
GAZİ ÜNİVERSİTESİ
Gazi
1926

WİNDOWS FONKSİYONLARI KULLANILARAK ÖZGÜN BİR CASUS YAZILIM TASARIMI VE ALINABİLECEK ÖNLEMLER

Mehmet DAMA

YÜKSEK LİSANS TEZİ

BİLİŞİM SİSTEMLERİ ANABİLİM DALI

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

KASIM 2014

Mehmet DAMA tarafından hazırlanan "WİNDOWS FONKSİYONLARI KULLANILARAK ÖZGÜN BİR CASUS YAZILIM TASARIMI VE ALINABİLECEK ÖNLEMLER" adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ / OY ÇOKLUĞU ile Gazi Üniversitesi Bilişim Enstitüsü Bilişim Sistemleri Anabilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Danışman: Doç. Dr. Bünyamin CİYLAN

Bilgisayar Mühendisliği, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum/onaylamıyorum …….

Başkan: Prof. Dr. Hadi GÖKÇEN

Endüstri Mühendisliği, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum/onaylamıyorum …….

Üye: Doç. Dr. Nurettin TOPALOĞLU

Bilgisayar Mühendisliği, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum/onaylamıyorum …….

Tez Savunma Tarihi: 20/11/2014

Jüri tarafından kabul edilen bu tezin Yüksek Lisans Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

……

Doç. Dr. Nurettin TOPALOĞLU

Bilişim Enstitüsü Müdürü

ETİK BEYAN

Gazi Üniversitesi Bilişim Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında**;**

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Mehmet DAMA

20.11.2014

WİNDOWS FONKSİYONLARI KULLANILARAK ÖZGÜN BİR CASUS YAZILIM TASARIMI VE ALINABİLECEK ÖNLEMLER

(Yüksek Lisans Tezi)

Mehmet DAMA

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

Kasım 2014

ÖZET

Siber Dünya'da bilgi güvenliğini tehdit eden önemli zararlı yazılım türlerinden birisi de casus yazılımlardır. Kullanıcıların bilgilerini toplayarak üçüncü taraflara ulaştıran casus yazılımlar siber suç, siber casusluk ve siber savaş gibi faaliyetlerde kullanılabilmektedirler. Koruyucu yazılımlar, casus yazılımlara karşı bir önlem olarak kullanılmaktadırlar. Ancak özgün olarak geliştirilmiş yani daha önce herhangi bir koruyucu yazılıma ait imza veritabanında imzası oluşturulamamış casus yazılımların, koruyucu yazılımlar tarafından zararlı olarak değerlendirilmeme riski bulunmaktadır. Bu problemi ortaya koymak ve çözüm sunmak için donanıma ve Windows işletim sistemi versiyonuna bağımlılığı en aza indiren, hedef kitlesi genişletilmiş, özgün yöntemlerle örnek bir casus yazılım geliştirilmiştir. Casus yazılım tasarımında, bilgilerin toplanabilmesi için üçüncü parti sınıf ve kütüphaneler yerine Windows işletim sistemlerinde yer alan fonksiyonları kullanan özgün sınıflar geliştirilmiştir. Özellikle tuş kaydedici özelliğinin (KEYLOGGER) kazandırılması için yaygın olarak kullanılan Hook yöntemi yerine GetAsyncKeyState fonksiyonunun kullanıldığı sınıf geliştirilmiştir. Geliştirilen casus yazılım aracılığıyla, basılan tuş bilgileri, IP bilgileri, açık port bilgileri, açık pencere bilgileri gibi bilgiler ile ekran görüntüleri ve ortam ses kayıtlarının kullanıcının bilgisi dışında üçüncü şahıslar tarafından nasıl edinildiği, bu yazılıma ait geliştirme süreci ve geliştirme motivasyonlarının neler olduğu ortaya konmuştur. Microsoft Visual Studio geliştirme ortamında C# dilinde geliştirilen casus yazılım, Windows tabanlı işletim sistemleri üzerinde yaygın olarak kullanılan 11 adet koruyucu yazılım (antivirüs, antispyware, firewall) ile test edilmiş olup sadece dört adet koruyucu yazılımın geliştirilen casus yazılımı tespit edebildiği, bir yazılımın ise sadece internet erişimini engellediği görülmüştür. Bu testlerin yanında casus yazılım, çevrimiçi virüs tarama sitesi üzerinde de taratılmış olup detaylı sonuçlar paylaşılmıştır. Casus yazılım geliştirme sürecinde edinilen tecrübeler ve gerçekleştirilen testler ile ulaşılan sonuçlar ışığında casus yazılımlardan korunmak için koruyucu yazılım geliştiricileri, kurumsal kullanıcılar ve son kullanıcılara yönelik öneriler sunulmuştur.

Bilim Kodu : 902.1.014

Anahtar Kelime : Bilgi güvenliği,Casus Yazılım, Antivirüs, Antispyware, Tuş Kaydedici

Sayfa Adedi : 94

Danışman : Doç. Dr. Bünyamin CİYLAN

AN ORIGINAL SPYWARE DESIGN BY USING WINDOWS FUNCTIONS AND PREVENTIVE MEASURES

(M. Sc. Thesis)

Mehmet DAMA

GAZİ UNIVERSITY

INFORMATICS INSTITUTE

November 2014

ABSTRACT

Spyware is one of the important dangerous malware type threats to Information Security in the cyber world. The spywares which are used to collect user data and send to third parties can be used in cyber spying, cyber war and cyber crime activities. Anti-malware (antispyware, antivirus, firewall) software are being used as a preventive measure to spyware. But, originally developed spyware which are not identified in the antivirus software signature database may not be detected by anti-malware software. To present that problem and solution, a spyware was developed using original methods. Having a large target audience, this spyware has minimum dependency on hardware and Windows operating system. Original classes using Windows operating system functions were developed instead of third party classes and libraries for collecting information. In particular, a class using GetAsyncKeyState function was developed to implement KEYLOGGER functionality, instead of using common Hook method. The methods for gathering keystrokes (KEYLOGGER) , IP address, open and established network port and open windows information, screenshots and environment voices without the knowledge of the user are presented and spyware development stage and the motivation factors are set forth. The spyware coded with Microsoft Visual Studio C# language is tested with 11 prevalent anti-malware software commonly used in Windows operating systems. It is seen that only four of these software products could detect this spyware and one can block Internet connection. Spyware is also scanned in online virus scanning website and detailed results have been presented. Some advices are presented for anti-malware developers, IT managers and end users by the view from spyware development experiences and test results.

Science Code : 902.1.014

Key Words : Information security, Spyware, Antivirus, Antispyware, Keylogger

Page Number : 94

Supervisor : Assoc. Prof. Bünyamin CİYLAN

TEŞEKKÜR

Çalışmalarım boyunca değerli yardım ve katkılarıyla beni yönlendiren Doç. Dr. Bünyamin CİYLAN'a, manevi destekleriyle beni hiçbir zaman yalnız bırakmayan çok değerli eşim ve aileme teşekkürü bir borç bilirim.

İÇİNDEKİLER

Sayfa

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

RESİMLERİN LİSTESİ

Resim **Sayfa**

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış bazı kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklamalar
BTK	Bilgi Teknolojileri Kurumu
DOS	Hizmet Engelleme Saldırısı (Denial of Service Attack)
DDOS	Dağıtık Hizmet Engelleme Saldırısı (Distributed Denial of Service Attack)
EPDK	Enerji Piyasası Düzenleme Kurumu
FBI	Federal Soruşturma Bürosu (Federal Bureau of Investigation)
IT	Bilişim Teknolojileri (Information Technology)
JVM	Java Sanal Makinesi (Java Virtual Machine)
RTÜK	Radyo ve Televizyon Üst Kurulu
URL	Evrensel Adres Gösterici (Uniform Resource Locator)

1. GİRİŞ

Teknoloji kullanımı yaygınlaştıkça, teknolojinin önemli faydalarıyla beraber çok önemli zararları da toplumsal yaşamı ve uluslararası ilişkileri etkilemektedir. Gerçek dünyaya ek olarak yaygın elektronik alt yapı kullanımıyla meydana gelen siber dünya; hem fiziki dünyada olan somut olaylardan etkilenmekte hem de siber alanda düzenlenen saldırılar yüzünden gerçek dünyayı etkilemektedir [1]. Bu çalışmada bahsedilen bazı kavramların tanımları aşağıda sunulmuştur.

"Siber Suçlar", bir bilgisayarın araç olarak kullanılması sonucu geleneksel suçlar olan dolandırıcılık ve hırsızlık gibi suçlar ile yeni tür suçlar olarak tanımlanabilecek servislerin çalışmaz hale getirilmesi (Denial of Service Attacks), verilere zarar verme (zararlı yazılımlar), kimlik bilgisi hırsızlığı, telif hakkı ihlallerinin gerçekleştirilmesi olarak tanımlanabilir [2-3].

"Siber Saldırı" askeri literatürde, devletlerin ulusal hukuk metinlerinde ve uluslararası hukuk kaynaklarında açıkça tanımlanmış ve üzerinde mutlak bir uzlaşı sağlanmış bir kavram değildir. Bu nedenle söz konusu ifadenin farklı tanımları bulunmaktadır. Literatürdeki en kapsamlı tanımlardan biri olarak değerlendirilen ABD Ulusal Araştırma Konseyi Bilgisayar Bilimler ve Telekomünikasyon Kurulu (Computer Science and Telecommunications Board of the National Research Council) Baş Bilim Uzmanı Herbert Lin'in açıklamasına göre, siber saldırı, düşmanın bilgisayar sistemlerini ve ağlarını veya bu sistem ve ağlarda bulunan ya da bunlardan geçen bilgiyi ve/veya programları değiştirmek, bozmak, yanıltmak, geriletmek veya ortadan kaldırmak için yapılan kasıtlı hareket ve harekatlardır [4-5].

Siber saldırı tanımında olduğu gibi siber savaş tanımının da herkesçe benimsenen bir tanımı yoktur. Siber savaş, "bilgi teknolojilerini korumak için siber alanda savunma yapmak veya saldırmak ya da rakip saldırıları engellemek için yapılan faaliyetlerin tümü olarak tanımlanmaktadır [1].

Siber casusluk (İng. Cyber Espionage) hedef bilgisayarın yapılandırmasını veya sistem savunmasını test etmeyi amaçlayan faaliyetler olabileceği gibi yetkisiz olarak dosyaların görüntülenmesi, kopyalanması, bilgisayar üzerinde gerçekleştirilen işlemlerin takip edilmesi şeklinde de tanımlanabilir [6]. 2010 yılında Çin siber savaşçıları tarafından Google firmasının entelektüel mülkiyetlerini çalmayı hedefleyen girişimlerin ortaya çıkmış

olması siber casusluğun sadece teorik bir kavram olmadığının kanıtı niteliğindedir [7]. Siber casusluk ile ilgili yaşanan bir diğer olay ise Moonlight Maze olayıdır. Bu olayda Rus hackerlar bir yıl boyunca Savunma bakanlığı bilgisayarlarına nüfuz ederek büyük miktarda kritik verileri çalmışlardır. Pentagon ve Federal Bureau of Investigation (FBI) yetkilileri bu olayı, Savunma Bakanlığı'nın yanı sıra Enerji Bakanlığı, NASA, askeri müteahhitler ve ordu ile bağlantılı sivil üniversiteleri de hedef alan, Rusya devletinin desteklediği ABD teknolojisini elde etme istihbarat kampanyası olarak tanımlamış ve bu olayda Savunma Bakanlığı ağlarında herhangi bir zarar ya da imha raporlanmadığı belirtilmektedir [8]. Bilişim teknolojileri öncesinde casusluk faaliyetlerinin fiziki koruma ile engellenebiliyor olmasına rağmen günümüzde bir zararlı yazılım aracılığıyla dünyanın herhangi bir noktasından casusluk faaliyetleri yürütülebilmektedir.

Siber dünyada gerçekleştirilen siber suçlar, siber casusluk ve siber savaşların hedefinde kişiler, şirketler, siyasi/ideolojik kurum ve kuruluşlar ile devletler olabilir. Yukarıda ifade edilen faaliyetlerde kullanılabilecek önemli zararlı yazılım araçlarından birisi de casus yazılımlardır. Casus yazılımlar arka planda çalışarak istenilen verileri sistemden edinebilirler [9]. Ne tür bilgilerin elde edileceği casus yazılımı oluşturan kişi/kurum tarafından belirlenir, bu bilgiler kredi kartı numaraları, kullanıcı adı-şifreleri, girilen web sayfa bilgileri, kişisel veya kurumsal yazışmalar, gizli dosyalar, bilgisayar kamerasına ait görüntü, ortamdaki konuşmalar (mikrofon aracılığıyla) gibi çeşitli bilgiler olabilirler. Bu çalışmada casus yazılımların oluşturdukları riskler bazı örnekleri ile birlikte detaylıca sunulmuştur.

Ülkemizde casus yazılımlar üzerinde yapılan çalışmalar genel olarak teorik veya hukuki çerçevede kalmakta olup bu yazılımların nasıl geliştirildikleri ve çalıştıkları hakkında bilgiler ortaya koyan teknik çalışma sayısı daha azdır [1, 3, 8, 10]. Bu çalışmada özgün bir casus yazılım geliştirme süreci ele alınmış olup casus yazılım geliştiren kişilerin, grupların, organizasyonların ve devletlerin bu yazılımları hangi motivasyonlarla geliştirmiş olabilecekleri de ele alınmıştır.

Koruyucu yazılımlar (antivirus/antispyware/firewall) casus yazılımlara karşı bir önlem olarak kullanılmaktadırlar. Ancak sanıldığının aksine özellikle özgün olarak geliştirilmiş yani daha önce herhangi bir koruyucu yazılıma ait imza veritabanında imzası oluşturulamamış casus yazılımların, koruyucu yazılımlar tarafından zararlı olarak değerlendirilememe riski bulunmaktadır [11-12]. Bu problemi ortaya koymak ve çözüm sunabilmek için çalışma kapsamında, donanım ve Windows işletim sistemi versiyon

bağımlılığını en aza indiren, hedef kitlesi genişletilmiş, özgün yöntemlerle bir casus yazılım geliştirilmiştir. Çözüme yönelik koruyucu yazılım geliştiricileri tarafından casus yazılımın kullandığı yöntemlerin nasıl engellenebileceği hususunda öneriler Bölüm 4 ve Bölüm 5'te sunulmuştur. Geliştirilen yazılım yaygın şekilde kullanılan işletim sistemleri üzerinde ve yaygın olarak kullanılan koruyucu yazılımlar ile test edilmiştir. Söz konusu testler, sanal makineler üzerinde kurulu işletim sistemlerinde çeşitli koruyucu yazılımların ayrı ayrı test edilerek casus yazılımın tespit edilebilirliğine yönelik bazı soruların cevaplarının aranması şeklinde gerçekleştirilmiştir. Bu kapsamda ilgili sorular ile cevaplarının oluşturulduğu çizelgeler çalışma sonucunda sunulmuştur.

Kullanıcıların kullanmakta olduğu koruyucu yazılımların sayısının fazla olması ve geliştirilen casus yazılımın koruyucu yazılımlar ile test edilmesinin süre alması nedeniyle, test edilen koruyucu yazılım sayısının sınırlandırılması gerekmiştir. Testler 11 adet koruyucu yazılım ile gerçekleştirilmiştir. Bununla birlikte farklı işletim sistemleri üzerinde de testlerin gerçekleştirilmesi hedeflenmiş olmasına rağmen test için kullanılabilecek bilgisayar sayısının bir tane ile sınırlı olması nedeniyle "Sanal Makine" yazılımları kullanılmış ve diğer işletim sistemleri sanal makinalar üzerinde test edilmiştir.

Çalışma sonucunda elde edinilen bulgular ışığında casus yazılımların oluşturdukları risklerin nasıl azaltılabileceğine ilişkin değerlendirmeler sunulmuştur. Bu değerlendirmeler koruyucu yazılım geliştiriciler başta olmak üzere kurumsal sistem yöneticileri ve son kullanıcılara yönelik hazırlanmış olup zararlı yazılımlar ile ilgili ilerde yapılacak çalışmalara ışık tutabilecek öneriler de sunulmuştur. Ayrıca geliştirilmesine milli imkânlarla katkı sağlanmış olan bir işletim sistemine olan ihtiyaç söz konusu öneriler kapsamında ele alınmıştır.

2. SİBER SUÇLAR

Yeni bir kavram olarak ortaya çıkan bilişim, Türk Dil Kurumu tarafından insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi olarak tanımlanmaktadır.

Suç kavramı ise, toplumsal düzen içerisinde oluşturulmuş kanunların yasakladığı ve yapıldığında cezai bir müeyyidesinin olduğu her türden davranış olarak tarif edilebilir. Günümüz dünyasında ise özellikle kişisel bilgisayarlar ve mobil iletişim cihazlarının gelişmesi ve sayılarındaki artış ile orantılı olarak karmaşıklaşan bir iletişim ağı sistemi bulunmaktadır. İnsan hayatını kolaylaştıran yönlerine paralel olarak, bu iletişim ağı üzerinde artan bir suç potansiyelinden de bahsetmek mümkündür [10].

Yukarıdaki bilişim ve suç tanımları dikkate alındığında bilişim suçu kavramı daha iyi anlaşılabilir olmakla birlikte, Avrupa Ekonomik Topluluğu Uzmanlar Komisyonunun Paris toplantısında (Mayıs 1983) ortaya koyduğu bilişim suçu tanımı, genel geçerliliği en kabul edilebilir tanım olarak görünmektedir. Bu tanımlamada bilişim suçları, sistem içinde bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan her türlü işlemi ahlaki ve kanuni olmayan, bununla birlikte yetki aşımı veya yetki tecavüzü ile gerçekleştirilen davranış olarak tarif edilmektedir [10, 13].

Bilişim suçu ise pek çok dilde farklı isimler altında ifade edilebilmektedir. Bilgisayar destekli suçlar (İng. Computerassisted Crimes), bilgisayara karşı işlenen suçlar (İng. Crimesagainst Computer), bilgisayar bağlantılı suçlar (İng. Computerrelated Crimes), bilgisayar ağları ile ilgili suçlar (İng. Computer Networks related Crimes), bilgisayar suçları (İng. Computer Crimes – Computer kriminalitat – la FraudeInformatique), bilgi teknolojileri suçları (Information Technologies – IT Crimes), siber suçlar (Cyber Crimes), ağ suçları (Crimes of Network) ve bilişim suçluluğu (la Criminalita Informatica) verilebilecek pek çok örnekten birkaçıdır [14].

Siber suçların işlenmesinde kullanılan saldırı yöntemleri ve zararlı yazılım türleri aşağıda ele alınmıştır.

2.1. Saldırı Yöntemleri

Siber saldırı, bilgisayar ve ağ sistemlerine ait güvenliği (erişilebilirlik, tutarlılık ve gizlilik vb.) riske sokan bir dizi bilgisayar aktivitesidir. Hayatımızın savunma, bankacılık, telekomünikasyon, ulaşım, enerji gibi birçok kritik alanında bilgisayar ve ağ sistemlerine olan güven arttıkça siber saldırılar toplum için önemli riskler oluşturmaya başlamıştır [15]. Bazı siber saldırı yöntemleri aşağıda sunulmuştur.

2.1.1. Bilgisayar korsanlığı

Bilgisayar korsanlığı yetkisiz erişim sağlamak amacıyla bir sistemin güvenlik tedbirlerini etkisiz hale getirmeye çalışmaktır. Bilgisayar korsanlığı maksadıyla kullanılan pek çok yöntem bulunmaktadır. Bu yöntemlerin başında işletim sistemlerinde, yaygın olarak kullanılan uygulama programlarında veya ağ bağlantılarında açıklar bularak bu açıklardan istifade edilmesi gelmektedir. Dolayısıyla güncellenmemiş işletim sistemi veya uygulama programlarının üzerinde çalışan sistemlerin daima risk altında oldukları değerlendirilebilir. Bununla birlikte "Zero-Day-Exploit" olarak adlandırılan, üretici firmanın da varlığından haberdar olmadığı yeni bir açığın tespit edilerek kullanılması ihtimali de her zaman söz konusudur [3].

Bilgisayar korsanlığı aktivitesi sonucunda sistem erişilmez hale getirilebilir, sistemde bulunan bilgiler çalınabilir, değiştirilebilir veya tahrip edilebilir. Daha da kötüsü sisteme sızan kişi alanında yeterince yetkin ise varlığından kimseyi haberdar etmeden veriler üzerinde değişiklikler yapıp yine fark edilmeden sistemi terk edebilir. Böyle bir durumda bilgi güvenliği tanımında da yer alan sistemde barındırılan verinin bütünlüğü hakkında kimsenin aklına bir şüphe gelmeyecek ve söz konusu işletme bütünlüğü bozulmuş veriyle günlük işlemlerine devam edecektir [3].

2.1.2. Hizmeti engelleme

Bilişim sistemlerinin erişilebilirliğine yönelik düzenlenen en meşhur saldırı türü "Denial of Service (DOS) saldırısı" olarak bilinen hizmeti engelleme saldırılarıdır. DOS saldırılarında kullanılan pek çok yöntem bulunmaktadır. Bu yöntemler ile hedeflenen, hizmeti engellenecek sunucu bilgisayarla çok sayıda sahte bağlantı kurmak suretiyle

sunucuya aşırı iş yükü yüklemek ve gerçekten bağlantı kurmaya çalışan kullanıcılara cevap veremez hale gelinmesini sağlamaktır. Günümüzde DOS saldırıları genellikle birden fazla hatta bazen binlerce bilgisayar kullanılarak yapılmaktadır. Bu tür saldırılar Dağıtık Hizmeti Engelleme Saldırıları anlamına gelen Distributed DOS (DDOS) saldırıları olarak isimlendirilmektedir. Bu tür saldırıların soruşturulması da kolay olmamaktadır çünkü DDOS saldırıları çoğunlukla bu iş için yazılmış botnet (bot networks) adı verilen zararlı yazılımlar vasıtasıyla gerçekleştirilmektedir. Botnet isimli yazılımlar kullanıcıların farkında olmadan bilgisayarlarına yüklenmekte ve botnet yöneticisinden talimat gelene kadar faaliyette bulunmamaktadır. Botnetler genellikle DDOS ataklarında kullanılmakta, yöneticiden talimat geldiğinde yazılımın bulaştığı bilgisayarlar saldırının hedefinde bulunan internet adresleriyle bağlantı kurarak sunucuyu meşgul etmektedirler [3, 16].

2.1.3. Sosyal mühendislik saldırıları

Siber saldırı tekniklerinden bir diğeri de sosyal mühendislik saldırılarıdır. Sosyal mühendislik saldırıları, insan doğasından istifade etmek üzere değişik aldatmacalar kullanarak hedef sistem hakkında bilgi edinmek, veri ele geçirmek veya sisteme girmektir. Oltalama (İng. Fishing) ve istenmeyen e-posta (İng. Spam) göndermek bir nevi sosyal mühendislik saldırısıdır çünkü kullanıcıları kandırarak belli eylemleri yaptırmayı hedeflemektedirler. Bunun yanında saldırganın hedeflenen kurum çalışanlarına telefon açarak kendisini bilgi işlem personeli olarak tanıtması suretiyle çeşitli bahanelerle sisteme bağlanırken kullandığı kullanıcı adı ve şifresini öğrenmesi de bir sosyal mühendislik saldırısıdır. Sosyal mühendislik saldırıları kişisel beceriye dayanan, basit ve etkili saldırılardır [3, 17].

2.1.4. Gizli dinleme

Bir ağ veya kanal üzerinden iletilen verinin, kötü niyetli üçüncü kişiler tarafından araya girilerek alınması; hatta kaynaktan hedefe giden verinin arada elde edilip, değiştirilerek hedefe gönderilmesi bile mümkündür. İngilizce “eavesdropping” (saçak damlası) olarak adlandırılan bu saldırının, sanıldığının aksine çok farklı uygulama alanı bulunmaktadır. Hiç bir bilgisayarla etkileşimi olmayan tek başına çalışan bir bilgisayar bile, mikroçip, ekran veya yazıcı gibi elektronik parçalarından yayılan elektrik veya elektromanyetik yayılım takip edilerek gizlice dinlenebilir. Bu cihazların bu tür dinlemelere olanak vermemesi için,

Amerikan hükümeti 1950'li yılların ortasından başlayarak TEMPEST adında bir standart geliştirmiştir [18].

Paket koklama (İng. packet sniffing) olarak da adlandırılan bu gizli dinleme saldırısı sistem yöneticileri tarafından kullanılan yönetimsel yazılımlar ile gerçekleştirilebileceği gibi kötü niyetli olarak geliştirilmiş yazılımlarla da gerçekleştirilebilir [19].

2.1.5. Doğrudan erişim saldırıları

Bir bilgisayar sistemine doğrudan fiziksel erişime sahip olan bir kişinin yaptığı saldırılar bu grupta toplanmaktadır. Bilgisayara fiziksel erişim sağlayan kişi, işletim sistemlerinde kendisi için bir kullanıcı belirlemek gibi ileride kullanılabilecek çeşitli değişiklikler yapabilir; yazılım solucanları, klavye dinleme sistemleri ve gizli dinleme cihazlarını sisteme kurabilir. Doğrudan erişime sahip olan saldırgan ayrıca, CD-ROM, DVD-ROM, disket gibi yedekleme ünitelerini; bellek kartları, sayısal kameralar, sayısal ses sistemleri, cep telefonu ve kablosuz/kızılötesi bağlantılı cihazları kullanarak, büyük miktarda bilgiyi kendi tarafına kopyalayabilir. Bu açıdan, bir bilgisayar sistemi üçüncü şahısların kullanımına kısa süreliğine bile olsa bırakılmamalıdır [18].

2.1.6. Kriptografik saldırılar

Şifrelenmiş bilgilerin şifresini kırmak veya çözmek için yapılan saldırılardır. Bu saldırılar, kriptoanaliz yöntemleri ile gerçekleştirilmektedir. Bunlar arasında kaba kuvvet saldırısı (brute force attack), sözlük saldırısı (dictionary attack), ortadaki adam saldırısı (man in the middle attack), sade şifreli metin (chipertext only), bilinen düz metin (known plaintext), seçilen düz metin veya şifreli metin (chosen plaintext, chipertext), uyarlanır seçili düz metin (adaptive chosen plaintext) ve ilişkili anahtar (related key attack) saldırılarını saymak mümkündür [20].

2.2. Zararlı Yazılım Türleri

Zararlı yazılım (İng. Malicious software, malware) yetkisiz olarak yüklenen ve bilgisayar sistemlerine zarar veren yazılımların genel adıdır [21].

Bazı zararlı yazılım türlerine ait sınıflandırma aşağıda sunulmuştur.

2.2.1. Bilgisayar virüsleri

Organizmalardaki hücrelere bulaşan biyolojik virüslerden esinlenerek adlandırılan bilgisayar virüsleri, kendi kopyalarını çalıştırabilen, diğer kodlara veya belgelere kendilerini yerleştirerek yayılan ve kendi kendine çoğalan yazılımlardır. Ekranda rahatsız edici, çalışmaya kısa süreliğine de olsa mani olan mesajlar göstermek gibi zararsız sayılabilecek türlerinin de bulunmasına karşın; çoğu virüs programlarının, önemli dosyaları silmek veya konak (İng. host) sistemini tamamen çalışmaz hale getirmek gibi yıkıcı etkileri bulunmaktadır. Bir bilgisayar solucanın bir parçası olarak ağ üzerinden yayılabilir olmalarına rağmen; tanım olarak virüsler, yayılmak için ağ kaynaklarını kullanmazlar. Bunun yerine disket, CD veya DVD gibi ortamlarla veya e-posta eklentileri ile hedef sistemlere bulaşırlar [18].

2.2.2. Bilgisayar solucanları (İng. Worms)

Bilgisayar virüslerine benzer yapıda olan solucanlar, virüsler gibi bir başka çalıştırılabilir programa kendisini iliştirmez veya bu programın parçası olmaz. Solucanlar, yayılmak için başka bir programa ihtiyaç duymayan, kendi kendini çoğaltan bir yapıya sahiptirler. Bir solucanın yayılmasında kullandığı en yaygın yöntemler arasında e-posta, FTP ve HTTP gibi İnternet hizmetleri bulunmaktadır. Solucanlar yayılmak için, hedef sistemdeki korunmasızlıklardan faydalanabilir ve/veya sosyal mühendislik yöntemlerini kullanabilirler. Solucanlar, başka dosyaları değiştirmezler, fakat etkin bir şekilde bellekte dururlar ve kendilerini kopyalarlar. Solucanlar otomatik olarak gerçekleştirilen ve genellikle kullanıcılar tarafından farkedilemeyen işletim sistemi yapılarını kullanırlar. Solucanların kontrol dışı çoğalmaları, sistem kaynaklarını aşırı kullandığında veya çalışmakta olan diğer görevleri yavaşlattığında veya bu görevlerin sonlanmalarına neden olduğunda farkına varılabilir [18].

2.2.3. Truva atları

Zararlı yazılım türlerinden bir diğeri olan Truva atları ismini bir efsaneden almıştır. Söz konusu efsane, hediye olarak gönderilmiş bir tahta atın içine saklanan düşman askerleri tarafından şehrin ele geçirilmesini konu edinmiştir.

Truva atları kullanıcı bilgisi ve yetkisi dışında çalışan zararlı yazılımlardır. Truva atları, virüsler ve solucanlardan farklı olarak kendilerini kopyalamazlar. Truva atlarının gerçekleştirdiği işlemleri şu şekilde sıralamak mümkündür [22];

- Verileri Silme,
- Verileri kullanılmaz hale getirme,
- Verileri değiştirme,
- Verileri kopyalayarak üçüncü taraflara gönderme,
- Bilgisayar veya ağ performansını olumsuz etkileme.

Truva atlarının en önemli özelliği efsanedeki tahta ata benzer şekilde bilgisayara kullanıcının isteği ile yüklenmesidir. Ancak kullanıcı çoğunlukla başka bir program yüklediğini düşünürken aslında yüklendiği zannedilen programın içinde saklanan başka bir yazılım mevcuttur. Saklanmakta olan bu yazılımı, efsanedeki truva atının içindeki askerlere benzetmek mümkündür. Saklanmakta olan bu yazılım programlanma amacına göre çeşitli koşullarda harekete geçebilir. Bu koşullarda çalışan Truva Atları şu şekilde örneklendirilebilir;

- Belirli zamanda çalışmak üzere programlanmış olan Truva atları.
- Belirli internet sitelerine giriş yapıldığında aktifleşmek üzere programlanan Truva atları (örneğin herhangi bir internet bankacılığı web sayfası açıldığında harekete geçerek bilgisayardaki faaliyetleri izlemeye alabilir.)
- Belirli saat dilimleri veya konumlarda harekete geçmek üzere programlanan Truva Atları, bu tür yazılımlar belirli ülkeleri veya belirli bölgeleri hedeflemektedirler.
- Geliştiricisi tarafından verilen talimatla harekete geçirilen Truva Atları, bu tür yazılımlar bilgisayar üzerinde ağ portlarını kullanarak sürekli dinleme yaparlar ve geliştiricisi tarafından söz konusu ağ portuna bağlantı yapılarak gönderilen talimatlara göre hareket ederler. Bu tür yazılımların diğer bir çalışma yöntemi ise dinleme yapmak yerine önceden truva atı içinde tanımlanan bir IP adresine belirli aralıklarla bağlantı yaparak ilgili IP adresinde tanımlanan komutlara göre hareket edilmesidir. İkinci yöntemin kullanılması sürekli dinleme yapılmadığından truva atı yazılımının daha zor tespit edilmesine neden olur.
-

2.2.4. Casus yazılımlar

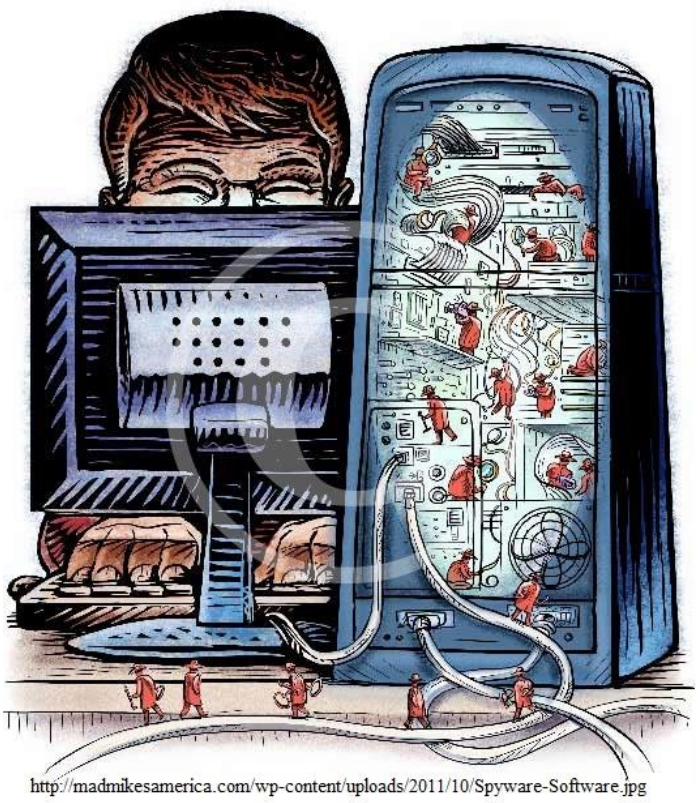
Casus yazılımlar kullanıcı aktivitelerini takip ederek kullanıcılara ait verileri toplarlar. Casus yazılımlar tarafından toplanan bu veriler üçüncü taraflara raporlanarak önemli güvenlik ihlalleri oluştururlar. Ayrıca arka planda gerçekleştirilen işlemlerden dolayı bilgisayar performansına olumsuz etki yaparlar [23].

Literatürde zararlı yazılımlar (İng. Malware) işlevlerine göre yukarda belirtildiği şekliyle sınıflandırılsalar dahi belirli amaçlar için tasarlanmış yazılımlar bu sınıflandırmadaki birden çok yazılımın özelliğini gösterebilirler.

Casus yazılımlar özel amaçlarla geliştirildiklerinden dolayı arka planda çalışarak geliştiricisi veya kullanıcısı tarafından belirlenen bazı verileri sistemden elde etmeyi hedeflerler. Bu veriler kimi zaman kredi kartı numarası gibi bir bilgi olabileceği gibi kimi zamanda gizli bir belge de olabilir [9]. Zarar gören veya kaybedilen gizli veri, önceden alınabilecek birtakım tedbirlerle geri kazanılabilir ancak casus yazılımlar aracılığıyla çalınan veri saldırgandan geri alınamaz. Bu durum gizli olması gereken verinin artık gizliliğinin kalmamasına neden olur.

Casus yazılımlar, bir sisteme fiziksel erişimi olan kişiler tarafından da yüklenebileceği gibi küçük maddi kazançlar karşılığı (ücretsiz programlar vb.) kendi bilgisayarlarının güvenliklerini göz ardı ederek indirilen çeşitli yazılımlar ile de bilgisayara bulaşabilirler [24, 25].

Casus yazılımlar, sisteme sızma işleminden sonra saldırgan tarafından önceden tanımlanan değişik özellikler aracılığıyla yetkisiz erişim kazanarak Resim 2.1'de temsili olarak sunulduğu gibi zararlı işlemler gerçekleştirirler. Casus yazılımlar genellikle kullanıcılar tarafından faydalı özellikleri taşıyan ancak lisanssız ve kopya ürünlerde gizlenecek şekilde geliştirilirler.



