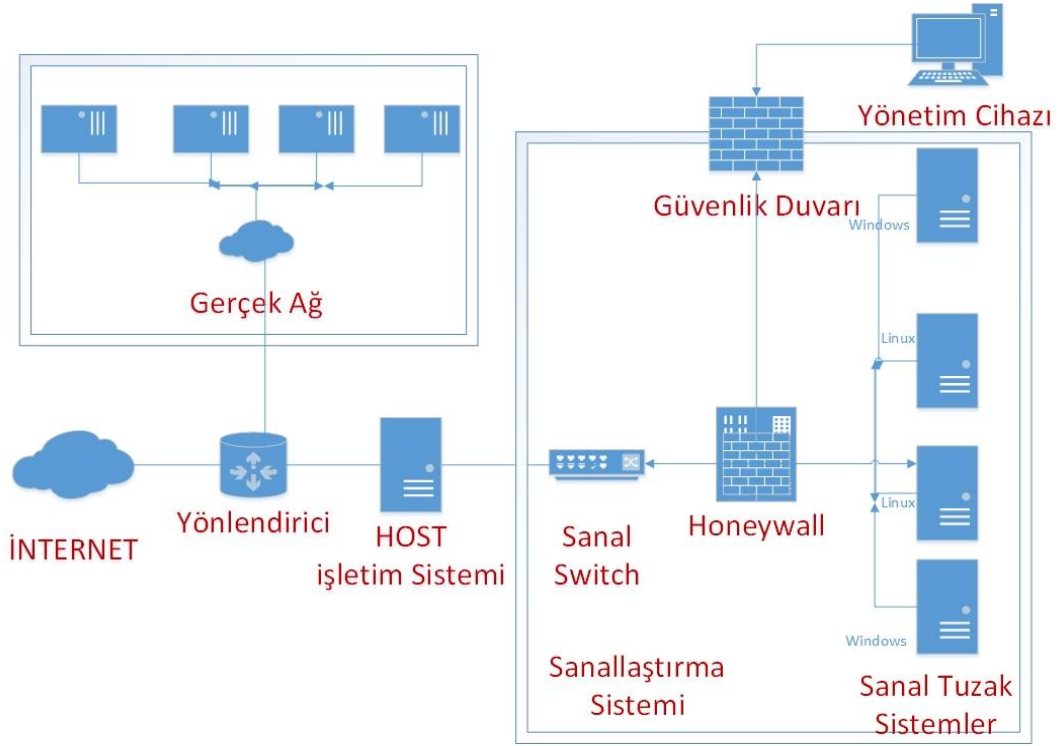
kartı bulunmaktaydı. Bir tanesi yönetim ara yüzü olarak belirlenirken, geri kalan iki ağ ara yüzü köprü modunda çalışmaktadır. GENII tuzak ağları genellikle ağ ve taşıma katmanında var olan saldırıları analiz etmek için kullanılmaktadır.



Şekil 2.5: İkinci nesil tuzak sistem ağı.

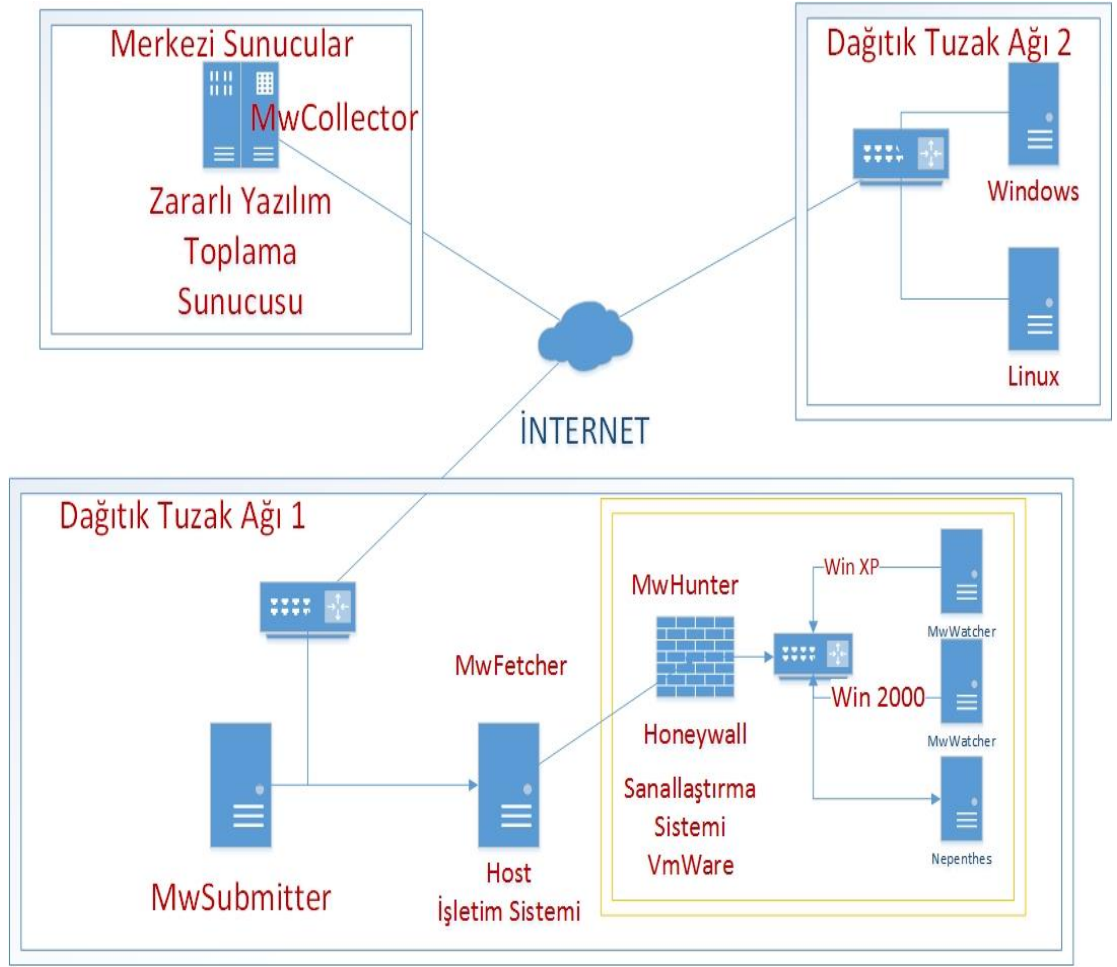
Üçüncü nesil tuzak ağı (GENIII Honeynet) 2004 yılında ikinci nesil tuzak ağlarının benzeri olarak tasarlandı [Abbasi and Harris, 2009]. Fakat sanallaştırma sistemleri üzerinde de çalışacak şekilde değiştirilmişti. Ek olarak yüksek etkileşimli tuzak sistemi olan sebek [Web 7] sunucusu ağ geçidine eklenmiş ve bu ağ geçidi bir web ara yüzü ile kontrol edilebilmektedir. .

