Windows Registry ile Bilgisayar Güvenliğinin Sağlanması

Nursel YALÇIN, Mehmet Serkan KILIÇ

Gazi Üniversitesi, Bilişim Enstitüsü, Bilişim Sistemleri
nyalcin@gazi.edu.tr mserkanklc@hotmail.com.tr
(Geliş/Received:26.02.2016; Kabul/Accepted:09.10.2016)
DOI: 10.17671/btd.34632

***Özet*—**Bu çalışmada, Windows İşletim Sistemlerinde bulunan ve sistemin veritabanı olarak tanımlanan windows registry'nin, bilgisayar güvenliğinin sağlanmasındaki rolü ele alınmıştır. Windows registry; başlangıçta çalışan uygulamalar, kurulu programlar, MS office dosya bilgileri, taşınabilir bellekler, paylaşım dosyaları, sanal makine bilgisi gibi çok sayıda ve farklı verileri kaydetmektedir. Çalışmada bu kayıtlar bilgisayar güvenliği bağlamında irdelenmiştir. Windows registry'de yer alan kayıtların incelenmesi, analizi ve bu kayıtlar üzerinde yapılacak değişiklikler ile kişisel bilgisayar güvenliğinin sağlanması arasında yakın bir ilişki bulunmaktadır. Çalışmada zararlı yazılımların tespit edilmesi açısından 4; bilgisayarda bulunan bazı fonksiyonların engellenmesi açısından 24 ve bilgisayarda gerçekleşen işlemlerin denetlemesi açısından 27 olmak üzere toplam 55 işleme ait windows registry girdisi incelenmiş ve değerlendirmelerde bulunulmuştur. Elde edilen sonuçlar ise özet tablolar haline sunulmuştur.

***Anahtar Kelimeler*—**Windows Kayıtları, Bilgisayar Güvenliği, İşletim Sistemi Güvenliği, Zararlı Yazılım Tespiti

Ensuring The Computer Security with Windows Registry

***Abstract*—**In this study, discussed the role of windows registry, which is database of windows operating system, in computer security. Windows registry is recorded different type of information like startup applications, installed applications, MS office document information, Portable Memory Storages information, shared folders, virtual computers. In study, this records are examined in the context of computer security. There is a close relationship between examining, analyzing and making same changes in the records of windows registry and ensuring the personel computer security. In study, totaly 55 windows registry keys and their functions are examined. 4 of them are related to detecting malicious software, 24 of them are related to preventing same functions of computer and 27 of them are related to auditing of process in computers. The results which are obtained are presented by summary tables.

***Keywords*—**Windows Registry, Computer Security, Operating System Security, Detect Malicious Software

1. GİRİŞ (INTRODUCTION)

Bilgi güvenliği kavramı, herkesin kullanımına açık bilgiye herkesin kolaylıkla erişmesi, herkesin kullanımına açık olmayan bilgiye ise sadece yetkili kişilerin erişmesi olarak ele alınmaktadır. Bu bağlamda "bütünlük" ve "erişilebilirlik" ilkeleri çerçevesinde bilgiye erişim güvenliği güvence altına alınmakta iken "gizlilik" ilkesi çerçevesinde ise yetkili erişim güvence altına alınmaktadır. Günümüzde en yaygın kullanılan bilişim ürününün bilgisayarlar olması sebebi ile en fazla tehdit de yine bilgisayarlar için söz konusudur. Bununla beraber bilgisayar güvenliğinde alınacak tedbirlerin çok disiplinli bir konu olduğu açıktır. Bilgisayar donanımlarının üretim aşamasında suiistimal riski, işletim sistemi açıklıkları, kullanılan yazılımlara ait kod güvenliği, tercih edilen antivirüs yazılımının kabiliyeti, son kullanıcı farkındalığı, meraklı iş arkadaşları, rakip firma çalışanlarının art niyetli amaçları gibi onlarca şekilde güvenlik tehdidi söz konusu olabilmektedir. Tüm bu güvenlik tehditlerinin tam bir listesini yapılması ise mümkün değildir.

Bilgisayar teknolojisinin; insan hayatını kolaylaştırmak için sürekli değişim içerisinde bulunması ve gelişmesinin doğal sonucu olarak, bilgi ve bilgisayar güvenliğinin önemi ve karşılaşılan tehditler, gerek sayı gerekse de çeşitlilik açısından artmaktadır[1]. Bilgisayar güvenliğinin sağlanması için birçok yazılım şirketi tarafından büyük yatırımlar yapılarak ticari ürünlerinin güvenli olmasına çalışılmasına rağmen en büyük tehdidin kullanılan kişisel bilgisayarlar ve kullanıcılardan kaynaklandığının belirtilmesi, [2] bilgisayar güvenliğinin sağlanmasında son kullanıcı farkındalığı ve kullanıcılar tarafından alınacak önlemlerin önemini ortaya koymaktadır.

Hayatın vazgeçilmez ve zorunlu bir aracı haline gelen bilgisayarların özel hayatın gizliliği, haberleşme hürriyeti, fikri ve sınai haklar açısından risk seviyesi en aza indirgenmiş şekilde gönül rahatlığı ile kullanılabilmesi tüm insanların en doğal beklentisidir. Bu beklentinin karşılanması ise ülkeler tarafından makro düzeyde ele alınan siber güvenlik ve siber savunma algısının son kullanıcılar açısından mikro düzeye indirgenmesi ile olacaktır. Bilgisayar güvenliğinin sağlanması için alınacak tedbirlerin, savaş terminolojisine uygun olarak savunma şeklinde tanımlanması ve savunma çerçevesinde ele alınması ise konuya çok detaylı şekilde yaklaşmayı zorunu kılmaktadır.

Bu çalışmada windows registry ile bilgisayar güvenliği arasında nasıl bir ilişki bulunduğu irdelenmiş ve "windows registry ile bilgisayar güvenliği nasıl sağlanır?" sorusuna somut cevaplar aranmaya çalışılmıştır. Günümüzde son derece önemli olan bilgisayar güvenliğinin gelecekte de artan bir şekilde önem arz ettiği düşünüldüğünde, bu çalışmanın kişisel bilgisayar güvenliğini sağlamada önemli olacağı düşünülmektedir. Bu nedenle çalışmanın windows registry konusunda daha önce bilgi sahibi olmayanların dahi rahatlıkla anlayabileceği şekilde hazırlanılması amaçlanmıştır.

Çalışmanın ilk bölümünde Windows İşletim Sitemi ve Windows Registry hakkında genel bilgi verilmiş, veri yığınlarının (hive) işlevleri açıklanmış ve Registry üzerinde manuel olarak değişiklik yapılabilmesine imkân sağlayan kayıt defteri düzenleyicisine değinilmiştir. İkinci bölümde ise araştırma sorusuna cevap aramaya çalışılmış ve 100'e yakın windows registry girdisi (yapılandırma ayarı kaydı) incelenmiştir. İnceleme sonucu, 55 windows registry girdisinin bilgisayar güvenliği bağlamında önemli işlevlere sahip olduğu anlaşılmıştır. Buna göre; windows registry'de yer alan kayıtların incelenmesi ve analizi ile bilgisayarda zararlı yazılım bulunduğu tespitinin yapılabilmesi, bilgisayar sahibinin bilgisi dışında yapılabilecek bazı işlemlerin engellenmesi ve bilgisayar üzerinde gerçekleşen işlemlerin bilgisayar sahibinin bilgisi dışında yapılıp yapılmadığının anlaşılmasının mümkün olduğu görülmüştür. Elde edilen bulgular 3 alt başlık altında toplamış ve bu başlıklar altında zararlı yazılımların tespit edilmesi açısından 4; bilgisayarda bulunan bazı fonksiyonların engellenmesi açısından 24 ve bilgisayarda gerçekleşen işlemlerin denetlemesi açısından 27 windows registry girdisine özet tablo halinde yer verilmiştir. Çalışmanın son bölümü olan sonuç ve değerlendirme kısmında ise çalışmanın genel bir değerlendirmesi yapılarak elde edilen bulgular maddeler halinde sıralanmıştır.

Yapılan literatür çalışmasında windows registry ile bilgisayar güvenliğinin sağlanması konusunda akademik her hangi yerli bir kaynağa rastlanamamış, yabancı kaynakların ise büyük çoğunluğunda windows registry' nin çok genel bir şekilde işlev ve fonksiyonları ile ele alındığı, bir kısım çalışmalarda ise yer yer bilgisayar güvenliğine atıflarda bulunulduğu gözlemlenmiştir. Bu açıdan tamamı windows 7 işletim sisteminde test edilmiş uygulama sonuçlarının yer aldığı "Windows Registry ile Bilgisayar Güvenliği" ismi ile hazırlanan bu çalışmanın alanında özgün olduğu değerlendirilmektedir. Diğer taraftan windows registry'nin çok geniş bir konu olması ve çok farklı işlevlere sahip windows registry girdilerinin bulunması çalışmanın en büyük sınırlılığıdır.