Resim 2.1. Casus yazılım aktiviteleri (temsili)

Örnek casus yazılımlar

Son zamanlarda isimlerinden sıklıkla bahsedilen casus yazılımlardan bazıları şunlardır;

- STUXNET
- DUQU
- FLAME
- CIPAV

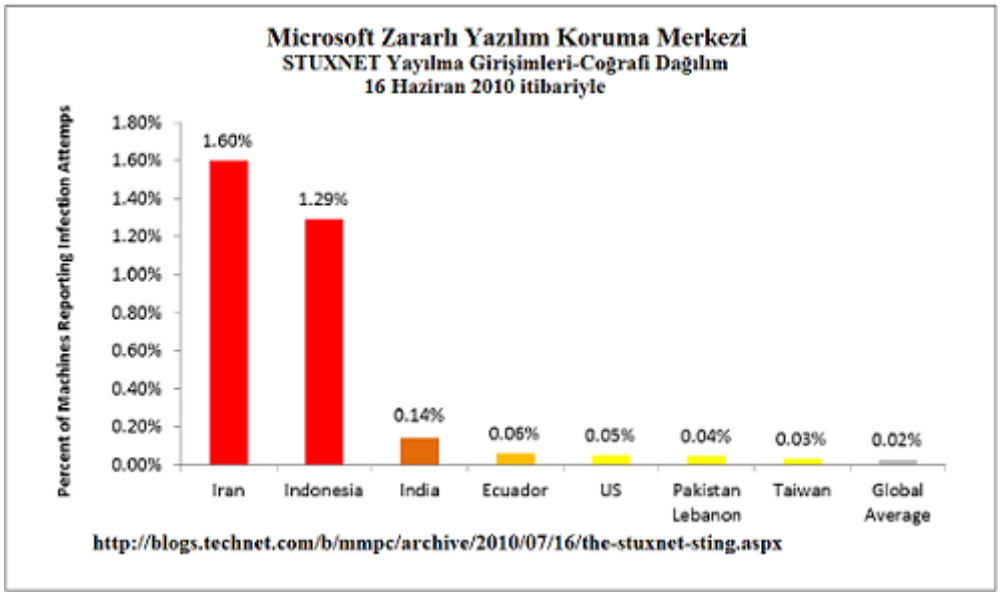
STUXNET

Stuxnet ilk defa Beyaz Rusya'daki küçük bir firma olan "VirusBlokAda" tarafından tespit edildi. Bu zararlı yazılım çok karmaşık bir yapıya sahipti. Bu karmaşık yapıyı dikkat çekici hale getiren en büyük özellik casus yazılımlar dahil birçok zararlı yazılım yöntemini kullanmanın yanı sıra dört adet Sıfır Gün (İng. Zero – Day) açıklığını beraber kullanması, güvenilir firmalardan çalınmış kök sertifikalar ile sürücü imzalaması ve ülkeler için belirli öneme haiz tesisleri hedef alarak süreç değişimi yapmaya çalışmasıdır [26].

Stuxnet casus yazılımının diğer bir özelliği bulaştığı bilgisayarda bir SCADA (Siemens supervisory control and data acquisition) sistemi mevcutsa ilk önce mevcut projelerin kod

ve dizaynlarını çalmaya çalışması, ardından programlama yazılım ara yüzü vasıtasıyla PLC'lere (İng. Programmable Logic Controllers) kendi kodlarını yüklemesidir. Ayrıca yüklenen bu kodlar, Stuxnet'in bulaşmış olduğu bir bilgisayardan, PLC'lerdeki bütün kodlar incelenmek istendiğinde dahi görülememektedir [26].

Siber Savaş kavramının hayata geçirildiğinin kanıtı olabilecek bir husus ta Şekil 2.1'de de görülebileceği gibi çoğunlukla Stuxnet yazılımının özellikle İran'da kendisini göstermesidir. Stuxnet yazılımı İran nükleer tesislerinde Temmuz 2010'da tespit edilmiş olup özellikle nükleer ve sanayi tesislerinin bilgisayar sistemlerini hedef alması dahası kontrol edebilmesi ses getirmiştir.



Şekil 2.1. Stuxnet yazılımının ülkeler için dağılımı

DUQU

DUQU, casus yazılım dahil birçok zararlı yazılım özelliği taşıyan bir yazılım olup 1 Eylül 2011 tarihinde tespit edilmiştir. Budapeşte Ekonomi ve Teknoloji Üniversitesi Kriptografi ve Sistem Güvenliği Laboratuvarı'nda tespit edilen bu yazılım hakkında 60 sayfalık bir rapor yayımlanmış olup söz konusu raporda yazılım DUQU olarak isimlendirilmiştir [27]. Dizayn yöntemi, iç yapısı ve çalışma yöntemi nedeniyle STUXNET ile çok benzediği ifade edilen DUQU yazılımının aynı ekip tarafından ancak farklı amaçlarla geliştirildiği değerlendirilmektedir. STUXNET yazılımı nükleer tesislerdeki PLC'lerin çalışmasını olumsuz etkilemekte iken DUQU yazılımı Microsoft Windows tabanlı bilgisayarlardan bilgi sızdırmayı hedeflediği ve bu hedefe ulaşmasına yardımcı olan bir özelliğinin tuş

kaydedici (keylogger) özelliği olduğu ifade edilmektedir. Söz konusu özellik ile basılan tuş bilgilerinin kaydedilmesi ile birlikte belirli aralıklarda ekran görüntüleri de kaydedilmektedir. Toplanan bilgiler, işletim sisteminin geçici dosyalarının saklandığı %TEMP% klasöründe sıkıştırılmış olarak kaydedilmektedir [28].

Küresel alanda bilgisayar güvenliği hizmeti veren RSA şirketinden Michael Sconzo tarafından, "DUQU'nun girdiği sistemde 36 gün kaldığı, bu süre içinde sistemi analiz ettiği, ardından elde ettiği bilgileri güvenli bir sunucuya aktardığı ve 36 günün sonunda kendini yok ettiği belirtilmiştir.

FLAME

CrySys raporuna göre FLAME zararlı yazılımı, hedef aldığı bilgi tipi doğrultusunda saldırı yapmak için tasarlanmış birçok modülden oluşmuş karmaşık bir kittir. FLAME ya da sKyWIper olarak adlandırılan bu yazılımın bilgi çalma amacıyla yazılmış olduğu ve tespit edildiği tarih itibariyle 5-8 yıldır aktif olabileceği değerlendirilmektedir. Ayrıca bu yazılımın beş farklı şifreleme yöntemi, üç farklı sıkıştırma yöntemi ve beş farklı dosya formatı kullandığı tespiti de yapılmıştır. Söz konusu yazılımın dikkat çekici bir diğer özelliği ise bulaştığı sistemden edindiği bilgileri yine aynı sistem içinde SQLite veritabanı üzerinde saklamasıdır. SKyWIper yazılımının yüksek ihtimalle klavye, ekran, mikrofon, depolama ve ağ gibi tüm bilgisayar unsurlarını kullanabildiği de değerlendirilmektedir. CrySys raporu SKyWIper yazılımının (FLAME) bir devlet organizasyonu tarafından önemli bir bütçe ve işgücü harcanarak Siber Savaş faaliyetleri kapsamında geliştirilmiş olabileceğini ifade etmektedir [29].

CIPAV

"Computer and Internet Protocol Address Verifier (CIPAV)" yazılımı FBI tarafından şüphelilerin takibi amacıyla geliştirilen bir veri toplama yazılımıdır. CIPAV yazılımı tıpkı diğer illegal casus yazılımlar gibi hedef bilgisayar üzerinde çalışırken kullanıcısı tarafından fark edilmeden bilgisayar aktivitelerini izler ve raporlar. CIPAV IP adresi, MAC adresi, açık ağ portları, çalışan uygulamalar, yüklü uygulamalar, son ziyaret edilen web sayfaları gibi bilgileri toplar. Söz konusu yazılım ayrıca yüklendikten sonra arka planda tüm giden ağ trafiğini, bağlanılan her IP adresini, zaman damgası ile birlikte kayıt altına alır. CIPAV

yazılımı, kendi okuluna bomba ihbarları yapan bir gencin soruşturulmasına ilişkin açık bir mahkemede isminin geçmesi ile haber başlıklarında yerini almıştır [30].

Siber dünyada casus yazılımların oluşturdukları riskler

Gün geçtikçe siber dünyanın sağladığı kolaylıkların artması nedeniyle bilişim sistemleri üzerinden gerçekleştirilen işlemlerin kapsamı ve miktarı artmaktadır. Örneğin internet bankacılığının yaygınlaşması sonucunda birçok kullanıcı bankaya gitmek yerine internet bankacılığını tercih etmektedir. İnternet üzerinden gerçekleştirilen alışverişler de bu kapsamda verilebilecek örneklerdir.

Günümüzde bankacılık, alışveriş, eğitim, sağlık gibi birçok önemli işler internet üzerinden halledilebilmekle birlikte sosyal ağlar, internet üzerinden oynanan oyunlar, haber takibi gibi insan hayatında yer tutan diğer faaliyetlerin de internet üzerinden yapılması kullanıcıları siber dünyaya daha da bağlamaktadır. Gerçekleştirilen işlem çeşitlerinin artması, suçluların siber dünyaya yönelmesine sebep olmaktadır. Ancak suçluların siber dünyaya olan ilgilerinin artmasına karşın kullanıcılarda aynı düzeyde farkındalık oluşmamaktadır. Söz konusu farkındalığın kullanıcılar ile birlikte bilişim hizmeti veren kurumlar/firmalar tarafından da oluşması ve gerekli önlemlerin alınması gerekmektedir.

Casus yazılımlar, aşağıda bahsedilen riskleri oluşturmaktadırlar;

- Kullanıcıların siber dünyadaki kimlik kartları olarak tanımlanabilecek kullanıcı adı ve parola/şifrelerinin ele geçirilmesi,
- Kullanıcı isteği dışında reklamlara maruz kalınması, reklam yazılımlarında bulunan bu özelliğin yanı sıra başka zararlı yazılımların yüklenmesinin de mümkün olması [31],
- Kullanıcıların internet ortamında kullandıkları kredi kartı bilgilerinin başka kişilerin eline geçmesi sonucu maddi zarara uğrama riski,
- Bilgisayarda elektronik ortamda bulunan gizli bilgi ve belgelerin yetkisiz kişilerin eline geçmesi,
- E-posta yazışmaları, takvim bilgileri gibi kişiye özel bilgilerin üçüncü tarafların eline geçmesi sonucunda kişinin yaptıklarının takip edilebilecek olması,
- Kişiye özel fotoğraf, müzik ve videoların kötü niyetli kişilerce ele geçirilmesi,

- Bant genişliği ve istemci işlemleri gibi sistem bileşenlerinin kullanıcı bilgisi dahilinde olmadan diğer kişilerce kullanılabilmesi (BOTNET vb.),
- Casus yazılımların arka planda çalışması sonucunda bilgisayar ve ağ performans kaybı yaşanabilmesi [32],
- Kullanıcının iradesi dışında gerçekleşen işlemlerden dolayı yasal yaptırımlarla karşılaşabilmesi (Örneğin casus yazılımın kullanıcı bilgisayarından gizlice e-posta göndermesi vb.) ,
- Banka şifrelerinin çalınarak kişilerin banka hesaplarından para çekilmesi. Mobil cihazlar tarafından kullanılan işletim sistemlerini de tehdit eden casus yazılımlar söz konusu durumun engellenebilmesi için bankalar tarafından oluşturulan uygulamalar içinde risk oluşturmaktadır [33],
- Kurumsal nitelikte çalışan şirketler ile askeri ve kamu kurumlarına ait yazışmalar gibi belgelerin sızma riski (endüstriyel ve askeri casusluk).
- Telefon dinlemelerinin (telekulak) çok tartışıldığı günümüzde, her yerde bulunan bilgisayarlar ile bilgisayar özelliği taşıyan akıllı telefon/tablet gibi mobil cihazların casus yazılımlar aracılığıyla kullanıcılarını izleyen bir gizli kamera ve dinleyen bir ses kaydedici olması riski [34].
- Kimlik bilgilerinin çalınarak kişinin bilgisi olmadan söz konusu kimlik bilgilerinin farklı amaçlarla kullanılması. Örneğin sahte kredi kartı hesapları açılması, şirketler kurularak bu şirketler üzerinden yasal olmayan faaliyetlerin yürütülmesi vb.
- Ülkelerin kritik altyapılarının zarar görmesi riski. Örneğin nükleer tesislerin, ulaştırma sağlık gibi kamu altyapılarının siber saldırı sonucu zarar görmesi,

2.2.5. Klavye dinleme sistemleri (İng. Keyloggers)

Temel olarak klavye dinleme sistemlerini donanımsal (İng. hardware) ve yazılımsal (İng. software) olmak üzere iki kategori altında toplamak mümkündür. Bunlardan birincisi olan donanımsal klavye dinleme sistemleri klavye ile bilgisayarın giriş/çıkış (I/O) portu arasındaki veri alışverişini takip etmeyi hedefler. Donanımsal klavye sistemlerinin ilgili bilgisayara fiziksel olarak yerleştirilmesi gerekmekte olup herhangi bir yazılım yüklenmediğinden koruyucu yazılımlar tarafından tespit edilememektedirler [35].
Windows işletim sistemlerinde, Yazılımsal Tuş Kaydediciler;

- Klavye durum tablosu yöntemi,

- Windows klavye çengeli (Hook) yöntemi
- Çekirdek tabanlı klavye süzgeç sürücüsü yöntemi

gibi bilinen üç yöntemi kullanmaktadırlar. Klavye durum tablosu yönteminde "GetKeyboardState" fonksiyonu ile etkin pencereye ait iş parçacığının işlediği klavye tablosu okunarak, o an basılı olan tuş bilgileri edinilir. Windows klavye çengeli yönteminde bir Windows uygulaması klavye mesaj mekanizmasına bir altyordam kurarak ("çengel atarak") gerçekleşen mesaj trafiğini izleyebilir, mesajı normalde gideceği hedefte bulunan pencereye ulaşmadan önce işleyebilir (izleme, değiştirme, engelleme). Çekirdek tabanlı klavye süzgeç sürücü yönteminde, Windows işletim sisteminin klavye cihaz sürücüsü ile klavyenin kendisi arasında bir sürücü geliştirilerek basılan tuş bilgileri Windows sistemine ulaşmadan önce geliştirilen yazılım üzerinden geçmesi sağlanır [18].

Donanımsal klavye dinleme sistemlerinde takip edilecek bilgisayara fiziksel erişim gerekiyor olmasına rağmen yazılımsal klavye dinleme sistemleri ise diğer zararlı yazılımlarda olduğu gibi sanal dünyada kendisini çoğaltabilir, başka yazılımlar arkasına gizlenebilir.

Klavye dinleme yazılımları, siber güvenlik açısından oluşturdukları riskler değerlendirildiğinde diğer zararlı yazılımlar arasında önemli bir yere sahiptirler. Kullanıcıların siber dünyadaki kimlikleri olarak tanımlanabilecek kullanıcı adı ve parola gibi bilgileri toplamayı hedefleyen bu yazılımların asıl amacı basılan klavye tuşlarını takip etmektir.

3. CASUS YAZILIM GELİŞTİRME SÜRECİ

Bu bölümde siber suçluların hazır geliştirilen bir casus yazılım edinmektense neden özgün bir casus yazılım geliştirmek isteyebileceği, casus yazılım geliştirmek için hangi motivasyonlara ihtiyaç duyulabileceği, hedeflerin nasıl seçilebileceği, casus yazılımların hangi yazılım dilleri kullanılarak geliştirilebileceği ve çalışma kapsamında geliştirilen casus yazılıma hangi işlevlerin kazandırıldığı konuları ele alınmıştır.

3.1. Neden Casus Yazılım Geliştirilir?

Casus yazılım geliştiricileri çoğunlukla siber suçlular olmasına karşın aşağıda da bahsedildiği üzere istihbarat birimleri, koruyucu yazılım geliştiricileri, akademik amaçla çalışan kişiler de casus yazılım geliştirebilirler. Casus yazılım geliştirilmesine yönelik motivasyonlar aşağıda sunulmaktadır.

- Programlama konusunda yeteneği olan kişi veya grupların bu yeteneklerini gösterme konusundaki aşırı isteği sonucunda zararlı bir yazılım (casus yazılım vb.) geliştirip bu yazılımı ulaştırılabilen tüm bilgisayarlara ulaştırarak elde edilen bilgilerin paylaşılması veya bu kişi/grupların hedefledikleri amaçları gerçekleştirmesi sonucu kendi tanıtımlarını yapmak istemesi,
- Siber suçlular para kazanmayı hedefleyerek casus yazılım geliştirebilirler. Geliştirilecek çeşitli casus yazılımlar ile internet bankacılığı kullanıcılarının bilgileri, internet alışverişleri esnasında kullanılan kredi kartı bilgileri gibi önemli bilgilerin hedeflenmesi,
- Casus yazılım ile kurumsal bilişim ağlarından elde edilecek gizli bilgilerin paylaşılması veya casus yazılımın sızdığı bilişim sistemlerinin işlemez hale getirilmesi sonucunda kurumların imaj kaybına uğratılması hedeflenebilmektedir. Bu tür aktiviteler çoğunlukla kurumların politikalarından rahatsız olan "hacker" grupları tarafından gerçekleştirilmektedir.
- Casus yazılımlar ile internet kullanıcılarının e-posta ve telefon gibi iletişim bilgilerinin toplanarak bu bilgilerin reklam, ideolojik ve politik amaçlar ile kullanılması,
- Enerji, sanayii, ulaşım, sağlık gibi kamu bilişim altyapılarına sızan casus yazılımların bu sistemlere zarar vermesi hedeflenebilmektedir. Bu tür aktiviteler

günümüzde siber savaş kavramının ortaya çıkmasına neden olmuştur. 2007 Nisan ayında Estonya'nın bir Rus anıtını kaldırması sonrasında Estonya siber saldırılara maruz kalmıştır. Siber saldırılar Estonya'nın ticaret ve kamu düzeninin çökmesine neden olmuştur [36],

- Düşman olarak nitelendirilen ülkelerin bilişim sistemlerinden casus yazılımlar ile gizli bilgi ve belgelerin elde edilmesi hedeflenebilmektedir. Bu aktiviteler siber casusluk olarak tanımlanabilmektedirler [6],
- Propaganda ve ses getiren eylemler gerçekleştirmeyi amaçlayan terörizm aktiviteleri için aracı olarak kullanılabilmesi [37] ,
- Polis veya istihbarat teşkilatları casus yazılımları kullanarak suçluları takip edebilmektedirler. Bir suçlunun bilgisayarına/mobil telefonuna yüklenecek bir casus yazılım ile edinilebilecek bilgiler söz konusu suçlunun fiziki takibi gibi masraflı olan diğer yöntemlerle edinilebilecek birçok bilgiyi kapsayabileceği düşünüldüğünde polis ve istihbarat teşkilatlarının kendi amaçları doğrultusunda casus yazılımlar geliştirmiş olabilecekleri varsayımı yapılabilir. Bu bağlamda suçluların takip edilmesini sağlayan "CIPAV" casus yazılımının FBI tarafından geliştirildiği ifade edilmektedir [30].
- İnternet ortamında işlenen suçların alınabilecek bazı önlemlerle tespit edilmesinin çok zor olması dolayısıyla suçluların siber dünyayı hedef seçmesi [38].

3.2. Hazır Casus Yazılım Edinmek ile Özgün Casus Yazılım Geliştirme Farkları

Siber suçlular amaçlarına ulaşmak için bir casus yazılıma ihtiyaç duyarlar. Ancak casus yazılımların edinilebilmesi için iki yöntem bulunmaktadır. Bu yöntemlerden birincisi internet üzerinden satın alınmasıdır. Ancak bir casus yazılımın internet üzerinden satın alınmasında aşağıdaki dezavantajlar mevcuttur;

- Genel erişime açık olduğundan koruyucu yazılım geliştiricileri tarafından kolaylıkla tanınarak engellenebilmektedirler,
- Edinilen hazır casus yazılımların, satın alan kişiye ait bilgileri de çalma riski bulunmaktadır. Örneğin bilgilerin toplanacağı bilgisayara yüklenen casus yazılımı kontrol edecek olan programın, yani satın alan kişinin kullanacağı programın da bir casus yazılım olma riski mevcuttur,

- Siber suçlunun hedefine ulaşması için casus yazılımdan beklediği tüm fonksiyonların satın alınacak olan bir yazılımda toplanması mümkün olmayabilir. Örneğin casus yazılımın sadece belirli bölgelerde, zaman dilimlerinde, belirli programlar çalışırken aktif olması istenebilir, ancak bu veya benzeri türdeki özel bir ihtiyacı satın alınacak olan casus yazılım karşılayamayacaktır.

Yukarıda ifade edilen dezavantajlar siber suç işleme amacı ile casus yazılım satın alınması durumunda geçerlidir. Ancak bazı özel ihtiyaçlardan dolayı suç işleme amacı dışında da hazır casus yazılım veya bu türdeki casus yazılım özelliklerine sahip yazılımların (ebeveyn takip programları, kayıt tutma araçları) satın alınması tercih edilebilmektedir, bu özel ihtiyaçlara verilebilecek bazı örnekler şu şekildedir;

- Ebeveynlerin, çocukların zararlı içerik barındıran web sitelerine girişini denetlemek istemesi,
- Kişisel bilgisayarın, sahibinin yanında olmadığı zaman dilimlerinde yetkisiz kişiler tarafından kullanılıp kullanılmadığının tespiti,
- Etik açıdan çeşitli tartışmaların mevcut olmasına rağmen işyerleri, okul, kütüphane gibi ortamlarda bilgisayarların amacı dışında kullanılıp kullanılmadığının yöneticiler tarafından takip edilmesi,
- Sistem yöneticilerinin yönetimleri altında bulunan bilgisayarların sistem aktivitelerini izlemesine yönelik çeşitli programları söz konusu bilgisayarlara kurması. Bu takip programları casus yazılım veya benzeri isimlerle ifade edilmiyor olmalarına rağmen gerçekleştirdikleri birçok işlev nedeniyle casus yazılımlara benzerlik gösterirler. Örneğin girilen web siteleri, açık uygulama bilgileri, ağ trafik bilgilerinin izlenmesi vb.

gibi nedenlerle hazır yazılımların satın alınması tercih edilebilmektedir.

Koruyucu yazılımların (antivirüs/antispyware) zararlı yazılımları tespit etme yöntemlerinden birisi de imza tabanlı karşılaştırma yöntemine dayanan statik analiz yöntemidir [11, 21]. Bu yöntem koruyucu programın inceleyeceği yazılımdan elde edeceği imzayı, imza veritabanlarıyla karşılaştırması sonucunda zararlı bir yazılıma ait imza ile eşleşme bulması durumunda söz konusu yazılımı riskli olarak değerlendirir. Bu durumda eğer incelenen yazılımın daha önce karşılaşılmamış veya ilgili antivirüs programına ait imza veritabanına girmemiş olması durumunda antivirüs programı tarafından tanınmaması durumu oluşacaktır. Bu nedenle siber suçluların bir suç aleti olarak kullanacakları casus

yazılımın herhangi bir imza veritabanına girmemiş olan özgün bir casus yazılım olması beklenir. Söz konusu mantıksal çıkarımdan yola çıkarak gerçek risklerin daha iyi ortaya konabilmesi için özgün bir casus yazılımın geliştirilerek koruyucu yazılımlar tarafından test edilmesi gerekmektedir. Özgün olarak bir casus yazılım geliştirilmesinin neden tercih edilebileceğine ilişkin sebepler şu şekilde sıralanabilir;

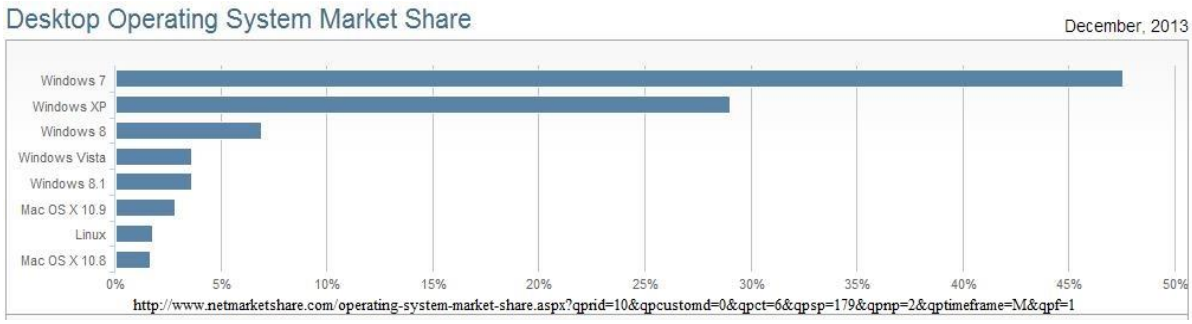
- Özgün olarak geliştirilecek bir casus yazılımın koruyucu yazılımların imza veritabanlarında herhangi bir kaydı bulunmayacağından tanınma riskinin az olması,
- Hedef veri türüne göre özelleştirmek; Sadece ihtiyaç duyulacak olan veriyi (örneğin IP bilgisi) elde edecek bir yazılımın geliştirilmesi ile koruyucu programlar tarafından tespit edilme riskini en aza indirmek. İhtiyaç duyulan veri türünden fazlasını elde edebilecek olan hazır casus yazılımlar (örneğin basılan tuş bilgisi, girilen web sayfa bilgisi vb.) koruyucu yazılımlar tarafından daha kolay tespit edilebilir,
- Değişecek olan ihtiyaçlara daha kolay adapte olunabilir. Örneğin yeni çıkan bir işletim sistemi için gerekli geliştirmelerin yapılması,
- Geliştirilen yazılımın topladığı bilgileri üçüncü taraflara gönderme riski bulunmamaktadır. Ancak bu risk hazır olarak satın alınacak casus yazılımlarda mevcuttur.

3.3. Casus Yazılım İçin Hedef Seçimi

Casus yazılım hedefi eğer bir kişi ise o kişinin davranış ve alışkanlıklarına göre casus yazılım oluşturulmalıdır. Örneğin hedefteki kişi işletim sistemi olarak “Windows” ailesinden bir işletim sistemi kullanıyorsa yazılacak casus yazılım "Windows" işletim sistemini hedeflemelidir. Eğer hedefte bir kitle varsa (Örneğin internet bankacılığı kullanıcıları, herhangi bir kuruma ait çalışanlar vb.) bu kitlenin çoğunlukla kullanmış oldukları işletim sistemleri (platformlar) dikkate alınmalıdır. Hedefteki kişinin/kitlenin kullandığı platformlar değişiklik gösterebilir. Bu platformları şu şekilde sıralayabiliriz;

Mobil Platformlar (Android, IOS vb.): Mobil platformların kullanımı günümüzde gittikçe yaygınlaşmaktadır. Özellikle kullanıcıların tüm işlemlerini mobil cihazlar üzerinden yapabilmesi kötü niyetli yazılımcıların ilgisini çekmektedir. Mobil platformlar aracılığıyla sesli aramaların, kısa mesajlaşmaların (SMS), bankacılık işlemlerinin, sosyal ağlarla ilgili işlemlerin ve hatta konum bilgileri ile ilgili işlemlerin yapılabilmesi bu platformları casus yazılımların hedefi haline getirmektedir.

Microsoft Windows Platformları: Şekil 3.1'de görüldüğü gibi kişisel bilgisayarlarda en yaygın olarak kullanılan işletim sistemi ailesinin "Windows" olduğu anlaşılmaktadır. Son kullanıcılara sağladığı kullanıcı dostu ara yüzler geniş bir kullanıcı kitlesine ulaşmıştır. Dolayısıyla casus yazılımlar gibi zararlı yazılımların hedefi haline gelmiştir. Aynı nedenle bu çalışma kapsamında geliştirilen casus yazılım, risklerin daha iyi ortaya konulabilmesi amacıyla Windows işletim sistemlerinde çalışacak şekilde geliştirilmiştir.



Şekil 3.1. İşletim sistemi kullanım oranları, NetMarketShare, Aralık 2013

Mac OS X: Apple firmasının geliştirmiş olduğu işletim sistemi olup A.B.D. ' de kullanımı daha yaygındır.

Linux Platformları: 1991 yılında hayat bulan Linux işletim sisteminin diğer işletim sistemlerinin aksine firma bağımlılığı yoktur. Farklı kurum ve kuruluşlarca geliştirilen Linux, farklı arayüzlerde diğer işletim sistemleriyle aynı işlevleri gerçekleştirebilmektedir. GNU GPL (Gnu General Public Licence) lisansı ile oluşturulan Linux işletim sisteminde çalışabilecek pek çok program İnternet üzerinde ücretsiz ve açık kaynak kodlu olarak sunulmaktadır [39]. Her ne kadar ücretsiz olarak edinilmesi mümkün olsa da Şekil 3.1'den de anlaşılacağı üzere kullanıcılar arasında diğer işletim sistemlerine göre daha az tercih edilmektedir. Bu platformlar, çoğunlukla teknik bilgisi iyi olan kullanıcılar ve sunucu sistemleri gibi çok kullanıcılı sistemler için tercih edilmektedir. Yapısal olarak daha güvenli oldukları için bu sistemler zararlı yazılımlar tarafından daha az tehdit edilmektedirler. Ayrıca bazı mobil platformların çekirdek yapılarında "Linux" işletim sistemleri olduğu da dikkate alındığında "Linux" platformları için risk oluşturabilecek bir casus yazılım ilgili mobil platformlarda da risk oluşturabilir.

3.4. Kodlamanın Yapılacağı Programlama Dili Altyapısı

Casus yazılım geliştirmek için hedef kitlenin işletim sistemlerine uyumlu olan yazılım dilleri seçilmelidir. Ayrıca bazı programlama dillerinde geliştirilen yazılımların çalışabilmesi için ilgili programlama dillerine ait Framework'lerin (uygulamanın çalışması için gerekli kütüphane ve derleyicilerin) çalıştırılacak bilgisayarda yüklü olması gerekmektedir. Programlama dilleri ile ilgili daha detaylı bilgiler Bölüm 3.4.1 ve Bölüm 3.4.2'de sunulmuştur.

3.4.1. Yaygın olarak kullanılan programlama dilleri

Programlama dillerinin yaygınlığı ile ilgili bir istatistik Şekil 3.2'de verilmiştir. Bu istatistikte geçen bazı programlama dilleri ile ilgili açıklamalar ve bu dillerin casus yazılım geliştirme açısından değerlendirmeleri şu şekildedir;

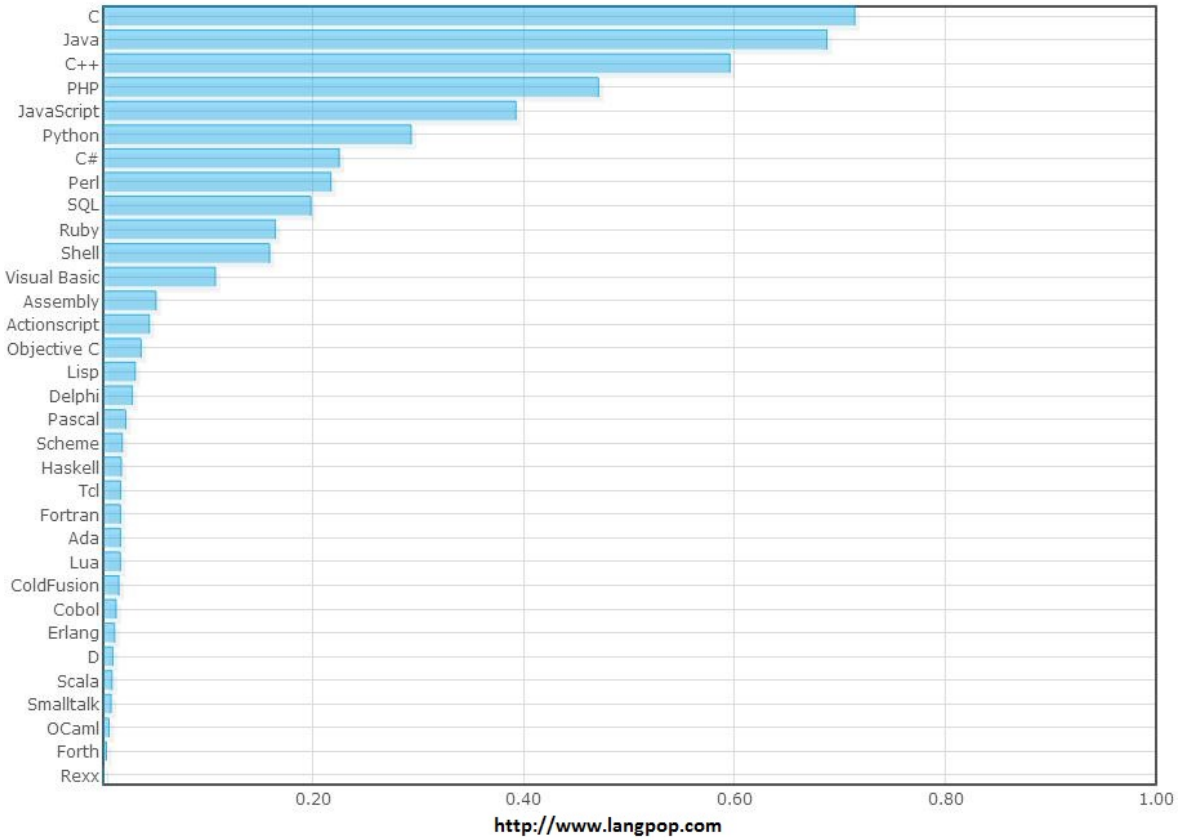
Java Programlama Dili : Java, Sun Microsystems tarafından geliştirilen nesneye yönelik, zeminden bağımsız bir programlama dilidir. Java uygulamaları bilgisayar mimarisine bağlı olmadan herhangi bir Java Virtual Machine (JVM)'de çalışabilen tipik bytecode'dur (sınıf dosyası) [40]. Şu anda özellikle kurumsal alanda ve mobil cihazlarda son derece popüler olmuştur. Java programlama dilinde geliştirilen yazılımların yüklenecekleri bilgisayarlarda uyumlu JVM paketinin yüklenmiş olmasına ihtiyaç duyduklarından dolayı casus yazılım geliştirme için kullanımı uygun değerlendirilmemektedir.

C++ Programlama Dili :_C programlama dilinden türetilen C++ programlama dili, Bell Laboratuvarlarında Bjarne Stroustrup tarafından 1980 yılından itibaren geliştirilmeye başlanmıştır. C++ genel olarak C programlama dili üzerine birçok özelliğin ilave edilmesi sonucu geliştirilmiştir. Bu özelliklerden en önemlisi sınıfların ve nesnelerin yeniden kullanılmasını ve kişiselleştirilmesini mümkün kılan Nesne Yönelimli Programlama (İng. Object Orianted Programming) özelliğidir [41]. C++ programlama dili birçok yazılımın geliştirilmesinde halen kullanılmaktadır. Özellikle donanımlar için geliştirilen sürücü gibi yazılımlar bu dil kullanılarak geliştirilmektedir. Bu dil kullanılarak çeşitli casus yazılımlar geliştirilebilir.

PHP ve Javascript: Bu programlama dilleri çoğunlukla "Web Tabanlı" yazılım geliştirme alanlarında kullanılmaktadırlar. Özellikle "PHP" tabanlı sunucu üzerinden çalışan

sistemlere “SQL Injection” gibi çeşitli siber saldırı yöntemleri ile saldırılabilmekle birlikte bu yöntemlerin casus yazılımların kullandığı yöntemlerden farklı bir kategoride ele alınması gerekmektedir.

C# Programlama Dili: C# Programlama Dili, Windows işletim sistemleri üzerinde .Net platformu oluşturulduktan sonra yaygın olarak kullanılmaya başlayan Nesnel bir dildir. C++ diline ait karışık özellikleri kullanmadaki başarısı ve Visual Basic diline ait kullanım kolaylığı sunması bu dilin özelliklerindendir. Sınıf mantığını desteklediğinden “Dll” dosyaları içinde ortak kullanılabilecek sınıflar sayesinde aynı kodların tekrar tekrar yazılmasına ihtiyaç duyulmamaktadır [42]. Casus yazılımın geliştirilmesi için Bölüm 3.4.2’de ifade edilen nedenlerden dolayı C# seçilmiştir.



