

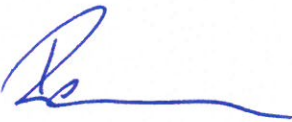
16 November 2017

To whom it may concern / İlgili Şahsa

This is to certify that the translation from English into Turkish of the enclosed document has been carried out by an experienced translator for and on behalf of Absolute Translations, and is, to the best of his ability, an accurate translation.

Bu mektup, ekteki belgelerin İngilizce'den Türkçe'ye Absolute Translations için ve onun adına, tecrübeli bir çevirmen tarafından elinden gelenin en iyisi ile doğru olarak çevrildiklerini tasdik etmektedir.

Yours faithfully / Saygılarımla,



Natalia Renans
Project Manager



Proje Adı: BREEZEWOOD

ByLock Soruşturması Hakkında Bilirkişi Raporu

Versiyon: 1.0

Fox-IT BV

13 Eylül 2017 - Hollanda

E-posta: fox@fox-it.com

Internet: www.fox-it.com

Telif Hakkı © 2017 Fox-IT BV

13 Eylül 2017

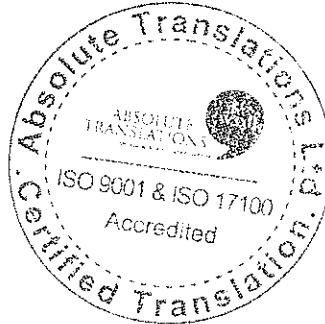
Versiyon: 1.0

Statü: Nihai

Sayfa Sayısı: 33

Yazan: Fox-BT

Sınıflandırma: HALKA AÇIK



HALKA AÇIK

Bu belge HALKA AÇIK olarak sınıflandırılmıştır.

Fox-IT BV

Olof Palmestraat 6
2616 LM Delft
Postbus 638
2600 AP Delft
Hollanda

Telefon: +31 (0)15 284 7999
Faks: +31 (0)15 284 7990
E-posta: fox@fox-it.com
İnternet: www.fox-it.com



Telif Hakkı © 2017 Fox-IT BV

Her hakkı saklıdır. Bu belgenin hiçbir kısmı Fox-IT'nin yazılı izni olmaksızın çoğaltılamaz, bir geri çağrı sisteminde saklanamaz veya herhangi bir yolla iletilemez. İhlaller, ilgili kanunlar uyarınca kovuşturulacaktır. Fox-IT B.V.'nin genel hizmet koşulları bu dokümantasyon için geçerlidir.

Ticari marka

Fox-IT ve Fox-IT logosu, Fox-IT B.V.'nin ticari markalarıdır.

Bu belgede bahsi geçen diğer tüm ticari markaların sahibi sözkonusu kalıntı kurum veya örgüttür.

daha güvenli bir toplum için

FOX-IT BV	T +31 (0)15 284 79 99
Olof Palmestraat 6, Delft	F +31 (0)15 284 79 90
POSTBUS 638, 2600 AP Delft	ABN AMRO 554697041
	KVK Haaglanden 27301624

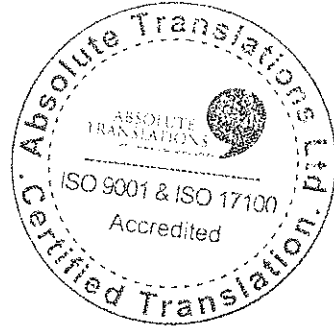
HALKA AÇIK - 2

BELGE YÖNETİMİ

Versiyon Yönetimi

Proje adı : BREEZEWOOD
Konu : ByLock soruşturması hakkında bilirkişi raporu
Tarih : 13 Eylül 2017
Versiyon : 1.0
Statü : Nihai
Yazanlar : Fox-IT

Bu versiyon, bu belgenin daha önceki tüm versiyonlarının yerine geçer. Daha önceki tüm nüshaları lütfen imha edin.