2. WINDOWS İŞLETİM SİSTEMİ VE WINDOWS REGISTRY (WINDOWS OPERATING SYSTEM AND WINDOWS REGISTRY)

İşletim sistemi, bilgisayar sistemini oluşturan donanım ve yazılım nitelikli kaynakları kullanıcılar arasında kolay, hızlı ve güvenli bir şekilde paylaştıran ve bu kaynakları yöneten bir yazılım sistemidir [3]. İngilizce Operating System'in kısaltılmış hali olan OS olarak da bilinen işletim sistemi; insanoğlu tarafından yapılan en karmaşık yapılardan biridir. Diğer taraftan işletim sistemi, eş zamanlı olarak işlemlerin yapıldığı, izin ve yetkilerin kontrol edildiği, yetkisiz erişimler için verilerin korunduğu, donanımsal ürünler ile etkileşim halinde olan bir yazılımdır [4].

Hayatın her alanında kullanılan bilgisayar medyalarının kullanım yeri ve amaçları açısından farklılıklar bulunsa da ortak olan en büyük özellikleri birer işletim sistemine sahip olmalarıdır. Bilgisayarlar, cep telefonları, güvenlik kamerası kayıt sistemleri, mp3 çalarlar v.s. gibi teknolojik cihazlar kendi işlevlerini yerine getirebilecek birer işletim sistemine ihtiyaç duymaktadırlar. Kullanım yeri (kişisel bilgisayar, sunucu, mobil, gömülü sistemler, vs.) açısından farklı yapıda işletim sistemleri bulunmakla birlikte windows işletim sistemi, kullanım yaygınlığı ile en çok tercih edilen işletim sistemi olarak ön plana çıkmaktadır.

Windows işletim sisteminin ev ve ofis kullanımında yoğun olarak tercih edilmesi, bilgisayar saldırılarında bu işletim sistemini öne çıkarmakta ve bilişim uzmanları tarafından bu işletim sisteminin detaylı olarak bilinmesini gerektirmektedir [5]. Diğer taraftan windows işletim sisteminin hiyerarşik yapısı sayesinde, bu yapının anlaşılması ve buna göre yazılım geliştirilmesi ise zor olmamaktadır [4]. Bilgisayar güvenliğini sağlayacak uzmanlar açısından da, windows işletim sisteminin yapısı, varsayılan ayarlar, windows registry yapısı, burada oluşan kayıtlar gibi konularda derinlemesine bilgi sahibi olmaları beklenmektedir.

İngilizce liste anlamına gelen "regis" kökünden türeyen "registry" kelimesi dilimize kayıt, tescil, sicil, kütük, defter, sicil dairesi, evlendirme dairesi, defterhane vb. şekilde çevrilmektedir. Benzer şekilde; registry book terimi sicil defteri, court registry terimi tapu kaydı, land registry terimi nüfus defteri ve cancer registry terimi kanser kaydı olarak kullanılmaktadır.

Windows registry, windows işletim sistemi veri tabanıdır. Sistem donanımları, kurulu programlar, ayarlar, her bir kullanıcıya ait hesap profili gibi önemli bilgileri içermekte ve windows tarafından devamlı güncellenmektedir [6]. Kullanıcıların büyük bölümü tarafından bu bilgilere doğrudan erişim sağlanma tercih edilmemekte ve tüm windows işletim sistemi versiyonlarında bulunan registry editor (regedit.exe) kullanılarak erişim sağlanmakta ve ihtiyaç duyulan değişiklikler yapılmaktadır.

Registry editör haricinde windows registry'i görüntülemek ve değişiklikleri izlemek için farklı uygulamalar bulunmaktadır. İşletim sistemi ve diğer uygulamaların registry üzerinde oluşturdukları kayıtları görmek için registry monitor ve windows 98 işletim sistemi ile birlikte gelen registry checker (scanreg.exe) kullanılabilmektedir [7].

Diğer taraftan mevcut adli bilişim yazılımları ve 3.parti registry editör yazılımlarının tamamına yakını, windows 7 işletim sistemine kadar olan ürünlerde başarılı iken windows 8 registry analizinde; registry ripper ve registry decoder isimli yazılımların ön plana çıktığı ve windows registry'i başarılı bir şekilde çözümlediği (decode) yapılan testler sonuçlarından anlaşılmıştır [8].

Windows registry, işletim sistemi dâhil sistem üzerinde bulunan bütün programlar ve uygulamalar için çok sayıda yapılandırma ayarının tutulduğu bir kılavuzdur. Buradaki değerler, gerek bilgisayar kullanıcısının kimliği gerekse de bilgisayardaki yazılımların hangi ayarlar ve özelliklerle çalıştırıldığını gösteren hassas verileri taşımaktadır (Çalışkan, 2013:39). Windows registry, 5 ana yığından (hive) oluşmakta olup bu yapı tablo-1'de gösterilmiştir.

Tablo 1. Registry Ana Yığınları (Registry Main Hives) (Çalışkan, 2013:40)

İsim	Kısaltma	Tanım
HKEY_CLASSES_ROOT	HKCR	Dosya uzantı bilgileri, hangi tip dosyanın hangi programla açılması gerektiği ve dosya tipleriyle ilgili tanımlamaların yapıldığı gruptur.
HKEY_CURRENT_USER	HKCU	Bu grupta uygulamaların bilgisayar kullanıcılarına özgü ayarları saklanmaktadır. Ortam değişkenleri, masaüstü ayarları ve uygulama yapılandırmalarına buna örnek olarak verilebilir.
HKEY_LOCAL_MACHINE	HKLM	Bu grupta bilgisayara özgü yapılandırma bilgileri bulunmaktadır. Donanım, SAM, güvenlik, yazılım ve sistem olmak üzere 5 alt başlığa daha ayrılmıştır.
HKEY_USERS	HKU	Bilgisayarda hali hazırda açık olan kullanıcıların ayarları ve çalıştırdıkları uygulamalara özgü çeşitli verileri taşımaktadır.
HKEY_CURRENT_CONFIG	HKCC	Bilgisayardaki donanım profili hakkında saklanan veriler bu grupta bulunmaktadır[56].

HKEY_LOCAL_MACHINE (HKLM), sistem hafızası, sürücüler ve başlangıçta çalışan uygulamaların kontrolü gibi donanım ve işletim sistemi verileri dâhil bilgisayar sistemi hakkında bilgiler içermektedir [9]. Bilgisayar kullanıcılarının en çok etkileşimli olduğu kayıtlar (SAM, SECURITY, SYSTEM ve SOFTWARE) HKLM altında bulunan anahtarlardır. SAM (Security Accounts Manager); PC'nin bağlı olduğu tüm domaindeki bilgilerin güvenlik bilgileri yer alır. Her SAM veri tabanı dosyası domain girişi kullanıcı adını ve parolasını şifreli bir şekilde tutmaktadır. Birçok kullanıcı için veri içermeyen SECURITY; domaine bağlantı yapıldıktan sonra ana serverda tanımlı güvenlik politikalarına göre şekillenmektedir. SYSTEM; Windows kurulum, ayarlar, mount edilmiş cihazlar ve sürücü bilgilerini içerir. SOFTWARE ise; Windows uygulamaları ve kurulu diğer programlara üretici tarafından belirlenen dosya uzantısı, MIME tipleri, Object Class ve ara yüz ID bilgilerini içerir [10].

Kayıt defteri düzenleyici veya benzeri programlar ile Windows registry üzerinde değişiklik yapmak mümkün iken yanlış yapılan bir değişiklik bilgisayarın düşük performans ile çalışmasına veya tamamen çalışmamasına sebep olabilmektedir [9].

Bununla beraber kayıtların dışa aktarılması (export edilmesi) da mümkündür. ".reg uzantılı" dosyalar halinde oluşturulan bu veriler registry editörler aracılığı ile okunabilmekte ve değiştirilebilmektedir. Ayrıca text editörler aracılığı ile de ".reg uzantılı" dosyalar görüntülenebilmektedir [10].

3. WINDOWS REGISTRY VE BİLSAYAR GÜVENLİĞİ (WINDOWS REGISTRY AND COMPUTER SECURITY)

Bilgisayar sistemi hakkında genel bilgiler ile uygulamalara ait geçmiş kayıtların tutulduğu yer olan registry; sistemin hızlı, tutarlı ve işlevsel olarak çalışması amacıyla otomatik olarak tutulan kayıtlardan oluşmaktadır [11].

Kullanıcı hesabı ve grubuyla ilgili veriler, MRU (Most Recently Used-Yakın Geçmiş Zaman) verileri, bilgisayara yüklenen çeşitli dosyalara ilişkin veriler, sistem saati bilgisi, taşınabilir disk bilgileri, kurulum verileri, dosya ve klasörlerin görüntülenmesiyle ilgili sınıflandırma bilgilerini tutan kabuk çantası (shellbag) verileri gibi önemli veriler registry'de tutulmaktadır [12]. Bu kayıtlar, işletim sisteminin düzgün çalışmasını sağladığı gibi bilgisayar güvenliğinin sağlanmasında da önemli rol oynamaktadırlar.