Sebek istemci sunucu mimarisi ile çalışan bir veri yakalama yazılımıdır. İstemci yazılım tuzak sistemi üzerinde işletim sistemi çekirdeği modülü olarak çalışmaktadır [Web 8]. Sebek klavye girişlerini, kullanıcı şifrelerini ve dosya yüklemelerini kayıt altına alarak HoneyWall [Web 9] üzerinde çalışan sebek sunucusuna göndermektedir.



Şekil 2.6: Üçüncü nesil tuzak sistem ağı.

Şekil 2.7’te gösterilen yapıya göre farklı kurumlarda bulunan GENIII mimarisindeki tuzak ağları HoneyBow bileşenleri ile tümleşik çalışmaktadır. Bir tuzak ağında MwHunter Honeywall üzerinde çalışırken başka bir tuzak ağında MwSubmitter ve MwWatcher gibi alt bileşenler çalışmaktadır.



Şekil 2.7: HoneyBow GENIII tuzak ağı topolojisi.

HoneyBow'u oluşturan yapılara gelecek olursak:

MwWatcher: Microsoft Windows işletim sistemleri üzerinde çalışarak tuzak sistemi dosya sistemini gerçek zamanlı izleyerek şüpheli dosyaları yakalamaya çalışmaktadır.

MwFetcher: Linux işletim sistemi üzerinde çalışarak potansiyel zararlı yazılımları dosya sistemindeki değişiklikleri karşılaştırarak VMware sanal diskinden çıkarmaya çalışmaktadır. MwSubmitter, MwWatcher ve MwFetcher tarafından toplanan potansiyel zararlı yazılım örneklerini mwcollect'e göndermektedir.

MwHunter: Snort saldırı tespit sistemine eklenti olarak yazılmış bir araçtır. Amacı ağ üzerinden PE (taşınabilir yürütülebilir) dosyaları diske kaydetmektir. Ağ üzerindeki paketleri dinleyip dosya başlığında bu dosyanın çalıştırılabilir bir dosya olduğunu belirten MZ ve PE bilgisini aramaktadır. Bu bilgileri bulduktan sonra dosyanın uzunluğunu da tespit edip bu uzunluktaki dosyayı ağ üzerinden diske kaydetmektedir.

Bahsedilen çalışmalar dışında [Takeda and Mizutani, 2011]'de sunulan sürekli zararlı yazılım toplama ve analiz çatısı, [Moore et al, 2004]'de sunulan Network telescope, NoAH [Kohlrausch, 2009] ve The Honeynet Project [Web 6] gibi birçok araştırma da dağıtık ortamda ağ saldırı analizi ve zararlı yazılım toplama üzerine yoğunlaşmıştır.

2.2. ÖNERİLEN YÖNTEM

Var olan zararlı yazılım toplama ve analiz sistemleri incelendiğinde [Sehgal, 2012], [Song et al., 2012], [Zhuge et al., 2007] tuzak sistemlerin ve bileşenlerinin büyük bir çoğunluğunun zararlı yazılımların toplanacağı kurumlara konumlandırıldığı görülmektedir. Kurumlar kendi ağ bileşenlerinin güvenliğinin sağlamak dışında zararlı yazılım toplama ve analiz altyapılarının bileşenlerinin büyük bir kısmına gelebilecek ağ ataklarına karşı koruması da gerekmektedir. Bunun yanında zararlı yazılım toplama ve analiz sistemlerinde yer alan tuzak sistemlerin, bilgisayar korsanları veya zararlı yazılımlar tarafından ele geçirilerek, bu sistemlerden kurum ağındaki diğer sistemlere, farklı kurumlardaki sistemlere saldırıda bulunduğu bu saldırıların da kontrol altına alınması gerekmektedir. Ayrıca farklı kurumlara konumlandırılacak cihazların olası yazılım ve donanım hatasında sistemin işleyişine devam edebilmesi mümkün olmayabilmektedir.

Bu sebeplerden dolayı kurumlara konumlandırılacak zararlı yazılım toplama ve analiz bileşenlerinin:

- En az sayıda olması,
- Kurumun ağ topolojisinde herhangi bir değişiklik olmadan kurulabilmesi,
- Ele geçirildiğinde kurum sistemlerini tehdit etmemesi,
- Kuruma bakım, onarım ve yönetme maliyeti getirmemesi

gibi koşulları sağlaması bir avantaj olarak görünmektedir. Bu avantajın yanında toplanan ve tespit edilen zararlı yazılımların niceliğinde negatif yönde bir değişiklik olmadığı takdirde sistemin başarılı olduğu söylenebilecektir.

Önerilen model zararlı yazılım toplanabilmesi için dağıtık haldeki sensörlerden ve toplanan dosyaların analizinin yapıldığı merkezi birimden oluşmaktadır. Diğer çalışmaların aksine dağıtık olarak konumlandırılan sensörler üzerinde herhangi bir servis ya da tuzak sistemi uygulaması sunmamaktadır. Üzerinde veri toplamakta ve

analiz yapılmamaktadır. Analiz merkezi birimdeki STS, anti virüs tarayıcılar, veri tabanları ve bu veriler üzerinde işlem yapan betikler ile gerçekleşmektedir.

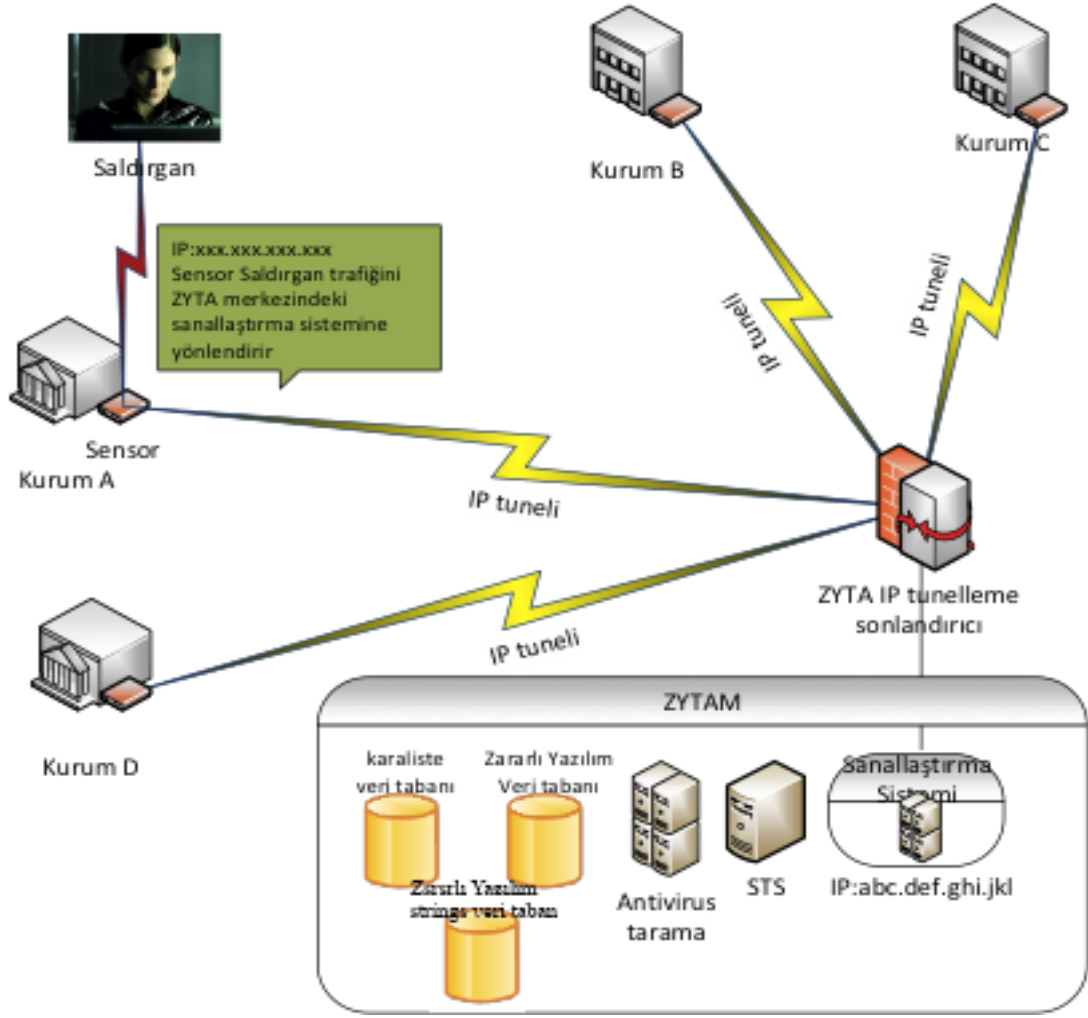
2.3. Dağıtık Zararlı Yazılım Toplama ve Analiz Modeli Bileşenleri