İÇİNDEKİLER

1. Giriş	5
2. Ele Alınan Konular	6
3. Yöntem	7
3.1. MIT Soruşturmasının ve MIT Raporunun Analizi	7
3.2. Olgu Kontrolü	7
4. Bulgular	8
4.1 ByLock Soruşturmasında MIT Tarafından Kullanılan Soruşturma Metodu Hakkında Fox-IT'nin Düşünceleri Nelerdir?	8
4.1.1. Saydamlık ve Kanıt Geçerliliği	8
4.1.2 Uygulama Sunucuları ve ByLock.net Etki Alanı	9
4.1.3 Açık Kaynak Araştırması	10
4.1.4 Ara Sonuçlar	14
4.2 MIT'in ByLock Uygulaması Kullanan Kişileri Tespit Etme Yöntemi Ne Kadar Sağlamdır?	15
4.2.1 ByLock Hesaplarını Kişilerle İlişkilendirmek İçin Nasıl Bir Metod Kullanılmıştır ve Bu Metod Ne Kadar Güvenilirdir?	15
4.2.2. ByLock Hesapları Nasıl Bir Yolla Yaratılmıştır ve Başka Kişiler ile İlişkilendirilebilecek Hesaplar Ekleme Mükün Müdür?	17
4.2.3. Bir ByLock Kullanıcısının Gerçekten Aktif Olduğunu Tespit Etmek İçin Nasıl Bir Metod Kullanılmıştır ve Bu Metod Ne Kadar Güvenilirdir?	17
4.2.4 Ara Sonuçlar	18
4.3 MIT'in, FETÖ/PDY ile ByLock Arasında İlişki Olduğu Hükmündeki Geçerlilik Yeterliliği Nedir?	19
4.3.1. ByLock Uygulamasının sadece FETÖ/PDY Tarafından Kullanıldığı Hükmüne Nasıl Varılmıştır?	19
4.3.2. İfade Edilen Bulgular ve Hüküm üzerinde Fox-IT'nin Görüşü nedir?	20
4.3.3. Güvenlik açısından, ByLock Uygulaması, Diğer Benzeri Mesajlaşma Uygulamaları ile Nasıl İlişkilidir?	22
4.3.4. Ara Sonuçlar	25
4.4. ByLock Soruşturması ile İlgili Olarak Fox-IT Tarafından Tespit Edilen Başka Hususlar Var mıdır?	26
4.4.1. Dikkat Çekici Tutarsızlıklar	26
4.4.2 Raporlama Bicimi ve Okunabilirlik	27
5. Sonuçlar	28
5.1. ByLock Soruşturmasında MIT Tarafından kullanılan Soruşturma Metodu Hakkında Fox-IT'nin Düşünceleri Nelerdir?	28
5.2 MIT'in ByLock uygulaması Kullanan Kişileri Tespit Etme Yöntemi Ne Kadar Sağlamdır/Geçerlidir?	28
5.3 MIT'in, FETÖ/PDY ile ByLock Arasında İlişki Olduğu Hükmünün Sağlamlık Niteliği Nedir?	28
5.4. Fox-IT Tarafından Tespit Edilen ByLock Soruşturması ile İlgili Başka Hususlar Var mıdır?	29
6. İncelenen Belgeler ve Veriler	30
7. Ekler	30
7.1 ByLock.net Zaman Çizelgesi	31
7.2 Teknik Terimler	33

1 - GİRİŞ

Fox-IT'den, Türkiye'de halen devam eden hukuki işlemler ile ilgili bilirkişi raporu talebinde bulunulmuştur. Bu talep, tutuklanmış bazı müşterileri temsil eden bir Türk avukat (bundan sonra Müvekkil olarak anılacaktır) tarafından yapılmıştır. Müvekkil aşağıdaki konuyla ilgili bilirkişi görüşü talep etmektedir.

