18/09/2013

Sayın Av. Kemal Yener SARAÇOĞLU,

İnceleme taleplerinize ilişkin, İzmir Cumhuriyet Başsavcılığı'nın 2010/xxx numaralı soruşturmasına delil olan sabit disk imajındaki dosya disteminin 2. bölümü olan suç unsuru içerdiği tespit edilen C: sürücüsü üzerinde bilimsel inceleme yapılmış ve elde edilen bulgular ekteki raporda bilgilerinize sunulmuştur.

Adli Bilirkişi
Tevfik Koray Peksayar

Mak. Müh. Lis. - Bilgi Tekn. Y. Lis.
İTÜ Diploma No: 76 - 387

Bilirkişi Hakkında

1975 İstanbul doğumluyum.

Hazırlık, ortaokul ve lise eğitimimi Nişantaşı Anadolu Lisesi'nde tamamladım. Nişantaşı Anadolu Lisesi Fen-Matematik bölümünden mezun oldum.

İstanbul Üniversitesi Mühendislik Fakültesi Makine Mühendisliği bölümünde lisans eğitimimi tamamladım.

İstanbul Teknik Üniversitesi Bilişim Enstitüsü Bilgi Teknolojileri Yüksek Lisans programıyla yüksek lisans eğitimi gördüm.

Elektronik, bilgisayar ve ağ sistemleri üzerine çalışmaya ortaokul yıllarında amatör olarak başladım.

Lise yıllarının sonunda bu çalışmalarım profesyonelliğe yöneldi.

Lisans eğitimimin son 3 yılında ve yüksek lisans eğitimim boyunca bilgisayar ve ağ sistemleri üzerine yaptığım çalışmalara profesyonel olarak devam ettim. Bu süre zarfında birden fazla işletmede, özellikle web uygulamaları, ağ ve intranet sistemleri ve bilişim sistemlerinin iyileştirilmesi konularında çalıştım.

1998 yılından itibaren sistem başarımı, güvenilirliği ve güvenliği üzerine çalışmalarda bulunmaya başladım.

Bu çalışmalarım sırasında Windows işletim sisteminin birçok sürümü, popüler uygulama yazılımları ve bu yazılımlarının belgelenmemiş çalışma şekil ve davranışları konusunda deneyim kazandım.

1999 yılından itibaren Windows tabanlı sistemlerin yanı sıra Linux işletim sistemi üzerine yoğunlaştım.

2000 yılından beri kendime ait şahıs firmam ile profesyonel hayatıma devam etmekteyim.

2010 yılından günümüze İstanbul Adli Yargı İlk Derece Mahkemesi Bilirkişi listesinde bilgi teknolojileri konusunda kayıtlı yeminli bilirkişiyim.

Bilimsel İnceleme ve Bilirkişi Görüşü

1. Giriş

İnceleme 02/07/2012 tarihinde xxxxxxxxxx'in taşınabilir bilgisayarına ait 320 GB sığalı HITACHI marka, HTS545032B9A300 model, 100602PBP300D6G7VVZPL seri numaralı sabit diskin imajındaki dosya disteminin 2. bölümü olan suç unsuru içerdiği tespit edilen C: sürücüsü üzerinde yapılmıştır.

2. İnceleme Yapılan Kütük Bilgileri

HITACHI marka CH4031532 model numaralı 320 GB sığalı sabit disk imajı

Cihaz Bilgileri	
Markası	HITACHI
Sığası	320 GB
Tipi	Sabit disk
Model Numarası	HTS545032B9A300
Seri Numarası	100602PBP300D6G7VVZPL

İmaj Bilgileri	
İmaj Dosyası	IMAGE.E01 ~ IMAGE.E36 adlı 36 parçadan oluşan imaj
İmaj Tarihi	02/07/2012 20:08
İmajın Alındığı Uygulama	Tableau TD1 cihazı
Sektör Sayısı	625.142,448
Sağlanan md5 İmzası	a7533c08f9cac1a01ca271855ddba2cd
Bulunan md5 İmzası	a7533c08f9cac1a01ca271855ddba2cd
Sağlanan sha1 İmzası	60aebd3bc2ad94ad52f55bc6506f2b71485c25ef
Bulunan sha1 İmzası	60aebd3bc2ad94ad52f55bc6506f2b71485c25ef

