ODATV SORUŞTURMASI DİJİTAL ADLİ ANALİZ EK RAPORU

12 KASIM 2012

Hazırlayanlar

Osman PAMUK
Ünal TATAR
Emin ÇALIŞKAN

İÇİNDEKİLER

1 KONU 6

KAPSAM 6

ANALİZ SORULARI 6

İNCELENEN DELİLLER 6

2 İNCELEME 7

KULLANILAN ARAÇLAR 7

METODOLOJİ 7

3 MÜZEKKERE SORULARI 8

SORU 1 8

Cevap 1 8

SORU 2 17

Cevap 2 17

SORU 3 22

Cevap 3 22

SORU 4 24

Cevap 4 24

SORU 5 43

Cevap 5 43

SORU 6 47

Cevap 6 47

SORU 7 52

Cevap 7 52

SORU 8 54

Cevap 8 54

SORU 9 59

Hanefi Avcı 1. Soru 59

Hanefi Avcı 2. Soru 59

Hanefi Avcı 3. Soru 59

Hanefi Avcı 4. Soru *60*
Hanefi Avcı 5. Soru *60*
Hanefi Avcı 6. Soru *61*
Hanefi Avcı 7. Soru *62*
Hanefi Avcı 8. Soru *62*
Hanefi Avcı 9. Soru *63*
Hanefi Avcı 10. Soru *64*
Hanefi Avcı 11. Soru *64*
SORU 10 65
Soner Yalçın 1. Soru *65*
Soner Yalçın 2. Soru *65*
Soner Yalçın 3. Soru *65*
Soner Yalçın 4. Soru *66*
Soner Yalçın 5. Soru *67*
Soner Yalçın 6. Soru *68*
4 EKLER 69
EK-1 69
EK-2 72
Ofis kullanıcısı "soner" *72*
Ofis kullanıcısı "Barış" *77*
Ofis kullanıcısı "pc" *79*
Ofis kullanıcısı "Your User Name" *82*
EK-3 84
Delil1 deki EK-1 dosyalarının izleri *84*
Delil2 deki EK-1 dosyalarının izleri *85*
Delil3 deki EK-1 dosyalarının izleri *86*

TABLOLAR

Tablo 1 - Delil 1, 2, 3 Ofis Ayarları 9
Tablo 2 - EK-1 Listesinde Tespit Edilebilen Ofis Üst Verileri 10
Tablo 3 - Erişim Zamanı Oluşturma Zamanından Sonra Olan Dosyalar 20
Tablo 4 - Delil 2 Eset Nod32 Taramasında Tespit Edilen “Jangomail” Eklentileri 28
Tablo 5 - Delil 2’ye “Jangomail” Kullanılarak Gönderilen E-postalar 31
Tablo 6 -Delil 3 “jangomail” E-posta Ekleri Antivirüs Tespit ve Güvenlik Uyarıları 41
Tablo 7 - Delil 2 “jangomail” E-posta Ekleri Antivirüs Tespit ve Güvenlik Uyarıları 41
Tablo 8 - Delil 3 “jangomail” E-posta Ekleri Antivirüs Tespit ve Güvenlik Uyarıları 41
Tablo 9 - Delil 3 İnternet Geçmişi Kayıtları 43
Tablo 10 - Delil 3 ESET Antivirüs Programı İnternet Kayıtları 45
Tablo 11 - Delil 1’e “jangomail” ile Gönderilen E-Posta Eklenti Özellikleri 53
Tablo 12 - "SY.doc" ve "prj_60.doc" Dosya ve Dosya Sistemi Üst Verileri 57
Tablo 13 - "sy.doc" ve "prj_60.doc" ile Alakalı $LogFile Kayıtları 58
Tablo 14 - Ofis yazar isminin "soner" olduğu diğer dokümanlar 76
Tablo 15 - Ofis son değiştiren isminin "soner" olduğu diğer dokümanlar 76
Tablo 16 - Ofis yazar isminin "soner" olduğu diğer dokümanlar 78
Tablo 17 - Ofis son değiştiren kullanıcı isminin "soner" olduğu diğer dokümanlar 78
Tablo 18 - Ofis yazar isminin "pc" olduğu diğer dokümanlar 80
Tablo 19 - Ofis son değiştiren kullanıcı isminin "pc" olduğu diğer dokümanlar 82
Tablo 20 - Ofis yazar kullanıcı isminin "Your User Name" olduğu diğer dokümanlar 82
Tablo 21 - Ofis son değiştiren kullanıcı isminin "Your User Name" olduğu diğer dokümanlar 83

ŞEKİLLER

Şekil 1 - Ofis Yazar Üst Verisi “soner” Olan “Seyyid.doc” Dokümanının İçeriği 11
Şekil 2 - “Seyyid.doc” Dokümanın “Soner Yalçın” Adıyla Yayınlanması 12
Şekil 3 - Yazar Üst Verisi "Barış" Olan “alevi.doc” Dosyası İçeriği 13
Şekil 4 - “alevi.doc” İsimli Dosyanın İçeriğinin Yayınlanmış Hali 14
Şekil 5 - “dilekçe.doc” İsimli Dosyanın İçeriği 15
Şekil 6 - Delil 2 Bilgisayarında Bulunan “CCleaner” Uygulamasının İzleri 18
Şekil 7 - Delil 1 E-posta Hesapları 25
Şekil 8 - Delil 1 “Atatürk ekran koruması” E-postası 26
Şekil 9 - Delil 2 Antivirüs Son Güncelleme Tarihi 27
Şekil 10 - Delil 2 Barış Pehlivan Outlook Hesabı 29
Şekil 11 - Delil 2 “Infected Items” Klasörü İlk Durum 29
Şekil 12 - Delil 2 “Infected İtems” Klasörü Son Durum 30
Şekil 13 - Delil 3 Başlangıç Programları Engelleme Uyarısı 32
Şekil 14 - Delil 3 “Windows Defender”’da İstenmeyen “wmplayer.exe” Başlangıç Programı 33
Şekil 15 - Delil 3 “Windows Defender” İstenmeyen “adobe.exe” Başlangıç Programı 34
Şekil 16 - Delil 3’te Engellenen Başlangıç Programları Menüsü 35
Şekil 17 - Delil 3 Windows Defender otomatik tarama uyarısı 35
Şekil 18 - Delil 3’te “Windows Defender” Otomatik Tarama Sonucu 36
Şekil 19 - Delil 3 Eset Güvenlik Riski Uyarısı 37
Şekil 20 - Delil 3 Eset Antivirüs Veritabanı Güncel Olmadığı Uyarısı 37
Şekil 21 - Delil 3 “kayseri2.scr” Otomatik Başlangıç Programı Uyarısı 38
Şekil 22 - Delil 3 “0tayyip2it2.scr” Otomatik Başlangıç Programı Uyarısı 39
Şekil 23 - Teamviewer Giriş Ekranı 48
Şekil 24 - Teamviewer Parola Ekranı 48
Şekil 25 - Bağlantı Sırasında Ekran Görüntüsü 49
Şekil 26 - Delil 1 Bilgisayarı Teamviewer Yapılandırma Ayarları 50
Şekil 27 - Delil 2 Bilgisayarı Teamviewer Yapılandırma Ayarları 50

1 KONU

Kapsam

T.C. 16. Ağır Ceza Mahkemesinin 2011/14 dosya No'lu 26.09.2012 tarihli yazısına istinaden gerçekleştirilen ek dijital adli analiz çalışma sonuçlarını içermektedir.

Analiz Soruları

26.09.2012 tarihinde teslim alınan müzekkerede bulunan 10 soru ile müzekkere ekinde bulunan ve Sanık Hanefi AVCI'nın 09.10.2012 tarihli 11 adet, Sanık Hüseyin Soner YALÇIN müdafii Av. Duygun YARSUVAT'ın 25.09.2012 tarihli 6 adet sorusunu kapsamaktadır.

İncelenen Deliller

ODATV'de yapılan arama sonucunda elde edilen Seagate Marka "ST3120827AS_4MS1TF89" seri numaralı bilgisayar hard diski, sanık Barış PEHLİVAN'ın evinde yapılan arama sonucunda elde edilen Fujitsu Marka "MHV2060BHNW18T6229459" seri numaralı hard disk ve sanık Müyesser Uğur YILDIZ'ın evinde yapılan aramada elde edilen Samsung Marka "S17HJ90Q816726" seri numaralı harddisk incelenmiştir. Raporda bulunan bazı yorumlarda; ODATV'den elde edilen ST3120827AS_4MS1TF89 seri numaralı imaj için **Delil 1,** Barış PEHLİVAN'dan elde edilen MHV2060BHNW18T6229459 seri numaralı imaj için **Delil 2**, Müyesser Uğur YILDIZ'dan elde edilen imaj için **Delil 3** isimlendirilmesi yapılmıştır.

2 İNCELEME

Kullanılan araçlar

Disklerin incelenmesi için AccessData® FTK® Imager 3.1.0.1514[1], Encase 6.18.0.59[2], Encase 7.03.01.203, SIFT 2.13 Linux İşletim Sistemi[3], R-Studio[4], Mount Image Pro[5], LiveView[6] vb. dijital adli analiz araçları kullanılmıştır.

Metodoloji

Müzekkerede ve müzekkere ekine iliştirilen dilekçelerde bulunan sorulara yönelik araştırmalar yapılmış, hard disk imajları adli analiz araçlarıyla detaylı tetkik edilmiş, zararlı yazılım incelemesine yönelik statik ve dinamik analizler yapılmıştır. Tespit edilen bulgular dijital adli analiz metodolojisine göre değerlendirilmiş ve oluşan kanı açık bir dille ifade edilmiştir.

[1] http://accessdata.com/
[2] http://www.guidancesoftware.com/encase-forensic.htm
[3] http://computer-forensics.sans.org/community/downloads
[4] http://www.r-studio.com/
[5] http://www.mountimage.com/
[6] http://liveview.sourceforge.net/

3 MÜZEKKERE SORULARI

Soru 1

EK-1 de yer alan ve raporda belirtilen dosyaların anılan bilgisayarlarda kesin olarak oluşturulup oluşturulmadığı, değiştirilip değiştirilmediğinin tespitinin mümkün olup olmadığı? Kesin olarak tespitinin mümkün olmaması halinde bunun nedenlerinin yalın ve açıklayıcı bir şekilde belirtilmesinin istenmesi?

Cevap 1

Herhangi bir dosyanın bir bilgisayarlarda oluşturulup oluşturulmadığı, değiştirilip değiştirilmediğinin **kesin tespiti mümkün değildir**. Bunun sebebi bir dosyanın bir bilgisayarda oluşturulduğuna veya değiştirildiğine işaret eden dijital bulguların kesinlik ifade etmemesi ve bilgi sahibi bir kullanıcı tarafından değiştirilebilir olmasıdır. Bunun yanında elde edilen ek bilgiler, normal kullanıcıların bilgisayar kullanım alışkanlıkları, tespit edilen bulguların değiştirilebilme zorluğu ve bulguların kendi içindeki uyumu göz önünde bulundurularak, bir dosyanın oluşturulduğu veya değiştirildiği bilgisayar konusunda **kanaat bildirmek mümkündür**.

Herhangi bir Microsoft ofis dokümanının, Microsoft ofis programları (word, excel ...) ile bir bilgisayarda oluşturulup oluşturulmadığını anlamak için göz atılan bulgulardan ilki, o dosyanın üst verileridir. Dosya üst verilerinden biri olan "Yazar" (Author) ve “Şirket” (Company) alanında bulunan bilgi, bir bilgisayarlardaki Microsoft ofis programının yazar ve şirket bilgisi ile aynı ise bu dokümanın bu bilgisayarda **oluşturulmuş olma ihtimali yüksektir**. Bunun yanında, eğer doküman bir bilgisayarda değiştirilmiş ise, doküman içindeki Microsoft ofis sürüm bilgisi ile dokümanın değiştirildiği düşünülen bilgisayarda kurulu olan Microsoft ofis programının sürüm bilgisi de uyumlu olmalıdır. Bunun bir istisnası ise bilgisayarda bulunan Microsoft ofis programının güncellenmesi sonucunda bilgisayardaki son ofis sürümünün daha ileri olma ihtimalidir. Buna ek olarak, ofis belgeleri güncellendikçe, dosyayı son değiştiren kullanıcının bilgisayarda kayıtlı olan ofis kullanıcı ismi, doküman içindeki "son değiştiren" üst verisini güncellemektedir. Bu sebeple dokümanda kayıtlı olan ofis kullanıcı bilgisi ve ofis sürümü incelenen bilgisayarlardaki verilerle karşılaştırılarak, o dokümanın **yüksek ihtimalle hangi kullanıcı tarafından değiştirildiği** tespit edilebilir.

Ofis dokümanlarını oluşturmak ya da değiştirmek için kullanılabilecek diğer programlar (Wordpad, OpenOffice, LibreOffice, ...) için yazar, son değiştiren, şirket ya da uygulama sürümü bilgilerinin nasıl güncelleneceği programdan programa değişebilir ve Microsoft Ofis

programlarından farklılıklar gösterebilir. Mesela Wordpad ile "DOCX" uzantılı bir doküman oluşturulduğunda yazar, son değiştiren, şirket ve uygulama sürümü bilgileri boş olmaktadır.

Dosya üst verileri dışında, dokümanın bir kopyasının ya da eski bir sürümünün bir bilgisayarda bulunması veya izlerine rastlanması da o dokümanın o bilgisayarda oluşturulduğuna veya değiştirildiğine dair kuvvetli bir bulgu oluşturabilir. Buna ek olarak, dosya sistemi üst verileri de bir dokümanın bir bilgisayarda oluşturulmuş veya değiştirilmiş olduğuna dair bilgi verebilir.

Delillere ait ofis ayarları Tablo 1'de, EK-1 listesinde bulunan dosyaların ofis üst verileri de Tablo 2'de gösterilmiştir.

Delil	Ofis Kullanıcı Adı	Şirket	Microsoft Ofis Sürümü
DELİL1	Sys		**11.9999** (**11.5606** 2010:12:30 öncesi)
DELİL2	TOSHIBA	SATELLITE	**11.5606**
DELİL3	user	SuSel	**11.9999** (**11.8036** 2009:10:04 öncesi)

Tablo 1 - Delil 1, 2, 3 Ofis Ayarları

Dosya ismi	Yazar	Son Değiştiren	Şirket	Uygulama, Sürüm
Ermeni Dosyası.doc	OPEY A.	OPEY A.	STRATEJİ	MS Word 8.3814
Koz.doc	soner	soner	Conqueror	MS Word 10.2605
Nedim.doc	soner	soner	Conqueror	MS Word 10.2605
EK-D MİLİ EĞİTİM.doc	KARA KUVVETLERI KOMUTANLIGI	bim	tsk	MS Word 9.0
YBelgesi.doc	nsener	nsener		MS Word 11.5606
Fabrikatör.doc	OPEY A.	OPEY A.	STRATEJİ	MS Word 8.3814
Ulusal Medya.doc	OPEY A.	OPEY A.	STRATEJİ	MS Word 8.3814
Tv Analiz Proje.doc	Ümit OĞUZTAN	OPEY A.	COMPAQ	MS Word 8.3814
Reosta Operasyonu.doc	OPEY A.	OPEY A.	STRATEJİ	MS Word 8.3814
panzehir.doc	OPEY A.	OPEY A.	STRATEJİ	MS Word 8.3814
mit medya.doc	OPEY A.	OPEY A.	STRATEJİ	MS Word 8.3814
mafia.doc	OPEY A.	OPEY A.	STRATEJİ	MS Word 8.3814
Sabri Uzun.doc	soner	soner	Conqueror	MS Word 10.2605
Konuşma Notu.doc	KARA KUVVETLERİ	Celalettin BACANLI	KARA KUVVETLE	MS Word 9.2812

	KOMUTANLIĞI		RI KOMUTANLIGI	
KADROLAŞMA KONUŞMA NOTU (OCAK2004).doc	KARA KUVVETLERI KOMUTANLIGI	KARA KUVVETLERI KOMUTANLIGI	KARA KUVVETLERI KOMUTANLIGI	MS Word 9.4402
Kadrolaşma en son0610170003.doc	bim	bim	kkk	MS Word 9.0
Kadrolaşma Bilgi Notu (Ocxak 2004).doc	bim	KARA KUVVETLERI KOMUTANLIGI	kkk	MS Word 9.4402
EK-E AKP'NİN ATAMALARI.xls	bim	KARA KUVVETLERI KOMUTANLIGI	KARA KUVVETLERI KOMUTANLIGI	MS Excel 9.4402
000KITAP.docx	a	sahmet	b	MS Word
Ulusal Medya 2010.doc	pc	soner		MS Word 10.2605
toplantı.doc	Barış	Barış		MS Word 11.5606
prj_60.doc	Barış	TOSHIBA		MS Word 11.5606
Yalçın hoca.doc	soner	user	Conqueror	MS Word 10.2605
SY.doc	soner	TOSHIBA	Conqueror	MS Word 11.5606
teRTEmiz.doc	Your User Name	soner		MS Word 10.2605
Hanefi.doc	soner	soner	Conqueror	MS Word 10.2605
Bilinçlendirme.doc	USER	soner		MS Word 10.2605
Sn. Komutanım.doc	pc	pc		MS Word 11.5606

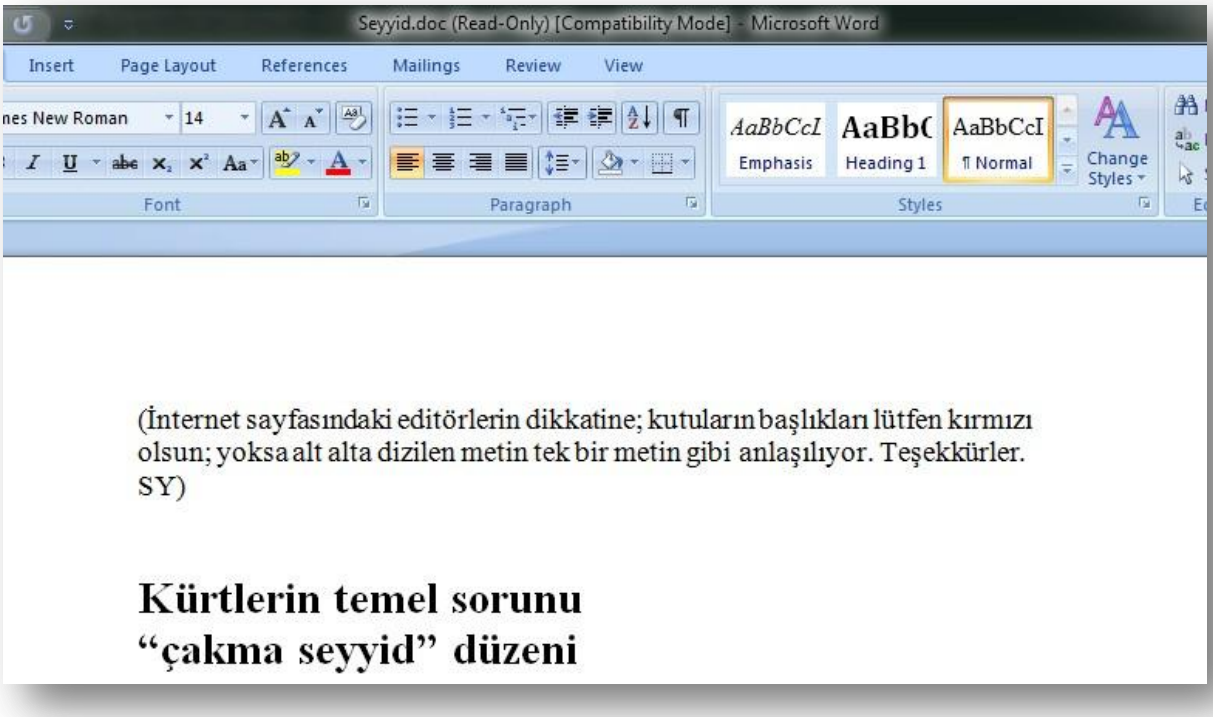
Tablo 2 - EK-1 Listesinde Tespit Edilebilen Ofis Üst Verileri

Tablo 2 deki üst verilerle uyumlu üst verilere sahip olan ve Delil 1, 2 ve 3 bilgisayarlarında bulunan diğer dokümanlar da incelenmiş ve EK-2'de listelenen tablolar çıkarılmıştır. Bu inceleme sonucunda elde edilen bulgular şu şekildedir:

- “soner”, “Barış”, “pc” ve “Your User Name” ofis kullanıcı isimleri, EK-1 listesindeki dosyalar dışında, delil bilgisayarlarındaki birçok dosyada bulunmaktadır.

- Bu dosyalar içinde, yazar alanında “soner”, “Barış”, “pc” ve “Your User Name”, son değiştiren alanında ise “Sys” ofis kullanıcı isimlerinin geçtiği dokümanlara rastlanmıştır. “Sys” Delil 1 bilgisayarındaki ofis kullanıcı ismidir. Bu şartları sağlayan dokümanlarda ofis üst verileri ve dosya sistemi üst verileri incelendiğinde, bu dokümanların **yüksek ihtimalle Delil 1 bilgisayar kullanıcısı tarafından değiştirildiği kanaatine varılmıştır.**

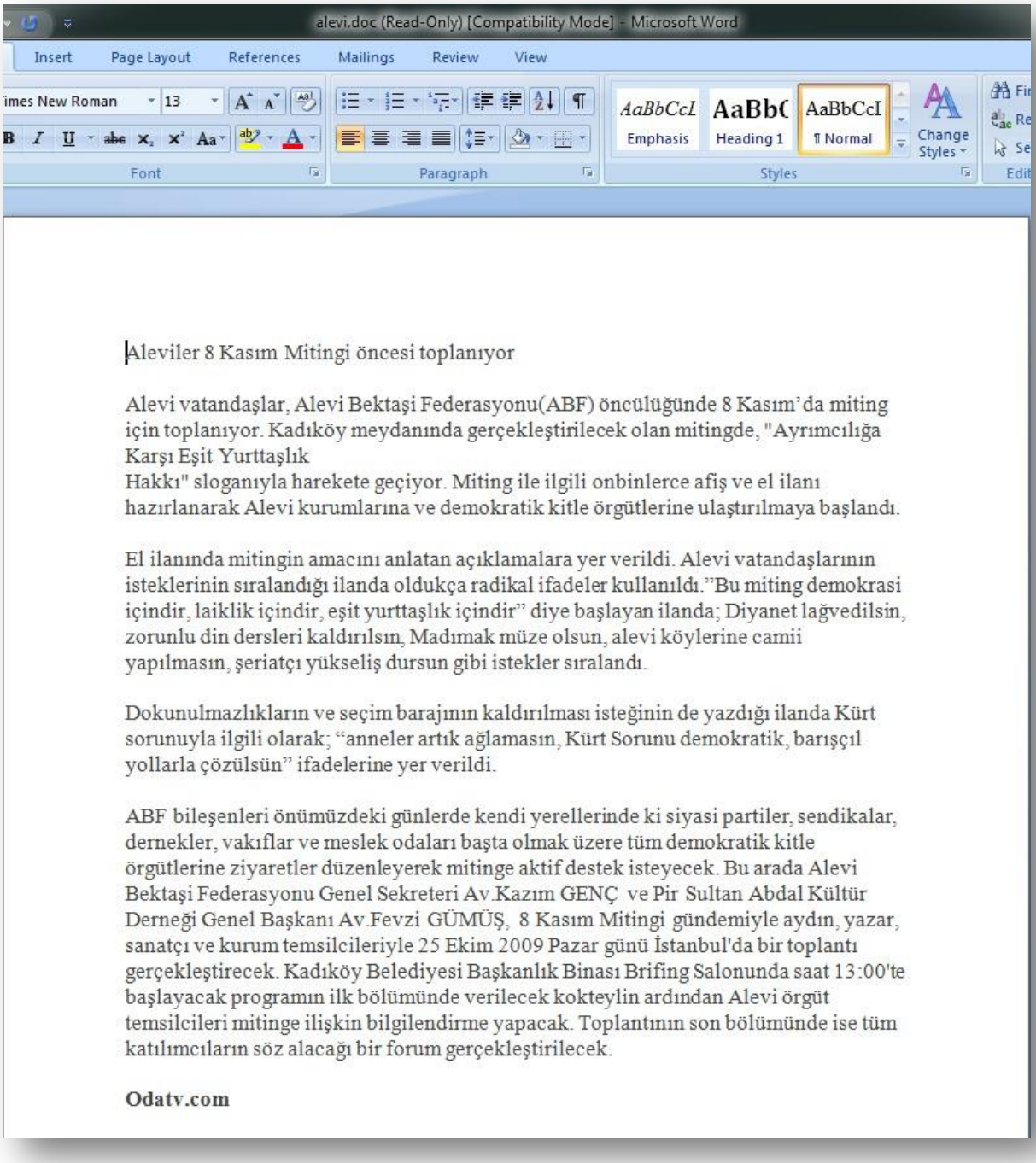
- Buna ek olarak yazar alanında “soner” ofis kullanıcı isminin olduğu, yüksek ihtimalle Delil 1 bilgisayar kullanıcısı tarafından değiştirilmiş dokümanlar içinde “Soner Yalçın” imzasıyla yayınlanan haber yazıları olduğu tespit edilmiştir. Örnek olarak tespit edilen “Seyyid.doc” dokümanın Delil 1 deki içeriği Şekil 1’de, internet üzerinde “Soner Yalçın” ismiyle yayınlanmış hali Şekil 2’de görüntülenmiştir.



Şekil 1 - Ofis Yazar Üst Verisi “soner” Olan “Seyyid.doc” Dokümanının İçeriği

Şekil 2 - "Seyyid.doc" Dokümanın "Soner Yalçın" Adıyla Yayınlanması

- Aynı şekilde yazar alanında "Barış" ofis kullanıcı isminin olduğu, yüksek ihtimalle Delil 1 bilgisayar kullanıcısı tarafından değiştirilmiş dokümanlar içinde Oda TV'nin web sayfasında yayınlanan haber yazılarına (bkz. Şekil 3 ve Şekil 4) rastlanmıştır. Aynı zamanda yazar alanında "Barış", son değiştiren alanında "Sys" (Delil 1'de tanımlı ofis kullanıcısı) bulunan "dilekçe.doc" (Şekil 5) dokümanının içeriğinde "Barış Pehlivan" ismine rastlanmıştır.