Türk Hükümeti terörist örgüt olduğu iddia edilen Fethullahçı Terör Örgütü / Paralel Devlet Yapılanması (FETÖ/PDY)¹ soruşturmalarını aktif olarak yürütmektedir. Bu amaçla, Türk İstihbarat Teşkilatı MİT (Millî İstihbarat Teşkilâtı), ByLock mesajlaşma uygulaması ile FETÖ/PDY arasındaki ilişkiyi araştırmıştır. MİT, ByLock uygulaması ve ByLock kullanıcılarının iddia edilen FETÖ/PDY ile olan ilişkisine dair bulguları içeren soruşturma hakkında bir rapor hazırlamıştır. Bu rapor (bundan sonra MİT raporu olarak anılacaktır) Ankara'daki başsavcılığa gönderilmiştir.

Müvekkile göre bu rapor, Türk savcıları tarafından, çok sayıda kişiyi iddia edilen FETÖ/PDY üyesi olarak tespit etmek ve ByLock'u kullandıkları gerekçesiyle tutuklamak için kullanılmaktadır. Müvekkile göre, MİT raporundaki bulgular ve sonuçlar dikkatlice incelenmemiştir ve yanlıştır. Bu nedenle, Müvekkil, Fox-IT'den raporu yeniden incelemesini ve raporda kullanılan metotların, bulguların ve sonuçların sağlamlığı ile ilgili bilirkişi görüşünü bildirmesini istemiştir.

Fox-IT, MİT'in Türkçe olan raporunu ve "ByLock Uygulaması Teknik Raporu" (ByLock Application Technical Report) başlıklı tercüme edilmiş iki kopyasını teslim almıştır. İlk çevrilen rapor, Türkçe'den Hollandaca'ya yeminli bir çeviridir. İkinci tercüme raporu, 19 Temmuz 2017'de yazılan Hollandaca'dan İngilizce'ye yeminli bir çeviridir. Bu ikinci rapor, Fox-IT tarafından bu bilirkişi raporu kapsamında gözden geçirilmiştir.

¹ FETÖ/PDY adı, Hizmet hareketi olarak da adlandırılan Türkiye'de sosyal bir hareketi ifade etmektedir. FETÖ/PDY ismi bir terörist örgütü anlamında kullanılmaktadır. Müvekkile göre, hareket genellikle Türk hükümeti dışında bir terör örgütü olarak tanınmamaktadır. Bu tartışma Fox-IT'nin uzmanlık alanı dışındadır. Çarpıklık izlenimini önlemek için, söz konusu organizasyon, bu raporda iddia edilen FETÖ/PDY olarak adlandırılacaktır.

2 - ELE ALINAN KONULAR

Bu bölüm, bilirkişi inceleme raporunda ele alınan konuları açıklamaktadır. Konular Müvekkil tarafından ortaya konulmuş ve Müvekkil ile iş birliği içinde Fox-IT tarafından formüle edilmiştir. Bu raporda, Fox-IT tarafından, aşağıdaki konular ele alınmaktadır:

1. ByLock Soruşturmasında MİT tarafından kullanılan Soruşturma Metodu Hakkında Fox-IT'nin Düşünceleri Nelerdir?
2. MİT'in ByLock uygulaması kullanan kişileri tespit etme yöntemi ne kadar sağlamdır?
 - a. ByLock Hesaplarını kişilerle ilişkilendirmek için nasıl bir metod kullanılmıştır ve bu metod ne kadar güvenilirdir?
 - b. ByLock hesapları nasıl bir yolla oluşturulmuştur ve başka bir kişiyle ilişkilendirilebilecek hesaplar eklemek mümkün müdür?
 - c. Bir ByLock kullanıcısının gerçekten aktif olduğunu tespit etmek için nasıl bir metod kullanılmıştır ve bu metod ne kadar güvenilirdir?
3. MİT'in, FETÖ/PDY ile ByLock arasında ilişki olduğu hükmündeki geçerlilik yeterliliği nedir?
 - a. ByLock uygulamasının sadece FETÖ/PDY tarafından kullanıldığı hükmüne nasıl varılmıştır?
 - b. İfade edilen bulgular ve hüküm üzerinde Fox-IT'nin görüşü nedir?
 - c. Güvenlik açısından, ByLock uygulaması, diğer benzeri mesajlaşma uygulamaları ile nasıl ilişkilidir?
4. ByLock soruşturması ile ilgili Fox-IT tarafından tespit edilen başka hususlar var mıdır?