3. Kurulu İşletim Sistemi Bilgileri

İşletim Sistemi	Windows 7 Home Premium build 7600 (7600.win7_gdr.120503-2030 / 7600.17017.amd64fre.win7_gdr.120503-2030)
Kayıtlı Kullanıcı	tosh
Kayıtlı Kurum	<boş>
Ürün Kimliği	00359-OEM-8992687-00017
Ürün Anahtarı	6GF36-P4HWR-BFF84-6GFC2-BWX77
Kurulum Yolu	C:\Windows
Kurulum Kaynağı	<bilinmiyor>
Kurulum Tarihi	23/01/2011 23:20:32
Son Kullanıldığı Tarih	01/07/2012 13:19:22

4. Ağ Bağlantısı Bilgileri

Makine Adı	TOSH-TOSH
IP Yapılandırması	DHCP ile otomatik
Son Kullanılan DHCP Sunucusu	192.168.2.1
Son Alınan IP Adresi	192.168.2.2
Ağ Geçidi	192.168.2.1
İsim Sunucusu	192.168.2.1
Son IP alınma Tarihi	01/07/2012 10:18:39

5. Kullanıcı Bilgileri

Kullanıcı Adı	Administrator (Etkin olmayan hesap)
Kullanıcı Kimliği (SID)	S-1-5-21-2366511350-2415315305-206194855-500

Kullanıcı Adı	tosh (Hesap parola gerektirmiyor)
Kullanıcı Kimliği (SID)	S-1-5-21-2366511350-2415315305-206194855-1000

Yapılan incelemede sistemin etkin olarak kullanıldığı kullanıcı adının "tosh" olduğu tespit edilmiştir.

6. Virüs ve Zararlı Yazılım Bilgileri

Disk imajındaki dosya sisteminde Clam Antivirus ile yapılan taramada, sistem üzerinde kullanıcı onayı ve bilgisi dışında işlem yapılması özelliğine sahip 2 önemli virüs bulunmuştur.

6.1. W32.Trojan.Locotout

"C:\Users\tosh\AppData\Local\Temp\~!#B03C.tmp" dosyasında bulunan ve Clam Antivirus tarafından "*W32.Trojan.Locotout*" olarak tanınan bir "Truva atı"dır.

Yapılan incelemede bulaşmanın 19/05/2012 13:39:07 tarihinde olduğu tespit edilmiştir. Bulaşmanın ne yolla olduğu bilinmemektedir.

Bu dosya en güncel virüs veritabanına sahip olan VirusTotal web sitesiyle de teyid edilmiştir.

Bu Truva atı Microsoft tarafından "*Trojan:Win32/Locotout.gen!A*" olarak tanınmaktadır.

Microsoft'un resmi sitesinde, http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?name=TROJAN:WIN32/LOCOTOUT.GEN!A adresinde de detaylı olarak verilen bilgiye göre bu Truva atı başka bir Truva atı tarafından indirilebilmekte ve uzaktan komut alarak "ortadaki adam" yöntemiyle SPAM e-postalar göndermek için kullanılmaktadır.

Yapılan incelemede "C:\Users\tosh\AppData\Local\Temp\~!#B03C.tmp" dosyası 178.32.84.196 IP adresini içerdiği tespit edilmiştir.

6.2. Trojan.Java-3

"C:\Users\tosh\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\25\31fddfd9-1f8483ef" dosyasında bulunan ve Clam Antivirus tarafından "*Trojan.Java-3*" olarak tanınan bir "Truva atı" ailesidir.

Yapılan incelemede bulaşmanın 23/03/2011 01:50:08 tarihinde olduğu tespit edilmiştir. Zararlı yazılımın çalışma şeklinden dolayı bulaşmanın ziyaret edilen bir web sistesi yoluyla olduğu tahmin edilmektedir.

Bu Truva atı Microsoft tarafindan "*Exploit:Java/CVE-2010-0840*" olarak tanınmaktadır.