Windows registry'de yer alan kayıtların incelenmesi, analizi ve bu kayıtlar üzerinde yapılacak değişiklikler ile kişisel bilgisayar güvenliğinin sağlanması arasında yakın ilişki bulunmaktadır. Bu ilişki; registry üzerinde zararlı yazılımlara ait girdilerden hareketle zararlı yazılım

tespitinin yapılması, bilgisayar sahibinin bilgisi dışında yapılabilecek bazı işlemlerin engellenmesi ve bilgisayar üzerinde gerçekleşen işlemlerin kontrol edilerek bilgisayar sahibinin bilgisi dışında işlem yapılıp yapılmadığının anlaşılması şeklindedir.

3.1. Zararlı Yazılımların Tespit Edilmesi (Detection Of Malicious Software)

2012 yılında microsoft'un dijital sertifikalarının imzalanması için kullandığı MD5 (Message-Digest) algoritmasındaki bir güvenlik açığından faydalanılarak sahte microsoft imzaları üreten ve windows işletim sistemlerine güncelleme olarak sızdığı tespit edilen flame isimli zararlı yazılımın [13] registry üzerinde izler bıraktığı anlaşılmıştır.

Zararlı yazılım tespiti amacıyla 2012 yılında geliştirilen bir uygulama ise; prosesler, servisler, registry ve bağlantı bilgilerini analiz edecek şekilde kodlanmış olup yapılan testlerde zararlı yazılım tespitlerinin %41'inin registry analizi ile gerçekleştiği görülmüştür [14]. Bu bağlamda bilgisayarlara bulaşan zararlı yazılımların tespitinde registry analizinin önemli bir yer tuttuğu anlaşılmaktadır.

Bilişim sistemlerine yönelik yapılan saldırıların doğru bir şekilde analiz edilebilmesi için adli bilişim sürecinde zararlı yazılımların tespit edilmesine ihtiyaç duyulmaktadır [11]. Gelişen teknoloji ile beraber ortaya çıkan bu tür güvenlik tehditlerine karşı windows registry incelemelerinin önemli olduğu değerlendirilmektedir.

Bilindiği üzere, işletim sistemi açılışında, registry'de bulunan girdilere göre sürücüler(driver) ve servisler otomatik olarak başlamaktadır. Sürücüler, küçük programlar olup donanımsal parçaların işletim sistemi ile haberleşmesini sağlamaktadır. Servisler ise etkileşimsiz programlar olup uygulamaların ve işletim sisteminin kendi görevlerini yapmalarına yardımcı olmaktadır. Bazı zararlı yazılımlar ise kendisini doğrudan servis veya sistem sürücüsü olarak kurabilmektedir [7]. Böylece antivirüs programları tarafından tespit edilememekte ve bilgisayarın her açılışında tekrar aktif olmaktadır. Bilgisayarın açılışında çalışan uygulamalar; registry'de Run dizini altında yer almakta olup zararlı yazılımlarca popüler olarak kullanılan bu dizinin kontrol edilmesi önemlidir [15]. Zararlı yazılımlar registry üzerinde farklı izler de bırakmaktadır. Örneğin Windows İşletim Sisteminde dosya sistemlerine kullanıcı arabirimi ile erişmek için kullanılan "File Explorer", bir takım zararlı yazılımlarca devre dışı bırakılabilmektedir. Bu durumun tespiti için HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft\WindowsNT\CurrentVersion\ Winlogon dizini altında yer alan Shell girdi değerinin "explorer.exe" olduğunun kontrol edilmesi ve aksi durumda değerin tekrar explorer.exe olarak değiştirilmesi gerekmektedir.

Zararlı yazılımlarca bir başka registry değişikliği ise AppInit_DLLs listesine zararlı DLLs eklenmesidir. Windows ara yüzünden sorumlu user32.dll, DLL_PROCESS_ATTACH sırasında AppInit_DLLs listesine DLLs yüklemektedir. DLL Injection olarak adlandırılan yöntem ile zararlı DLLs, user32.dll ile güvenli olarak tanımlanmakta ve AppInit_DLLs listesine eklenmektedir [16]. Windows registry'de bulunan AppInit_DLLs değeri boş olmaktadır. Kullanıcılar tarafından bu dizinin kontrol edilerek boş olup olmadığının kontrol edilmesi; zararlı yazılım tespitine katkı sağlayacaktır [15].

Symantec tarafından 2008 yılında tespit edilen Infostealer.Scrapkut isimli zararlı yazılımın, Brezilya bankacılık ve finans web sitelerine yönelik bilgi topladığı ve saldırganlara gönderdiği tespit edilmiştir. Zararlı yazılımın "plugddownload.ifastnet.com" internet sitesinden partizan.exe isimli dosyayı indirdiği ve Windows Registry'de bulunan BootExecute değerinde kayıt oluşturduğu tespit edilmiştir [17]. Windows Registryde bulunan BootExecute, windows işletim sisteminin beklenmedik bir şekilde kapanması durumunda tekrar açılışta dosya sisteminin kontrol edilmesini sağlamakta olup varsayılan değeri; "autocheck autochk *" şeklindedir. Bu değerin kontrol edilmesi, zararlı yazılım analizine katkı sağlayacaktır.

Registry değişiklikleri tespitinde, orijinal windows registry listesini tutan açık kaynak kodlu Regshot yazılımı veya benzeri yazılımlar kullanılmaktadır. Bu sayede istenilen zaman, windows registry tekrar listelenerek ilk oluşturulan liste ile karşılaştırılabilmekte ve Regshot yazılımı ile bu iki tarama sonucu oluşturulan listeler karşılaştırılarak farklılıklar tespit edilebilmektedir [14]. Manuel olarak windows registry üzerinde yer alan girdilerin kontrol edilerek zararlı yazılım tespiti ile ilgili özet bilgiler tablo-2'de yer almaktadır.

Tablo 2. Windows Registry'de Zararlı Yazılım Tespiti (Detection Of Malicious Software In Windows Registry)

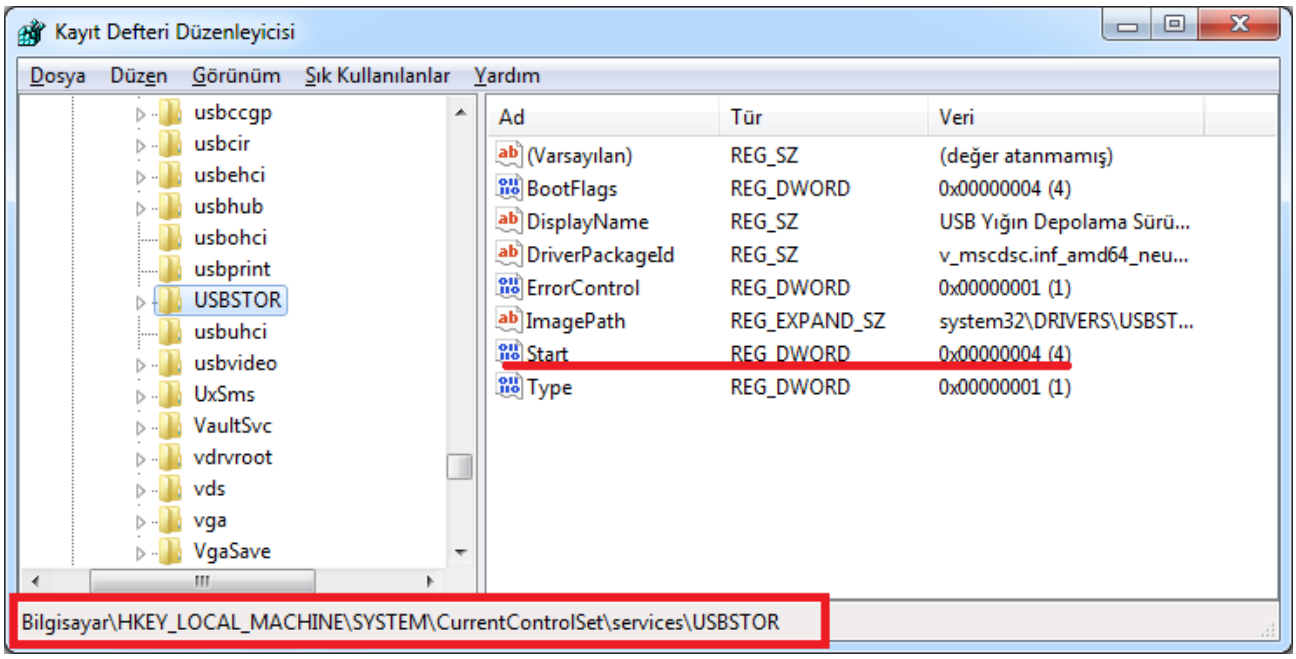
Kontrol Amacı	Kontrol Yeri	Kontrol İşlemi
Başlangıçta çalışan uygulamaların kontrol edilmesi	HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\Windows\CurrentVersion\Run	Run dizini altında çalışan uygulamalar kontrol edilmelidir
Girdi değerlerinde zararlı yazılımlar tarafından değişiklik yapılıp yapılmadığının kontrol edilmesi	HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\WindowsNT\CurrentVersion\Winlogon	**Shell** girdi değerinin **explorer.exe** olduğu kontrol edilmelidir
	HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\Windows NT\CurrentVersion\Windows	**AppInit_DLLs** girdi değerinin boş olduğu kontrol edilmelidir
	HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Control\Session Manager	**BootExecute** girdi değerinin **autocheck autochk *** olduğu kontrol edilmelidir

Bilgisayarda zararlı yazılım bulunup bulunmadığının Windows Registry aracılığı ile denetlenmesinin yanı sıra, zararlı yazılım dâhil hiçbir uygulamanın Windows Registry'e erişmesinin ve kayıtlar üzerinde değişiklik yapmasının engellenmesi de mümkündür. Bunun için Kayıt Defteri Düzenleyicisi açıldıktan sonra; HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE, HKEY_USERS ve HKEY_CURRENT_CONFIG isimli 5 ana yığının her biri üzerinde sağ tıklanarak izinlerin kısıtlanması yeterlidir. Bu işlemin Windows Registry'de okuma/yazma işlemi gerektiren tüm işlemleri engelleyeceği unutulmamalıdır.