3- YÖNTEM

Bu bölüm, bu bilirkişi raporunda talep edilen soruşturmayı yürütmek için Fox-IT tarafından kullanılan yöntemi açıklamaktadır. Yöntem iki kısma ayrılabilir: MIT raporunun analizi ve MIT raporunda bahsi geçen gerçekleri ve gözlemleri doğrulamak için orijinal verilerin analizi. Her iki kısım da aşağıdaki alt bölümlerde açıklanmıştır.

3.1- MIT Soruşturmasının ve MIT Raporunun Analizi

Bu araştırma sırasında Fox-IT, MIT tarafından kullanılan dijital soruşturma sürecinin sağlamlığı bağlamında MIT raporunu analiz etmiştir. Özellikle, MIT soruşturmasının metodu, öne sürdüğü tezleri, bulguları ve hükümleri değerlendirilmiştir. ByLock soruşturmasının sonuçları yasal işlemlerde kanıt olarak sunulduğundan, soruşturma bir adli soruşturma olarak değerlendirilmiştir. Adli kanıt ve adli soruşturma ilkeleri üzerine çok sayıda ilgili makale ve kitap yazılmıştır. Fox-IT, soruşturmaları yürütürken, "Dijital Kanıt ve Bilgisayar Suçu"² (kitabın orijinal ismi "Digital Evidence and Computer Crime") kitabında tanımlanmış olan aşağıdaki ilkelere bağlı kalmaktadır.

1. Nesnellik: Kararların, gerçeklerin olabildiği en net hali ile verilebilmesi için, kanıtların yorumlanması ve sunulması tamamen çarpıtmasız olmalıdır. Araştırmacının bakış açısının sınırlandırılmaması ve araştırılmasında tarafsız olmasının garanti altına alınabilmesi için olası tüm hipotezler analiz edilmeli ve değerlendirilmelidir.

2. Delil Geçerliliği: Delillerin doğrulanması, delillerin iddia edildiği gibi olup olmadığının belirlendiği süreçtir. Buna, sunulan delilin toplandığı zamanki ile aynı olduğunun gösterilmesi ile birlikte, delillerin toplandığı yerin tarihi ve yeri de dahildir. Bir kanıt zinciri belgesi, kanıtları kimlerin ve ne amaçla ulaştığını göstermek açısından önemlidir.

3. Kanıt bütünlüğü: Bütünlük denetimi, kanıtların toplanma aşamasından itibaren değiştirilmediğini doğrulamak için gereklidir. Böylece kanıtların geçerliliği desteklenmiş olur. Dijital verilerin doğrulama işlemi genellikle kriptografik özet fonksiyonu hesaplanmasına dayanır. Kriptografik özet fonksiyonu verinin (neredeyse) benzersiz bir parmak izini üretir. Bu parmak izi, verilerin kriptografik özet fonksiyonu hesaplandığı andan itibaren değişmediğini doğrulamak için her zaman kullanılabilir.

4. Şeffaflık / Tekrarlanabilirlik: Dijital adli süreç, bütünüyle bağımsız olarak sınanabilmeli ve doğrulanabilmelidir. Doğrulamanın anahtar bir unsuru, işlemin aynı koşullar altında her çalıştırıldığında, tutarlı bir kalite seviyesi ile adli sürecin yeniden üretebilmesidir. Tüm hipotezlerin kökenleri dahil edilmelidir.

Bu ilkeler, MIT soruşturmasını ve raporunu değerlendirmek için geçerli kriterler olarak uygulanmıştır.