Şekil 3 - Yazar Üst Verisi "Barış" Olan "alevi.doc" Dosyası İçeriği

Şekil 4 - "alevi.doc" İsimli Dosyanın İçeriğinin Yayınlanmış Hali

Şekil 5 - "dilekçe.doc" İsimli Dosyanın İçeriği

Yukarıda listelenen bulgular ile Cevap 3'te açıklandığı üzere, EK-1 listesindeki dosyaların Delil 1 ve 2 bilgisayarlarına, bahse konu olan zararlı yazılımlar ile yüksek ihtimalle gönderilmediği de göz ününde bulundurulduğunda; yazar alanında ofis kullanıcı ismi "soner" olan dokümanların (bkz. EK-2) **yüksek ihtimalle** "Soner Yalçın" isimli şahsa ait farklı bir bilgisayarda oluşturulduğu, yazar alanında "Barış" yazan dokümanların da (bkz. EK-2) **yüksek ihtimalle** "Barış Pehlivan" isimli şahsa ait farklı bir bilgisayarda oluşturulduğu ve

daha sonra ilgili bilgisayarlara CD/DVD, USB tarzı veri depolama cihazları ile taşındığı değerlendirilmektedir. Benzer şekilde, son değiştiren kullanıcı alanında “soner” ve “Barış” kullanıcı isminin geçtiği dokümanların da sırasıyla “Soner Yalçın” ve ”Barış Pehlivan” kullanıcılarına ait farklı bilgisayarlarda son olarak **değiştirilmiş olma ihtimalinin yüksek olduğu** değerlendirilmektedir.

Tablo 1 ve Tablo 2 deki veriler ve yukarıda verdiğimiz bilgiler ışığında “prj_60.doc” ve “SY.doc” dosyaları dışındaki diğer dosyaların Delil 1, 2 veya 3 bilgisayarında **oluşturulmuş veya değiştirilmiş olma ihtimali çok düşüktür**. **İncelemeye konu olan EK-1 dosyaları için işletim sistemi izleri ve dosya sistemi üst verileri, ofis üst verileri değerlendirildiğinde oluşan kanaati kuvvetlendirmektedir.** “prj_60.doc” ve “SY.doc” dosyalarının durumu cevap 8’de açıklanmıştır.

Soru 2

EK-1 de yer alan ve raporda belirtilen dosyaların anılan bilgisayarlarda 'açıldığına dair bulguya rastlanılmadığı' olgusunun yalın bir şekilde açıklanması, belgenin açıldığına dair izlerin nerede ve ne şekilde bulunacağının açıklanması, 'bu tür bulguya rastlanmamış olmasının kullanıcı tarafından kesin olarak açılmadığı anlamına gelmeyeceği' belirlemesinin yine yalın bir şekilde açıklanması, kesin olarak belirleme yapılamamasının nedenlerinin hangi olasılıklardan kaynaklandığının ayrıntılı bir şekilde belirtilmesi? Belgenin açılması veya açılmaması konusunda bir oran verilip verilemeyeceğinin tartışılması? Harici bir taşıyıcı üzerinden, bilgisayar hard diskine dosyanın kaydedilmeden açılması halinde, açılan belgenin o bilgisayarda açıldığına dair iz bırakıp bırakmayacağı? Bilgisayarda mevcut işletim sistemini kullanılmadan, cd/dvd sürücüsü üzerinden doğrudan çalıştırılan işletim sisteminin anılan bilgisayarlarda kullanılıp kullanılmadığı, kullanılmış ise belgelerin bu yöntemle açılıp açılmadığının tespitinin mümkün olup olmadığı? Bu yöntemle açılmış ise kullanılmayan işletim sistemi üzerinde açılma izlerinin bulunup bulunmayacağının açıklanması? Belirtilen bilgisayarlarla aynı ağa bağlı paylaşım izni verilen başka bilgisayar bulunup bulunmadığının tespiti? Aynı ağa başka bilgisayar tarafından dosyaların açılıp açılmadığının tespitinin mümkün olup olmadığı? Dosyaların bu şekilde açılması halinde iz bırakıp bırakmayacağı, bu halin tespit edilip edilemeyeceğinin belirtilmesi?

Cevap 2

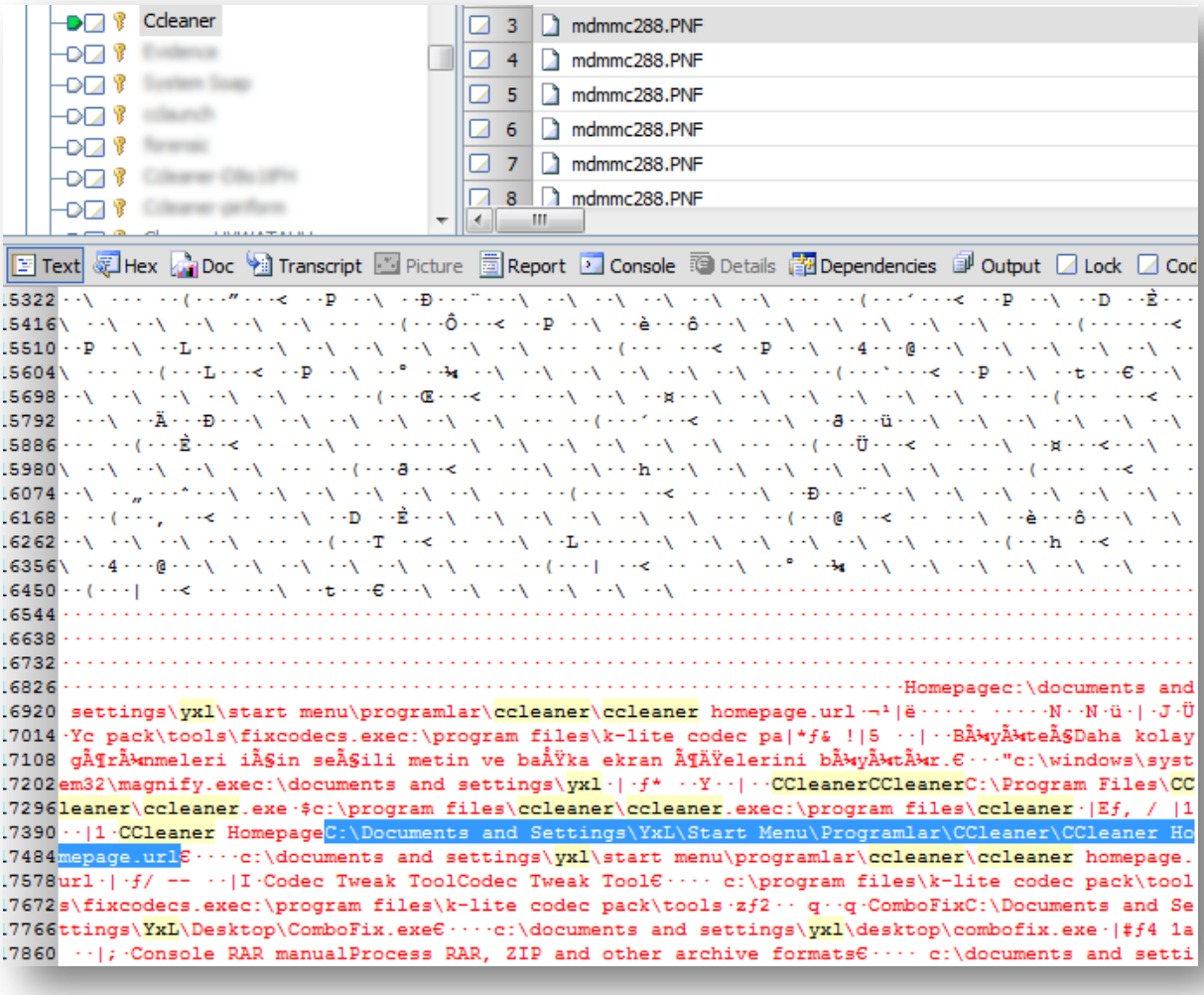
Microsoft Windows ailesi işletim sistemlerinde bir ofis dokümanı açıldığında oluşan izler[7] şu şekilde kategorize edilebilir;

- İşletim sistemi izleri
    - Açılan dokümanlar için oluşturulan LNK uzantılı dosyalar
    - Kayıt defterinde (Registry) işletim sistemi tarafından oluşturulan kayıtlar
- Dokümanı açan programın izleri
    - Kayıt defterinde (Registry) dokümanı açan programlar tarafından oluşturulan kayıtlar
    - Dokümanı açan programın PF uzantılı "prefetch" dosyaları
    - Dokümanı açan programın kayıt girdileri
- Dosya sistemi üst verileri değişiklikleri
    - Dosya erişim tarihinin güncellenmesi
    - Dosya değiştirme tarihinin güncellenmesi

[7] http://blogs.sans.org/computer-forensics/files/2012/06/SANS-Digital-Forensics-and-Incident-Response-Poster-2012.pdf

Bu izlerin bir kısmı **geçici izlerdir** (zaman geçtikçe bu izler silinip üzerlerine yeni açılan dokümanların izleri gelebilir). Aynı zamanda bu izler bilgili bir kullanıcı tarafından elle veya çeşitli yardımcı programlar vasıtasıyla (Ccleaner[8] gibi) silinebilir.

Delil 2 bilgisayarında bu tür izleri silmek için kullanılan "Ccleaner" uygulamasına ait izlere rastlanmıştır. Araştırma sonucunda yukarıda bahsi geçen "Ccleaner" uygulamasıyla ilgili çeşitli izlere Delil 2 bilgisayarında rastlanılmıştır (Şekil 6).



Şekil 6 - Delil 2 Bilgisayarında Bulunan "CCleaner" Uygulamasının İzleri

Bilgisayardaki bir dosyanın "slack" alanında tespit edilen bu izler *C:\program files\ccleaner\ccleaner.exe* ve *C:\Documents and Settings\YxL\Start Menu\Programlar\CCleaner\CCleaner Homepage.url* dosyalarını işaret etmektedir. Delil 2 bilgisayarındaki "C" sürücüsünün adının "YxL" olması ve diskteki birçok dizin ve dosyada

[8] *www.piriform.com/CCLEANER*

"YxL" kelimesinin geçmesi, kullanıcı adının bilgisayar kullanıcısıyla ilişkili olduğunu göstermektedir. Buna ek olarak tespit edilen dosya yolları isimlerinde *C:\program files* ve *C:\Documents and Settings\YxL\Start Menu\Programlar* klasör isimlerinin geçmesi, uygulamanın **yüksek ihtimalle** kullanıcı tarafından Delil 2 bilgisayarına kurulmuş olduğuna işaret etmektedir.

Dava kapsamında incelenen Delil 2 bilgisayarında $LogFile sistem dosyasında, EK-1 dosyalarının birçoğunun ismi geçmesi[9], bununla birlikte dosya içeriklerine ve MFT kayıtlarına dair hiçbir izin bulunmamasının sebebi, dosyaların "Ccleaner" ile temizlenmiş olması olabilir.

Ayrıca bu izler, dokümanların bilgisayarlarda kurulu bulunan işletim sistemi içinde açılması ile oluşan izlerdir. Bilgisayarlar "live" işletim sistemleri[10] (işletim sisteminin CD, DVD ya da USB depolama birimi içinde olduğu ve çoğunluğu itibariyle diskte herhangi bir iz bırakmayan sistemler) ile açıldığında bu izler oluşmayabilir. Bu işletim sistemleri kendilerini CD, DVD ya da USB üzerinden çalıştırır ve genellikle "Linux" tabanlıdır[11]. İşletim sistemi açıldığında dosya sistemi için bilgisayarın hafızasını (RAM) kullanır. Bu işletim sistemlerinde bilgisayarda bulunan hard disk(ler) sadece okunur (read-only) olarak yüklenip (mount), içindeki dokümanları açma imkânı vardır. Bu durumda bilgisayar kapatıldıktan sonra bilgisayarda disk üzerinde bir dokümanın açıldığına dair veya bu işletim sisteminin çalıştırıldığına dair **herhangi bir iz kalmayacaktır**.

Genelde ofis dosyalarını açmak için Microsoft Word, Microsoft Excel gibi programlar kullanılmaktadır. Fakat bunların yanında alternatif ofis programları (OpenOffice, LibreOffice, ...) da dosyaları açabilmekte ve bunların bıraktığı izler Microsoft ofis programlarının bıraktığı izlerden farklılık göstermektedir. Ayrıca yapılan testlerde "DOC" ve "DOCX" uzantılı dosyalar için yine Microsoft şirketinin işletim sistemleri içinde ücretsiz dağıttığı Wordpad uygulamasının da kullanılabildiği tespit edilmiş ve bu programın da farklı izler oluşturduğu görülmüştür. Bütün bu programların yanında Microsoft Vista işletim sistemi ile birlikte ana dosya sistemi görüntüleme aracı olan "Windows Explorer (*Windows* gezgini)" programına "ön izleme" (Preview) özelliği eklenmiş bulunmaktadır. Bu ön izleme seçeneği açık iken dosyaların üzerine gelindiğinde dosya açılmadan içeriğinin görüntülenmesi mümkün olmaktadır. Bu şekilde yapılan görüntülemelerde dosyanın içeriği değiştirilememekte ve dosyanın açıldığına dair herhangi bir iz oluşmamaktadır.

[9] **Error! Reference source not found.**
[10] http://en.wikipedia.org/wiki/Live_CD
[11] http://www.livecdlist.com

Harici disk ya da ağ üzerinden bir dosya açıldığı zaman, işletim sistemi izleri ve dokümanı açan programın izleri oluşacaktır. Dosya sistemi türlerine göre farklılık gösterse de, bu durumda dosyalar incelenen bilgisayar üzerinde olmadığından, oluşacak üst veriler incelenemeyecektir. Microsoft Windows işletim sisteminde, kayıt defteri (registry) girdileri ve LNK uzantılı dosyalar incelenerek, ağ üzerinden veya harici bir depolama biriminden açılan ya da değiştirilen dosyalar tespit edilebilecektir. Bunun istisnası ise cevabın ilk bölümünde bahsedildiği üzere, bu izlerin belli bir zaman sonra üzerine yazılabilmesi veya elle/program yardımıyla silinebilir olmasıdır.

Yukarıda ayrıntılı bir şekilde açıklandığı üzere dosyaların açılmasıyla alakalı izlere rastlanmamış olması, ilgili dokümanların açılmadığını kesin olarak göstermemektedir. Bu izlere rastlanılması ise kuvvetli bir ihtimalle bu dokümanların açıldığına işaret etmektedir.

Dosya sistemi erişim tarihlerine bakılarak yapılan incelemede, erişim tarihleri dosya sistemi oluşturma tarihlerinden yeni olan dosyalar aşağıdaki tabloda gösterilmiştir.

Dosya Konumu	Std Oluşturma Tarihi	Std Değiştirme Tarihi	Std Erişim Tarihi	Std Giriş Tarihi
Delil1\D\Yedek\desktop\yeni\Hanefi.doc	2010-07-26 09:55:57.546875	2010-07-12 09:17:48	**2011-01-26 12:07:37.390625**	2010-07-26 09:55:57.562498
Delil1\D\Yedek\desktop\yeni\Sn.Komutanim.doc	2010-07-26 09:55:57.500000	2010-07-01 14:19:34	**2010-12-24 11:08:23.281248**	2010-07-26 09:55:57.500000
Delil1\D\toplanti.doc	2010-04-26 08:36:39.140625	2010-04-25 11:33:56	**2010-12-24 11:09:03.187500**	2010-04-26 08:36:39.140625

Tablo 3 - Erişim Zamanı Oluşturma Zamanından Sonra Olan Dosyalar

Daha önceki raporda[12] da belirtildiği üzere: "STD erişim zamanı güncellenmesi ya dosyanın üzerine fare işaretçisinin getirilmesi ile, ya tek bir kere fare ile dosyanın ikonu üzerine tıklanması ile ya da çift tıklanarak dosyanın açılması ile oluşabilmektedir". Buna ek olarak "Hanefi.doc" dosyasının oluşturma tarihi ile son erişim tarihleri arasında yaklaşık **6 ay**, "Sn.Komutanım.doc" dokümanı için yaklaşık **5 ay**, "toplantı.doc" dosyası için yaklaşık **8 ay** fark bulunmaktadır. Bunun anlamı "Hanefi.doc" dosyasının en az 6 ay, "Sn.Komutanım.doc"

[12] 24 Ağustos 2012 tarihli ODATV SORUŞTURMASI DİJİTAL ADLİ ANALİZ RAPORU

dosyasının en az 5 ay ve “toplantı.doc” dosyasının en az 8 ay silinmeden önce ilgili bilgisayarda kullanıcının erişebileceği bir konumda bulunmuş olmasıdır.

Sonuç olarak, Cevap 3’de açıklandığı üzere, Delil 1 ve 2 bilgisayarlarına, EK-1 listesindeki dosyaların yüksek ihtimalle zararlı yazılımlar ile gönderilmediği göz önünde bulundurulduğunda, **bu üç dosyanın yüksek ihtimalle kullanıcı bilgisi dâhilinde Delil 1 bilgisayarında bulunduğu** ve erişim tarihlerindeki güncellemelerden ötürü **bu dosyalar üzerinde kullanıcı tarafından bir işlem yapıldığı** değerlendirilmektedir. Aynı şekilde Cevap 8’de açıklandığı üzere, yüksek ihtimalle Delil 2 bilgisayarında değiştirilmiş olan “SY.doc” ve “prj_60.doc” dosyalarının, Delil 2 bilgisayar kullanıcısı tarafından **yüksek ihtimalle** açıldığı değerlendirilmektedir. Diğer dosyalar için ise bu tür bir yargıya varabilmek için yeterli veri mevcut değildir.

Soru 3

EK-1 de yer alan ve raporda belirtilen dosyaların anılan bilgisayarlarda 'zararlı bir yazılım tarafından gönderildiğine veya değiştirildiğine dair bir bulguya rastlanmamıştır' olgusunun yine yalın bir şekilde açıklanması? Zararlı bir yazılım ile gönderilmesi halinde nasıl bulguların oluşacağının bilgisayar kullanım düzeyinde birinin anlayacağı açıklıkta belirtilmesi? Yine raporda geçen 'Dosyanın zararlı bir yazılım tarafından kesin olarak gönderilmemiş veya değiştirilmemiş olduğu anlamına gelmemektedir' ibaresinin yalın bir şekilde açıklanması? Zararlı yazılımla gönderilip gönderilmeme olasılığının neden ve sonuçları ile tartışılarak açıklanması'? Kesin belirleme yapılamamasının nedenlerinin açıklanması? Zararlı yazılımla gönderilip gönderilmeme konusunda oran verilip verilemeyeceği? Zararlı yazılımla bu dosyaların gönderildiğinin belirlenmesi halinde, kimler tarafından, nasıl ve ne şekilde gönderildiğinin tespitinin istenmesi ve açıklanması? Zararlı yazılımla dosyanın gönderilmiş olduğunun tespiti halinde, zararlı yazılımla dosya göndericisinin bunun ortaya çıkmaması için almış olduğu tedbirlerin bulunup bulunmadığının açıklanması?

Cevap 3

Bir dosyanın herhangi bir zararlı yazılım yoluyla uzaktan gönderildiğini tespit edilebilmek için bahse konu zararlı yazılımın özellikleri, çalıştığı zaman bırakacağı izler, dosyanın üst verileri üzerindeki etkileri, bunların normal kullanıcı davranışları ile uyumu gibi faktörler gözden geçirilmiştir. Bu inceleme sonucunda ilgili belgelerin zararlı yazılımlar vasıtasıyla gönderilip gönderilmediği hususuyla alakalı tespit edilen bulgular şu şekildedir:

- İlgili bilgisayarlara hedefli olarak uzaktan yönetim özelliği bulunan zararlı yazılımlar gönderilmiştir.
- Bu zararlı yazılımların ilgili bilgisayarlarda çalışmış olduğu tespit edilmiştir.
- EK-3 tablolarında, davaya konu dosyalarla alakalı, delil bilgisayarlarında tespit edilen üst veri türleri gösterilmektedir. Bu tablolardan da anlaşılacağı üzere, dosyaların çoğunun dosya sistemi zaman üst verilerine ulaşılmıştır.
- Erişilen bu dosya sistemi tarih üst verilerine göre, **dosyaların oluşturulma zamanları**, ilgili **zararlı yazılımların gönderilme zamanlarından <u>öncedir</u>**.
- EK-1 listesindeki dosyaların, bahse konu olan zararlı yazılımlar ile gönderilmiş olabilmesi için, bu tarih üst verilerinin değiştirilmiş ve önceki bir tarihe alınmış olması gerekmektedir. Bu dosya sistemi tarih üst verilerinin değiştirildiğine dair herhangi bir ize rastlanmamıştır. Herhangi bir iz bırakmadan dosya sistemi tarih üst verilerinde bir değişiklik yapılabilme olasılığı **çok düşüktür**.

Sonuç olarak yukarıdaki bulgular doğrultusunda, Delil 1 ve Delil 2 bilgisayarlarında EK-1 listesinde bulunan dokümanların yüksek ihtimalle bahse konu olan zararlı yazılımlarla bu bilgisayarlara gönderilmediği değerlendirilmektedir.

Delil 3 bilgisayarındaki durum ise şu şekildedir:

- Bahse konu olan 4 dosyanın **yüksek ihtimalle** zaman üst verileri değiştirilmeye çalışılmıştır. Bu konu ilk raporda Cevap 5 başlığı altında ilgili dosyalar için ayrıntılı olarak açıklanmıştır.
- Bahse konu olan zararlı yazılımlar, bu dosyaların değiştirilmeye çalışıldığı tarihten önce bilgisayar kullanıcısına gönderilmiştir ve ilgili tarihte çalışır durumda olma ihtimali mevcuttur.
- Cevap 5'te açıklandığı üzere, Delil 3 bilgisayarında zaman üst veri değişikliğini yapabilme yetkinliğine sahip bir bilgisayar kullanıcısı bulunmaktadır.
- İlgili dosyaların zararlı yazılımlar vasıtasıyla geldiği veya gelmediği hakkında bir bulguya rastlanmamıştır.

Sonuç olarak, Delil 3 bilgisayarında bahse konu olan dosyaların zararlı yazılımlar tarafından **gönderilmiş olması** ve daha sonra yine zararlı yazılımlar ile ilgili zaman değişikliğinin **yapılmış olması ihtimali mevcuttur**. Aynı şekilde bu dosyaların zararlı yazılımlar tarafından **gönderilmemiş olması** ve bilgili bilgisayar kullanıcısı tarafından ilgili zaman değişikliklerinin **yapılmış olması ihtimali de** mevcuttur. Bu konuda daha net bir sonuca varabilmek için kullanılabilecek herhangi bir veriye ulaşılamamıştır.

Soru 4

Her üç bilgisayardaki Güvenlik önlemlerinin, uzaktan dosya gönderme özelliğine sahip zararlı yazılımların çalışmasını engelleyip engellemeyeceğinin ayrıntılı olarak açıklanması? Zararlı yazılım ile oluşturulmuş dosyaların bilgisayarlarda mevcut güvenlik önlenmeleri ile tespit edilip edilemeyeceği, edilebiliniyor ise zararlı yazılım ile oluşturulan dosyaların silinip silinemeyeceğinin araştırılarak açıklanması?

Cevap 4

E-posta yoluyla zararlı yazılım gönderilmesinde, zararlı yazılımın göndericiden alıcıya ulaşmasına kadar geçen süredeki tespit ve engellenmesinde sırasıyla; gönderen e-posta hizmet sağlayıcı veya sunucusu, alıcı e-posta hizmet sağlayıcı veya sunucusu, alıcı tarafından kullanılan e-posta yönetim aracı ve alıcının bilgisayarı üzerinde bulunan güvenlik mekanizmaları rol oynamaktadır. Bu güvenlik mekanizmalarını atlatarak çalıştırılan uzaktan dosya gönderme özelliğine sahip bir zararlı yazılımın gönderdiği, resim, ofis dosyası, vb. gibi içerisinde herhangi bir zararlı kod parçası içermeyen dosyalar, bilgisayar üzerindeki antivirüs yazılımı tarafından tespit edilemez ve engellenemezler. Antivirüs yazılımının tespit edip, engellemesi ancak uzaktan gönderilen dosyalar içerisinde **antivirüs yazılımı tarafından tanınan** zararlı kodların olması durumunda mümkün olabilir. Bu sebeple herhangi bir zararlı yazılım parçası içermeyen EK-1 listesinde belirtilen dosyaların, anti-virüs yazılımları ile tespit edilmesi veya silinmesi mümkün değildir.

Delil bilgisayarları üzerinde bulunan güvenlik önlemleri ile e-posta yönetim aracı üzerindeki güvenlik önlemleri ve uyarılar incelenmiştir. Elde edilen bulgular her delil için ayrı ayrı olarak takip eden bölümlerde ele alınmıştır.

Delil 1 güvenlik önlemleri ve uyarılar

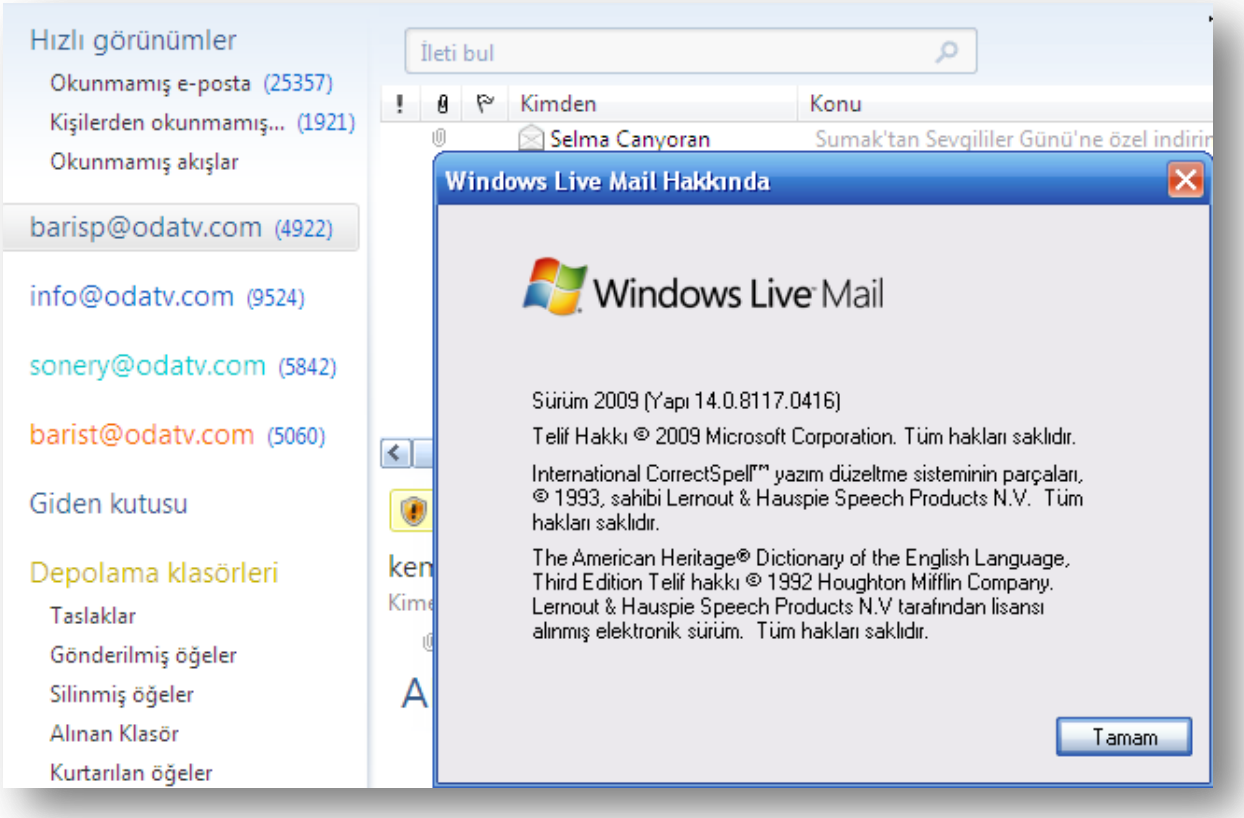
Delil 1 bilgisayarında “ESET NOD32 Antivirüs 4” isimli antivirüs uygulamasının çalıştığı ve Windows güvenlik duvarının aktif olduğu, Antivirüs programının en son 03.12.2010 tarihinde güncellendiği tespit edilmiştir.