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

- Saldırgan veya zararlı yazılım ağ trafiğini sanallaştırma ortamına yönlendiren, farklı kurumlarda konumlandırılan yönlendirici sensör bilgisayarlar.
- Yüksek ve düşük etkileşimli tuzak sistemlerini içinde barındıran sanallaştırma ortamı.
- Düşük etkileşimli tuzak sistemlere gelen saldırgan ağ trafiğinden alarmlar üreten STS.
- Yüksek etkileşimli tuzak sistemlere gelen ikili dosyaları ağ üzerinden çıkaran modül.
- Zararlı yazılım MD5 değeri veri tabanı.
- Zararlı yazılım tarama sistemi.
- IP&DNS Kara liste veri tabanı.
- Zararlı yazılım ‘strings’ veri tabanı.

Sensöre gelen ağ trafiği analiz merkezine IP tüneli ile gönderilerek, merkezde bulunan ve bu sensöre ait kurulmuş olan tuzak sistemlerinde çalıştırılarak analiz edilmesini sağlamaktadır. Merkez ise tespit ve analiz sunucularını barındırmaktadır.

Şekil 2.8’de dağıtık zararlı yazılım toplama ve analiz modelinin topolojisi görülmektedir.



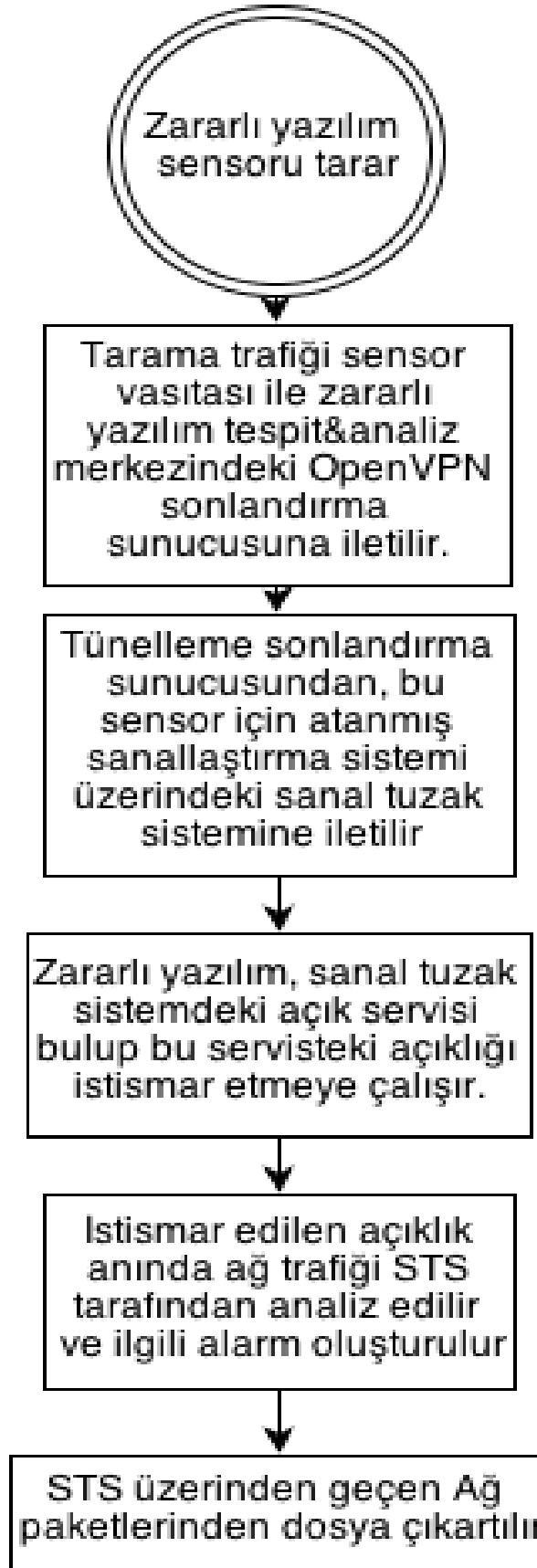
Şekil 2.8: Dağıtık zararlı yazılım toplama ve analiz modeli topolojisi.

2.3.1. Sensör

Sensör olarak kullanılacak cihazın görevi sadece ağ trafiğini yönlendirmektir. Buradaki yönlendirme klasik bağlamda kullanılan yönlendirici cihaz gibi değildir. Bir ağ geçidi gibi davranıp sensöre gelen ağ trafiğini zararlı yazılım tespit ve analiz merkezine göndermekte, buradan dönen cevapları yine sensör cihaz üzerinden geçirerek saldırgana iletmektedir. Bu işlem IP tünelleme ile yapılarak sensör cihazın bir ağ ve içerisinde barındırdığı sunucu ve istemci bilgisayarlar gibi gösterilmesini sağlamaktadır. Ayrıca sensör bilgisayar, üzerinde hiçbir servis sunmamaktadır. Bu sebeple işlemci ve bellek kullanımı çok az olmaktadır. Dolayısıyla bu cihaz için donanım seçerken maliyeti az olan Raspberry-pi [Web 10] gibi mikro-pc'ler seçilebilmektedir.

IP tüneli için açık kaynak VPN çözümü OpenVPN [Web 11] kullanılmaktadır. Sensör ZYTAM'a IP tüneli ile bağlanırken istemci olarak bağlanmaktadır. Bu yapıda OpenVPN'in iç yönlendirme tablosu kullanılmaktadır. Böylece hangi sensör hangi kurumda bilgisi OpenVPN tarafından tutulmaktadır.

