
# FETÖ'nün ByLock kumpasını çözen isimden kritik uyarılar

18 Ocak Perşembe 2018 02:26

A- A+

FETÖ'nün ByLock kumpasını çözen adli bilişim uzmanlarından biri olan Tuncay Beşikçi, programa dair kritik uyarlarda bulundu...

FETÖ'nün ByLock kumpasını çözen adli bilişim uzmanlarından biri olan Tuncay Beşikçi, programa dair kritik uyarlarda bulundu.

Kendi bloğunda bir yazı kaleme alan Beşikçi, Mor Beyin sonrasında, **"Propaganda malzemesi verecek ve ByLock'un tamamını masum bir uygulama gibi gösterecek toptancı açıklamalardan dikkatle kaçınmaları elzemdir"** diyerek ByLock'un tamamen delil olmaktan çıkmış gibi yapılmaması gerektiğini savundu.

Beşikçi, "Soruşturmalarda en önemli kriter, maddi gerçeğin ortaya çıkarılarak masum insanlar ile örgüt mensuplarının ayrıştırılmasıdır" diyen Beşikçi, içeriğinde çok sayıda örgütsel yazışma içeren bir sistemle karşı karşıya kalındığını vurguladı.

**İşte Beşikçi'nin yazısının tamamı:**

Bu yazı için örnek olarak sevgili Yıldıray Oğur'un 15 Ocak 2018 tarihli Karar Gazetesi'nde "Adaletten Sinyal Bekleyenler" başlıklı makalesini seçmemin nedeni, her ne kadar babalarımız çocukluk arkadaşı olsa da kendisiyle tanışmamızın, 2 yıl kadar önce Balyoz davasında kumpas iddialarına ilişkin soruşturulduğunda eski cep telefonunu bana getirip inceletmesine (İsviçre'den gönderildiği iddia olunan bir mesaja dair araştırmadır ve bulunamamıştır) ve o gün konuştuklarımıza dayanır. O

günlerde hakkındaki iddiaların aksini kanıtlamak için doğal olarak telefon incelemesi yapabilecek bir uzmana ihtiyaç duymuş ve benimle irtibat kurmuştu. Beşiktaş'taki buluşmamızda kendisine Ergenekon davaları sırasında çalışmakta olduğu Taraf Gazetesi'ndeki manşetleri de sormuş, kendisinin ve gazetedekilerin "dijital delillerin gerçek mi sahte mi olduğunu anlayabilecek yetkinliğe sahip olmadığını" ve "delillerin sahte olup olmadığını" bilemeyeceklerini cevabını almıştım. İşte tam olarak bugün yazmak istediğim konu budur. Çünkü bilişim, teknoloji ve dijital delillerin öne çıktığı son derece hassas ve dikkatili yürütülmesi gereken ByLock soruşturmalarında da medya üzerinden dezenformasyon ve bilgi kirliliği oluşmaya başlamıştır.

ByLock kumpasının ortaya çıkarılış sürecinde bizi en çok zorlayan, Emniyet, Yargı hatta sıradan vatandaşların medya tarafından yanlış yönlendirilmeleri sonucunda konuya önyargılı bakmaları ve ByLock soruşturması geçiren herkese suçlu muamelesi yapmaları olmuştur. Bugün, 1.5 yıldan beri medyada konu hakkında çıkan asılsız haberlerin ve konu uzmanı olmayan kişiler tarafından yapılan yanlış teknik bilgilendirmelerin bu önyargıyı oluşturan bir numaralı etken olduğunu söyleyebiliyoruz.

Halen, yazılı ve görsel medyada devam eden, teknik konularda yorum yapabilecek düzeyde görünmeyen bazı medya mensuplarının hatalı veya yanlış değerlendirilebilecek bilgileri paylaştığını gözlemlemekteyim. Özellikle ByLock gibi hassas bir konuda dezenformasyonun yayılmasının önüne geçmek amacı ile uzmanlık alanıma giren bu konuyu FETÖ ile mücadelede önemli gördüğümden açıklama yapma gereği duyuyorum. Teknik bazı detayları örnek olarak seçtiğim ve bazı teknik hususlarda yanlış yönlendirildiğini düşündüğüm Yıldıray Oğur'un, 15 Ocak 2018 tarihli Karar Gazetesi'nde yayımlanan "Adaletten Sinyal Bekleyenler" başlıklı makalesinde yer verdiği bazı teknik hususlar üzerinden anlatmaya çalışacağım.

