18/02/2013

Sayın Av. İhsan Nuri Tezel,

Konu: T.C. İstanbul 12. Ağır Ceza Mahkemesi'nde 2010/34 esas numarasıyla görülen davayı ilgilendiren, 5 numaralı sabit diskin son kullanılma tarihinden sonra kaydedildiği tespit edilen dosyalar

Tarafınızca talep edilen inceleme isteklerine istinaden değerlendirilen deliller üzerinde yapılan çalışmada geri tarihli işlemlere rastlanmış, bunların bir bölümü tam olarak tespit edilmiş, bir bölümü ise şüphe olarak değerlendirilmişti.

Teknik olanaklardaki gelişmeyle yapılan ek çalışma sonucunda tespit edilen söz konusu geri tarihli işlemler ayrıştırılmış, aşağıdaki özet rapor ve ek liste ile sunulmuştur.

Bu araştırmada dosyaların NTFS MFT girdileri, öbek kullanım sıra numaraları ve NTFS $LogFile girdileri incelenmiştir.

Adli Bilirkişi
Tevfik Koray Peksayar

Makine Mühendisliği Lisans
Bilgi Teknolojileri Yüksek Lisans
(İTÜ Diploma No: 76 – 387)

1. NTFS DOSYA SİSTEMLERİNDE ANA DOSYA TABLOSU (MFT)

Bir dosya sistemi, üzerine kaydedilecek dosyaların düzenli olarak depolanmasını ve kolay erişim sağlanmasını amaçlar.

NTFS dosya sistemlerinde dosyalar öbek (İng.: cluster) tabir edilen yapılarla saklanır.

Öbeklerin boyutları sabittir ve bir disk ilk kez kullanıma hazırlandığında (formatlandığında) diskin toplam boyutuna göre dosyalara en uygun erişim ve sistem başarımının sağlanması için önceden belirlenir.

Dosyalar disk üzerinde bu öbeklere parçalanarak depolanır. Bilgisayarlarda tüm işlemlerin 2'li sayı sistemi ile yapılmasından dolayı bir dosyanın kapladığı öbek sayısı her zaman tam sayıdır.

Örneğin 5.3 kilobayt boyutunda bir dosya 4 kilobayt boyutunda öbek tanımı olan bir FAT dosya sisteminde 2 öbekle depolanır. Diğer bir deyişle dosya disk üzerinde 8 kilobayt yer kaplar.

Öbekler disk üzerinde serbestçe yerleştirilebilir, disk üzerinde yer alan bir öbekten sonra gelen öbeğin bir önceki öbeğin depoladığı dosya parçasını içeriyor olması şart değildir.

Ana dosya tablosu (İng.: master file table / İng. Kıs.: MFT) ya da dosya yerleşim tablosu, öbekler hakkında bilginin depolandığı yapıdır. Dosya yerleşim tablosunda her öbeğin nasıl kullanıldığı hakkında girdi depolanır. Bu girdilerle işletim sistemine dosyaların depolandığı öbeklerin numaraları, diskin hangi bölümlerinin dosyalar tarafından kullanıldığını ve hangi bölümlerinin kullanım için serbest olduğu bilgisi sağlanır.

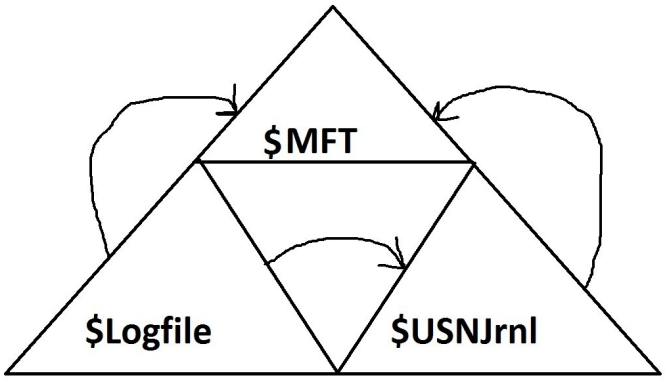
Bu dosya yerleşim tablosu girdileri, işletim sistemi tarafından kullanılarak öbeklere zincir şeklinde erişilip dosyaların okunmasını sağlar. İşletim sistemi bir dosyanın ard arda hangi öbeklerde depolandığını dosya yerleşim tablosundan öğrenip öbekleri sırayla okuyarak depolanmış dosyaya erişir.