3.2. Bilgisayarın Bazı Fonksiyonlarının Pasif Yapılması (Making Passive of Some Functions of Computer)

Özel hayatın gizliliği, haberleşme hürriyeti ve kişisel verilerin korunması Anayasa ve diğer ilgili kanunlarla koruma altına alınan önemli haklardandır. Bu bağlamda bilgisayar sahibinin bilgisi dışında yapılabilecek bazı işlemlerin engellenmesi; kişisel bilgisayar güvenliğinin sağlanması ve özel hayatın gizliliğine katkı sağlayacağı açıktır. Son kullanıcıların sıklıkla karşılaştığı istem dışı program kurulumu (zararlı yazılım, oyun, reklam gibi) veya aynı bilgisayarı kullanan başka kişilerce program kurulması engellenebilmektedir. Bunun için windows registry'de DisallowRun isimli yeni bir girdi oluşturulması, girdi değerinin 1 yapılması ve DisallowRun isimli anahtar oluşturularak çalışması istenilmeyen program isimlerinin uzantıları ile beraber girdi değeri olarak eklenmesi (black list oluşturulması) gerekmektedir. Registry'de yapılan bu işlemin aktif olabilmesi için işletim sisteminin tekrar başlatılmasına ihtiyaç duyulmaktadır.

USB diskler, kullanımı basit ve kolay taşınabilir harici bellekler olmasının yanı sıra zararlı yazılımların yayılmasında en çok suiistimal edilen araçlardan birisidir. Bilgisayar sahibinin bilgisi dışında USB bellek kullanımının engellenmesi ile bilgisayar güvenliğine katkı sağlanacağı açıktır [18]. Bilişim sistemlerinin fiziksel güvenliğin sağlanmasında USB bellek kullanımının sınırlandırılması veya tamamen engellenmesi önemlidir. Bunun için otomatik yazılımlar kullanılabileceği gibi HKEY_LOCAL_MACHINE\SYSTEM\CurrentControl Set\Services\UsbStor dizini altında bulunan Start girdisinin varsayılan değeri olan 3'ün 4 olarak değiştirilmesi ile de USB kullanımı pasif hale getirilebilmektedir [19]. Registry üzerinde USB bellek çalışmasının engellenmesi şekil-1'de yer almaktadır.



Şekil 1. USB Belleğin Çalışmasının Engellenmesi (Disabling Operation Of USB Memory)

Windows işletim sistemi tarafından CD-ROM, DVD veya USB belleklerin bilgisayara bağlanması ile AutoRun.inf dosyası aracılığı ile CD veya USB içerisinde bulunan uygulamaların otomatik olarak çalışması mümkündür. Otomatik başlatma (autoplay), kullanıcılar açısından ikinci bir işleme gerek kalmaksızın programların çalışmasını sağlayarak kolaylık sağlamaktadır [20]. Bununla beraber bilgisayar kullanıcılar CD içerisindeki uygulamanın istem dışı şekilde çalışmamasını isteyebilmektedir. Varsayılan olarak aktif olan bu özellik; Kayıt Defteri Düzenleyici içerisinde HKEY_LOCAL _MACHINE\SYSTEM\CurrentControlSet\Services\Cdrom dizini altında yer alan AutoRun girdisine ait değerin 0 olarak değiştirilmesi ile pasif hale getirilebilmektedir [19]. Benzer şekilde bilgisayara haricen takılan donanımların otomatik olarak kullanımına imkân tanıyan tak-çalıştır (Plug and Play) özelliğinin pasif edilmesi mümkündür. Bu işlem, aynı servis dizininde bulunan PlugPlay anahtarı altında yer alan Start girdisine ait varsayılan 2 değerinin 4 yapılması ile gerçekleştirilmektedir. Yapılan bu işlem ile bilgisayar sahibinin bilgisi olmaksızın cep telefonu veya harici kameraların bağlantı kablosu ile bilgisayara bağlanması engellenebilmektedir.

Windows 2000, XP, 2003 ve Vista işletim sistemlerinde varsayılan olarak gizli yönetici paylaşımı (administrative shares) alanı oluşturulmaktadır. Eğer kullanıcı tarafından ilave paylaşım alanı oluşturulursa, HKEY_LOCAL _MACHINE \ SYSTEM \ CurrentControl Set \ Services\ lanmanserver\ Shares dizini altında kayıt oluşmaktadır. Bilgisayar yöneticisi tarafından bu dizin altında yer alan AutoShareServe girdi değerinin 0 yapılması ile gizli yönetici paylaşımı yapılması engellenmektedir [7]. Windows 7, Windows 8 ve Windows 10 İşletim Sistemlerinde ise HKEY_LOCAL_MACHINE\SYSTEM \CurrentControl Set\services\LanmanServer\Parameters dizini altına AutoShareWks isimli yeni bir girdi değeri oluşturularak girdi değerinin 0 yapılması gerekmektedir.

Bilgisayar üzerinde birçok değişikliğin yapıldığı yer Denetim Masası'dır. Bilgisayar sahibinin bilgisi olmaksızın bu alanda yapılacak değişiklikler ile yeni programlar kurulabileceği gibi bazı programlar kaldırılabilmekte, ağ bağlantıları veya güvenlik duvarı ayarları değiştirilebilmektedir. Bu açıdan HKEY_ LOCAL_MACHINE \ SOFTWARE\Microsoft\Windows\ CurrentVersion\Policies\Explorer dizini altına NoControlPanel isimli yeni bir girdi oluşturularak değerinin 1 yapılması ile kullanıcıların denetim masasına erişim engellenebilmektedir.

Program ekle / kaldır menüsünün pasif edilmesi için ise; aynı dizinin altında yer alan uninstall anahtarına NoChooseProgramsPage isimli yeni bir girdi oluşturulması ve değerinin 1 yapılması gerekmektedir.

Denetim masasında bulunan menülerin pasif edilmesi için bir diğer yöntem ise HKEY_LOCAL_MACHINE\ SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ControlPanel\NameSpace dizini altında yer alan ve windows 7, windows 8 ve windows 10 işletim sistemleri için aynı değere sahip anahtar isimlerinin değiştirilmesi/silinmesi şeklindedir. Bu dizin altında yer alan {D20EA4E1-3957-11d2-A40B-0C5020524153} anahtar değeri "yönetimsel araçlar" menüsünü, {4026492F-2F69-46B8-B9BF- 5654FC07E423} anahtar değeri "Windows Firewall" menüsünü, {7B81BE6A-CE2B-4676-A29E-EB907A5126C5} anahtar değeri "programlar ve özellikler" menüsünü, {8E908FC9-BECC-40F6-915B-F4CA0E70D03D} anahtar değeri ise "Ağ ve Paylaşım Merkezi" menüsünü ifade etmektedir.

Microsoft office word, excel, powerpoint dosyası açılışı başlangıç ekranında daha önce açılan/işlem yapılan doküman isimleri ve bulundukları dizinler yer almaktadır. Kullanıcılara kolaylık sağlaması beklenen bu özellik, bazı kullanıcılar tarafından eleştirilmektedir.

Özellikle ortak olarak kullanılan bilgisayarlarda kullanıcılar, daha önce işlem yaptığı dosya isimlerinin diğer kullanıcılar tarafından bilinmesini istemeyebilmektedir. Özel hayatın gizliliği kapsamında değerlendirilebilecek bu istek Registry üzerinde yapılacak değişiklik ile gerçekleştirilebilmektedir. Bunun için Kayıt Defteri Düzenleyicisi içerisinde HKEY_CURRENT_ USER\SOFTWARE\Microsoft\Office\15.0\Common\ General dizini altına DisableBootToOfficeStart isimli girdinin varsayılan 0 değerinin 1 yapılması yeterlidir.

Ayrıca HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft\ Windows\ CurrentVersion\ Policies\ Explorer dizini altında NoRecentDocsHistory isimli yeni bir girdi oluşturularak değerinin 1 yapılması ile bu konuda endişe giderilmiş olacaktır.