**NOKİA TUŞLU TELEFONUYLA BYLOCK'A GİRDİĞİ İDDİA EDİLENLER**

Tarafıma adli inceleme için intikal eden bazı telefonlarda, başka telefonlara ait IMEI bilgisinin kopyalandığı durumlarla karşılaşmaktayım. Android işletim sistemli bitakım telefonlarda IMEI kopyalama işi kolaylıkla gerçekleştirilebilmektedir. Yurtdışından kayıt dışı olarak getirilen veya Nokia'nın kullanılmayan eski telefonlarına ait IMEI numaraları kopyalanarak kullanılmaktadır. Böyle bir cihazda ByLock kullanılmışsa, IMEI bilgisi olarak eski cihaza ait numara görünecektir ve bu işlem FETÖ mensupları arasında tahmin edilenden çok daha yaygın bir durumdur.

**NAT MİMARİSİNDEKİ SORUNLAR**

NAT mimarisi halen dünyadaki çoğu operatör tarafından kullanılmaktadır. Dünya çapında hizmet veren birçok İnternet Servis Sağlayıcı firma IPv4 teknolojisindeki kısıtlı IP adresi havuzu bulunmasından dolayı NAT teknolojisi sayesinde abonelerin İnternet erişimlerini sağlamaktadır. NAT işlemi sırasında bir IP adresinin aynı anda birden çok abone tarafından kullanılmasına karşın, doğru abone tespiti için Özel IP olarak yer alan tanımlayıcı bilgi İnternet trafik verisine işlenmektedir ve her abonenin özel IP adresi farklıdır. Türkiye'de hizmet veren operatör firmaların tamamına yakını, İnternet ortamında belirli bir zamanda gerçekleştirilen işlemi, NAT teknolojisi kullanmak sureti ile abone bazında ayrıştırmaktadır. Sadece ByLock değil, tüm bilişim suçlarının ve gerektiği takdirde İnternet üzerinden işlenen tüm suçların tespitinde NAT verisi kullanılmaktadır. Europol'ün CGNAT kullanımını tavsiye etmemiş ve bu konuda haklı olarak her aboneye tek bir IP adresi verilebilen IPv6 teknolojisine geçilmesini önermiştir. Bununla birlikte ByLock soruşturmalarının 2014-15 yıllarını kapsadığı, Türkiye ve dünyada IPv6'ya geçiş için bugün dahi operatör altyapısı ve abone cihazlarının tamamının bu teknoloji ile uyumlu olmadığı gözardı edilmemelidir.

ByLock soruşturması geçirenlerin dikkatini çeken başka bir detay, ByLock kullanım tespiti yapılan belirli bir tarihte NAT ve HTS deki lokasyon bilgileri arasındaki tutarsızlıktır. Örneğin NAT verisinde Kocaeli'nden sinyal almış görünen bir kişi HTS verisinde İstanbul'da görünmektedir. Bunun nedeni her iki verinin farklı sistemlerde kayıt altına alınmasıdır. HTS, ses şebekesi üzerinden çalışmakta, abone yer değiştirdikçe sinyal alınan baz istasyonuna göre lokasyon bilgisi güncellenmektedir. Öte yandan, CGNAT verisinde, baz istasyonunu tarafından aboneye atanan IP adresi uzun süre (sinyal kaybolana veya telefon kapanana kadar) korunmaktadır ve IP adresi atandığı andaki lokasyon kayıt edilmektedir. Dolayısıyla Kocaeli'nden IP adresi alan bir abone, sinyal kesilmedikçe İstanbul'da da aynı IP adresini kullanmaya devam edebilir.