Öbekler disk üzerine rastgele yazılmalarına rağmen dosya yerleşim tablosunda öbeklerin numaralanması her zaman birbirini takip eder.

MFT girdileri dosya oluşturulma tarihleriyle uyumluluk içinde sayıları ardışık olarak artarak birbirini takip ederler.

Bu girdi numaraları takip edilerek hangi dosyanın hangisinden sonra oluşturulduğu kolaylıkla belirlenebilir. Dolayısıyla, dosyaların işlem tarihlerinden bağımsız olarak bu girdi numaralarından kayıt sıraları kolayca tespit edilebilir.

$LogFile adlı sistem dosyası bu girdilerin işlem sırasını depolamakta, bu işlemleri, eğer işletim sisteminde etkinleştirilmişse, $USNJrnl adlı jurnal dosyasına da yazmaktadır.



Dosya sisteminde olası bir sorunda, başarısız işlemler $LogFile, $USNJrnl dosyası ve MFT ile kıyaslanarak başarısız işlemin doğru olarak gerçekleştirilmesine çalışılır.

$LogFile'da sıra numaraları kullanılarak, sürücü üzerinde yapılan dosya işlemlerinin kaydı tutulur.

Yukarıda da anlatıldığı üzere, disk üzerine yeni dosyalar kaydedildikçe MFT girdi numaraları artmaktadır. Bu girdiler üzerinde yapılan değişiklikler ise $LogFile sıra numaralarında artış olarak görünmektedir.

Böylece, MFT girdi numaraları ve $LogFile sıra numaraları takip edilerek dosya kayıt işlemlerinin ayrıntısına ulaşmak kolaylaşır.

Disk üzerinde yer kalmayınca ve dosya sistemi üzerinde tanımlanabilecek dosya sayısının sonuna ulaşılmışsa daha önce silinmiş olan girdi numaraları ve dosyaların kapladığı öbekler kullanılmaya başlanır.

NTFS dosya sistemi yerleşim tablosunda en çok 4,294,967,295 (dört milyon iki yüz doksan dört bin iki yüz doksan beş) dosya tanımlanabilir.

2. 5 NUMARALI SABİT DİSKİN ÖZET MFT İNCELEMESİ

2.1. C: Sürücüsü

5 numaralı sabit diskin C: sürücüsünün sığası yaklaşık 21 gigabayt olarak ayrılmıştır. Bu sığanın yaklaşık 5 gigabaytlık alanı kullanılmıştır ve yaklaşık 16 gigabaytlık alan boştur.

5 numaralı sabit diskin C: sürücüsünde 19,798 (on dokuz bin yedi yüz doksan sekiz) dosya ve 1475 (bin dört yüz yetmiş beş) dizin kayıtlıdır.

Bu durum, depolanması istenen dosyalar için boş alanın yaklaşık %76 olduğunu ve yeni kaydedilecek dosyaların silinmiş dosyalara ait eski MFT girdilerinin kullanılması gerekmeden depolanabileceklerini göstermektedir.

Bu bulgu ışığında, MFT girdilerinin ardışık olarak numaralandırılarak yeni kaydedilecek dosyaların bu numaraları takip edecek şekilde C: sürücüsü'nün dosya tablosunda temsil edilmeleri normal olan durumdur.

5 numaralı sabit diskin 1. bölümü olan C: sürücüsünde bulunan virüs, diskin takılı olduğu sistemin başka bir sistemden her işleviyle kontrol edilmesine olanak sağladığı düşünülmektedir.

