AKADEMİK BAKIŞ DERGİSİ
Sayı: 52 Kasım – Aralık 2015
Uluslararası Hakemli Sosyal Bilimler E-Dergisi
ISSN:1694-528X İktisat ve Girişimcilik Üniversitesi, Türk Dünyası
Kırgız – Türk Sosyal Bilimler Enstitüsü, Celalabat – KIRGIZİSTAN
http://www.akademikbakis.org

TÜRKİYE'DE ZARARLI YAZILIMLARLA MÜCADELENİN UYGULAMA VE HUKUKİ BOYUTUNUN DEĞERLENDİRİLMESİ

İlker KARA*

Öz

Bilişim teknolojilerinin gelişmesiyle özellikle internetin sağladığı faydaları ve zararlarını farklı bakış açılarıyla ele almak gerekmektedir. Bilişim teknolojilerindeki buluşlar kullanıcıların hayatında pek çok şeyi kolaylaştırmıştır. Teknolojide yaşanan bu olumlu gelişmeler kötü niyetli insanlar içinde yeni fırsatlar doğurmuştur. Önceleri bir kazanç kapısı olarak görülmeyen kötü amaçlı yazılımlar, günden güne çok büyük bir ticarî sektör haline gelmiştir. Bu çalışmada; ülkemizde kötü amaçlı zararlı yazılımların yol açabileceği zararlarının önlenmesi amacıyla yapılan mücadele noktasını, bu zararlı yazılımların hukuki boyutu ve alınması gereken tedbirler hakkında görüş ve öneriler sunmaktadır.

Anahtar Sözcükler: Bilgi güvenliği, siber güvenlik, tehdit analizi, zararlı yazılım

ANALYZING THE LEGAL and PRACTICE ELEMENTS OF STRUGGLING WITH MALWARES IN TURKEY

Abstract

In parallel with developing computer technologies, the advantages and disadvantages of internet, especially, must be handled with a different point of view. Inventions in the field of computer technologies have simplified many things of internet users about life. Such positive developments in technology caused new opportunities for bad people, too. Malwares which were not accepted as an income source previously have become a growing business sector day by day. This study presents the methods of struggle to avoid any damages caused by malwares. It also presents offers and opinions about necessary precautions and handles the connection between malwares and law.

Key Word: Information security, cyber security, threat analysis, malicious software.

1. Giriş

Bilişim suçu veya bilgisayar suçu terimi bir bilgisayar ve bilgisayar ağı kullanılarak işlenen herhangi bir suçu ifade etmek için kullanılır (Moore, Richard, 2005, Kara, 2015). Bilgisayar, bir suçun işlenmesinde kullanılmış olabileceği gibi bir suçun hedefi de olabilir (David Mann And Mike Sutton, 2011, Kara, 2014). Bilişim sektörü büyüdükçe, bilişim suçları büyümeye devam etmekte, içinde bulunduğumuz dönemde ise zirve yapmış durumdadır (Timisi, 2003). İnternet'in herkes için güvenli ve dürüst bir yer olduğu düşünülmekte fakat

* Dr, Siber Suçlarla Mücadele Daire Başkanlığı, Ankara, Türkiye, Adli Bilişim Uzmanı.
Adres: Kızılırmak Mah. Anadolu Bulvarı 2185.Sk. No:14 06510 Söğütözü- Çankaya/ANKARA
Tel: 0312 286 93 00 Faks: 0312 286 92 06 Gazi Üniversitesi Fizik Bölümü *Teknikokullar 06560 Beşevler/ANKARA*

AKADEMİK BAKIŞ DERGİSİ
Sayı: 52 Kasım – Aralık 2015
Uluslararası Hakemli Sosyal Bilimler E-Dergisi
ISSN:1694-528X İktisat ve Girişimcilik Üniversitesi, Türk Dünyası
Kırgız – Türk Sosyal Bilimler Enstitüsü, Celalabat – KIRGIZİSTAN
http://www.akademikbakis.org

internet suçlularının ve bilgisayar korsanlarının sorun çıkarmaya hazırlandığını bilincinde olunmalıdır (Erbay, 1998).

Zararlı yazılımlar günümüz siber dünyasının en büyük tehditlerinden biridir. [Provos ve Holz, 2007]. Kötü amaçlı yazılım; bilgisayarlara zarar vermek üzere tasarlanmış olan her türlü yazılımlardır. Kötü amaçlı yazılımlar, bilgisayardan hassas bilgileri çalabilir, bilgisayarı adım adım yavaşlatabilir ya da e-posta hesaplarından sahte e-postalar bile gönderebilir. Günümüzde internet kullanan hemen herkes; virüs, solucan, truva atı, adware gibi pek çok zararlı yazılımın (malware) etkilerine maruz kalmaktadır [Sehgal, 2012]. Virüsler, solucan, adware vb. zararlı yazılımlar; reklam, sanal suçlar, bazen sadece ego tatmini gibi çeşitli çıkarlar için bilgisayar, tablet, akıllı cep telefonu vb. sisteminize zarar vermek için tasarlanırlar. Son zamanlarda, zararlı yazılımlar öyle bir duruma gelmiştir ki artık herhangi bir anti virüs programı kurulu olmayan bilgisayarlar internete bağlandıkları anda virüs bulaşmaktadır. Hatta anti virüs programı görünümünde sahte yazılımlar dahi türemiş durumadır. Çoğu zaman bu zararlı yazılımların hepsine virüs olarak nitelendirilmekte olsa da, aslında birbirlerinden farklıdırlar ve kimi zaman yazılımın türüne göre özel önlem veya işlem yapmak gereklidir.