Delil 1 bilgisayarı, alınan imaj dosyaları kullanılarak tekrar çalıştırılıp üzerinde yüklü bulunan “ESET NOD32 Antivirüs 4” isimli antivirüs uygulaması ile bu bilgisayara hedefli bir saldırı amacıyla gönderilmiş olabilecekleri düşünülerek önceki raporda ayrıntılı bir şekilde incelenen e-posta dosyaları ve eklerinde yer alan zararlı yazılımlar taratılmış, fakat bu zararlı yazılımların hiç biri antivirüs tarafından tespit edilememiştir.

E-posta yolu ile gönderilen zararlı yazılımlar ile ilgili olarak; e-posta hizmeti veren web sitesi veya e-posta yönetim aracı tarafından sağlanan güvenlik önlemleri ve oluşturulan uyarılar takip eden bölümde açıklanmıştır.

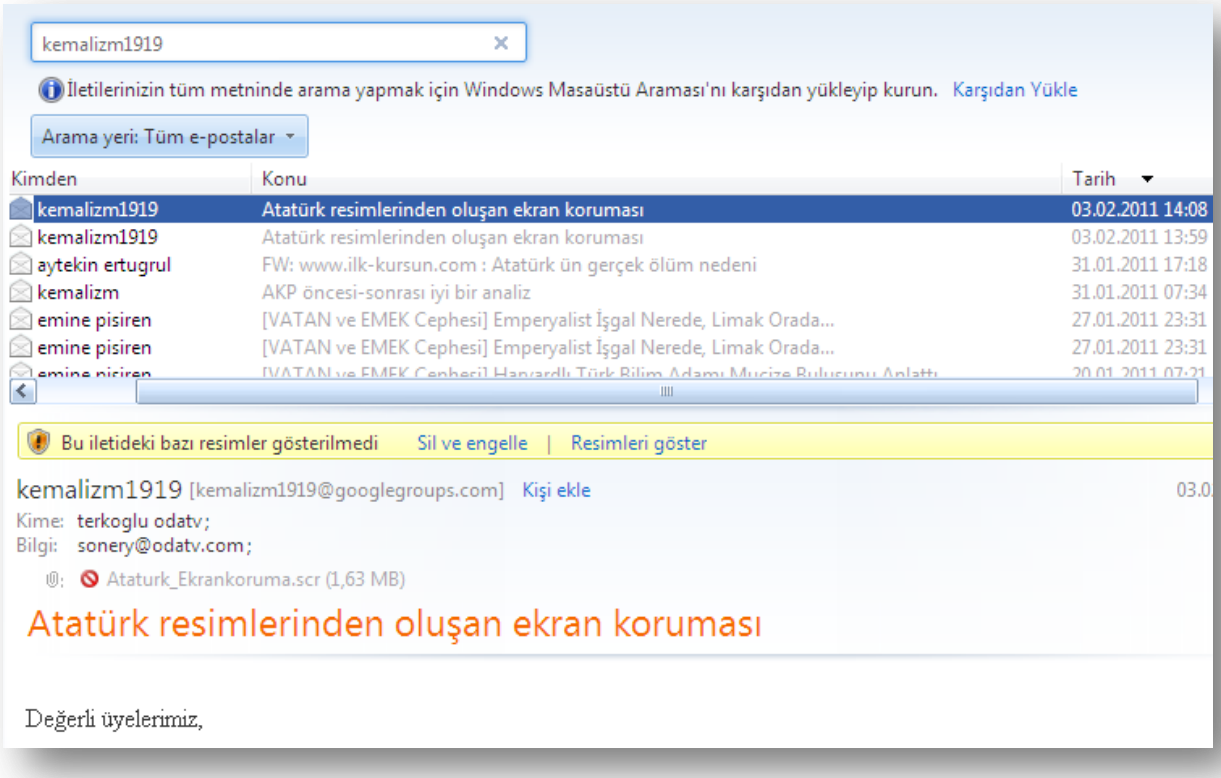
Delil 1 e-posta güvenlik önlemleri ve uyarılar

Delil 1 bilgisayarında e-posta yönetim aracı olarak Windows Live Mail kullanıldığı ve üzerinde tanımlı barisp@odatv.com, barist@odatv.com, info@odatv.com ve sonery@odatv.com e-posta hesaplarının bulunduğu tespit edilmiştir.



Şekil 7 - Delil 1 E-posta Hesapları

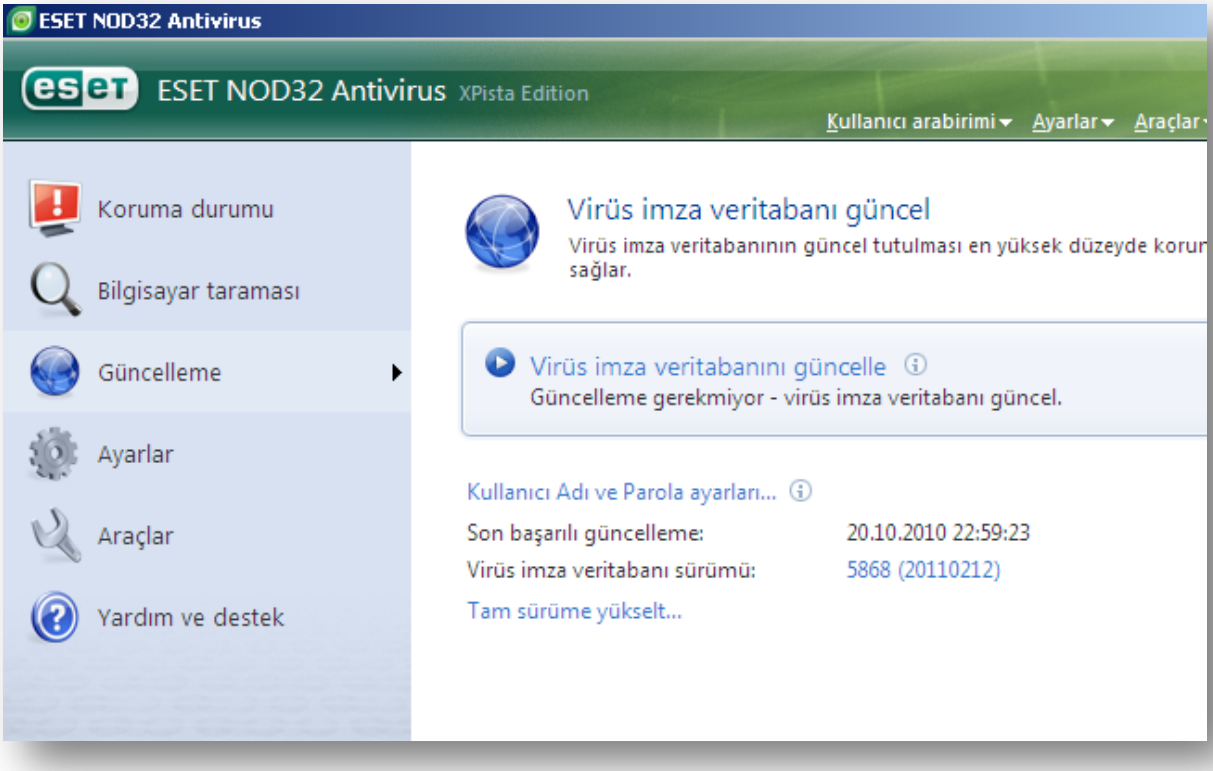
Jangomail e-posta hizmeti kullanılarak hedefli bir saldırı amacıyla gönderilmiş olabilecekleri düşünülen e-postalardan "Atatürk_Ekrankoruma.scr" zararlı dosyasını içeren 2 adet e-postadaki eklentiler, Şekil 8'de görüldüğü gibi Windows Live Mail e-posta yönetim aracı tarafından zararlı olduğu düşünülerek kullanıcıların erişimi engellenmiştir.



Şekil 8 - Delil 1 "Atatürk ekran koruması" E-postası

Delil 2 güvenlik önlemleri ve uyarılar

Delil 2 bilgisayarında "ESET NOD32 Antivirüs Xpista Edition" isimli antivirüs uygulamasının çalıştığı fakat Windows güvenlik duvarının aktif olmadığı tespit edilmiştir. Antivirüs programında otomatik güncellemenin en son 20.10.2010 tarihinde başarılı olmasına karşın kullanıcı tarafından virüs veritabanı bilgisinin elle 12.02.2011 tarihli sürümüne güncellendiği tespit edilmiştir.



Şekil 9 - Delil 2 Antivirüs Son Güncelleme Tarihi

Delil 2 bilgisayarı, alınan imaj dosyaları kullanılarak tekrar çalıştırılıp üzerinde yüklü bulunan "ESET NOD32 Antivirüs Xpista Edition" isimli antivirüs uygulaması ile virüs taramasına tabii tutulmuştur. Tarama sonucu, Jangomail kullanılarak gönderilmiş Tablo 5'deki e-postalardan "Message18701" ve "Message18700" isimli e-postaların ekinde yer alan "Duyuru.pdf" dosyası ve bu dosyanın çalıştırılmasıyla oluşan "Dhq.dll" dosyası virüs olarak Tablo 4'de görüldüğü gibi tespit edilebilmiştir.

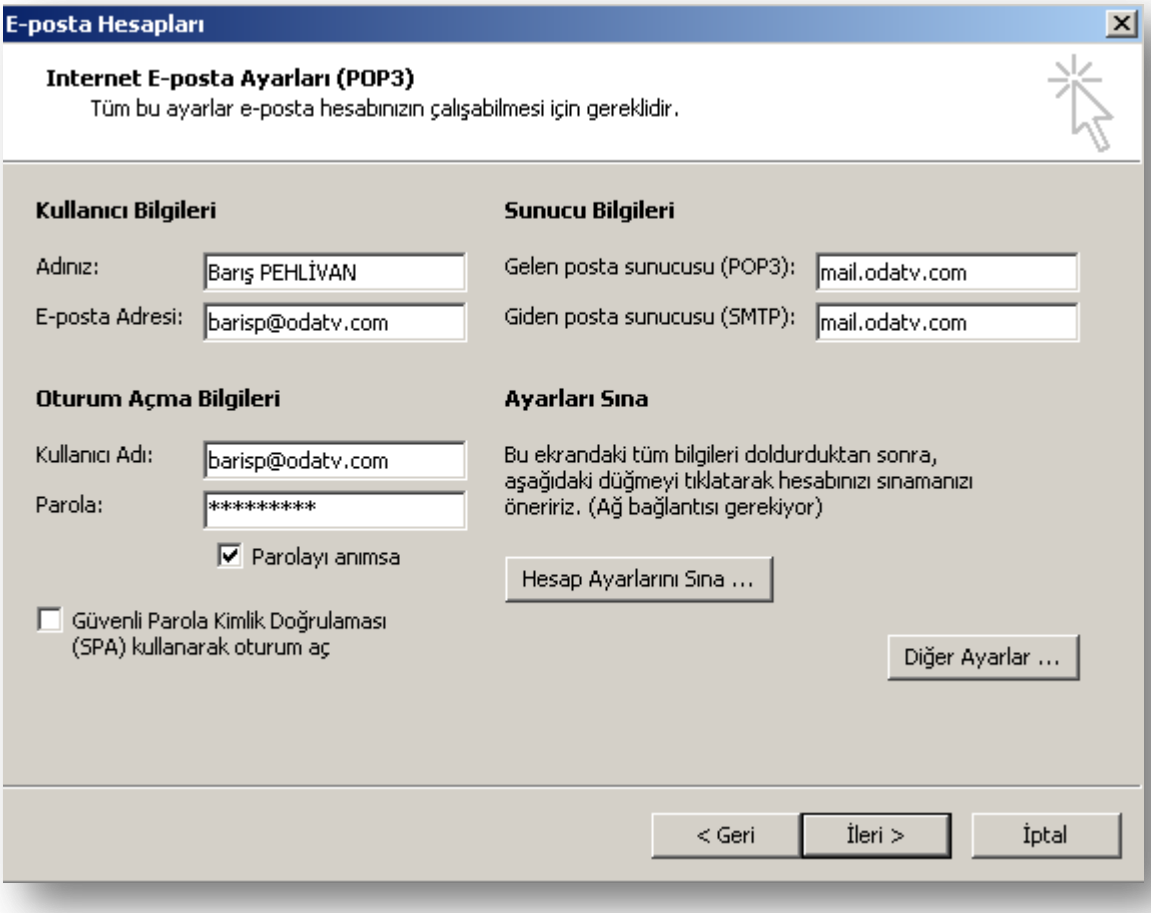
Tespit Edilen Dosya ve Yolu	Virüs Türü
D:\Documents and Settings\Barış\Local Settings\Temp\dhq.dll	Win32/TrojanDropper.Small.NLW truva atı türevi
D:\Documents and Settings\Barış\Local Settings\Temporary Internet Files\OLK4\Duyuru (2).pdf	JS/Exploit.Pdfka.OQB truva atı
D:\Documents and Settings\Barış\Local Settings\Temporary Internet Files\OLK4\Duyuru (3).pdf	JS/Exploit.Pdfka.OQB truva atı

D:\Documents and Settings\Barış\Local Settings\Temporary Internet Files\OLK4\Duyuru (4).pdf	JS/Exploit.Pdfka.OQB truva atı
D:\Documents and Settings\Barış\Local Settings\Temporary Internet Files\OLK4\Duyuru.pdf	JS/Exploit.Pdfka.OQB truva atı
D:\Documents and Settings\Barış\Local Settings\Temp\dhq.dll	Win32/TrojanDropper.Small.NLW truva atı türevi

Tablo 4 - Delil 2 Eset Nod32 Taramasında Tespit Edilen "Jangomail" Eklentileri

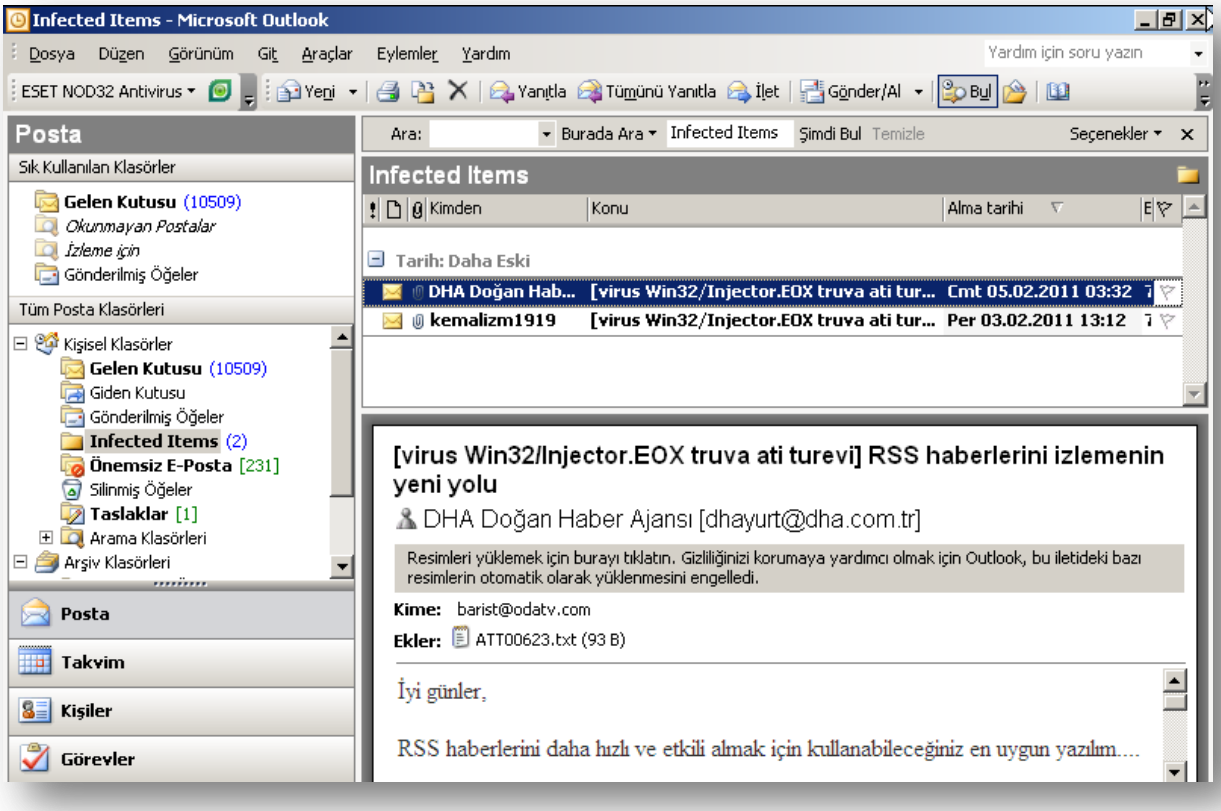
Delil 2 e-posta güvenlik önlemleri ve uyarılar

Delil 2 bilgisayarında bulunan Barış kullanıcısının, e-posta yönetim aracı olarak Microsoft Outlook 2003 kullandığı ve tanımlı e-posta hesabının Barış Pehlivan adıyla kayıtlı barisp@odatv.com hesabı olduğu tespit edilmiştir.



Şekil 10 - Delil 2 Barış Pehlivan Outlook Hesabı

Outlook e-posta yönetim aracı içinde yer alan ve zararlı yazılım içerdiği tespit edilen e-postaların, ekinde yer alan zararlı dosyaların silinerek tutulduğu "Infected Items" klasörü kontrol edilmiştir. Yapılan ilk incelemede "Infected Items" klasöründe 2 e-postanın tutulduğu ve bu e-postaların içerdiği virüs türünün adının konu bölümünde yer aldığı tespit edilerek eklentilerinin silindiği görülmüştür.

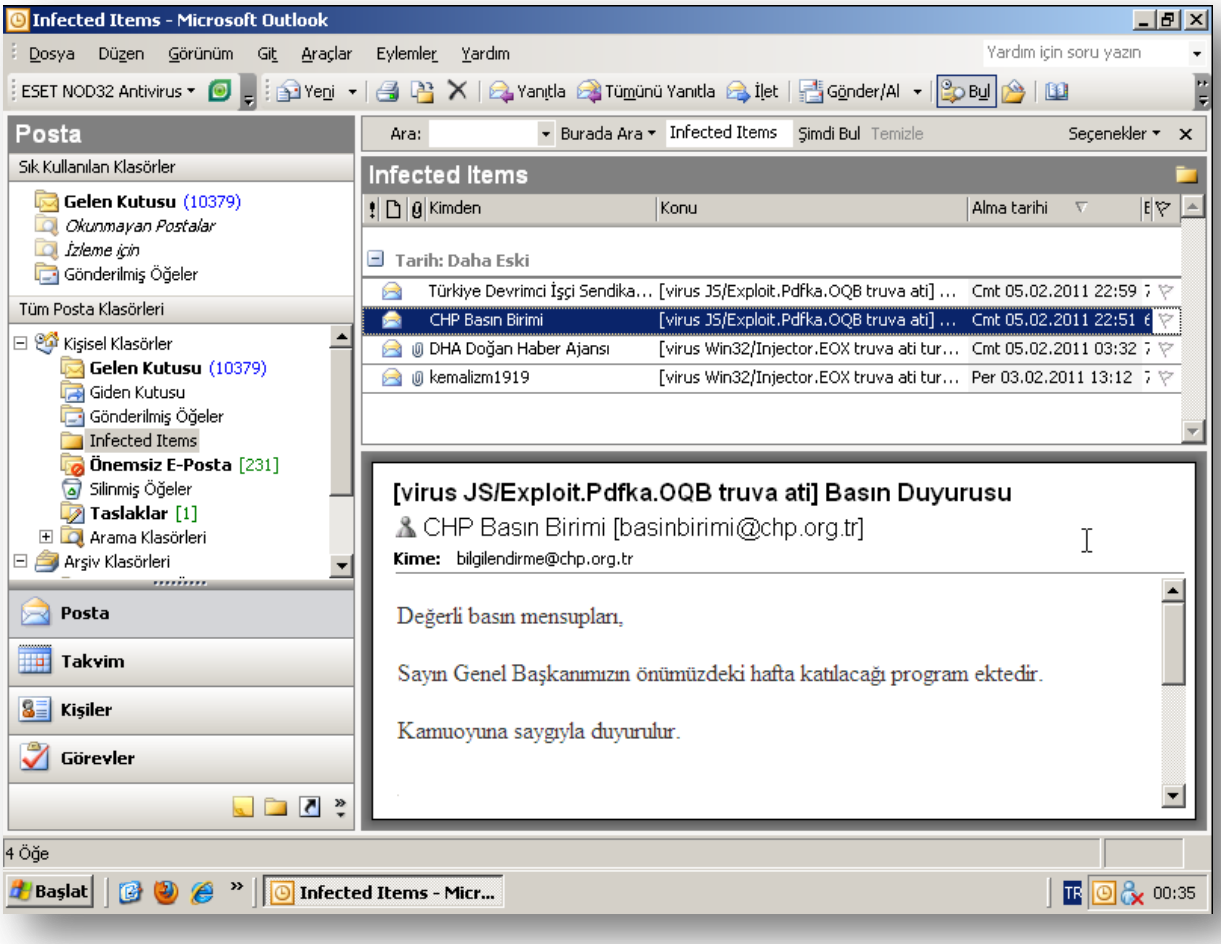


Şekil 11 - Delil 2 "Infected Items" Klasörü İlk Durum

Bunlara ek olarak, gelen kutusundaki e-postalar kontrol edilirken, seçilir seçilmez eklenti olarak virüs içerdiği tespit edilip "infected items" klasörüne taşınan 2 e-posta daha tespit edilmiştir. Son durumda Şekil 12'te görüldüğü gibi "infected items" klasöründe, zararlı yazılım içerdiği tespit edilip, eklenti olan zararlı dosyaların çıkartılmış olduğu 4 tane e-posta bulunduğu görülmüştür.

Tablo 4'deki dosya yolunda görülen "OLK4" klasörünün Outlook e-posta yönetim aracı üzerinden açılan dosyaların geçici olarak tutulduğu bir klasör olması sebebiyle, "Duyuru.pdf" dosyasının Outlook üzerinde bulunduğu e-postaların ekinden çalıştırılarak antivirüs yazılımına yakalanmadan açıldığı, o tarihte imzası antivirüs veritabanında bulunmadığı için,

fakat 12.02.2012 tarihinde elle yapılan antivirüs veritabanı güncellemesi sonrasında bu dosyadaki zararlı yazılımın antivirüs tarafından tespit edilir hale gelmesi sebebiyle bu dosyanın ekinde gönderildiği e-postaların tekrar okunması sırasında eklenti dosyasının silinip, e-postaların "infected items" klasörüne taşındığı düşünülmektedir.



Şekil 12 - Delil 2 "Infected İtems" Klasörü Son Durum

Yapılan incelemede barisp@odatv.com e-posta hesabında bulunan, Jangomail e-posta hizmeti kullanılarak ve yanıltıcı şekilde sahip olunmayan bir e-posta adresinden geliyor izlenimi verilerek gönderildiğinden dolayı, hedefli bir saldırı amacıyla gönderilmiş olabilecekleri düşünülen e-postalar Tablo 5'de listelenmiştir.

E-posta Adı	E-posta Yeri	Gönderen	Alıcı	Geldiği Tarih		E-posta Konusu	Jangomail Dönüş Adresi
Message00	Infected	kemalizm19	barisp@oda	3	Şubat	Atatürk	winnerr5@j

001	Items	19@yahoo.com	tv.com	2011 13:11	resimlerinden oluşan ekran koruması	angomail.com
Message00002	Infected Items	dhayurt@dha.com.tr	barisp@odatv.com	5 Şubat 2011 3:32	RSS haberlerini izlemenin yeni yolu	winnerr5@jangomail.com
Message18700	Gelen Kutusu[13]	basinbirimi@chp.org.tr	barisp@odatv.com	5 Şubat 2011 22:51	Basın Duyurusu	winnerr51@jangomail.com
Message18701	Gelen Kutusu[1]	disk@disk.org.tr	barisp@odatv.com	5 Şubat 2011 22:58	Torba yasa'ya karşı dört koldan Ankara yürüyüşü ve programı	winnerr51@jangomail.com

Tablo 5 - Delil 2'ye "Jangomail" Kullanılarak Gönderilen E-postalar

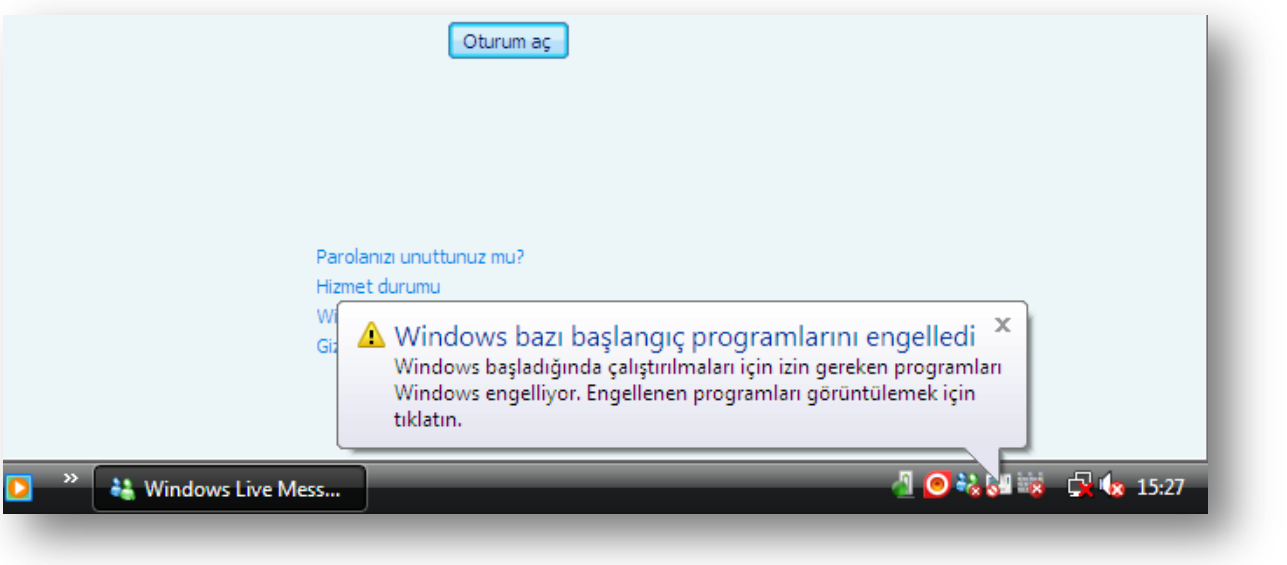
Outlook e-posta yönetim aracı üzerinde, hedefli saldırı olarak gönderilmiş olabileceği düşünülen Tablo 5'deki e-postaların tümünün, Şekil 12'te görülebileceği gibi zararlı yazılım içerdiği tespit edilip, eklentileri çıkartılarak "infected items" klasörüne gönderildiği tespit edilmiştir.