Şekil 3.2. Programlama dili karşılaştırılmalı kullanım oranları

3.4.2. Casus yazılım için programlama dili seçimi

Geliştirilen eğitim amaçlı casus yazılımın en geniş kullanıcı kitlesine ulaşılabilirliğini sağlayabilmek için Şekil 3.1' de sunulduğu gibi en yaygın şekilde kullanılan Windows

tabanlı işletim sistemleri hedeflenmiştir. Bu kapsamda "Yaygın olarak kullanılan programlama dilleri" başlığında da belirtildiği gibi;

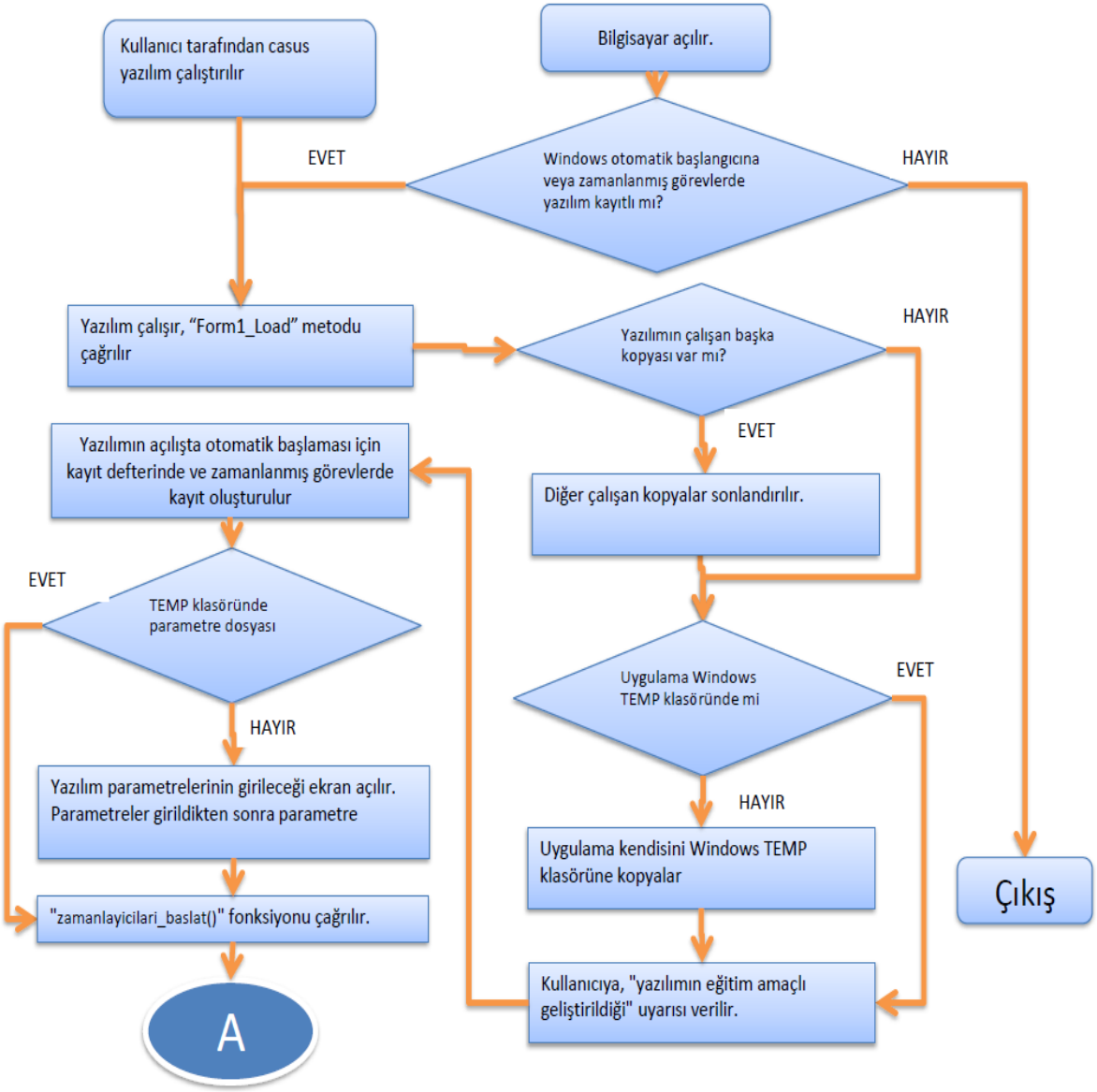
- Casus yazılım için hedef işletim sistemi olarak “Windows” seçildiğinden, söz konusu işletim sisteminin üreticisi olan Microsoft firmasının sağladığı “.NET” geliştirme ortamında “C#” dilini kullanmak, geliştirilecek casus yazılımın uyumsuzluk risklerini en aza indirecektir,
- C# dilinin nesneye dayalı programlama esaslarına uygun olması nedeniyle geliştirilme sürecinin daha kısa sürmesi,
- “Visual Studio” geliştirme aracı ile C# dilinde geliştirilen bir yazılımın Windows Vista ve üstü (Windows 7, Windows 8…) işletim sistemlerinde herhangi bir Framework kurulumuna ihtiyaç duymadan çalışabilmesi,
- C# yazılım diline yönelik hazır kütüphanelerin, dokümanların, forum ve paylaşım sitelerinin oldukça fazla olmasından dolayı, geliştirme esnasında kolaylıkla başvurulabilecek veya kullanılabilecek hazır kütüphanelerin bulunması,

Nedenlerinden dolayı casus yazılım için C# programlama dili seçilmiştir.

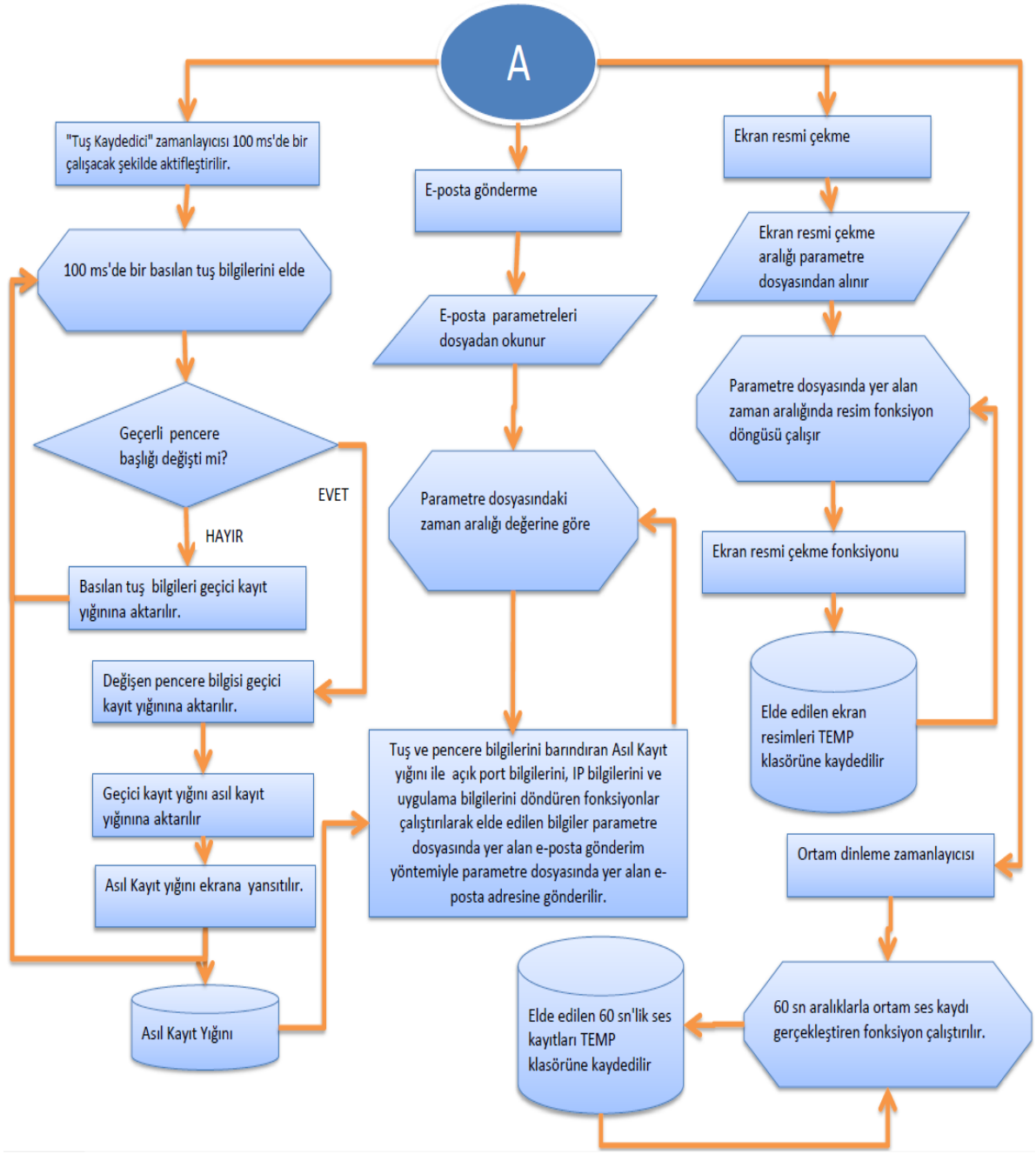
C# dilinin seçilmiş olması ile birlikte, editör bir programa da ihtiyaç duyulmaktadır. Bu kapsamda yine Microsoft firması ürünü olan "VisualStudio" programının son sürümü "Microsoft Visual Studio 2010" aracı yazılımın geliştirilmesi için kullanılmıştır. Bu editör programının seçilmesinde kullanım kolaylığı, hazır nesneleri barındırması (zamanlayıcılar, metin göstericiler vb.), Vista ve üzeri Windows işletim sistemlerinde çalışabilecek şekilde derleme yapabilmesi gibi nedenler etkili olmuştur.

3.5. Casus Yazılım Akış Şeması

Akış şemalarının yazılım geliştirme süreçlerinde akışın belirlenmesi, geliştirilecek sınıfların yapısının daha iyi tasarlanması gibi çeşitli faydaları bulunmaktadır. Bu nedenle geliştirilen casus yazılıma yönelik bir akış şeması oluşturulmuş olup Şekil 3.3’te sunulmuştur.



Şekil 3.3. Casus yazılım akış şeması



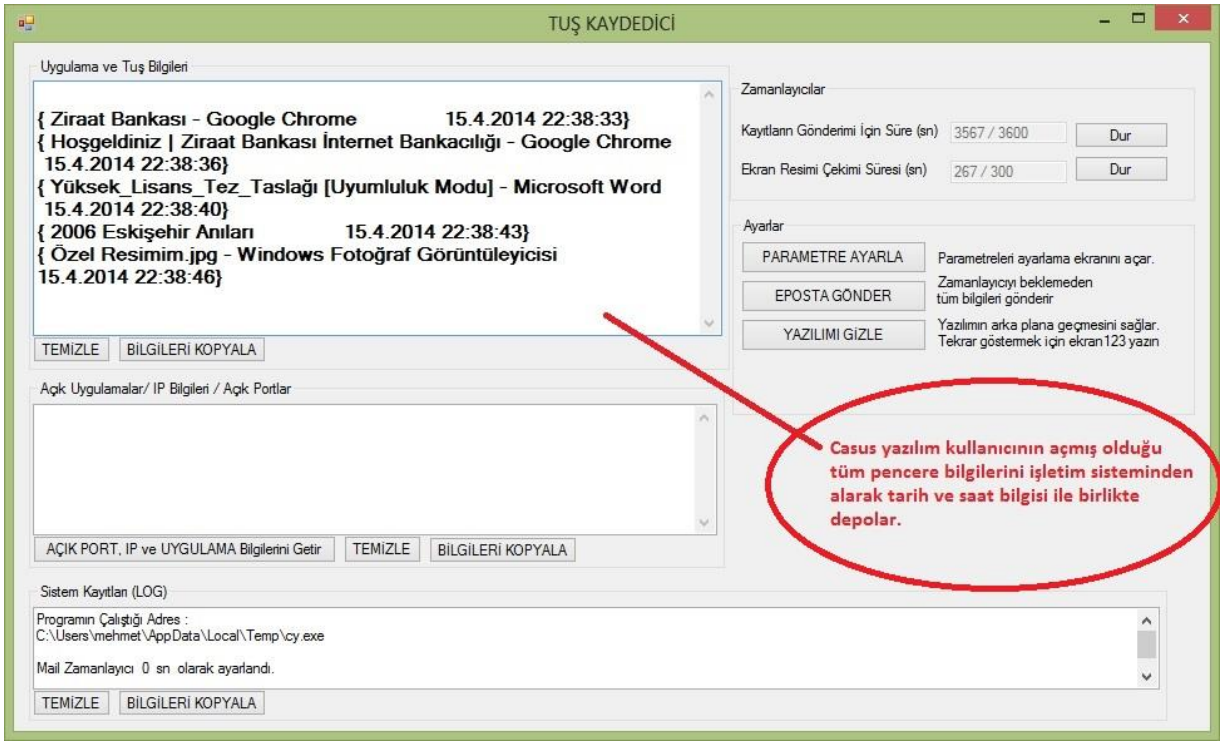
Şekil 3.3. (devam) Casus yazılım akış şeması

3.6. Casus Yazılıma Kazandırılacak İşlevlerin Belirlenmesi

Geliştirilmiş olan casus yazılım bu tür zararlı yazılımların siber güvenlik açısından nasıl tehlikeler oluşturabileceği konusunda fikir verebilmesi amacıyla bazı özellikler ile donatılmıştır. Bu özellikler başlıklar halinde sunulmuştur.

3.6.1. Açık uygulama pencerelerine ait bilgilerin toplanması

Kullanıcılar tarafından hangi uygulamaları hangi saatte ne kadar süreyle açık tuttukları bilgileri casus yazılım geliştiriciler tarafından takip edilmek istenebilmektedir. Geliştirilen uygulamaya bu özellik eklenmiştir. Resim 3.1'de görülebileceği gibi kullanıcının açmış olduğu "İnternet Bankacılığı" web sayfası bilgisi ardından bilgisayarda bulunan dosyalardan açmış olduğu resim dosyasına ait bilgiler ve bu resim dosyasını hangi program aracılığı ile açmış olduğu bilgileri casus yazılım tarafından elde edilmiştir.

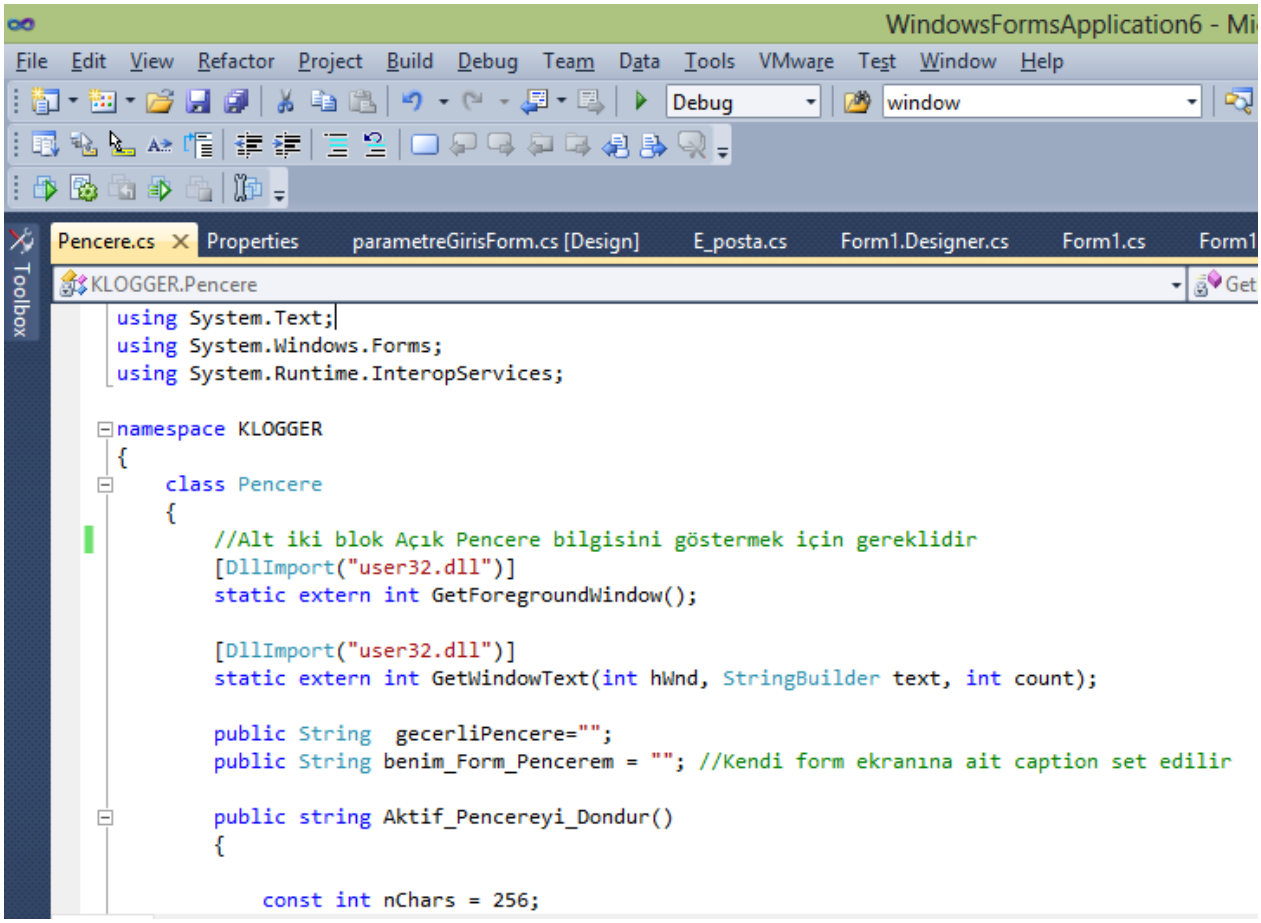


Resim 3.1. Açık uygulamaların pencere bilgileri casus yazılım üzerinde gösterilmesi

Resim 3.1'de de sunulduğu gibi açık pencere bilgisi "Windows" işletim sisteminde bulunan "GetForegroundwindow()" ve "GetWindowText(…)" fonksiyonları aracılığıyla edinilmektedir. Ancak bu fonksiyonlardan gelen sonuçların doğrudan kullanılması mümkün olmadığından "Pencere.cs" sınıfı ve bu sınıf içinde iki adet fonksiyon oluşturulmuştur;

"Aktif_PencereyiDondur()" *:* Resim 3.2'de sunulan fonksiyonlar yardımıyla kullanıcının o an üzerinde bulunduğu pencereyi döndürür. Örneğin kullanıcı internet bankacılığı ile ilgili bir web sayfasında ise ilgili web sayfasının başlığında bulunan açıklama elde edilir veya bir video oynatılıyorsa, oynatılan videonun ismi elde edilir.

“DegisenPencereyiDondur()” : Casus yazılım yaklaşık 100 mili saniyelik aralıklarla (saniyenin onda biri) pencere bilgisini sorgulayarak kayıtlara ekler. Ancak kullanıcının uzun süre bir pencere üzerinde çalışması durumunda yazılım tarafından ilgili pencereye ait bilgi tekrar tekrar alınarak kayıtların boyutunun artması ve okunurluğunun azalması riski oluşacaktır. Dolayısıyla “DegisenPencereyiDondur” fonksiyonu her 100ms’de bir, önceki Aktif_Pencere bilgisi ile güncel pencere bilgisini karşılaştırır ve değişim varsa saat bilgisi ile birlikte kaydını gerçekleştirilir. Böylelikle 100ms’den kısa aralıklı olmaması koşuluyla tüm pencere değişimleri takip edilebilmektedir.



Resim 3.2. Açık pencere bilgisini işletim sisteminden alan kodlar

Kullanıcının açmış olduğu uygulamalara ait bilgiler ile kullanıcı hakkında aşağıdaki bilgiler edinilebilir;

- Çalışmış olduğu bankaya ait bilgiler,
- Kişisel bilgiler (Seyrettiği filmler, Dinlediği müzikler…),
- Mesleği ile ilgili bilgiler (Açmış olduğu ofis dosya isimlerinden),
- Kullanmakta olduğu sosyal ağlar,

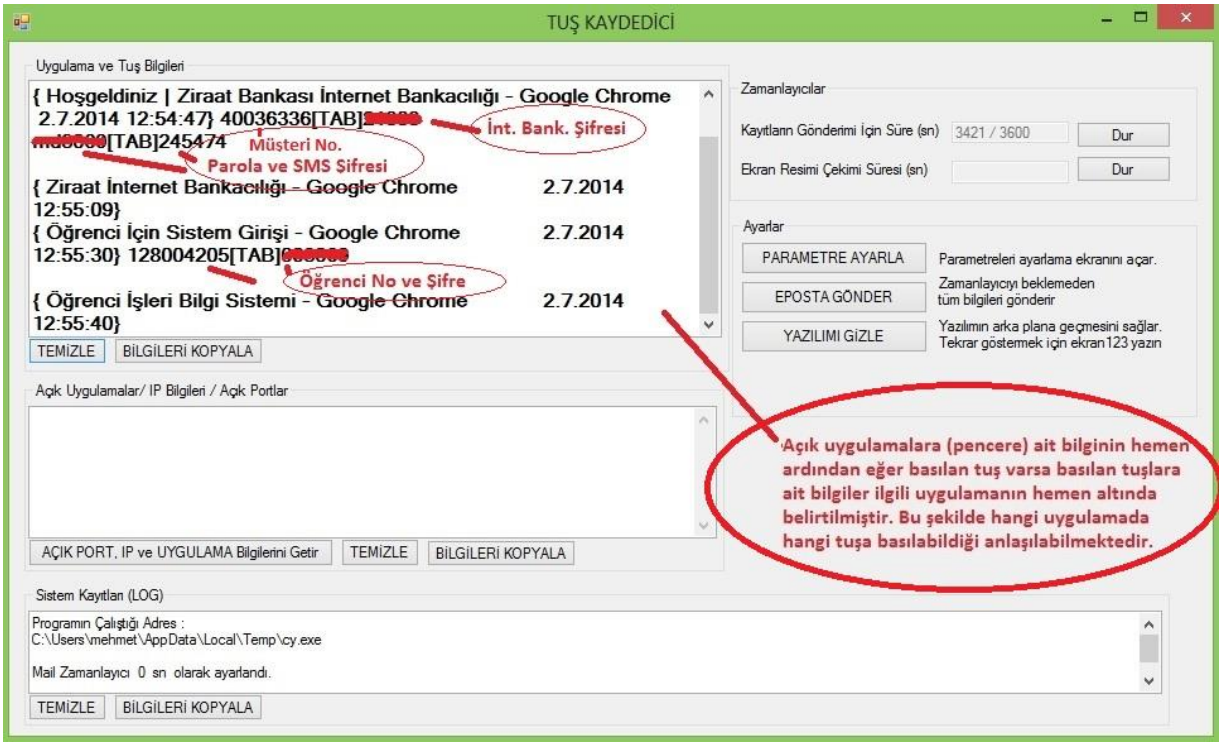
Gibi daha birçok konuda kullanıcı hakkında bilgi edinilebilir.

3.6.2. Basılan tuşların kayıtlanması (Keylogger)

Kullanıcılar açısından en büyük bilgi güvenliği tehditlerinden birisi, basılan tuşların kaydedilip başka kişilerin eline geçmesidir. Çünkü kullanıcılar; şifreleri, özel yazışmaları, mesleki yazışmaları, arama motorları ile yaptığı aramaları ve daha birçok işlemi klavye tuşlarını kullanarak yapmaktadırlar.

Yazılımsal tuş kaydedici geliştirme yöntemleri Bölüm 2.2.5'te sunulmuştur. Bu yöntemlerden Windows klavye çengeli (Hook) yöntemi yaygın olarak kullanılmaktadır [35]. Koruyucu yazılımlar, bilinen yöntemleri kullanan zararlı yazılımları kolay tespit edebildiklerinden bu çalışma kapsamında geliştirilen casus yazılımın tuş kaydedici özelliğinin sağlanması için Bölüm 2.2.5'te sunulan yöntemlerden farklı olarak Windows işletim sistemleri içinde yer alan ve oyun programlamada kullanılabilen "GetAsyncKeyState" fonksiyonu kullanılarak bir sınıf geliştirilmiştir. Bu fonksiyon, klavye durum tablosu yönteminde olduğu gibi Windows mesaj kuyruğuna bakmaz, tuşlara basıldığı müddetçe değer döndürmektedir. Bu nedenle nadiren işletim sisteminin yorumladığı basılan tuş bilgilerinden farklı sonuçlar üretilebilir. Ayrıca "GetAsyncKeyState" fonksiyonu çengel (hook) yönteminde olduğu gibi kendisini herhangi bir işletim sistemi altyordamına kaydettirmez. Klavye durum tablosu yöntemi sadece Capslock ve Numlock tuşlarının statüsünün alınması için kullanılmıştır. Sürücü geliştirme yöntemi ise her donanım için ayrı tasarım gerektirdiğinden kullanılmamıştır.

Tuş kaydetme özelliği Bölüm 3.6.1'de ifade edilen açık uygulama bilgilerinin gösterilmesi özelliği ile entegre olarak çalışmaktadır. Bu entegrasyon sonucunda Resim 3.3'te görülebileceği gibi (açıklamalar ekran görüntüsü üzerine işlenmiştir) hangi pencere açık iken hangi tuşlara basıldığı bilgisi edinilmektedir. Bu şekilde yazılan bir şifrenin elektronik posta adresine ait bir şifre mi yoksa internet bankacılığı uygulamasına ait bir şifre mi olduğu kötü niyetli kişiler tarafından ayırt edilebilir.



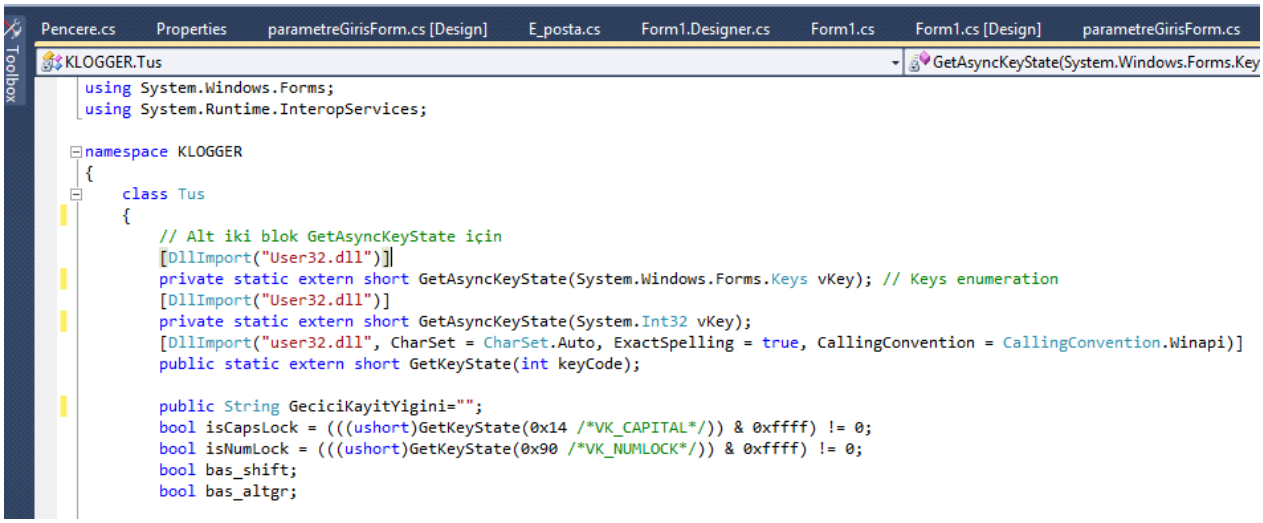
Resim 3.3. Basılan tuş bilgilerinin kaydedilmesi (KEYLOGGER özelliği)

Bir bankaya ait internet bankacılığı sayfasında basılan tuş bilgilerinin (örnek bir parola girilmiştir) casus yazılım tarafından elde edilebildiği Resim 3.3'te görülmektedir. Benzer şekilde üniversite öğrenci işleri bilgi sistemi hesabına girişi sağlayan web ara yüzünden girilen bilgilerin de elde edilebildiği görülmektedir. Ayrıca tuş kaydedici yazılımlar için bir önlem olabileceği düşünülen Windows işletim sistemlerinde yer alan "Ekran Klavyesi" uygulaması ile basılan tuşlarında bu çalışma kapsamında geliştirilen casus yazılım tarafından izlenebildiği de görülmüştür.

Kullanıcının açmış olduğu pencere bilgileri yanında basılan tuş bilgilerinin de kaydedilmesi sonucu aşağıdaki bilgiler casus yazılım tarafından elde edilebilir;

- Eposta kullanıcı adları ve parola bilgileri,
- Kredi kartı bilgilerinin girilerek alışveriş yapılması sonucu kredi kartı bilgileri,
- Fikri ve sınai hakları barındıran dokümanlar,
- Kişisel yazışmalar (sosyal medya, eposta vb.) bilgiler casus yazılım tarafından elde edilebilir.

Ancak bazı kurumların kendi sanal klavye ara yüzlerini oluşturması ile yukarıdaki bazı bilgilerin casus yazılım tarafından elde edilmesi engellenebilir. Örneğin parolalar, kredi kartı bilgileri gibi.



Resim 3.4. Basılan tuş bilgilerini işletim sisteminden alan fonksiyonlar

Resim 3.4'te görüleceği üzere casus yazılım basılan tuş bilgilerini elde edebilmek için bazı işletim sistemi fonksiyonlarını kullanması gerekmektedir. Bu fonksiyonlar şu şekildedir;

"GetAsyncKeyState (System.Int32 vKey)" *:* Bu fonksiyon 0-255 arasında olmak kaydıyla her bir tuşa karşılık gelen "ascii" değeri parametre olarak almaktadır. Parametre olarak alınan numaranın karşılık geldiği tuşun basılı olup olmadığı "short" formatında döndürdüğü değer ile ifade edilir. Ancak dönen değer yorumlanmaya ihtiyaç duyan bir değerdir. Ayrıca her bir klavye düğmesinin kontrol edilebilmesi için belirli bir algoritmaya uygun olarak tüm 255 değer bir döngü ile kontrol edilmelidir. Bununla birlikte bazı özel tuşlar için belirli koşulları içeren kontroller gerekmektedir. Örneğin GetAsyncKeyState(65) fonksiyonu kontrol edildiğinde basıldığına işaret eden değer dönüyorsa "a" tuşuna basıldığı anlamı çıkartılabilir. Ancak "CapsLock" tuşu aktif ise veya aynı anda "Shift" tuşu basılı ise gerçekte büyük "A" karakterine basılıyordur. Bir İşletim sistemi fonksiyonu olan "GetAsyncKeyState" bir parametre almakta olup sadece "short" türünde bir sayı döndürmektedir. Ancak bu casus yazılım ile hedeflenen klavyeden girilen bilgilerin doğru şekilde alınmasıdır. Beklenen işlevi gerçekleştirmek için geliştirilen önemli fonksiyonlar şu şekildedir;

"Basilan_Tusu_Dondur ()" : "Timer" nesnesi kullanılarak bu fonksiyon her 100 mili saniyede bir çağrılmaktadır. Her çağrıldığında "0" ile "255" değerlerini parametre olarak

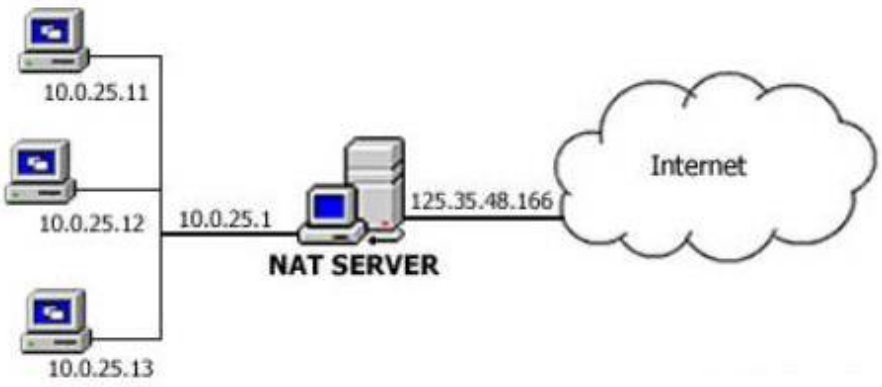
GetAsyncKeyState fonksiyonuna gönderir ve gelen değerin “1” veya “-32767” olması durumunda ilgili parametre değerine karşılık gelen tuşun basılı olduğu anlaşılır. Bununla birlikte basılan tuşun beraberinde basılan diğer tuşlarla birlikte değerlendirilmesi gerekmektedir. Örneğin klavyede bulunan “1” tuşuna basıldığında “shift” tuşu da kontrol edilmeli ve eğer “shift” tuşu da basılı ise aslında “!” simgesine basıldığı değerlendirilmelidir. Bu fonksiyon gerçekleştirdiği kontrollerden dolayı casus yazılım içindeki en fazla satıra sahip olan fonksiyondur.

“Basilan_Tusu_Yigina_Aktar()”: Basılan her tuş bu fonksiyon aracılığı ile, bir karakter dizisinin en sonuna eklenir. Ancak bu fonksiyonun önemli bir diğer özelliği ise normal klavye kullanımı esnasında yazılan bir karakterin “Backspace” tuşu ile silinmesi durumunu, son girilen karakter(ler)in oluşturulan karakter dizisinden silinmesini sağlayarak casus yazılım kayıtları ile gerçek klavye kullanımının tutarlı olmasını sağlamasıdır.

3.6.3. Yerel IP ve Genel IP bilgilerinin edinilmesi

Casus yazılım geliştiricilerin öğrenmek isteyebilecekleri bir diğer bilgi IP bilgisidir. IP numarasını temel olarak iki gruba ayırabiliriz.

- Yerel IP Adresi: Dış dünyadan (İnternet) bağımsız olarak bir güvenlik duvarı veya bir modemin arkasında bilgisayara verilen IP adresidir. Bu IP adresi üniversite vb. kuruluşlarda kurumun kendi belirleyeceği standartlar ile oluşturulan IP verme sistemidir. Örneğin Bilişim Enstitüsü için "10.1.x.x" bloğu verilirken Mühendislik Fakültesi için 10.2.x.x" bloğunun verilmesi gibi. Ancak iki bloğun da dış dünyaya bağlanırken kullandıkları IP adresi Üniversite'ye ait IP adresidir. Şekil 3.4'te "10.0…" ile başlayan IP adresleri yerel IP adreslerine örnek olarak gösterilebilir.
- Genel IP Adresi: İnternet servis sağlayıcıların kişi veya kurumlara vermiş oldukları İnternet üzerinden kurulan iletişimlerde karşı tarafın da gördüğü IP adresidir. Bilişim suçları işlendiğinde çoğunlukla Genel IP adresi üzerinden suçlulara ulaşılmaktadır. Genel IP adreslerini öğrenmek için çeşitli web siteleri bulunmaktadır. Örneğin www.iplocationfinder.com , www.whatismyip.com gibi web sayfalarından genel IP adresi öğrenilebilmektedir. Ayrıca Genel IP adresi kullanılarak kişilerin yaklaşık konumları hakkında bilgi edinilebilmektedir. Şekil 5.3'te 125.35.48.166 olarak ifade edilen IP adresi Genel IP adresine bir örnektir.