Sensörler kurumun kullanılmayan IP adresleri içerisinde seçilmektedir. Sensörlere birden fazla IP ataması yapılabilmekte dolayısıyla tek cihaz üzerinden kurumda kullanılmayan IP adresi kadar tuzak sistemi oluşturulabilmektedir. Yani kurumun kullanılmayan C blok ağ adresi var ise tek sensör ile 254 adet tuzak sistemi bu kuruma tahsis edilebilmektedir. Gerçek IP ataması yapılan sensöre karşılık tuzak sistem için özel IP adresi atanmaktadır. Bu özel IP cihazın iç ağ IP adresi gibi düşünülebilmektedir. Örnek verecek olursak A Kurumu IP bloğu 8.8.8.0/24 olsun, bu kurum sensör cihazı için 8.8.8.8 gerçek IP adresini kullanabilir. ZYTAM tarafında ise tuzak sistem IP adresi ise 192.168.1.8 eşlemesi yapılabilmektedir. Böylece 8.8.8.8 ile 192.168.1.8 IP çifti bu kuruma ait tuzak sistemin IP adresleri olarak tanımlanmaktadır. Yani tuzak sistemin dış IP adresi 8.8.8.8 olarak, iç ağ IP adresi ise 192.168.1.8 olarak ifade edilebilmektedir.



Şekil 2.9: Zararlı yazılım toplama akış diyagramı.

Şekil 2.9’de sensör cihazdan tuzak sisteme kadar zararlı yazılımların kaydedilme adımları listelenmiştir. Bu adımlara göre;

- Zararlı yazılım öncelikle sensörün gerçek IP adresini ağ paketi gönderir.
- Gönderilen ağ paketi OpenVPN IP tüneli vasıtasıyla VPN sonlandırma sunucusundan bu sensör için hazırlanan sanallaştırma sistemi üzerindeki yüksek etkileşimli tuzak sistemine iletilmektedir. YETS olarak Windows XP, Windows XP SP1 ve SP2 kullanılmıştır. Ayrıca DETS dionaea da sanallaştırma sistemi üzerinde çalışan tuzak sistemlerindendir.
- Saldırgan ya da zararlı yazılım tarafından gönderilen ağ paketleri tuzak sistemin açıklığını istismar edebilecek bir kod içeriyor ise tuzak sistemi ele geçirecektir.
- Saldırı tespit sistemi sanallaştırma sisteminin önüne konumlandırılmıştır ve VPN sonlandırma cihazı ile sanallaştırma sistemi arasında kalmaktadır. Dolayısıyla sanallaştırma sistemi üzerindeki tuzak sistemlerin ağ hareketleri STS üzerinde tespit edilebilmekte ve zararlı içerik bulunduğu anda alarm üretebilmektedir.
- Saldırgan tarafından gönderilen ağ paketleri çalıştırabilir dosya içeriyor ise bu dosya ağ üzerinden diske kaydedilmektedir. Daha ayrıntılı bilgi için Şekil 2.10 ve Şekil 2.11’e bakılabilir.

2.3.2. Sanallaştırma Sistemi

ZYTAM içerisinde aşağıda listelenen avantajları sebebi ile sanallaştırma kullanılmasına karar verilmiştir.

- Farklı ağlarda kurulacak tuzak sistemlerini bir merkezden yönetmek,
- Zararlı yazılım bulaşmış tuzak sistemlerini zararlı yazılımdan arındırıp yeniden kurmak,
- Tuzak sistemlerin sayısının genişletilebilir olması.

Tuzak Sistemlerini barındıracak olan sanallaştırma ortamı açık kaynak sanallaştırma çözümü olan Oracle VirtualBox [Web 12] seçilmiştir.

Oracle VirtualBox;

- Açık kaynak olması
- 32 ve 64 bit platformda çalışabilmesi
- 32 ve 64 bit işletim sistemlerini çalıştırabilmesi
- Uzaktan kontrol edilebilmesi,
- Web ara yüzü ile yönetilebilmesi,

- Komut satırı desteđi olması,
- Sanal makinelerin dışarıdan komut alabilmesi,
- VLAN desteđi sağlaması

gibi yeteneklere sahiptir. Özellikle tuzak sistemler için belirli işleri otomatik olarak yapılabilmesine olanak sağlayan, sanal makine dışından komut çalıştırma özelliđi sayesinde

- Tuzak sistemlerin otomatik olarak oluşturulmasına,
- Zararlı yazılım black-box testi yapılmasına,
- Belirli web sitelerinin tuzak sistemler tarafından ziyaret edilmesine,
- Tuzak sistem tarafından yakalanan zararlı dosyaların herhangi bir dosya transfer protokolü olmadan kaydedilmesine

imkân vermektedir. Sanallaştırma sistemi üzerindeki tuzak sistemlerin her biri farklı bir VLAN'a alınmakta ve bu VLAN'lar arası geçiş güvenlik duvarı yardımıyla erişime kapatılmıştır. Böylece zararlı yazılım bulaşan herhangi bir tuzak sistemi diğerlerini etkilemeyecektir.

Sanallaştırma sistemi üzerinde yüksek etkileşimli tuzak sistemi olarak kullanılacak olan işletim sistemleri Microsoft Windows XP, Windows XP SP1, Windows XP SP2'dir. Ayrıca düşük etkileşimli tuzak sistemi olarak dionaea [Web 13] kullanılmıştır. Dionaea Tablo 2.1 verilen protokol ve servisleri taklit ederek zararlı yazılımları üzerine çekmeye çalışmaktadır. Sistemin çalışması sırasında görülmüştür ki en fazla saldırı 445 SMB servisine ve 5060 SIP servisine yöneliktir.

Tablo 2.1: Dionaea tarafından dinlenen portlar ve verilen servisler.

Port Numarası	Verilen Servis
21	FTP
42	WINS
80	HTTP
135	DCE/RPC
443	HTTPS
445	SMB
1433	MSSQL
3306	MySQL
5060	SIP
5061	SIP

2.3.3. Saldırı Tespit Sistemi

Popüler açık kaynak saldırı tespit sistemi Snort'un [Web 14] yerine bu çalışmada Suricata IDP [Web 15] kullanılmıştır. Suricata yüksek performanslı ağ saldırı tespit, engelleme ve ağ güvenliği gözetleme motoru olarak kullanılmaktadır. Suricata, birden fazla işlemci çekirdeğine sahip veya birden fazla işlemcili sistemlerde farklı işlemcilere farklı öncelikler, farklı işlemci çekirdeklerine farklı işler atayabilecek şekilde tasarlanmıştır.