Delil 3 güvenlik önlemleri ve uyarılar

Delil 3 bilgisayarında "ESET Smart Security 4" isimli antivirüs uygulamasının çalıştığı, Windows güvenlik duvarının aktif olduğu, kötücül yazılımlara karşı "Malwarebytes Anti-Malware" uygulamasının çalıştığı, Ayrıca Windows işletim sistemi içerisinde gelen "Windows Defender" ve "Windows Kötü amaçlı yazılımları temizleme aracı" uygulamalarının aktif olarak çalıştığı tespit edilmiştir. Antivirüs programının en son 28.08.2010 tarihinde, Anti-Malware uygulamasının en son 30.12.2009 tarihinde, Windows Defender Uygulamasının en son 01.03.2011 tarihinde ve Windows kötü amaçlı yazılımları temizleme aracı uygulamasının en son 11.02.2011 tarihinde güncellendiği tespit edilmiştir.

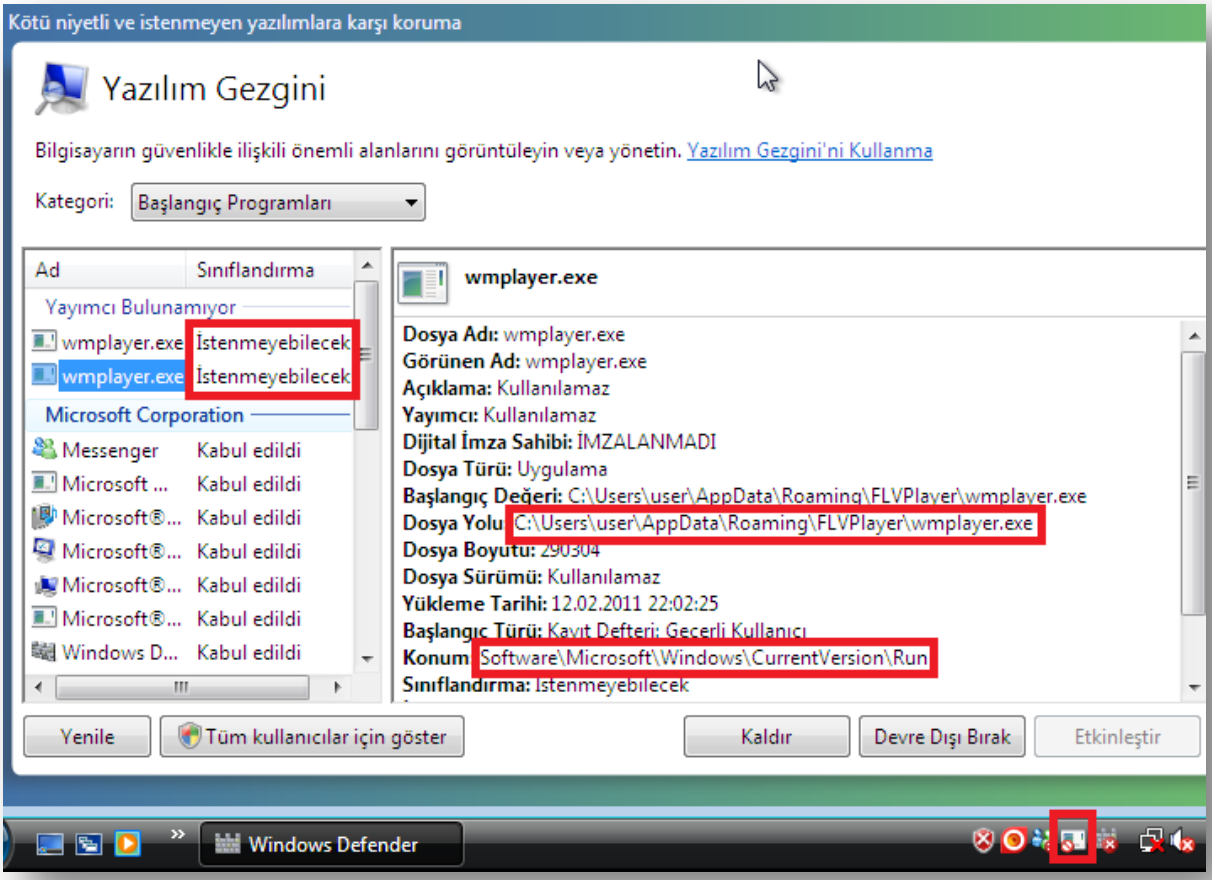
[13] Gelen kutusundaki bu e-postalarda seçilir seçilmez virüs tespit edilip "Infected Items" klasörüne taşınmıştır.

Delil 3 bilgisayarı, alınan imaj dosyaları kullanılarak tekrar çalıştırılıp üzerinde yüklü bulunan güvenlik uygulamaları tarafından oluşturulan uyarılar incelenmiş ve ekran görüntüleri gösterilmiştir. Delil 3 bilgisayarı ilk açıldığında, görev çubuğunda sistem ile ilgili uyarı ve simgelerin bulunduğu bölümde uyarıların bulunduğu ve kullanıcıya açıklama balonları aracılığıyla bu uyarılar hakkında bildirimde bulunulduğu görülmüştür. Açılış sonrası çıkan ilk uyarı, Şekil 13'da görüldüğü gibi işletim sistemi tarafından bazı başlangıç programlarının engellendiği uyarısıdır.



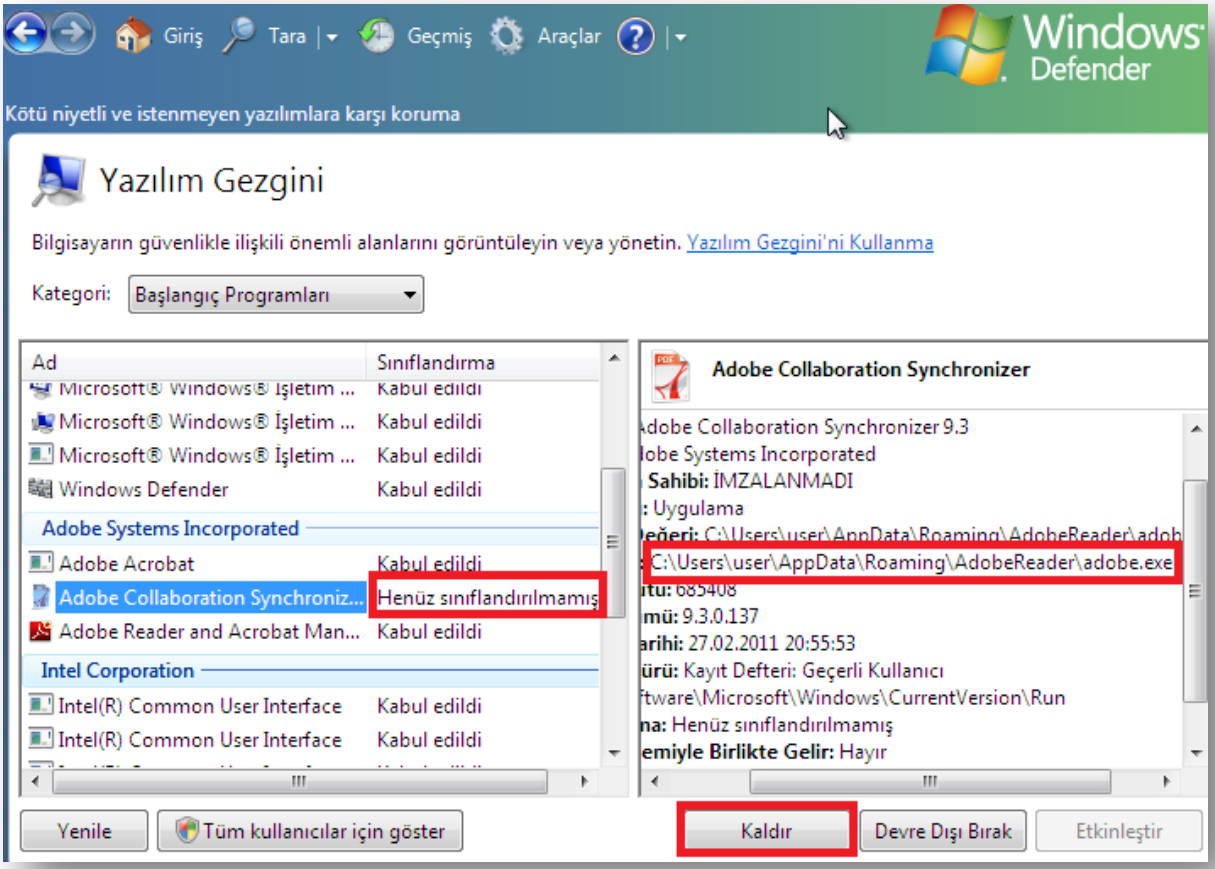
Şekil 13 - Delil 3 Başlangıç Programları Engelleme Uyarısı

Uyarı baloncuğuna tıklandığında Windows Defender uygulamasının açıldığı ve Şekil 14'de gösterildiği gibi yayımcısı bulunamayan şüpheli başlangıç programlarından birinin "wmplayer.exe" uygulamasının olduğu görülmüştür.



Şekil 14 - Delil 3 "Windows Defender"'da İstenmeyen "wmplayer.exe" Başlangıç Programı

Açılan Windows Defender uygulamasındaki başlangıç programları listesi araştırıldığında, önceki raporda başlangıç programları için oluşturulan olay kaydında da görülen "adobe.exe" zararlı programının da listede bulunduğu ve bunun sistem tarafından doğrulanamadığı görülmüştür.



Şekil 15 - Delil 3 "Windows Defender" İstenmeyen "adobe.exe" Başlangıç Programı

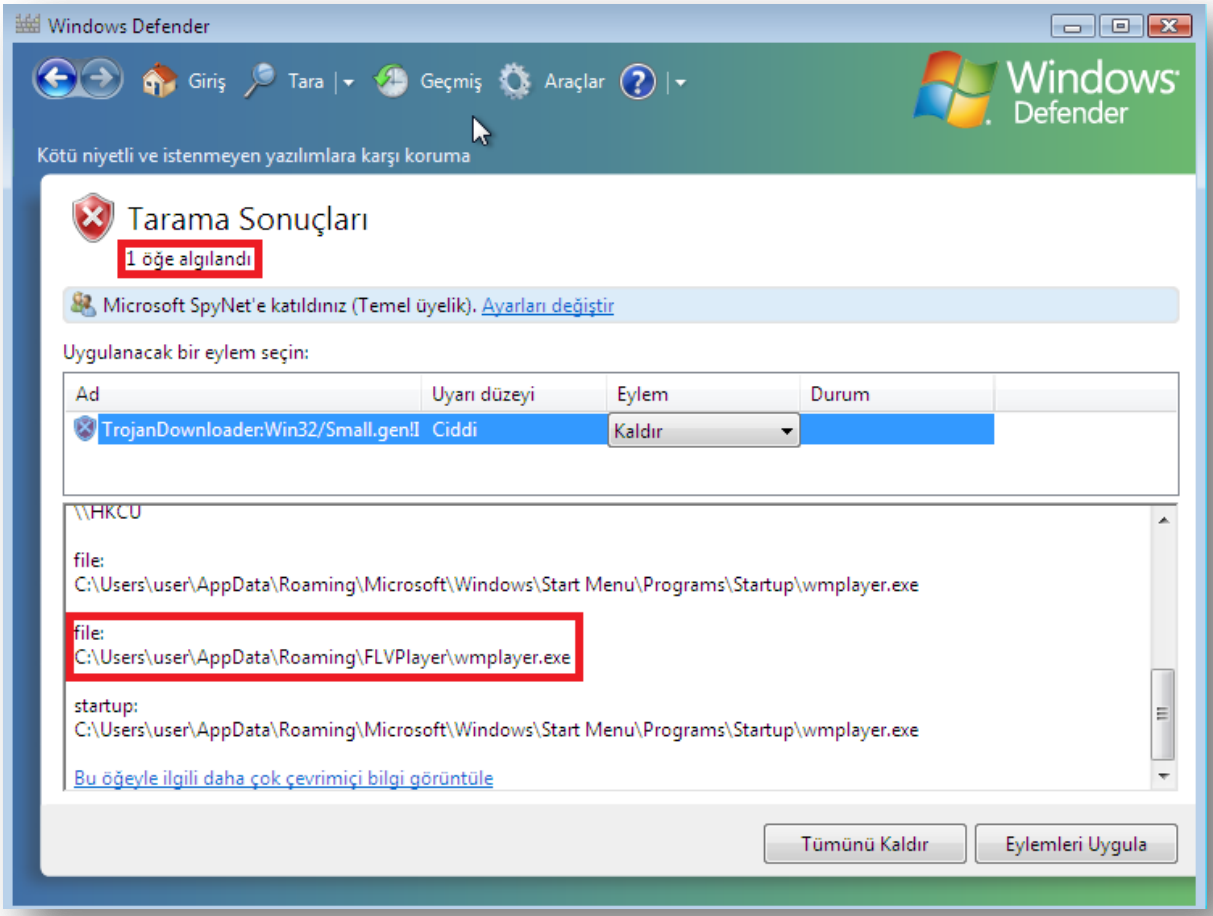
Engellenen başlangıç programlarıyla ilgili görev çubuğunda uyarı amaçlı bir simge bulunduğu ve simgeye sağ tıklanması ile çıkan menüde engellenen programların gösterilmesini veya istenirse kaldırılmalarını sağlayan seçeneklerin bulunduğu görülmüştür.

Şekil 16 - Delil 3'te Engellenen Başlangıç Programları Menüsü

Windows Defender'ın günlük otomatik antivirüs taraması yapmak üzere ayarlandığı ve son yapılan tarama sonucu zararlı yazılım tespit edilmesi sebebiyle açılış sonrası uyarı baloncuğu çıktığı görülmüştür.

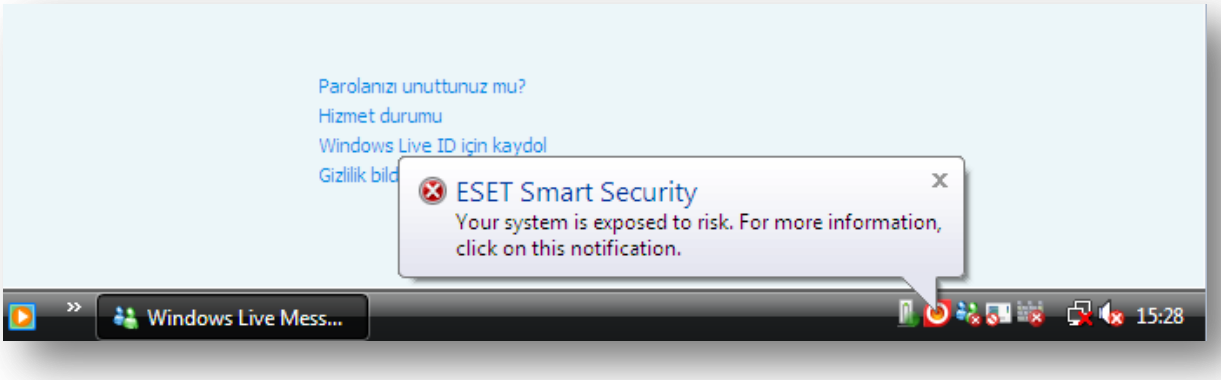
Şekil 17 - Delil 3 Windows Defender otomatik tarama uyarısı

Otomatik tarama sonucu zararlı yazılım tespit edilmesi ile ilgili uyarı baloncuğuna tıklanıp, gelen tarama sonuçları ekranında ayrıntılarının görüntülenmesi sonucu, Şekil 18'de görüldüğü gibi "wmplayer.exe" adlı zararlı yazılım tespit edilmiştir.

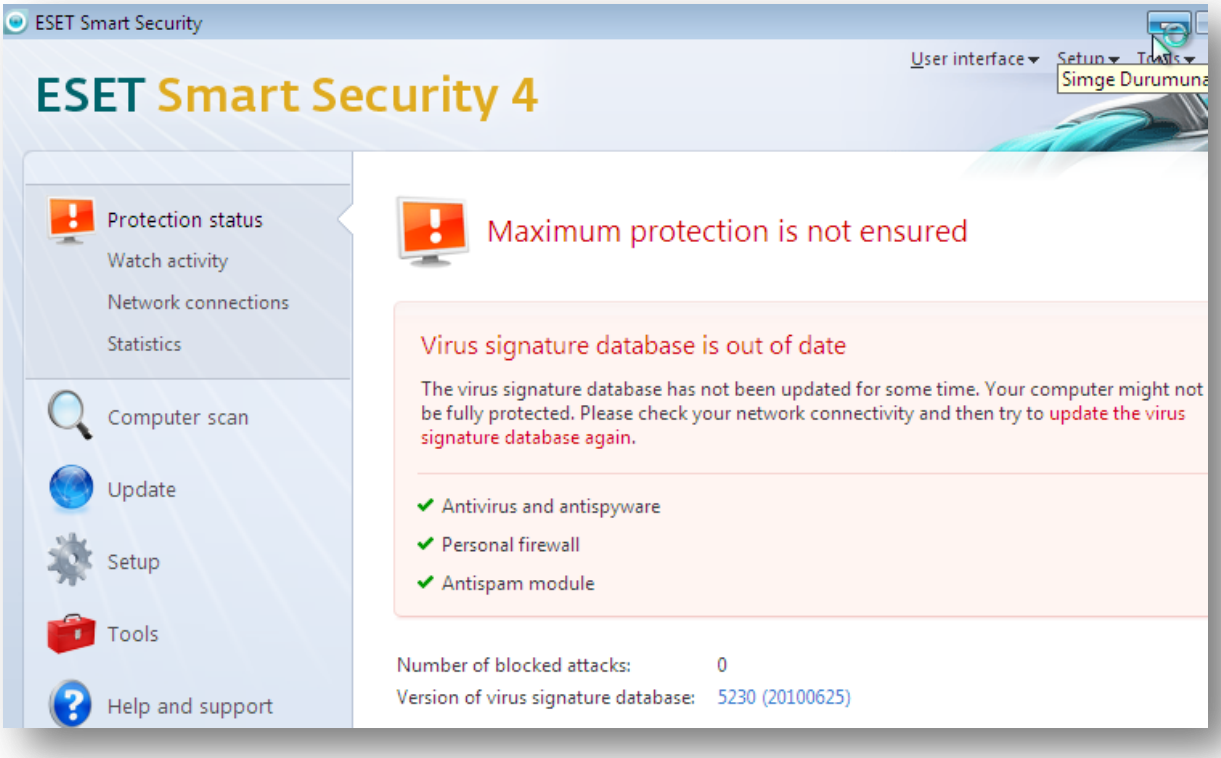


Şekil 18 - Delil 3'te "Windows Defender" Otomatik Tarama Sonucu

Ayrıca açılış sonrası Şekil 19'de görüldüğü gibi "ESET Smart Security 4" antivirüs uygulaması tarafından uyarı baloncuğu aracılığıyla sistemin risk altında bulunduğu uyarısının verildiği görülmüş, baloncuğa tıklanması sonrasında ise "ESET Smart Security 4" antivirüs uygulaması arayüzü üzerinde antivirüs veritabanının güncel olmadığı konusunda kullanıcının uyarıldığı tespit edilmiştir.



Şekil 19 - Delil 3 Eset Güvenlik Riski Uyarısı



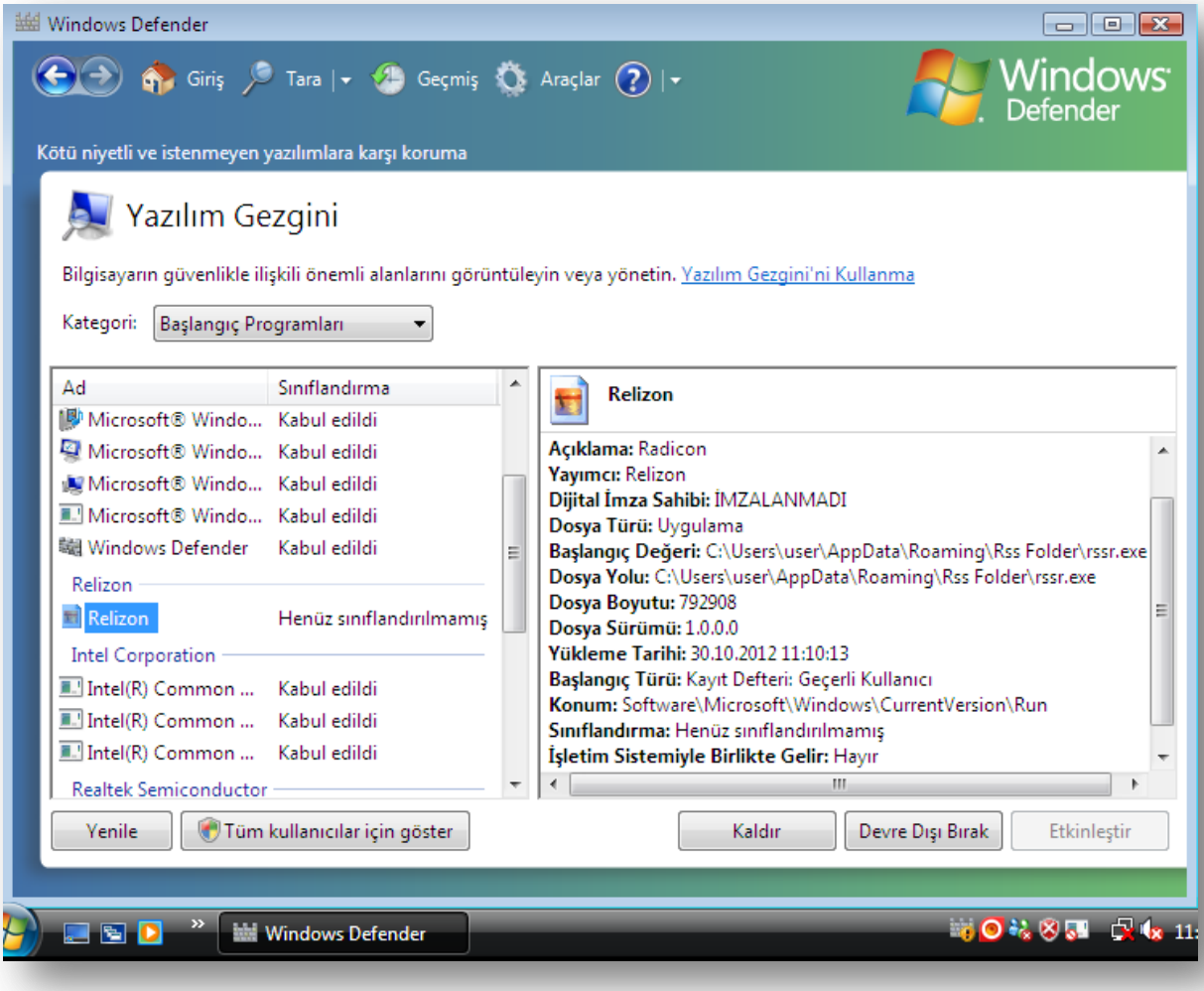
Şekil 20 - Delil 3 Eset Antivirüs Veritabanı Güncel Olmadığı Uyarısı

Delil 3 AKPkarikatürleri.zip ve Kayseri.rar çalıştırılması ile oluşan güvenlik uyarıları

Bu bölümde hedefli bir saldırı amacıyla gönderildiği iddia edilen ve önceki raporda ayrıntılı incelenen "AKPkarikatürleri.zip" ve "Kayseri.rar" sıkıştırılmış arşiv dosyaları içerisindeki

zararlı yazılımlar, alınan imaj dosyaları kullanılarak tekrar çalıştırılan Delil 3 bilgisayarında çalıştırılmış ve oluşan güvenlik uyarıları gösterilmiştir.

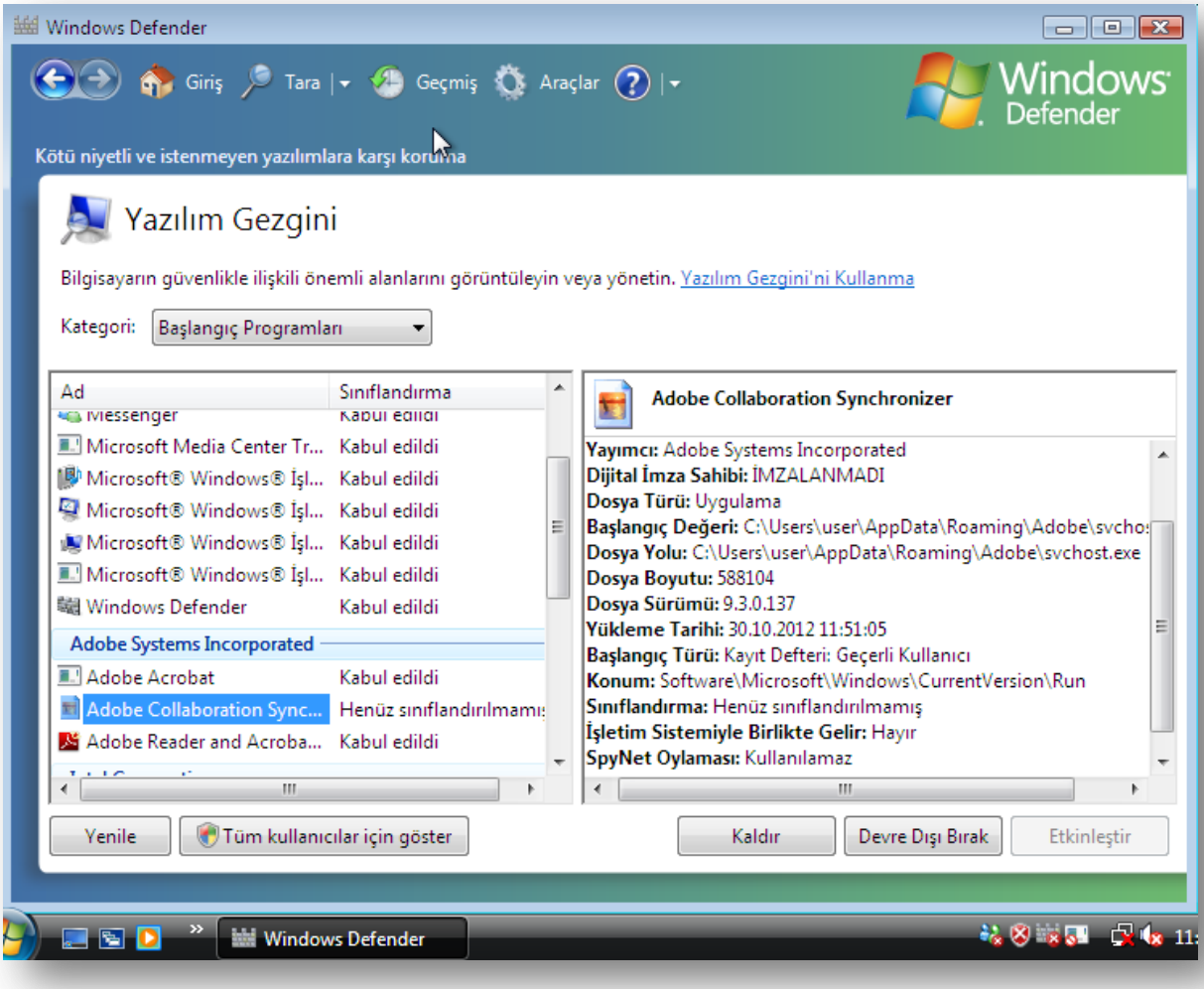
"Kayseri.rar" sıkıştırılmış arşiv dosyası içerisinde yer alan ve önceki raporda ayrıntılı analizi yapılan "kayseri2.scr" dosyasının Delil 3 bilgisayarında çalıştırılması sonucu oluşturduğu asıl virüs dosyasının başlangıç programı olarak kaydedildiği ve bu dosyanın Windows Defender uygulamasındaki başlangıç programları listesinde Şekil 21'de görüldüğü gibi sınıflandırılmamış ve imzasız olarak şüpheli bir program olarak tespit edildiği görülmüştür.