Benzer şekilde, HKEY_CURRENT_USER\SOFTWARE \Microsoft\Office\15.0 \Common\General dizini altında bulunan NoTrack isimli girdinin varsayılan 0 değerinin 1 olarak değiştirilmesi ile Microsoft Office dokümanları üzerinde yapılan çalışma süreleri gizlenebilmektedir.

Bilgisayar üzerinde bulunan herhangi bir doküman üzerinde değiştirme işlemi yapılmadan sadece erişim sağlanması (okuma) durumunda doküman erişim tarihi güncellenmektedir. Bu özelliğin pasif yapılmasının istenilmesi durumunda ise NtfsDisableLastAccessUpdate isimli girdinin varsayılan 0 değerinin 1 olarak değiştirilmesi yeterlidir. Windows Registry üzerinde yapılabilecek bu değişikler ile özellikle ortak olarak kullanılan bilgisayarlarda kullanıcı mahremiyeti sağlanmış olacaktır.

Tablo 3. Bilgisayarda Gerçekleştirilebilecek Bazı İşlemlerin Windows Registry ile Engellenmesi (Inhibiting Some Processes That Could Be Run In Computers With Windows Registry)

İşlem Amacı	İşlem Yeri	İşlem Özeti	Yapılan İşlem	Bilgisayarın Tekrar Başlatılması İhtiyacı
Istenilmeyen uygulamaların çalışmasının engellenmesi	HKEY_CURRENT_USER\SOFTWARE\ Microsoft\Windows\CurrentVersion\Policies\Explorer	**DisallowRun** isimli yeni girdi oluşturulması ve değerinin 1 yapılması. Ayrıca DisallowRun anahtarı oluşturularak engellenecek uygulama isimlerinin girdi değeri olarak eklenmesi		Evet
Kullanıcıların bilgisayarı kapatmasının engellenmesi	HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft\Windows\CurrentVersion\Policies\Explorer	**NoClose** isimli yeni girdi oluşturulması ve değerinin 1 yapılması		Evet
Bilgisayarım altında bulunan C,D,E gibi sürücülerin gizlenmesi	HKEY_CURRENT_USER\ SOFTWARE\ Microsoft\Windows\CurrentVersion\Policies\Explorer	**NoDrives** isimli yeni girdi oluşturulması. Girdi değerine sürücü harfinin decimal olarak yazılması (ör: C için 4, D için 8, tümü için 67108863)		Evet
Bilgisayara yeni yazıcı eklenmesinin engellenmesi	HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\Windows\CurrentVersion\Policies\Explorer	**NoAddPrinter** isimli yeni girdi oluşturulması ve değerinin 1 yapılması		Evet
Denetim masasına erişimin engellenmesi	HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\Windows\CurrentVersion\Policies\Explorer	**NoControlPanel** isimli yeni girdi oluşturulması ve değerinin 1 yapılması		Hayır
Fare (mouse) ile sağ tıklama özelliğinin pasif edilmesi	HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\Windows\CurrentVersion\Policies\Explorer	**NoViewContextMenu** isimli yeni girdi oluşturulması ve değerinin 1 yapılması		Evet
Erişilen MS Office isimlerinin gösteriminin engellenmesi	HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\Windows\CurrentVersion\Policies\Explorer	**NoRecentDocsHistory** isimli yeni girdi oluşturulması ve değerinin 1 yapılması		Hayır
USB belleklerin çalışmasının engellenmesi	HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Services\UsbStor\	**Start** isimli girdinin varsayılan 3 değerinin 4 olarak değiştirilmesi		Evet
Tak-çalıştır özelliğinin pasif edilmesi	HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Services\PlugPlay	**Start** isimli girdinin varsayılan 2 değerinin 4 olarak değiştirilmesi		Evet
Application loglarının tutulma süresinin değiştirilmesi	HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Services\eventlog\Application	**MaxSize** isimli girdinin varsayılan 140000 değerinin değiştirilmesi		Evet
Security loglarının tutulma süresinin değiştirilmesi	HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Services\eventlog\Security	**MaxSize** isimli girdinin varsayılan 140000 değerinin değiştirilmesi		Evet
System loglarının tutulma süresinin değiştirilmesi	HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Services\eventlog\System	**MaxSize** isimli girdinin varsayılan 140000 değerinin değiştirilmesi		Evet
Denetim masasında bulunan Program Ekle/Kaldır menüsünün gizlenmesi	HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft\Windows\CurrentVersion\Policies\Uninstall	**NoChooseProgramsPage** isimli yeni girdi oluşturulması ve değerinin 1 yapılması		Evet
Denetim masasında bulunan Yönetimsel Araçlar menüsünün gizlenmesi	HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\Windows\CurrentVersion\Explorer\ ControlPanel\NameSpace	{D20EA4E1-3957-11d2-A40B-0C5020524153} anahtar değerinin silinmesi/değiştirilmesi		Hayır
Denetim masasında bulunan Windows Firewall menüsünün gizlenmesi	HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\Windows\CurrentVersion\Explorer\ ControlPanel\NameSpace	{4026492F-2F69-46B8-B9BF-5654FC07E423} anahtar değerinin silinmesi/değiştirilmesi		Hayır
Denetim masasında bulunan Program Ekle/Kaldır menüsünün gizlenmesi	HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\Windows\CurrentVersion\Explorer\ ControlPanel\NameSpace	{7B81BE6A-CE2B-4676-A29E-EB907A5126C5} anahtar değerinin silinmesi/değiştirilmesi		Hayır
Denetim masasında bulunan Ağ ve Paylaşım menüsünün gizlenmesi	HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\Windows\CurrentVersion\Explorer\ ControlPanel\NameSpace	{8E908FC9-BECC-40F6-915B-F4CA0E70D03D} anahtar değerinin silinmesi/değiştirilmesi		Hayır
CD içerisindeki uygulamanın otomatik olarak çalışmasının engellenmesi	HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Services\Cdrom	**AutoRun** isimli girdinin varsayılan 1 değerinin 0 olarak değiştirilmesi		Evet
Gizli yönetici paylaşımı alanı (administrative shares) oluşturulmasının engellenmesi	HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\services\LanmanServer\Parameters	**AutoShareWks** isimli yeni girdi oluşturulması ve değerinin 0 yapılması		Evet
Bilgisayar üzerinde paylaşıma açılan klasörlere yapılan erişimlere ait bilgilere ulaşılabilmesi	HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Services\SharedAccess\ Parameters\FirewallPolicy\StandardProfile	**EnableFirewall** isimli girdinin varsayılan 0 değerinin 1 olarak değiştirilmesi		Evet
Bilgisayar kapatılmadan önce "pagefile.sys dosyasının" temizlenmesi	HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Control\Session Manager\Memory Management	**ClearPageFileAtShutdown** isimli girdinin varsayılan 0 değerinin 1 olarak değiştirilmesi		Evet
Daha önce oluşturulan MS Office belgelerinin yer aldığı MS Office başlangıç ekranının gösterilmemesi	HKEY_CURRENT_USER\SOFTWARE\ Microsoft\Office\15.0\Common\General	**DisableBootToOfficeStart** isimli girdinin varsayılan 0 değerinin 1 olarak değiştirilmesi		Hayır
Erişim sağlanan dosyalara ait "Erişim Tarihi" bilgisinin güncellenmesinin engellenmesi	HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Control\FileSystem	**NtfsDisableLastAccessUpdate** isimli girdinin varsayılan 0 değerinin 1 olarak değiştirilmesi		Evet
Oluşturulan MS Office belgelerine ait çalışma süresinin gizlenmesi	HKEY_CURRENT_USER\ SOFTWARE\ Microsoft\Office\15.0\Common\General	**NoTrack** isimli girdinin varsayılan 0 değerinin 1 olarak değiştirilmesi		Evet

Bilgisayarlarda veri yazma-okuma işlemi yapılırken, harddisklere göre çok daha hızlı işlem yapabilen RAM (Random Access Memory) teknolojisi kullanılmaktadır. Geçici bellek olarak kullanılan RAM kapasitesinin yetersiz olması durumunda ise bilgisayar üzerinden sanal bellek oluşturulmaktadır. Windows işletim sisteminde pagefile.sys olarak adlandırılan bu dosya içerisinde; parola bilgileri, anlık mesajlaşma (IM) uygulama kalıntıları ve diğer işlemlere ait izler bulunmakta ve bilgisayarın kapatılması ile kaybolmamaktadır. Bilgisayar kapatılmadan önce "pagefile.sys dosyasının" temizlenmesi, bu verilere ulaşılmasını zorlaştırmaktadır [7]. Kayıt Defteri Düzenleyici (registry editör) içerisinde HKEY_LOCAL_MACHINE \ SYSTEM\CurrentControl Set\Control\SessionManager\Memory Management dizini altında yer alan ClearPageFileAtShutdown değerinin 1 olarak değiştirilmesi ile her bilgisayar kapanması öncesi "pagefile.sys dosyası" temizlenecektir (sıfırlanacaktır). Bilgisayar tarafından kullanıcıların gerçekleştirdikleri işlemlerin otomatik olarak kaydedildiği log dosyalarının boyutunun değiştirilmesi ile bu kayıtları saklama süreleri artacak veya azalacaktır. Bunun için HKEY_ LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services\eventlog\ dizini altında yer alan Application, Security ve System anahtarlarına ait MaxSize isimli girdi değerinin varsayılan 140000 byte değerinin değiştirilmesi gereklidir.

HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft\ Windows\CurrentVersion\ Policies\Explorer dizini altında NoDrives isimli yeni bir girdi oluşturularak Bilgisayarım altında bulunan C,D,E gibi sürücülerin (partitionların) gizlenmesi mümkündür. Bunun için girdi değeri olarak C için 4, D için 8, tümü için 67108863 gibi sürücü harfinin decimal karşılığının yazılması gerekmektedir.

Kullanıcılar tarafından bilgisayardaki kendi oturumlarını kapatabilmesi ancak bilgisayarı tamamen kapatamamaları için NoClose isimli yeni bir girdi oluşturulması ve değerinin 1 yapılması gereklidir.

Bilgisayar yöneticisinin bilgisi dışında yeni bir yazıcının eklenmemesi için ise NoAddPrinter isimli yeni bir girdi oluşturulması ve değerinin 1 yapılması yeterlidir.

Kullanıcıların bilgisayarda fare'nin (mouse) sağ tıklama özelliğini kullanmamaları da aynı dizin altına NoViewContextMenu isimli yeni bir girdi oluşturulması ve değerinin 1 yapılması ile mümkündür.

Bilgisayar üzerinde gerçekleştirilen birçok işlemin Windows Registry üzerinde yapılacak değişiklikler ile engellenmesi mümkündür.

Yapılan değişikliklerin bir kısmı hemen aktif olurken bir kısmı bilgisayarın tekrar başlatılması ile aktif olabilmektedir. Bu konuda incelenen 24 işleme ait registry değişiklikleri ve özet bilgiler tablo-3'de yer almaktadır.

3.3. Gerçekleşen İşlemlerin Denetlenmesi (Auditing of Process in Computers)

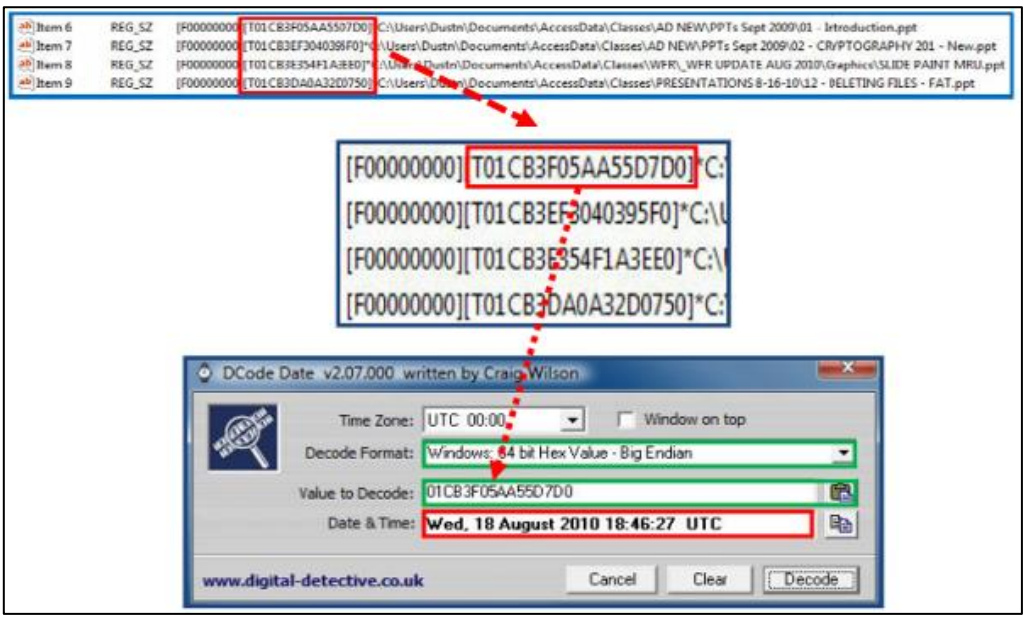
Birçok kullanıcı, üçüncü kişilerce bilgisayarına fiziksel veya uzaktan erişim sağlanarak kullanılmasından şüphelenmekte ve buna karşı; parola ile oturum açma, misafir oturumlarının iptal edilmesi, anti virüs programları kullanma gibi çeşitli önlemler almaktadır. Alınan güvenlik tedbirlerine ek olarak, bilgisayar üzerinde yapılan iş ve işlemlerin kaydedildiği Windows Registry üzerinde oluşan kayıtların kontrol edilerek gerçekleşen işlemlerin istem dışı olup olmadığı anlaşılabilmektedir.

Microsoft Windows ailesi işletim sistemlerinde bir ofis dokümanı açıldığında; kayıt defterinde (Registry) işletim sistemi tarafından oluşturulan kayıtlar ve dokümanı açan programlar tarafından oluşturulan kayıtlar olmak üzere 2 tür iz oluşmaktadır. Dokümanı açan program tarafından, LNK uzantılı dosyalar, dokümanı açan programın PF uzantılı "prefetch" dosyaları ve dosya üst veri bilgileri (erişim tarihi, değiştirme tarihi) otomatik olarak oluşan izlerdir [12]. Microsoft Office 2007 ile birlikte bilgisayarda işlem gören son 50 dokümana ait dokümanın adı, açılma tarihi, zaman damgası bilgisi, son kaydeden bilgisi ve kayıt yeri bilgileri şeklinde MRU (Most Recently Used) bilgileri Windows Registry'de otomatik olarak oluşmaktadır. MRU kayıtlarına ait Registry dizinleri Microsoft Office versiyonlarına göre değişmekte olup buna ilişkin bilgiler özet olarak tablo-4'de yer almaktadır.

Tablo 4. Microsoft Office MRU Kayıt Yerleri (Microsoft Office MRU Registry Locations)

Microsoft Office Adı	Versiyon Adı	Office Dokümanlarına Ait Bilgilerin Registry Kayıt Yeri
Microsoft Office 2007	12.0	HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Access\File MRU HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\PowerPoint\File MRU HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Publisher\File MRU
Microsoft Office 2010	14.0	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\File MRU HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Access\File MRU HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\PowerPoint\File MRU HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Publisher\File MRU
Microsoft Office 2013	15.0	HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Reading Locations HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Reading Locations HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Access\Reading Locations HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\PowerPoint\Reading Locations HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Publisher\Reading Locations

MRU kayıtlarında, doküman adı ve bulunduğu yer açık bir şekilde yer almakta iken Microsoft Word ve Excel için son erişim zamanı, Microsoft PowerPoint için ise son erişim veya son kaydetme zamanı "hexadecimal little endian" formatında tutulmaktadır. Bu bilgi adli bilişim yazılımları, 3.parti yazılımlar veya online internet siteleri aracılığı ile kullanılan zaman bilgisine çevrilebilmektedir. Şekil-2'de ise Craig Wilson tarafından geliştirilen DCode converter yazılımı ile örnek bir zaman çevrimi gösterilmektedir [21].



Şekil 2. Örnek Zaman Bilgisi Çevrimi (Sample Decoding of Information On Time and Date)(Hurlbut, 2010:8)

MRU kayıtları sadece Microsoft Office ürünleri için değil, bilgisayarda yer alan birçok doküman türü için tutulmaktadır. Bilgisayar kullanıcısının yakın zaman önce açtığı dosyalar, çalıştırdığı programlar gibi yapmış olduğu işlemler hakkında bir çok MRU kaydı Registry'de bulunmaktadır[12]. Kayıt Defteri Düzenleyicisinde HKEY_CURRENT_USER\ SOFTWARE\ Microsoft\ Windows\CurrentVersion\ Explorer\ RecentDocs dizini altında; bilgisayarda açılan dosyalar. doc, .txt, .html şeklinde uzantılarına göre klasörler halinde ve işlem yapılan klasörler ise Folder isimli klasör altında yer almaktadır. Kayıtlar, rakam olarak sıralanmakta olup erişim sağlanan dosya isimleri ise binary olarak tutulmaktadır [7].

Kayıt Defteri Düzenleyici içerisinde HKEY_CURRENT_ USER\SOFTWARE\Microsoft\Windows\CurrentVersion\ Explorer\ ComDlg32\ OpenSaveMRU dizini altında Windows Explorer diyalog kutusu aracılığı ile açılan veya kaydedilen her bir uzantıdaki son 10 dokümana ait bilgiler yer almaktadır. HKEY_CURRENT_USER\SOFTWARE\ Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\ LastVisitedMRU dizini altında ise daha önceki OpenSaveMRU anahtarına ait ilave bilgiler yer almaktadır. Bu ilave bilgiler, önceki kaydı oluşturan uygulamaya ait bilgiler ve dokümanın kaydedildiği yer bilgisidir [22]. Windows 7 işletim sistemi ile beraber bu kayıtlar LastVisitedPidlMRU anahtarı altında yer almaktadır.