3.2- Olgu Kontrolü

Fox-IT, MIT raporunun sonuçları ile ilgili olgu ve gözlemleri doğrulamaya çalışmıştır. Bu amaçla, açık ve kapalı kaynaklar araştırılmış ve bu araştırmanın yapıldığı sırada mevcut olan veriler ile ByLock verisi analiz edilmiştir. Analiz, ByLock Android uygulamasının kaynak koda dönüştürülmesi ve dönüştürülen kodun statik analizini de içermektedir. Bölüm 5, hangi ByLock uygulama verisinin Fox-IT tarafından incelendiğini açıklamaktadır.

Ayrıca, Google aramaları, Twitter ve diğer çevrimiçi platformlarla ilgili olarak MIT tarafından açıklanan gözlemleri doğrulamak için çevrimiçi açık kaynak araştırılmıştır. ByLock sunucularından gelen veriler Fox-IT tarafından analiz için uygun değildir. Bu nedenle, MIT tarafından belirtilen gözlemler ve olgular, ByLock sunucu verileri dikkate alınarak kontrol edilememiştir.

Çeşitli olaylarla ilgili net bir genel görünüm oluşturmak için Fox-IT ve MIT tarafından sunulmuş olan çeşitli gözlemler ve olgular bir zaman çizelgesine yerleştirilmiştir. MIT raporunda, 15 Temmuz 2016'da darbe girişimi önemli bir nokta olarak görüldüğü için bu tarih, Fox-IT'nin raporunda da defalarca bir referans noktası olarak belirtilmiştir.

² "Digital Evidence and Computer Crime" kitabı, 3. basım, 2014, Eoghan Casey.

4- BULGULAR

4.1- ByLock Soruşturmasında MİT Tarafından Kullanılan Soruşturma Metodu Hakkında Fox-IT'nin Düşünceleri Nelerdir?

ByLock uygulaması ve ilgili iletişim sunucuları, MİT tarafından teknik incelemeye tabi tutulmuştur. MİT raporunda, izlenen metod açık bir şekilde tanımlanmamıştır. Fox-IT, MİT tarafından yapılan soruşturmayı açıklamaya çalışmış ve MİT raporunun bölüm içeriklerini aşağıdaki gibi özetlemiştir:

Bölüm 2, ByLock uygulaması hakkında genel bilgi vermektedir.

Bölüm 3.1, ByLock uygulama sunucularında saklanan verilerin elde edilmesindeki yasal gerekçeleri ve kullanılan yöntemleri açıklamaktadır.

Bölüm 3.2, ByLock ile ilgili IP adreslerinin ve alan adlarının MİT tarafından gerçekleştirilen bir analizini açıklamaktadır. Uygulamanın farklı sürümlerinin ve açık kaynak araştırmalarının analizi sayesinde MİT gözlem yapmakta ve uygulama altyapısı üzerine sonuçlara varmaktadır.

Bölüm 3.3, MİT tarafından gerçekleştirilen ByLock ile ilgili açık kaynak araştırmasının sonuçlarını açıklamaktadır. MİT, arama motorlarında "ByLock" sözcüğü için Türkiye'den ve dünyadan yapılan aramaları karşılaştırmıştır. MİT bu gözlemlere dayanarak, ByLock uygulamasının kullanımına ve hedeflerine ilişkin hükümler çıkarmaktadır.

Bölüm 3.4, ByLock tarafından kullanılan şifreleme protokollerinin analizinden ve MİT tarafından gerçekleştirilen ters mühendislikten elde edilen sonuçları açıklamaktadır.

Bölüm 3.5, MİT tarafından gerçekleştirilen bir ByLock sunucusunun analiz sonuçlarını açıklamaktadır. ByLock altyapısını izah etmekte ve ByLock sunucusu ile sunucunun iddia edilen yöneticisi hakkındaki gözlemlerini açıklamaktadır. Yöneticinin niyetlerine ilişkin gözlemlere dayalı çıkarımlar yer almaktadır.