Şekil 21 - Delil 3 "kayseri2.scr" Otomatik Başlangıç Programı Uyarısı

"AKPkarikatürleri.zip" sıkıştırılmış arşiv dosyası içerisinde yer alan ve önceki raporda ayrıntılı analizi yapılan "0tayyip2it2.scr" dosyasının Delil 3 bilgisayarında çalıştırılması sonucu oluşturduğu asıl virüs dosyasının başlangıç programı olarak kaydedildiği ve bu dosyanın Windows Defender uygulamasındaki başlangıç programları listesinde Şekil 22'de görüldüğü

gibi sınıflandırılmamış ve imzalanmamış olması sebebiyle şüpheli bir program olarak tespit edildiği görülmüştür.



Şekil 22 - Delil 3 "0tayyip2it2.scr" Otomatik Başlangıç Programı Uyarısı

Çalıştırılan "Kayseri.rar" arşiv dosyası içerisindeki "kayseri2.scr" ve "AKPkarikatürleri.zip" arşiv dosyası içerisinde yer alan "0tayyip2it2.scr" virüs dosyaları ile bu dosyaların çalışması sonucu oluşturdukları asıl virüs dosyaları, imaj dosyaları kullanılarak tekrar çalıştırılan Delil 3 bilgisayarında yer alan ESET Smart Security 4 antivirüs uygulaması, antivirüs özelliğine sahip Malwarebytes Anti-Malware ve Windows Defender uygulamaları tarafından taratılmış, virüs olarak tespit edilmemişlerdir.

Genel Değerlendirme

Delil bilgisayarlarına Jangomail e-posta hizmeti kullanılarak hedefli bir saldırı amacıyla gönderilmiş olabilecekleri düşünülen ve önceki raporda ayrıntılı olarak incelenen e-posta

eklerindeki zararlı yazılımların, delil bilgisayarlarında yer alan güvenlik mekanizmaları tarafından tespit edilip edilemediği ve güvenlik uyarısı oluşturulup oluşturulmadığı her bir delil bilgisayarı için ayrı tablolarda aşağıdaki gibi özetlenerek listelenmiştir.

Delil 1 için;

E-posta Adı	Gözüken Gönderici	Alıcı	Geldiği Tarih	Eklenti	AV Tespiti	Güvenlik Uyarısı
187E16C5-000056A4.eml	kemalizm1919@yahoo.com	barisp@odatv.com, sonery@hurriyet.com.tr	31 Ocak 2011 7:34	AKP_oncesi-sonrasi.pdf	Hayır	Hayır
5A9C4EFE-0000E9F3.eml	kemalizm1919@yahoo.com	info@odatv.com	3 Şubat 2011 13:59	Ataturk_Ekrankoruma.scr	Hayır	Evet
66B46747-000042CF.eml	kemalizm1919@yahoo.com	barist@odatv.com, sonery@odatv.com	3 Şubat 2011 14:08	Ataturk_Ekrankoruma.scr	Hayır	Evet
37EA0857-00004396.eml	dhayurt@dha.com.tr	barisp@odatv.com	5 Şubat 2011 4:32	RssReader 2.1.zip	Hayır	Hayır
1609770D-000058F0.eml	dhayurt@dha.com.tr	barist@odatv.com	5 Şubat 2011 4:32	RssReader 2.1.zip	Hayır	Hayır
56825A91-00004377.eml	basinbirimi@chp.org.tr	barist@odatv.com	5 Şubat 2011 23:51	Duyuru.pdf	Hayır	Hayır
56AF62F7-000058C2.eml	basinbirimi@chp.org.tr	barisp@odatv.com	5 Şubat 2011 23:51	Duyuru.pdf	Hayır	Hayır
29C64C6C-000058C1.eml	disk@disk.org.tr	barisp@odatv.com	5 Şubat 2011 23:58	Duyuru.pdf	Hayır	Hayır

72010E0A-00004376.eml	disk@disk.org.tr	barist@odatv.com	5 Şubat 2011 23:59	Duyuru.pdf	Hayır	Hayır
21974EA4-00004375.eml	info@leman.com.tr	barist@odatv.com	6 Şubat 2011 0:35	AKPkarikaturleri.zip	Hayır	Hayır

Tablo 6 -Delil 3 "jangomail" E-posta Ekleri Antivirüs Tespit ve Güvenlik Uyarıları

Delil 2 için;

E-posta Adı	Gözüken Gönderici	Alıcı	Geldiği Tarih	E-posta Konusu	AV tespiti	Uyarı
Message00001	kemalizm1919@yahoo.com	barisp@odatv.com	3 Şubat 2011 13:11	Atatürk resimlerinden oluşan ekran koruması	Evet	Evet
Message00002	dhayurt@dha.com.tr	barisp@odatv.com	5 Şubat 2011 3:32	RSS haberlerini izlemenin yeni yolu	Evet	Evet
Message18700	basinbirimi@chp.org.tr	barisp@odatv.com	5 Şubat 2011 22:51	Basın Duyurusu	Evet[14]	Evet
Message18701	disk@disk.org.tr	barisp@odatv.com	5 Şubat 2011 22:58	Torba yasa'ya karşı dört koldan Ankara yürüyüşü ve programı	Evet[14]	Evet

Tablo 7 - Delil 2 "jangomail" E-posta Ekleri Antivirüs Tespit ve Güvenlik Uyarıları

Delil 3 için;

Gözüken Gönderici	Alıcı	Konu	Geldiği Tarih	Eklenti	AV Tespiti	Güvenlik Uyarısı
info@leman.com.tr	iletisim1@leman.com.tr	AKP Karikatürleri	5 Şubat 2011 23:33	AKPkarikaturleri.zip	Hayır	Evet
chptbmm@gmail.com	muyesserugur@mynet.com	3. Kayseri Dosyası!!	24.01.2011 20:58	Kayseri.rar	Hayır	Evet

Tablo 8 - Delil 3 "jangomail" E-posta Ekleri Antivirüs Tespit ve Güvenlik Uyarıları

[14] 12.02.2011 tarihinde yapılan güncelleme sonrası tespit edilmeye başlandığı düşünülmektedir

Sonuç olarak, zararlı yazılımların gönderildiği tarihte, Delil bilgisayarlarında o zamanki güvenlik ürünleri tarafından tespit edilebilmeleri ve engellenmeleri mümkün olmamıştır.

Soru 5

Raporda Delil-3 olarak belirtilen bilgisayarla ilgili olarak "Bu imajda yapılan incelemelerde, ilgili bilgisayarda İlim isimli yetkili bir kullanıcının da işlem yaptığı tespit edilmiştir. ilimugur@gmail.com e-posta adresiyle işlem yapan bu kullanıcının, bilgisayarlar ve zararlı yazılımlar konusunda bilgi sahibi olduğu düşünülmektedir. Aynı kullanıcının bu imajda bir takım zararlı yazılımlar oluşturduğu tespit edilmiştir. " konusunun açıklanması? Bu kullanıcının oluşturmuş olduğu zararlı yazılımların imkân ve kabiliyetlerinin ne olduğunun açıklanması? Bu kullanıcı tarafından oluşturulduğu belirtilen zararlı yazılımların, EK-1 listesinde olan dosyalar ile bir ilgisinin bulunup bulunmadığının araştırılarak açıklanması?

Cevap 5

Raporda Delil-3 olarak isimlendirilen Müyesser Yıldız'a ait S17HJ90Q816726 seri nolu imajda, bilgisayar teknolojisine hâkim olan yetkin bir kullanıcının işlem yaptığı tespit edilmiştir.

Bu kullanıcının kimliğine yönelik tespit edilen veriler arasında; ilimugur@gmail.com e-posta adresi, **ilimtherummer** skype mesajlaşma programı hesap adı ve **ilimugur** Windows Live anlık mesajlaşma hesabı görülmektedir. Aynı kullanıcının birçok defa ODTÜ üniversitesi bilgisayar mühendisliği bölümü ile alakalı olan http://www.ceng.metu.edu.tr/ ve https://online.metu.edu.tr/ web adreslerine giriş yaptığı tespit edilmiştir.

İlgili imajda, bilgisayar programcılığı ile ilgili çeşitli elektronik kitaplara ve notlara rastlanmıştır. "CProgramming.pdf", "C & C++ Programming Style Guidelines.pdf" ve "Expert C Programming: Deep C Secrets" örnek olarak verilebilir.

İlim isimli kullanıcının internet geçmişi incelendiğinde bilgisayar programcılığı ile ilişkin aşağıdaki bulgular elde edilmiştir.

Tarih	Saat	Kaynak	Bağlantı	Açıklama
1/11/2011	12:17:29	Firefox 3 history	URL: https://mail.google.com/mail/?shva=1#inbox/12d748fa4d20e3e0	Gmail - **Hacker Cup Results** - ilimugur@gmail.com
1/11/2011	11:52:46	Firefox 3 history	URL: https://mail.google.com/mail/?shva=1#inbox/12d51266d62d8ae3	Gmail - **ACM ICPC Kampı Taahhüt ve Bilgi Formu** - ilimugur@gmail.com

Tablo 9 - Delil 3 İnternet Geçmişi Kayıtları

Hacker Cup, Facebook'un düzenlediği ve bilgisayar uygulamalarının açıklıklarını tespit ve istismar etmeye yönelik yarışmaların yapıldığı bir organizasyondur[15]. ACM ICPC ise, en eski ve bilinen programcılık yarışma organizasyonlarından biridir.[16]

İlgili imajda tespit edilen;

- Çeşitli bilgisayar programlarına ait kaynak kodlar ve bilgisayar programcılığı eğitim kitapları,
- Kullanılan Vista işletim sisteminin *timerstop.sys* programı ile aktivasyonunun devre dışı bırakılması ve lisanssız kullanılabiliyor olması,
- İmajda bulunan anti-virüs programının offline (çevrimdışı) güncellenecek şekilde kurulmuş olması (Tablo 10) gibi durumlar bilgisayar kullanıcısının teknik bilgi seviyesinin yüksek olduğunu göstermektedir.

Tarih	Saat	Kaynak		Bağlantı	Açıklama
8/28/2010	16:03:24	Firefox history	3	URL: http://hotfile.com/dl/53297021/beb0b5c/ESET_Smart_Security__NOD32_Offline_Update_www.mayonez.net_Deleserna_.rar.html	http://hotfile.com/dl/53297021/beb0b5c/ESET_Smart_Security__NOD32_Offline_Update_www.mayonez.net_Deleserna_.rar.html (Hotfile.com: One click file hosting) [count: 1] Host: hotfile.com (URL not typed directly) type: LINK
8/28/2010	16:00:56	Firefox history	3	URL: file:///C:/Users/user/Desktop/ESET**%20Smart%20Security%20%26%20NOD32%20Offline%20Update_www.mayonez.net_Deleserna_.rar**	file:///C:/Users/user/Desktop/ESET%20Smart%20Security%20%26%20NOD32%20Offline%20Update_www.mayonez.net_Deleserna_.rar (file:///C:/Users/user/Desktop/ESET%20Smart%20Security%20%26%20NOD32%20Offline%20Update_www.mayonez.net_Deleserna_.rar) [count: 1] Host: (URL not typed directly) type: LINK
8/28/2010	16:00:46	Firefox history	3	URL: http://s207.hotfile.com/get/5e9cecdfc70a444ccb5603ccb7fc7acfbdde00f9/4c790876/0/10daec9ae5d06/32d3f7d/ESET	http://s207.hotfile.com/get/5e9cecdfc70a444ccb5603ccb7fc7acfbdde00f9/4c790876/0/11110daec9ae5d06/32d3f7d/ESET

[15] www.facebook.com/hackercup
[16] http://icpc.amrita.ac.in/2012/

				1110daec9ae5d06/32d3f7d/ESET%20Smart%20Security%20%26%20NOD32%20Offline%20Update_www.mayonez.net_Deleserna_.rar	%20Smart%20Security%20%26%20NOD32%20Offline%20Update_www.mayonez.net_Deleserna_.rar (http://s207.hotfile.com/get/5e9cecdfc70a444ccb5603ccb7fc7acfbdde00f9/4c790876/0/11110daec9ae5d06/32d3f7d/ESET%20Smart%20Security%20%26%20NOD32%20Offline%20Update_www.mayonez.net_Deleserna_.rar) [count: 1] Host: s207.hotfile.com (URL not typed directly) type: LINK
8/28/2010	15:56:24	Firefox history	3	URL: http://digg.com/news/technology/**How_to_Manually_Update_Eset_NOD32_Offline**	http://digg.com/news/technology/How_to_Manually_Update_Eset_NOD32_Offline (Digg - How to Manually Update Eset NOD32 Offline) [count: 1] Host: digg.com (URL not typed directly) type: LINK
8/28/2010	15:56:14	Firefox history	3	URL: http://www.fullydown.net/software/security-antivirus/170465-eset-nod32-offline-updater-5381-20100820.html	http://www.fullydown.net/software/security-antivirus/170465-eset-nod32-offline-updater-5381-20100820.html (ESET NOD32 Offline Updater 5381 (20100820) Ã‚Â» indir Full Download Rapidshare Hotfile - FullyDown.Net) [count: 1] Host: www.fullydown.net (URL not typed directly) type: LINK

Tablo 10 - Delil 3 ESET Antivirüs Programı İnternet Kayıtları

Bulgular neticesinde Delil 3'te, bilgisayar programı yazabilen ve bilgisayarlar konusunda bilgi sahibi olan ileri düzey bir kullanıcının düzenli işlem yaptığı tespit edilmiştir. İlk raporda belirtilen "Zaman değiştirme işlemi, yazılmış özel bir program ile ya da basit bir "visual basic script" ile olabilmektedir."[17] yorumuna paralel olarak, ilgili imajda bulunan "Hanefi.doc", "SY.doc", "Ulusal Medya 2010.doc" ve "Yalçın hoca.doc" dosyalarındaki zaman tarih

[17] TÜBİTAK, *ODATV SORUŞTURMASI DİJİTAL ADLİ ANALİZ RAPORU*, 153,182,192 ve 201. sayfalar

tutarsızlıklarının oluşma ihtimalleri arasında bilgisayar kullanıcısının kendi müdahalesi de ihtimal dâhilindedir. Zararlı yazılımla veya kullanıcının kendisi tarafından yapılabilecek bu tür bir manipülasyona ilişkin bir ize ilgili imajda rastlanmadığından, dosya tarih tutarsızlıklarının hangi şekilde oluştuğu net olarak söylenememektedir.

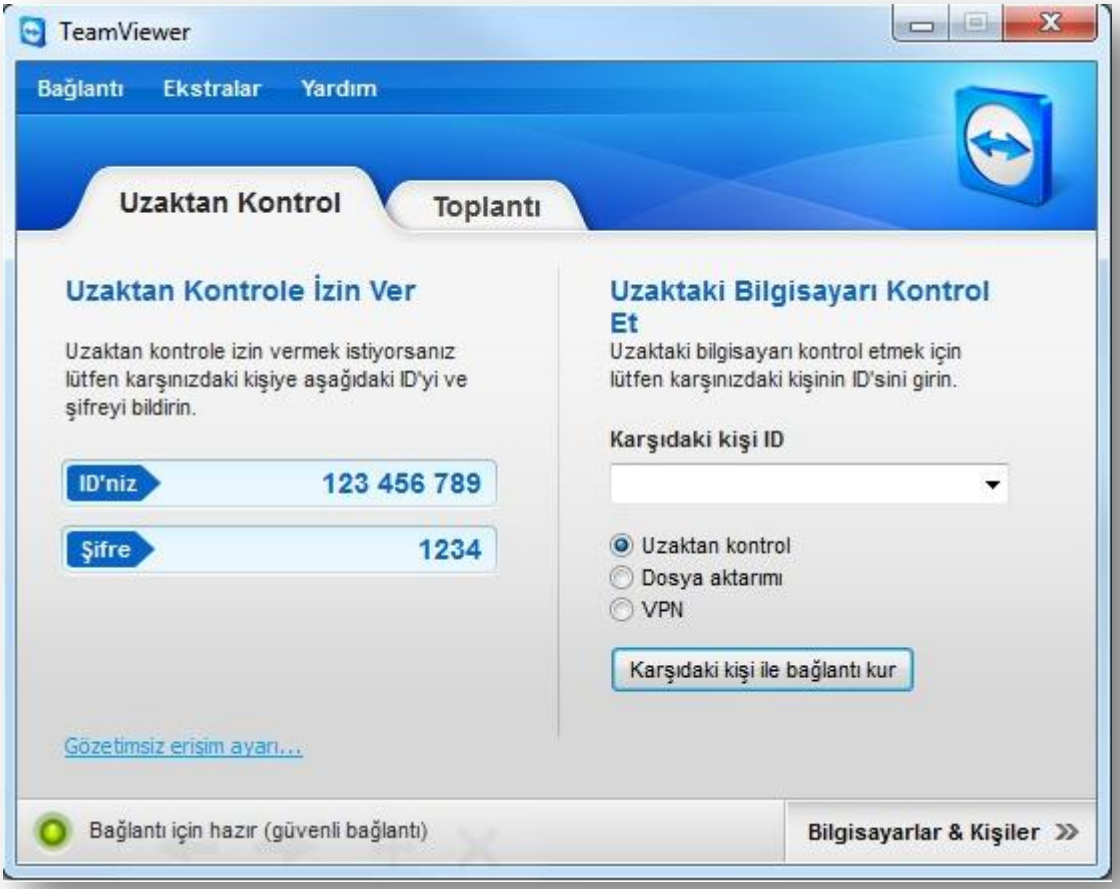
Soru 6

Raporun 215. sayfasında belirtilen her üç bilgisayarda da kurulu olduğu ve kullanıcı numaraları ile kullanıldığı belirtilen Teamviewer isimli uzaktan bağlantı ve yönetim programı ve özellikleri hakkında açıklamada bulunulması? Bu program aracılığı ile uzaktan erişim ile bilgisayara dosya gönderilip gönderilemeyeceği? Bu 3 bilgisayar arasında bu program üzerinden birbirleri ile bağlantı kurulup kurulmadığı? Kurulmuş ise dosya alış verişinde bulunulup bulunulmadığı? Her 3 bilgisayarda bu program kullanılmak sureti ile Ek- 1 de belirtilen dosyalarla ilgili oluşturma, değiştirme, gönderme veya açma gibi işlemlerin yapılıp yapılmadığının ayrıntılı bir şekilde araştırılarak belirtilmesinin istenmesi?

Cevap 6

Teamviewer uygulaması, uzaktaki başka bir bilgisayarı internet üzerinden yönetmeye yarayan bir araçtır[18]. Programın özellikleri arasında dosya transferi, uzaktan bağlanan kullanıcı ve bağlanılan bilgisayar arasında VPN[19] ile şifreli haberleşme, grafik arayüz desteğiyle uzak masaüstü bağlantısı imkânları bulunmaktadır. Uzaktan bağlanılacak bilgisayara, o bilgisayar kullanıcısının izni ve haberi olmadan erişmek mümkün değildir.[20] Teamviewer uygulaması kurulduğunda, o bilgisayara özel bir kimlik bilgisi (id) ve parola tanımlanır (Şekil 23). Bu bilgisayara erişmek isteyen uzaktaki başka bir Teamviewer kullanıcısı, bağlanmak istediği bilgisayarın kimlik bilgisini ve parolasını bilmeden ilgili bilgisayara erişemez (Şekil 24).

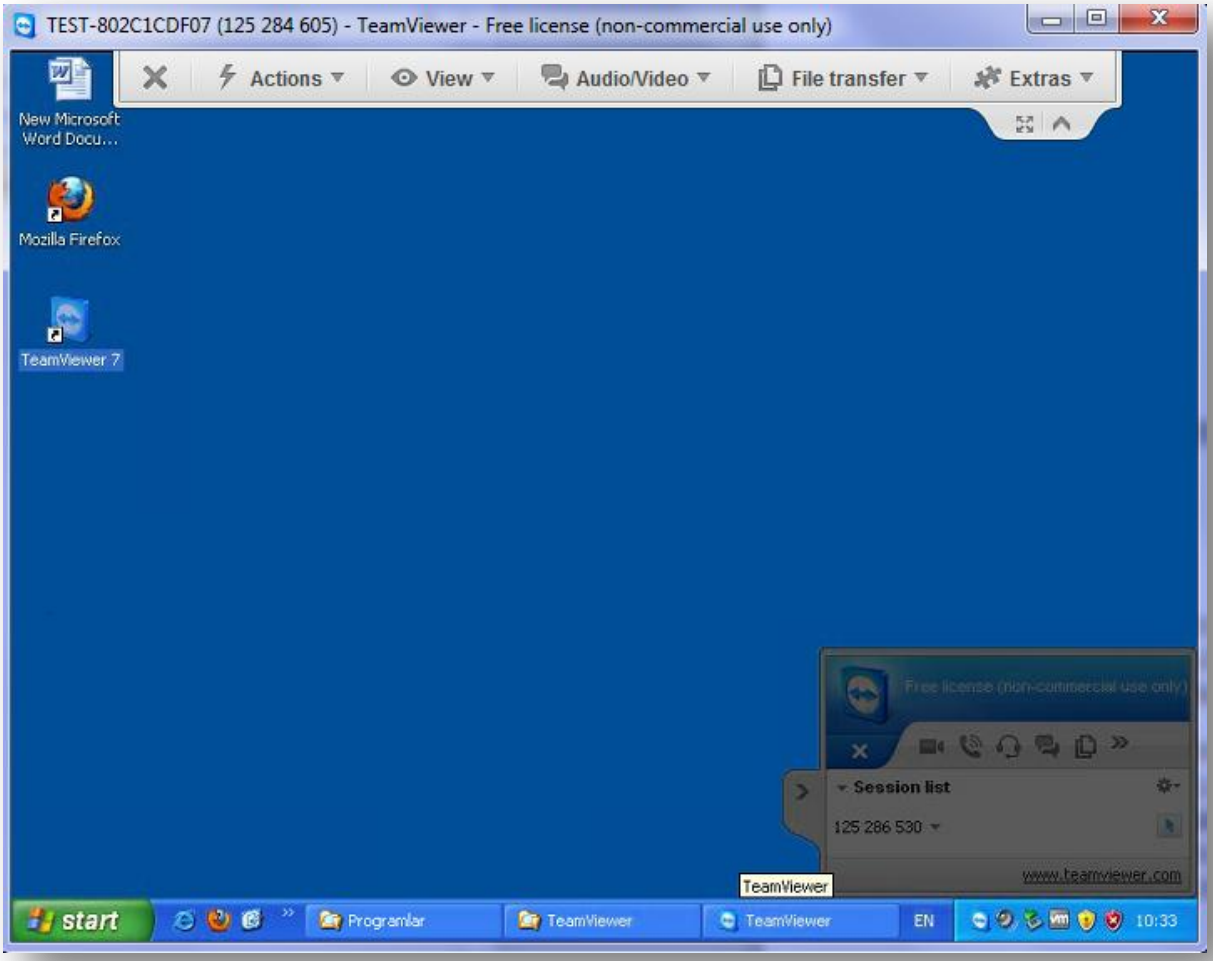
[18] http://www.teamviewer.com/tr/index.aspx
[19] http://en.wikipedia.org/wiki/Virtual_private_network
[20] http://www.teamviewer.com/en/products/security.aspx



Şekil 23 - Teamviewer Giriş Ekranı

Şekil 24 - Teamviewer Parola Ekranı

Bağlantı kurulduktan sonra her iki tarafın ekranında da bağlantı detayları görünmektedir. (Şekil 25)



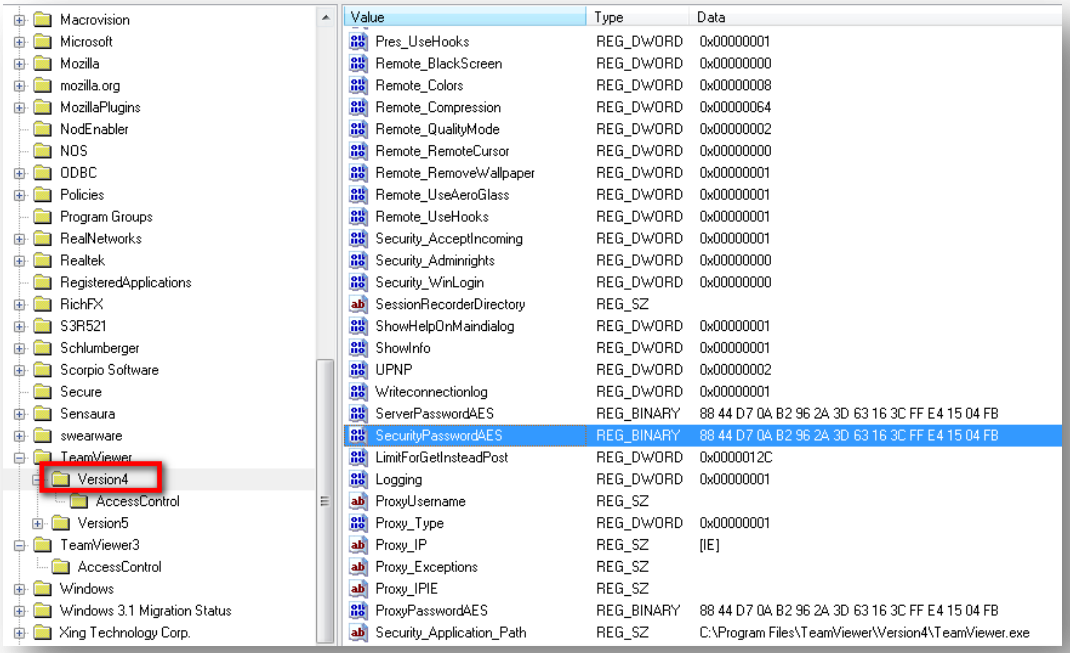
Şekil 25 - Bağlantı Sırasında Ekran Görüntüsü

Gerek bağlantı kurulması için kullanıcı adı ve parola ihtiyacı, gerekse bağlantı kurulduktan sonra ekranlarda çıkan uyarılar ve bilgi notları, Teamviewer uygulamasının karşılıklı onay mekanizmasına dayalı bir uzaktan erişim programı olduğunu göstermektedir.