Virüsün çalıştığı sisteme işletim sistemi özellikleri ve işletim sistemi müdahalesi dışında kalan, sistem seviyesinde dosya kopyalama dahil, işlemler yaptırabileceği tespit edilmiştir.

r6r.exe bulaştığı sürücü her okunduğunda, kök dizinde bulunan autorun.inf dosyası ile çalışmasını garantilemektedir.

r6r.exe sisteme bulaştığında, sistem kayıt defterine herhangi bir dizine her girilişte kendisini çalıştıracak şekilde bir kayıt yazmaktadır. Ayrıca sistem üzerinde çalışmasının devamlılığını sağlamak için kendisinin kopyasını çıkarmaktadır.

C: sürücüsündeki girdilerin tarihleri incelendiğinde dosya yerleşim tablosundaki 13432 numaralı girdi göze çarpmaktadır. Bu girdinin r6r.exe adlı virüs dosyasına işaret ettiği görülmektedir.

13432 numaralı girdiye göre dosya verisindeki son değişiklik, diğer bir deyişle ilk oluşturulduğu tarih, 11/05/2008 07:54:36'yı göstermektedir. Bu dosyanın diskte oluştuğu tarih ise 18/09/2008 17:44:08'i göstermektedir.

Fakat 13432 numaralı girdinin diskte son değişikliğe uğradığı tarih oluşturulma tarihinden geride ve 18/08/2004 08:00:50'dir.

Bu dosya girdisinin ardışık sıra numarasının (İng.: sequence number) 83 olduğu tespit edilmektedir. Bu bulgu, söz konusu girdinin 83 kez işlem gördüğünü göstermektedir.

Yapılan incelemede bu virüslü dosyanın aynı ilk oluşma ve diskte oluşma tarihini gösterecek şekilde, fakat diskte son değişiklik zamanı farklı olarak defalarca otomatik yedeğinin alındığı görülmektedir.

Bu bilgiler ve yukarıdaki bulgular ışığında, söz konusu virüsün C: sürücüsünde, kendisinin 18/08/2004 tarihini ve 08:00:50 saatini gösterecek şekilde bir kopyasını oluşturduğu anlaşılmaktadır.

Dolayısıyla, 5 numaralı sabit diske 18/09/2008 tarihinden sonra, sistem saati geri alınmış bir bilgisayar kullanılarak dosya kopyalandığı anlaşılmaktadır.

Bu kopyalama işleminin yapıldığı gerçek zamanı tespit etmek mümkün değildir.

C: sürücüsündeki 13432 numaralı girdinin son erişim tarihi 28/07/2009 11:09:34'tür. Bu tarih sistemin en son kullanıldığı tarihi göstermektedir.

Bu girdiden sonraki girdiler arasında son erişim tarihi 28/07/2009'u gösteren birçok girdi mevuttur.

Geri tarihli kopyalama işlemi sırasında, diskin takıldığı bilgisayarın sistem saatinin virüsün ilk oluşturulduğu tarihten geri bir tarihi göstermesi sebebiyle virüsün kendisinin kopyasını tekrar yazdığı ve girdinin gösterdiği dosyanın disk üzerinde değiştiği anlaşılmaktadır.

Ancak, bu tekrar yazma işlemi sırasında C: sürücüsüne kullanıcı erişimi yapılmadığı, olayın sistem seviyesinde ve kullanıcı farkındalığı dışında oluşması dolayısıyla, girdinin son erişim tarihinin değişmediği anlaşılmaktadır.

2.2. D: Sürücüsü

5 numaralı sabit diskin D: sürücüsünün sığası yaklaşık 55 gigabayt olarak ayrılmıştır. Bu sığanın yaklaşık 2.5 gigabaytlık alanı kullanılmıştır ve yaklaşık 53 gigabaytlık alan boştur.

5 numaralı sabit diskin D: sürücüsünde 3,889 (üç bin sekiz yüz seksen dokuz) dosya ve 442 (dört yüz kırk iki) dizin kayıtlıdır.