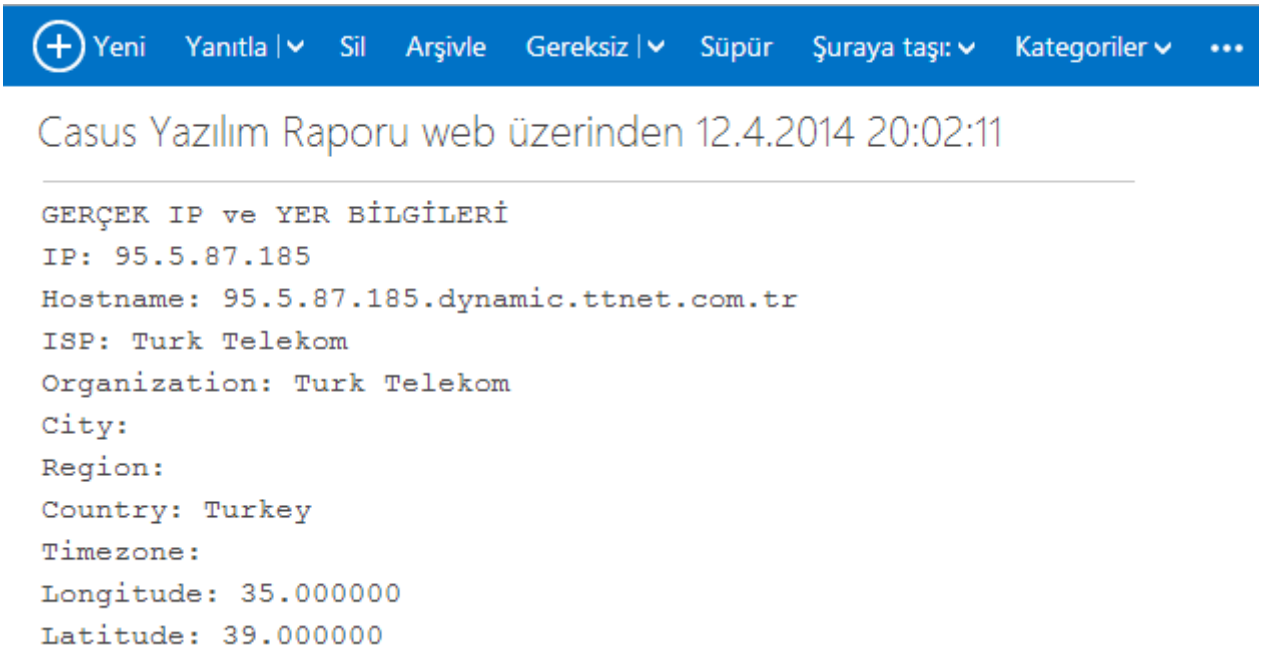


Şekil 3.4. Yerel IP ve Genel IP örnek şeması

Geliştirilmiş olan eğitim amaçlı casus yazılım uygulamasına hem Genel IP adresini hem de yerel IP adresini belirleme özelliği eklenmiştir. Genel IP bilgileri kullanılarak kullanıcının eğer kurumsal bir ağ üzerinden İnternet'e çıkıyorsa hangi kurumda bulunduğu hakkında, eğer kişisel amaçlı İnternet kullanıyorsa bulunduğu konum hakkında yaklaşık bir tahminde bulunulması sağlanabilmektedir.

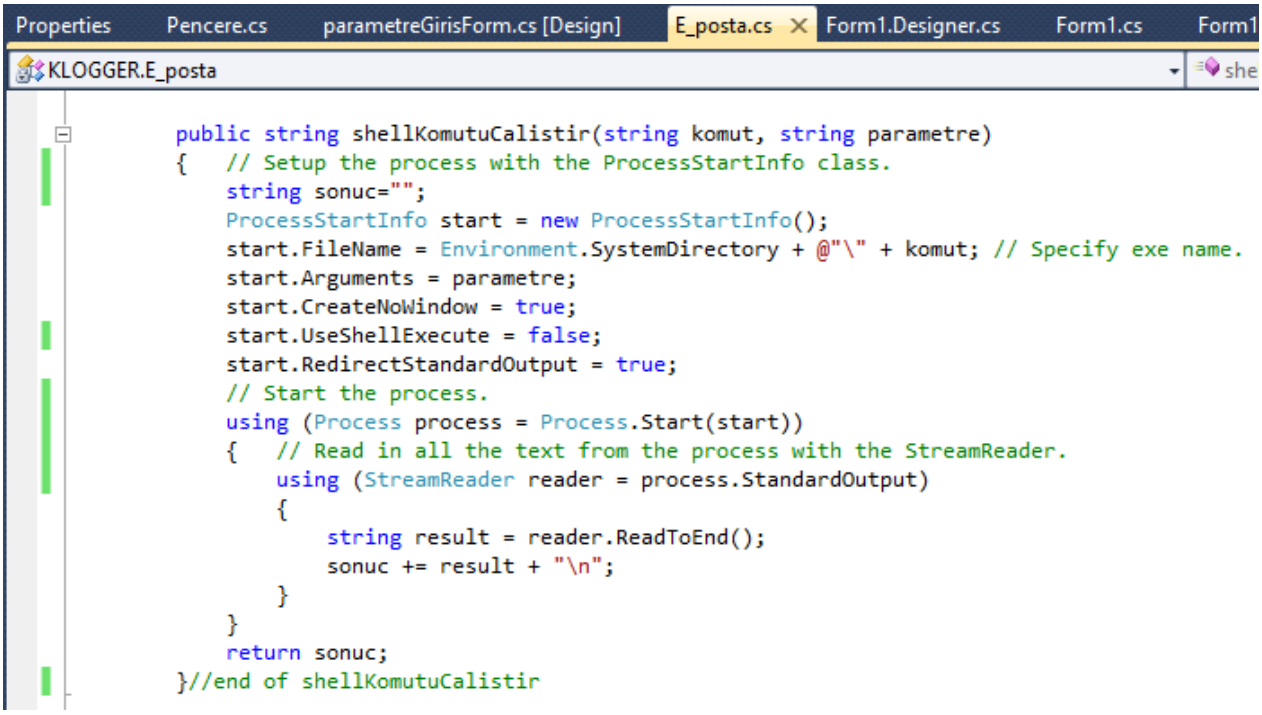
Ayrıca kullanıcıdan alınan yerel IP bilgileri aracılığıyla kullanıcının kurumsal IP yapılanmasında ki konumu hakkında fikir edinilebilir. Örneğin Yerel IP bloğu bilgisi kullanılarak üniversitenin hangi bölümünde olduğu öğrenilebilir.

Programın e-posta yoluyla gönderdiği bilgilerde, casus yazılımın edindiği IP bilgileri de yer almaktadır. Resim 3.5'te görülebileceği gibi "GERÇEK IP ve YER BİLGİLERİ" başlığında Genel IP bilgisi ile birlikte yaklaşık konum bilgisi de yer almaktadır. "BİLGİSAYAR YEREL IP BİLGİLERİ" başlığında ise "Windows komut terminali " üzerinden yerel IP bilgilerini detayları ile sunan "ipconfig /all" komutunun çıktısı casus yazılım tarafından edinilmektedir. Yerel IP bilgileri alınırken"IPV6" standardı bilgisayar tarafından destekleniyorsa edinilen IPV6 adresi de casus yazılım kayıtlarına da eklenir. Yerel ve Genel IP adreslerine ait casus yazılım kayıtlarının detayları Ek-1'de sunulmuştur.



Resim 3.5. Eposta adresine gönderilen "Gerçek Ip ve Yer Bilgisi" kaydına ait görüntü

Casus yazılım geliştiricisinin ihtiyaç duyabileceği birçok bilgi Windows komut terminali ile elde edilebilecek bilgidir. Örneğin yukarda bahsedilen "ipconfig /all" gibi bir komut ile yerel ip bilgileri elde edilebilir. Resim 3.6'da Windows komut satırına komut gönderip sonuçlarını casus yazılıma aktaran "shellKomutuCalistir()" fonksiyonuna ait kodlar sunulmuştur. Söz konusu fonksiyona "ipconfig /all" gibi komut ve parametreler gönderilerek çeşitli sistem bilgileri elde edilebilmektedir.

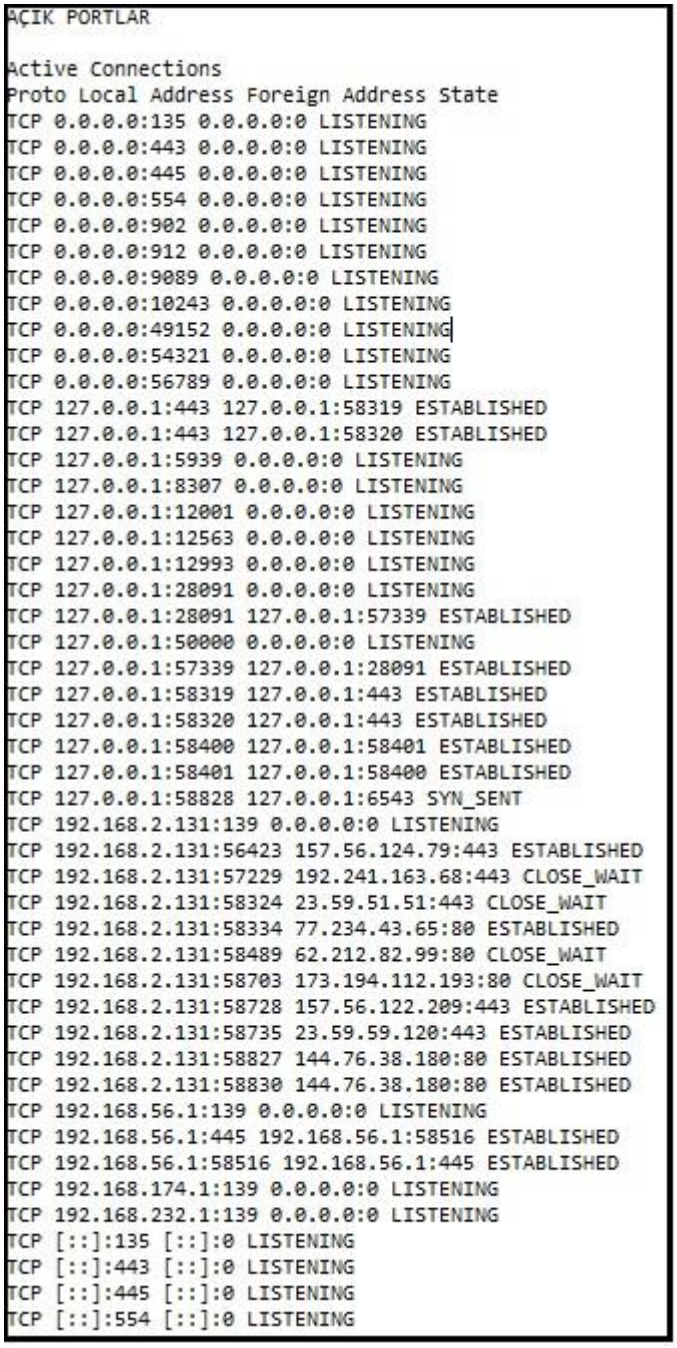


Resim 3.6. Windows komut terminaline komut göndererek sonuçlarını alan fonksiyon

3.6.4. Açık port bilgileri ve kurulan ağ bağlantı bilgilerinin edinilmesi

Ağ portları programların ağ üzerinden iletişim gerçekleştirdikleri geçiş kapılarıdır. Herhangi bir program dışardan erişim beklediğinde bir ağ portunu kendisine tahsis eder ve ilgili porttan gelecek iletişimi bekler. Örneğin "MYSQL" veritabanı sunucu servisi 3309 numaralı portu dinlemeye açarak gelen bağlantıları bekler. Programlar için gerekli olan açık ağ portları aynı zamanda önemli bir güvenlik açığı olarak da görülür. Çünkü açık portlar yetkisiz kişilerin sisteme girebilecekleri bir kapı görevi de görebilirler.

Mevcut ağ bağlantıları da kullanıcı hakkında önemli bilgiler verir. Örneğin bir kullanıcının herhangi bir IP adresi ile 3309.port numarası üzerinden iletişime geçmesi o kullanıcının yüksek ihtimal ile bir MYSQL veritabanı ile bağlantı kurduğunu gösterir. Özellikle kurumsal bir yerde MYSQL veritabanına ait IP bilgisinin saklanması gerektiği göz önüne alındığında kullanıcıya ait yapılmış bağlantıların bilgilerinin önemi daha iyi anlaşılmaktadır. Sunucu IP adresleri, iletişim kurulan ağ portları gibi bilgiler kurumsal sistemlerde kritik olarak değerlendirilirler.



Şekil 3.5. Casus yazılımın sistemden edindiği ağ ve port bilgilerine ait bir örnek

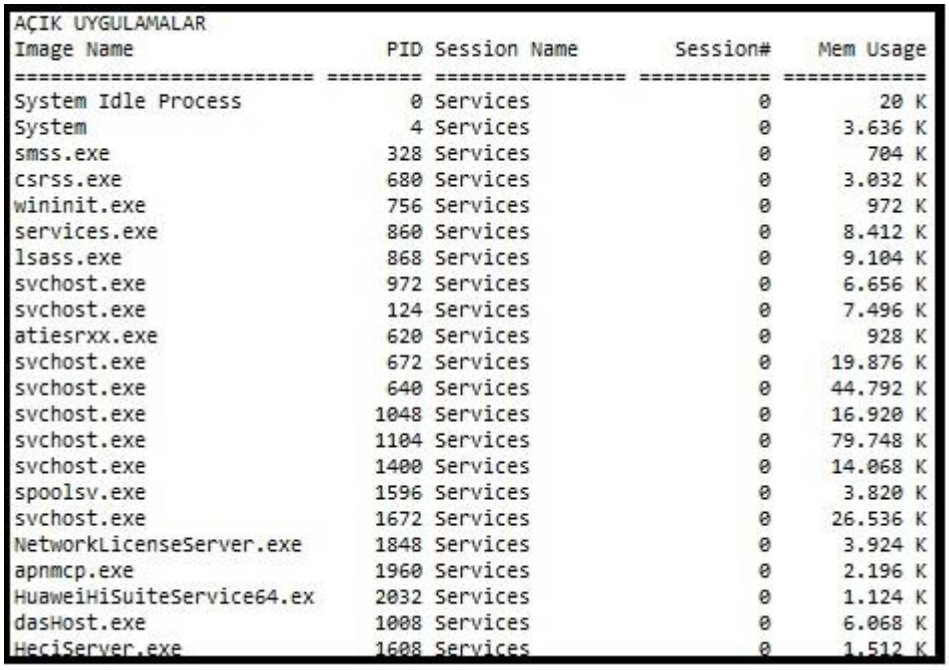
Casus yazılım yukarda ifade edilen ağ port bilgileri ile kurulan iletişim bilgilerini “shellKomutuCalistir()” fonksiyonunu kullanarak sisteme "netstat -an" komut ve parametresini gönderir. “netstat” komutu “-an” parametresi ile kullanıldığında bilgisayarda dinleme durumunda bulunan port bilgilerini, kurulu olan ağ bağlantı bilgilerini (yerel ip, yerel port, karşı tarafa ait IP ve karşı tarafa ait port bilgileri ile birlikte) döndürür. Casus yazılımın kurulu olduğu bilgisayarda IPV6 ağı mevcutsa aynı tür bilgiler IPV6 ağı içinde elde edilmektedir. Dönen bu bilgiler bilgisayara ve bilgisayarın iletişim içinde olduğu

ağlara ait kritik bilgiler sağlar. Şekil 3.5'te casus yazılım tarafından yukarıda ifade edildiği şekilde elde edilerek eposta ile iletilen örnek bilgiler sunulmuştur. Casus yazılımlar bu gibi bilgileri elde ederek aşağıdaki riskleri oluştururlar;

- Girilen web sayfalarına ait IP bilgileri aracılığı ile hangi web sitelerine girildiği bilgisi edinilebilir
- Açık ağ portu bilgilerinin elde edilmesi ile açık portlar üzerinden gerçekleştirilebilecek saldırılara maruz kalınma riski mevcuttur,
- Port bilgileri aracılığı ile bilgisayarın ne tür sunuculara bağlı olduğu bilgisi edinilebilir. Örneğin bilgisayar ağ üzerinden başka bir bilgisayara 1521 numaralı port üzerinden bağlanıyor ise karşı bilgisayarın yüksek olasılıkla "Oracle" veritabanı sunucusu olduğu bilgisine ulaşılabilir. Sonuç olarak özellikle kurumsal ağlarda ağa bağlı bir bilgisayar üzerindeki casus yazılım ile söz konusu kurumsal ağda bulunan önemli sunuculara ait bilgiler (ne tür sunucular oldukları, hangi portları kullandıkları vb.) elde edilebilir,

3.6.5. Çalışan uygulama bilgilerinin edinilmesi

Casus yazılım geliştiricilerinin elde etmek isteyebilecekleri bir diğer bilgi türü ise çalışan uygulama bilgileridir. Windows işletim sistemi kullanıcılarının "CTRL+ALT+DEL" tuş kombinasyonu ile ulaştıkları "Görev Yöneticisi" yazılımı aracılığıyla çalışan uygulamalara ait bilgiler elde edilebilmektedir. Geliştirilen casus yazılım ""shellKomutuCalistir()" fonksiyonu aracılığı ile Windows komut terminaline "tasklist" komutunu göndererek çalışan uygulama bilgilerini elde eder.



```
AÇIK UYGULAMALAR
Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0         20 K
System                           4 Services                   0      3.636 K
smss.exe                       328 Services                   0        704 K
csrss.exe                      680 Services                   0      3.032 K
wininit.exe                    756 Services                   0        972 K
services.exe                   860 Services                   0      8.412 K
lsass.exe                      868 Services                   0      9.104 K
svchost.exe                    972 Services                   0      6.656 K
svchost.exe                    124 Services                   0      7.496 K
atiesrxx.exe                   620 Services                   0        928 K
svchost.exe                    672 Services                   0     19.876 K
svchost.exe                    640 Services                   0     44.792 K
svchost.exe                   1048 Services                   0     16.920 K
svchost.exe                   1104 Services                   0     79.748 K
svchost.exe                   1400 Services                   0     14.068 K
spoolsv.exe                   1596 Services                   0      3.820 K
svchost.exe                   1672 Services                   0     26.536 K
NetworkLicenseServer.exe      1848 Services                   0      3.924 K
apnmcp.exe                    1960 Services                   0      2.196 K
HuaweiHiSuiteService64.ex     2032 Services                   0      1.124 K
dasHost.exe                   1008 Services                   0      6.068 K
HeciServer.exe                1608 Services                   0      1.512 K
```

Şekil 3.6. Casus yazılımın sistemden edindiği uygulama bilgilerine ait bir örnek

Casus yazılımın “tasklist” komutunu “shellKomutuCalistir()” fonksiyonuna göndererek elde etmiş olduğu uygulama bilgilerinin bir kısmına ait örnek Şekil 3.6’da sunulmuştur. Elde edilen bu bilgiler casus yazılım tarafından geliştiricisinin tanımlamış olduğu eposta adresine gönderilir.

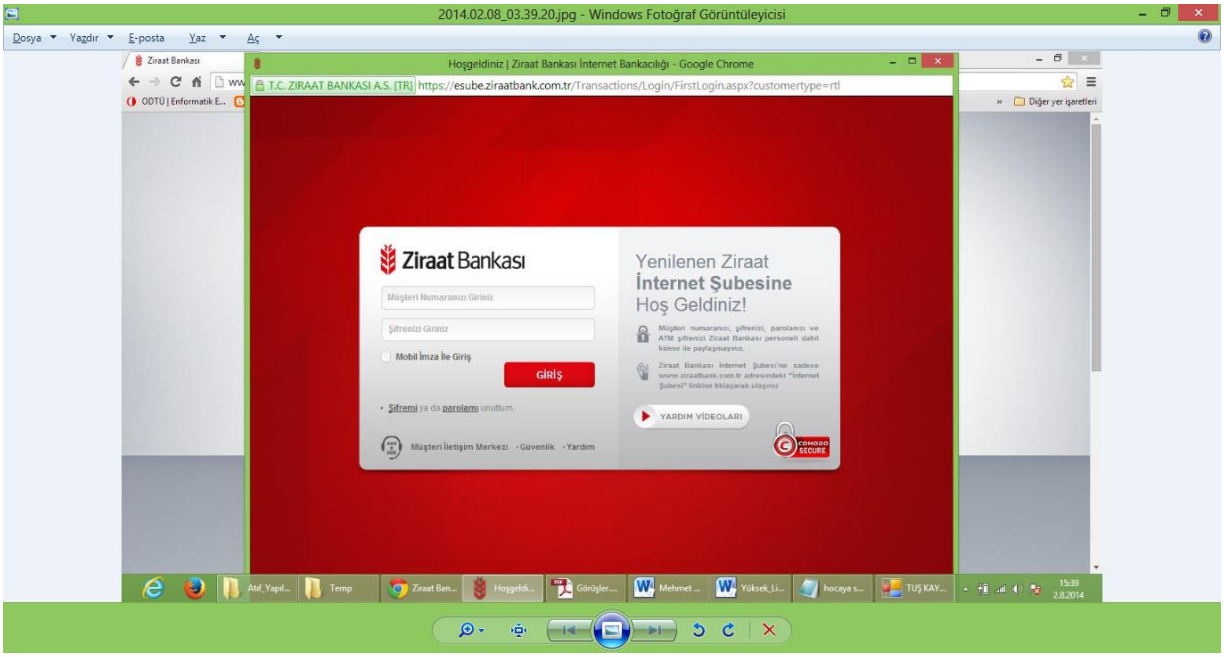
Bilgisayarda çalışan uygulama bilgilerinin ele geçirilmesi özellikle kurumsal yerlerde çalışan kullanıcıların işlerine özgü kullandıkları uygulamaların neler olduğunun anlaşılması riskini oluşturur. Örneğin “devenv.exe” uygulamasının çalışıyor olması kullanıcının “Visual Studio” ortamında geliştirme yapıyor olduğunu, “toad.exe” uygulamasının çalışıyor olması kullanıcının yüksek ihtimal ile “Oracle” veritabanı ile çalıştığının anlaşılmasına neden olur.

3.6.6. Bilgisayar ekran görüntülerinin elde edilmesi

Kullanıcılar için önemli risklerden birisi de bilgisayar ekran görüntülerinin ele geçirilmesidir. Temelde kullanıcının kendi isteği ile “PrintScreen” tuşuna basarak bilgisayarın o anki ekran görüntüsünün hafızaya alınmasını ve daha sonra kullanılmasını sağlayan özelliğe benzer olarak casus yazılımların ekran görüntüsünü kullanıcının isteği dışında elde ettikleri bilinmektedir. Elde edilen bu görüntüler e-posta veya internet

üzerinden casus yazılım geliştiriciye ulaştırılabileceği gibi, bilgisayarda gizli bir klasörde saklanması da mümkündür.

Eğitim amaçlı geliştirilen casus yazılımda ekran görüntüsünün elde edilebilirliğinin kanıtlanması amaçlandığından elde edilen görüntüler e-posta adreslerine gönderilmemektedir. Bunun yerine Bölüm 2.2.4'te de ifade edilen DUQU yazılımının kullandığı yönteme benzer bir şekilde, elde edilen resimler işletim sisteminin "%TEMP%" klasörüne kaydedilmektedir. Resim 3.7'de kaydedilen resimlere ait bir örnek sunulmuştur.



Resim 3.7. "TEMP" klasörüne kaydedilen örnek ekran görüntüsü

Casus yazılımın parametre ayarlama ekranında belirtilen sıklıklarla ekran resmi çekilir ve kaydı gerçekleştirilir. Ekran resimlerine ait dosya isimleri çekildikleri tarih ve saat bilgisinden oluşmaktadır. Böylece incelenmek istediklerinde sistematik bir şekilde incelenmeleri mümkün olabilir. Casus yazılımlar tarafından Ekran resimlerinin elde edilmesi kullanıcılar açısından aşağıdaki riskleri oluşturmaktadır;

- Kullanıcıların klavye bilgi girişi gerektirmeyen doküman inceleme, e-posta okuma, web sayfası inceleme gibi çalışmaları esnasında, incelenen dokümanların ekran görüntülerinin casus yazılım geliştiricilerin eline geçme riski bulunmaktadır,
- Kişilere ait video, resim gibi multimedya unsurlarına ait ekran görüntülerinin ele geçme riski bulunmaktadır,

- Sahipleri açısından kritik olabilecek proje, çizim, tasarım gibi çalışmaların ele geçirilebilmesi riski bulunmaktadır,
- Son zamanlarda “keylogger” yazılımları için bir önlem olarak geliştirilen sanal klavye uygulamalarından yeterince güvenli olmayan sanal klavyeler ile gerçekleştirilen işlemlerin takip edilebilme riski bulunmaktadır. Örneğin sanal klavye uygulaması her düğmesine basıldığında tuşları gizleme ve sonrasında tuş kombinasyonunu değiştirme özelliği barındırmıyorsa, sanal klavye uygulaması casus yazılımın ekran çekme özelliğine karşı etkisiz kalacaktır. Casus yazılım geliştiricilerin bankacılık aktivitelerini hedef aldığı durumda (Açık pencere başlık bilgisi içinde “bank”, “banka” gibi kelimelerin geçtiği durumları kontrol eden algoritmalar ile) ekran resim çekme sıklığını oldukça arttırabilecekleri ve bu şekilde sanal klavye güvenliğini aşabilecekleri dikkate alınması gereken bir durumdur.

3.6.7. Toplanan bilgilerin e-Posta veya web üzerinden gönderilmesi

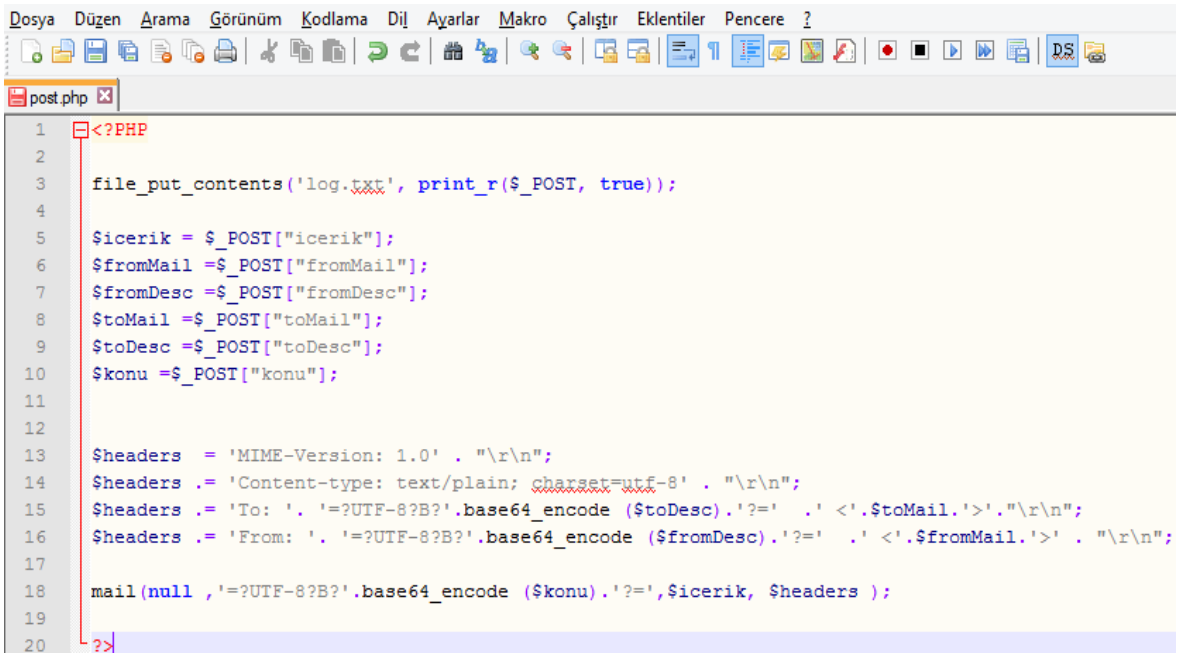
Casus yazılımlar, geliştirilme amaçları gereği edindikleri bilgileri yazılımcılarına çeşitli yöntemlerle gönderirler. Aksi halde toplanan bilgiler yazılımcısı (veya kullanmakta olan siber suçlu) tarafından kullanılamayacağından herhangi bir anlam ifade etmeyecektir. Bu kapsamda birçok casus yazılımın kullandığı yöntem olan bilgileri e-posta üzerinden gönderme özelliği bu çalışma kapsamında geliştirilen uygulamaya eklenmiştir. Casus yazılım çekilen ekran görüntüsü dışındaki tüm topladığı bilgileri e-posta ile göndermektedir.

E-posta gönderiminde yaygın olarak kullanılan 25 numaralı port, kimlik doğrulamasını zorunlu tutmadığından “SPAM” olarak ifade edilen istem dışı e-postaların gönderimi için kullanılmaktadır. Ancak ülkemizde internet servis sağlayıcılığı hizmeti veren TTNET, VODAFONE gibi firmalar yaptıkları duyurular ile Bilgi Teknolojileri Kurumu (BTK) koordinasyonu neticesinde “SPAM” e-posta ile mücadele etmek için “25 numaralı portların erişime kapatılması” uygulamasına geçildiğini ifade etmişlerdir. Bu nedenle e-posta gönderimi için ülkemizde, kimlik doğrulaması ile e-posta gönderiminin mümkün olduğu 587 numaralı port gibi birkaç port kullanılabilmektedir.

Casus yazılım içinde geliştirilen bir modül aracılığıyla, 587.port üzerinden kimlik doğrulama yöntemiyle e-posta gönderilebilmesi sağlanmaktadır. Resim 3.9’da e-posta ile ilgili parametreler bulunmaktadır. Bu örnekte e-posta sunucusu olarak "Gmail" seçilmiştir.

İlgili e-posta sunucusunda açılacak bir hesap üzerinde aşağıdaki formda belirlenen aralıklarla yukarıdaki bilgiler belirlenen e-posta adresine gönderilmektedir.

Gelişen bilgi güvenliği farkındalığı ile birlikte özellikle kurumsal sistemlerde casus yazılımların sistemlerden elde ettikleri bilgileri e-posta portları (SMTP:25, POP3:110, IMAP:143, SMTP (SSL): 465, MSA:587) üzerinden gönderdikleri bilindiğinden söz konusu e-posta gönderimine ilişkin portlar engellenmektedir. Bu önlem casus yazılımlar çalışsa bile toplanan bilgilerin gönderilememesi sonucu bilgi güvenliği açısından riskleri azaltmaktadır. Ancak bu tür önlemlere rağmen casus yazılım geliştiricilerin bilgileri sistemlerden dışarı çıkartmak için kullanabilecekleri alternatif bir yöntem, bu çalışma kapsamında geliştirmiş olan casus yazılıma kazandırılmıştır.

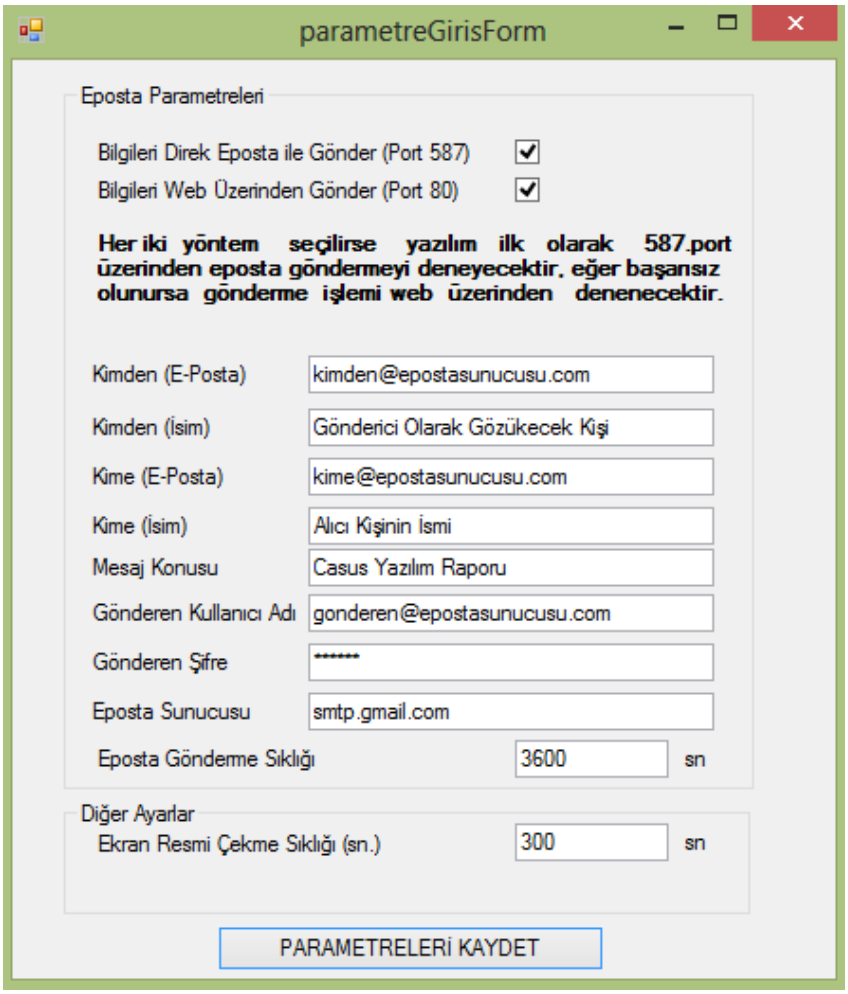


Resim 3.8. Web üzerinden e-posta gönderimini sağlayan "post.php" dosyası

Alternatif yöntem temelde casus yazılımın topladığı bilgileri ilgili eposta sunucusuna göndermek yerine bilgileri ve bilgilerin gönderileceği e-posta bilgilerini casus yazılım geliştiricisinin kontrolünde bulunan bir web sunucusuna gönderme esasına dayanmaktadır. Böylece 80. port olan web erişim portunun halen birçok kurumsal ağlarda engellenmediği dikkate alındığında casus yazılımın, bilgileri 80.port üzerinden bir web sunucusuna göndermesinin daha kolay olacağı değerlendirilebilir. Alternatif yönteme ilişkin akış aşağıdaki şekilde gerçekleşir;

1. Casus yazılım topladığı bilgileri 587. Port üzerinden detay bilgileri parametre giriş ekranında girilen eposta adresine göndermeyi dener,

2. Erişimin engellenmesi gibi bir durumdan dolayı başarısız olunması durumunda, alternatif gönderim yöntemi denenir,
3. Alternatif yöntemin çalışabilmesi için "PHP" tabanlı bir web sunucusunda bulunan "post.php" dosyasının aktif olması gerekmektedir, söz konusu "php" dosyası özel bir web sunucusunda bulunmaktadır. "post.php" dosyasına ait kaynak kod Resim 3.8'de sunulmuştur. Alternatif yöntem çalıştırıldığında casus yazılımın bu sunucuya erişmesi için ilgili sunucu casus yazılımda tanımlanmıştır.
4. Bu çalışma kapsamında geliştirilen casus yazılım topladığı bilgileri ve alıcı e-posta bilgilerini 3.madde de belirtilen web sunucusuna gönderir,
5. Web sunucusunda bulunan "PHP" dosyası kendisine gelen bilgileri üzerinde bulunduğu sistemde yer alan e-posta sunucuları aracılığıyla, yine kendisine gelen e-posta adresine gönderir.



Resim 3.9. Bilgilerin E-posta ile gönderilmesini sağlayan parametre ekranı

Bu çalışma kapsamında geliştirilen casus yazılım bilgileri hangi e-posta adresine ne sıklıkla göndereceği gibi bilgileri barındıran bir örneği Resim 3.13'te sunulan parametre dosyası ile birlikte kurulmalıdır. Ancak bu dosya oluşturulmadan casus yazılım çalıştırılırsa casus yazılımın ilk çalıştığı anda Resim 3.9'da sunulan parametre ekranındaki bilgilerin doldurulması istenir. Dolayısıyla söz konusu bilgiler casus yazılımın kurulduğu esnada kuran kişi tarafından girilmelidir. Formda iki adet "checkbox" bulunmaktadır, bunlardan ilki bilgilerin 587.port üzerinden e-posta adresine gönderilmesini sağlayacak olan onay kutusudur, ikincisi ise bilgilerin web üzerinden gönderilmesini sağlayacak olan onay kutusudur. Her iki onay kutusunun seçilmesi durumunda casus yazılım öncelikle 587.port üzerinden göndermeyi deneyecektir, başarısız olması durumunda web üzerinden (80.port) göndermeyi deneyecektir. Parametre formunda istenen diğer parametrelere ilişkin açıklamalar aşağıda sunulmuştur;

Kimden (E-Posta) :Casus yazılımın bilgileri göndereceği e-postada gönderen e-posta adresi olarak gözükecek adrestir.