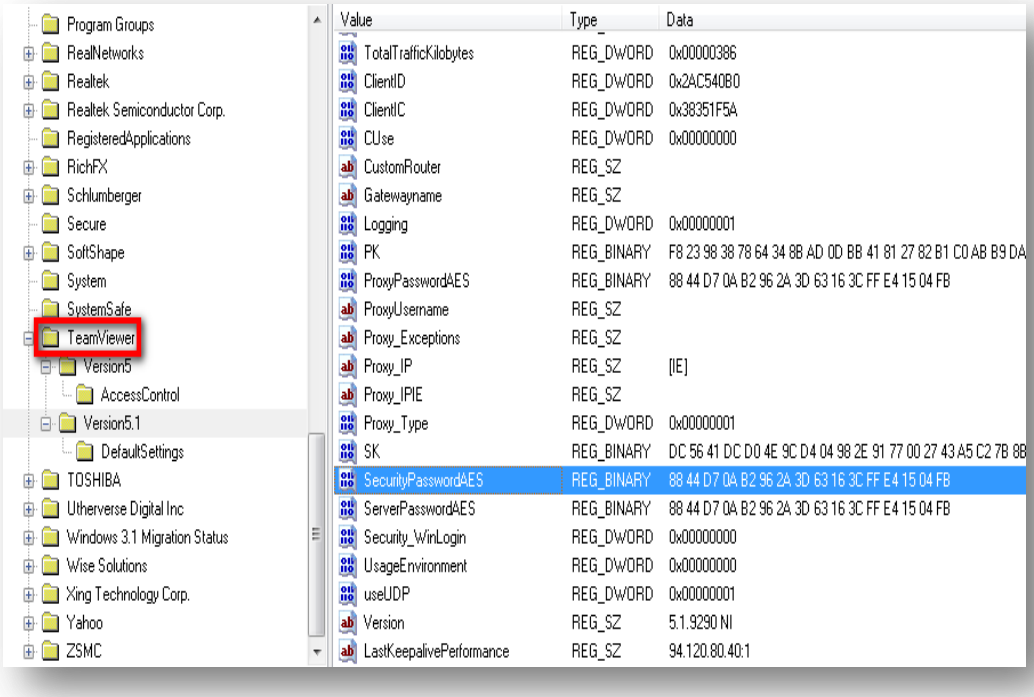
Bu teknik özellikleriyle Teamviewer; bilgisayarını uzaktan yönetmek isteyenlere yönelik, birden çok kişinin bağlanarak sanal toplantılar yapabildiği ve dosya alış verişi imkânları bulunan bir uygulamadır. Uzaktaki bir bilgisayarı yönetme ihtiyacı olan sistem yöneticileri ve teknik destek personelinin kullandığı ürünler arasında sayılabilir. Ancak kolay kullanımı nedeniyle birden fazla bilgisayarı olan kişisel kullanıcılar da tercih edebilmektedir.

İmajlarda Teamviewer Programına Dair İzler

İncelenen imajlarda Teamviewer uygulamasının kullanıldığı tespit edilmiştir.



Şekil 26 - Delil 1 Bilgisayarı Teamviewer Yapılandırma Ayarları



Şekil 27 - Delil 2 Bilgisayarı Teamviewer Yapılandırma Ayarları

Delil 1 bilgisayarı (Şekil 26) ve Delil 2 bilgisayarında (Şekil 27) kurulu olan Teamviewer uygulamasında aynı parolanın kayıtlı olduğu görülmüştür. Bu sayede kullanıcıların birbirilerinin bilgisayarlarına aynı parola ile uzaktan bağlanabildikleri ve yönetebildikleri düşünülmektedir.

Teamviewer uygulamasının özellikleri ve davaya konu hard disk imajlarındaki bulgular birlikte değerlendirildiğinde;

- Teamviewer uygulamasının ilgili hard disk imajlarında silinmiş halde eski sürümlerinin olması,
- Teamviewer kullanılarak açılan veya değiştirilen dosyalara ilişkin kayıtların Teamviewer uygulamasınca kaydedilmiyor olması,
- Davaya konu hard disklerde bulunan Teamviewer uygulamalarında kayıtlı parolaların aynı olması,
- Uygulama erişim kayıtlarında, davaya konu bilgisayarların birbirleriyle haberleştiğine dair işaretler bulunması,

Bulgularına dayanarak, bu kullanıcıların Teamviewer uygulaması ile birbirlerinin bilgisayarlarına uzaktan erişim sağladığı düşünülmektedir. Bu nedenle, davaya konu dosyaların ilgili hard disklere Teamviewer aracılığıyla gelmiş olması ihtimaller arasındadır.

Soru 7

Bilirkişi raporunun 230. Sayfasında yer alan jangomail kullanılarak gönderildiği belirtilen e-posta ekindeki "Ataturk_Ekrankoruma.scr" ve "Duyuru.pdf' dosyaları seçildiği ve analiz edildiğinin belirtildiği, diğer dosyaların aynı yöntemle analizin yapılmadığı anlaşılmakla, e-posta ekindeki diğer dosyaların da analiz edilerek sonuçların yalın bir şekilde karşılaştırmalı olarak açıklanması?

Cevap 7

Delil 1 bilgisayarında jangomail kullanılarak gönderilen e-postalar, e-postaların ekinde yer alan zararlı dosyalar, bu dosyaların türleri ve bağlantı kurmaya çalıştıkları saldırgana ait adres için gerçekleştirdikleri alan adı sorguları çıkartılarak, ilk bilirkişi raporunun 230. sayfasında e-postalar ile ilgili verilen tablonun eklentiler ile ilgili daha geniş bilgiler içerecek şekilde tekrar düzenlenmesiyle Tablo 11'de verilmiştir.

E-posta Adı	Eklenti	Eklenti Türü	Asıl Virüs Dosyası ve Yolu	Alan Adı Sorgusu
187E16C5-000056A4.eml	AKP_oncesi-sonrasi.pdf	Turkojan-RAT	C:\Documents and Settings\Türker\Application Data\FLV Player\svchost.exe	driver.myftp.org
5A9C4EFE-0000E9F3.eml	Ataturk_Ekrankoruma.scr	Turkojan-RAT	C:\WINDOWS\FLVPlayer\svchost.exe	antivirus.myftp.org
66B46747-000042CF.eml	Ataturk_Ekrankoruma.scr	Turkojan-RAT	C:\WINDOWS\FLVPlayer\svchost.exe	antivirus.myftp.org
37EA0857-00004396.eml	RssReader2.1.zip	Turkojan-RAT	C:\WINDOWS\FLVPlayer\svchost.exe	antivirus.myftp.org
1609770D-000058F0.eml	RssReader2.1.zip	Turkojan-RAT	C:\WINDOWS\FLVPlayer\svchost.exe	antivirus.myftp.org
56825A91-00004377.eml	Duyuru.pdf	Bandook-RAT	C:\Documents and Settings\Türker\Application Data\Adobe\svchost.exe	adobupdate.serveftp.com
56AF62F7-000058C2.eml	Duyuru.pdf	Bandook-RAT	C:\Documents and Settings\Türker\Application Data\Adobe\svchost.exe	adobupdate.serveftp.com
29C64C6C-000058C1.eml	Duyuru.pdf	Bandook-RAT	C:\Documents and Settings\Türker\Application Data\Adobe\svchost.exe	adobupdate.serveftp.com
72010E0A-00004376.eml	Duyuru.pdf	Bandook-RAT	C:\Documents and Settings\Türker\Application	adobupdate.serveftp.com

			Data\Adobe\svchost.exe	
21974EA4-00004375.eml	AKPkarikaturleri.zip	Bandook-RAT	C:\Documents and Settings\Türker\Application Data\Adobe\svchost.exe	adobupdate.serveftp.com

Tablo 11 - Delil 1'e "jangomail" ile Gönderilen E-Posta Eklenti Özellikleri

Tablo 11'den listelendiği üzere, Jangomail kullanılarak toplamda 5 farklı eklenti dosyası (AKP_oncesi-sonrasi.pdf, Ataturk_Ekrankoruma.scr, RssReader2.1.zip, Duyuru.pdf ve AKPkarikaturleri.zip) gönderilmiş olmakla birlikte, kullanıcının açmasını sağlamak ve antivirüs tarafından tespitlerini zorlaştırmak amacıyla farklı formattaki dosyalara dönüştürülmüş veya sarmalanmış olarak 3 farklı zararlı yazılım dosyası olduğu tespit edilmiştir.

Oluşturulan asıl virüs dosyası, asıl virüs dosyası yolu ve gerçekleştirilen alan adı sorgularına bakılarak tespit edilen 3 farklı zararlı yazılım dosyasından, 2 zararlı yazılımın Turkojan-Rat türünde ve 1 zararlı yazılımın ise Bandook-Rat türünde oldukları görülmüştür. Aynı türde oldukları için benzer izler ve işlemler gerçekleştiren Turkojan-Rat türü zararlı yazılımlardan "Ataturk_Ekrankoruma.scr" dosyası seçilmiş, bu zararlı yazılımı içeren dosyanın detaylı analiz adımları, gerçekleştirdikleri faaliyetler ve tespit edilen izleri önceki bilirkişi raporunda listelenmiştir. Kullanılan Bandook-Rat türü zararlı yazılımın ise iki farklı dosya içinde sarmalanıp gönderilmesinden dolayı, bu aynı zararlı yazılımı barındıran dosyalardan "Duyuru.pdf" dosyası seçilerek detaylı analiz adımları, gerçekleştirdikleri işlemler ve tespit edilen izleri de ayrıca raporda belirtilmiştir. Diğer zararlı yazılımların da analiz sonuçları aynı veya rapor sonucu değiştirmeyecek şekilde benzer olduğu için diğer zararlı yazılımların analiz sonuçları raporda belirtilmemiştir.

Soru 8

Bilirkişi raporunun sonuç kısmında " EK-1 de listelenen dosyalardan sy.doc ve prj_60.doc dosyaları dışındakilerin ilgili bilgisayarlarda oluşturulduğuna veya değiştirildiğine dair bir bulguya rastlanmamıştır. sy.doc ve prj_60.doc dosyalarının delil 2 bilgisayarında değiştirilmiş olma ihtimali mevcuttur. Bu iki dosya dışındaki dosyaların bilgisayar kullanıcıları tarafından açıldığında, işletim sistemi üzerinde oluşabilecek izler incelenmiş ve ilgili bilgisayar kullanıcıları tarafından açıldıklarına dair kuvvetli bir bulgu olmadığı tespit edilmiştir. " açıklamasının bulunduğu, sy.doc ve prj_60.doc dosyalarının hangi bilgisayarda oluşturulmuş olabileceğinin yeniden araştırılması, DELİL-2 bilgisayarda değiştirilmiş olma olasılığından bahsedilmekle, bu olasılığın neden ve sonuçları ile yalın olarak açıklanması? Belirtilen 2 dosyanın her 3 bilgisayar için ayrı ayrı açılma, oluşturulma, değiştirilme durumlarının yeniden ayrıntılı olarak açıklanması? EK- 1 listede yer alan diğer dosyalar ile anılan bu iki dosyanın diskteki konumları, kullanılan yazı karakteri, oluşturulma, değiştirilme tarihleri v.s gibi açılardan karşılaştırılmasının istenmesi? Kesin kanıya ulaşılıp ulaşılamayacağı? Ulaşılamıyor ise nedenlerinin açıklanması?

Cevap 8

"SY.doc" ve "prj_60.doc" ile alakalı elde edilen dosya sistemi ve ofis üst verileri Tablo 12 ve Tablo 13'de verilmiştir. Bu verilerin incelenmesi sonucunda konu ile alakalı görülen noktalar şu şekilde özetlenebilir:

- Her iki dosya da Delil 1'de içerik olarak mevcuttur. Ancak dosyalar silinmiş olduğu ve $MFT kayıtları bulunmadığından sadece $LogFile kayıtlarındaki zaman bilgilerine ulaşılmıştır.
- Delil 2 bilgisayarında bu dokümanlarla ilgili olarak sadece $LogFile kayıtları mevcuttur. Dosyanın içeriğine veya $MFT kayıtlarına rastlanmamıştır.
- Delil 3 bilgisayarında sadece "SY.doc" dosyası bulunmaktadır ve silinmemiş durumdadır.
- Delil 1'deki $LogFile kayıtlarından, "SY.doc" ve "prj_60.doc"dosyalarının Delil 1 bilgisayarında "2010:11:11 17:42:31" zamanında **bir işlem** gördüğü anlaşılmaktadır.
- Delil 2'deki $LogFile kayıtlarından, "SY.doc" dosyasının "2010:07:26 23:05:53" ve "2010:07:26 23:52:58" zamanlarında, "prj_60.doc" dosyasının ise "2010:10:20 22:59:41" zamanında, Delil 2 bilgisayarında **bir işlem** gördüğü anlaşılmaktadır.
- **Bu işlem** dosya oluşturma, taşıma, kopyalama veya silme gibi işlemlerden herhangi birisi olabilir.
- Delil 1 ve Delil 2 bilgisayarlarında "SY.doc" ve "prj_60.doc" dosyalarına ait yukarıda belirtilen dosya sistemi zamanları, bu bilgisayarlara hedefli olarak gönderilen zararlı yazılımların gönderilme zamanlarından öncedir. Bu dosyalara ait $LogFile

kayıtlarındaki dosya sistemi zamanlarının değiştirilmesi çok zor olduğu için, **bu iki dosyanın zararlı yazılımlar aracılığı ile uzaktan gönderilmiş olma ihtimalinin çok düşük olduğu değerlendirilmektedir**.

- "SY.doc" ve "prj_60.doc" ofis dosyalarının son değiştiren alanında "TOSHIBA" ofis kullanıcı ismi, ofis uygulama versiyonu olarak ise "11.5606" bilgisi bulunmaktadır. Cevap 1'de yapılan açıklamalar doğrultusunda bu veriler bu **dosyaların Delil 2 bilgisayarında değiştirilmiş olma ihtimalini doğurmaktadır.**

- Delil 2'deki $LogFile kayıtlarından, "SY.doc" dosyasının, "26/07/10 23:05:31" zaman bilgilerine sahip "SY.rar" dosyası ile, "prj_60.doc" dosyasının da "20/10/10 22:56:47" zaman bilgilerine sahip "20_10.rar" dosya ile büyük ihtimalle bir ilişkisinin olduğu değerlendirilmektedir.

- Bu ilişki; "SY.doc" dosyasının "SY.rar" arşiv dosyasından çıkarılması, "prj_60.doc" dosyasının da "20_10.rar" arşiv dosyasından çıkarılması şekilde olabileceği gibi "SY.doc" dosyasının "SY.rar" dosyası olarak arşivlenmesi sonra taşınması veya silinmesi, "prj_60.doc" dosyasının "20_10.rar" olarak arşivlenmesi sonra taşınması veya silinmesi şeklinde de olabilir. Hangi tür bir işlemin gerçekleştirildiğini **kesin olarak belirlemek mümkün değildir**.

- "SY.doc" ve "prj_60.doc" dosyalarının ofis belge değiştirme üst verisinde geçen, sırasıyla "2010:07:26 06:05:00" ve "2010:10:20 16:34:00" zamanları, Delil 2 $LogFile kayıtlarında bu iki dosyanın bir işlem gördüğünü gösteren (Tablo 13) zamanlar ile aynı gün içinde olması, bu dosyaların son olarak Delil 2 bilgisayarında **değiştirilmiş olma ihtimalini arttırmaktadır**.

- Aynı şekilde, "SY.doc" ve "prj_60.doc" dosyalarının ofis belge değiştirme zamanlarında (Bkz Tablo 12), Delil 2 bilgisayarındaki diğer kullanıcı işlemleri tespit edilmeye çalışılmıştır. Delil 2 bilgisayarında bu tarihlere kadar uzanan sistem kayıtları bulunmadığından, ilgili tarihlerde bilgisayarın açık olup olmadığı tespit edilememiştir. Buna ek olarak, bahsi geçen günde dosya sistemi üst verilerine rastlanmasına rağmen, ilgili saatlerde değişen başka bir dosya sistemi üstverisine rastlanmamıştır. Bu tür bir üst verinin bulunmaması bahse konu olan zamanlarda, Delil 2 bilgisayarı üzerinde **herhangi bir işlem yapılmadığı anlamına gelmemektedir**.

- "SY.doc" ofis dosyasının, yazar alanında "soner" ofis kullanıcı ismi, şirket alanında ise "Conqueror" adı geçmektedir. Cevap 1'de yapılan açıklamalar doğrultusunda bu veriler, **bu dosyanın "Soner Yalçın" isimli şahıs tarafından kullanılan başka bir bilgisayarda yazılmış olma ihtimalini doğurmaktadır.**

- "prj_60.doc" ofis dosyasının, yazar alanında "Barış" ofis kullanıcı ismi bulunmaktadır, şirket alanı ise boştur. Cevap 1'de yapılan açıklamalar doğrultusunda bu veriler, **bu dosyanın "Barış Pehlivan" isimli şahıs tarafından kullanılan başka bir bilgisayarda yazılmış olma ihtimalini doğurmaktadır.**

Yukarıdaki bilgiler ve yorumlar doğrultusunda, **"SY.doc" dosyasının "Soner Yalçın" isimli şahıs tarafından başka bir bilgisayarda, "prj_60.doc" dosyasının "Barış Pehlivan" isimli şahıs tarafından başka bir bilgisayarda oluşturulmuş olma ihtimalinin yüksek**

olduğu, yine bu iki dosyanın **Delil 2 bilgisayarında değiştirilmiş olma ihtimalinin de yüksek olduğu değerlendirilmektedir**.

Dosya Adı	**SY.doc**	**SY.doc**	**prj_60.doc**
Delil No	Delil1	Delil3	Delil1
Dosya Konumu	D:\Yedek\desktop\Sağır Oda\SY.doc	C:\Users\user\Documents \SY.doc	D:\Yedek\desktop\SağırOda\prj_ 60.doc
Dosya Durumu	Silinmiş, $MFT kaydı yok, unallocated clusterda bulunuyor	Aktif	Silinmiş, $MFT kaydı yok, unallocated clusterda bulunuyor
Uygulama Versiyonu	11.5606	11.5606	11.5606
Yazar	soner	soner	Barış
Son Değiştiren Kullanıcı	TOSHIBA	TOSHIBA	TOSHIBA
Şirket	Conqueror	Conqueror	
Belge Oluşturma	2010:07:23 12:20:00	2010:07:23 12:20:00	2010:10:19 07:21:00
Belge Değiştirme	2010:07:26 06:05:00	2010:07:26 06:05:00	2010:10:20 16:34:00
LogFile Kayıt Tarihi	2010:11:11 17:42:31		2010:11:11 17:42:31
Nesne Tipi	Microsoft Office Word Belgesi	Microsoft Office Word Belgesi	Microsoft Office Word Belgesi
Karakter Tipi	Unicode (UTF-8)	Unicode (UTF-8)	Unicode (UTF-8)
Std Oluşturma Tarihi		2010-08-01 20:35:12	
Std Değiştirme Tarihi		2010-07-26 10:05:55	
Std Erişim Tarihi		2010-08-01 21:34:50	
Std Giriş Tarihi		2011-02-14 07:33:43.984529	

FN Oluşturma Tarihi		2011-02-14 07:30:19.242128	
FN Değiştirme Tarihi		2011-02-14 07:30:19.242128	
FN Erişim Tarihi		2011-02-14 07:30:19.242128	
FN Giriş Tarihi		2011-02-14 07:30:19.242128	
MD5 Hash	6a83edf0fc27d3f49867a2d5128f66dc	6a83edf0fc27d3f49867a2d5128f66dc	aa7bce47c9dc16844695f05b5f7a6c13

Tablo 12 - "SY.doc" ve "prj_60.doc" Dosya ve Dosya Sistemi Üst Verileri

Dosya Adı	Delil No	Dosya Konumu	Belge Oluşturma	Belge Değiştirme	LogFile Kayıt Tarihi
SY.rar	Delil2	D\BARIS YEDEK 11122009\DEKSTOP\DEPO			2010:07:26 23:05:31
SY.doc	Delil2	D:\BARIS YEDEK 11122009\DEKSTOP\DEPO			2010:07:26 23:05:53
SY.doc	Delil2	D:\BARIS YEDEK 11122009			2010:07:26 23:52:58
SY.doc	Delil1	D:\Yedek\desktop\SağırOda\SY.doc	2010:07:23 12:20:00	2010:07:26 06:05:00	2010:11:11 17:42:31
SY.doc	Delil3	C:\Users\user\Documents\SY.doc	2010:07:23 12:20:00	2010:07:26 06:05:00	
20_10.rar	Delil1	D:\BARIS YEDEK 11122009\DEKSTOP\DEPO			2010:10:20 22:56:47
prj_60.doc	Delil2	D:\BARIS YEDEK 11122009\DEKSTOP\DEPO			2010:10:20 22:59:41
prj_60.doc	Delil1	D:\Yedek\desktop\SağırOda\prj_60.doc	2010:10:19 07:21:00	2010:10:20 16:34:00	2010:11:11 17:42:31

Tablo 13 - "sy.doc" ve "prj_60.doc" ile Alakalı $LogFile Kayıtları

Soru 9

Sanık Hanefi AVCI'nın 09.10.2012 havale tarihli 7 sayfa ve 11 sorudan oluşan dilekçe içeriğinde yöneltilen sorulara ilişkin açıklamalarda bulunulması?

Hanefi Avcı 1. Soru

İncelenen her üç bilgisayarda da varlığı ve çalıştırılmış olduğu belirlenen zararlı yazılımın bilgisayarda neler yapabileceğinin açıkça belirtilmesi. Eğer saldırıyı yapanlar bu bilgisayarlarla zararlı yazılım üzerinde bağlantı kurmuş iseler neleri ekleyebilir, değiştirebilir ve ne işlerini ne kadar yok edebilirler?

Cevap

Bu konu ilk raporun Cevap 12 başlığı altında ve "Av. Celal Ülgen'in 30.01.2012 tarihli dilekçesinde yönelttiği sorular"'ın Cevap 1 başlığı altında açıklanmıştır.

Hanefi Avcı 2. Soru

Zararlı yazılım bu bilgisayarlarda çalıştırıldığına göre neler yapmıştır? ..bu yazılımların tüm yaptıkları tespit edilemiyorsa nedeni

Cevap

Bu konu ilk raporun Cevap 12 başlığı altında ve "Av. Celal Ülgen'in 30.01.2012 tarihli dilekçesinde yönelttiği sorular"'ın Cevap 1 başlığı altında açıklanmıştır.

Hanefi Avcı 3. Soru

Tübitak raporunda her üç bilgisayarda da bulunduğu belirtilen "yalcın hoca.doc" dosyasının üçü de aynı kabul edilmiş, ancak iyi bakıldığında görüleceği üzere " Müyesser yıldız " delil 3 bilgisayarındaki dosya büyüklük olarak "karakter sayısı" ve "revizyon numarası" farklıdır. Dosyanın da son iki cümlesinde " (Müyesser bakacak " ve " (Müyesser ilgilensin " cümlelerinin yerine " ilgilen" yazdığı görülecektir. Ayrıca bu dosya delil 3'de revizyon numarası diğerlerinden bir büyük 17'dir. Yani ODATV delil 1 ve 2 bilgisayarında bulunan dosya değiştirilip sonra gönderilmiştir. Bu dosyanın Müyesser Yıldız bilgisayarına geldiği ve tarihlerinin değiştirildiği 14.02.2011 tarihinde ODATV'deki delil 1. ve 2. Bilgisayarlarına el konmuş, kişiler gözaltındadır. Tübitak raporunda bu dosya delil 3 bilgisayara zararlı yazılımla gelmiş olması çok büyük ihtimaldir. o zaman diğer dosyalarında aynı yöntemle geldiği anlamına gelmez mi?

Cevap

Bu sorunun cevabı, bu raporun Cevap 3 ve "Soner Yalçın Soru 4" başlığı altında açıklanmıştır.

Hanefi Avcı 4. Soru

Zararlı yazılımlar çalıştığında 443 Port üzerinde bağlantı kurmaya çalıştığı/kurduğu ABD'de bulunan "adobupdate.serveftp.com" ve "adobupdate.servehttp.com" siteleriyle irtibat kurduğu zamandaki bu sitenin IP numarası nedir? Her üç bilgisayarında bağlantı kurduğunda tespit edilen IP'lerin zamana göre çıkarılması. (Bu IP'ler belirlendiğinde 2. Aşamada TIB'de bu IP'ler ile başka bağlantı kuran IP olup olmadığı araştırma imkânı böylece saldırganlar konusunda bilgi alma imkânı olabilecektir.

Cevap

Bu konu, ilk raporun "Av. Celal Ülgen'in 30.01.2012 tarihli dilekçesinde yönelttiği sorular" altındaki "Cevap 7" başlığı altında açıklanmıştır.

Hanefi Avcı 5. Soru

Tübitak raporunun tarih uygunsuzluğu da her dosya ile ilgili anlatımında aslında yeni zamanda bilgisayara yüklenmesine rağmen üst verilerinde eski tarih gözükmesinin sebebi anlatılırken dosyaların .rar uzantılı arşivleme ve sıkıştırma yöntemiyle taşınmasında geri yükleme sırasında eski tarihlerin dosyalar üzerinde görülebileceği winrar yazılımında bu özelliğin olduğu ima edilmektedir. Ayrıca delil 2 bilgisayarına bazı dosyaların .rrr uzantılı dosya halinde gelip içerisinde birçok dosyanın çıkarıldığı belirtilmektedir. Bundan bu dosyaların .rar uzantılı arşivleme dosyaları olarak uzaktan erişimli zararlı yazılımla yüklenip, yüklenme sırasında winrar'ın bu özelliği çalıştırılarak eski tarihli üst verilere sahip olarak yüklenmesi teknik olarak mümkün müdür?

Cevap

Delil 2 de davaya konu olan dosyaların dosya sistemi üst verileri NTFS dosya sisteminde bulunan $Logfile dosyasından çıkarılmıştır. Winrar programının $Logfile dosyasını değiştirme yeteneği yoktur. Soruda belirtildiği şekilde dosyaların dosya sistemi üst verilerinin **Winrar programı ile değiştirilmiş olma ihtimali yoktur**.