Bir virüs (ing:spyware), bilgisayara girip dosya ya da verilere zarar verip, tahrif edebilir. Virüsler bilgisayarda verileri bozabilir hatta silebilirler. Ayrıca kendilerini çoğaltabilirler (gerçek virüsler gibi). Bilgisayar virüsleri pek çok zararlı yazılımdan çok daha tehlikelidir çünkü doğrudan dosyalara ve verilere zarar verirler.

Virüsler genel olarak imaj, ses, video dosya ekleri ile bilgisayara bulaşırlar [Zhuge ve diğerleri 2007]. Ayrıca internetten indirilen programların da içine gizlenmiş olabilirler. Virüsler kullanıcı tarafından izin vermedikçe yayılamazlar. Kullanılan programları, indirilen programları, mailler kontrol edilerek virüslerden korunulabilir. Bu nedenle orijinal anti virüs programı kullanılması, virüslerden korunmada etkili bir yöntemdir.

Davranışları ve bulaştıkları konuma göre çeşitli virüsler vardır [Sehgal, 2012], bu virüsler kısaca:

- **Dosya virüsü:** Bu tür virüsler .exe, .com, .bat gibi program dosyalarına bulaşırlar. Bu virüs hafızaya yerleştiği anda, o an hafızada yüklü olan tüm programlara yayılmaya çalışır.
- **Macro virüsü:** Word, excel, powerpoint ve diğer veri dosyalarına bulaşırlar ve bulaştıkları dosyanın onarımı çok güçtür.

- **MBR** (Master boot redord) **virüsü:** MBR virüsü bilgisayar hafızasına yerleşir ve kendini bir depolama aygıtının bölümleme tablolarının ya da işletim sistemi yükleme programlarının bulunduğu ilk sektörüne (Master boot redord) kopyalar. MBR virüsü normal dosyalar yerine depolama aygıtının belli bir bölümüne bulaşır. En kolay kaldırma yöntemi MBR alanının temizlenmesidir.

- **Boot sektör virüsü:** Boot sektör virüsü, hard disklerin boot sektörüne yerleşir. Ayrıca yapısı itibariyle bilgisayar hafızasına da yerleşebilir. Bilgisayar açılır açılmaz boot sektöründeki virüs hafızaya yerleşir. Bu tarz virüsleri temizlemesi oldukça zordur.

- **Multipartite (**çok bölümlü **) virüs:** Boot ve dosya/ program virüslerinin melezi olarak tanımlanabilir. Program dosyalarına bulaşır ve program açıldığında boot kayıtlarına

AKADEMİK BAKIŞ DERGİSİ
Sayı: 52 Kasım – Aralık 2015
Uluslararası Hakemli Sosyal Bilimler E-Dergisi
ISSN:1694-528X İktisat ve Girişimcilik Üniversitesi, Türk Dünyası
Kırgız – Türk Sosyal Bilimler Enstitüsü, Celalabat – KIRGIZİSTAN
http://www.akademikbakis.org

yerleşir. Bilgisayarın bir dahaki açılışında hafızaya yerleşir ve oradan diskteki diğer programlara da yayılır.

- **Polimorfik virüs:** Bu virüs tipi kodunu farklı biçimlerde şifreleyebilir, böylece her bulaşmada kendini farklı gösterebilir. Bu tarz virüsleri tespit etmesi oldukça güçtür.

- **Gizlilik virüsü:** Bu tarz virüsler tespit edilmemek için çeşitli yöntemler kullanır. Disk kafasını başka bir sektörü okuması için yönlendirebilir ya da dizin listesinde gösterilen dosya boyutunda oynama yapabilir. Örneğin Whale adlı bir virüs, bulaştığı dosyaya 9216 byte ekler ancak dizinde gösterilen dosya boyutundan 9216 çıkartır.

Truva atı (Trojan): Truva atı bir virüs değildir. Gerçek bir uygulama gibi gözüken zararlı bir program türüdür. Trojan kendini çoğaltmaz ama virüs kadar yıkıcı olabilir. Truva atı bilgisayarda güvenlik açığı oluşturur ki bu da zararlı programların, kişilerin sistemine girmesi için bir yol açar. Bu şekilde kullanıcıların kişisel bilgileri çalınabilir. Tarihteki Truva savaşındaki olduğu gibi zararsız zannedilen Truva atı, sisteme girer ve Grek askerlerinin ordunun girmesi için kale kapılarını içeriden açması gibi zararlı yazılımların, hackerların sisteme girmesi için bir güvenlik açığı oluştururlar. Virüslerde olduğu gibi farklı amaçlara hizmet eden Trojan türleri de bulunmaktadır:

- **Uzaktan kontrol yapan Truva atları:** En yaygın trojan türlerinden biridir. Kötü niyetli kişilerin asıl kullanıcı bilgisayarın başındayken sistemde kullanıcıdan çok daha fazlasını yapabilmelerine olanak sağlar. Bu tarz bir trojan kullanan biri bilgisayardaki her veriye ulaşabilir.
- **Şifre gönderen Truva atları:** Bu trojanlar sistemde, tarayıcı hafızasında kayıtlı olan şifreleri, kullanıcı fark etmeden belli bir adrese mail atar. Web sayfalarında, uygulamalarda girilen tüm kullanıcı adı ve şifreleri alabilir.
- **Keylogger:** Bu Truva atı tipi yapı olarak oldukça basittir. Klavyede basılan her tuşun kaydını tutar ve belli aralıklarla belli bir mail adresine gönderir. Saldırgan bu kayıtları inceleyip sık tekrar eden girdileri tespit ederek kullanıcı adı ve şifrelerine ulaşır.
- **Yıkıcı tip:** Bu tür Truva atının tek işlevi dosyalara zarar vermek ve silmektir. Otomatik olarak sistem dosyalarını silebilir. Saldırgan tarafından aktifleştirilebilir ya da belli bir gün saatte çalışacak şekilde ayarlanabilir.
- **DOS (Denial Of Services) Saldırısı Truva atı:** Dos saldırısı yapmakta kullanılan bu Truva Atı oldukça yaygındır. Ddos saldırısı, bir sisteme mümkün olduğu kadar çok kullanıcı ile aynı anda saldırılması ile gerçekleştirilir. Yaratılan aşırı trafik nedeniyle (çoğu zaman kurbanın bant genişliğinden daha fazla) sistemin internete erişimi durur. Çoğu büyük web sitesi bu şekilde çökertilmiştir. Saldırgan binlerce kullanıcının bilgisayarına bu Truva atlarından yerleştirir ve saldırı anında kullanıcıların makineleri kullanır.
- **E-posta bombası:** Dos Truva atının bir varyasyonu olan bu trojan türü mümkün olduğu kadar çok makineye bulaşır ve mail adreslerine rastgele konu, içeriklerle aynı anda çok sayıda saldırı gerçekleştirir.
- **Proxy/Wingate Truva atı:** Pek çok trojan kurbanın bilgisayarını bir proxy / wingate sunucusuna dönüştürür ki bu da bilgisayara tüm dünyanın ya da sadece saldırganın erişimine açık bir hale getirir.

AKADEMİK BAKIŞ DERGİSİ
Sayı: 52 Kasım – Aralık 2015
Uluslararası Hakemli Sosyal Bilimler E-Dergisi
ISSN:1694-528X İktisat ve Girişimcilik Üniversitesi, Türk Dünyası
Kırgız – Türk Sosyal Bilimler Enstitüsü, Celalabat – KIRGIZİSTAN
http://www.akademikbakis.org

- **FTP Truva atı:** En basit Truva atı olan bu tür artık demode olmuştur çünkü yapabildiği tek şey FTP transferi için kullanılan Port 21'i açıp herkesin ya da sadece saldırganın, kullanıcı bilgisayarına ulaşmasına olanak sağlamaktır. Daha yeni sürümleri parola korumalıdır yani bir tek saldırgan bilgisayara bağlanabilir.
- **Solucan (Worm):** Solucanlar yerel sürücüde ya da ağda kendini tekrar tekrar kopyalayan bir programdır. Tek amacı sürekli kendini kopyalamaktır. Herhangi bir dosya ya da veriye zarar vermez ancak sürekli kopyalama yaparak sistemi meşgul eder ve performansı etkiler. Virüslerin aksine bir programa bulaşmaya ihtiyacı yoktur. İşletim sistemlerindeki açıklardan yararlanarak yayılırlar.
- **Adware:** Genel olarak Adware, herhangi bir program çalışırken reklam açan yazılımdır. Adware internette gezerken otomatik olarak bilgisayarlara inebilir ve pop-up pencereleri ile görüntülenebilir. Kullanıcıları oldukça rahatsız eden Adware tipi uygulamalar çoğunlukla şirketlerce reklam amaçlı olarak kullanılırlar.
- **Casus Yazılım (Spyware):** Casus yazılım, kullanıcının izniyle veya izni dışında bilgisayara yüklenen ve kullanıcı, (örneğin webde gezdiği sayfalar, vb.) ya da bilgisayar hakkında bilgi toplayıp bunları uzaktaki bir kullanıcıya gönderen bir program türüdür. Ayrıca bilgisayara zararlı yazılımlar indirip yükleyebilir. Adware gibi çalışır ama çoğunlukla kullanıcı başka bir program yüklerken onun bilgisi dışında, gizli bir biçimde yüklenir.
- **Spam:** Aynı mesajdan çok sayıda göndererek bir mail adresini, forumu vb. boğmaya spam yapmak adı verilmektedir. Spamların çoğu reklam amaçlıdır ve kullanıcıların isteği dışında posta adreslerine gönderilmektedir.
- **Tracking Cookie:** Cookie yani çerezler internette gezinilen siteler vb. ile ilgili veri barındıran basit metin dosyalarıdır ve bilgisayarda çerez (ing:cookies) klasöründe bulunurlar. Pek çok site de ziyaretçileri hakkında bilgi almak için çerezleri kullanırlar. Örneğin bir sitedeki ankette her kullanıcının bir oy kullanma hakkı bulunmaktadır. Bu web sitesi çerez bilgilerini kontrol ederek kişinin ikinci defa oy kullanmasına engel olabilir. Ancak çerezleri kötü niyetli kişiler de kullanabilir. Tracking cookie adı verilen bu çerez türü bulaştığı bilgisayarda internette yapılan tüm işlemlerin, gezilen sayfaların kaydını tutar. Hackerlar bu şekilde kredi kartı ve banka hesap bilgilerine ulaşabilirler.