Kimden (İsim) :Gönderilecek e-posta üzerinde gönderici olarak gösterilecek isim. Bu bilgi sistematik bir şekilde bilgi toplamak istendiği durumda kullanışlı olabilir. Örneğin bir siber suçlunun birden çok bilgisayara casus yazılım yüklemesi durumunda toplanan bilgilerin iletildiği e-postaların birbirinden ayrılması bu özellik sayesinde mümkün olabilir.

Kime (E-Posta) : Toplanan bilgilerin gönderileceği E-posta adresinin belirlendiği parametredir.

Kime (İsim) :Toplanan bilgilerin gönderileceği E-posta adresine ait isim bilgisidir.

Mesaj Konusu : Gönderilecek olan E-posta adresinin konu kısmının belirlendiği parametredir. Gönderici ismi gibi bu parametre de birçok yerden bilgi toplandığı durumlarda gelen e-postaların ayırt edilebilmesi için önemlidir.

Gönderen Kullanıcı Adı : Bilgiler "587" numaralı port üzerinden gönderilirken kullanılan bu parametre, e-posta sunucusu ile gerçekleştirilen kimlik doğrulama işleminde kullanılmaktadır. Birçok e-posta sunucusunda e-posta adresi ile aynı olmasına karşın ilave güvenlik sağlamasından dolayı bazı e-posta sunucularında e-posta adresinden farklı olabilmektedir.

Gönderen Şifre: E-posta sunucusu ile gerçekleştirilen kimlik doğrulama işleminde kullanılmakta olan bir parametredir.

E-posta Sunucusu: Gönderici e-posta adresinin kayıtlı olduğu sunucu bilgisi bu parametre ile kaydedilmektedir. “E-posta Sunucusu”, “Gönderen Kullanıcı Adı” ve “Şifre” parametreleri, “web (80.port)” üzerinden gönderimin yapıldığı durumda kullanılmazlar. “Web” üzerinden gönderimi sağlayan “php” dosyası web sunucusuna ait e-posta sunucusu üzerinden gönderim yaptığından söz konusu parametreler kullanılmaz.

3.6.8. Casus yazılımın bilgisayar açılışında otomatik çalışması

Zararlı yazılımların ortak özelliği bilgisayar başlatıldığında sistem başlangıç ayarlarına kendilerini yerleştirerek otomatik başlamalarıdır. Otomatik başlama özelliğini edinmedikleri takdirde zararlı yazılımlar, bilgisayar yeniden başlatıldığında işlevlerini kaybedeceklerdir.

```
//Zamanlanmış Görev Kaydı Oluşturuluyor
String sonuc = posta.shellKomutuCalistir("schtasks", "/create /tn My_App /tr " + kopyalanacakYer +
    " /sc onstart /f /DELAY 0000:10");

//Sistem Kayıtlarına Otomatik Başlanması İçin Gerekli Girdi Yapılıyor
RegistryKey key = Registry.CurrentUser.OpenSubKey(@"Software\Microsoft\Windows\CurrentVersion\Run", true);
key.SetValue("cy", "\"" + Application.ExecutablePath + "\"");
```

Resim 3.10. Casus yazılımın sistem başlatılırken çalışmasını sağlayan kodlar

Bu çalışma kapsamında geliştirilen casus yazılım, bilgisayar her açıldığında başlaması için sistem başlangıcına yerleşecek şekilde tasarlanmıştır. Otomatik başlama işlemi Resim 3.10’da sunulan kodlar aracılığı ile iki farklı şekilde sağlanmaktadır. İlk yöntem sistem başlangıcında çalışacak şekilde “Registry” ayarlarının güncellenmesidir. İkinci yöntem ise kendisini "schtasks" sistem komutunu kullanarak bilgisayarın zamanlanmış görevler listesine eklemesidir. İkinci yöntemde casus yazılımın başlaması, bilgisayar açıldıktan 10 saniye sonrasında gerçekleşecek şekilde programlanmıştır.

3.6.9. Ortam dinlemesi için ses kaydı

Güncel bir konu olan ortam dinlemelerinin çoğunluklu cep telefonları kullanılarak yapıldığı düşünülmektedir. Ancak günümüzde hemen hemen her bilgisayarda bulunan

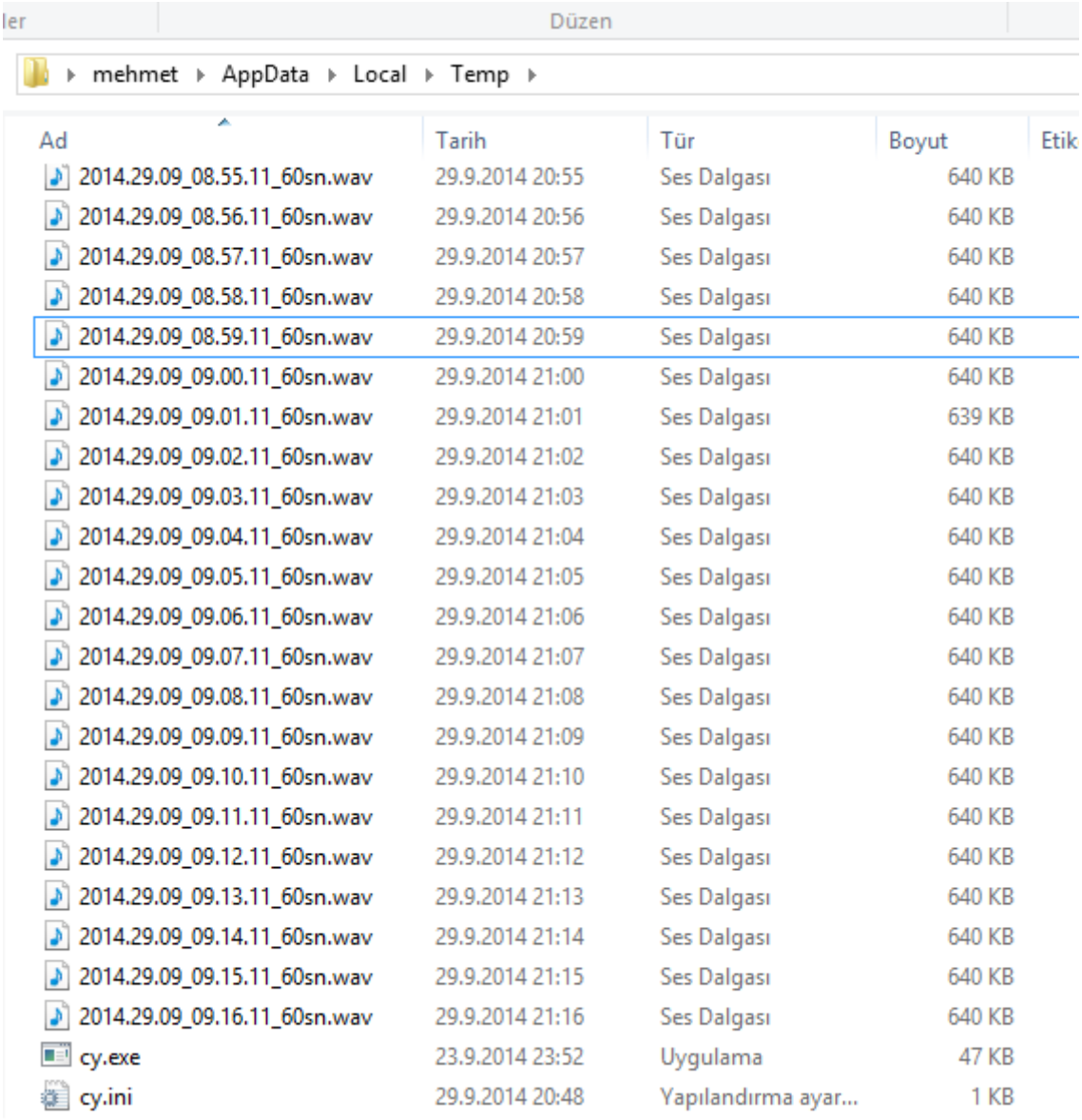
mikrofonlar, casus yazılımlar kullanılarak ortam dinlemesini mümkün kılmaktadır. Casus yazılımların yayılma potansiyeli ve mikrofon taşıyan bilgisayarların ev, iş, eğlence ortamlarındaki yaygınlığı dikkate alındığında ortam dinleme riskinin boyutları daha iyi anlaşılabilmektedir.

Söz konusu riski daha iyi anlayıp analiz edebilmek için geliştirilen casus yazılıma ortam dinlemesi yapmak üzere ses kaydı özelliği eklenmiştir. "Windows" işletim sistemlerinde standart olarak bulunan "winmm.dll" dosyası içinde tanımlı olan "mciSendStringA" fonksiyonunu kullanarak birer dakikalık aralıklarla ses kaydı alınmakta olup kaydın bittiği tarih ve saat bilgisi dosya ismi olarak atanmaktadır. Bir dakikalık ses kaydı, casus yazılımın dosyalarının yer aldığı işletim sisteminin "TEMP" klasörüne kaydedilmektedir. Ses kaydı özelliğini sağlayan kodlar Resim 3.11'de sunulmuştur. Ses kaydına ait "bitspersample", "samplespersec", "bytespersec" gibi özellikler de ayarlanabilmektedir.

```
private void sesKaydıBaslat()
{   mciSendString("open new Type waveaudio Alias recsound wait", "", 0, 0);
    mciSendString("record recsound", "", 0, 0);
    log.Text += "\r\n" + DateTime.Now.ToString() + " Ses Kaydı Başlatıldı ";
}//end of seskaydıbaslat
private void ses_Tick(object sender, EventArgs e)
{   String sesIsmi = Environment.GetEnvironmentVariable("Temp") + @"\" +
                DateTime.Now.ToString("yyyy.dd.MM_hh.mm.ss") + "_60sn.wav";
    mciSendString("save recsound "+sesIsmi+"", "", 0, 0);
    mciSendString("close recsound ", "", 0, 0);
    log.Text += "\r\n" + DateTime.Now.ToString() + " Ses Kaydı "+ sesIsmi+
        " dosyasına kaydedildi.";
    sesKaydiBaslat();
```

Resim 3.11. Ses kaydı özelliğini sağlayan kodlar

Ses kaydı işlemi sonucu "TEMP" klasöründe oluşan ses kayıt dosyaları Resim 3.12'de sunulmuştur. Her bir ses kaydı 60 saniyelik olup ortalama boyutu 640 KB boyutundadır. Ancak "Winrar" programı kullanılarak sıkıştırma işlemi gerçekleştirildiğinde boyut 140 KB olmaktadır.



Resim 3.12. Casus yazılımın "TEMP" klasöründe oluşturduğu ses kayıt dosyaları

Ses kaydı dosyalarının sürekli olarak e-posta ile gönderilmesi bilgisayarın kullandığı bant genişliğini azaltacağından dosyaların "TEMP" klasörüne kaydedilmesi tercih edilmiştir.

3.6.10. Ortam izlemesi için görüntü kaydı

Ortam dinlemesi gibi ortam izleme özelliği de önemli bir risk olarak değerlendirilmektedir. Söz konusu riskin daha iyi anlaşılabilmesi için bilgisayar üzerindeki kamera kullanılarak görüntü kayıt özelliği casus yazılıma eklenmeye çalışılmıştır.

Casus yazılımın bilgisayar üzerindeki kamerayı kullanarak görüntü elde edebilmesi amacıyla "Windows" işletim sistemlerinde bulunan "avicap32.dll" dosyası üzerinde

çalışılmıştır. Ortam görüntü kaydı için bir dakikalık aralıklarla kameradan görüntü alınması hedeflenmiştir. Ancak “Windows 8” işletim sistemi üzerinde gerçekleştirilen testlerde “avicap32.dll” dosyası kullanıldığında, ilk görüntünün “avicap32.dll” tarafından sağlanabildiği sonraki dakikalarda ise aynı dosyanın içinde yer alan fonksiyonların görüntü sağlayamadığı görülmüştür. Bu problemin sistem yeniden başlatılana kadar devam ettiği görülmüştür. Dolayısıyla “avicap32.dll” dosyasının “Windows 8” işletim sisteminde uyumlu çalışmadığı tespit edilmiş, söz konusu dosya kullanılarak görüntü kaydı özelliği casus yazılıma eklenmemiştir.

Kamera görüntülerini elde etmek için kullanılabilecek bir diğer yöntemde üçüncü parti yazılımların kullanılmasıdır. Ancak üçüncü parti yazılımların casus yazılıma eklenebilmesi için gerekli olan ilave dosyalar (sınıflar, kütüphaneler, dll dosyaları vb.) yaygın olarak kullanıldıklarından ve casus yazılımın boyutunu arttırdıklarından dolayı casus yazılımların koruyucu yazılımlar tarafından tespit edilmesine neden olmaktadır.

Sonuç olarak ortam izlemesi için görüntü kaydı özelliği casus yazılıma eklenmemiştir.

3.7. Casus Yazılımın Kodlanması

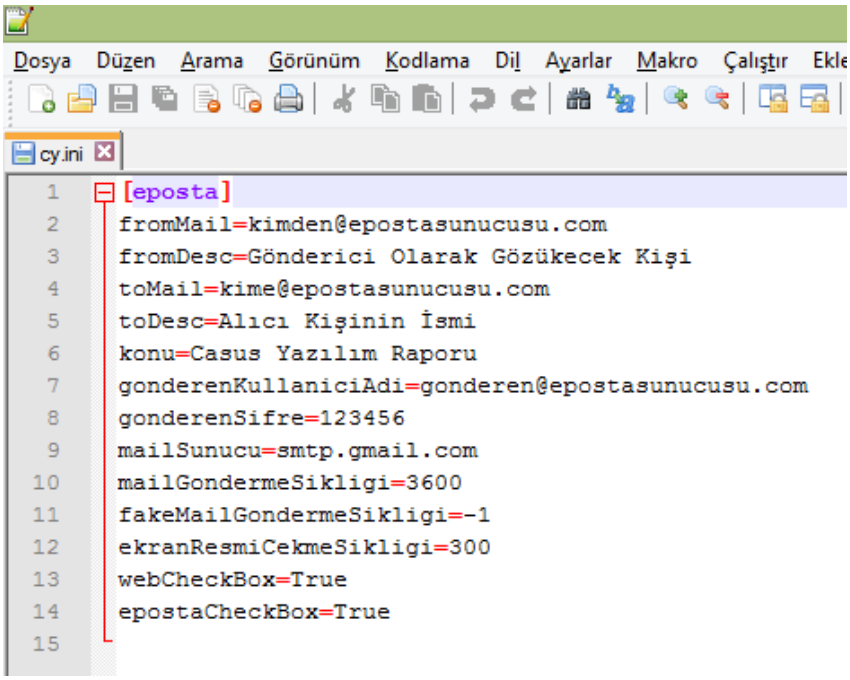
Casus yazılım uygulaması Microsoft firmasına ait "Visual Studio 2010" aracı kullanılarak C# dilinde geliştirilmiştir. Ayrıca geliştirme sürecinde “Nesne Yönelimli Programlama" (İng. ObjectOriented Programming) kuralları uygulanmıştır. Yukarıda tanımlanan işlevler sınıflara ayrılarak programlamanın daha sistematik yapılması sağlanmıştır.

Mevcut casus yazılımın antivirüs programları tarafından tanınarak imza veritabanlarına eklenmesi durumunda, sınıflara ayrılmış kodların çok az bir değişiklikle koruyucu yazılımların tanıyamayacağı bir hale gelmesi mümkündür. Ayrıca daha sonradan eklenmesine ihtiyaç duyulabilecek bazı özelliklerin nesne yönelimli programlama teknikleri ile yazılmış kodlara eklenmesi çok daha kolaydır. Casus yazılımı oluşturan başlıca sınıflar şu şekildedir;

- "Pencere.cs" : Açık pencere (uygulama) başlık bilgilerini işleyerek sistem kayıtlarına işler. Kullandığı temel sistem fonksiyonu "GetForegroundWindow()".
- "Tus.cs": Temel tuş kayıtlama (KEYLOGGER) işlemlerini gerçekleştiren sınıftır. Kullandığı temel sistem fonksiyonu "GetAsyncKeyState" olup bu fonksiyonu

kullanan başka fonksyionlar geliştirilmiştir. Bu sınıf içinde özellikle Türkçe tuşlara (ş,ğ,ü,ö,ç) yönelik özel tanımlamalar yapılması gerekmiştir.

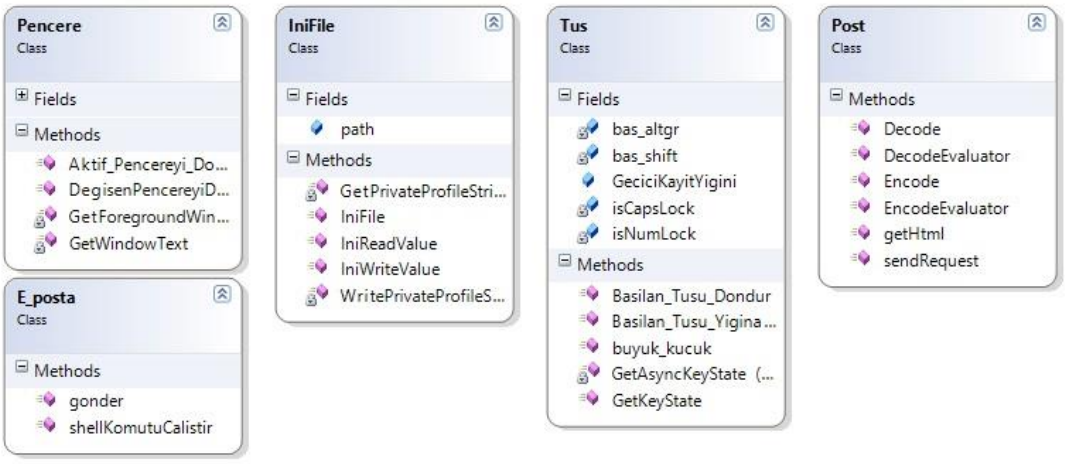
- "E-Posta.cs":Bu sınıf toplanan bilgilerin 587 numaralı port üzerinden e-Posta olarak gönderilmesi ile ilgili işlemleri içeren fonksiyonlardan oluşmaktadır. Visual Studio C# içinde tanımlı olan "System.Net.Mail" isim uzayında bulunan "SmtpClient" sınıfını kullanır.
- "IniFile.cs" : Parametre giriş ekranı ile girilen çeşitli parametrelerin bilgisayarda "ini" dosyası olarak saklanabilmesini ve gerektiğinde saklanan parametrelerin okunabilmesini sağlayan sınıftır. Resim 3.13'te bilgisayarın "TEMP" olarak tanımlanmış klasörüne kaydedilen "ini" dosyası sunulmuştur. Aynı zamanda casus yazılımın da kaydedildiği yer olan "TEMP" klasörüne "ini" dosyası, "cy.ini" ismi ile kaydedilmekte olup bu dosya herhangi bir metin editörü (notepad, notepad++) aracılığı ile rahatlıkla görüntülenebilir. Bu çalışmada geliştirilen casus yazılım eğitim amaçlı olduğundan parametre dosyası şifrelenmemiş veya "binary" olarak ifade edilen makine dilinin anlayacağı formatta oluşturulmamıştır. Siber suçluların kendilerini ele verebilecek bu tür verileri şifreleyerek başka türde saklayabilecekleri dikkate alındığında, birçok casus yazılıma ait parametre dosyalarının işletim sistemine ait farklı yerlerde ve şifreli olacağı çıkarımı yapılabilir.



Resim 3.13. "cy.ini" dosyasına kaydedilen bilgiler

- "Post.cs" : 80 numaralı port dışında ağ portlarının engellenmiş olduğu durumlarda alternatif e-posta gönderimini sağlayan fonksiyonları içermektedir. “System.Net” isim uzayı içerisinde yer alan “HttpWebRequest” sınıfı kullanılarak çeşitli fonksiyonlar “Post.cs” içinde geliştirilmiştir. Bilgiler ilgili web sayfalarına “POST” yöntemi kullanarak gönderildiğinden, bu sınıfa da “POST” ismi verilmiştir. İçinde bulunan en önemli fonksiyon olan “sendRequest” fonksiyonu aşağıdaki parametreleri almaktadır;
    - “URL” : Uniform Resource Locator (URL) “String” olarak gelen bu parametre, iletişime geçilecek web sayfasına ait adres bilgisini içerir.
    - “dataGonder”: “Bool” veri tipinde olan bu parametre web sayfasına bilgi gönderilecekse “True” değerini alır. Örneğin geliştirilmiş olan casus yazılımda gerçek IP bilgisinin alınması için www.iplocationfinder.com web adresine istek gönderilirken herhangi bir bilgi gönderilmeyeceğinden “dataGonder” parametresi “False” olarak atanır.
    - “method” : Bilgilerin web sayfasına gönderim yönteminin atandığı parametredir. “POST” ve “GET” olarak set edilebilmektedir. Geliştirilen casus yazılımda gönderilecek verilerin fazlalığı nedeniyle “POST” yöntemi seçilmiştir.
    - “dizi” : “String” veri tipinde bir dizi olan bu parametre, iletilecek bilgileri barındıran parametredir. Dizi içinde yer alan bilgiler “method” parametresi ile belirlenen yönteme göre web sitesine yollanır.

Geliştirilen casus yazılıma ait “Visual Studio” yazılımı ile oluşturulan sınıf diyagramı Şekil 3.7’de sunulmuştur.



Şekil 3.7. Casus yazılıma ait sınıf diyagramı

4. BULGULAR

Zararlı yazılımlara karşı "antivirüs, antispyware ve firewall" gibi koruyucu yazılımlar önlem olarak düşünülmektedir. Ancak birçok koruyucu yazılımın aynı zararlı yazılıma karşı farklı tepkiler verdiği de bilinmektedir. Bu nedenle zararlı yazılımların farklı işletim sistemlerinde farklı koruyucu yazılımlara karşı test edilerek koruyucu yazılımların gerçekte ne kadar koruma sağladığının anlaşılması mümkün olabilir. Bu husus dikkate alınarak geliştirilen casus yazılım farklı işletim sistemlerinde ve farklı koruyucu yazılımlarla test edilmiştir. Test sonuçları ve testlerde elde edilen bulgular aşağıda sunulmuştur.

4.1. Casus Yazılımın İşletim Sistemlerinde Test Edilmesi

Özgün olarak geliştirilen casus yazılım Şekil 3.1'de belirtilen işletim sistemlerinden en çok kullanılan üç işletim sisteminde (Windows 7, Windows XP, Windows 8) test edilmiştir. Testler "Vmware Workstation" aracılığıyla oluşturulan sanal makinelerde gerçekleştirilmiştir. Testler yeni yüklenmiş ve işletim sistemi ile birlikte gelen programlar dışında herhangi bir programın yüklenmediği işletim sistemlerinde gerçekleştirilmiş olup varsayılan (İng. default) işletim sistemi güvenlik ayarları ile gerçekleştirilmiştir. Gerçekleştirilen test sonuçları kapsamında Çizelge 4.1'de bulunan sorular cevaplandırılmıştır.

Geliştirilen casus yazılımın bazı özelliklerinin kısıtlandığı eğitim amaçlı olarak hazırlanan bir versiyonu ve yazılıma ait bazı ekran görüntüleri http://siberdunyadaguvenlik.blogspot.com.tr/ adresinden edinilebilir.

Çizelge 4.1. İşletim sistemlerine göre casus yazılım test sonuçları

	Windows XP Pro Service Pack 3	**Windows 7 Ultimate Build 7600**	**Windows 8**
Casus yazılımın çalıştırılabilmesi için ön yüklü bir program olması gerekiyor mu?	Uygulama düzgün olarak başlatılamadı, ".NET FRAMEWORK 2.0" ve üstü kurulu olması gerekmektedir.	Hayır	Hayır
Casus yazılım kullanıcı tarafından çalıştırıldığında işletim sistemi herhangi bir ikaz veriyor mu?	Hayır	Hayır	Hayır
Casus yazılım basılan tuş bilgileri ve diğer bilgileri toplamaya başladığında işletim sistemi herhangi bir ikaz veriyor mu?	Hayır	Hayır	Hayır
Casus yazılım, topladığı bilgileri e-posta ile gönderirken işletim sistemi herhangi bir ikaz veriyor mu?	Hayır	Hayır	Hayır

4.2. Casus Yazılımın Koruyucu Yazılımlara Karşı Test Edilmesi

Özgün olarak geliştirilen casus yazılımın koruyucu yazılımlara karşı da test edilmesi gerekmektedir. Bilişim sistemleri altyapıları için güvenlik çözümleri sunan OPSWAT yazılım firması tarafından Ağustos 2013 tarihinde yayınlanan "Antivirüs Ürünlerinin Market Dağılımı" raporu ve "IEEE Computer Society-Computer" dergisinde yayınlanan bir makalede [43] yaygın olarak kullanıldığı değerlendirilen koruyucu yazılımlardan sekiz adedi seçilmiştir. Ayrıca güvenlik duvarı özelliği bulunan ve casus yazılımlara karşı tasarlanan üç adet koruyucu yazılım da çalışma kapsamına dâhil edilerek geliştirilen casus yazılım toplam 11 adet koruyucu yazılım ile test edilmiştir. Gerçekleştirilen testler 21 Haziran 2014- 10 Ağustos 2014 tarihleri arasında koruyucu yazılımların web sitelerinde yer alan ücretsiz deneme sürümleri ile gerçekleştirilmiş olup koruyucu yazılımların varsayılan ayarları kullanılmıştır. Koruyucu yazılımlar numaralandırılarak sonuçlar Çizelge 4.2'de paylaşılmıştır.

Çizelge 4.2. Koruyucu yazılımlara Göre Casus Yazılım Test Sonuçları

Koruyucu Yazılım Numarası	1	2	3, 4	5	6	7, 8, 9, 10, 11
Casus yazılım çalıştırılmadan önce herhangi bir tarama esnasında ikaz verilmiş midir?	Evet, NOT 1	Hayır	Evet, NOT 2	Hayır	Hayır	Hayır
Casus yazılım çalıştırılırken herhangi bir ikaz verilmiş midir?	Çalışmasına izin verilmemiştir	Evet, NOT 2	Çalışmasına izin verilmemiştir	Evet, NOT 4	Hayır	Hayır
Casus yazılım basılan tuş bilgileri ve diğer bilgileri toplarken herhangi bir ikaz verilmiş midir?	Çalışmasına izin verilmemiştir	Çalışmasına izin verilmemiştir	Çalışmasına izin verilmemiştir	Hayır	Evet, İnternet erişimi gerektiren işlemlerde uyarı vermiştir.	Hayır
Casus yazılım bilgileri 587.port üzerinden e-posta ile gönderirken herhangi bir ikaz verilmiş midir?	Çalışmasına izin verilmemiştir	Çalışmasına izin verilmemiştir	Çalışmasına izin verilmemiştir	Evet, NOT 5	Evet, e-posta gönderilirken uyarı vermiştir,	Hayır
Casus yazılım bilgileri 80.port üzerinden e-posta ile gönderirken herhangi bir ikaz verilmiş midir?	Çalışmasına izin verilmemiştir	Çalışmasına izin verilmemiştir	Çalışmasına izin verilmemiştir	Hayır	Evet, e-posta gönderilirken uyarı vermiştir,	Hayır

Not 1: Otomatik taramada TR/Spy.Gen olarak tespit edilmiş ve silinmiştir.

Not 2: Casus yazılımın çalışması engellenmiş olup "Trojan" olarak tespit edilmiş ve silinmiştir.

Not 3: Casus yazılımı içeren klasör açılır açılmaz, virüslü bir dosya algılandığı uyarısı verildi ve yazılım silindi.

Not 4: İlk çalıştırılma esnasında 15 saniye kadar programın incelendiğini ifade eden bir bildirim yapılmış ancak herhangi bir şey bulunamamıştır. Bu esnada casus yazılım hata mesajı (exception) vermiştir, hata mesajı onaylandıktan sonra normal çalışma devam etmiştir.

Not 5: Gönderilen e-postaya, e-postanın tarandığını ifade eden bir metin eklemiştir ancak kayıtlar başarı ile gönderilmiştir

Not 6:10 nolu yazılımın çalışması esnasında tuş kaydetme fonksiyonu bazı uygulamalarda bilgi toplayamamıştır. Ancak söz konusu koruyucu yazılım herhangi bir şekilde casus yazılımı tespit edememiş olup casus yazılım diğer işlevlerini tam olarak yerine getirmiştir.

1-Avira Antivirus Suite 14.0.3.350	**7-Norton Internet Security 21.3.0.12**
2-Kaspersky Pure 3.0	**8-Nod32 7.0.317.4 (Virüs İmza Vt. Sürüm: 10471)**
3-McAfee 12.8	**9- Windows Defender 4.5.218.0**
4-ZoneAlarm	**10- WebRootSecureAnywhere (13.07.2014 tarih)**
5-avast! Free Antivirus (2014.9.0.2021)	**11-Spybot S & D 2.4**
6-AVG Anti-Virus Free Edition	

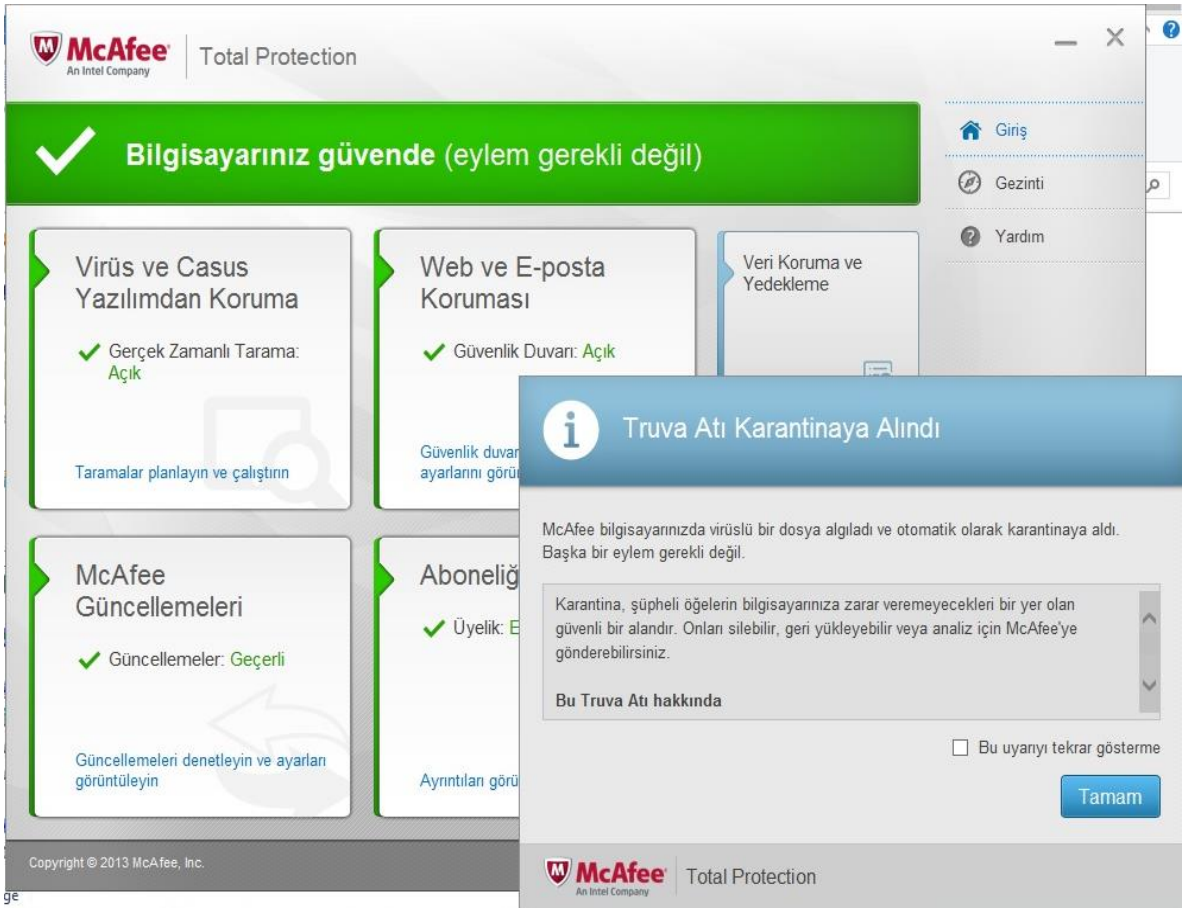
Gerçekleştirilen testlerde koruyucu yazılımlar kurulduktan sonra bir müddet beklenmiştir. Söz konusu bekleme sürecinde koruyucu yazılımların arka planda tarama yaptığı bilindiğinden ilgili taramada dosya sisteminde mevcut bulunan geliştirilmiş casus yazılımı tespit edip edemeyeceği gözlemlenmiştir. Koruyucu yazılımlardan bazıları casus yazılımı

tespit ederken bazıları tespit edememiştir. Casus yazılımı tespit edemeyen koruyucu yazılımların ilgili ekran görüntüleri Ek-2'de sunulmuştur.

Resim 4.1'de sunulan bildirim mesajına ait ekran görüntüsü geliştirilen casus yazılım çalıştırılmadan koruyucu yazılım tarafından kullanıcıya gösterilmiştir. Resim 4.1'de görülebileceği gibi koruyucu yazılım geliştirilen casus yazılımı "TR/Spy.Gen" olarak nitelemiştir. Uyarı sonrasında casus yazılıma erişim mümkün olmamıştır.

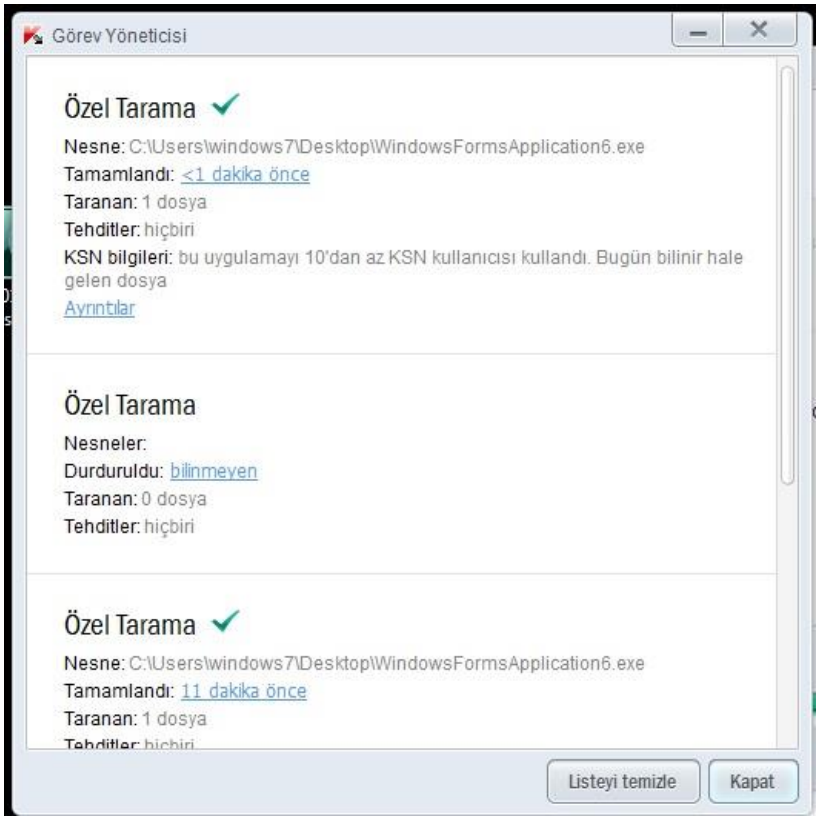
Resim 4.1. Avira yazılımının casus yazılımı tespit ettiğini belirten bildirim

Resim 4.2'de bildirimi sunulan koruyucu yazılım geliştirilen casus yazılımı arka planda yaptığı tarama esnasında tespit etmiştir. Koruyucu yazılım, geliştirilen casus yazılımı "Truva Atı" olarak tanımlamıştır.