Hanefi Avcı 6. Soru

Delil 1 ve delil 2 bilgisayarlarında işlem gördüğü belirtilerek polis tarafından $logfile dosya kayıtlarına dayanılarak çıkarılan delil 1 bilgisayarına ait K-45 dizin 37-33 arasında bulunan 180 dosyanın, yine delil 2 bilgisayarına ait K-45 dizin 31-28 arasındaki dosyaların çoğu mükerrer dosyalar olduğu, hatta aynı klasörde aynı dosyanın birden fazla kayıtlı görüldüğü, 40 dosyanın mükerrer olduğu, bunun sebebinin Bandook –RAT Zararlı yazılımının iki defa yüklenmiş olması veya barisp@odatv.com ve barist@odatv.com e-posta adreslerine gönderilen zararlı yazılımların haber amaçlı diyerek iki imajları da barisp@odatv.com bilgisayarlarında açıldığı bundan dolayı zararlı yazılımın birden fazla çalışarak mükerrer dosya yüklediği aynı şekilde Tübitak raporunun 64 sahifesinde de 28-08(2).rar dosyasının internet-web-e-posta da mükerrer indirmelerde olabileceği belirtilmektedir. Tüm bu bilgiler birleştirildiğinde sıkıştırılmış .rar dosyalarıyla gönderilen dosyaların mükerrer açılıp bilgisayarlara yerleştiği anlaşılmaktadır. Dosyaların toplu olarak ve mükerrer olarak indirilmesinin zararlı yazılım ve sıkıştırılmış .rar dosyaları halinde eski tarihli olarak indirilmiş olması mümkün müdür?

Cevap

Bahsi geçen zararlı yazılımların davaya konuya edilen dosyalarla ilişkisi yorumlanmadan önce, bu verilere kaynak olarak gösterilen $LogFile dosyasının nasıl oluştuğu ve içerdiği verilerin ne anlama geldiği irdelenmelidir. Bir önceki raporda $LogFile dosyası ile detaylı bilgi verilmiştir[21].

Soruda geçen *"Dava klasörlerinden K-45 dizin 31-28 ve 37-33 arası sayfalarda belirtilen dosyalar ile bir önceki TÜBİTAK raporunun 64. sayfasındaki 28-08(2).rar dosyasının, internet ortamından mükerrer indirilmiş olabileceği"* yorumunun, $Logfile dosyasından hareketle yapıldığı düşünülmektedir.

Burada dikkat edilmesi gereken nokta, $LogFile'da görüntülenen kayıtlara ilişkin tarih verileridir. Bu tarih verilerinin değiştirilmesi çok zordur**.** Dolayısıyla bir dosyanın $LogFile kaydı bulunması halinde, ilgili kaydın göründüğü tarihte o dosyanın bir işlem gördüğü kabul edilmektedir.

Sonuç olarak; $LogFile tarih kayıtlarının değiştirilme ihtimali çok düşük olduğu ve bahse konu olan zararlı yazılımların gönderilme tarihlerinin, EK-1 listesindeki dosyaların tarihleri ile alakası olmadığı için böyle bir ilişki kurmak mümkün değildir. Soruda iddia edilen *"zararlı*

[21] TÜBİTAK, *ODATV SORUŞTURMASI DİJİTAL ADLİ ANALİZ RAPORU,* 220. sayfa

yazılımların 2 kez çalışması ve $LogFile kayıtlarının bu nedenle birden çok kez oluşması" teknik olarak **mümkün görünmemektedir.**

Hanefi Avcı 7. Soru

Müyesser Yıldız (delil 3) bilgisayarında bulunan 80'den fazla rakam, parantez vs. işaretten oluşan bir isme sahip içerisinde SY.doc, yalcinhoca.doc, ulusalmedya2010.doc , Hanefi.doc dosyalarından oluştuğu söylenen ancak bu dört dosyanın toplam 136 kb olması gerekirken bu dosyanın 2.146.971.648 bayt büyüklükte olan 01.03.2011 tarihli K-43 dizin 421 bulunan dosyanın Tübitak tarafından incelenmesi ve zararlı yazılım-virüs tarafından oluşturulup, oluşturulmadığının belirlenmesi

Cevap

Bu dosyaların adının geçtiği dosya Microsoft Windows Vista işletim sisteminde bulunan "gölge kopya" (Shadow Copy[22]) servisi tarafından oluşturulan bir yedekleme dosyasıdır. Bu gölge kopya servisi aynı "RAR" ya da "ZIP" arşivlerde olduğu gibi birçok dosyayı arşivlemek/yedeklemek için tek bir dosya oluşturup bu dosyanın içine dosyaları kaydetmektedir. Bu yüzden soruda bahsedilen ve gölge kopya servisi çalışırken disk üzerinde bulunan dosyaların isminin gölge kopya dosyasında bulunması normaldir. Bunun yanında sorunun ikinci kısmında sorulan dosya boyutu farklılığı da aynı mantıkla anlaşılabilir. Gölge kopya dosyasında sadece bu dosyaların değil disk üzerindeki diğer birçok dosyanın da olması, gölge kopyanın boyutunun büyük olmasının sebebidir.

Hanefi Avcı 8. Soru

Zararlı yazılımlarla 3 bilgisayara da yapılan saldırılar ve dosya göndermeler hakkında adli istinabe veya diğer yollarla ABD'den bilgi talep edilecek olsa jangomailde gelen sahte mailler ve yazılımın bağlanmaya kalktığı siteler hakkında hangi bilgilerin istenmesinin teknik incelemeyi daha ileri götürebilir. Bu bilgiler nelerdir, tespiti ile bildirilmesi. ABD gibi ülkelerin e-posta çıktılarını kayıt altına alındığı bilindiğinden bu tür bilgilerin talep edilmesi için saldırıya uğrayan bilgisayarlar için verilmesi gereken temel bilgiler IP numarası, zararlı yazılımın geldiği tarih aralığı ..vs. gibi bilgiler nelerdir?

[22] http://en.wikipedia.org/wiki/Shadow_Copy

Cevap

Bahse konu olan e-postaların gönderildiği tarihler ilk raporun Cevap 12 bölümünde verilmiştir. E-postaları göndermek için kullanılan e-posta servisi hakkında ve zararlı yazılımların bağlanmaya çalıştığı adresler hakkındaki bilgiler de ilk raporun Cevap 12 başlığı altında ve "Av. Celal Ülgen'in 30.01.2012 tarihli dilekçesinde yönelttiği sorular" altındaki "Cevap 7" başlığı altında verilmiştir.

Hanefi Avcı 9. Soru

TÜBİTAK raporunda sahife.286 cevap A3'te Emniyet Bilirkişilerinden ne istenmişse o çıkarılmış olup, istenmeyen hususlar çıkarılmaz….. mealinde açıklama yapılmıştır. Ancak dava dosyasında Bilirkişi atama belgeleri incelendiğinde bu kişilerin genel amaçlı bilirkişi olarak CMK 64. Maddesine göre atandıkları tüm teknik inceleme için görevlendirildikleri ve ODATV davasıyla ilgili baştan beri virüs-trojan iddiasını baştan beri dillendirdiği, buna rağmen her dosya hakkında TÜBİTAK ve diğer inceleme yapan Üniversite Bilirkişileri en az 6–8 tarih çıkarmaları Windows gezginin de bile 4 tarihin çıkarılabilmesine rağmen emniyetin 2 tarih çıkararak eksik bilgi vermesi, tüm dosyaları oluşturan ve yazan kullanıcı tanımlı elde bilgisayar olmamasına, TÜBİTAK ve diğer bilirkişilerin tespit ettiği bu dosyalar " bu bilgisayar kullanıcıları tarafından oluşturulmamış, değiştirilmemiş " tespiti yapılmasına rağmen emniyet bilirkişilerinin hiçbir tespiti yapmaması kusurlu davranış değil midir?

Cevap

Adli analiz çalışmalarındaki başarı, görevlendirilen bilirkişinin; konuya hâkimiyeti, ayırabileceği zaman, içinde bulunduğu iş yükü ve talep edilen analizin kapsamıyla ilgili detaylara haiz olması ile ilintilidir.

Bir bilirkişi, konuyla ilgili daha önce hazırlanmış raporları ancak teknik açıdan inceleyebilir ve kendi açısından gördüğü eksiklikleri yorumlayabilir. Nitekim dava hakkında hazırlanmış önceki bilirkişi incelemeleri, önceki raporda tarafımızdan etraflıca değerlendirilmiştir[23].

Raporlarda yer alan tarih bilgilerinin yorumlanması bilirkişiler arasında farklılık gösterebilmektedir. En doğrusu elde edilen bütün tarih verilerinin raporda ayrıntılı şekilde yer almasıdır. Bununla birlikte tarihlerin detaylı olması kadar, tarihlerden hareketle yapılan yorumların da tutarlı olması önem arz eder. Raporu inceleyecek makamların teknik bilgi seviyesinin bilirkişiler kadar olması beklenemez. Dolayısıyla bazı bilirkişilerin, raporun uzamaması ve daha kolay anlaşılabilir olması için sadece özet bilgileri rapora yansıttığı

[23] TÜBİTAK, *ODATV SORUŞTURMASI DİJİTAL ADLİ ANALİZ RAPORU,* 220. sayfa

durumlar olabilmektedir. Dolayısıyla bilirkişilerin hazırlayacağı raporların başarısı, gerek teknik detaylar gerekse teknik bulgulardan hareketle yapılacak yorumlarla kendini gösterir.

İlk raporda yapılan ve dosyaların birkaçı hariç bu bilgisayarlarda oluşturulduğuna ve değiştirildiğine dair bir bulguya rastlanılmadığı yorumu, "dosyaların hiçbir şekilde bilgisayar kullanıcılarıyla ilintili olmadığı, dosyaları açmadıkları, dosyaların varlıklarından bihaber oldukları" anlamına gelmeyip, bulguların kesinlik dereceleri göz önüne alınarak yapılmıştır. Nitekim hazırlanılan bu ek raporun 1. ve 2. cevaplarında konu daha detaylı olarak izah edilmiştir.

Hanefi Avcı 10. Soru

Dava dosyasındaki belgelere göre virüs-trojan saldırılarının olduğu tarihlerden önce 04.02.2011 tarihinden itibaren mahkeme kararıyla barisp@odatv.com ve barist@odatv.com e-postaların TIB üzerinde işlemeye alındığı ve bu kayıtların şu an adli emanette bulunduğu, bu kayıtların incelenmesi ek bilgi sağlayabilir mi?

Cevap

"barisp@odatv.com" ve "barist@odatv.com" e-posta hesaplarındaki 04.02.2011'den öncesine ait e-postalar, Delil 1 ve Delil 2 bilgisayarlarında mevcuttur ve bu e-postalarda gerekli incelemeler yapılmıştır.

Hanefi Avcı 11. Soru

Sanıklar açısından tüm şüpheli dosyalar bilgisayarlara 05.02.2011 tarihinden sonra gelmiş ve gelmesiyle silinmesi zararlı yazılım tarafından yapılmıştır. Bunun aksini kesin olarak ispatlayan durum, bilgi ve emare var mıdır?

Cevap

Delil 1 ve 2 bilgisayarlarına, EK-1 listesinde belirtilen dosyaların hepsi 05.02.2011 tarihinden önce gelmiştir. İlk raporda ve bu ek raporda elde edilen bulgular bunu göstermektedir.

Soru 10

Sanık Hüseyin Soner YALÇIN müdafii Av. Duygun YARSUVAT'ın 25.09.20 12 havale tarihli dilekçesi ve ekinde bulunana 2 sayfa toplam 6 sorudan oluşan konulara ilişkin açıklamalarda bulunulması?

Soner Yalçın 1. Soru

Dosyanın kullanıcı tarafından açılmamış olması ne anlam ifade etmektedir? Bu durumun adli bilişim açısından yorumlanması yapılırsa hangi sonuca ulaşılabilir?

Cevap

Bu konu Cevap 2'de açıklanmıştır.

Soner Yalçın 2. Soru

Dokümanlar ile silinmiş olarak tespit edildikleri bilgisayarlarda kurulu MSOffice sürümünün versiyonları nedir?

Cevap

Bu konu Cevap 1'de açıklanmıştır.

Soner Yalçın 3. Soru

Müyesser Yıldız'ın kullandığı bilgisayarda özel hedefli sosyal mühendislik saldırısının sonucu olarak aktif olarak çalıştığı tespit edilen ve dosyaların yüklenmesinde kullanıldığı düşünülen virüs/kötü amaçlı yazılım ile diğer bilgisayarlarda özel hedefli sosyal mühendislik saldırısının sonucu olarak bulunan ve aktif olarak çalıştığı tespit edilen virüs/kötü amaçlı yazılım isimleri nelerdir? Bu virüsler/kötü amaçlı yazılımlar tanınmış anti-virüs üreticilerince nasıl sınıflandırılmakta ve ne isimlerle anılmaktadır? Söz konusu virüs/kötü amaçlı yazılımların sistem üzerindeki etkileri ve kabiliyetleri nelerdir? Bu unsurların özellikleri aktif olarak çalıştıkları sistemi nasıl etkilemekte, sistem üzerinde tam olarak ne gibi işler yapabilmektedirler?

Cevap

Bu konu ilk raporun Cevap 12 başlığı altında ve "Av. Celal Ülgen'in 30.01.2012 tarihli dilekçesinde yönelttiği sorular"'ın Cevap 1 başlığı altında açıklanmıştır.

Soner Yalçın 4. Soru

İncelemeye konu hard diskler içerisinde özel hedefli sosyal mühendislik saldırısı sonrası zararlı yazılımların bulunması, bilimsel olarak bu hard disklerin güvenilir olmadığını söylemek için yeterli midir? Konuyu delil sağlığı ve güvenilirliği açısından irdeleyiniz?

Cevap

Parola çalma, uzaktan erişim sağlama, veri hırsızlığı veya başka amaçlar için kullanılabilen zararlı içerikli e-posta saldırıları günümüzde hızla yaygınlaşan bir saldırı unsuru olmaktadır. Farklı amaçlar ve motivasyonlarla yapılabilen bu tür ataklar, karşı tarafın bilişim teknolojileri hakkında bilgi seviyesiyle orantılı olarak başarılı veya başarısız olabilir.

Dijital adli analiz çalışmalarında zararlı yazılımların etkisi, farklı açılardan incelenmesi gereken bir konudur.

Ana başlıklar halinde;

- Zararlı yazılımın nasıl bulaştığının ortaya çıkarılması,
- Zararlı yazılımın yetkinlikleri,
- İncelenen hard diskte aktif olup olmadığı,
- Aktif olarak çalıştıysa ne tür işlemler yaptığı,
- Zararlı yazılımının çalışmasını engelleyecek ayar ve programların durumu,
- Zararlı yazılımın hangi tarihlerde bulaştığı, hangi tarihlere kadar aktivitesine devam etmiş olduğu,
- Kullanıcının zararlı yazılımın varlığından haberdar olup olmadığı,
- Kullanıcının zararlı yazılımla herhangi bir ilişkisinin olup olmadığı,
- Zararlı yazılımın delil karartma (anti forensics) amacıyla kullanılıp kullanılamayacağının tespiti

şeklinde sıralanabilecek çeşitli analizler yapılmalıdır.

Dijital adli analiz biliminde herhangi bir bulgunun delil niteliğinde olması ancak kapsamlı çalışmalar neticesinde ortaya çıkabilir. Herhangi bir tespitin tek başına bir anlam ifade etmesi çoğu zaman mümkün olmamaktadır.

Sonuç olarak incelenen disklerde görülen zararlı yazılımların varlığı tek başına bir anlam ifade etmez. Dava kapsamında incelenen hard disklerde tespit edilen zararlı yazılımların **varlığı ve bulaşma tekniği kadar**, ilgili zararlı yazılımların **hangi tarihlerde** aktif olarak çalıştığı, ne tür işlemler gerçekleştirdiği ve dava kapsamında incelenen dosyalarla ilişkisi

tespit edilmelidir. Dolayısıyla hard disklerde bulunan delillerin sağlığı ve güvenilirliği hakkında ancak bütün bu faktörler incelenerek yorum yapılabilir.

Soner Yalçın 5. Soru

3 ayrı delil bilgisayarına (Odatv, Barış Pehlivan ve Müyesser Yıldız'ın bilgisayarları), ayni tarihte (5 Şubat 2011), aynı kaynaktan (Jangomail), aynı yöntemle (e-mail), aynı trojan türüyle (Bandook RAT), aynı virüsle (Svchost.exe), aynı kabiliyete sahip zararlı yazılımla (uzaktan yönetim ve dosya atma) özel hedefli sosyal mühendislik saldırısının yapılması ve bu saldırı sonrası zararlı yazılımların aynı işlevi görmesiyle (aktif olarak çalışması) Müyesser Yıldız'ın bilgisayarındaki dosyaların (24 Ağustos 2012 tarihli TÜBİTAK raporundaki EK-1 listesindeki dosyalar) zararlı yazılımlar gönderildiğinin düşünülmesi; Müyesser Yıldız'ın bilgisayarlarındaki ilgili dosyaların diğer delil bilgisayarlarında da (Odatv ve Barış Pehlivanın bilgisayarları) bulunması ve bu dosyalar üzerinde ilgili bilgisayar kullanıcıları tarafından hiçbir işlem gerçekleştirmemiş olmaları toplu olarak düşünüldüğünde; ilgili dosyaların tüm delil bilgisayarlarına zararlı yazılım aracılığıyla gönderilmesi ihtimalini güçlü kılar mı?

Cevap

Gerçekleştirilen tetkikler neticesinde, Müyesser Yıldız'ın kullandığı Delil 3 bilgisayarında aktif olma şansı bulmuş bir takım zararlı yazılımların varlığı tespit edilmiştir. Benzeri zararlı yazılımlara dair bir takım izler Delil 1 ve Delil 2'de de bulunmuştur.

Bir önceki soruya verilen cevapta da belirtildiği gibi (Soner Yalçın 4.soru), zararlı yazılımların varlığı ile zararlı yazılımla dosya gönderildiği iddiası birbirinden farklıdır. Dolayısıyla bir dosyanın zararlı yazılımlar aracılığıyla gönderilip gönderilmediği hakkında ancak bir önceki soruda belirtildiği gibi detaylı analizler neticesinde yorum yapılabilir. Zararlı yazılımların her 3 delil bilgisayarına etkileri, EK-1 dosyalarının bu zararlı yazılımlar ile gönderilip gönderilmediğine ilişkin değerlendirmeler ve kullanıcıların EK-1 dosyaları üzerinde yaptıkları işlemlerin incelenmesi; bir önceki raporun 8. ve 12. sorularında, bu raporun ise 1. 2. ve 3. sorularında açıklanmıştır.

Soner Yalçın 6. Soru

“sydoc” ve ‘prj_60.doc” dosyalarının Delil 1 bilgisayarlarındaki üstverilerinden hareketle ilgili dosyalann “TOSHIBA isimli bir bilgisayarda Değiştirildiği ama aynı dosyaların kullanıcı adı ‘TOSHIBA” olan Delil 2’ye geliş saatlerinin, ilgili dosyalann Delil 1'de görünen son değiştirme saatinden saatler sonra gibi görünmesi, yine ayni dosyalarin Delil 2’de açılmamış olması bu dosyaların Delil 2'de değiştirilmediği anlamına gelmez mi?

Cevap

Bu sorunun cevabı 8. soruda verilmiştir.

Bilirkişi	Bilirkişi	Bilirkişi
Osman PAMUK	**Ünal TATAR**	**Emin ÇALIŞKAN**

4 EKLER

EK-1

Davaya konu olan dosyaların listesi:

Dosya Adı	Dosya Konumu
000KITAP.docx	Delil 1\D\Yedek\desktop\AÇIL SUSAM AÇIL\Yeni Klasör\S.U\000KITAP.docx
ABDULKADIR AYGAN.pdf	Delil 1\D\Yedek\desktop\AÇIL SUSAM AÇIL\snrylcn\kozinoğlu3\ABDULKADİR AYGAN.pdf
Bilinçlendirme.doc	Delil 1\D\Yedek\desktop\yeni\Bilinçlendirme.doc
chp.doc	Delil1\
EK-D MİLLİ EĞİTİM.doc	Delil 2\D\Lost Files\Kadrolaşma\Kadrolaşma GPP Çalışması\EK-D MİLİ EĞİTİM.doc
EK-D MİLLİ EĞİTİM.doc	Delil 2\D\Lost Files\001 AKP-KADROLASMA ÇALISMALARI\EK-D MILLI EGITIM.doc
EK-E AKP'NİN ATAMALARI.xls	Delil 2\D\Lost Files\Kadrolasma\Kadrolasma GPP Çalismasi\EK-E AKP'NIN ATAMALARI.xls
Ermeni Dosyası.doc	Delil 1\D\Yedek\desktop\AÇIL SUSAM AÇIL\snrylcn\proje\Ermeni Dosyası.doc
Fabrikatör.doc	Delil 1\D\Yedek\desktop\AÇIL SUSAM AÇIL\snrylcn\proje\Fabrikatör.doc
Hanefi.doc	Delil 1\D\Yedek\desktop\yeni\Hanefi.doc
Hanefi.doc	Delil 3\C\Users\user\Documents\Hanefi.doc
Kadrolasma_Konusma_Notu_Ocak_2004_1160580.doc	Delil1\
Kadrolaşma Bilgi Notu (Ocxak 2004) .doc	Delil 2\D\Lost Files\Kadrolasma\Kadrolasma GPP Çalismasi\Kadrolasma Bilgi Notu (Ocxak 2004).doc
KADROLAŞMA EK-A.doc	Delil 2\D\Lost Files\Kadrolasma\Kadrolasma GPP Çalismasi\KADROLASMA EK-A.doc
KADROLAŞMA EK-C.doc	Delil 2\D\Lost Files\Kadrolasma\Kadrolasma GPP Çalismasi\KADROLASMA EK-C.doc
Kadrolaşma en son0610170003.doc	Delil 2\D\Lost Files\Kadrolasma\Kadrolasma GPP Çalismasi\Kadrolasma en son 0610170003.doc
KADROLAŞMA KONUŞMA NOTU(OCAK 2004) .doc	Delil 2\D\Lost Files\Kadrolasma\Kadrolasma GPP Çalismasi\KADROLASMA KONUSMA NOTU(OCAK 2004).doc

KADROLAŞMA KONUŞMA NOTU(OCAK 2004) .doc	Delil 2\D\Lost Files\001 AKP-KADROLASMA ÇALISMALARI\KADROLASMA KONUSMA NOTU(OCAK 2004).doc
Kadrolaşma_Bilgi_Notu_Ocak_2004_1167314.doc	Delil1\
Konuşma Notu.doc	Delil 2\D\Lost Files\Kadrolasma\Kadrolasma GPP Çalismasi\Konusma Notu.doc
Koz.doc	Delil 1\D\Yedek\desktop\AÇIL SUSAM AÇIL\Yeni Klasör\Koz.doc
mafia.doc	Delil 1\D\Yedek\desktop\AÇIL SUSAM AÇIL\snrylcn\proje\mafia.doc
mit medya.doc	Delil 1\D\Yedek\desktop\AÇIL SUSAM AÇIL\snrylcn\proje\mit medya.doc
Nedim.doc	Delil 1\D\Yedek\desktop\AÇIL SUSAM AÇIL\Yeni Klasör\Nedim.doc
panzehir.doc	Delil 1\D\Yedek\desktop\AÇIL SUSAM AÇIL\snrylcn\proje\panzehir.doc
prj_60.doc	Delil1\
radikal dini grupların faaliyet alanları.pdf	Delil 1\D\Yedek\desktop\AÇIL SUSAM AÇIL\snrylcn\kozinoglu3\radikal dini gruplari faaliyetleri\radikal dini guruplarin faaliyet alanlari.pdf
Reosta Operasyonu.doc	Delil 1\D\Yedek\desktop\AÇIL SUSAM AÇIL\snrylcn\proje\Reosta Operasyonu.doc
Sabri Uzun.doc	Delil 1\D\Yedek\desktop\AÇIL SUSAM AÇIL\Yeni Klasör\Sabri Uzun.doc
simon son.doc	Delil 1\D\Yedek\desktop\AÇIL SUSAM AÇIL\Yeni Klasör\simon son.doc
Sn. Komutanım.doc	Delil 1\D\Yedek\desktop\yeni\Sn.Komutanim.doc
SY.doc	Delil 3\C\Users\user\Documents\SY.doc
SY.doc	Delil1\
teRTEemiz.doc	Delil 1\D\Yedek\desktop\yeni\teRTEmiz.doc
toplantı.doc	Delil 1\D\toplanti.doc
TRT.doc	Delil 2\D\BARIS YEDEK 11122009\DEKSTOP\DEPO\trt.doc
Tv Analiz Proje.doc	Delil 1\D\Yedek\desktop\AÇIL SUSAM AÇIL\snrylcn\proje\Tv Analiz Proje.doc
Ulusal Medya 2010.doc	Delil 1\D\Yedek\desktop\AÇIL SUSAM AÇIL\snrylcn\proje\Ulusal Medya 2010.doc
Ulusal Medya 2010.doc	Delil 3\C\Users\user\Documents\Ulusal Medya 2010.doc

Ulusal Medya.doc	Delil 1\D\Yedek\desktop\AÇIL SUSAM AÇIL\snrylcn\proje\Ulusal Medya.doc
Yalçın hoca.doc	Delil 3\C\Users\user\Documents\Yalçin hoca.doc
YBelgesi.doc	Delil 1\D\Yedek\desktop\AÇIL SUSAM AÇIL\Yeni Klasör\Nedim\YBelgesi.doc

EK-2

Tablo 2'de listelenen ofis kullanıcı isimlerinin "yazar" veya "son değiştiren kullanıcı ismi" kısımlarında geçen ve incelenen bilgisayarlarda bulunan diğer dokümanlar:

Ofis kullanıcısı "soner"

Ofis kullanıcısı "soner"'in yazar alanında geçtiği dokümanlar:

Delil	Dosya	Yazar	Son Değiştiren	Şirket	Uygulama Versiyonu
Delil1	C:/Documents and Settings/Türker/Belgelerim/haftasonu/Hangi Ergenekon.doc	soner	Sys	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/didemm/masaüstü/PROJE-CT/Soner yalçın/Mahrem Hayat.doc	soner	Ata_Pc	Conqueror	11.9999
Delil1	C:/Documents and Settings/Türker/Desktop/didemm/masaüstü/PROJE-CT/Soner yalçın/Menekşecan.doc	soner	Ata_Pc	Conqueror	11.9999
Delil1	C:/Documents and Settings/Türker/Desktop/didemm/masaüstü/PROJE-CT/Soner yalçın/Temmuz Devrimi.doc	soner	Ata_Pc	Conqueror	11.9999
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/Anıt.doc	soner	Baris	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/Liberal darbe.doc	soner	PROJE-CT	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/Türkçe Konuş.doc	soner	Baris	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/kokain isimler.doc	soner	Baris	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/Masaustu/masaüstü/haftasonu ekler/Gladio.doc	soner	Sys	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/Yeni Klasör/TAKSİM.doc	soner	Baris	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/Nazım Ergenekon.doc	soner	Sys	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/odaTV/odatv/İran musiki.doc	soner	ASUS	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/Eski Data/deşifreler/İran Kadın.doc	soner	Baris	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/SONER YALÇIN/MSP bölünme.doc	soner	Baris	Conqueror	11.5606