Kayıt Defteri Düzenleyicisinde HKEY_CURRENT_ USER\SOFTWARE\Microsoft\Windows\CurrentVersion\ Explorer\MountPoints2 dizini altında kullanıcıların ağ üzerinde erişim sağladığı paylaşımlar yer almaktadır. RemotePath değeri bilgisayar kullanıcısının bağladığı ve sürücü harfi aldığı paylaşımları göstermektedir [23]. Kullanıcı tarafından paylaşıma açılan klasör listesi ise HKEY_LOCAL_MACHINE\ SYSTEM\ CurrentControl Set\services\LanmanServer\Shares dizini altında; klasör adı, paylaşım yeri ve paylaşım izin bilgileri ile birlikte yer almaktadır.

Kullanıcılar tarafından Internet Explorer (IE) veya Windows Explorer adres çubuğu aracılığı ile en son erişim sağlanan son 25 URL veya dosya yolu bilgisi; HKEY_CURRENT_USER\SOFTWARE\Microsoft\Inter net Explorer\TypedURLs dizini altında yer alan kayıtlardan anlaşılmaktadır. Bu kayıtlar, kullanıcının bilinçli şekilde tam adresini yazarak erişim sağladığı internet adresleri, otomatik tamamlanan adresler ve bağlantıların (link) tıklanması ile ulaşılan adreslerden oluşmaktadır. Bu kayıtlar içerisinde IE Favori adresler aracılığı ile yapılan erişimler ise yer almamaktadır [22].

Bilgisayar yöneticisinin bilgisi dışında bilgisayara çeşitli programlar kurulması mümkündür. Windows Registry'de yer alan kayıtların incelenmesi ile bu yönde bir işlemin tespiti yapılabilmektedir. HKEY_LOCAL_MACHINE\ SOFTWARE dizini altında bilgisayara kurulan tüm programlar, HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft dizini altında ise bilgisayara kurulan Microsoft programlarına ait kayıtlar yer almaktadır. Örneğin, Yahoo! Messenger uygulaması; HKEY_CURRENT _USER\SOFTWARE\Yahoo dizini, MSN Messenger uygulaması; HKEY_CURRENT_USER\ SOFTWARE\ Microsoft \ MSNMessenger ve HKEY_LOCAL_ MACHINE\ SOFTWARE\ Microsoft \MessengerService dizinleri, ICQ uygulaması; HKEY_LOCAL_MACHINE \SOFTWARE\Mirabilis\ICQ dizini ve AIM(AOL Instant Messenger) uygulaması; HKEY_CURRENT_USER\ SOFTWARE\America Online\AIM6 dizini altında iz ve kalıntılar bırakmakta (Farmer, 2007:10) olup bu yerlerin kontrol edilmesi ile istem dışı anlık mesajlaşma (IM) uygulaması kurulup kurulmadığı anlaşılabilmektedir.

Benzer şekilde Facebook Chat Instant Messenger uygulaması için; HKEY_LOCAL_MACHINE\ SOFTWARE\Facebook Messenger dizini ; Skype uygulaması için; HKEY_CURRENT_USER\ SOFTWARE \Skype \Phone\ ve HKEY_CURRENT_ USER\SOFTWARE\Skype\Toolbar dizinleri ve Google+ Hangouts uygulaması için; HKEY_CURRENT_USER\ SOFTWARE\ Google\ Google Talk dizinleri kontrol edilmelidir.

Windows işletim sistemi kurulu bilgisayara USB belleklerin takılması durumunda Registry üzerinde iz ve kalıntılar bırakmaktadır. USB bellek bilgisayara takıldığı zaman Plug and Play (PnP) Manager tarafından belleğe ait üretici firma gibi tanımlayıcı bilgiler elde edilerek uygun bir sürücü harfi tahsis edilir ve gerekli ise USB bellek driver yazılımı yüklenir. USB bellek tanımlandıktan sonra HKEY_LOCAL_MACHINE\ SYSTEM\ CurrentControlSet \Enum\ USBSTOR dizini altında kayıtlar oluşturulur. USB belleğin bilgisayara son takılma zamanı ise; HKEY_LOCAL_MACHINE\ SYSTEM\ CurrentControlSet \Control \DeviceClasses dizini altındaki kayıtlarda tutulur [7]. Bir bilgisayara hangi USB belleklerin takıldığı veya suç unsuru içerdiği tahmin edilen USB belleğin hangi bilgisayarda kullanıldığı bu kayıtlar ile anlaşılabilir. Bu kayıtları incelemek için USBDeview isimli ücretsiz yazılım kullanılabilir [24].

Yukarıda detaylı olarak anlatıldığı üzere windows registry, bilgisayar üzerinde yapılan iş ve işlemlere ait detaylı bilgilerin kaydedildiği bir ortamdır. Bu kayıtların tutulması, işletim sisteminin düzenli ve performanslı çalışmasını sağlamasının yanı sıra kullanıcıların gerçekleştirdiği iş ve işlemlerin bilgisayar yöneticisi tarafından denetlenmesine de imkân tanımaktadır. Bu kayıtların incelenmesi çeşitli programlar aracılığı ile otomatik olarak gerçekleştirilebileceği gibi manuel kontroller ile de yapılabilmektedir. Bu konuda incelenen 12 işleme ait registry kontrol yeri ve kontrol amacı özet şekilde tablo-5'de yer almaktadır.

Tablo 5. Bilgisayarda Gerçekleştirilebilecek Bazı İşlemlerin Windows Registry ile Denetlenmesi (Auditing Some Processes That Could Be Run In Computers With Windows Registry)

Kontrol Amacı	Kontrol Yeri
Başlangıçta çalışan uygulamaların kontrol edilmesi	HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\Windows\CurrentVersion\Run
Kurulan programların listelenmesi	HKEY_LOCAL_MACHINE\SOFTWARE
Kurulan Microsoft programlarının listelenmesi	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft
Bilgisayarda açılan/erişilen dokümanların listelenmesi	HKEY_CURRENT_USER\SOFTWARE\ Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
Internet Explorer tarayıcısı ile ziyaret edilen internet sitelerinin listelenmesi	HKEY_CURRENT_USER\SOFTWARE\ Microsoft\Internet Explorer\TypedURLs
Bilgisayarda son erişilen dokümanlara ait bilgilerin listelenmesi	HKEY_CURRENT_USER\SOFTWARE\ Microsoft\Windows\CurrentVersion\Explorer\ ComDlg32\LastVisitedPidlMRU
Bilgisayarda bulunan dosya uzantılarının listelenmesi	HKEY_CURRENT_USER\SOFTWARE\ Microsoft\Windows\CurrentVersion\Explorer\FileExts
Bilgisayara takılan USB belleklere ait kayıtların listelenmesi	HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Enum\USBSTOR
Bilgisayara takılan USB belleklerin son takılma zamanlarının öğrenilmesi	HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Control\DeviceClasses
Kullanıcıların ağ üzerinde erişim sağladığı paylaşım adreslerinin listelenmesi	HKEY_CURRENT_USER\SOFTWARE\ Microsoft\ Windows\CurrentVersion\Explorer\MountPoints2
Kullanıcılar tarafından paylaşıma açılan klasörlerin listelenmesi	HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\services\LanmanServer\Shares
Bilgisayarda sanal makine bulunup bulunmadığının öğrenilmesi	HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Enum\PCI

4. DEĞERLENDİRME VE SONUÇ (EVALUATION AND CONCLUSION)

Gelişen teknoloji ile beraber hayatın her alanında kullanılan bilişim sistemleri sağladığı olumlu katkıların yanı sıra, bilgisayar güvenliği açısından tehditler oluşturmaktadır. Siber suç, siber savaş, siber güç, siber güvenlik, siber savunma vb. terimlerin kullanıldığı günümüzde; en yaygın kullanılan bilişim ürünü olan ”bilgisayarların” güvenliği önemli bir konu olarak karşımıza çıkmaktadır.

Bilgisayar güvenliğinin sağlanması; donanım güvenliğinden başlayarak, ağ protokolleri güvenliği, yazılım güvenliği, kod güvenliği gibi çok sayıda bileşenden oluşmaktadır. Bununla beraber en güvenli sistemde dahi insan faktörü bulunduğu için kullanıcı farkındalığı da bir diğer önemli bilgisayar güvenliği bileşenidir. Windows işletim sisteminin veri tabanı konumunda olan ve sistemin düzenli şekilde çalışması amacıyla kayıtların tutulduğu windows registry, bilgisayar güvenliğinin sağlanmasında önemli bir öğedir.

Bu çalışmada, windows işletim sistemlerinde bulunan windows registry’nin bilgisayar güvenliğinin sağlanmasındaki rolü el alınmış, zararlı yazılım analizinde ve alınacak güvenlik önlemlerinde; windows registry üzerinde inceleme yapılması gereken yerler ve değiştirilmesi fayda sağlayacak girdiler (ayarlar) hakkında bilgi verilmiştir. Çalışmada zararlı yazılımların tespit edilmesi açısından 4; bilgisayarda bulunan bazı fonksiyonların engellenmesi açısından 24 ve bilgisayarda gerçekleşen işlemlerin denetlemesi açısından 27 olmak üzere toplam 55 işleme ait windows registry girdisi incelenmiş ve değerlendirmelerde bulunulmuştur.