Sağladığı dosya çıkarma özelliği ile ağ üzerinden canlı olarak veya ağ paket kaydı içerisinden, belirli uzantılı dosyaları veya dosya tipine göre veya dosya uzunluğuna göre diske kaydedebilmekte, ayrıca dosyaların MD5 özet değerini de saklayabilmektedir. Bu adımların gerçekleşebilmesi için suricata yapılandırma dosyasında Şekil 2.10'da belirtilen değişikliklerin yapılması ve Şekil 2.11'de belirtilen STS imzalarının düzgün bir şekilde yüklenmesi gerekmektedir.

```

...
...
- file-store:
    enabled: yes # set to yes to enable
    log-dir: files # directory to store the files
    force-magic: yes # force logging magic on all stored files
    force-md5: yes # force logging of md5 checksums
stream:
    memcap: 128mb
    checksum-validation: no # reject wrong csums
    inline: no # no inline mode
reassembly:
    memcap: 256mb
    depth: 0 #
    toserver-chunk-size: 25600
    toclient-chunk-size: 25600
...
rules:
- files.rules
...
libhttp:
    default-config:
        personality: IDS
        # Can be specified in kb, mb, gb. Just a number indicates
        # it's in bytes.
        request-body-limit: 0
        response-body-limit: 0

```

Şekil 2.10: Suricata ağ üzerinden dosya çıkarma için yapılandırma dosyası değişiklikleri.

```

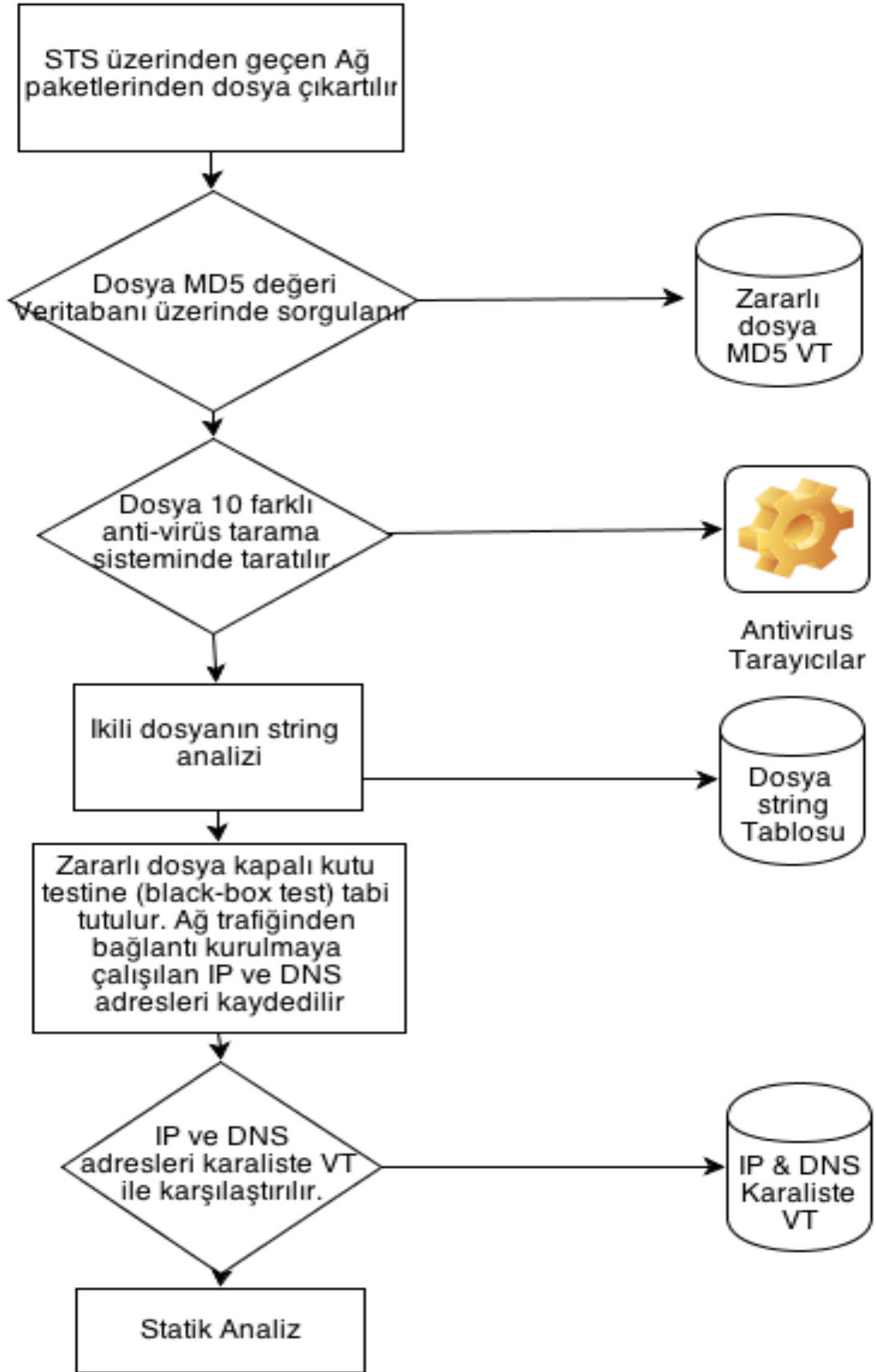
alert http any any -> any any (msg:"FILE store all"; filestore; sid:5500015;
rev:1;)
alert http any any -> any any (msg:"80386"; filemagic:"Intel 80386"; filestore;
sid:5500221; rev:1;)
alert http any any -> any any (msg:"FILE magic -- windows";
filemagic:"executable for MS Windows"; filestore; sid:5500018; rev:1;)
alert http any any -> any any (msg:" PE32 executable "; filemagic:"PE32
executable for MS Windows (GUI) Intel 80386 32-bit"; filestore; sid:5500101;
rev:1;)
alert http any any -> any any (msg:"extension=EXE"; fileext:"exe"; filestore;
sid:55000102; rev:1;)

```

Şekil 2.11: Ağ üzerinden bütün dosyaları diske kaydetme için STS imzası.

Zararlı dosya toplamak Şekil 2.9'deki adımları izledikten sonra elimize geçen dosyaların tespiti ve analizi yapılma safhasına geçilmiştir. Şekil 2.12'de Zararlı yazılım analiz sistemi akış diyagramı verilmiştir. Buna göre:

- Ağ üzerinden yakalanan ya da sanallaştırma sistemi üzerinden tuzak sistemlere kaydedilmiş dosyaların MD5 değerleri hesaplanır.
- Hesaplanan MD5 değerleri zararlı yazılım MD5 veri tabanı üzerinde sorgulanır. Sorgulama sonucu bu MD5 değeri var ise dosyanın hangi virüs ailesine ait olduğu tespit edilmiş olmaktadır.
- Eğer MD5 özet değeri veri tabanı içerisinde yer almıyor ise bu dosya 10 farklı anti virüs tarayıcı üzerinden taratılır.
- Taratma sonucu pozitif ise bu dosyanın hangi virüs ailesine ait olduğu bulunmuştur.
- Taratma sonucunda herhangi bir veriye ulaşılamıyor ise bu ikili dosyanın içerisindeki karakter dizileri tespit edilir. Zararlı dosya eğer bir sıkıştırma işleminden geçirilip paketlenmiş ise PEiD [Web 16] gibi unpacker programı vasıtası ile bu dosyanın sıkıştırılmamış hali açılır.
- Paketi açılan dosyanın içerdiği 'string'ler, zararlı yazılım string veri tabanı içinde sorgulanır ve daha önceden keşfedilen, bilinen bir virüs ailesine ait olup olmadığının tespiti yapılır.
- Eğer string sorgulamaları da cevap vermiyor ise dosya sanallaştırma sistemi içerisinde çalışan yüksek etkileşimli tuzak sistemlerinde black-box teste tabi tutulur.
- Black-box test ile dosya Windows XP YETS içerisinde çalıştırılır. Hangi dosyalara erişti, hangi dosyaları oluşturdu, hangi ağ bağlantılarını kurdu bilgileri kaydedilir.
- Kurulan ağ bağlantı bilgilerinden IP ve DNS bilgileri tespit edilir ve IP ve DNS kara liste veri tabanı içerisinde sorgulama yapılır. Sorgular olumlu dönerse zararlı yazılımın hangi aileden olduğu bulunur.
- Sorgular olumsuz döner ise dosyanın fonksiyon çağrıları tespit edilip var olan zararlı yazılımların fonksiyon çağrıları ile karşılaştırılır.