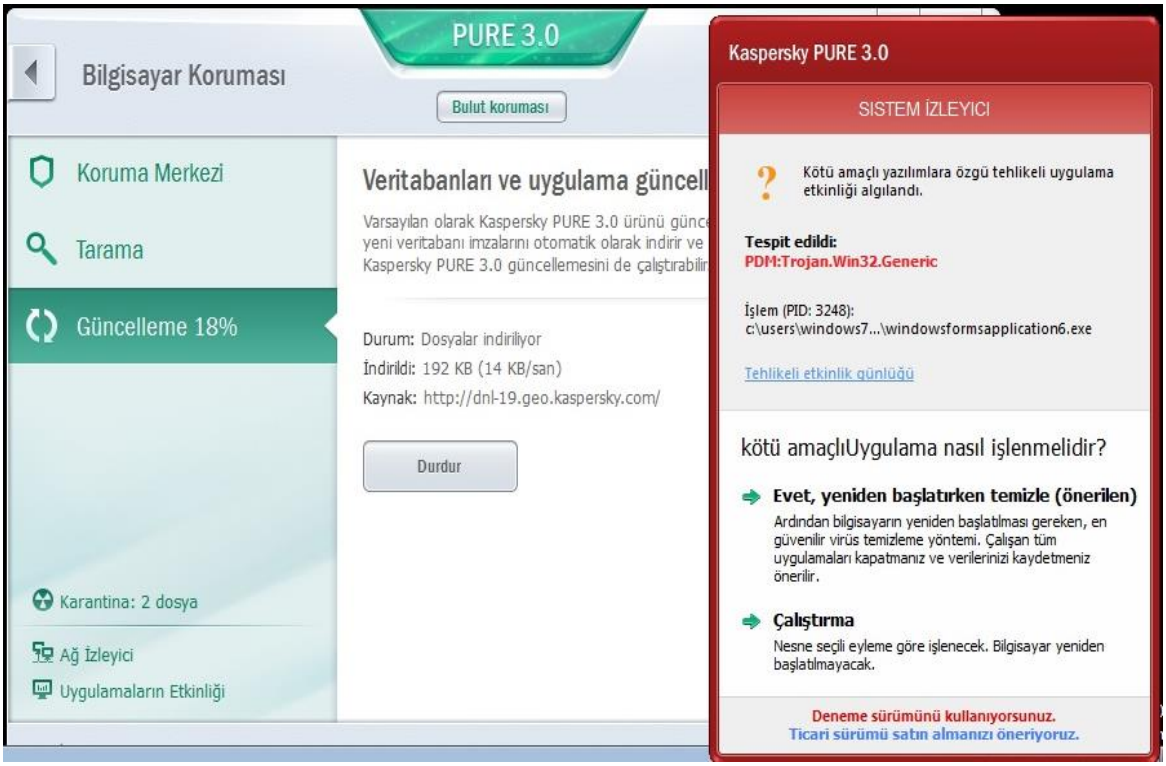
Resim 4.2. Koruyucu yazılımın geliştirilen casus yazılımı tespit ettiğini belirten bildirim

Bazı koruyucu yazılımlar işletim sisteminin aktif alanlarını inceler. Örneğin dosya sistemi, açık portlar, kullanılan işletim sistemi fonksiyonları vb. Bu inceleme sonucunda koruyucu yazılımlar işletim sisteminde çalışan uygulamalara ait gerçekleştirilen işlemleri inceleyerek, söz konusu yazılımların zararlı yazılım olup olmadıklarına ilişkin değerlendirme yaparlar. Dolayısıyla normal taramada tespit edilemeyen zararlı yazılımların, çalıştırıldıktan sonra tespit edilme durumu oluşabilmektedir. Resim 4.3'te sunulan ekran görüntüsü casus yazılımı, çalışırken tespit edebildiği halde normal tarama esnasında tespit edemeyen bir koruyucu yazılıma aittir.



Resim 4.3. Kaspersky yazılımı ile casus yazılımın taratılmasına ait sunulan sonuçlar

Resim 4.4'te sunulan ekran görüntüsü, casus yazılımın çalıştırıldıktan sonra koruyucu yazılım tarafından tespit edildiğini ifade eden bildirimi içermektedir. Koruyucu yazılım casus yazılımın aktivitelerini durdurmuştur. Casus yazılım "Trojan.Win32.Generic" olarak sınıflandırılmıştır.



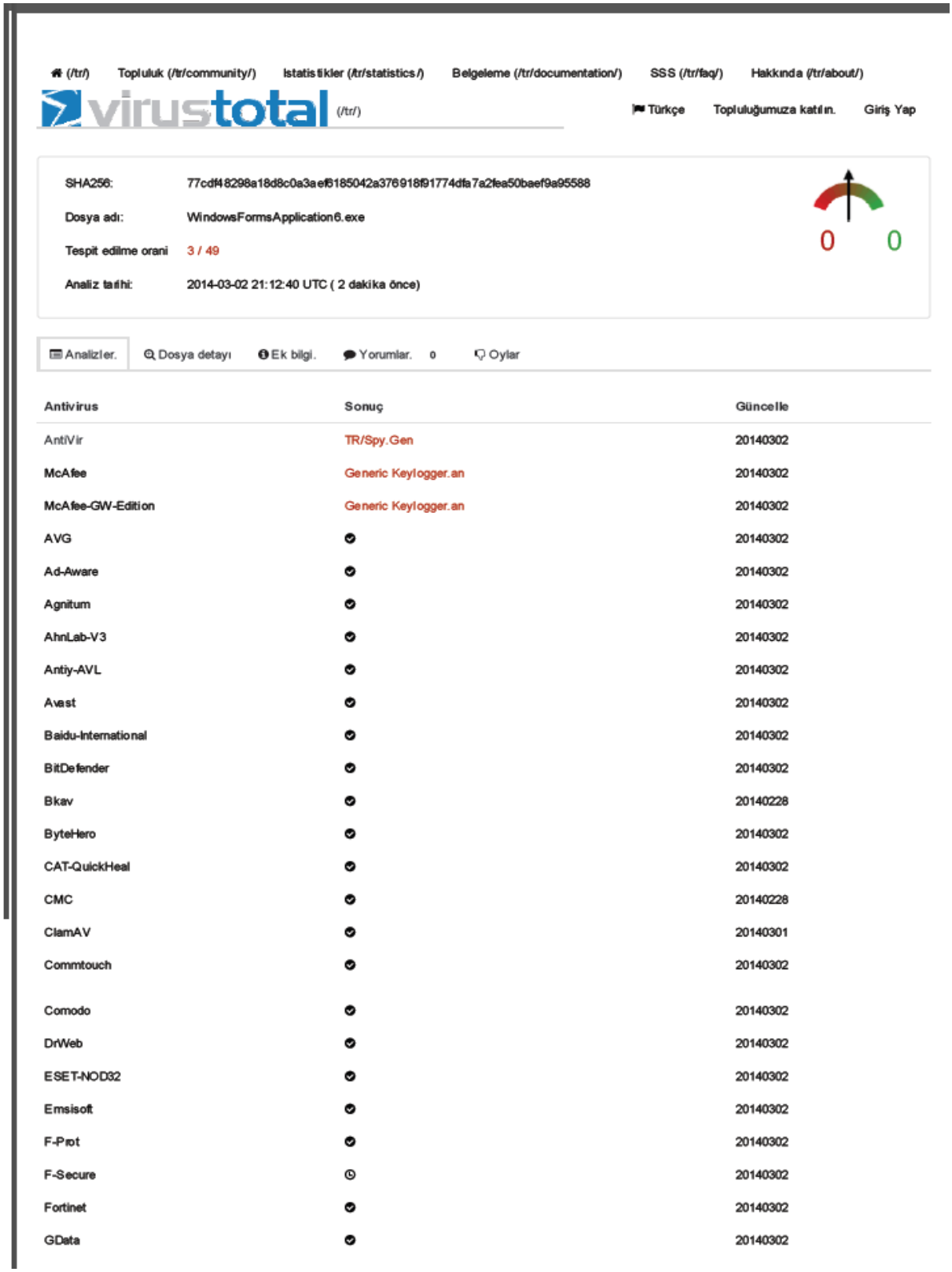
Resim 4.4. Casus yazılımın çalıştırıldıktan sonra tespit edildiğini belirten bildirim

Yukarda ifade edilen koruyucu yazılımlarla birlikte Çizelge 6.2'de belirtilen diğer koruyucu yazılımlardan güvenlik duvarı özelliği olan üç adet koruyucu yazılımın, casus yazılımı topladığı bilgileri göndermek üzere internete bağlandığı sırada tespit ettiği gözlemlenmiştir. Güvenlik duvarı özelliği sayesinde tespit edilen bu durum her zaman tespit edilen yazılımın zararlı yazılım olduğu anlamına gelmemektedir. Normal yazılımların da güncelleme, bilgi alıp gönderme gibi çeşitli nedenlerle internete bağlanma ihtiyacı duymalarından dolayı, internete bağlanma girişimi tek başına casus yazılım davranışı olarak nitelendirilebilecek bir davranış değildir. Dolayısıyla güvenlik duvarı özelliği olan koruyucu yazılımların kullanıcıya gösterdikleri uyarılar fazla olacağından, uyarılar kullanıcı açısından önem ifade etmeyebilir.

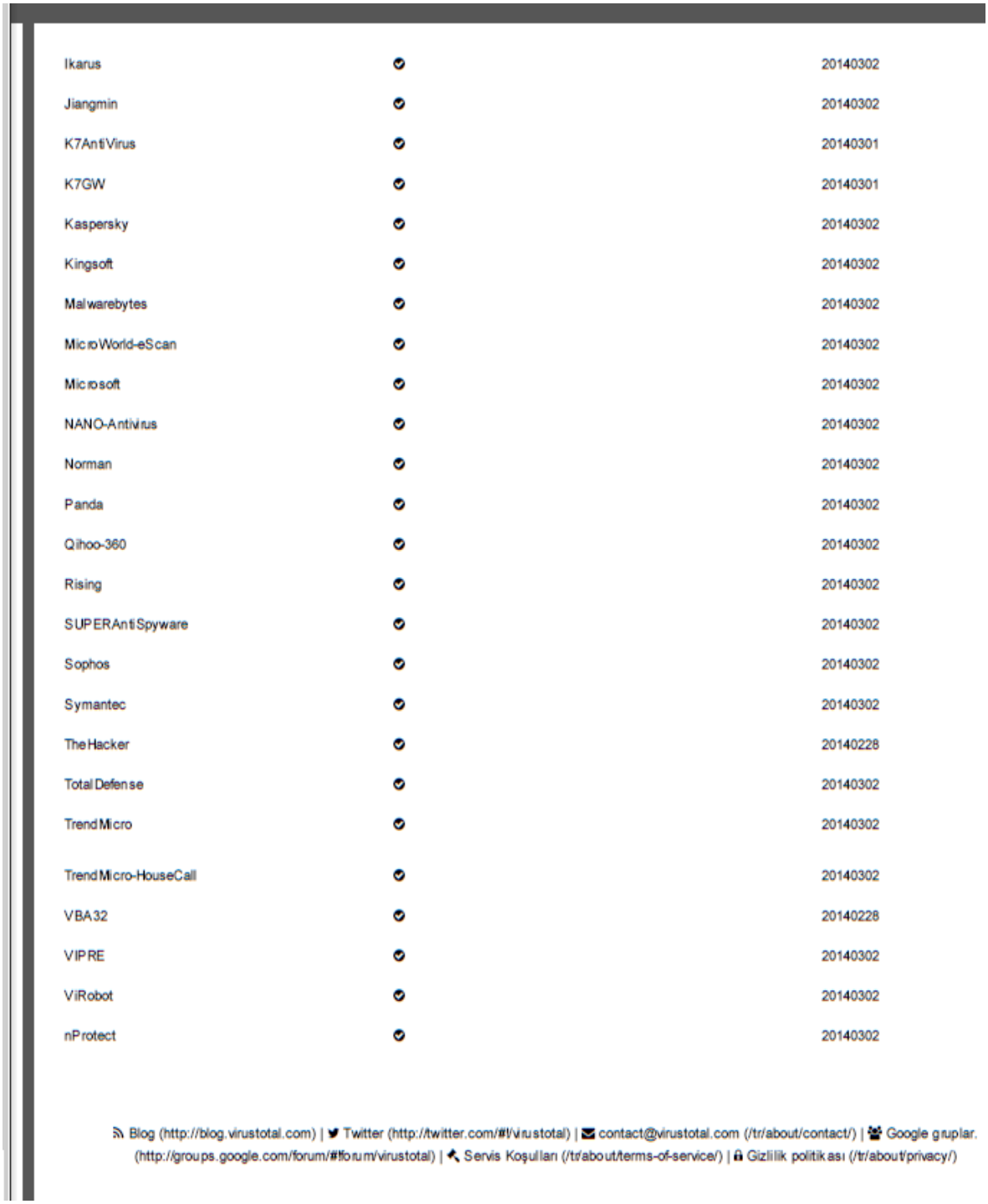
4.3. Casus Yazılımın Çevrimiçi Virüs Tarama Sayfasında Test Edilmesi

Antivirüs programlarının casus yazılım karşısında verdikleri tepkiyi öğrenmenin bir diğer yöntemi de çevrimiçi şüpheli dosya tarama siteleridir. Örneğin "Virustotal.com" sitesi, yüklenmiş bir dosyayı yaygın antivirüs programlarına (49 adet) inceleterek her bir koruyucu yazılıma ait sonucu listelemektedir. Söz konusu çevrimiçi tarama sitesine

geliştirilmiş olan casus yazılımın yüklenerek taranması sonucu elde edilen sonuçlar Resim 4.5'te sunulmuştur.



Resim 4.5. VirusTotal.com sitesinden alınan tarama sonuçları



Ikarus	✔	20140302
Jiangmin	✔	20140302
K7AntiVirus	✔	20140301
K7GW	✔	20140301
Kaspersky	✔	20140302
Kingsoft	✔	20140302
Malwarebytes	✔	20140302
MicroWorld-eScan	✔	20140302
Microsoft	✔	20140302
NANO-Antivirus	✔	20140302
Norman	✔	20140302
Panda	✔	20140302
Qihoo-360	✔	20140302
Rising	✔	20140302
SUPERAntiSpyware	✔	20140302
Sophos	✔	20140302
Symantec	✔	20140302
TheHacker	✔	20140228
TotalDefense	✔	20140302
TrendMicro	✔	20140302
TrendMicro-HouseCall	✔	20140302
VBA32	✔	20140228
VIPRE	✔	20140302
ViRobot	✔	20140302
nProtect	✔	20140302

Blog (http://blog.virustotal.com) | Twitter (http://twitter.com/#!/virustotal) | contact@virustotal.com (/tr/about/contact/) | Google gruplar. (http://groups.google.com/forum/#!forum/virustotal) | Servis Koşulları (/tr/about/terms-of-service/) | Gizlilik politikası (/tr/about/privacy/)

Resim 4.5. (devam) VirusTotal.com sitesinden alınan tarama sonuçları

Sonuçlardan da görülebileceği gibi birçok koruyucu yazılım geliştirilmiş olan casus yazılımı tehlikeli olarak değerlendirmemektedir. VirusTotal.com sitesinin Bölüm 3.6.6 ve Bölüm 3.6.9'da sunulan özellikler dışındaki özellikleri barındıran casus yazılım üzerinde yaptığı taramada 49 antivirüs yazılımından sadece 3'ünün casus yazılımı tehlikeli olarak değerlendirdiği görülmüştür. Ardından geliştirilen casus yazılıma Bölüm 3.6.6.'da belirtilen ekran resmini çekme özelliği eklenerek tekrar websitesi üzerinden tarama

yapıldığında casus yazılımı tespit eden koruyucu yazılım sayısının 15 adede çıktığı görülmüştür. Son olarak Bölüm 3.6.6'da sunulan özelliği barındırmayan ancak Bölüm 3.6.9'da belirtilen "Ses Kaydı" özelliğini barındıran casus yazılım websitesi üzerinden taratıldığında casus yazılımı tespit eden koruyucu yazılım sayısının yedi olduğu görülmüştür. Farklı özellikleri barındıran casus yazılımların tarama sonuçlarının farklı olması, koruyucu yazılımların farklı yöntemlerle casus yazılımları tespit ettiğini göstermektedir.

Çizelge 4.2'de casus yazılımı tespit eden bazı casus yazılımların Resim 4.5'de sunulan listede casus yazılımı tespit edemediği görülmektedir. "Virustotal.com" web sitesinde, bünyesinde barındırdığı antivirüs çözümlerinin ticari olanlarla tamamen aynı olmayabileceği hususu ifade edilmektedir. Web sitesinin açıklamasında antivirüs şirketlerinin söz konusu web sitesine sağladıkları motorları ticari olanlardan farklı parametrelerle ayarlayabilecekleri, bu nedenle sonuçların ticari olanlardan farklı olabileceği hususu ifade edilmektedir.

4.4. Edinilen Bulgular Işığında Casus Yazılımların Oluşturduğu Riskler

Bölüm 2.2.4'te casus yazılımların oluşturdukları riskler anlatılmıştır. Gerçekleştirilen deneysel çalışma sonucunda bahsedilen risklerin bazılarının nasıl gerçekleştiği ortaya konulmuştur.

4.4.1. Herhangi bir koruyucu yazılımın yüklü olmadığı bilgisayarlarda riskler

Çizelge 4.1'de sonuçları belirtilen çalışma sonucunda bahsedilen işletim sistemlerinin varsayılan güvenlik ayarları ile geliştirilen casus yazılımı engellemedikleri ortaya konulmuştur. Dolayısıyla bu çalışma kapsamında geliştirilen casus yazılım ile aşağıda belirtilen riskler herhangi bir koruyucu yazılımın yüklü olmadığı bilgisayarlarda gerçekleşmiştir;

- Kullanıcıların siber dünyadaki kimlik kartları olarak tanımlanabilecek kullanıcı adı ve şifrelerinin ele geçirilmesi (Bölüm 3.6.1 ve Bölüm 3.6.2'de belirtilen basılan tuş bilgileri ile açık uygulama bilgilerinin elde edilmesi),
- E-posta, sosyal medya gibi yazışmaların diğer kişilerin eline geçebilmesi (Basılan tuş bilgilerinin ele geçirilmesi ile)

- Kişiye özel fotoğraf, video gibi görsel medyaların kötü niyetli kişilerce ele geçirilebilmesi (Bölüm 3.6.6'da tanımlanan ekran görüntülerinin elde edilmesi aracılığıyla),
- Casus yazılımların bilgisayarın arka planında çalışması sonucunda bilgisayarda performans kaybı yaşanması,
- Banka şifrelerinin çalınarak kişilerin banka hesaplarından para çekilmesi (Basılan tuş bilgilerinin elde edilmesi ve bilgisayar ekran görüntülerinin elde edilmesi aracılığıyla).
- Kurumsal nitelikte çalışan şirketler ile askeri ve kamu kurumlarının kritik bilişim varlıklarına ait envanterin elde edilmesi (Bölüm 3.6.3'te sunulan özellikler ile kurum içi ağ hiyerarşisinin anlaşılması ve Bölüm 3.6.4'te sunulan özellikler ile ne tür sunucuların sistemde mevcut olduğunun belirlenebilmesi).
- Bölüm 3.6.3 ile detayları anlatılan Genel IP adresinin elde edilmesi ile kullanıcının yaklaşık konumunun elde edilmesi,
- Bölüm 3.6.9 ile detayları anlatılan ortam dinleme özelliği ile gizli toplantıların, özel veya kurumsal görüşmelerin üçüncü kişiler tarafından da takip edilebilmesi riski mevcuttur.

4.4.2. Koruyucu yazılım yüklenmiş olan bilgisayarlardaki riskler

Bölüm 4.2'de sunulan koruyucu yazılımlar, bu çalışma kapsamında geliştirilen casus yazılıma karşı test edilmişlerdir. Söz konusu testlere ait sonuçlar Çizelge 4.2'de sunulmuştur. Çizelge 4.2'de sunulan sonuçlar çerçevesinde;

- Beş adet koruyucu yazılımın geliştirilen casus yazılımı herhangi bir şekilde tespit edemediği,
- Bir adet koruyucu yazılımın casus yazılımı sadece internet erişimi esnasında tespit ettiği ancak casus yazılımı zararlı bir yazılım olarak sınıflandırmadığı,
- Bir adet koruyucu yazılımın, casus yazılımı çalıştırılmasından sonra tespit edip engellediği (Çalışma öncesi yapılan taramada casus yazılımı tespit edemediği),
- Üç adet koruyucu yazılımın ise casus yazılım henüz çalışmıyorken bile, daha dosya sistemi üzerinde iken zararlı yazılım olarak tespit ettiği ve engellediği,

gözlemleri yapılmıştır. Bu gözlemler dikkate alındığında koruyucu yazılımların farklı tepkiler verdiği dolayısıyla da koruyucu yazılımların yüklü olduğu bilgisayarlardaki risklere yönelik genel bir değerlendirmenin yapılamayacağı değerlendirilmiştir. Yukarda sunulan farklı koruyucu yazılımların göstermiş oldukları farklı tepkilere ilişkin risk değerlendirilmeleri aşağıda sunulmuştur.

Casus yazılımı hiçbir şekilde tespit edemeyen koruyucu yazılımların yüklü olduğu bilgisayarlar; Bu tür koruyucu yazılımların yüklü oldukları bilgisayarlardaki riskler Bölüm 4.4.1.de sunulan riskler ile aynı değerlendirilebilir. Casus yazılıma ilişkin hiçbir uyarı belirtmeyen bu yazılımlar temelde hiçbir koruyucu yazılımın yüklü olmadığı bilgisayarlardan farksızdırlar. Bununla birlikte kullanıcılar, bilgisayarlarında bulunan bir koruyucu yazılım olduğundan zararlı yazılımlardan korunduklarını düşüneceklerdir dolayısıyla riskler karşısında zafiyet gösterebilirler. Örneğin zararlı bir yazılım olabilecek çalıştırılabilir bir dosyayı (İng. Executable file) koruyucu yazılımının var olduğunu düşünerek çalıştırabilir ve bunun sonucunda bilgisayara casus yazılım engellenmeden bulaşmış olur.

Casus yazılıma ait internet erişimini tespit eden koruyucu yazılımların yüklü olduğu bilgisayarlar; Güvenlik duvarı özelliğinin aktif olduğu koruyucu yazılımların yüklü olduğu bilgisayarlarda istisna listesine alınmamış tüm programlar internete erişmeyi denediklerinde bu durum koruyucu yazılım tarafından kullanıcıya bildirilir. Kullanıcı, koruyucu yazılım ara yüzü aracılığıyla internete erişmeyi deneyen yazılıma izin verir ya da reddeder. Kullanıcı ile interaktif bir iletişim gerektiren bu tür koruyucu yazılımlar, kullandıkları programların internet gerektirip gerektirmeyeceğini ayırt etmekte zorlanacak kullanıcılar için bir anlam ifade etmeyecektir. Ayrıca internete erişmeyi deneyen yazılımın her zaman zararlı yazılım olduğu çıkarımı da yapılamaz. Normal yazılımların da güncelleme, bilgi alıp gönderme gibi çeşitli nedenlerle internete bağlanma ihtiyacı duymalarından dolayı, internete bağlanma girişimi tek başına zararlı yazılım davranışı olarak nitelendirilebilecek bir davranış değildir. Ayrıca casus yazılımın internet erişimi engellense bile topladığı bilgileri bilgisayar üzerinde saklayabilir, bu durum bilgisayara fiziksel erişimin mümkün olduğu durumlarda riskin devam ettiği anlamına gelmektedir. Tüm bu hususlar dikkate alındığında bu tür bilgisayarlarda da risklerin olduğu değerlendirilebilir.

Casus yazılımı tespit eden yazılımlar; Bu koruyucu yazılımların kendilerinden beklenen işlevleri yerine getirdiğini değerlendirmek mümkündür. Çizelge 4.2'de de ifade edildiği gibi bu tür yazılımlar casus yazılımın çalışmasına müsaade etmeden olası tehlikeyi kullanıcıya bildirdiğinden ve casus yazılım istisna listesine alınmadığı müddetçe çalışması engellendiğinde riskler engellenmiş olur. Ancak birçok casus yazılımın kullanıcıya fayda sağlayan normal bir yazılımın arkasında gizlendiği gerçeği dikkate alındığında kullanıcılar zaman zaman risk içerse bile kendilerine sağlayacağı faydayı kullanabilmek için (lisansı kırılmış bir uygulama, korsan yazılım vb.) casus yazılım içeren yazılımı istisna listesine ekleyerek çalışmasına izin verirler bu durumda riskin oluşmasına neden olur.

4.5. Casus Yazılımlara Karşı Alınabilecek Önlemler

Bilgisayar kullanıcılarında koruyucu yazılım yükleyerek zararlı yazılımlardan tamamen korunulabileceği düşüncesi yaygındır. Ancak Bölüm 4 ve Bölüm 5'te sonuçları sunulmuş olan çalışma ile casus yazılımların koruyucu yazılımlar karşısında bile riskli olabilecekleri ortaya konulmuştur. Dolayısıyla koruyucu yazılımlar ile birlikte bazı önlemlerin de alınması gerekmektedir. Bu önlemler kategorize edilerek aşağıda sunulmuştur.

4.5.1. Koruyucu yazılım geliştiriciler tarafından alınabilecek önlemler

Zararlı yazılımların tespit edilmesi için temelde iki yöntem kullanılmaktadır. Bunlardan ilki "Statik Analiz" yöntemi olup bu yöntem temel olarak yazılıma ait "binary" kodların çalıştırılmadan, zararlı olup olmadıklarına ilişkin imza karşılaştırmasına tabi tutulması prensibine dayanmaktadır. Statik analiz yöntemi bilinen zararlı yazılımların tespitinin çok hızlı yapılabilmesini sağlamakla birlikte statik analiz yöntemine yönelik yanıltıcı önlemler alan bazı zararlı yazılılar ile imzası oluşmamış zararlı yazılımlara karşı yetersiz kalmaktadır. Birçok koruyucu yazılım statik analiz yöntemine oldukça benzeyen yöntemler kullanmaktadır. Zararlı yazılımların tespitinde kullanılan diğer yöntem ise "Dinamik Analiz" yöntemidir. Dinamik analiz yöntemi, zararlı yazılımın çalıştığı esnada aktivitelerinin (İng. process) incelenerek, zararlı yazılım aktivitelerine benzerlik göstermesi durumunda zararlı yazılımın tespitini sağlar. Dinamik analiz yönteminin statik analiz yöntemi ile karşılaştırıldığında özellikle tespit edilmemeyi hedefleyen zararlı yazılımlara karşı daha etkili olduğu kanıtlanmıştır [21, 44].

Dünyada, bilişim alanında gelişmiş birçok ülkenin bünyesinde firma veya kuruluşlar tarafından geliştirilmiş koruyucu yazılımlar bulunmaktadır. Ancak bilişim sistemleri altyapıları için güvenlik çözümleri sunan OPSWAT yazılım firması tarafından Ağustos 2013 tarihinde yayınlanan "Antivirüs Ürünlerinin Market Dağılımı" raporu gibi uluslararası düzeyde raporlar da incelendiğinde ülkemizde bu konu ile ilgili gerek kamu kurumu düzeyinde gerekse özel firma düzeyinde henüz ortaya varlık gösterebilmiş bir ürün çıkmadığı görülmektedir. Bu kapsamda yapılabilecek bir koruyucu yazılım geliştirilmesi çalışmasına katkı sağlayabileceği düşünülen öneriler aşağıda sunulmuştur.

- Geliştirilen casus yazılımda bilgi güvenliği açısından en tehlikeli özelliklerden birisinin basılan tuşları kaydetme özelliği (İng. Keylogger) olduğu düşünüldüğünde bu özelliği sağlayan işletim sistemi fonksiyonlarından "GetAsyncKeyState" fonksiyonu üzerinde durulmalıdır. Windows işletim sistemi içinde "User32.dll" dosyasında tanımlanmış olan bu fonksiyonun kullanım amaçları arasında oyun programlama, uygulamalara kısa yol tuşu oluşturma gibi özellikler bulunsa da Bölüm 3.6.2'de ki gibi bazı tanımlamalar ve değişiklikler yardımıyla basılan tuşları kaydetme özelliğine sahip bir casus yazılım geliştirilebilmiştir. İnternet ortamında basılan tuşları kaydetme işlevine yönelik kullanıma hazır halde çeşitli kütüphaneler/sınıflar bulunmakla birlikte bu sınıfları kullanan casus yazılımlar statik analiz yöntemini kullanan birçok koruyucu yazılım tarafından (ilgili kütüphaneler/sınıflar imza veritabanlarında kayıtlı olduklarından) tespit edilebilmektedir. Ancak Bölüm 3.6.2.'de detayları sunulan kodlar özgün olarak geliştirildiklerinden statik analiz yöntemi ile tespit edilmeleri zorlaşmıştır. Özellikle dinamik analiz yöntemi ile ilgili yukarda ifade edilen bilgiler de dikkate alındığında geliştirilecek olan bir koruyucu yazılımın statik analiz yöntemi ile birlikte işletim sisteminin "GetAsyncKeyState" fonksiyonunu kullanan uygulamaları ve bu uygulamaların davranışlarını dinamik analiz yöntemi ile riskli sınıfa alması, bu fonksiyonu kullanarak geliştirilecek casus yazılımların tespitini mümkün kılacaktır. Bu fonksiyon ile ilgili detaylı teknik bilgi Microsoft firmasının resmi internet sitesinde ilgili linkte "http://msdn.microsoft.com/en-us/library/windows/desktop/ms646293(v=vs.85).aspx" bulunabilir.
- Bu çalışma kapsamında geliştirilen casus yazılıma kazandırılan bir diğer bilgi güvenliğini tehdit eden önemli özellik ise, açık pencerelerin bilgilerinin kaydedilmesidir. Bu özelliğin oluşturduğu risklere ait detaylar Bölüm 3.6.1'de

sunulmuştur. Casus yazılıma bu özelliği kazandıran işletim sisteminde "user32.dll" dosyası içindeki "GetForegroundWindow()" fonksiyonunun da dikkate alınması gerekmektedir. Dinamik analiz yöntemini kullanacak olan bir koruyucu yazılımda bu fonksiyonu kullanan uygulamaların özellikle "GetAsyncKeyState" fonksiyonu ile birlikte kullanıldığında dikkate alınması gerekmektedir.

- Ortam dinlemesi için ses kaydı özelliği, casus yazılımın oluşturduğu önemli risklerden birisidir. Bu özellik "Windows" işletim sistemlerinde standart olarak bulunan "winmm.dll" dosyası içinde tanımlı olan "mciSendStringA" fonksiyonu ile gerçekleştirildiğinden dinamik analiz yöntemi kapsamında bu fonksiyonunda dikkate alınması gerekmektedir.
- E-posta gönderme özelliği hâlihazırda birçok koruyucu yazılım tarafından riskli işlem olarak değerlendirilmektedir. Ancak bu çalışma kapsamında geliştirilen casus yazılımda toplanan bilgilerin e-posta ile gönderiliyor olması koruyucu yazılım geliştiricilerin bu hususu dikkate almaları gerekliliğini güçlendirmiştir. Bununla birlikte Bölüm 3.6.8'de detayları sunulan casus yazılım özelliği ile bir uygulamanın topladığı bilgileri e-posta ile gönderirken kullanılan klasik yöntemlerin dışına çıkabileceği gösterilmiştir. Yani e-posta gönderiminin gerçekleştiği e-posta portları (SMTP:25, POP3:110, IMAP:143, SMTP (SSL): 465, MSA:587) dışında da "http" protokolü (80.port) aracılığıyla web sunucuları ile iletişime geçilip toplanan bilgiler gönderilebilmektedir. Bu özellik dikkate alındığında dinamik analiz yöntemiyle çalışacak bir koruyucu yazılımın, 80.port üzerinden yapılan özellikle e-posta içeriğine benzeyen (Gönderici, Alıcı, Konu ve İçerik gibi bilgileri içeren) ve belirli aralıklarda tekrarlanan veri alışverişlerinin yukarda belirtilen diğer riskli işlemlerle birlikte değerlendirme yapması, e-posta ile veri alışverişi yapan casus yazılımların tespit edilmesine yardımcı olacaktır.
- Yapay zeka bir bilgisayarın ya da bilgisayar denetimli bir makinenin, genellikle insana özgü nitelikler olduğu varsayılan akıl yürütme, anlam çıkartma, genelleme ve geçmiş deneyimlerden öğrenme gibi yüksek zihinsel süreçlere ilişkin görevleri yerine getirme yeteneği olarak tanımlanmaktadır [45, 46]. Yapay zeka algoritmaları bilgileri birleştirir, analiz eder, sonuca varır ve bu sonucu ise bir nedene bağlar. Uzman sistemler yapay zeka uygulamalarından olup zararlı yazılım tespiti amacıyla kullanılmaktadır [45]. Bu kapsamda geliştirilecek bir yapay zeka algoritması ve işbu çalışma kapsamında edinilen bulguların değerlendirilerek oluşturulacak uzman sistem kural tabanı ile zararlı yazılımların risklerinin değerlendirilmesine yönelik

bir yazılım modülünün koruyucu yazılımlara entegre edilmesi mümkündür. Söz konusu uzman sisteme ait kural veritabanında Bölüm 3'te sunulduğu gibi çeşitli aktivitelerin risk puanlamasına tabi tutulması (örneğin açık uygulama bigileri ile belirli peryotlarda e-posta gönderiminin bir arada bulunması durumu için bir risk puanı, basılan tuş bilgilerinin saklanması durumu için belirli bir risk puanı belirlenmesi vb.) ve bu kural veritabanının dinamik olarak yapay zeka algoritmaları ile güncellenebilir olması zararlı yazılımların tespitine katkı sağlayabilecektir.

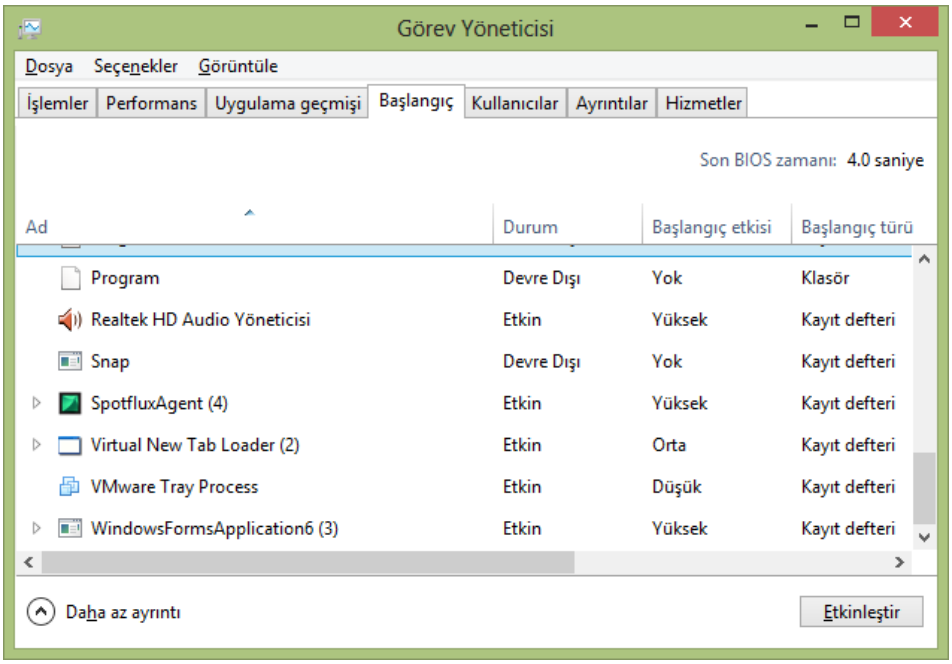
4.5.2. Kişisel önlemler

Casus yazılımlara karşı kullanıcının çalıştığı işyerinde sistem yöneticileri çeşitli kurumsal önlemler almış olabilir ancak bu kurumsal önlemlerin yanı sıra güvenliği arttırıcı kişisel önlemler de alınabilir. Nitekim "bir zincir en zayıf halkası kadar güçlüdür" prensibi gereği kişiler bilgi güvenliği konusunda sorumluluklarını yerine getirmediği takdirde tüm kurumsal sistemi bilgi güvenliği açısından tehlikeye atabilir.