2. Kötü amaçlı yazılımlar nasıl yayılır?

Kötü amaçlı yazılımlar bilgisayarına bir dizi farklı yolla yerleşebilir. Aşağıda, bazı sık rastlanan örnekler verilmiştir:

- ❖ Fark edilmeyecek şekilde kötü amaçlı yazılım içeren ücretsiz bir yazılımı İnternet'ten indirme yoluyla,
- ❖ Fark edilmeyecek şekilde kötü amaçlı yazılımla bir arada sunulan yasal bir yazılımı indirme yoluyla,
- ❖ Kötü amaçlı yazılım bulaşmış bir web sitesini ziyaret etme yoluyla,
- ❖ Kötü amaçlı bir yazılımı indirme işlemini başlatmak üzere tasarlanmış sahte bir hata mesajını veya pop-up pencereyi tıklama yoluyla,
- ❖ Kötü amaçlı yazılım içeren bir e-posta ekini açma yoluyla.

AKADEMİK BAKIŞ DERGİSİ
Sayı: 52 Kasım – Aralık 2015
Uluslararası Hakemli Sosyal Bilimler E-Dergisi
ISSN:1694-528X İktisat ve Girişimcilik Üniversitesi, Türk Dünyası
Kırgız – Türk Sosyal Bilimler Enstitüsü, Celalabat – KIRGIZİSTAN
http://www.akademikbakis.org

Kötü amaçlı yazılımların yayılabileceği yollar çok çeşitlidir. Ancak bu durum, kullanıcıların kötü amaçlı yazılımları durdurmak konusunda çaresiz olunduğu anlamına gelmemektedir.

3. Kötü amaçlı yazılımlar nasıl önlenir?

Kullanıcıların zararlı yazılımlardan korunmanın en basit ve en etkili yolu güncel bir anti virüs programı kullanmaktır. Olası bir kötü amaçlı yazılıma maruz kalma ihtimaline karşı düzenli veri yedekleme yapılmalıdır. Sadece Cryptolocker'a (şifreli dosyalar) karşı değil her türlü saldırıya karşı alınabilecek en iyi önlem verilerin yedeklemesinin yapmasıdır [Provos ve Holz, 2007]. Anti-virüs, Anti-Spyware ve Anti-Malware programları[3] zero day olmayan zararlı yazılım varyasyonlarını listelerine eklemişlerdir ve tespit edebilmektedirler. Bu tür yazılımlar zararlı yazılımları Signature'ları (imzaları) üzerinden tespit ettiği için yeni bir zararlı yazılım varyasyonu ortaya çıktığında (zero day) tespit edilene kadar etkisiz kalabilmektedirler. En basit korunma yolu yöntem statik bazı değerleri kontrol etmektir.

- ✓ Bilgisayarın ve yazılımların daima güncel olması,
- ✓ Mümkün oldukça yönetici ayrıcalıkları olmayan bir hesap kullanılması,
- ✓ Bağlantıları tıklamadan veya bir şeyler indirmeden önce güvenli olduğunun bilinmesi,
- ✓ Bilinmeyen e-posta eklerini veya resimleri açılmaması,
- ✓ Yazılım indirmenizi isteyen pop-up pencerelere güvenilmemesi,
- ✓ Dosya paylaşımların sınırlandırılması,
- ✓ Anti-virüs yazılımları kullanılması gereklidir.

4. Zararlı Yazılım Analizini Engelleme Yöntemleri

Zararlı yazılımlar üretilirken analiz işlemini gerçekleştirilememesi için çeşitli yollara başvurmaktadırlar. Bu analiz engelleme yöntemlerinden bazıları şunlardır;

- ❖ Gizleme, Anti Disasemble,
- ❖ Şifreleme, Encoding Paketleme,
- ❖ Anti-VM, Anti-Sandbox, Görünmezlik,
- ❖ Hem yetkili hem yetkisiz moda çalışma,

yöntemleri ile zararlı yazılımlar kullanıcılar tarafından analizi engellenmeye çalışılmaktadır (http://dionaea.carnivore.it/, Erişim Tarihi:10.05.2015)

5. Kötü Amaçlı Yazılımların Adli İncelemeleri:

Kötü amaçlı yazılımların adli incelemeleri için 2008 yıllında, Mallicious Code (ing:kötü amaçlı kod) araştırma ve inceleme programı ile bu alanda kullanılmaya başlanmıştır(http://www.syngress.com/digital-forensic/Malware-Forensic/.Erişim Tarihi :22.05.2015). Symantec firmasının internet güvenliği tehdit raporunda 2011 yılında 286 milyondan fazla zararlı yazlım tespit edildiği açıklanmıştır. (http://www.symantec.com/connect/2011_Internet_Security_Threat_Report_Identifies_Risks _For_SMBs. Erişim Tarihi: 22.05.2015). Diğer anti-virüs satıcı firmalar F-Secure (ing: İnternet Güvenliği Programı), cep telefonu ve SCADA (Supervisory Control and Data Acquisition, ing: Kapsamlı ve Entegre bir Veri Tabanlı Kontrol ve Gözetleme Sistem) gibi

AKADEMİK BAKIŞ DERGİSİ
Sayı: 52 Kasım – Aralık 2015
Uluslararası Hakemli Sosyal Bilimler E-Dergisi
ISSN:1694-528X İktisat ve Girişimcilik Üniversitesi, Türk Dünyası
Kırgız – Türk Sosyal Bilimler Enstitüsü, Celalabat – KIRGIZİSTAN
http://www.akademikbakis.org

programların 2011 yıllında geliştirilmeye başlanmışlardır (http://www.f-secure.com/en_EMEA-Lab/new-info/threat-summaries/2011/2011_1.html, Erişim Tarihi: 22.05.2015).