Şekil 2.12: Zararlı yazılım analiz sistemi akış diyagramı.

2.4. Test Sonuçları ve Analiz

15 – 30 Mayıs 2013 tarihleri arasındaki 16 günlük süre zarfında 2 farklı kurumda bulunan 3 farklı sensör ve bu sensörlere ait 20 farklı gerçek IP adresine gelen ağ atakları sonucu toplanan şüpheli dosyalar zararlı yazılım toplama ve analiz sistemi üzerinde analize tabi tutulmuştur. Tuzak sistemi 2 farklı tipte kullanılmıştır. Bu tuzak sistemlerinin 10 tanesi YETS: 5 tanesi Windows XP, 5 tanesi Windows XP SP1 ve geriye kalan 10 tanesi de DETS: dionaea'dır. Tablo 2.2'de belirtildiği üzere yakalanan toplam dosya sayısı 20889 olarak tespit edilmiştir. Analiz aşamasında bu dosyaların bazılarının daha önceden yakalandığı ve analiz edildiği sebebiyle bu dosyaların MD5 veri tabanında kaydı bulunmaktadır. Dolayısıyla bu dosyalar tekrardan taratılmamış, tekilleştirilmiştir. Tekil dosyaların sayısı 1058 olarak görülmektedir. 1058 dosyadan 52'sinin anti virüs tarayıcılar tarafından tespit edilemediği de gözlemlenmiştir. Tespit edilemeyen dosyalar strings karşılaştırması, black-box test gibi yöntemler ile tespit edilmeye çalışılmıştır.

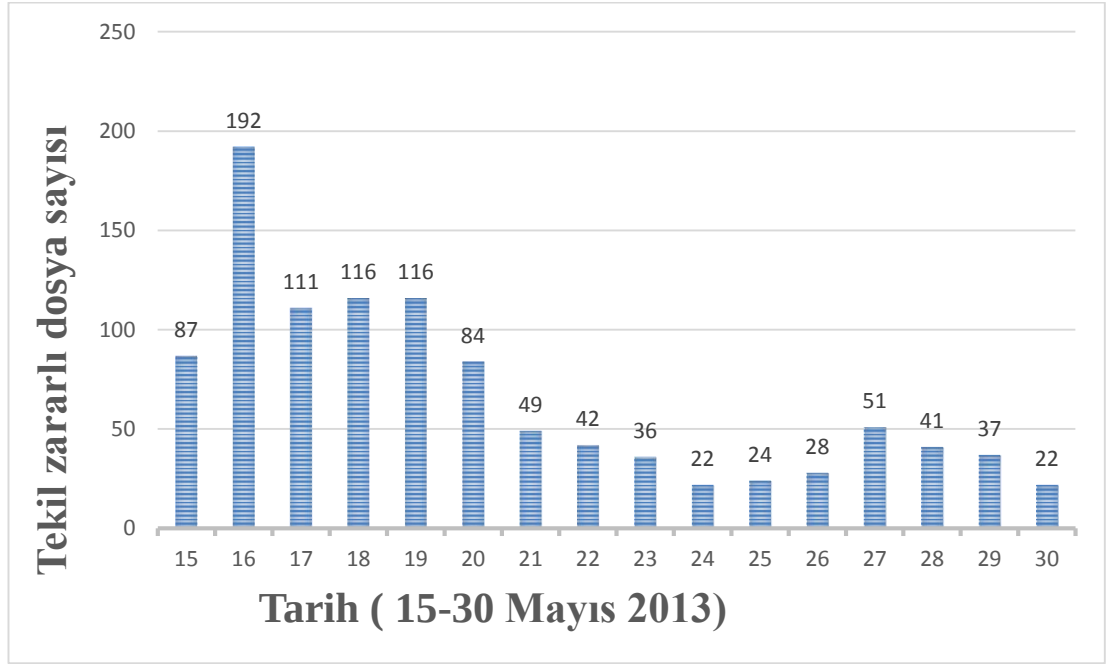
Tablo 2.2: Dağıtık zararlı yazılım toplama ve analiz modeli tarafından toplanan dosyalar.

Tip	Sayı
Toplam zararlı yazılım	20889
Tekil zararlı yazılım	1058
Anti-virüs tarayıcıların tespit edemediği zararlı yazılım	52

Toplanan dosyalar anti virüs tarama sisteminden geçirildikten sonra farklı tipte virüs, worm, backdoor, trojan olduğu tespit edilmiştir. Bunların zararlı yazılım ailelerine göre sınıflandırılması ve kaç adet yakalandığı bilgisi Tablo 2.3'de verilmiştir. Aile isimleri Microsoft zararlı yazılım koruma merkezi isimlendirme standardına göre yapılmıştır [Web 17]. Buna göre yakalanan zararlı yazılımları arasında Rbot gibi çeşitli Botnet dropper'larının yeni sürümleri, Virut botneti zararlısı, Sality polimorfik solucanı, Neeris solucanı, Parite solucanı, Allaple solucanı gibi zararlı yazılımlar tespit edilebilmektedir. Ayrıca Microsoft sistemleri hedef alana Conficker kurtçuğu da yakalanan zararlı yazılımlar arasındadır. Conficker zararlı yazılımının sayısının çok fazla olmasının nedeni YETS olarak kullanılan Windows

iřletim sistemlerinin MS08-067 [Web 18] açıklığına sahip olmaları, ayrıca DETS olarak kullanılan dionaea'nın Windows paylaşım hizmetini taklit etmesidir.

Sistem tarafından yakalanan tekil zararlı dosyaların günlere göre dağılımı Şekil 2.13'da verilmiştir. Buna göre günlük ortalama 66 zararlı yazılım tespit edilmiştir. Yeni oluşturulan zararlı yazılımların ya da varyantların yayılmasına göre bazı günler daha fazla zararlı yazılım yakalanmıştır.



Şekil 2.13: Yakalanan tekil dosyaların günlere göre dağılımı.

Tablo 2.3: Tespit edilen zararlı yazılım aileleri ve adetleri.