Delil1	C:/Documents and Settings/Türker/Desktop/SONER YALÇIN/6-7 Eylül.doc	soner	Sys	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/SONER YALÇIN/Ali Kemal.doc	soner	Baris	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/SONER YALÇIN/Anıt.doc	soner	soner	Conqueror	10.2625
Delil1	C:/Documents and Settings/Türker/Desktop/SONER YALÇIN/Ata Sırp.doc	soner	Sys	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/SONER YALÇIN/Atatürk Basın.doc	soner	Sys	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/SONER YALÇIN/Atatürk Çocukluğu.doc	soner	Baris	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/SONER YALÇIN/Babalar ve Oğullar.doc	soner	Sys	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/SONER YALÇIN/Nurettin Topçu.doc	soner	Baris	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/SONER YALÇIN/Obama.doc	soner	SYSTEM	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/SONER YALÇIN/Osmanlı Klasik.doc	soner	Baris	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/SONER YALÇIN/Psikolojik harp.doc	soner	Sys	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/SONER YALÇIN/Ruh Çağırma.doc	soner	Baris	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/SONER YALÇIN/Seyyid.doc	soner	Sys	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/SONER YALÇIN/titrek hamsi25ocak.doc	soner	Sys	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/SONER YALÇIN/TMT.doc	soner	soner	Conqueror	10.2625
Delil1	C:/Documents and Settings/Türker/Desktop/SONER YALÇIN/Tophane.doc	soner	Baris	Conqueror	11.9999
Delil1	C:/Documents and Settings/Türker/Desktop/SONER YALÇIN/VEHİB PAŞA1şubat.doc	soner	SYSTEM	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/SONER YALÇIN/Özür.doc	soner	Sys	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/SONER YALÇIN/İran Kadın.doc	soner	Baris	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/SONER YALÇIN/İslam dergisi.doc	soner	Baris	Conqueror	11.9999

Delil1	C:/Documents and Settings/Türker/Desktop/SONER YALÇIN/İslam Para.doc	soner	Baris	Conqueror	11.9999
Delil1	C:/Documents and Settings/Türker/Desktop/SONER YALÇIN/İsrail Saldırı.doc	soner	Sys	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/SONER YALÇIN/Şair Aşkı.doc	soner	Baris	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/SONER YALÇIN/CHP Çarşaf.doc	soner	Sys	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/SONER YALÇIN/CIA.doc	soner	Baris	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/SONER YALÇIN/Dönme.doc	soner	Baris	Conqueror	11.9999
Delil1	C:/Documents and Settings/Türker/Desktop/SONER YALÇIN/Ergenekon.doc	soner	Baris	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/SONER YALÇIN/Gladio.doc	soner	Sys	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/SONER YALÇIN/Hangi Ergenekon.doc	soner	Sys	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/SONER YALÇIN/Karl Marks.doc	soner	Sys	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/SONER YALÇIN/Kravat.doc	soner	Baris	Conqueror	11.9999
Delil1	C:/Documents and Settings/Türker/Desktop/Cihan/Alevi.doc	soner	ASUS	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/Cihan/Nazım-Kore.doc	soner	ASUS	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/Cihan/Yeni Evrak Çantası/s/Padişah Aşk.doc	soner	systm	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/Cihan/Yeni Evrak Çantası/s/S.Zaimportre.doc	soner	systm	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/Cihan/Yeni Evrak Çantası/wonr/Padişah içki 18 kasım 2007.doc	soner	systm	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/Cihan/Yeni Evrak Çantası/wonr/çemberli.doc	soner	systm	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/Cihan/Yeni Evrak Çantası/yazılar/İnönü musiki.doc	soner	systm	Conqueror	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/Cihan/İran musiki.doc	soner	ASUS	Conqueror	11.5606
Delil1	D:/Yedek/desktop/AÇIL SUSAM AÇIL/Misyonerler.doc	soner	Exper Computer	Conqueror	11.5606

Delil1	D:/Yedek/desktop/AÇIL SUSAM AÇIL/snrylcn/Abide-i Hürriyet.doc	soner	Apple IMC	Conqueror	11.0000
Delil1	D:/Yedek/desktop/AÇIL SUSAM AÇIL/snrylcn/Avrupa İmaj.doc	soner	5N1K	Conqueror	11.5606
Delil1	D:/Yedek/desktop/AÇIL SUSAM AÇIL/snrylcn/Düello.doc	soner	soner	Conqueror	10.2625
Delil1	D:/Yedek/desktop/AÇIL SUSAM AÇIL/snrylcn/Misyonerler.doc	soner	Bilkom	Conqueror	11.0000
Delil1	D:/Yedek/desktop/AÇIL SUSAM AÇIL/snrylcn/Rektörler.doc	soner	Bilkom	Conqueror	11.0000
Delil1	D:/Yedek/desktop/AÇIL SUSAM AÇIL/snrylcn/Sabah.doc	soner	5N1K	Conqueror	11.5606
Delil1	D:/Yedek/desktop/Düello.doc	soner	Exper Computer	Conqueror	11.5606
Delil2	D:/aysel silme/odaTV/odatv/İran musiki.doc	soner	ASUS	Conqueror	11.5606
Delil2	D:/BARIS YEDEK 11122009/BELGELERIM/Hafta sonu Haberler/SONERY.doc	soner	Sys	Conqueror	11.5606
Delil2	D:/BARIS YEDEK 11122009/DEKSTOP/BARIŞ/hafasonu/Nazım Ergenekon.doc	soner	Sys	Conqueror	11.5606
Delil2	D:/BARIS YEDEK 11122009/DEKSTOP/BARIŞ/hafta/soner yalçın flaş.doc	soner	AYHAN	Conqueror	10.2625
Delil2	D:/BARIS YEDEK 11122009/DEKSTOP/BARIŞ/Hafta sonu Haberler/SONERY.doc	soner	YTU	Conqueror	11.9999
Delil2	D:/BARIS YEDEK 11122009/DEKSTOP/BARIŞ/haftasonu/Atatürk Basın.doc	soner	Sys	Conqueror	11.5606
Delil2	D:/BARIS YEDEK 11122009/DEKSTOP/BARIŞ/haftasonu/HAFTASONU/Seyyid.doc	soner	Sys	Conqueror	11.5606
Delil2	D:/BARIS YEDEK 11122009/DEKSTOP/BARIŞ/haftasonu/haftasonu ekler/Gladio.doc	soner	Sys	Conqueror	11.5606
Delil2	D:/BARIS YEDEK 11122009/DEKSTOP/BARIŞ/haftasonu/Hangi Ergenekon.doc	soner	Sys	Conqueror	11.5606
Delil2	D:/BARIS YEDEK 11122009/DEKSTOP/BARIŞ/haftasonu(2)/CHP Çarşaf.doc	soner	AYHAN	Conqueror	10.2625
Delil2	D:/BARIS YEDEK 11122009/DEKSTOP/BARIŞ/haftasonuoo/haftasonu/SONERY.doc	soner	AYHAN	Conqueror	10.2625
Delil2	D:/BARIS YEDEK 11122009/DEKSTOP/BARIŞ/hqaftasonu/Obama.doc	soner	SYSTEM	Conqueror	11.5606
Delil2	D:/BARIS YEDEK 11122009/DEKSTOP/BARIŞ/soner yaz[1]...doc	soner	YTU	Conqueror	11.9999
Delil2	D:/BARIS YEDEK 11122009/DEKSTOP/BARIŞ/titrek hamsi25ocak.doc	soner	YTU	Conqueror	11.9999

Delil2	D:/BARIS YEDEK 11122009/DEKSTOP/BARIŞ/yazılar ve görseller/titrek hamsi25ocak.doc	soner	AYHAN	Conqueror	10.2625
Delil2	D:/BARIS YEDEK 11122009/DEKSTOP/BARIŞ/YENİ KILASÖR/BAYRAM SEYRAN/BAYRAM/Babalar ve Oğullar.doc	soner	YTU	Conqueror	11.9999
Delil2	D:/BARIS YEDEK 11122009/DEKSTOP/BARIŞ/İsrail Saldırı.doc	soner	YTU	Conqueror	11.9999
Delil3	C:/Users/user/Documents/SY.doc	soner	TOSHIBA	Conqueror	11.5606
Delil3	C:/Users/user/Documents/Hanefi.doc	soner	soner	Conqueror	10.2605
Delil3	C:/Users/user/Documents/Yalçın hoca.doc	soner	user	Conqueror	10.2605

Tablo 14 - Ofis yazar isminin "soner" olduğu diğer dokümanlar

Ofis kullanıcısı "soner"'in "son değiştiren" alanında geçtiği dokümanlar:

Delil	Dosya	Yazar	Son Değiştiren	Şirket	Uygulama Versiyonu
Delil1	C:/Documents and Settings/Türker/Desktop/SONER YALÇIN/Anıt.doc	soner	soner	Conqueror	10.2625
Delil1	C:/Documents and Settings/Türker/Desktop/SONER YALÇIN/TMT.doc	soner	soner	Conqueror	10.2625
Delil1	D:/Yedek/desktop/AÇIL SUSAM AÇIL/snrylcn/Düello.doc	soner	soner	Conqueror	10.2625
Delil3	C:/Users/user/Documents/Ulusal Medya 2010.doc	pc	soner		10.2605
Delil3	C:/Users/user/Documents/Hanefi.doc	soner	soner	Conqueror	10.2605

Tablo 15 - Ofis son değiştiren isminin "soner" olduğu diğer dokümanlar

Ofis kullanıcısı "Barış"

Ofis kullanıcısı "Barış"'ın yazar alanında geçtiği dokümanlar:

Delil	Dosya	Yazar	Son Değiştiren	Şirket	Uygulama Versiyonu
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/çetinkayas.doc	Barış	Sys		11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/haber/muro.doc	Barış	Sys		11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/başbuğ.doc	Barış	Sys		11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/başbuğs.doc	Barış	Sys		11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/başbuğss.doc	Barış	AEC		12.0000
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/Masaustu/masaüstü/açılım.doc	Barış	Sys		11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/Masaustu/masaüstü/üçok.doc	Barış	Barış		11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/Masaustu/masaüstü/tigran.doc	Barış	Sys		11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/Masaustu/masaüstü/haber sen.doc	Barış	Sys		11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/ORADAYDIM/müjdat gezen g.ç.doc	Barış	Sys		11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/temizlenecek/Yeni Microsoft Word Belgesi.doc	Barış	Sys		11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/temizlenecek/dilekçe.doc	Barış	Sys		11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/temizlenecek/sahinnn(1).doc	Barış	Sys		11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/temizlenecek/sahinnn.doc	Barış	Sys		11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/temizlenecek/aysel+g.ç.doc	Barış	Sys		11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/temizlenecek/kemaltürklerrr.doc	Barış	Sys		11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/temizlenecek/Rutkay Aziz g.ç.doc	Barış	Sys		11.5606

Delil2	C:/Documents and Settings/Barış/Local Settings/Temporary Internet Files/OLK4/Yeni Microsoft Word Belgesi.doc	Barış	Barış	11.5606
Delil2	D:/BARIS YEDEK 11122009/DEKSTOP/BARIŞ/alevi.doc	Barış	Barış	11.5606
Delil2	D:/BARIS YEDEK 11122009/DEKSTOP/BARIŞ/haber/muro.doc	Barış	Sys	11.5606

Tablo 16 - Ofis yazar isminin "soner" olduğu diğer dokümanlar

Ofis kullanıcısı "Barış"'ın "son değiştiren" alanında geçtiği dokümanlar:

Delil	Dosya	Yazar	Son Değiştiren	Şirket	Uygulama Versiyonu
Delil 1	C:/Documents and Settings/Türker/Desktop/ODATV/haber/DOKSANBEŞ OZAN.doc	Sys	Barış		11.5606
Delil 1	C:/Documents and Settings/Türker/Desktop/ODATV/haber/FAKİR BAYKURT haberi.doc	new	Barış		11.5606
Delil 1	C:/Documents and Settings/Türker/Desktop/ODATV/Masaustu/masaüstü/üçok.doc	Barış	Barış		11.5606
Delil 1	C:/Documents and Settings/Türker/Desktop/ODATV/bektaş.doc	Celal ÜLGEN	Barış	Av. Celal Ülgen	11.5606
Delil 1	C:/Documents and Settings/Türker/Desktop/temizlenecek/_Ne.doc	Ahmet Mümtaz İDİL	Barış	AYDA Optik	11.5606
Delil 2	C:/Documents and Settings/Barış/Local Settings/Temporary Internet Files/OLK4/soner pazar.doc	user	Barış		11.5606
Delil 2	C:/Documents and Settings/Barış/Local Settings/Temporary Internet Files/OLK4/Yeni Microsoft Word Belgesi.doc	Barış	Barış		11.5606
Delil 2	D:/BARIS YEDEK 11122009/DEKSTOP/BARIŞ/alevi.doc	Barış	Barış		11.5606
Delil 2	D:/BARIS YEDEK 11122009/DEKSTOP/BARIŞ/haber/DOKSANBEŞ OZAN.doc	Sys	Barış		11.5606
Delil 2	D:/BARIS YEDEK 11122009/DEKSTOP/BARIŞ/haber/FAKİR BAYKURT haberi.doc	new	Barış		11.5606

Tablo 17 - Ofis son değiştiren kullanıcı isminin "soner" olduğu diğer dokümanlar

Ofis kullanıcısı "pc"

Ofis kullanıcısı "pc"'nin yazar alanında geçtiği dokümanlar:

Delil	Dosya	Yazar	Son Değiştiren	Şirket	Uygulama Versiyonu
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/Hareket 2023.doc	pc	Ahmet Mümtaz İDİL		12.0000
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/Madımak.doc	pc	Sys		11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/altioklar.doc	pc	pc		10.2625
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/ibrahim.doc	pc	Baris		11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/phelpls-bolt.doc	pc	Baris		11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/baydar.doc	pc	pc		10.2625
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/Goody.doc	pc	Ahmet Mümtaz İDİL		12.0000
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/osmanli cumhuriyeti.doc	pc	pc		10.2625
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/son bulusma.doc	pc	Baris		11.9999
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/Icisleri Bakanligi'na Basvuru FD-YA.doc	pc	User		11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/TS.doc	pc	Ahmet Mümtaz İDİL		12.0000
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/şefaat.doc	pc	Sys		11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/Kamil Park.doc	pc	Ahmet Mümtaz İDİL		12.0000
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/Masaustu/masaüstü/odatv-taraf.doc	pc	pc		10.2625
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/Masaustu/masaüstü/haftasonu ekler/odatv-kitap.doc	pc	pc		10.2625
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/Masaustu/masaüstü/haftasonu	pc	pc		10.2625

	ekler/spotlar.doc			
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/odatv-kusturica.doc	pc	pc	10.2625
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/5888.doc	pc	Sys	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/YENİ CV/CVLER/Yeliz Karakütük-Özgeçmiş.doc	pc	Baris	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/temizlenecek/AVRASYA+İ...doc	pc	Sys	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/temizlenecek/MEB-Yeni.doc	pc	Sys	11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/temizlenecek/MEB.doc	pc	Ahmet Mümtaz İDİL	12.0000
Delil1	C:/Documents and Settings/Türker/Desktop/temizlenecek/KİM.doc	pc	user	12.0000
Delil1	C:/Documents and Settings/Türker/Desktop/temizlenecek/Anayasa Mahkemesi.doc	pc	Sys	11.5606
Delil2	D:/BARIS YEDEK 11122009/DEKSTOP/BARIŞ/haftasonu/haftasonu ekler/odatv-kitap.doc	pc	pc	10.2625
Delil2	D:/BARIS YEDEK 11122009/DEKSTOP/BARIŞ/haftasonu/haftasonu ekler/spotlar.doc	pc	pc	10.2625
Delil2	D:/BARIS YEDEK 11122009/DEKSTOP/BARIŞ/odatv-kitap.doc	pc	YTU	11.9999
Delil2	D:/BARIS YEDEK 11122009/DEKSTOP/BARIŞ/sonbahar.doc	pc	YTU	11.9999
Delil2	D:/BARIS YEDEK 11122009/DEKSTOP/BARIŞ/spotlar.doc	pc	pc	10.2625
Delil3	C:/Users/user/Documents/Ulusal Medya 2010.doc	pc	soner	10.2605
Delil3	C:/Users/user/Documents/yedek belgeler/KAYNAKÇA.doc	pc	pc	10.2625
Delil3	C:/Users/user/Documents/yedek belgeler/PATRİKHANE VE 551 YILLIK HESAP.doc	pc	ILIM	10.2625
Delil3	C:/Users/user/Documents/yedek belgeler/İÇİNDEKİLER.doc	pc	pc	10.2625

Tablo 18 - Ofis yazar isminin "pc" olduğu diğer dokümanlar

Ofis kullanıcısı "pc"'nin "son değiştiren" alanında geçtiği dokümanlar:

Delil	Dosya	Yazar	Son Değiştiren	Şirket	Uygulama Versiyonu
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/altioklar.doc	pc	pc		10.2625
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/baydar.doc	pc	pc		10.2625
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/osmanli cumhuriyeti.doc	pc	pc		10.2625
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/Masaustu/masaüstü/odatv-taraf.doc	pc	pc		10.2625
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/Masaustu/masaüstü/haftasonu ekler/odatv-kitap.doc	pc	pc		10.2625
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/Masaustu/masaüstü/haftasonu ekler/spotlar.doc	pc	pc		10.2625
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/odatv-kusturica.doc	pc	pc		10.2625
Delil2	D:/BARIS YEDEK 11122009/DEKSTOP/BARIŞ/haftasonu/haftasonu ekler/odatv-kitap.doc	pc	pc		10.2625
Delil2	D:/BARIS YEDEK 11122009/DEKSTOP/BARIŞ/haftasonu/haftasonu ekler/spotlar.doc	pc	pc		10.2625
Delil2	D:/BARIS YEDEK 11122009/DEKSTOP/BARIŞ/spotlar.doc	pc	pc		10.2625
Delil3	C:/Users/user/Documents/yedek belgeler/Giriş-sonuç-istanbul.doc	Noname	pc		10.2625
Delil3	C:/Users/user/Documents/yedek belgeler/Hedef Kent İstanbul.doc	Noname	pc		10.2625
Delil3	C:/Users/user/Documents/yedek belgeler/KAYNAKÇA.doc	pc	pc		10.2625
Delil3	C:/Users/user/Documents/yedek belgeler/SS-İSTANBUL-KİTAP1.doc	Noname	pc		10.2625

Delil3	C:/Users/user/Documents/yedek belgeler/İSTANBUL-KİTAP.doc	Nonam e	pc	10.2625
Delil3	C:/Users/user/Documents/yedek belgeler/İÇİNDEKİLER-istanbul.doc	Nonam e	pc	10.2625
Delil3	C:/Users/user/Documents/yedek belgeler/İÇİNDEKİLER.doc	pc	pc	10.2625

Tablo 19 - Ofis son değiştiren kullanıcı isminin "pc" olduğu diğer dokümanlar

Ofis kullanıcısı "Your User Name"

Ofis kullanıcısı "Your User Name"'in yazar alanında geçtiği dokümanlar:

Delil	Dosya	Yazar	Son Değiştiren	Şirket	Uygulama Versiyonu
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/fet.doc	Your User Name	Sys		11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/soner 5 eylul pazar.doc	Your User Name	Sys		11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/KRİZDE DOLMABAHÇE ETKİSİ VAR MI.doc	Your User Name	Your User Name		12.0000
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/Meral Tamer.doc	Your User Name	Sys		11.5606
Delil1	C:/Documents and Settings/Türker/Desktop/ORADAYDIM/yeni/(E)Tbp. TuÃ°gn.Nihat ÃLHAN.doc	Your User Name	Your User Name		11.6360
Delil2	C:/Documents and Settings/Barış/Local Settings/Temp/son yazışma hakkında.doc	Your User Name	Your User Name		12.0000
Delil2	D:/aysel silme/oradaydım/yeni/(E)TBP~1.DOC	Your User Name	Your User Name		11.6360

Tablo 20 - Ofis yazar kullanıcı isminin "Your User Name" olduğu diğer dokümanlar

Ofis kullanıcısı "Your User Name"'in "son değiştiren" alanında geçtiği dokümanlar:

Delil	Dosya	Yazar	Son Değiştiren	Şirket	Uygulama Versiyonu
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/KRİZDE DOLMABAHÇE ETKİSİ VAR MI.doc	Your User Name	Your User Name		12.0000
Delil1	C:/Documents and Settings/Türker/Desktop/ODATV/doğandan.doc	ilknur	Your User Name		
Delil1	C:/Documents and Settings/Türker/Desktop/ORADAYDIM/yeni/(E)Tbp. TuÃ°gn.Nihat ÃLHAN.doc	Your User Name	Your User Name		11.6360
Delil1	C:/Documents and Settings/Türker/Local Settings/Temporary Internet Files/Content.IE5/SPQB81UN/ODATV TEKZIP.doc	xxx xxxx	Your User Name	privat	12.0000
Delil2	C:/Documents and Settings/Barış/Local Settings/Temp/son yazışma hakkında.doc	Your User Name	Your User Name		12.0000
Delil2	D:/aysel silme/oradaydım/yeni/(E)TBP~1.DOC	Your User Name	Your User Name		11.6360

Tablo 21 - Ofis son değiştiren kullanıcı isminin "Your User Name" olduğu diğer dokümanlar

EK-3

Delil1 deki EK-1 dosyalarının izleri

DOSYA İSMİ	$MFT KAYDI	$LOGFILE KAYDI	$USNJRNL KAYDI	DOSYA SİSTEMİ TARİH BİLGİLERİ	DOSYA İÇ META VERİLERİ	SİLİNMİŞ Mİ?
000KITAP.docx	X	X		X	X	X
ABDULKADIR AYGAN.pdf	X	X		X	X	X
Bilinçlendirme.doc	X	X		X	X	X
CHP.doc		X			X	X
EK-D MiLi EĞİTİM.doc		X			X	X
EK-E AKP'NİNATAMALARI.xls		X			X	X
Ermeni Dosyası.doc	X	X		X	X	X
Fabrikatör.doc	X	X		X	X	X
Hanefi.doc	X	X		X	X	X
Kadrolasma Bilgi Notu (Ocxak 2004).doc		X			X	X
KADROLASMA EK-A.doc		X				X
KADROLASMA EK-C.doc		X				X
Kadrolasma en son 0610170003.doc		X			X	X
KADROLASMA KONUSMA NOTU(OCAK 2004).doc		X			X	X
Konusma Notu.doc		X			X	X
Koz.doc	X	X		X	X	X
mafia.doc	X	X		X	X	X
mit medya.doc	X	X		X	X	X
Nedim.doc	X	X		X	X	X
panzehir.doc	X	X		X	X	X
prj_60.doc		X			X	X
radikal dini grupların faaliyet alanları.pdf	X	X		X	X	X
Reosta Operasyonu.doc	X	X		X	X	X
Sabri Uzun.doc	X	X		X	X	X
simon son.doc		X		X*	X	X
Sn. Komutanım.doc	X	X		X	X	X
SY.doc		X			X	X
teRTEemiz.doc	X	X		X	X	X
toplantı.doc	X	X		X	X	X
TRT.doc						
Tv Analiz Proje.doc	X	X		X	X	X
Ulusal Medya 2010.doc	X	X		X	X	X
Ulusal Medya.doc	X	X		X	X	X
Yalçın hoca.doc		X			X	X
YBelgesi.doc	X	X		X	X	X

X* : Bir kısmı elde edilebilen veriler

Delil2 deki EK-1 dosyalarının izleri

DOSYA İSMİ	$MFT KAYDI	$LOGFILE KAYDI	$USNJRNL KAYDI	DOSYA SİSTEMİ TARİH BİLGİLERİ	DOSYA İÇ META VERİLERİ	SİLİNMİŞ Mİ?
000KITAP.docx						
ABDULKADIR AYGAN.pdf						
Bilinçlendirme.doc		X		X*		X
CHP.doc				X		X
EK-D MiLi EĞİTİM.doc	X	X		X		X
EK-EAKP'NİN ATAMALARI.xls	X	X		X		X
Ermeni Dosyası.doc						
Fabrikatör.doc						
Hanefi.doc						
Kadrolasma Bilgi Notu (Ocxak 2004).doc	X	X		X		X
KADROLASMA EK-A.doc	X	X		X		X
KADROLASMA EK-C.doc	X	X		X		X
Kadrolasma en son 0610170003.doc	X	X		X		X
KADROLASMA KONUSMA NOTU(OCAK 2004).doc	X	X		X		X
Konusma Notu.doc	X	X		X		X
Koz.doc						
mafia.doc						
mit medya.doc						
Nedim.doc						
panzehir.doc						
prj_60.doc		X		X*		X
radikal dini grupların faaliyet alanları.pdf						
Reosta Operasyonu.doc						
Sabri Uzun.doc						
simon son.doc						
Sn. Komutanım.doc		X		X*		X
SY.doc		X		X*		X
teRTEemiz.doc		X		X*		X
toplantı.doc						
TRT.doc						
Tv Analiz Proje.doc						
Ulusal Medya 2010.doc		X		X*		X
Ulusal Medya.doc						
Yalçın hoca.doc		X		X*		X
YBelgesi.doc						

X* : Bir kısmı elde edilebilen veriler

Delil3 deki EK-1 dosyalarının izleri

DOSYA İSMİ	$MFT KAYDI	$LOGFILE KAYDI	$USNJRNL KAYDI	DOSYA SİSTEMİ TARİH BİLGİLERİ	DOSYA İÇ META VERİLERİ	SİLİNMİŞ Mİ?
000KITAP.docx						
ABDULKADIR AYGAN.pdf						
Bilinçlendirme.doc						
CHP.doc						
EK-D MiLi EĞİTİM.doc						
EK-EAKP'NİN ATAMALARI.xls						
Ermeni Dosyası.doc						
Fabrikatör.doc						
Hanefi.doc	X			X	X	
Kadrolasma Bilgi Notu (Ocxak 2004).doc						
KADROLASMA EK-A.doc						
KADROLASMA EK-C.doc						
Kadrolasma en son 0610170003.doc						
KADROLASMA KONUSMA NOTU(OCAK 2004).doc						
Konusma Notu.doc						
Koz.doc						
mafia.doc						
mit medya.doc						
Nedim.doc						
panzehir.doc						
prj_60.doc						
radikal dini grupların faaliyet alanları.pdf						
Reosta Operasyonu.doc						
Sabri Uzun.doc						
simon son.doc						
Sn. Komutanım.doc						
SY.doc	X			X	X	
teRTEemiz.doc						
toplantı.doc						
TRT.doc						
Tv Analiz Proje.doc						
Ulusal Medya 2010.doc	X			X	X	
Ulusal Medya.doc						
Yalçın hoca.doc	X			X	X	
YBelgesi.doc						