6. Zararlı Yazılım Analiz Aşamaları

Zararlı yazılımlarla mücadelede ilk adım incelenen materyalde hangi tür zararlı yazılımın olduğunun tespitidir (http://www.virtualbox.org/, (Erişim Tarihi: 05.05.2015). Bu adım zararlı yazılımla mücadelenin en önemli aşamasıdır. Adli bilişim uzmanlarının nasıl bir zararlı yazılımla karşı karşıya olduğunun bilinmesi gereklidir. Türü tespit edilen zararlı yazılımın cihaz üzerinde etkili olduğu bölgeler karantina altına alınarak diğer sektörlere dağılması önlenir. Daha sonraki adımda; anti virüs programlarının yetersiz olması, zararlı yazılımın hangi güvenlik zafiyetlerini kullanıldığını öğrenmek, hedef bilgisayara neler yaptırdığını tespit etme, hedef bilgisayarda hangi dizinler altında eyleme geçtiğini saptama işlemleri adli bilişim alanındaki davaların çözümlenmesi için yapılmaktadır. Genel çerçevede ise zararlı yazılım analiz işlemleri dinamik ve statik olarak ikiye ayrılır. İster dinamik ister statik analizi olsun ilk adım her zaman zararlı yazılımın tespitidir.

6.1. Zararlı Yazılımın Tespit Aşaması

Güncel bir anti virüs programı ile periyodik olarak yapılan taramalar sonucunda zararlı yazılımın tespiti canlı sistemler için kolay olacaktır. Bu yöntem ile tespit edilemezse; zararlı yazılımın bulaştığı sistemin imajı (kopyası) alınarak uluslararası adli bilişim standartlarına uygun bir analiz programı ile alınan imaj içerisindeki tüm dosyaların özet (hash) değerleri hesaplatılır [Song ve diğerleri 2012], elde edilen hash list dosyası,“www.virustotal.com” sitesine yüklenerek sitede mevcut olan tüm anti virüs programı tarafından hash analizi karşılaştırması yapılarak tespit edilir.

AKADEMİK BAKIŞ DERGİSİ
Sayı: 52 Kasım – Aralık 2015
Uluslararası Hakemli Sosyal Bilimler E-Dergisi
ISSN:1694-528X İktisat ve Girişimcilik Üniversitesi, Türk Dünyası
Kırgız – Türk Sosyal Bilimler Enstitüsü, Celalabat – KIRGIZİSTAN
http://www.akademikbakis.org

Şekil 1:"Hata! Köprü başvurusu geçerli değil." karşılaştırması.

Adli incelemelerde iki farklı analiz yöntemi mevcuttur. Bunlar;

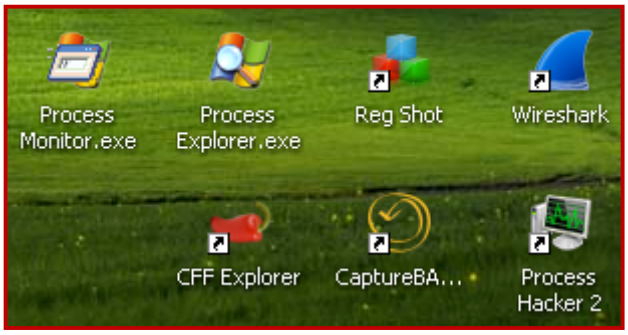
6.1.1. Dinamik Analiz

Zararlı yazılım, kullanılan mevcut anti virüs programı ile tespit edilememiş ise incelenen adli kopya içerisindeki tüm dosyaların MD5 hash değeri (özet doğrulama değeri) "www.virustotal.com" sitesine yüklenerek zararlı yazılım tespit edilir. Tespit edilen zararlı yazılım hakkında yine "www.virustotal.com" üzerinden ön bilgi elde etmek mümkündür. Tespit edilen zararlı yazılımın türüne göre dinamik analiz yöntemini kullanılır. Dinamik analiz yöntemi, statik analiz yöntemine göre daha hızlı ve kolaydır. Dinamik analiz yöntemi; "davranış analizi" ve "hafıza dökümü analizi" olarak ikiye ayrılır.

Davranış analizinde; tespiti yapılan zararlı yazılım, kullandığımız fiziksel bilgisayarın güvenliği için sanal bir işletim sistemi içerisinde çalıştırılıp, zararlı yazılımın davranışları incelenir. Davranış analizinde, sanal işletim sisteminin öncelikle temiz (zararlı yazılımın bulaşmadan önceki) görüntüsü alınır. Zararlı yazılım sanal sisteme bulaştırılır ve tekrar görüntüsü alınır. Bu iki sistem görüntüsü karşılaştırılarak zararlı yazılımın davranışları, oluşturduğu hareketler ve değişiklikler tespit edilir. Davranış analiz yöntemi için kullanılan programların seçimi son derece önemlidir. Zararlı yazılımın işletim sistemi üzerinde yaptığı

AKADEMİK BAKIŞ DERGİSİ
Sayı: 52 Kasım – Aralık 2015
Uluslararası Hakemli Sosyal Bilimler E-Dergisi
ISSN:1694-528X İktisat ve Girişimcilik Üniversitesi, Türk Dünyası
Kırgız – Türk Sosyal Bilimler Enstitüsü, Celalabat – KIRGIZİSTAN
http://www.akademikbakis.org