Kurumsal sistemler dışında kişilere ait özel bilgilerin tutulduğu özel bilgisayarlar da, alınabilecek kişisel önlemlerle bilgi güvenliği açısından casus yazılımlara karşı korunabilir.

- Kaynağı belirsiz olan veya şüphe duyulan ancak işlevsel olarak ihtiyaç duyulan dosyaları, bilgisayarda çalıştırmadan önce çevrimiçi zararlı tarama web siteleri üzerinden (Resim 4.5'te bir örneği sunulanVirusTotal.com gibi web sayfaları) ilgili dosyanın koruyucu yazılımlar tarafından zararlı olarak tanınıp tanınmadığı konusunda fikir edinilebilir.
- Özellikle kurumsal yerlerde çalışan kullanıcıların kısa süreli de olsa bilgisayar başından ayrılacakları durumlarda bilgisayarları kilitlemeleri (Windows işletim sistemleri için Windows Tuşu ile "L" tuşuna birlikte basarak sağlanabilir) gerekmektedir. Çünkü kötü niyetli kişilerin açık olan bir bilgisayarın başına geçerek bir dosyayı çalıştırması çok kısa sürelerde sağlanabilir. Casus yazılımların bir sefer çalıştırılması işletim sistemine yerleşmesine yeterli olduğu hususu dikkate alındığında (bakınız bu çalışma kapsamında geliştirilen casus yazılıma kendini otomatik başlatma özelliğinin eklenmesi Bölüm 3.6.8) başında olunmadığı zamanlarda bilgisayar oturumunun kilitlenmesi gerekmektedir.
- Bilgisayar görev yöneticisi programından (CTRL+ALT+DEL tuş kombinasyonu ile ulaşılabilir) çalışan programlar takip edilmeli kullanıcıya ve sisteme ait olmayan

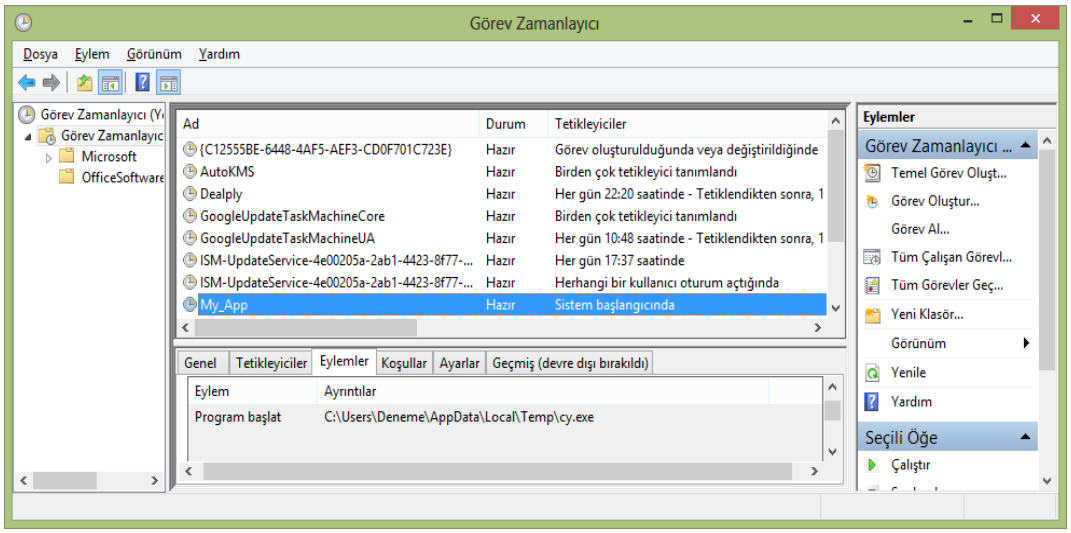
programlara şüphe ile yaklaşılmalıdır. İhtiyaç duyulmayan programların sistemden ve başlangıçtan kaldırılması gerekmektedir. Örneğin bir programa ait güncelleme servis hizmetinin arka planda sürekli çalışması hem performans kaybına neden olacaktır hem de ilgili hizmet adı ile bir casus yazılımın arka planda çalışma riskini barındıracaktır. Resim 4.6'da sunulan görüntü bu çalışma kapsamında geliştirilen casus yazılımın "Windows 8" işletim sistemi görev yöneticisi "Başlangıç" sekmesindeki görünümünü barındırmaktadır. Söz konusu casus yazılım "WindowsFormApplication6 (3)" adı ile "Kayıt Defteri" ne eklenmiştir. Ancak siber suçluların kullanacakları isim ve uygulama logoları kullanıcılar açısından çok daha yanıltıcı olacaktır. Kullanıcıların başlangıç listesindeki uygulamalara aşina olması bu tür saklanacak olan zararlı yazılımları etkisiz hale getirecektir.



Resim 4.6. Windows 8'de otomatik başlayan uygulamaları gösteren görev yöneticisi

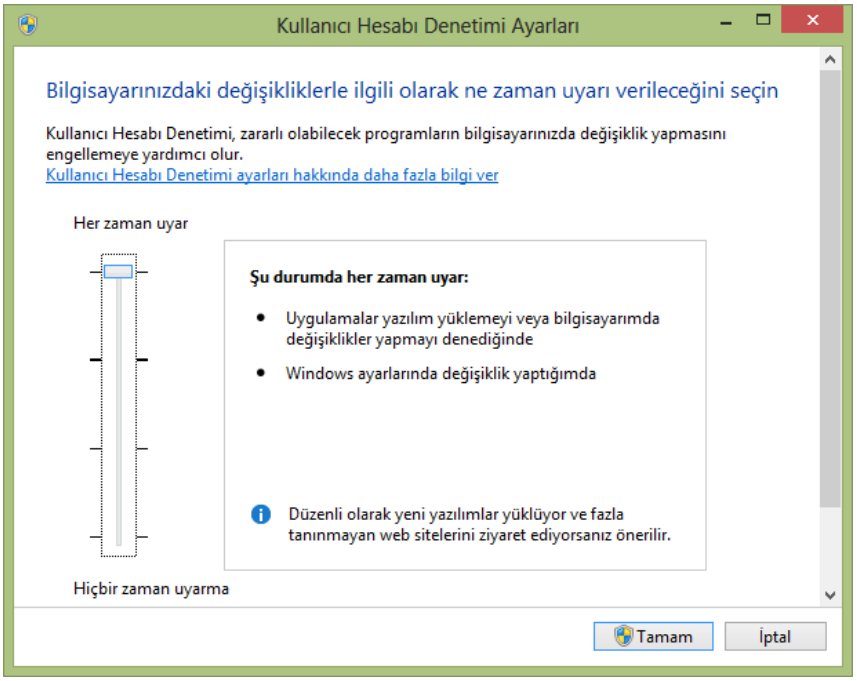
- Bilgisayar üzerinde tanımlanmış zamanlanmış görevler takip edilmeli tanınmayan programlar buralardan kaldırılmalıdır. Bu bölgelerde yapılacak iyileştirmeler (optimizasyonlar) ayrıca bilgisayarın performansına da olumlu katkı sağlayacaktır. Resim 4.7'de "Windows 8" işletim sisteminde bulunan "Görev Zamanlayıcı" uygulamasına ait ekran görüntüsü sunulmuştur. Söz konusu uygulamaya "Denetim Masası" üzerinden ulaşılabilmektedir. Resim 4.7'de sunulan görüntüde de görülebileceği gibi birçok uygulama belirli saat dilimlerinde veya sistem başlangıcında çalışmaya programlanmış durumdadır. Listede sunulan

uygulamalardan “My_App” isimli yazılım bu çalışma kapsamında geliştirilmiş olan casus yazılımdır. Casus yazılımı zamanlanmış görev listesine ekleyen yazılım kodu Bölüm 3.6.8’de sunulmuştur. Zamanlanmış görevler birçok kullanıcı tarafından bilinmediğinden işletim sistemlerine ait bu özellik siber suçlular tarafından kullanılmaya müsaittir. Bilinmeyen yazılımların bu listelerden silinmesi gerekmektedir.



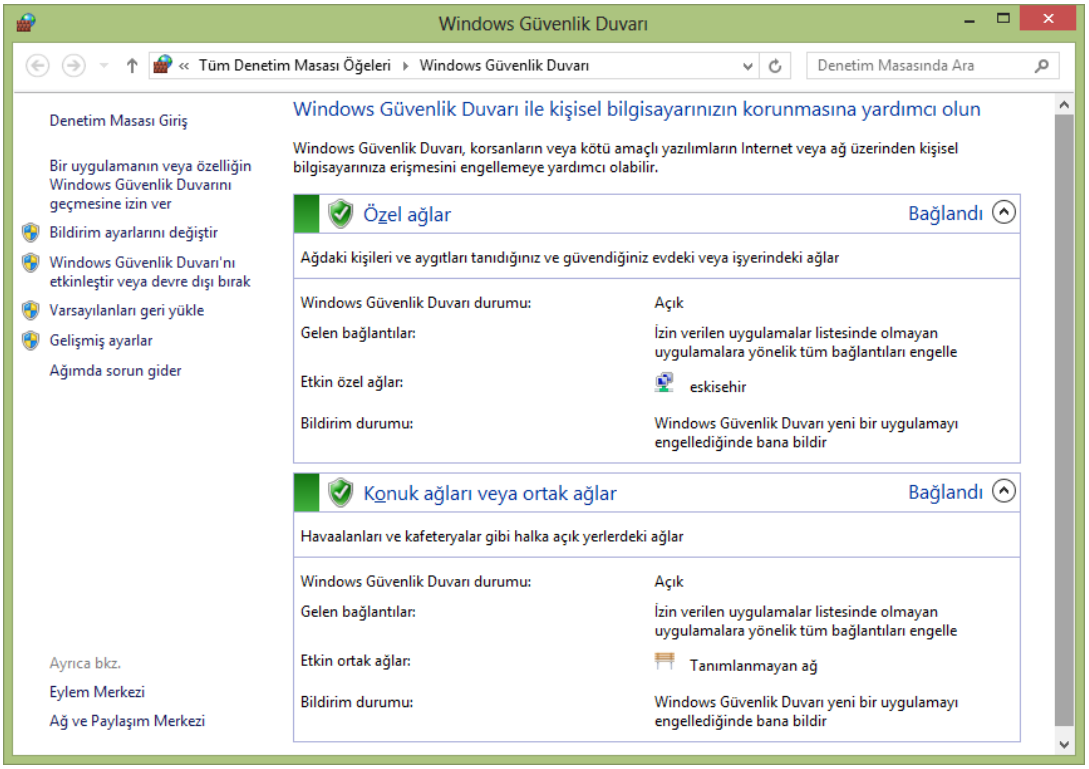
Resim 4.7. Windows 8 işletim sistemi “Görev Zamanlayıcı” uygulaması

- Windows işletim sistemlerinde bulunan kullanıcı hesabı denetimi özeliği (UAC) açık tutulmalıdır. Bu özellik programların arka planda bile olsa önemli işlemleri yapmadan önce kullanıcılardan onay alınmasını sağlar. Şüpheli görülen işlemlerin kullanıcılar tarafından reddedilmesi gerekmektedir. Resim 4.8’de “Windows 8” işletim sistemine ait kullanıcı hesabı denetim ekranı sunulmuştur. İlgili ekrana Denetim Masası üzerinden ulaşılabilmektedir.



Resim 4.8. Windows 8 işletim sisteminde kullanıcı hesabı denetim ekranı

- İşletim sistemine ait güvenlik duvarı ayarlarını aktif etmek bilgi güvenliğini arttırabilecek diğer önlemlerden bir tanesidir. Üstelik "Windows" işletim sistemi ailesinde "Güvenlik Duvarı" işletim sistemi ile birlikte kurulan standart bir özelliktir. Koruyucu yazılımlar bünyesinde de bulunabilen bu özellik sayesinde özellikle uygulamalara ait istenmeyen ağ trafiği kontrol altına alınabilir. Resim 4.9'da "Windows 8" işletim sisteminde Denetim Masası üzerinden ulaşılan Güvenlik Duvarı yönetim ekranı görülmektedir. Bu ekran kullanılarak güvenlik ayarları özelleştirilebilir. Örneğin işletim sisteminde internet ile iletişime geçmesi istenmeyen programlar belirlenebilir veya tüm programlar varsayılan olarak engellenir sadece izin verilen uygulamaların internet erişimi sağlanabilir.



Resim 4.9. Windows 8 işletim sistemi "Güvenlik Duvarı" ayarlarına ait ekran görüntüsü

4.5.3. Kurumsal önlemler

Kurumsal bilgisayarlarda siber suçlara karşı önlemler alma konusunda son kullanıcılar kadar sistem ve güvenlikten sorumlu personele de büyük sorumluluklar düşmektedir. Özellikle kurum içi ağda (intranet) bulunabilecek bir açıklık siber suçlular tarafından tespit edildiğinde tüm kurumsal kullanıcılar siber güvenlik açısından tehlikeye düşebilirler. Bu kapsamda kurumsal bilişim sistemlerinin yöneticilerinin, bu çalışma kapsamında geliştirilmiş olan casus yazılıma ait süreçteki tecrübelerden de faydalanılarak hazırlanan önlemler şu şekildedir;

- Kurumsal bilgisayarlarda son kullanıcılara, gerekmiyorsa bilgisayar yönetici yetkisi verilmemelidir. Örneğin birçok kurum kullanıcısının, temel ofis programları dışında başka herhangi bir programa ihtiyaç duymayacağı dikkate alınacak olursa son kullanıcılardan yeni program kurma yetkisi kaldırılabilir. Son kullanıcılara gerekli olabilecek diğer programlar da sistem yöneticisi kontrolünde kurulabilir. Çünkü geliştirilmiş olan casus yazılımın bilgisayarın bazı kaynaklarına yönetici yetkisi ile eriştiği dikkate alındığında (başlangıca yerleşme

vb.), yönetici yetkisi olmayan bir kullanıcı istese bile bilgisayara casus yazılım kuramayacaktır.

- İşletim sistemleri içinde en yaygın olarak kullanılan Windows tabanlı işletim sistemleri olduğu Şekil 3.1'de görülmektedir. Bu durum beraberinde zararlı yazılımların çoğunlukla Windows tabanlı işletim sistemlerini hedef almasına sebep olmaktadır. Dolayısıyla kurumsal son kullanıcıların, ihtiyaçlarını karşılayabilecek alternatif bir işletim sistemini kullanmaları birçok zararlı yazılımın sisteme bulaşmasını engelleyecektir.

  Ülkemizde bazı kurumlar bir LINUX dağıtımı olan ve TÜBİTAK tarafından geliştirilmiş olan PARDUS işletim sistemini kullanmaktadır. Bu kurumlar Milli Savunma Bakanlığı Asker Alma Dairesi (ASAL), Milli Savunma Bakanlığı yanı sıra birçok üniversite, sivil toplum örgütleri, kamu kuruluşları ve özel şirketlerde PARDUS işletim sistemini tercih etmişlerdir. Ayrıca Radyo ve Televizyon Üst Kurulu (RTÜK) ve Enerji Piyasası Düzenleme Kurumu (EPDK) PARDUS'a geçiş yapma kararı almışlardır [47].

  Ayrıca ülkemizde kurumsal kullanıcıların çoğunlukla işletim sistemi olarak yabancı firmalara ait ücretli işletim sistemlerini tercih ettikleri düşünüldüğünde söz konusu işletim sistemi lisans ücretleri, ilgili işletim sistemleri üzerinde çalışan ofis uygulamalarına ait lisans ücretleri, bu sistemlerin oluşturduğu kurumsal ağların yönetiminde kullanılan çoğunlukla işletim sistemi ile aynı firma tarafından üretilen sistem yönetimi ile ilgili yazılımlar, bu sistemler ile ilgili teknik personele verilen eğitimlere ilişkin maliyetler gibi harcama kalemleri dikkate alındığında PARDUS gibi yerli ihtiyaçlara göre bir işletim sistemi geliştirilmesinin ve bu işletim sistemi üzerinde kurumsal sistemlerin ihtiyaçlarını karşılayacak yardımcı yazılımların geliştirilmesinin daha maliyet etkin olacağı değerlendirilmektedir. Yerli imkanlarla geliştirilip idame ettirilecek bir işletim sistemi ve bu kapsamda yardımcı yazılımlara harcanacak bütçenin birçoğunun (yazılım geliştirme, eğitim vb.) yurtiçinde kalacağı da dikkate alındığında yerli işletim sistemi geliştirilmesi alternatifinin bir devlet politikası olarak uygulanması gerektiği değerlendirilmektedir.

  PARDUS gibi yerli imkanlarla bir işletim sisteminin geliştirilmesinin ve idamesinin sağlanmasının, ekonomik faydalarının yanı sıra siber güvenlik açısından da çok önemli faydaları bulunmaktadır. Ülkenin kritik kurumlarına ait bilişim sistemlerinde yabancı firmalara ait işletim sistemi ve yönetim

yazılımlarının bulunması her zaman için ilgili sistemlerin söz konusu firma tarafından izlenme riskini barındırmaktadır. Örneğin söz konusu işletim sisteminin güncelleme adı altında yapacağı bir internet erişiminin kurumsal ağdan bir bilgiyi gönderen siber casusluk faaliyeti olma riski mevcuttur.

- Geliştirilen casus yazılım kullanıcı girişi (authentication) gerektiren bir "proxy" sunucusu ile internet erişiminin mümkün olduğu ağ üzerinde de test edilmiştir. Test sonucunda gerekli kimlik bilgilerine sahip olmayan casus yazılımın "proxy" sunucusu üzerinden internete ulaşamadığı ve bilgileri gönderemediği görülmüştür. Dolayısıyla kurumsal ağlarda kullanıcılara sağlanacak kimlik bilgileri ile ağ erişimini mümkün kılan "proxy" sunucularının bulundurulması casus yazılımların bilgi göndermesini engelleyebilecektir.

5. SONUÇ VE ÖNERİLER

Geliştirilen casus yazılım yaygın olarak kullanılan Windows XP, Windows 7 ve Windows 8 işletim sistemlerinde test edilmiştir. Bilgisayar kısıtlılığı nedeniyle Windows 7 ve Windows XP işletim sistemleri sanal makine yazılımları ile test edilmiştir. Casus yazılımın, Windows XP işletim sistemi dışında herhangi bir çalışma problemi yaşamadığı görülmüş olup Windows XP işletim sisteminin normal kullanıma yönelik birçok programın yüklenebilmesi için de ön koşul olan ".NET FRAMEWORK 2.0" ve üstü paketin yüklenmesi ile çalışabilirlik sağlanmıştır. Herhangi bir koruyucu yazılım olmadan işletim sistemlerinin varsayılan ayarları ile gerçekleştirilen testlerde casus yazılımın bilgi toplama ve bu bilgileri e-posta ile gönderme aktiviteleri hiçbir engelleme ve problem ile karşılaşmadan gerçekleşmiştir.

İşletim sistemleri ile gerçekleştirilen testler sonrasında geliştirilen casus yazılım yaygın olarak kullanılan koruyucu yazılımlar ile de test edilmiştir. Testler koruyucu yazılım yüklendikten sonra, casus yazılımı barındıran dosyanın çalıştırılmadan önce taratılması, çalıştırılma esnasında koruyucu yazılımın herhangi bir uyarı verip vermediğinin gözlemlenmesi ve casus yazılımın (eğer çalışmasına izin verildi ise) topladığı bilgileri e-posta ile gönderimi esnasında koruyucu yazılımın herhangi bir uyarı verip vermediğinin gözlemlenmesi şeklinde icra edilmiştir. Bu testler sonucunda 11 adet koruyucu yazılımın sadece dördünün geliştirilen casus yazılımı zararlı olarak nitelendirdiği, bir adet koruyucu yazılımın ise sadece internet erişimini engelleyebildiği görülmüştür. Altı adet koruyucu yazılım ise geliştirilen casus yazılıma yönelik herhangi bir uyarı vermemiştir. Bu durum zararlı yazılımlardan korunmak için bir önlem olarak düşünülen koruyucu yazılımların bir kısmının aslında yeterli koruma sağlamadığını göstermekte ve siber suçlar için risk oluşturmaktadır.

İşbu çalışma özelinde geliştirilen casus yazılım, Windows işletim sistemlerinde "User32.dll" ve "Winmm.dll" dosyaları tarafından sağlanan uygulama programlama arayüzleri (İng. application programming interface -API) aracılığıyla basılan tuş bilgileri, açık uygulama bilgileri ve mikrofon üzerinden ses kaydı elde etmek amacıyla işletim sistemi fonksiyonlarını kullanmaktadır. Ayrıca geliştirilen casus yazılım, 587 ve 80 numaralı ağ portları üzerinden e-posta gönderimi ve web sayfaları üzerinden gerçek IP sorgulamaları yaparak ağ kaynaklarını, ekran görüntülerinin kaydedilmesi gibi özellikleri nedeniyle de disk kaynaklarını kullanmaktadır. Casus yazılım, bilgisayarın her açılışında

kendisini başlatabilmesi için de sistem kayıt defterine (registry) kaydını gerçekleştirmektedir. Dinamik Analiz yöntemi kullanılarak, geliştirilen casus yazılımın amacına ulaşmak için gerçekleştirdiği bu ve benzeri türdeki aktiviteler izlenebilir.

Yapay zeka uygulamalarından olan uzman sistemler kullanılarak oluşturulacak bir kural veritabanı ile casus yazılımların risk değerlendirmeleri yapılabilir. Söz konusu uzman sisteme ait kural veritabanında Bölüm 3'te sunulan casus yazılım aktiviteleri de dahil olmak üzere çeşitli aktivitelerin risk puanlamasına tabi tutulması (örneğin açık uygulama bigileri ile belirli aralıklarda e-posta gönderiminin bir arada bulunması durumu için bir risk puanı, basılan tuş bilgilerinin saklanması durumu için belirli bir risk puanı belirlenmesi vb.) mümkündür. Risk puanlama işlemi esnasında normal yazılım aktivitelerinin de dikkate alınması gerekmekte olup "otomatik başlama, e-posta gönderimi vb." gibi bu tür aktivitelerde casus yazılımlar tarafından gerçekleştirilmektedir.

Oluşturulacak uzman sistem kural veritabanının hâlihazırda tespit edilen casus yazılımların işlevlerine yönelik yapacağı risk değerlendirmelerinin incelenmesi ve bu sonuçlar çerçevesinde eğer gerekiyorsa kural veritabanının güncellenmesi ve bu sürecin ideal (optimum) noktaya ulaşılana kadar tekrar edilmesi, risk puanlama işleminin zararlı yazılım tespitinde daha doğru ve tutarlı sonuçlar vermesini sağlayacaktır. Söz konusu tekrarlama (İng. iteration) sürecinde veri madenciliği tekniklerinin kullanılması mümkündür.

İncelenmesi faydalı olacak bir diğer konu ise mobil platformlardır. Bu çalışma, kapsam itibariyle "Windows" işletim sistemi ailesini incelemiştir. Ancak günümüzde mobil cihazların yaygın olarak kullanıldığı ve günlük hayatta gerçekleştirilen işlemlerde (bankacılık, iletişim, eğlence, iş takibi vb.) mobil cihazların daha fazla tercih edilmeye başlanması ile birlikte siber suçluların mobil platformları hedef aldığı bilinmektedir. Bu kapsamda mobil cihazların bilgi güvenliğini sağlamak üzere çeşitli koruyucu yazılımlar da piyasaya sürülmüştür. Dolayısıyla mobil cihazlarda risklerin ortaya konduğu ve bu riskleri mobil platformlar için geliştirilen koruyucu yazılımların ne düzeyde engelleyebildiklerini inceleyecek bir deneysel çalışmanın faydalı olacağı değerlendirilmiştir.

KAYNAKLAR

1. Gürkaynak, M., İren, A. A. (2011). Reel dünyada sanal açmaz: Siber alanda uluslararası ilişkiler. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 16(2), 263-279.

2. Cassim, F. (2011). Addressing the growing spectre of cyber crime in Africa: evaluating measures adopted by South Africa and other regional role players. *Comparative and International Law Journal of Southern Africa*, 44(1), 123-138.

3. Hekim, H., Başıbüyük O. (2013). Siber suçlar ve Türkiye'nin siber güvenlik politikaları. *Uluslararası Güvenlik ve Terörizm Dergisi*, 4(2), 135-158.

4. Çelik, Ş. (2013). STUXNET saldırısı ve ABD'nin siber savaş stratejisi: uluslararası hukukta kuvvet kullanmaktan kaçınma ilkesi çerçevesinde bir değerlendirme. *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, 15(1), 137-175.

5. Lin, H. S. (2010). Offensive Cyber Operations and the Use of Force. *Journal of National Security Law & Policy*, 4(1), 63-86.

6. Wilson, C. (2008). Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. *USA Congressional Research Service, The Library of Congress Report*, ADA477642, Washington.

7. Hartnett, S. J. (2011). Google and the "Twisted Cyber Spy" affair: US-Chinese communication in age of globalization. *Quarterly Journal of Speech*, 97(4), 411-434.

8. Türkay, Ş. (2013). Siber savaş hukuku ve uygulama sorunsalı. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, 71(1), 1177-1228.

9. Young, S., Aitel, D. (2003). *The Hacker's Handbook The Strategy behind Breaking into and Defending Networks* (First edition). New York: Auerbach Publicatıons, CRC Press, 72-74.

10. Akdağ, P. (2009). *Siber suçlar ve Türkiye'nin ulusal politikası*, Yüksek Lisans Tezi, T.C. Polis Akademisi Güvenlik Bilimleri Enstitüsü Uluslararası Güvenlik Anabilim Dalı, Ankara, 4-9.

11. Shahzad, R. K., Haider, S. I., and Lavesson, N. (2010, 15-18 Şubat). *Detection of Spyware by Mining Executable Files.* Paper presented at 5th International Conference On Availability, Reliability, And Security, Cracow, POLONYA.

12. Schultz, M. G., Eskin, E., Zadok, E., and Stolfo, S. J. (2001). *Data mining methods for detection of new malicious executables*. Paper presented at 2001 IEEE Symposium on Security and Privacy, S&P 2001 Oakland, California.

13. Kurt, L. (2005). *Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması*, Ankara: Seçkin Yayıncılık.

14. Pocar, F. (2004). New Challenges for International Rules Against Cyber-Crime, *European Journal on Criminal Policy and Research*, 10(1), 27-37.

15. Ye, N., Zhang, Y., and Borror, C.M. (2004). Robustness of the Markov-chain model for cyber-attack detection, *Reliability, IEEE Transactions on*, 53(1), 116-123.

16. Mirkovic, J., Reiher, P. (2004). A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. *ACM SIGCOMM Computer Communication Review*, 34(2), 39-53.

17. Chen, T., Walsh, P. J. (2012). Guarding Against Network Intrusions. Vacca, J.R. (Ed.). *Computer and Information Security Handbook.* (Second Edition). Massachusetts, Morgan Kaufmann, s.81-95

18. Canbek, G. (2005). *Klavye dinleme ve önleme sistemleri*, Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara, 21-40.

19. Ansari, S., Rajeev, S., Chandrashekar, H. (2003). Packet sniffing: a brief introduction. *Potentials, IEEE*, 21(5), 17-19.

20. Canbek, G., Sağıroğlu, Ş. (2005). Şifre Bilimi Tarihine Genel Bakış – I. *Telekom Dünyası*, s.26-44.

21. Bai, H., Hu, C., Jing, X., Li, N. and Wang, X. (2014). Approach for malware identification using dynamic behaviour and outcome triggering. *Information Security, IET*, 8(2), 140-151.

22. İnternet: Kaspersky, What is a Trojan Virus? *usa.kaspersky.com*. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fusa.kaspersky.com%2Finternet-security-center%2Fthreats%2Ftrojans%23.VEi-DtIRBLC&date=2014-10-23 , Son Erişim Tarihi: 2014-10-23.

23. Lee, Y., Kozar, K. A. (2008). An empirical investigation of anti-spyware software adoption: A multitheoretical perspective. *Information and Management*, 45(2), 109-119.

24. Acquisti, A., Grossklags, J. (2005). Privacy and Rationality in Individual Decision Making. *IEEE Security & Privacy*, 3(1), 26-33.

25. Good, N., Dhamija, R., Grossklags, J., Thaw, D., Aronowitz , S., Mulligan, D., Konstan, J. (2005). *Stopping spyware at the gate: a user study of privacy, notice and spyware.* Paper presented at SOUPS '05 Proceedings of the 2005 symposium on Usable privacy and security, New York, USA.

26. İnternet: Pamuk, O. (Eylül 2010). Stuxnet'i özel yapan ne? *TÜBİTAK BİLGEM Ulusal Bilgi Güvenliği Kapısı*. Web: http://www.bilgiguvenligi.gov.tr/zararli-yazilimlar/stuxneti-ozel-yapan-ne.html adresinden 23 Ekim 2014'te alınmıştır.

27. Laboratory of Cryptography and System Security Budapest University of Technology and Economics Department of Telecommunications. (2011). Duqu: A Stuxnet-like malware found in the wild. *CrySys v0.93*, Budapest, 5-9.

28. Bencsáth, B., Pék, G., Buttyán, L. and Félegyházi, M. (2012). The Cousins of Stuxnet: Duqu, Flame, and Gauss. *Future Internet* , 4(4), 971-1003.

29. Laboratory of Cryptography and System Security Budapest University of Technology and Economics Department of Telecommunications. (31 May 2012). A complex malware for targeted attacks. *Crysis, SkyWiper-v1.05,* Budapest, 2-8.

30. Hunter, P. (2007). FBI spyware admission opens can of worms. *Computer Fraud & Security,* 2007(8), 14-15.

31. Ames, W. (2004). Understanding Spyware: Risk and Response. *IEEE Computer Society,* 6(5), 25-29.

32. Shaw, G. (2003). Spyware & Adware: the Risks facing Businesses. *Network Security,* 2003(9), 12-14.

33. Ghost, A. K., Swaminatha, T. M. (2001). Software security and privacy risks in mobile e-commerce. *Communications of the ACM,* 44(2), 51-57.

34. Aycock, J. (2010). *Spyware And Adware.*New York: Springer-Verlag New York Inc., 2-3.

35. Sağıroğlu, Ş., Canbek, G. (2009). Keyloggers Increasing Threats to Computer Security and Privacy. *IEEE Technology And Socıety Magazıne,* 2009 (Fall), 10-17.

36. Ottis, R. (2008). *Analysis of the 2007 cyber attacks against estonia from the information warfare perspective.* Paper presented at Proceedings of the 7th European Conference on Information Warfare and Security, Plymouth, UK.

37. Tulum, İ. (2006). *Bilişim suçları ile mücadele,* Yüksek Lisans Tezi, Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü, Isparta, 100-104.

38. Salimi, E. (2013). Cyber Criminology: investigating the characteristics of internet crimes and criminals. *International Journal of Law in the New Century,* 1(1), 25-37.

39. ODTÜ Bilgi İşlem Daire Başkanlığı. (2002). *LINUX İşletim Sistemi.*Ankara, ODTÜ Bilgi İşlem Daire Başkanlığı, 2-5.

40. Gosling, J., Joy, B., Steele, G. and Bracha, G. (2005). *The Java Language Specification* (Third Edition). Boston, San Francisco, New York, Toronto, Montreal, ADDISON-WESLEY, 1,4.

41. Deitel, H. M., Deitel, P. J. (2012). *C++ How To Program* (Eight Edition). New York, London, Paris, Prentice Hall,1-20.

42. Demirli, N. (2006). *Visual C# .NET 2005.* İstanbul, Palme Yayıncılık, 1-20.

43. Sukwong, O., Kim, H., Hoe, J. (2010). Commercial Antivirus Software Effectiveness: An Empirical Study. *Computer,* 44(3), 63-70.

44. Wang, T., Horng, S., Su, M. And Wu, C. (16-21 June 2006). *A Surveillance Spyware Detection System Based on Data Mining Methods*. Paper presented at Evolutionary Computation, 2006. CEC 2006. IEEE Congress on, Vancouver, BC.

45. Şenkaya, Y., Adar, U. G., (2014). *Siber Savunmada Yapay Zeka Sistemleri Üzerine İnceleme.* Akademik Bilişim 2014 Konferansında sunuldu, Mersin.

46. Kalaycı, T. E. (2006). *Yapay zeka teknikleri kullanan üç boyutlu grafik yazılımları için "Extensible 3D" (X3D) ile bir altyapı oluşturulması ve gerçekleştirimi*. Yüksek Lisans Tezi, Ege Üniversitesi Fen Bilimleri Enstitüsü, İzmir, 66-67.

47. Akyıldız, F., (2012). Kamu yönetiminde açık kaynak kodlu yazılımlar. *C.Ü. İktisadi ve İdari Bilimler Dergisi,* 13(1). 17-41.

