Murat Yetkin

Darbe yolundaki gizli yazışmalar: ByLock

12 Eylül 2016

Halen görevde olan bakan üzüntüyle anlatıyordu.

Çocukluğundan beri tanıdığı, Milli Görüş hareketinde birlikte yer aldığı bir arkadaşıydı söz konusu olan. Kendisi AK Parti'ye geçmiş ama o geçmemişti, bir ilde üst düzey bir görevdeydi.

15 Temmuz kanlı darbe girişimi ardından bir gün arkadaşının eşi arayıp yardım istemişti: Arkadaşı "Fethullahçı Terör Örgütü (FETÖ)" üyesi olmak suçlamasıyla gözaltına alınmıştı.

Bakan hemen ne olduğunu anlamaya çalıştı, güvenlik yetkililerinden bilgi istedi.

Bu işte bir yanlışlık olmalıydı. Arkadaşının gerçekten de Gülen cemaatiyle hiç bir teması görünmüyordu. Çocuklarını o okullara göndermemiş, Bank Asya'da hesap açmamıştı, hatta Zaman gazetesine bırakın abone olmayı okuduğu dahi görülmemişti.

Bakan inanamıyordu ama bir de MİT'ten gelen bir dosya sunuldu Bakana. Buna göre arkadaşının cep telefonunda ByLock yazılım programı yüklenmişti. Bu uygulama aracılığıyla yalnızca bir kişiyle haberleşmişti. Bir yıl içinde 109 kere ve sadece aynı kişiyle haberleşmişti ve o kişi istihbarat kayıtlarına göre o ildeki "kıta imamı" idi, yani askeri birlikler ona bağlıydı.

"Hemen elimi çektim" dedi Bakan üzüntüyle, "Yapacağım bir şey yok bu durumda."

Bakanın çizdiği tablo, Başbakan Yardımcısı Numan Kurtulmuş'un "kripto FETÖ'cüler" tanımına uyuyordu.

Kendisini ne kadar iyi gizlemiş olsa da, ByLock yazışması, bakanın çocukluk arkadaşının tutuklanmasına yetmişti.

MİT 2014 yılında ByLock yazılımının Litvanya'daki sunucusuna sızınca, MİT ile FETÖ arasındaki siber savaş yeni bir seyre girdi.

ABİLER, ABLALAR, İMAMLAR ARASI

Türkiye 15 Temmuz darbe girşimi ardından tıpkı "kıta imamları" gibi ByLock (okunuşu Baylok) diye bir kavramla da tanıştı.

FETÖ soruşturmaları Gülen 'hareketi üyelerinin Türkiye'yi 15 Temmuz darbe girişimine götüren süreçte bu iletişim sistemi üzerinden gizli haberleşmeyi yürüttüğü üzerinde yoğunlaşıyordu.

Oysa MİT Cemaatin ByLock dosyasını geride bırakıp gizli örgütlenmenin haberleşmeyi Eagle yazılımı üzerinden yürüttüğünü saptamış, onun peşine düşmüştü bile. Eagle kodları tam olarak kırılıp yapılan hazırlığın darbe girişimi olduğu ortaya çıkarılamadan 15 Temmuz kanlı girişimi yaşandı.

Bunda MİT'in Mayıs ayı sonlarına doğru ByLock kayıtlarından saptayabildiği 40 bin kadar isimden devlet kurumlarında çalışanları, kendi kurumlarına bildirmeye başlamasının da payı olmuştu. Bu kayıtlara göre, örneğin 600 kadar subayın ismi Genelkurmay'a bildirilmişti. Öte yandan Genelkurmay'da konuyla ilgilenecek, örneğin Personel Dairesinda Fethullahçı örgütlenme vardı ve alarm zilleri çalmaya başlamıştı.

NASIL DEŞİFRE OLDU?

Örgütlenme ağı, Temmuz sonunda yapılacak Yüksek Askeri Şura'da (YAŞ) bu subayların çoğunun tasfiye edileceği bilgisine böyle ulaştı.