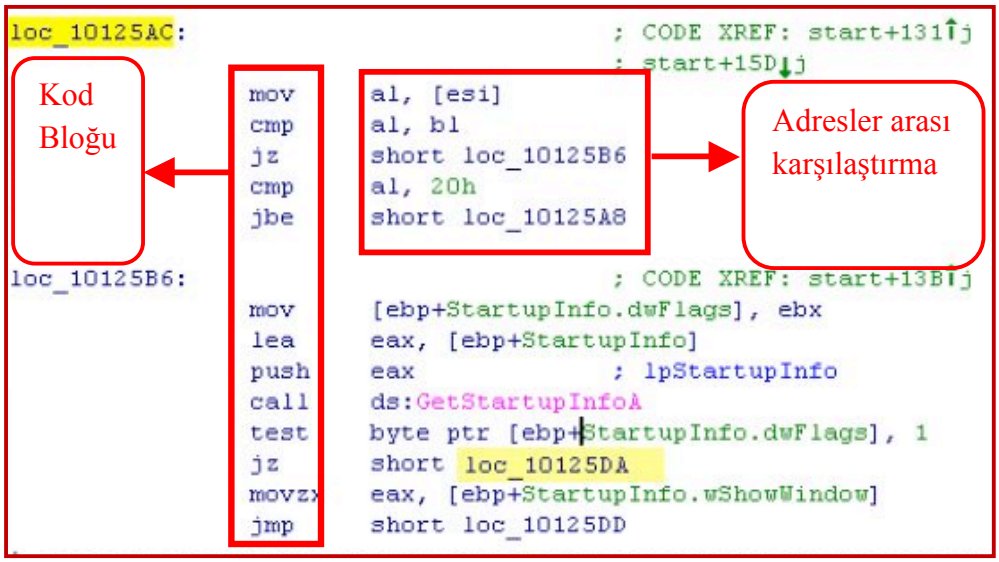
işlemlerin tümünü görmemizi sağlayacak araçların seçimi analiz sürecinin eksiksiz olmasını sağlayacaktır. Proccess Monitor, Proccess Hacker, Proccess Explorer, CaptureBAT, Regshot, WireShark, Network Monitor, FakeNet, Honeyd, netcat programları davranış analizinde kullanılan temel programlardandır.



Şekil 2: Temel araçlar kısa yol ekran görüntüsü.

6.1.2. Statik Analiz

Statik analizin temel hedefi, zararlı yazılım hareketlerinin incelenmesinden ziyade, zararlı yazılım hakkında tüm bilgiye sahip olmaktır. Statik analiz süreci; programlama, shellcode (kabuk kod) ve "assembly" dili bilmeyi gerektirir.



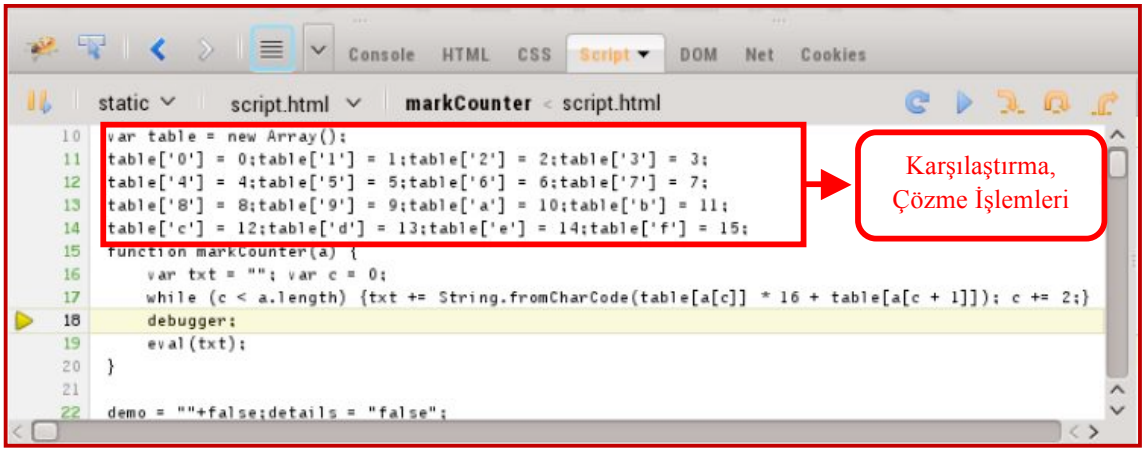
Şekil 3: Statik analiz işlem süreci.

Dinamik analizde olduğu gibi statik analizde de ilk iş zararlı yazılımın tespit edilerek "www.virüstotal.com" da zararlı yazılım hakkında ön bilgiye sahip olmaktır. Tespit edilen zararlı yazılımın, başlık bilgisi, imza bilgisi ve paketleyici bilgileri statik analizi oluşturmaktadır.

Statik analiz; "imza arama" ve "kod analizi" olarak ikiye ayrılır. Statik analiz dinamik analizden daha çok bilgi vermesine karşın çok daha zor bir analiz yöntemidir. Statik analizde zararlı yazılımın içinde mevcut string (ing: kelime katarı) ifadelerin anlamlandırılması ile

AKADEMİK BAKIŞ DERGİSİ
Sayı: 52 Kasım – Aralık 2015
Uluslararası Hakemli Sosyal Bilimler E-Dergisi
ISSN:1694-528X İktisat ve Girişimcilik Üniversitesi, Türk Dünyası
Kırgız – Türk Sosyal Bilimler Enstitüsü, Celalabat – KIRGIZİSTAN
http://www.akademikbakis.org

genel bilgiler elde edilir. Her zaman zararlı yazılımların string ifadelerine erişilebilmek mümkün olmayabilir. Bazı zararlı yazılımlar oluşturulma zamanında paketlendiği için öncelikle paketlemenin hangi program ile yapıldığı tespit edilir. Daha sonraki adımda "son imza" ve "kod analizi" işlemlerine geçilir. Statik analizde, string ifadelerin anlamlandırılması kadar karakter dizilerinin analizi de önemlidir. Statik analiz için ASCII (ing: American Standard Code for Information Interchange, Türkçe: Bilgi Değişimi İçin Amerikan Standart Kodlama Sistemi) karakter dizinini kodlamayı iyi bilmek faydalıdır. Statik analizde, Bintex, CFF Explorer programları en çok kullanılan programlardandır.