Bu durum, depolanması istenen dosyalar için boş alanın yaklaşık %95 olduğunu ve yeni kaydedilen dosyaların silinmiş dosyalara ait eski MFT girdilerinin kullanılması gerekmeden depolanabileceklerini göstermektedir.

Bu bulgu ışığında, MFT girdilerinin ardışık olarak numaralandırılarak yeni kaydedilecek dosyaların bu numaraları takip edecek şekilde D: sürücüsünün dosya tablosunda temsil edilmeleri normal olan durumdur.

Diğer bir deyişle, dosyaları temsil eden MFT girdi numaralarının dosya kayıt tarihiyle doğru orantılı olarak artması normal olan durumdur.

D: sürücüsü tarih - MFT girdisi tutarlılığı açısından incelendiğinde ilk göze çarpan r6r.exe dosyasına işaret eden 2480 numaralı girdidir.

2480 numaralı MFT girdisinin ayrıntılarına bakıldığında aşağıdaki tarih özellikleri tespit edilmektedir:

Tarih	İşlem	Boyut
08/04/2004 19:34:17	Dosyanın diskteki durumunda değişiklik	104253 bayt
11/05/2008 07:54:36	Dosya verisinde değişiklik	104253 bayt
18/09/2008 17:44:09	Dosyanın diskte oluşması	104253 bayt
28/07/2009 11:09:34	Dosyaya erişim	104253 bayt

Bu tarih özellikleri incelendiğinde dosyanın diskteki değişiminin oluşturulma tarihinden önce olduğu, yani diskte geri tarihli bir işlem sonucu virüslü dosyanın kendisini tekrar yazdığı görülmektedir.

08/04/2004 tarihine bakıldığında, bu tarihi gösteren 132 MFT girdisinin bulunduğu görülmektedir. Bu girdiler incelendiğinde, D: sürücüsüne sistem saati geri alınmış bir bilgisayar kullanılarak geri tarihli işlemlerle dosyalar kopyalandığı anlaşılmaktadır.

2480 numaralı dosya girdisinin ardışık sıra numarasının (İng.: sequence number) 564 olduğu tespit edilmektedir. Bu bulgu, söz konusu girdinin 564 kez işlem gördüğünü göstermektedir.

Geri tarihli kopyalama işlemi sırasında, diskin takıldığı bilgisayarın sistem saatinin virüsün ilk oluşturulduğu tarihten geri bir tarihi göstermesi sebebiyle virüsün kendisinin kopyasını tekrar yazdığı ve girdinin gösterdiği dosyanın disk üzerinde değiştiği anlaşılmaktadır.

Normal şartlarda, virüs bulaşması sonucunda etkilenen sistemler üzerindeki virüslü dosyaların tarihleri geri tarihleri gösterecek şekilde değişmez ve virüsler temizlenemedikleri durumda kendilerini tekrar diske yazarlar.

D: sürücüsünde sadece 2480 numaralı girdi r6r.exe'ye işaret etmektedir.

Bu bulgu, virüsün bir anti-virüs tarafından temizlenemediğini ve virüsün 564 kez kendisini yenilediğini göstermektedir.

Bu yenileme işlemlerinin sebebinin birden fazla tarih değişikliği içeren işlem yapılması olduğu düşünülmektedir.

2480 numaralı girdinin $LogFile'da kayıtlı sıra numarası 2,619,648,723 olarak belirlenmektedir.

Bir sonraki, 2481 numaralı girdi, yine virüs tarafından oluşturulan, her dosya işlemi sonrası yenilenen, autorun.inf dosyasını temsil etmektedir.

2481 numaralı MFT girdisinin ayrıntılarına bakıldığında aşağıdaki tarih özellikleri tespit edilmektedir:

Tarih	İşlem	Boyut
18/09/2008 17:44:09	Dosyanın diskte oluşması	541 bayt
28/07/2009 11:09:35	Dosya verisinde değişiklik Dosyanın diskteki durumunda değişiklik Dosyaya erişim	541 bayt

2481 numaralı girdinin $LogFile'da kayıtlı sıra numarası 2,618,903,679 olarak belirlenmektedir.