Microsoft'un resmi sitesinde, http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Exploit%3AJava%2FCVE-2010-0840 adresinde de detaylı olarak verilen bilgiye göre bu kötü amaçlı yazılım bir Java apleti olarak web tarayıcısında çalışmakta, belirli bir adresten çeşitli dosyalar ve başka zararlı yazılımlar indirmektedir, bu dosyalar geçici sistem dizinine yazılmaktadır ve indirilen zararlı yazılımlar da bu dizinde çalışmaktadır.

Bu Truva atı ailesinin birbirinden farklı özelliklere sahip değişik hallerinin bulunduğu bilinmektedir.

7. 16/01/2013 tarihli "BİLİRKİŞİ İNCELEME RAPORU"ndaki Hatalar ve Ek Bilgiler

7.1. Suç Konusu Dosyaların Bulunduğu Disk Bölümü

Söz konusu yazının 2. sayfasında imajda yer alan disk bölümleri listesi verilmiştir.

PARTITIONS (Disk Bölümleri)

Code	Type(Sistem Tipi)	Start Sector (Başlangıç Sektörü)	Total Sectors (Toplam Sektör)	Size (Boyut)
07	NTFS	2.048	819.200	400MB
07	NTFS	821.248	312.569.856	149GB
07	NTFS	313.391.104	311.750.656	148,7GB

Ancak bu bölümlerden 400MB sığalı bölümün C: sürücüsü, 149GB sığalı bölümün ise D: sürücüsü olduğu varsayılmıştır.

Halbuki, yapılan incelemeyle, işletim sisteminin kurulu olduğu bölüm olan C: sürücüsünün disk üzerinde 149 GB sığa ayrılmış 2. bölüm olduğu tespit edilmektedir.

Bu sebeple söz konusu yazıda yer alan dosyaların bulunduğu söylenen D: sürücüsü ibaresi hatalıdır ve aslında C: sürücüsünü göstermelidir.

Bu sebeple, okumakta olduğunuz bu raporda, D: sürücüsü yerine tam ve doğru olarak C: sürücüsü belrteci kullanılmıştır.

7.2. "Lost Files" Dizini

16/01/2013 tarihli "BİLİRKİŞİ İNCELEME RAPORU" başlıklı yazıda bir kısım dosyanın "Lost Files" dizininde yer aldığı bilgisi yer almaktadır.

"*Lost Files*" olarak tabir edilen bu dizin "*Kayıp veya silinmiş dosyaların bulunduğu alan*" olarak açıklanmaktadır.

Bu dizinin vasfının bu şekilde açıklanması teknik olarak eksik ve hatalıdır. "Lost Files" dizini,

incelemeyi yapan uzmanın kullandığı inceleme yazılımınca kullanılan bir terimdir.

Silinmiş ve diske yeni yazılacak dosyalar için ayrılan alanlarda diskten tamamen silinmek üzere bekleyen dağılmış parçalar olarak yer almakta olan dosyalar, kullanılan inceleme yazılımınca sanal olarak "Lost Files" dizini içindeymiş gibi gösterilmektedir.

Bu tür dosyalar "yetim dosyalar (orphan files)" ya da "kayıp dosyalar" olarak da adlandırılır.

"Yetim dosyalar", silinmiş fakat üst verileri dosya sisteminde geride kalmış dosyalardır. Bu üst veriler; dosya işlem tarihleri ve dosya parçalarının diskin hangi bloklarında yer aldığı gibi bilgileri içerir. Bu bilgiler kullanılarak dosya parçaları birleştirilerek dosyalar kurtarılabilir.

Fakat bu işlem sadece bazı disk bakım ve disk inceleme yazılımları tarafından yapılabilmektedir.

Yetim dosyalara normal kullanıcı tarafından erişilemez.

Windows dosya sisteminde "Lost Files" ismini taşıyan, kullanıcı tarafından görülebilen ve erişilebilen bir dizin bulunmamaktadır.

Yapılan incelemede de dosya sisteminde "Lost Files" isminde bir dizine rastlanmamıştır.