Bölüm 3.6, sunucudan elde edilen veri tabanı dosyalarının incelenme sonuçlarını açıklamaktadır. MİT, ByLock uygulama verisinin depolandığı 109 GB'lık bir veri tabanı dosyası elde etmiştir. Bu bölüm veri tabanı modeli ve içeriği üzerinde durmaktadır.

Bölüm 3.7, MİT tarafından analiz edilen ByLock sunucusunun istatistiksel verilerini açıklamaktadır.

Bölüm 4, değerlendirme ve sonucu içermektedir. MİT, ByLock'un sözde FETÖ/PDY terör örgütü üyelerinin özel kullanımına sunulduğu hükmüne varmaktadır.

➤ 4.1.1. Saydamlık ve Kanıtların Doğruluğu

Fox-IT, MİT raporunda genel bir şeffaflık eksikliği gözlemlemiştir. Ayrıca, araştırılan verilerin bütünlüğünün doğrulanmasına olanak sağlayan hiçbir bilgi bulunamamıştır. Bu bölümde bu iki bulgu üzerinde durulacaktır.

Fox-IT, MİT raporuna dayanarak yaptığı çalışmada, ByLock verilerinin işlenmesi sırasında delillerin etkilenmediğini doğrulayamamıştır. Bir veri kümesinin kriptografik özet fonksiyonunun hesaplanması, verideki bütünlüğün daha sonra doğrulanabilmesi için adli veri üzerinde parmak izi alma amaçlı kabul edilmiş bir yöntemdir. Sonraki aşamalarda, dijital adli süreç sırasında kanıtların bütünlüğünün değiştirilmediğini bağımsız olarak doğrulamayı mümkün kılacak biçimde, kriptografik özet fonksiyon çıktılarını belgelemek ve bir denetim izi oluşturmak iyi bir uygulamadır. MİT raporunda hiçbir kriptografik özet fonksiyonu çıktısı, yazı veya denetim izi bulunmamaktadır. Bu kriptografik özet fonksiyon çıktılarının elde olması, özellikle önemli bulguların ByLock veri tabanı veri kümesinden türetildiğinden emin olunabilmesi açısından zorunludur.

MİT raporunda birçok bulgular ve hükümler açıklanmakta ancak raporda bulguların elde edilmesinde kullanılan analiz adımlarına ilişkin bir açıklama bulunmamaktadır. Bu, okuyucuların kullanılan soruşturma yöntemini incelemelerini zorlaştırmaktadır. Şeffaflık, adil yargı gereğidir. Soruşturmanın güvenilir ve kesin olduğunu doğrulamak mümkün olmalıdır. MİT raporunda, şeffaflık hususunda en önemli eksikliklerin olduğu bölüm Bölüm 3.6'dır. Bu bölüm, ByLock soruşturmasının önemli bir bölümü olup ByLock sunucusunda yapılan soruşturmanın sonuçlarına yer vermektedir. Bu bölüm kendi içinde tutarsız bulunan ekran görüntüleri ile ait olduğu metin ile tutarsız ekran görüntüleri içermektedir. Bu da, kaynak verilerin veya ekran görüntüsünün (veya her ikisinin de) manipüle edildiğini

göstermektedir. Bölüm 4.4.1'de bu konu üzerinde durulmuştur. MİT Raporu, analistin ekran görüntüsünü elde etmek için kullandığı adımları detaylandırmış olsaydı, tutarsızlıkları açıklığa kavuşturmak mümkün olabilirdi. Ancak durum böyle değildir. Sonuçların bütünlüğüyle ilgili soruları gündeme getirmesi ve bulguların elde edilme yöntemlerini incelemek ve sonuçlarını onaylayıp doğrulamak için hiçbir yolu mümkün kılmaması nedeniyle, Fox-IT bunu ciddi bir sorun olarak görmektedir.