Ancak, Hürriyet'e konuşan ve isimlerinin saklı kalmasını isteyen MİT yetkililerine göre, örgütün sadece Genelkurmay'da değil Türkiye genelinde deşifre olmaya başlaması Emniyet ve Başbakanlık'taki bilgi sızmalarıyla oldu.

MİT'in saptamasına göre Cemaatin Emniyet İstihbaratında mühendis olarak çalışan bir elemanı 40 bin kadar ismi toplu halde Başbakanlık eski Veri Toplama Merkezi İstihbarat Şefi Mustafa Koçyiğit'e iletti. Koçyiğit'in de "Burak" ismiyle tanıdığı mühendisten alınan bilgileri (Koçyiğit ifadesinde 20 bin isim diyor) örgütte bağlı bulunduğu "Selahattin" ve "Furkan" ismiyle bildiği "abilere" ilettiğini ifadesinde söylüyor.

İstihbaratçılar bu gelişmelerin darbe girişimini YAŞ öncesine çekmiş olabileceği yorumunda bulunuyor.

İşte MİT'in siber ajanlarının 'kırmasıyla' ele geçen, ByLock yazılım programını kullanan ilk 25 isim...

NASIL FARK EDİLDİ?

MİT'in ByLock sisteminin farkına varıp üstüne gitmesi, izlemeye alınan bazı Fethullahçı isimler

arasındaki telefon, SMS, Whatsapp irtibatının bıçakla kesilir gibi durması olmuş.

Bunun üzerine Cemaatin gizli bir haberleşme sistemi kurduğu sonucuna varılarak bu araştırılmaya başlamış.

Peki, Fethullahçıların telefon vs haberleşmesini terk etmeleri neden sonra olmuş?

İstihbaratçıların cevabı 17-25 Aralık 2013 soruşturmalarından sonra.

Bunun arkasında da polisiye, casusiye romanlarını solda sıfır bırakacak gelişmeler yaşanmış.

MİT Müsteşarı Hakan Fidan'ın 2014 yılı başından itibaren önemli önceliklerinden biri, ByLock sistemini çözmek oldu. Ancak sistemin çözüldüğünü anlayan FETÖ bu kez Eagle programına geçti.

MOBESE'NİN B'SİNDEN SONRA O'SU

Dönemin Başbakanı olan Cumhurbaşkanı Tayyip Erdoğan'ın talimatı ile ilk adımlar 19 Aralık'ta atılmış. Bu çerçevede kilit bir gelişme, dönemin Ulaştırma ve Haberleşme Bakanı olan Başbakan Binali Yıldırım'a bağlı kurulan merkezi dinleme kurumu Telekomünikasyon İletişim Başkanlığında (TİB) atılmış.

TİB'in Başkan ardımcısı ve İnternat Dairesi Başkan Vekili olan Osman Nihat Şen ve Bilgi Sistemleri Daire Başkanı İlhan Elieyioğlu'nun görevden alınması 23 Aralık Resmi Gazetesinde yayınlanarak resmileşmiş.

Osman Nihat Şen önemli bir isim. Sokak kameraları sistemi MOBESE'nin B'sinin Basri Aktepe ise, O'su Osman Nihat Şen idi.

TİB'deki en önemli değişiklik ise bir süre önce Fethi Şimşek'in ayrılmasıyla boşalan TİB Başkanlığına MİT'ten bir simin getirilmesi oldu. Hakan Fidan'ın Başbakanlık Müsteşar Yardımcılığı dönemde Başbakanlık Güvenlik İşleri Genel Müdürü olarak birlikte çalıştığı ve 2010'da MİT Müsteşarlığına

Başbakanlık Güvenlik İşleri Genel Müdürü olarak birlikte çalıştığı ve 2010'da MİT Müsteşarlığına atanınca MİT'e aldığı Ahmet Cemalettin Çelik 18 Ocak 2014'te TİB başkanlığına getirildi. (Bu arada 25 Aralık soruşturması da açılmış ve Erdoğan bunun bir yolsuzluk soruşturması değil, Gülen'in darbe girişimi olduğunu söylemeye başlamıştı. Bu atamanın sabahında Gaziantep'te Suriye'ye giden MİT'a ait TIR'lar jandarma tarafından durdurulup aranacak, bir skandal patlayacaktı.)