Zararlı Yazılım Ailesi	Adet
Backdoor:Win32/Rbot	2
Trojan:Win32/Brambul.A	10
Trojan:Win32/Dynamer!dte	1
TrojanDownloader:Win32/Small.gen!AO	1
VirTool:Win32/DelfInject.gen!N	1
Virus:Win32/Parite.B	1
Virus:Win32/Sality.AT	1
Virus:Win32/Sality.G	1
Virus:Win32/Virut.AA	3
Virus:Win32/Virut.AC	17
Virus:Win32/Virut.BB	1
Worm:Win32/Allapple.L	9
Worm:Win32/Autorun.AHA	1
Worm:Win32/Conficker.A	6
Worm:Win32/Conficker.B	631
Worm:Win32/Conficker.C	222
Worm:Win32/Conficker.gen!A	31
Worm:Win32/Dipasik.A	2
Worm:Win32/Gnoewin.A	3
Worm:Win32/Hamweq.A	2
Worm:Win32/Msblast.B	1
Worm:Win32/Neeris.gen!C	1
Worm:Win32/Networm.A	2
Worm:Win32/Small.AF	1
TOPLAM	951

Toplamda tespit edilen 951 adet zararlı dosyanın yanında 52 adet tespit edilememiş dosya vardır. Fakat yakalanan tekil dosya sayısı Tablo 2.2’de 1058 olarak belirtilmişti. Daha sonradan yapılan incelemelerde görülmüştür ki arada kalan 55 dosya yine bu zararlı yazılımlar vasıtasıyla tuzak sistem üzerine eklenmek istenen Tablo 2.4’de içeriği verilen *autorun.inf* gibi yardımcı dosyalardır. Bunun dışında zararlı yazılımın kendini güncellenmek istemesi sırasında ulaşmaya çalıştığı web sunucunun çalışmaması ya da indirmeye çalıştığı güncelleme dosyasının artık web sunucu üzerinde olmaması sebebi ile Tablo 2.5’te belirtilen web sunucunun hata kodu ile dönmesinden dolayı oluşan html dosyalardır.

Tablo 2.4: Zararlı dosya tarafından indirilen autorun.inf dosyası içeriği.

```
[autorun  
open=  
shell\open\Command=RECYCLER\NTDETECT.EXE  
shell\open\Default=1  
shell\explore\Command=RECYCLER\NTDETECT.EXE
```

Tablo 2.5: Zararlı yazılımın güncellenmesi sırasında web sunucudan alınan hatalar.

```
<HTML><HEAD><TITLE>401 Unauthorized</TITLE></HEAD>  
<BODY><H1>401 Unauthorized</H1>  
Your client does not have permission to get URL /xaydjhss from this server.  
</BODY></HTML>  
<h1>Bad Request (Invalid Hostname)</h1>
```

Anti virüs tarayıcıların tespit edemediği bazı zararlı dosyalar içerisinde anlamlı veri aranmıştır. Bunun için ikili dosyanın paketlenip paketlenmediği bilgisi PEid programı ile tespit edilmiştir. Daha sonra bir Unix komutu olan strings [Web 19] ile ikili dosya içerisindeki anlamlı veriler daha önceden yakalanmış zararlı yazılımların strings veri tabanı üzerinde sorgulanarak karşılaştırılmıştır.

Buna göre Microsoft Security Essentials [Web 20] ile tespit edilemeyen 870f5f36745f3c0b90ab391f6f383f41 MD5 özet değerine sahip zararlı yazılımın içerdiği verilerden bunun *Worm:Win32/Lovgate.AF@mm* isimli bir solucan olduğu görülmekte. Başka kaynaklarda ise bu solucanın *Worm:Win32/Virut.4960* yani Virut botnetinin bir zararlısı olarak ön plana çıkmakta.

Tablo 2.6: 870f5f36745f3c0b90ab391f6f383f41 MD5 özetli zararlı yazılım içeriği.

```
...
psapi.dll
DispatchMessageA
GetStockObject
OpenSCManagerA
ShellExecuteA
WNetCancelConnection2A
WSAIoctl
GetModuleBaseNameW
configserversmtp.163.com#ab89d@yahoo.com.cn#yf23668@163.com#eWYyMzY2OA==#MjM5O
DYzMg=-#DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD
DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD
DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD
DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD
DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD
DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD
DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD
DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD
{NThisu^L
8Pet
Getu
Procu
Addru
CloseHandle
CreateEventA
GetLastError
VT_3
...
```

Bu zararlı yazılımın STS tarafından da tespitini yapmak için ilgili imzayı oluşturmak gerekmektedir.

Tablo 2.7: Virut zararlısı STS imzası.

alert tcp any -> any 445 (msg: "lovgate virüs tespit edildi."; content: "configserversmtp.163.com#ab89d@yahoo.com"; flow:to_server,established; classtype:misc-activity;)
--

Strings veri tabanında yer almayan zararlı yazılımlar Black-box teste tabi tutularak sanallaştırma sistemi içerisindeki YETS Windows XP üzerinde çalıştırılmıştır. Oluşturduğu dosyalar ve erişmeye çalıştığı IP ve DNS bilgileri kaydedilmiştir. Buna göre *afb134ea9029631e273d63257c9ca552* MD5 özet değerine sahip zararlı yazılımın erişmeye çalıştığı 209.85.223.33 IP adresi, IP kara liste veri tabanında aratılmıştır. Bu IP adresi Google'a ait olduğu ve zararlı yazılımın spam göndermek için eriştiği bilgisi ortaya çıkmaktadır. Bu tarz mail gönderen diğer zararlı yazılımlar incelendiğinde Trojan:Win32/Brambul'a zararlı ailesine ait bir dosya olduğu belirlenmiştir.

Tespit edilen zararlı yazılımlar arasında en yaşlı zararlı yazılım 6 yıl 11 ay ile *7097c55ee0535457025dd158bb1988bb* MD5 özet değerine sahip Worm:Win32/Msblast.B adlı solucanı iken, 1 gün ile en genci *e557534a446e1c59168be54ac22c3a95* MD5 özet değerine sahip Virus:Win32/Virut.AA adlı virüsün yeni bir varyantı olmuştur.

3. SONUÇLAR VE ÖNERİLER

Zararlı yazılımların erken tespiti kişisel bilgisayarların, kurumsal sistemlerin en az şekilde etkilenmesini sağlamaktadır. Defakto standart olan anti virüslerin yetersiz kaldığı durumlarda tuzak sistemler araştırma amacıyla kullanılmıştır.

Bu tez çalışmasında zararlı yazılım tespiti için yüksek ve düşük etkileşimli tuzak sistemlerin bir arada yer aldığı bir model sunulmuştur. Literatürde yer alan modellerin aksine dağıtık tuzak sistemi ağı merkezileştirilmiş ama tuzak sistem ağını mantıksal olarak dağıtık göstermiştir. Tuzak ağına gelecek ağ saldırılarını ağ trafiği yönlendirme amacıyla kullanılan sensörler kullanılmıştır. Sensörler kurumlara yönetim ve bakım maliyetini azaltacaktır. Kurumun ağ topolojisinde herhangi bir değişiklik yapmadığı için sorunsuz bir şekilde bütün kurumlara kurulabilecektir. Sensörü temsile eden tuzak sistemi ele geçirilse bile kuruma ve zararlı yazılım tespit ve analiz merkezine sızamayacaktır.

