Giriş Tarihi: 4.6.2017 15:17

FETÖ'nün dosya temizleme yöntemi deşifre edildi

İzmir'de, FETÖ kapsamında tutuklanan Mehmet Tabanca'nın bilgisayarında tespit edilen program, örgütün, yakalanan sözde üst düzey yöneticilerin elindeki gizli dosyaları nasıl kamufle ettiğini ve bunların silinmesini sağladığını ortaya koydu.

Fetullahçı Terör Örgütü'nün (FETÖ), yakalanan sözde üst düzey örgüt mensuplarına ait bilgisayarlardaki gizli dosyaların silinmesini ve cihazların yurt dışındaki sunucuya otomatik bağlanmasını sağlayan özel programı deşifre edildi. AA muhabirinin aldığı bilgiye göre, Aliağa Cumhuriyet Başsavcısı Adem Aydemir'in yürüttüğü FETÖ/PDY soruşturması kapsamında 30 Kasım 2016'da İzmir'in Bayraklı ilçesinde yakalanan ve çıkarıldığı mahkemece tutuklanan Mehmet Tabanca'ya ait akıllı telefon, dizüstü bilgisayar ve tablet incelenmeye alındı.

FETÖ elebaşı Fetullah Gülen ile aracısız görüştüğü ve terör örgütünün Türkiye'deki üst düzey isimlerinden olduğu belirtilen Tabanca'nın, ele geçirilen cihazlara ait şifreyi rahat tavırlarla vermesi,

bilgisayardaki şüpheleri daha da artırdı.

Başsavcı ve uzman ekip nezaretinde açılan dizüstü bilgisayarda, ana işletim sisteminin arka planında çalışan başka bir program olduğu fark edildi. Başka bir işletim sistemi içine gizlenen dosyaların bir anda silinmeye başladığını belirleyen ekipler, bilgisayarı kapattı.

Bilgisayar, daha sonra uydu bağlantısı kurulamayan, zemin kat altı, izole edilmiş ortamda IP'si sabitlenerek yeniden açıldı.

Bilişim uzmanları, zanlının verdiği şifrenin, bilgisayarın ana işletim sistemi altındaki başka bir yazılıma gizlenen dosyaları silmek için kullanılan ikinci bir kod olduğunu belirledi.

Bu çalışmayla, FETÖ'nün, yakalanan sözde üst düzey yöneticilerin elindeki gizli dosyaları nasıl kamufle ettiği ve bunların silinmesini sağladığı da anlaşıldı.

Dizüstü bilgisayar üzerindeki incelemede sistemin çalışmasına dair şu bilgilere ulaşıldı:

"Zanlının verdiği şifrenin girilmesiyle açılan dizüstü bilgisayar, en yakın kablosuz ağa şifresini kendiliğinden çözerek bağlanıyor. Daha sonra internet ortamında uzak sunucuya ulaşarak buradan aldığı IP ile işlemlerini sürdürüyor. Birinci şifresi zanlıda mevcut olan gizli dosyalar böylece otomatik olarak silinmeye başlıyor."

Silme işlemine başlamak için dizüstü bilgisayarın hangi ülkedeki uzak sunucuya bağlandığı da araştırılıyor.

Dizüstü bilgisayarda geriye dönük iz süren ekipler, örgüt hiyerarşisi ve işleyişiyle ilgili önemli belgelere ulaştı.

Cihazı tüm hafızası silinmeden kurtaran ekipler, örgütün 15 Temmuz darbe girişimi sonrası yapılanmasına ilişkin de önemli bilgiler elde etti.

EAGLE VE BYLOCK KULLANDIĞI BELİRTİLİYOR

Mehmet Tabanca'nın örgütün gizli haberleşme programları Eagle ve ByLock'u da kullandığı belirtildi.

Zanlıya ait diğer dijital cihazlarda da hazırlanan ikinci şifreyle onaylanan özel programla tüm bilgileri geri getirilemeyecek şekilde silen başka program saptandığı öğrenildi.

Titiz çalışmayla ortaya çıkarılan ikinci şifre bilgi silme yöntemiyle örgütün, mahrem bilgilerinin başkalarının eline geçerek deşifre olmaması için gizliliği en üst düzeyde tuttuğunun görüldüğü kaydedildi.

Aliağa Cumhuriyet Başsavcılığının yürüttüğü FETÖ/PDY soruşturması kapsamında 30 Kasım 2016'da Bayraklı ilçesinde yakalanan örgütün sözde üst düzey yöneticisi Mehmet Tabanca, tutuklanmıştı. Örgüt elebaşı Fetullah Gülen'in zanlıdan, "En sevdiğim öğrencilerimdir." diye bahsettiği ileri sürülmüştü.