2481 numaralı dosya girdisinin ardışık sıra numarasının 866 olduğu tespit edilmektedir.

Bu bulgu, söz konusu girdinin 866 kez işlem gördüğünü göstermektedir.

Bu bulgu, autorun.inf dosyasının 866 kez yenilediğini, diğer bir deyişle, D: sürücüsünde disk üzerinde en az 866 dosya işlemi yapıldığını göstermektedir.

Bu iki girdi incelendiğinde, 28/07/2009 11:09:35 tarihinden sonra, 08/04/2004 19:34:17 değişiklik tarihini gösterecek şekilde dosya işlemi yapıldığı ve bu dosya işleminden sonraki virüs etkinliği dolayısıyla 2,619,648,723 numaralı $LogFile kaydının diske yazıldığı görülmektedir.

Ancak, D: sürücüsündeki son MFT girdisi 4384 numaralı girdidir ve "İKK/Amiral Listesi1.xls" dosyasına işaret etmektedir.

4384 numaralı MFT girdisinin ayrıntılarına bakıldığında aşağıdaki tarih özellikleri tespit edilmektedir:

Tarih	**İşlem**	**Boyut**
17/10/2002 18:45:07	Dosya verisinde değişiklik	48128 bayt
08/04/2004 19:36:50	Dosyanın diskte oluşması Dosyanın diskteki durumunda değişiklik Dosyaya erişim	48128 bayt

4384 numaralı girdinin $LogFile sıra numarası 2,619,721,224 olarak belirlenmektedir.

08/04/2004 tarihli bir dosyanın sürücüdeki en son MFT kaydına sahip olması teknik olarak saati geri alınmış bir sistemle dosya kopyalandığı anlamını taşımaktadır.

4384 numaralı girdinin işaret ettiği "İKK/Amiral Listesi1.xls" dosyası incelendiğinde bu dosyanın sahiplik bilgisisinin BUILTIN\Administrators olduğu görülmektedir.

Bu bulgu dosyanın diskin sökülüp başka bir bilgisayara takılıp kopyalanarak oluşturulduğunu göstermektedir.

Söz konusu dosyanın $LogFile sıra numarasının 28/07/2009 tarihinde oluşturulan dosyalardan büyük olması da bu bulguyu doğrulamaktadır.

4384 numaralı girdinin işaret ettiği "İKK/Amiral Listesi1.xls" dosyasının D: sürücüsüne sistem saati geri alınmış bir bilgisayar kullanılarak geri tarihli işlemlerle oluşturulan 132 girdiden biri olduğu anlaşılmaktadır.

D: sürücüsünde tarih ve tarih-MFT kaydı uyumluluğu açısından son işlem gören girdi 2976 MFT girdi numarasına sahip "System Volume Information/_restore{3D63EA63-1173-413D-9F74-AB1925127957}/RP303" adlı otomatik sistem geri yükleme dizini olarak görülmektedir.

2976 numaralı MFT girdisidinin ayrıntılarına bakıldığında aşağıdaki tarih özellikleri tespit edilmektedir:

Tarih	**İşlem**	**Boyut**
27/07/2009 09:38:21	Dosyanın diskte oluşması	56 bayt
28/07/2009 11:05:20	Dosya verisinde değişiklik Dosyanın diskteki durumunda değişiklik Dosyaya erişim	56 bayt

2976 numaralı girdinin $LogFile'da kayıtlı sıra numarası 2,618,870,490 olarak belirlenmektedir.

D: sürücüsünde tarih-MFT kaydı uyumluluğu açısından bir önceki işlem gören girdi 2978 MFT girdi numarasına sahip "System Volume Information/_restore{3D63EA63-1173-413D-9F74-AB1925127957}/RP303/change.log.1" adlı otomatik sistem geri yükleme günlük dosyası görülmektedir.