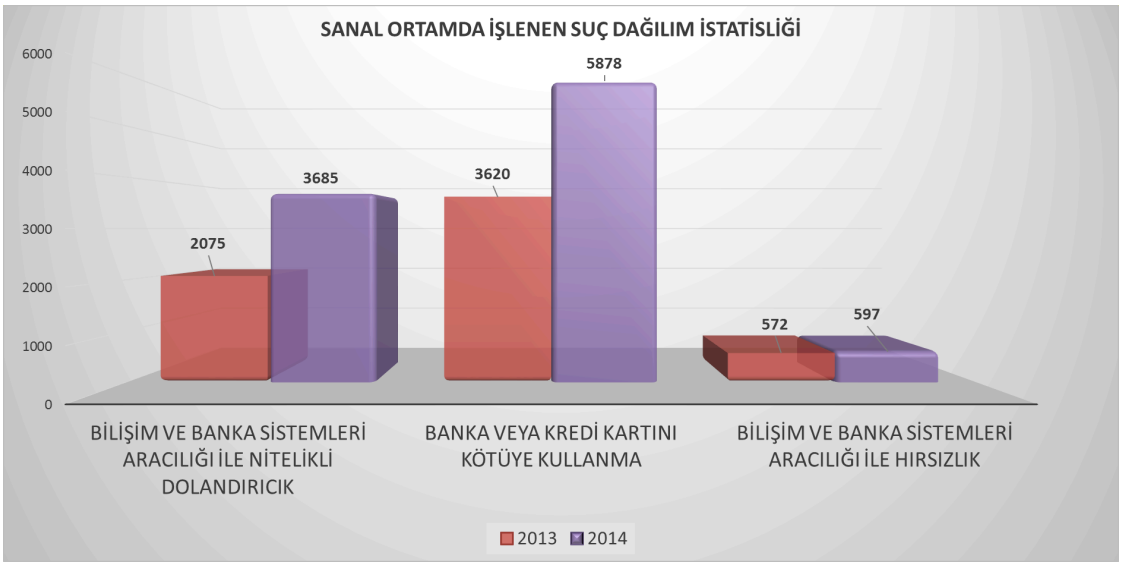


Şekil 4: Spesifik karıştırma çözme yöntemleri.

7. Ülkemizde Kötü Amaçlı Yazılımlarla Mücadelenin Hukuki Boyutu

Türkiye'de bu tür suçlar ile mücadele 2007 yılında çıkartılan 5651 sayılı "İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkında kanun" uyarınca yapılmakta, bu yolla erişimin engellenmesi, izlenmesi sağlanarak içerik sağlayıcı, yer sağlayıcı ve erişim sağlayıcıların yükümlülükleri düzenlenmektedir. Ayrıca Türk Ceza Kanununun 243-244-245'inci maddelerinde zararlı yazılım suçları ile ilgili yaptırımlar bulunmaktadır.

AKADEMİK BAKIŞ DERGİSİ
Sayı: 52 Kasım – Aralık 2015
Uluslararası Hakemli Sosyal Bilimler E-Dergisi
ISSN:1694-528X İktisat ve Girişimcilik Üniversitesi, Türk Dünyası
Kırgız – Türk Sosyal Bilimler Enstitüsü, Celalabat – KIRGIZİSTAN
http://www.akademikbakis.org



Şekil 5: Türkiye'de sanal ortamda işlenen suçların 2013-2014 yılları arasındaki değişim grafiği[1].

[1]2013-2014 yılları arası istatistikleri, Emniyet Genel Müdürlüğü, Siber Suçlarla Mücadele Şube Müdürlüğü, Ankara

Şekil 5'de Türkiye'de son iki yılda sanal ortamda işlenen suçların değerleri verilmiştir. İstatistiklerde "Banka veya Kredi Kartının Kötüye Kullanma" en çok işlenen suç olmuştur. 2013 yılında 2014 yılına sanal ortamda işlenen suçların toplam sayısında % 38,3 gibi çok yüksek boyutta artışı dikkat çekicidir. Burada "Bilişim ve Banka Sistemleri Aracılığı ile Nitelikli Dolandırıcılık" suçu % 43,6 ile en çok artan suç olmuştur

TCK'nın 243, 244 ve 245. maddeleriyle bilişim sistemlerine hukuk dışı girme ve orada kalma (m. 243/1), sistemin içeriğine veya sistemdeki verilere sisteme girilmesinden dolayı zarar verme (m. 243/3), bilişim sistemine veya burada bulunan verilere zarar verme (m. 244/1, 2), bilişim sistemi marifetiyle haksız yarar sağlama (m. 244/4), haksız olarak elde edilen başkasına ait banka veya kredi kartının kötüye kullanılması suretiyle yarar sağlama (m. 245/1) ve başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üretme, satma, devretme, satın alma ya da kabul etme (m. 245/2) ve sahte olarak üretilen veya üzerinde sahtecilik yapılan banka veya kredi kartıyla haksız menfaat elde etme (m. 245/3) suçları düzenlenmiştir.