**BYLOCK MAĞDURLARI TARİH ARALIĞI**

Morbeyin kumpasının ilk ortaya çıktığı ekran görüntüsünde dosyanın yaratılma tarihi 3 Haziran 2014 ve son değiştirilme tarihi 30 Mart 2015'tir. Fakat burada gözden kaçan, ilgili dosyanın sadece morbeyin.com verisini değil, bu tarihler arasında ziyaret edilen tüm İnternet sayfalarından oluştuğudur. Sırf ilgili ekran görüntüsünden morbeyin.com sitesi üzerinden yapılan yönlendirme tarihi kesin olarak söylenemez. Bununla birlikte yapılan veri analitiği çalışması ByLock yönlendirmelerinin 10 Ağustos 2014 tarihinde sunucunun ABD'den Litvanya'ya transferinden hemen sonra başladığını bilimsel olarak ortaya koymuştur, 15 Kasım 2014 tarihi itibarı ile de ByLock sunucusunun Türk IP adreslerinin tamamına yakınına bloklandığı ve bu tarihten sonra ByLock'a sadece VPN ile erişim sağlanabildiği bilinmektedir.

**AHMET TANER KIŞLALI'NIN KIZI**

Rahmetli Ahmet Taner Kışlalı'nın kızı Nil Dolunay Kışlalı Edis'e ait olan ve havaalanında bulunan bir işletmedeki ADSL hattı

üzerinden ByLock uygulaması kullanılmış ve WiFi mağduru olmuştur. Konu gerçek kullanıcının tespitine yönelik çalışmaların adli işlemler öncesinde tamamlanması gerekliliğiyle ilgilidir. Ayrıca söz konusu ADSL hattı üzerinden uygulamayı kullanan kişi Haziran 2017'de tespit edilmiştir. ADSL kullanımına bağlı gerçek kullanıcı tespitlerinin kolluk makamlarınca olay bazında gerçekleştirilmesi gerekmektedir.

Sonuç olarak, aklın yolu birdir, bilimdir ve bu yoldan gidilmelidir. Örneğin, 11,480 masum insanın tespiti Cumhuriyet Gazetesi davasında verdiğim mahkeme ifadesinde anlattığım yöntemle yapılmıştır. Onbinlerce kişiyi kapsayan soruşturmalarda elbette hatalar olabilir, kalan mağduriyetlerin giderilmesi için bilimsel çalışmalar devam etmektedir ve kısa zamanda mutlaka giderilecektir.

Halen, son derece sinsi, planlı ve gizli çalışan, örgütün menfaatleri doğrultusunda aile bireylerini dahi tehlikeye atmaktan çekinmeyen bölücü bir yapıyla mücadele edilmektedir. Morbeyin kumpası, örgütün masum insanların hayatlarını nasıl mahvettiklerini bir kere daha göstermiştir. Teknolojiyi çok iyi kullanan, onbinlerce kişinin kullanmasına rağmen ByLock'u aylarca gizleyebilen, uygulama kurulum ve güncellemeleri bölge bilişim görevlileri tarafından yapılan ve içeriğinde çok sayıda örgütsel yazışma içeren bir sistemle karşı karşıya kalınmıştır. Öte yandan, tamamen gizlilik ilkesi üzerine tasarlanmış ByLock uygulamasına ait sunucudaki tüm veri ele geçirilememiş, örneğin bazı tarihlerdeki log kayıtlarına ve ses ile yapılan aramaların içeriğine ulaşılamamıştır. Bu şartlar altında, medyada görev yapan arkadaşların, özellikle teknik bilgi gerektiren konularda soruşturmanın ciddiyetini kaybettirecek, örgüte propaganda malzemesi verecek ve ByLock'un tamamını masum bir uygulama gibi gösterecek toptancı açıklamalardan dikkatle kaçınmaları elzemdir. Soruşturmalarda en önemli kriter, maddi gerçeğin ortaya çıkarılarak masum insanlar ile örgüt mensuplarının ayrıştırılmasıdır.

**Odatv.com**

tuncay beşikçi arşiv