2978 numaralı MFT girdisinin ayrıntılarına bakıldığında aşağıdaki tarih özellikleri tespit edilmektedir:

Tarih	**İşlem**	**Boyut**
27/07/2009 09:38:21	Dosyanın diskte oluşması	472288 bayt
27/07/2009 18:02:19	Dosya verisinde değişiklik Dosyaya erişim	472288 bayt
28/07/2009 09:12:55	Dosyanın diskteki durumunda değişiklik	472288 bayt

2978 numaralı girdinin $LogFile'da kayıtlı sıra numarası 2,618,218,083 olarak belirlenmektedir.

Otomatik sistem geri yükleme günlük dosyaları gibi dosyalar kullanıcı müdahalesi dışında, işletim sistemi tarafından oluşturulmakta ve değiştirilmektedir.

Dolayısıyla bu tür dosyalar da, virüslü dosyalarda olduğu gibi, disk üzerinde yapılan işlemlerin tespitini kolaylaştırmaktadır.

Yukarıdaki MFT ve $LogFile girdileri incelendiğinde özetle;

1. D: sürücüsüne son kaydedilen "İKK/Amiral Listesi1.xls" dosyasıdır.
2. "İKK/Amiral Listesi1.xls" dosyası 4384 numaralı MFT girdisiyle temsil edilmektedir.
3. "İKK/Amiral Listesi1.xls" dosyasının $LogFile girdisi 2,619,721,224 olarak belirlenmektedir.
4. D: sürücüsünde bulunan virüslü dosya olan r6r.exe dosyası sadece 2480 numaralı girdiyle temsil edilmektedir.
5. r6r.exe dosyasının $LogFile'da kayıtlı sıra numarası 2,619,648,723 olarak belirlenmektedir.
6. D: sürücüsünde tarih ve tarih-MFT kaydı uyumu açısından son işlem gören dosya "System Volume Information/_restore{3D63EA63-1173-413D-9F74-AB1925127957}/RP303" adlı otomatik sistem geri yükleme günlük dizinidir.
7. "System Volume Information/_restore{3D63EA63-1173-413D-9F74-AB1925127957}/RP303" dosyası 2976 MFT girdi numarasıyla temsil edilmektedir.
8. "System Volume Information/_restore{3D63EA63-1173-413D-9F74-AB1925127957}/RP303" dizininin $LogFile'da kayıtlı sıra numarası 2,618,870,490 olarak belirlenmektedir.

Bu bulgulara göre;

1. Diskte en son 08/04/2004 19:34:17 tarihinde değişen r6r.exe dosyasının $LogFile sıra numarası, tarih ve tarih-MFT kaydı uyumu açısından son işlem gören dosyanın $LogFile sıra numarasından ileridedir.
2. r6r.exe dosyasının diskteki değişimi geri tarihlidir.
3. Diske son kaydedilen "İKK/Amiral Listesi1.xls" dosyasının diskte oluşturulması geri tarihlidir.

Bu sebeplerle;

1. "System Volume Information/_restore{3D63EA63-1173-413D-9F74-AB1925127957}/RP303" dizinini gösteren 2,618,870,490 $LogFile kayıt numarasından büyük olan $LogFile kayıt numarasına
2. "İKK/Amiral Listesi1.xls" dosyasını gösteren 2,619,721,224 $LogFile kayıt numarasından küçük olan $LogFile kayıt numarasına
3. "İKK/Amiral Listesi1.xls" dosyasını gösteren 2,619,721,224 $LogFile kayıt numarasından büyük olan $LogFile kayıt numarasına

sahip dosyaların geri tarihli işlemlerle diske yüklendiği anlaşılmaktadır.

Adli Bilirkişi
Tevfik Koray Peksayar

Makine Mühendisliği Lisans
Bilgi Teknolojileri Yüksek Lisans
(İTÜ Diploma No: 76 – 387)

Ek:
T.C. İstanbul 12. Ağır Ceza Mahkemesi'nde 2010/34 esas numarasıyla görülen davayı ilgilendiren dosyaların, 5 numaralı sabit diskin son kullanılma tarihinden sonra kaydedildiği tespit edilen dosyaların dökümü