Şen halen VIP telekulak davası olarak birlinen 949 kişinin (TÜBİTAK kriptolu telefonlar dahil) usulsüz dinlenmesi davasında tutuklu yargılanıyor.

CEMATTE ALARM VE BYLOCK

Cemalettin Çelik MİT'teki son görevi olan Elektronik Teknik İstihbarat (ETİ) Başkanlığına ise kimin yerine getirilmiş biliyor musunuz? Basri Aktepe'nin. Emniyet İstihbaratı ve TİB'deki çalışmaları ile AK Parti'nin Cemaat ile arası iyi iken Fidan tarafından MİT'e alınmış olan Aktepe'nin 17 Aralık'tan bir kaç ay önce "kuşkuların artması üzerine" ETİ Başkanlığından "pasif bir göreve" alınmış olduğu bilgisi var.

İstihbarat analistlerinin değerlendirmesine göre MİT ve TİB'te telefon ve internet trafiği üzerindeki konntrolünü yitiren örgütlenme ByLock'u devreye alıyor.

Emniyet ve MİT, 17-25 Aralık sonrası FETÖ şüphesiyle gözaltına alınanların telefonlarında, pek da yaygın olmayan bu iletişim sisteminin yüklü olduğunu görünce üzerine gidiyor ve ortaya çıkarıyor.

KAYDI ABD'DE, YAZILIM TÜBİTAK'TAN

ByLock görünüşte herkese açık ve aslında basit, kolay kırılabilecek bir sistem.

Ancak önemli bir özelliği var. Mesela Whatsapp'a girdiğinizde olduğu gibi telefon defterinizdeki bütün isimleri, ya da numaraları arayıp iletişime geçemiyorsunuz.

Kaydolduğunuzda size sayılardan oluşan bir kod veriliyor ve ancak kod numarasını bildiğiniz kişiyle irtibat kurabiliyorsunuz; aynı şekilde sizin kod numaranızı bilen kişi sizinle irtibat kurabiliyor.

ByLock uygulaması ABD'de David Keynes tarafından piyasaya sürülmüş. MİT yetkilileri yaptıkları araştırmada yazılımın sahibi görünen şirketin de tabela şirketi olduğu, hatta kullanılan yabancı isimler

arkasında da Türklerin bulunduğu sonucuna varmışlar.

ByLock'un aslında Cemaat tarafından sanki ABD'de bir şirketmiş gibi kurulup yazılımın da Türkiye'de üretildiği sonucuna varmışlar.

Cemaatçilerin burada bir açık verdiği ve ByLock yazılımının kaynak kodları arasında bazı Türkçe komutların unutulduğunun saptanmış.

TÜBİTAK eski yöneticilerinden Mesut Yılmazer, 11 Eylül'de ByLock'u yazan ekipte yer aldığı kuşkusuyla çıkarıldığı mahkemede tutuklandı.

LİTVANYA BAĞLANTISI

Kaydı ABD'de görünen ByLock sunucusunun Litvanya'da çıktığını öğrendiğim an geçen yıl başıma gelen bir olayı hatırladım.

Geçen yıl Twitter hesabım gasp edilmişti. Gecenin bir yarısı banka hesabımı, kredi kartlarımı dondurduktan ve Twitter merkezine başvurumu yaptıktan sonra bu işten anlayan genç dostlarımdan "Şu işe bir bakar mısınız?" diye yardım istedim.

Bir süre sonra, sabaha karşı üç gibi, gençlerden biri aradı. "Tamam abi" dedi, "Cevabını da verdik, patlattık"; kendi lisanınca benim hesabımı gasp eden sunucuya bir darbe vurduklarını anlatıyordu.

"Peki ülkücülerin benle hesabı neymiş?" diye sordum, çünkü gaspçılar ekranımı üç hilaller, bozkurtlarla donatmışlardı.

"Ülkücü filan değil bunlar abi" dedi bilgisayar sihirbazı genç dostum; "Cemaat bunlar, kendilerini başka şekillerde gösteriyor."

O nedenle MİT yetkilisi sunucuyu Litvanya'da bulduklarını söylediği zaman daha bir can kulağıyla dinlemeye başladım.