Tuzak ağında bulunan yüksek etkileşimli sanal işletim sistemleri, saldırı tespit sistemleri, ağ üzerinden dosya çıkarma servisleri, zararlı yazılım tarama sistemi, zararlı yazılım özet değerlerinin tutulduğu veri tabanı, IP & DNS kara liste veri tabanları ile bulut güvenlik çözümü gerçekleştirilmiştir. Oluşturulan model ile anti virüs tarayıcıların imza veri tabanında olmayan yeni zararlı yazılımların ya da varyantlarının tespiti mümkün kılınmıştır.

Oluşturulan sistem yeni zararlı yazılım tespiti ve engellenmesine yönelik bütüncül çalışması ortaya koymaktadır. Yakalanan zararlı yazılımların black-box testi sırasında eriştiği IP ve DNS bilgileri kara liste olarak veri tabanında tutulmakta ve farklı zararlı yazılımların aynı IP ve DNS adresine eriştiğinde alarm vermektedir. Ayrıca bu bilgiler saldırı tespit sistemi imzalarında da kullanılması geri besleme mekanizması olarak da çalışmaktadır. STS imzası oluşturma yapısı sadece IP ve DNS bilgilerine göre yapılmamaktadır. Zararlı yazılım içeriğinde bulunan paternler de STS imzasında içerik olarak kullanılmaktadır. Sunulan model CERT'ler tarafından rahatlıkla kullanılabilecek ve yaygınlaştırılabilir yapıdadır.

Proaktif olarak çalışan sistemin daha ayrıntılı olarak zararlı yazılım tespit edebilmesi için anti virüs tarama, IP&DNS kara liste karşılaştırması, strings karşılaştırması ve black-box testi'nin [Web 21] yanında dinamik analiz ve statik analiz yöntemlerinden olan fonksiyon çağrıları listesi karşılaştırması ile daha iyi sonuç

alınabilecektir. Ayrıca Zararlı yazılımın ailesi gerçeğe en yakın olarak tespit edilebilecektir.

KAYNAKLAR

Abbasi F. H., and Harris R. J., (2009), "Experiences with a Generation III virtual Honeynet" 2009 Australasian Telecommunication Networks and Applications Conference (ATNAC), pp. 1–6.

Kohlrausch J., (2009), "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.

Moore D., Shannon C., Voelker G. M., and Savage S., (2004), "Network Telescopes?: Technical Report", pp. 1–14.

Provos N., Holz T., (2007), Virtual Honeypots: From Botnet Tracking to Intrusion Detection. Addison-Wesley Professional.

Sehgal R. K., (2012), "An Integrated Framework for Malware Collection and Analysis for Botnet Tracking Integrated Botnet tracking System,"no. 10, pp. 50–55.

Song J., Choi J., and Choi S., (2012), "A Malware Collection and Analysis Framework Based on Darknet Traffic", Neural Information Processing, pp. 624–631, 2012. pp.

Spitzner L., (2003), Honeypots: Tracking Hackers. Addison-Wesley.

Takeda K., and Mizutani M., (2011), "Design and prototyping of framework for automated continuous malware collection and analysis" Security Technology (ICCST).

Zhuge J., Holz T., Han X., Song C., and Zou W., (2007), "Collecting Autonomous Spreading Malware Using High-Interaction Honeypots" Information and Communications Security Lecture Notes in Computer Science Volume 4861, pp 438-451.

Web 1, (2013), <http://blogs.comodo.com/pc-security/computer-protection/50000-malware-created-daily/>, (Eriřim Tarihi: 02/04/2013).

Web 2, (2013), <http://eugene.kaspersky.com/2011/10/28/number-of-the-month-70k-per-day/>, Eriřim Tarihi: 02/04/2013).

Web 3, (2013), <http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2012.pdf/>, (Eriřim Tarihi: 12/04/2013).

Web 4, (2013), <http://www.honeyd.org/>, (Eriřim Tarihi: 14/04/2013).

Web 5, (2013), <http://www.team-cymru.org/Services/darknets.html> (Eriřim Tarihi: 16/04/2013).

Web 6, (2013), <http://www.honeynet.org>, (Eriřim Tarihi: 18/04/2013).

Web 7, (2013), <https://projects.honeynet.org/sebek>, (Erişim Tarihi: 01/05/2013).

Web 8, (2013), <http://old.honeynet.org/papers/honeynet/>, (Erişim Tarihi: 01/05/2013).

Web 9, (2013), <https://projects.honeynet.org/honeywall>, (Erişim Tarihi: 01/05/2013).

Web 10, (2013), <http://www.raspberrypi.org/>, (Erişim Tarihi: 04/05/2013).

Web 11, (2013), <http://www.openvpn.net/>, (Erişim Tarihi: 05/05/2013).

Web 12, (2013), <http://www.virtualbox.org/>, (Erişim Tarihi: 05/05/2013).

Web 13, (2013), <http://dionaea.carnivore.it/>, (Erişim Tarihi: 10/05/2013).

Web 14, (2013), <http://www.snort.org/>, (Erişim Tarihi: 11/05/2013).

Web 15, (2013), <http://www.suricata-ids.org/>, (Erişim Tarihi: 11/05/2013).

Web 16, (2013), <http://www.aldeid.com/wiki/PEiD/>, (Erişim Tarihi: 14/05/2013).

Web 17, (2013), www.microsoft.com/security/portal/shared/malwarenaming.aspx, (Erişim Tarihi: 15/05/2013).

Web 18, (2013), <http://technet.microsoft.com/en-us/security/bulletin/ms08-067>, (Erişim Tarihi: 15/05/2013).

Web 19, (2013), http://en.wikipedia.org/wiki/Strings_%28Unix%29, (Erişim Tarihi: 20/05/2013).

Web 20, (2013), <http://windows.microsoft.com/tr-tr/windows/security-essentials-download>?, (Erişim Tarihi: 21/05/2013).

Web 21, (2013), http://en.wikipedia.org/wiki/Black-box_testing, (Erişim Tarihi: 11/05/2013).

ÖZGEÇMİŞ

2005 yılında Kocaeli Bilgisayar Mühendisliğinden mezun olan Bâkır EMRE 2006 yılında TÜBİTAK bünyesinde faaliyet gösteren UEKAE'de araştırmacı olarak iş hayatına başlamış, halen TÜBİTAK-BİLGEM Siber Güvenlik Enstitüsü'nde uzman araştırmacı olarak görevine devam etmektedir. BSD/Unix sistemler, güvenlik duvarları, saldırı tespit sistemleri, tuzak sistemleri, sandboxlar, ağ adli analizi ve zararlı yazılım tespitine yönelik araştırmalar yapmaktadır. Ulusal ve uluslararası siber güvenlik tatbikatlarına katılan Bâkır EMRE, NATO'nun düzenlediği siber güvenlik tatbikatlarında ülkemizi temsilen yer almıştır.

EKLER

Ek 1:Tez Çalışması Kapsamında Yapılan Yayınlar

Emre B., Mantar H.A., (2013), "Dağıtık Zararlı Yazılım Toplama ve Analiz Modeli", First International Symposium On Innovative Technologies In Engineering And Science 7-9 Haziran 2013, Sakarya, TÜRKİYE.