EKLER

EK-1. Casus Yazılım Tarafından E-posta Adresine Gönderilen Bilgilere Ait Örnek

```
{ Ziraat Bankası - Google Chrome 13.5.2014 23:26:17}
{ Adsız - Google Chrome 13.5.2014 23:26:18}
{ Hoşgeldiniz | Ziraat Bankası İnternet Bankacılığı - Google
Chrome 13.5.2014 23:26:18}
40046421[TAB]BankacılıkSifrem
{ Ziraat Bankası - Google Chrome 13.5.2014 23:26:41}
{ Bilişim Enstitüsü - Google Chrome 13.5.2014 23:26:43}
{ Yüksek_Lisans_Tez_Taslağı - Microsoft Word 13.5.2014 23:26:56}
Bu doküman yüksek lisans kapsamında hazırlanan Tez dosyasıdır.
{ Bilişim Enstitüsü - Google Chrome 13.5.2014 23:27:24}
GERÇEK IP ve YER BİLGİLERİ
IP: 78.162.45.166
Hostname: 78.162.45.166.dynamic.ttnet.com.tr
ISP: Turk Telekom
Organization: Turk Telekom
City: Ankara
Region: Ankara
Country: Turkey
Timezone: Asia/Istanbul
Longitude: 32.840300
Latitude: 39.911700

BİLGİSAYAR YEREL IP BILGILERI

Windows IP Configuration
Ethernet adapter Yerel A§ Ba§lant□s□ 2:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Yerel A§ Ba§lant□s□* 4:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Ethernet adapter Ethernet 2:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Ethernet adapter Bluetooth A§ Ba§lant□s□:
Media State . . . . . : Media disconnected
```

EK-1. (devam) Casus Yazılım Tarafından E-posta Adresine Gönderilen Bilgilere Ait Örnek

```
Connection-specific DNS Suffix . :
Wireless LAN adapterWi-Fi:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::a14f:5251:57ae:b8d1%13
IPv4 Address. . . . . . . . . . . : 192.168.2.131
SubnetMask . . . . . . . . . . . . : 255.255.255.0
DefaultGateway . . . . . . . . . : 192.168.2.1
Ethernet adapterVMware Network Adapter VMnet1:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::75c9:a1bd:dbc5:8114%24
IPv4 Address. . . . . . . . . . . : 192.168.174.1
SubnetMask . . . . . . . . . . . . : 255.255.255.0
DefaultGateway . . . . . . . . . :
Ethernet adapterVMware Network Adapter VMnet8:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::ed37:93aa:f14a:2218%26
IPv4 Address. . . . . . . . . . . : 192.168.232.1
SubnetMask . . . . . . . . . . . . : 255.255.255.0
DefaultGateway . . . . . . . . . :
Ethernet adapterVirtualBox Host-Only Network:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::90e2:4cdc:8611:f530%31
IPv4 Address. . . . . . . . . . . : 192.168.56.1
SubnetMask . . . . . . . . . . . . : 255.255.255.0
DefaultGateway . . . . . . . . . :
Tunneladapterisatap.{3ED4699E-B3D6-4864-BC94-B1FC278007D3}:
Media State . . . . . . . . . . . : Media disconnected
Connection-specific DNS Suffix . :
TunneladapterTeredoTunnelingPseudo-Interface:
Media State . . . . . . . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Tunneladapterisatap.{91E269CB-CB29-4F07-BCFF-AE80C57009C7}:
Media State . . . . . . . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Tunneladapterisatap.{F2021E15-A998-4CB4-B6C9-9F295ACA962A}:
Media State . . . . . . . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Tunneladapterisatap.{D9C8C048-E9C6-40FB-AEEC-11458122836F}:
Media State . . . . . . . . . . . : Media disconnected
Connection-specific DNS Suffix . :
```

EK-1. (devam) Casus Yazılım Tarafından E-posta Adresine Gönderilen Bilgilere Ait Örnek

```
AÇIK PORTLAR

Active Connections
ProtoLocalAddressForeignAddressState
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:443 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:554 0.0.0.0:0 LISTENING
TCP 0.0.0.0:902 0.0.0.0:0 LISTENING
TCP 0.0.0.0:912 0.0.0.0:0 LISTENING
TCP 0.0.0.0:2869 0.0.0.0:0 LISTENING
TCP 0.0.0.0:5357 0.0.0.0:0 LISTENING
TCP 0.0.0.0:9089 0.0.0.0:0 LISTENING
TCP 0.0.0.0:9393 0.0.0.0:0 LISTENING
TCP 0.0.0.0:9494 0.0.0.0:0 LISTENING
TCP 0.0.0.0:10243 0.0.0.0:0 LISTENING
TCP 0.0.0.0:15990 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49152 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49153 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49154 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49156 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49157 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49158 0.0.0.0:0 LISTENING
TCP 0.0.0.0:54321 0.0.0.0:0 LISTENING
TCP 0.0.0.0:56789 0.0.0.0:0 LISTENING
TCP 127.0.0.1:5939 0.0.0.0:0 LISTENING
TCP 127.0.0.1:6543 0.0.0.0:0 LISTENING
TCP 127.0.0.1:6543 127.0.0.1:57695 ESTABLISHED
TCP 127.0.0.1:6544 0.0.0.0:0 LISTENING
TCP 127.0.0.1:8307 0.0.0.0:0 LISTENING
TCP 127.0.0.1:12001 0.0.0.0:0 LISTENING
TCP 127.0.0.1:28091 0.0.0.0:0 LISTENING
TCP 127.0.0.1:28091 127.0.0.1:57685 ESTABLISHED
TCP 127.0.0.1:50000 0.0.0.0:0 LISTENING
TCP 127.0.0.1:52001 0.0.0.0:0 LISTENING
TCP 127.0.0.1:52001 127.0.0.1:57696 ESTABLISHED
TCP 127.0.0.1:52001 127.0.0.1:57697 ESTABLISHED
TCP 127.0.0.1:52001 127.0.0.1:57698 ESTABLISHED
TCP 127.0.0.1:52001 127.0.0.1:57699 ESTABLISHED
TCP 127.0.0.1:57685 127.0.0.1:28091 ESTABLISHED
TCP 127.0.0.1:57695 127.0.0.1:6543 ESTABLISHED
TCP 127.0.0.1:57696 127.0.0.1:52001 ESTABLISHED
TCP 127.0.0.1:57697 127.0.0.1:52001 ESTABLISHED
TCP 127.0.0.1:57698 127.0.0.1:52001 ESTABLISHED
TCP 127.0.0.1:57699 127.0.0.1:52001 ESTABLISHED
TCP 192.168.2.131:139 0.0.0.0:0 LISTENING
```

EK-1. (devam) Casus Yazılım Tarafından E-posta Adresine Gönderilen Bilgilere Ait Örnek

```
TCP 192.168.2.131:57750 157.56.124.152:443 ESTABLISHED
TCP 192.168.2.131:58434 107.170.115.234:443 CLOSE_WAIT
TCP 192.168.2.131:59067 195.175.116.41:80 CLOSE_WAIT
TCP 192.168.2.131:59068 195.175.116.41:80 CLOSE_WAIT
TCP 192.168.2.131:59069 195.175.116.41:80 CLOSE_WAIT
TCP 192.168.2.131:59070 195.175.116.41:80 CLOSE_WAIT
TCP 192.168.2.131:59071 195.175.116.41:80 CLOSE_WAIT
TCP 192.168.2.131:59110 23.33.15.21:443 ESTABLISHED
TCP 192.168.2.131:59143 193.149.92.171:443 ESTABLISHED
TCP 192.168.2.131:59144 157.56.192.114:443 ESTABLISHED
TCP 192.168.2.131:59177 195.177.206.17:80 TIME_WAIT
TCP 192.168.2.131:59178 195.177.206.17:80 TIME_WAIT
TCP 192.168.2.131:59179 195.177.206.17:80 TIME_WAIT
TCP 192.168.2.131:59180 195.177.206.17:80 TIME_WAIT
TCP 192.168.2.131:59181 195.177.206.17:80 TIME_WAIT
TCP 192.168.2.131:59182 195.177.206.17:80 TIME_WAIT
TCP 192.168.2.131:59183 64.15.117.26:443 TIME_WAIT
TCP 192.168.2.131:59185 195.177.206.156:443 ESTABLISHED
TCP 192.168.2.131:59186 195.177.206.156:443 ESTABLISHED
TCP 192.168.2.131:59193 23.33.8.144:443 ESTABLISHED
TCP 192.168.2.131:59197 23.52.244.185:443 ESTABLISHED
TCP 192.168.2.131:59201 173.194.79.136:443 ESTABLISHED
TCP 192.168.2.131:59205 64.15.117.52:443 ESTABLISHED
TCP 192.168.2.131:59206 64.15.117.212:443 ESTABLISHED
TCP 192.168.2.131:59207 64.15.117.123:443 ESTABLISHED
TCP 192.168.2.131:59208 194.27.18.25:80 ESTABLISHED
TCP 192.168.2.131:59209 64.15.117.116:80 ESTABLISHED
TCP 192.168.2.131:59210 144.76.38.180:80 ESTABLISHED
TCP 192.168.56.1:139 0.0.0.0:0 LISTENING
TCP 192.168.174.1:139 0.0.0.0:0 LISTENING
TCP 192.168.232.1:139 0.0.0.0:0 LISTENING
TCP [::]:135 [::]:0 LISTENING
TCP [::]:443 [::]:0 LISTENING
TCP [::]:445 [::]:0 LISTENING
TCP [::]:554 [::]:0 LISTENING
TCP [::]:2869 [::]:0 LISTENING
TCP [::]:3587 [::]:0 LISTENING
TCP [::]:5357 [::]:0 LISTENING
TCP [::]:9089 [::]:0 LISTENING
TCP [::]:9393 [::]:0 LISTENING
TCP [::]:9494 [::]:0 LISTENING
TCP [::]:10243 [::]:0 LISTENING
TCP [::]:49152 [::]:0 LISTENING
TCP [::]:49153 [::]:0 LISTENING
TCP [::]:56789 [::]:0 LISTENING
```

EK-1. (devam) Casus Yazılım Tarafından E-posta Adresine Gönderilen Bilgilere Ait Örnek

```
TCP [::1]:8307 [::]:0 LISTENING
TCP [::1]:9393 [::1]:57700 ESTABLISHED
TCP [::1]:12001 [::]:0 LISTENING
TCP [::1]:49155 [::]:0 LISTENING
TCP [::1]:57700 [::1]:9393 ESTABLISHED
UDP 0.0.0.0:68 *:*
UDP 0.0.0.0:500 *:*
UDP 0.0.0.0:3702 *:*
UDP 0.0.0.0:3702 *:*
UDP 0.0.0.0:3702 *:*
UDP 0.0.0.0:3702 *:*
UDP 0.0.0.0:3702 *:*
UDP 0.0.0.0:3702 *:*
UDP 0.0.0.0:4500 *:*
UDP 0.0.0.0:5004 *:*
UDP 0.0.0.0:5005 *:*
UDP 0.0.0.0:5355 *:*
UDP 0.0.0.0:56104 *:*
UDP 0.0.0.0:61712 *:*
UDP 0.0.0.0:62686 *:*
UDP 127.0.0.1:1900 *:*
UDP 127.0.0.1:53494 *:*
UDP 127.0.0.1:62136 *:*
UDP 192.168.2.131:137 *:*
UDP 192.168.2.131:138 *:*
UDP 192.168.2.131:1900 *:*
UDP 192.168.2.131:62132 *:*
UDP 192.168.56.1:137 *:*
UDP 192.168.56.1:138 *:*
UDP 192.168.56.1:1900 *:*
UDP 192.168.56.1:62135 *:*
UDP 192.168.174.1:137 *:*
UDP 192.168.174.1:138 *:*
UDP 192.168.174.1:1900 *:*
UDP 192.168.174.1:62133 *:*
UDP 192.168.232.1:137 *:*
UDP 192.168.232.1:138 *:*
UDP 192.168.232.1:1900 *:*
UDP 192.168.232.1:62134 *:*
UDP [::]:500 *:*
UDP [::]:3540 *:*
UDP [::]:3702 *:*
UDP [::]:3702 *:*
UDP [::]:3702 *:*
UDP [::]:61713 *:*
UDP [::]:62687 *:*
```

EK-1. (devam) Casus Yazılım Tarafından E-posta Adresine Gönderilen Bilgilere Ait Örnek

```
UDP [::1]:62131 *:*
UDP [fe80::75c9:a1bd:dbc5:8114%24]:1900 *:*
UDP [fe80::75c9:a1bd:dbc5:8114%24]:62128 *:*
UDP [fe80::90e2:4cdc:8611:f530%31]:1900 *:*
UDP [fe80::90e2:4cdc:8611:f530%31]:62130 *:*
UDP [fe80::a14f:5251:57ae:b8d1%13]:546 *:*
UDP [fe80::a14f:5251:57ae:b8d1%13]:1900 *:*
UDP [fe80::a14f:5251:57ae:b8d1%13]:62127 *:*
UDP [fe80::ed37:93aa:f14a:2218%26]:1900 *:*
UDP [fe80::ed37:93aa:f14a:2218%26]:62129 *:*

AÇIK UYGULAMALAR

Image Name PID Session Name Session# MemUsage
========================= ======== ================ ===========
============
SystemIdleProcess 0 Services 0 20 K
System 4 Services 0 5.332 K
smss.exe 332 Services 0 540 K
csrss.exe 620 Services 0 3.472 K
wininit.exe 752 Services 0 2.516 K
services.exe 856 Services 0 10.592 K
lsass.exe 864 Services 0 11.268 K
svchost.exe 972 Services 0 8.680 K
svchost.exe 1012 Services 0 8.396 K
atiesrxx.exe 628 Services 0 1.764 K
svchost.exe 768 Services 0 26.404 K
svchost.exe 908 Services 0 62.784 K
svchost.exe 1124 Services 0 21.880 K
svchost.exe 1164 Services 0 90.080 K
RwcTaskService.exe 1276 Services 0 1.492 K
svchost.exe 1408 Services 0 24.912 K
spoolsv.exe 1644 Services 0 5.064 K
svchost.exe 1700 Services 0 34.452 K
NetworkLicenseServer.exe 1868 Services 0 4.608 K
apnmcp.exe 1920 Services 0 4.248 K
HuaweiHiSuiteService64.ex 1184 Services 0 2.076 K
dasHost.exe 380 Services 0 13.696 K
HeciServer.exe 1652 Services 0 1.520 K
Jhi_service.exe 952 Services 0 1.016 K
KinectManagementService.e 2020 Services 0 1.900 K
SpotfluxConnectionManager 2176 Services 0 50.644 K
svchost.exe 2288 Services 0 4.588 K
TeamViewer_Service.exe 2376 Services 0 5.856 K
vmware-usbarbitrator64.ex 2404 Services 0 2.512 K
vmnat.exe 2492 Services 0 2.552 K
```

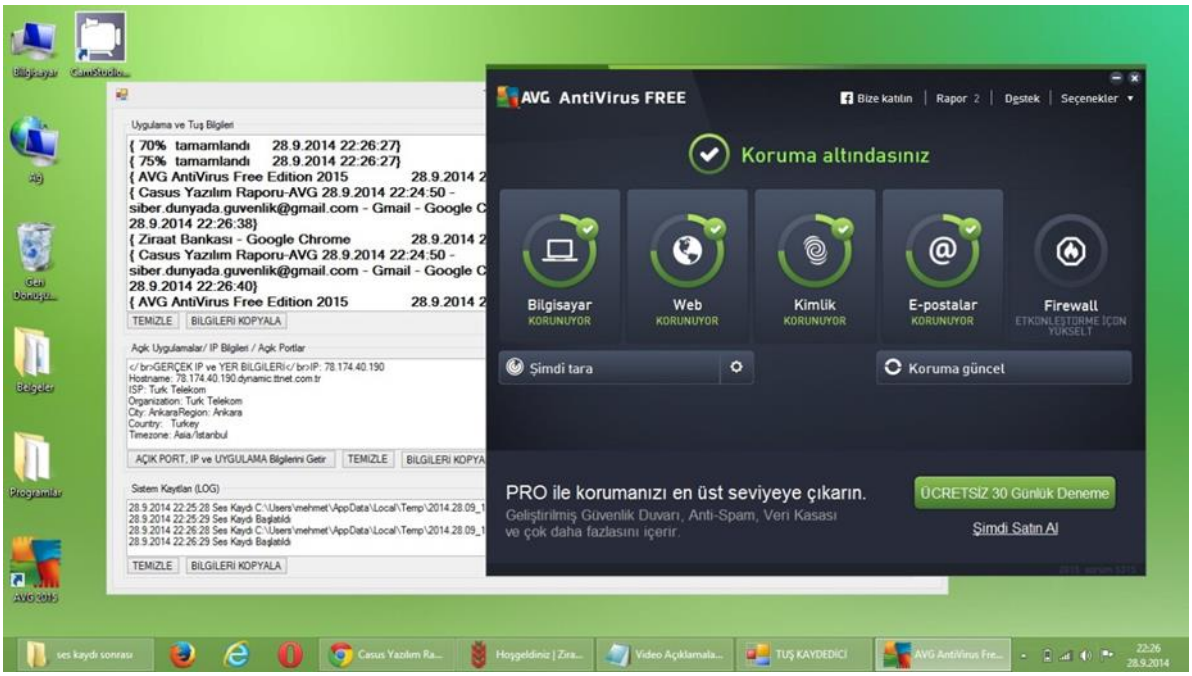
EK-1. (devam) Casus Yazılım Tarafından E-posta Adresine Gönderilen Bilgilere Ait Örnek

```
vmware-converter-a.exe 2528 Services 0 10.172 K
vmware-converter.exe 2572 Services 0 15.484 K
vmware-converter.exe 2608 Services 0 10.656 K
MsMpEng.exe 2656 Services 0 107.728 K
Ath_CoexAgent.exe 2780 Services 0 3.528 K
vmware-authd.exe 2848 Services 0 5.076 K
vmnetdhcp.exe 2064 Services 0 1.148 K
vmware-hostd.exe 1828 Services 0 27.384 K
WmiPrvSE.exe 2192 Services 0 9.572 K
svchost.exe 3648 Services 0 2.772 K
svchost.exe 3668 Services 0 18.580 K
svchost.exe 2808 Services 0 13.052 K
SearchIndexer.exe 4352 Services 0 44.212 K
dllhost.exe 4396 Services 0 2.920 K
IAStorDataMgrSvc.exe 4764 Services 0 23.016 K
IntelMeFWService.exe 6304 Services 0 840 K
LMS.exe 6308 Services 0 3.560 K
SWMAgent.exe 6832 Services 0 10.980 K
UNS.exe 3444 Services 0 6.512 K
wmpnetwk.exe 7132 Services 0 2.024 K
OSPPSVC.EXE 7736 Services 0 8.116 K
SpotfluxUpdateService.exe 5680 Services 0 17.220 K
PresentationFontCache.exe 6904 Services 0 18.396 K
csrss.exe 9436 Console 3 44.220 K
winlogon.exe 1196 Console 3 5.100 K
dwm.exe 7028 Console 3 27.480 K
taskhostex.exe 8860 Console 3 15.964 K
SynTPEnh.exe 8808 Console 3 936 K
explorer.exe 9664 Console 3 136.672 K
ismagent.exe 8168 Console 3 3.256 K
taskhost.exe 9472 Console 3 816 K
updateui.exe 2060 Console 3 3.120 K
RAVCpl64.exe 7880 Console 3 9.440 K
BtTray.exe 8320 Console 3 48.804 K
BtvStack.exe 8044 Console 3 22.100 K
igfxtray.exe 4456 Console 3 5.908 K
ActivateDesktop.exe 1396 Console 3 4.632 K
hkcmd.exe 5488 Console 3 5.640 K
igfxpers.exe 4364 Console 3 8.304 K
IDMan.exe 1336 Console 3 31.936 K
IEMonitor.exe 9548 Console 3 5.700 K
SpotfluxAgent.exe 7792 Console 3 80.148 K
vmware-tray.exe 3224 Console 3 4.912 K
TBNotifier.exe 9744 Console 3 12.924 K
vntldr.exe 3976 Console 3 4.752 K
SynTPHelper.exe 9884 Console 3 292 K
```

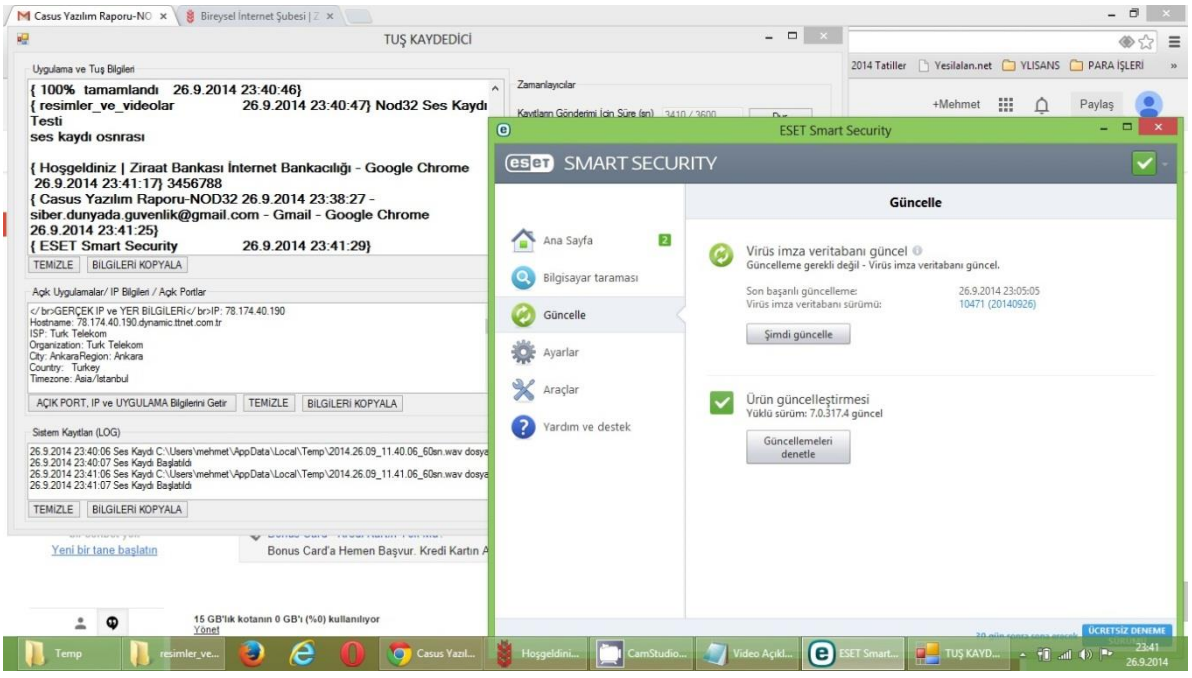
EK-1. (devam) Casus Yazılım Tarafından E-posta Adresine Gönderilen Bilgilere Ait Örnek

```
CommonAgent.exe 9840 Console 3 440 K
IAStorIcon.exe 9508 Console 3 26.240 K
MOM.exe 668 Console 3 4.444 K
CCC.exe 428 Console 3 5.696 K
LiveComm.exe 9724 Console 3 2.572 K
RuntimeBroker.exe 580 Console 3 4.388 K
WINWORD.EXE 8216 Console 3 85.288 K
splwow64.exe 7688 Console 3 7.792 K
chrome.exe 5696 Console 3 90.580 K
chrome.exe 10128 Console 3 105.892 K
chrome.exe 9728 Console 3 64.628 K
chrome.exe 4612 Console 3 51.120 K
AdobeARM.exe 4272 Console 3 11.344 K
chrome.exe 8316 Console 3 98.696 K
chrome.exe 9412 Console 3 77.572 K
notepad.exe 7724 Console 3 6.388 K
cy.exe 5008 Console 3 30.800 K
tasklist.exe 8800 Console 3 5.400 K
conhost.exe 1136 Console 3 3.084 K
```

EK-2. Casus Yazılımı Tespit Edemeyen Koruyucu Yazılım Ekran Görüntüleri

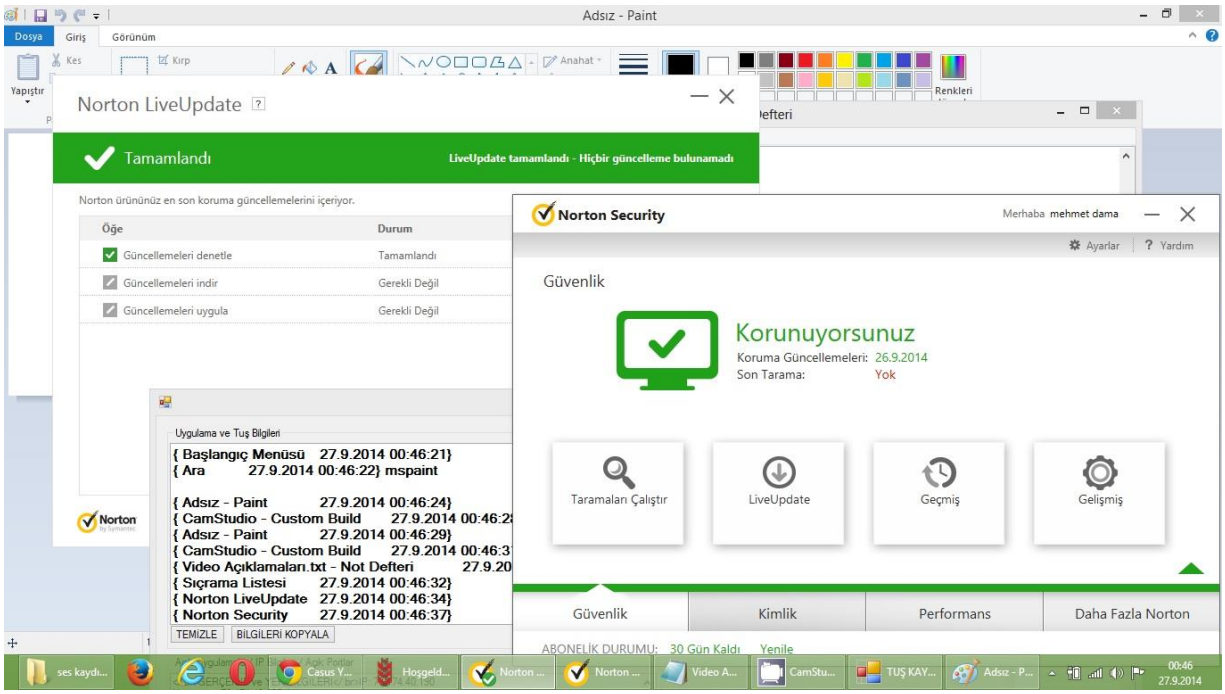


Resim 2.1. "AVG AntiVirus Free" yazılımına ait ekran görüntüsü

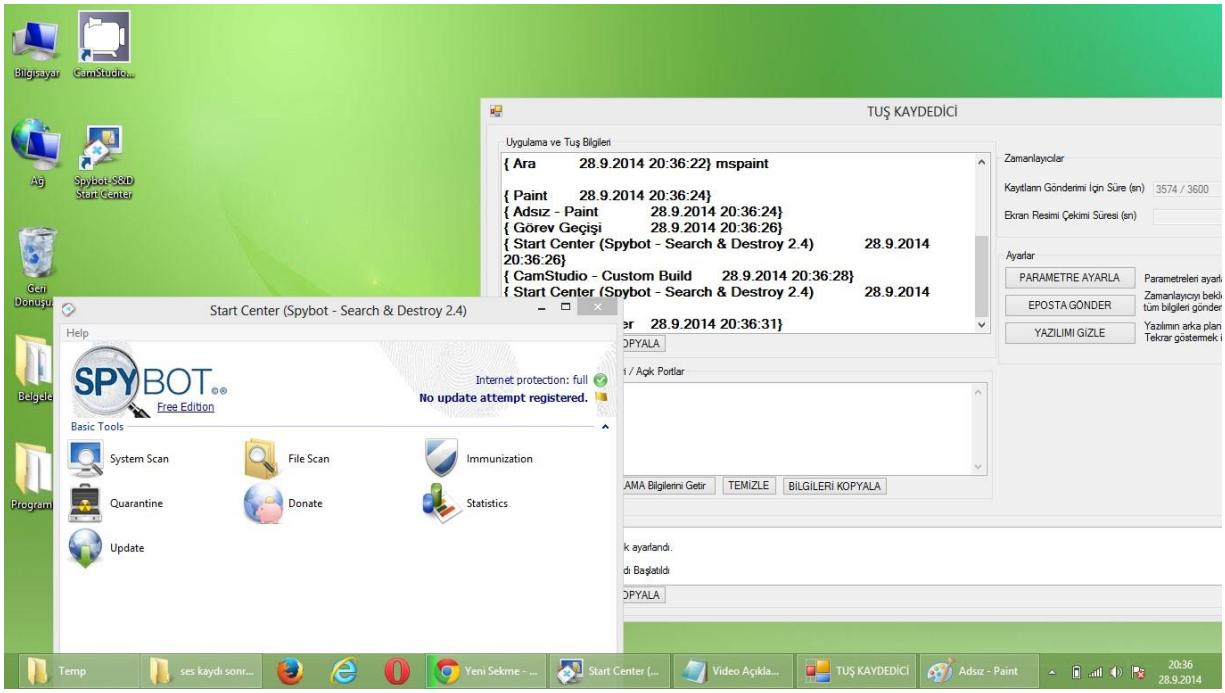


Resim 2.2. "NOD 32" yazılımına ait ekran görüntüsü

EK-2. (devam) Casus Yazılımı Tespit Edemeyen Koruyucu Yazılım Ekran Görüntüleri

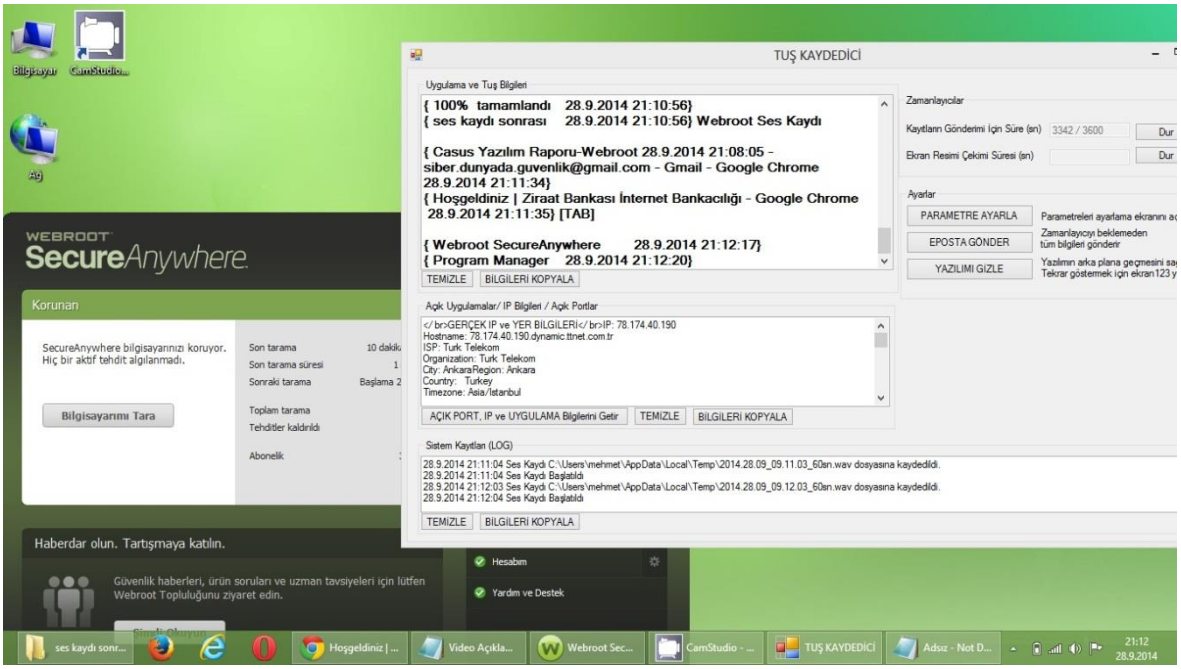


Resim 2.3. "Norton Security" yazılımına ait ekran görüntüsü

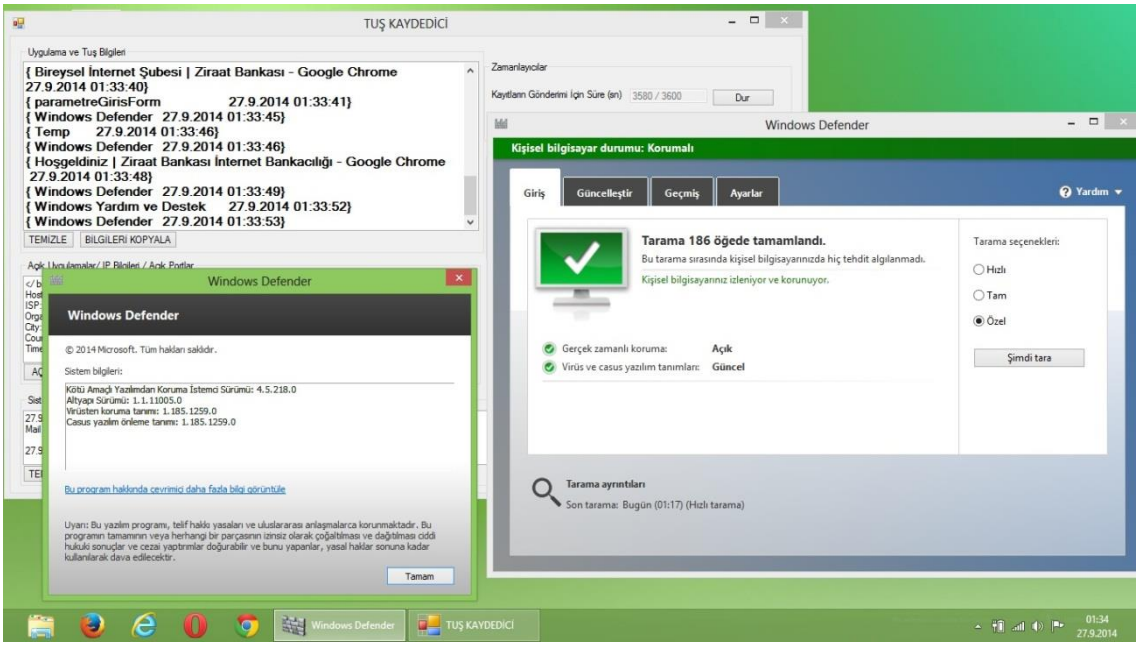


Resim 2.4. "SPYBOT" yazılımına ait ekran görüntüsü

EK-2. (devam) Casus Yazılımı Tespit Edemeyen Koruyucu Yazılım Ekran Görüntüleri

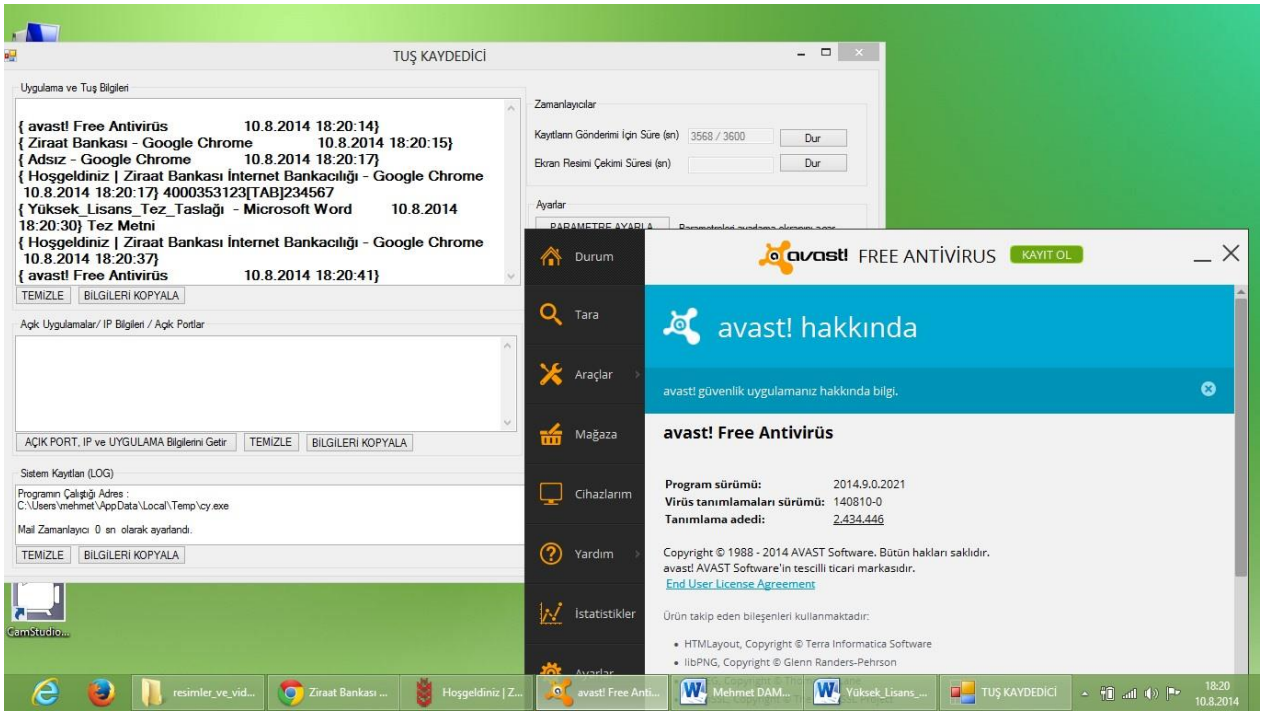


Resim 2.5. “WEBROOT Secure AnyWhere” yazılımına ait ekran görüntüsü



Resim 2.6. “Windows Defender” yazılımına ait ekran görüntüsü

EK-2. (devam) Casus Yazılımı Tespit Edemeyen Koruyucu Yazılım Ekran Görüntüleri



Resim 2.7. “Avast” yazılımına ait ekran görüntüsü

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı	:	DAMA, Mehmet
Uyruğu	:	T.C.
Doğum tarihi ve yeri	:	02/01/1986 Trabzon
Medeni hali	:	Evli
Telefon	:	0 (533) 818 84 47
e-posta	:	damamehmet@hotmail.com

Eğitim Derecesi	Okul/Program	Mezuniyet yılı
Yüksek lisans	Gazi Üniversitesi /Bilişim Sistemleri	Devam Ediyor
Lisans	Anadolu Üniversitesi/ Bilgisayar Mühendisliği	2007

İş Deneyimi, Yıl	Çalıştığı Yer	Görev
2012- devam ediyor	Savunma Sanayii Müsteşarlığı	Uzman Yardımcısı
2011-2012	Kredi Yurtlar Kurumu	Mühendis
2009-2011	İçişleri Bakanlığı	Mühendis

Yabancı Dili

İngilizce

Yayınlar

1. Dama, M., Ciylan, B. (2014). Casus yazılımların siber güvenlik açısından oluşturduğu risklere deneysel yaklaşım. *SAVTEK2014 7.Savunma Teknolojileri Kongresinde sunulmuştur, Ankara, ODTÜ.*

GAZİ GELECEKTİR...