Çalışma sonucu, windows registry üzerinde yapılacak işlemler ile bilgisayara istem dışı olarak fiziksel veya uzaktan erişimin engellenmesi, yapılan erişimlerin tespit edilmesi ve oluşacak zararın en aza indirilmesinin mümkün olduğu anlaşılmıştır. Windows Registry üzerinde yapılacak işlemler ile aşağıda sayılan önlemlerin alınabileceği ve bilgisayar güvenliğine katkı sağlayabileceği değerlendirilmektedir.

-Bilgisayar açılışında otomatik çalışan uygulamaların kontrol edilebilmektedir.

-DLL Injection saldırılarının tespit edilebilmektedir.

-Çalışması istenmeye uygulamalar için black-list oluşturulabilmektedir.

-Taşınabilir USB belleklerin kullanımı engellenebilmektedir.

-CD içerisindeki uygulamanın otomatik çalışması engellenebilmektedir.

-Varsayılan olarak açık olan gizli yönetici paylaşımı özelliği pasif edilebilmektedir.

-Denetim Masası’na erişim engellenebilmektedir.

-Denetim Masası altında yer alan Yönetimsel Araçlar, Windows Firewall, Programlar ve Özellikler, Ağ ve Paylaşım Merkezi gibi menülerin pasif edilerek erişilmesi ve ayarlarda değişiklik yapılması engellenebilmektedir.

-Bilgisayarda işlem gören microsoft office doküman isimlerinin kullanıcılar tarafından görülmesi engellenebilmektedir.

-Bilgisayarda işlem gören microsoft office dokümanlarının çalışma süresi ve son erişim tarihlerinin kullanıcılar tarafından görülmesi engellenebilmektedir.

-Bilgisayarın her kapanışında Pagefile.sys dosyası temizlenebilmekte ve buradan veri elde edilmesi engellenebilmektedir.

-Bilgisayarım altında bulunan C, D, E gibi sürücüler gizlenebilmektedir.

-Kullanıcılar tarafından bilgisayarın kapatılması ve printer eklenmesi engellenebilmektedir.

-Yakın geçmiş zamanda işlem yapılan (oluşturulan, değiştirilen) dosyalar tespit edilebilmekte ve denetlenebilmektedir.

-Microsoft office dokümanlarına ait işlem gören son 50 doküman tespit edilebilmektedir.

-Windows explorer diyalog kutusu aracılığı ile açılan veya kaydedilen son 10 doküman bilgisi tespit edilebilmektedir.

-Internet explorer veya windows explorer adres çubuğu aracılığı ile son erişim sağlanan 25 URL adresi tespit edilebilmektedir.

-Kullanıcı tarafından ağ üzerinde paylaşıma açtığı klasörlere yapılan erişimler tespit edilebilmektedir.

-Anlık mesajlaşma uygulamalarına ait kayıtlar tespit edilebilmekte ve bilgisayarda kurulu bulunan uygulamalar denetlenebilmektedir.

Bilgisayar güvenliğinin sağlanması açısından Windows Registry’de yapılan işlemler ile bilgisayarın bazı fonksiyonlarının pasif yapılmasının Anayasamızca güvence altına alınmış olan özel hayatın gizliliği, haberleşme hürriyeti ve kişisel verilerin korunması haklarına pozitif katkı sağladığı değerlendirilmektedir. Diğer taraftan özellikle son dönemde kamuoyunda büyük yankı uyandıran yargılamalarda; suç unsuru elektronik belgelerin bilgisayarlara virüs yolu ile veya uzaktan erişim sağlanmak sureti ile yüklendiği iddialarının açıklığa kavuşturulmasında windows registry’de yer alan kayıtların incelenmesinin fayda sağladığı anlaşılmıştır. Benzer şekilde zararlı yazılım dâhil hiçbir uygulamanın windows registry’de okuma/yazma işlemi gerçekleştirmesi, dolayısıyla

bilgisayarda çalışmasının engellenmesinin mümkün olduğu görülmüştür.

KAYNAKLAR (REFERENCES)

[1] N. ,Yalçın, "*Türkiye'de Bilişim Suçları ve Bilgi Güvenliği"*, II. Uluslararası Bilgisayar ve Öğretim Teknolojileri Eğitimi Sempozyumu, (ICITS'08), Ege Üniversitesi Eğitim Fakültesi, Kuşadası, Aydın, 16 - 18 Nisan 2008.

[2] F. ,Kramer, S. Starr, L. Wentz**,** *Cyberpower and National Security*, National Defense University Press, ABD, 2009.

[3] N. ,Yalçın, *İşletim Sistemleri Ders Notları*, Gazi Üniversitesi Bilgisayar ve Öğretim Teknolojisi Eğitimi Bölümü, Ankara, 2015.

[4] D., Comer, *Operating System Design: The Xinu Approach*, CRC Press, ABD, 2015.

[5] D. J. ,Farmer, A Forensic Analysis Of The Windows Registry, www.forensicfocus.com/a-forensic-analysis-of-the-windows-registry, 02.08.2015.

[6] İnternet: Microsoft, What is The Registry? http://windows.microsoft.com/en-us/windows-vista/what-is-the-registry, 02.08.2015.

[7] D., Garza, *Investigating Hard Disks, File and Operating Systems*, EC-Council Press, ABD, 2010.

[8] G., TingTing, *Challenges in Windows 8 Operating System For Digital Forensic Investigations*, Yüksek Lisans Tezi, Auckland Teknoloji Üniversitesi, Forensic Information Technology Bölümü, Yeni Zelanda, 2014.

[9] İnternet: Microsoft, HKEY_LOCAL_MACHINE, https://technet.microsoft.com/en-us/library/cc959046.aspx, 02.08.2015.

[10] M., Halsey, A., Bettany, *Windows Registry Troubleshooting*, Apress, ABD, 2015.

[11] H. ,Çakır, M. S., Kılıç, *"Bilişim Suçlarına İlişkin Elektronik Delil Elde Etme Yöntemlerine Genel Bir Bakış*", Polis Bilimleri Dergisi, 15 (3), ss: 23-44, 2013.

[12] E., Çalışkan, *Zararlı Yazılımların Etkisinde Dijital Adli Delillerin Güvenilirliği*, Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul, 2013.

[13] N., Yalçın, "Siber Suçlarda Yeni Trendler", Güncel Tehdit:Siber "Suçlar, (Ed. H. Çakır, M. S. Kılıç), Ankara: Seçkin Yayınevi, ss. 285-325, 2014.

[14] A., Pektaş, *Behavior Based Malicious Software Detection and Classification*, TUBİTAK Uzmanlık Tezi, İstanbul, 2012.

[15] P., Nemcek, *Analysis of Malware Classification Schemas*, Yüksek Lisans Tezi, Masaryk Üniversitesi, İnformatike Fakültesi, Çek Cumhuriyeti, 2013.

[16] A. Alasiri, M. ,Alzaidi, D., Lindskog, P., Zavarsky, R., Ruhl, S., Alassmi, "Comparative Analysis of Operational Malware Dynamic Link Library (DLL) Injection Live Response vs. Memory Image", International Conference on Computing, Communication System and Informatics Management, 29 – 30 Temmuz 2012, Dubai, BAE.

[17] İnternet: Symantec Raporu, Infostealer.Scrapkut www.symantec.com/security_response/ writeup. sp?docid=2008-030415-3841-99, 16.08.2015.

[18] Z,. Chunyang, W., Weiping, "USB Storage Device Protection Software", Journal of Advanced Materials Research, Sayı: 722, ss. 244-249, 2013.

[19] M., Zarouni, "The Reality of Risks From Consented Use of USB Devices", 4. Australian Information Security Management Conference, 05.12.2006, Avustralya.

[20] R., Tahir, Z., Hamid, H., Tahir, "Analysis of AutoPlay Feature via the USB Flash Drives", World Congress on Engineering, 02-04 Temmuz 2008, Londra, İngiltere.

[21] D. ,Hurlbut, Microsoft Office 2007, 2010 – Registry Artifacts, https://ad-pdf.s3.amazonaws.com/Microsoft_Office_2007-2010_Registry_ArtifactsFINAL.pdf, 16.08.2015.

[22] L., W. Wong, Forensic Analysis of The Windows Registry, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.85.3567&rep=rep1&type=pdf, 09.08.2015.

[23] İnternet: J. McQuaid, Finding and Analyzing Windows System Artifacts with IEF, https://www.magnetforensics.com/computer-forensics/finding-and-analyzing-windows-system-artifacts-with-ief, 02.08.2015.

[24] T. Henkoğlu, Adli Bilişim (Dijital Delillerin Elde Edilmesi ve Analizi), Pusula Yayıncılık, 1. Baskı, Ankara, 2013.