TCK 243. maddesi hükmüyle bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girerek orada kalmaya devam etmeyi fiili suç olarak tanımlamıştır. Burada suçun oluşabilmesi için bilişim sisteme hukuka aykırı olarak girip orada kalmaya devam etmek gerekli görülmüştür. Yani suçun tamamlanması için bilişim sistemine girmeyi yeterli saymamış hukuka aykırı olarak girilen bilişim sisteminde kalmadığı sürece suç meydana gelmeyeceği gibi bir yoruma ulaşmak mümkündür. Bu tanıma göre; bu fiili gerçekleştiren fail cezalandırılmayacaktır.

Ayrıca hukuka aykırı olarak bilişim sistemlerine girmek ve suçun işlenmiş sayılması için; girilen sistemde en az ne kadar süreyle kalınması gerektiğine ilişkin bir tanımlama

bulunmamaktadır. Bu durum suçun işlenmiş halimi ya da teşebbüs hali mi olduğu uygulama ve değerlendirme yönünden tartışmaya açıktır (Kara, 2015:1-7).

Bu anlam kargaşasını son verebilmek için bilişim sistemine yetkisiz girişin dahi suç olarak tanımlaması gerekmektedir. Böylece suç işleme düşüncesine önlenmesi bakımından çok önemlidir.

8.Sonuç ve Değerlendirme:

Bilişim suçları günümüzde oldukça önemli bir suç haline gelmiştir. Bilişim suçları herkesin kullandığı telefon, bilgisayar, internet gibi teknolojileri kullanarak haksız bir şekilde kazanç elde etmek veya karşı tarafa zarar vermek olarak tanımlanmaktadır. Bu suç şekli özellikle, internetin akıl almaz bir şekilde yaygınlaştığı son zamanlarda kendisini iyice hissettirmeye başlamıştır. Bu yüzden, Türkiye dâhil olmak üzere pek çok ülke bu konu ile ilgili yasal düzenlemeler çalışmaları devam etmektedir.

Teknolojik suç işlemeyi amaçlayan kişiler genelde maddî kazanç ya da en azından kişisel tatmin için bu işlemi gerçekleştirdiklerinden ve genelde bilgisayar yazılımı konusunda oldukça bilgili olduklarından teknolojik önlemleri kırabilmektedir. Sanal ortamda işlen suçları sanal ortamda işlendiğinden genelde kişiler suç işlediklerini farketmez ya da kabullenmek istemezler.

Güvenlik açıkları, gelişen teknolojiyle birlikte tüm kamu kurumları ve özel şirketler tarafından çok ciddi para, zaman, kritik bilgi ve itibar gibi maddi ve manevi kayıplara sebep olmaktadır. Gelişen teknolojiyle birlikte siber saldırıların artması, kurumların ve şahısların daha güvenli sistemler kullanmasını zorunlu hale getirmektedir.

Burada dikkat edilmesi gereken önemli bir nokta yapılan bu hukuksal düzenlemelerin sadece teorikte düzenleme olarak kalmaması, başarılı bir şekilde uygulanması gereğidir. Bu şekilde her türlü suçta olduğu gibi bilişim suçlarında da azalma sağlanacaktır.

Değişen ve gelişen yenidünya düzeninde hukuksal düzenlemelerin gerçekleştirilmesi noktasında önerilebilecek diğer bir husus ise; uluslararası boyutta hukuksal gelişmelerin ve düzenlemelerin Türk Hukukunda takibinin iyi yapılması gerekliliğidir. Özellikle Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesinde de yer alan (Bu sözleşme, Türkiye'nin de yer aldığı taraf devletlerinin imzasıyla onaylanmıştır. Onay sonucu taraf devletler en kısa sürede iç hukukuna entegre çalışmalarını yapması gerekmektedir. Bilişim Suçlarının caydırıcı olması için ceza hukuki bağlamında da gerekli düzenlemeler ve detaylı suç kavramları ortaya konulmalıdır.

Kaynaklar

Sözlü Kaynaklar

ERBAY, Yusuf. (1998). "Kavram Olarak Küreselleşme", Yeni Türkiye, 21. Yüzyıl Özel Sayısı-I, Sayı 19.

David Mann And Mike Sutton (2011). "Netcrime". Bjc.oxfordjournals.org. Erişim tarihi: 2011-11-10.

KARA İlker, Sönmez Ümit, Kaya Gamze, Kaymakçıoğlu Özge. (2014). "5271 Sayılı Ceza Muhakemesi Kanununun 134 üncü Maddesinin Uygulama Yönünden Değerlendirilmesi", Kazancı Hakemli Hukuk Dergisi Bahçeşehir Üniversitesi, 73-81.

KARA İlker, Kaya Gamze. (2015). "Türkiye'de Bilişim Alanında İşlenen Suçların Uygulama Bakımından Hukuki Boyutunun Değerlendirilmesi", Kazancı Hakemli Hukuk Dergisi Bahçeşehir Üniversitesi, 154-168.

Moore, Richard. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.

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.

TİMİSİ, Nilifer. (2003). Yeni İletişim Teknolojileri ve Demokrasi, Dost Kitapevi, Ankara, 84.

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.

Elektronik Kaynaklar

http://www.syngress.com/digital-forensic/Malware-Forensic/ (Erişim Tarihi: 22.05.2015).

http://www.symantec.com/connect/2011_Internet_Security_Threat_Report_Identifies_Ri_sks_For_SMBs. (Erişim Tarihi: 22.05.2015).

http://www.f-secure.com/en_EMEA-Lab/new-info/threat-summaries/2011/2011_1.html.

http://dionaea.carnivore.it/, (Erişim Tarihi: 10.05.2013).
http://www.virtualbox.org/, (Erişim Tarihi: 05.05.2013).