Ayrıca, soruşturulan verilerin hangi yöntemle ve hangi lokasyonda elde edildiğini ve hangi özel tekniklerin kullanıldığını belgelemek iyi bir adli tıp uygulamasıdır. MİT raporunda veri toplama ile ilgili dokümantasyon bulunmamaktadır. Bu durum, veri kümesinin eksiksiz olup olmadığının ve tüm ilgili verileri içerip içermediğinin doğrulanmasını imkânsız kılmaktadır.

➤ 4.1.2. Uygulama Sunucuları ve ByLock.net Etki Alanı

MİT raporu Bölüm 3.2'de sunulan ilk bulgu, 1 Eylül 2015 - 9 Ekim 2016 arasındaki dönemde bylock.net için sadece 46.166.160.137 numaralı IP adresinin kullanıldığınıdır. MİT, "David Keynes" adına düzenlenmiş, kendisinin oluşturup imzaladığı SSL sertifikası ile ilişkili olarak yürütülmüş çalışmalarla dokuz farklı IP adresini tespit etmiştir. Fox-IT, bulguları doğrulamak için ByLock tarafından kullanılan IP adresleri ve alan adları hakkında araştırma yapmıştır.

Fox-IT, PassiveTotal^{3,4} kullanarak yaygın adı "David Keynes" olan SSL sertifikasını barındıran IP adresleri için bir arama gerçekleştirmiştir. Bu arama, aşağıdaki 10 IP adresiyle sonuçlanmıştır:

46.166.160.137
46.166.164.176
46.166.164.177
46.166.164.178
46.166.164.179
46.166.164.180
46.166.164.181
46.166.164.182
46.166.164.183
69.64.56.133

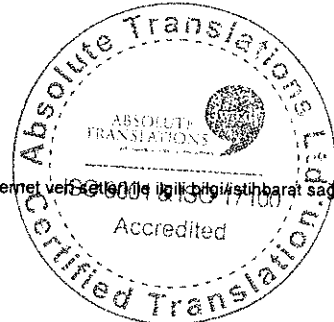
İlk dokuz IP adresi MİT raporunda belirtilmiştir. Son IP adresi MİT raporunda belirtilmemiştir.

Bylock.net, bu IP adresini Nisan 2014'ten Ağustos 2014'e kadar kullanmıştır. Bu nedenle bu IP'nin ilk ByLock uygulama sunucusu olması mümkündür. MİT raporunda bundan neden bahsedilmediği bilinmemektedir.

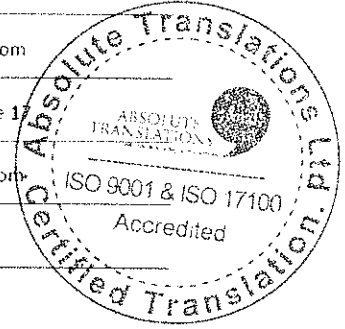
Fox-IT, bylock.net etki alanı sahipliğinin ve IP adreslerinin belirlenmesi amacıyla, bylock.net ve IP adresi 46.166.160.137 için açık kaynaklı bir soruşturma gerçekleştirmiştir. Bu bilgilerde zaman içinde yapılan değişiklikler ek 7.1'de listelenmiştir. Bylock.net alanının 46.166.164.137 adresine çözümlenmesi yalnızca Ağustos 2014 ile Mart 2016 arasındadır. Bu, bylock.net'in 1 Eylül 2015'ten 9 Ekim 2016'ya kadar bu IP adresinde çözümlendiğine dair MİT Raporunda bulunan ifade ile çelişmektedir. Fox-IT, bylock.net alanının yalnızca Mart 2016'ya kadar etkin olduğu ve Nisan 2016'dan 15 Temmuz 2016 tarihine kadar olan zaman aralığında ise kullanılmış olamayacağı sonucuna varmıştır. Tablo 1, ByLock versiyonlarının zaman çizelgesini içermektedir.

³ RiskIQ şirketinin ürünü olan PassiveTotal, pasif DNS, WHOIS, SSL sertifika verileri, ağ iz sürücüleri vb. Internet verileri için ilgili bilgileri sunar ve sağlar.