YAZIŞMALARIN YÜZDE 99'U TÜRKÇE

Basri Aktepe'nin kızağa çekilmesi, Osman Nihat Şen'in görevden uzaklaştırılması ve Cemalettin Çelik'in TİB'in başına geçmesini takip eden günlerde, yani 2014 Ocak-Şubat aylarında MİT'in siber güvenlik uzmanları MİT, Emniyet ve Jandarma'dan TİB'e giden verilerin yazılımında bir casus program saptadı.

Toplam 14 bin satır civarındaki yazılıma gizlice yerleştirilmiş bu program, bütün veri akışını ABD'de bir adrese e-posta olarak kopyalıyordu.

Hükümetin TİB'i söndürmeye karar vermesiyle MİT'in ByLock'a Litvanya operasyonuna başlaması hemen hemen aynı süreçte oldu.

MİT'in siber güvenlik ekibi Litvanya'daki sunucuya girerek verileri Yenimahalle'deki karargaha aktarmaya, ByLock'un içini boşaltmaya başladılar.

Boşalttıkça onlar da şaşırdı: ABD'de kurulan, Litvanya'da işletilen ByLock'taki 18 milyon küsur yazışma ve 3,5 milyon e-postanın yüzde 99'u Türkçe idi.

Aynı şekilde IP'lerin yüzde 98'i Türkiye kaynaklıydı. Görünüşte şirket 2014 Kasım ayında Orta Doğu'dan gelen hesapları kapatmıştı ama bu Türkiye'den girişleri VPN ve Proxy gibi kimlik gizleme yollarına sevk etmek içindi. Zaten ByLock'taki kullanıcı adlarının tamamına yakını da Türkçe isim ve ünvanlardan oluşuyordu.

KİMLİKLER ORTAYA ÇIKIYOR

ByLock'un VPN'e geçmesi bir şeyden kuşkulandıklarına işaret ettiği için MİT 2015 Aralık ve 2016 Ocak'ta hafızada ne varsa alıp sistemden çıkıyor.

Zaten bu aşamada Fethullahçılara atfedilen ByLock sistemi de kapatılıp, başta söylediğimiz gibi Eagle üzerinden bir başka gizli haberleşme sistemi çalışmaya başlatılıyor.

MİT'çiler bugünde dek ByLock'a kayıtlı 215 bin 92 hesaptan Eylül başı itibarıyla 165 bin 178'inin kimliklerinin saptandığını söylüyor.

Bunlar içinde en önemlisinin ise ilk 25 kişi olduğu, yayılmanın bu ilk katılımcılardan aşağı doğru olduğu bilgisi veriliyor.

Çünkü başlarda az sayıda da olsa doğrudan internetten uygulama indirme şeklinde yapılan kayıtların bir aşamadan sonra irtibat görevlisi “abiler ve ablalar” kanalıyla Bluetooth yoluyla indirildiği saptanmış.

Gerçek kimliklerin saptanmasını zorlaştıran unsurlar arasında, hiyerarşide yüksek düzeyde bazı üyelerin başkalarına ait SIM kartlarıyla, ya da başkalarına ait ADSL bağlantıları üzerinden haberleşme sağladıkları anlaşılmış.

GİZLİ YÖNTEMLERE GİZLİ TEDBİRLER

ByLock’un çözülmesi belki de darbecilerin hazırlıklarını tamamlayamadan harekete geçmesine yol açtı, belki 15 Temmuz’un yenilmesinde pay sahibi oldu. Her halükarda 15 Temmuz kanlı girişime giden son hazırlıkların Eagle sistemi üzerinden yapıldığı anlaşılıyor.

Öte yandan Eagle programının çözülememesi, bu haberleşme sistemiyle ele geçen 1 dolarlık banknotlar arasında bağlantı olup olmadığının kesinleştirilememesi gibi zor problemler hala tamamıyla çözülebilmiş değil.

Şimdi bir yandan Eagle programının nasıl kullanıldığını tam olarak çözmeye, diğer yandan başka benzeri haberleşme sistemleri olup olmadığını bulmaya çalışıyor uzmanlar.