8. Suç Konusu Dosyaların İncelenmesi

Suç konusu olduğu tespiti 16/01/2013 tarihli İzmir Cumhuriyet Başsavcılığı'na sunulmak üzere düzenlenmiş "BİLİRKİŞİ İNCELEME RAPORU" başlıklı yazıyla yapılan ve söz konusu yazının ekinde listesi bulunan tüm dosyalar diskin C: sürücüsü üzerinde sayısal olarak izi kalmış dosyalardır.

Bu dosyalardan;

1. "C:\Users\tosh\AppData\Local\Microsoft\Windows\Temporary Internet Files" dizininde yer alanlar **silinmiş**,
2. 16/01/2013 tarihli "BİLİRKİŞİ İNCELEME RAPORU" başlıklı yazıda "C:\Lost Files" dizininde yer aldığı belirtilenler ise **yetim** dosyalardır.

Özet olarak, bu dosyaların tamamı kullanıcının göremediği dosyalardır.

Diskte yapılan dosya sistemi taramasında, C: sürücüsünde suç konusu dosyaların da aralarında bulunduğu 2932 (iki bin dokuz yüz otuz iki) dosyanın disk üzerinde oluşturulma, son erişim ve son değişiklik tarihlerinin eşit olduğu görülmektedir. Bu durum dosyaların diskte kopyalanarak oluşturulduklarını ve oluşturulduktan sonra hiç açılmadıklarına işaret etmmektedir.

Söz konusu dosyaların ilkinin diskte oluşturulma tarihi 18/06/2012 23:50:58 ve sonuncusunun diskte oluşturulma tarihi ise sistemin son kapatıldığı tarihten 2 dakika öncesi olan 01/07/2012 13:17:12'dir.

Söz konusu dosyaların işlem tarihleri incelendiğinde, dosya oluşturulma (dosya içindeki verinin son kez değişikliğe uğrayarak dosya haline geldiği) tarihinin sistemin kullanıldığı tarih aralığı dışında ve geçersiz tarihler taşıdıkları görülmektedir.

Bazı zararlı yazılımlar, sistem üzerinde çalışırken, sistemin başarımını (performansını) etkilememek için çeşitli sistem özelliklerini kullanmazlar, bu özellikler yerine kendi iç programlarında yer alan işlemlerle bazı işleri gerçekleştirirler. Bu işler arasında bazı tarih bilgilerinin rastgele ya da zararlı yazılıma özgü olarak oluşturulduğu da bilinmektedir.

9. Sonuç

Sözü edilen;

1. Dosyaların disk üzerinde oluşturulma, son erişim ve son değişiklik tarihlerinin eşit olduğu görülmektedir.

2. Suç konusu dosyalarda tarih tutarsızlığı görülmektedir.

3. Internet Explorer'ın kullanıcı farkındalığı dışında internetten dosya indirmesine sebep olan Trojan.Java-3 zararlı yazılımı dosyaların diske kaydedildiği tarihte etkindir.

4. Suç konusu yetim dosyaların kurtarılabilenleri incelendiğinde, internet sitelerinde yer alan küçük resimler ve tam boy olmayan resimler oldukları izlenimi vermektedir.

5. Sistem 23/01/2011 23:20:32 ile 01/07/2012 13:19:22 tarihleri arasında, yaklaşık 1yıl 6 ay boyunca, kullanımda olmasına rağmen 8. maddede bahsedilen 2932 (iki bin dokuz yüz otuz iki) suç konusu dosyanın 18/06/2012 23:50:58 ile 01/07/2012 13:17:12 tarihleri arasında 13 günde diskte oluşması dikkat çekicidir.

Söz konusu dosyaların Trojan.Java-3 zararlı yazılımı veya bu yazılımla sisteme bulaştırılan diğer zararlı yaılımlar kullanılarak diske indirildiğinden şüphelenilmektedir.

Yukarıda sıralanan sebepler dolayısıyla disk üzerindeki suç konusu dosyaların ve benzer nitelikteki diğer dosyaların kullanıcı isteği ve farkındalığı dahilinde kaydedilmiş olması derin şüpheye haizdir.

Adli Bilirkişi
Tevfik Koray Peksayar

Mak. Müh. Lis. - Bilgi Tekn. Y. Lis.
İTÜ Diploma No: 76 - 387