⁴ <https://community.riskiq.com/search/certificate/issuerCommonName/David%20Keynes>



Date	Description	Source
April 2014	ByLock.net domain resolving 69.64.56.133	PassiveTotal
11 July 2014	Android ByLock 1.1.3 uploaded to downloadatoz	downloadatoz.com
13 July 2014	Android ByLock 1.1.3 uploaded to Google Play Store	web.archive.org
10 August 2014	ByLock.net domain resolving to 46.166.160.137	PassiveTotal
22 August 2014	iOS ByLock 1.1.3 uploaded to Apple App Store	sensortower.com
23 August 2014	Android ByLock 1.1.4 uploaded to downloadatoz	downloadatoz.com
24 August 2014	Email confirmation from balticServers that IP range 46.166.164.176/29 is ready for use	MIT report, page 14
4 September 2014	Android ByLock 1.1.6 uploaded to downloadatoz	downloadatoz.com
15 November 2014	Blog announcement re blocking of IP addresses	MIT report, page 1
24 Dec 2014	Android ByLock 1.1.7 uploaded to downloadatoz	downloadatoz.com
26 Dec 2014	Android ByLock 1.1.7 uploaded to Google Play Store	web.archive.org
March 2016	ByLock.net domain deactivated	PassiveTotal
15 July 2016	Attempted coup	Various



Tablo 1. ByLock versiyonlarının ve bylock.net alan kayıtlarının zaman çizelgesi

Daha sonra Fox-IT, uygulama sunucularının IP adreslerinin belirlenmesi için, ByLock uygulamasının Android sürüm 1.1.6 ve 1.1.7 versiyonlarını incelemiştir. ByLock 1.1.6 versiyonunda sabit kodlanmış 46.166.164.177 IP adresinin ve Sürüm 1.1.7 versiyonunda ise 46.166.164.181 IP adresinin kullanıldığı tespit edilmiştir. Her iki IP adresi de MIT raporunda listelenen IP adresleri arasında yer almaktadır. ByLock sürüm 1.1.6, 4 Eylül 2014'ten itibaren bir yükseltme olarak kullanıma sunulmuştur. Sonuç olarak, 4 Eylül 2014'ten sonra, versiyonu yükseltilen ya da yeni kurulan ByLock uygulaması, bylock.net adresindeki sunucu yerine bu iki IP adresinden birine bağlanmıştır. Söz konusu iki sunucu da (1) ya ByLock uygulama sunucusu olarak (2) ya da ByLock uygulama sunucusuna bir vekil sunucu olarak ByLock altyapısının aktif bir parçası olmuştur.

MIT raporunda bu sunucuların araştırılmasıyla ilgili hiçbir şey belirtilmemiştir. Bu durum, aşağıdaki soruları ortaya çıkarmaktadır.

- Bu iki sunucu ByLock altyapısında nasıl kullanıldı ve neden bu sunucuların araştırılması MIT raporuna dahil edilmemiştir?

- Bunlar gerçekten vekil sunucularsa, IP adreslerinin Türkiye'den engellenmesine ilişkin Türkçe MIT raporunun 26. sayfasındaki ifadelerle ilişkisi nedir? MIT raporunda, "Uygulama sunucusu yöneticisinin gerçekleştirdiği IP engellemesinin [...] kullanıcıların gerçek IP adresleri ile sunucuya bağlanmasının tespit edilmesini önlemeyi amaçladığı sonucuna varılmaktadır" ifadesi yer almıştır. ByLock sürüm 1.1.6 ve 1.1.7, 46.166.160.137 adresine başvurmadığından, söz konusu sunucuda sözü edilen güvenlik duvarı engellemesi bu (v1.1.6 ve v1.1.7) ByLock kullanıcılarına uygulanamayacaktır. Bu gözlem, VPN bağlantıları yoluyla kullanıcıları zorlamaya çalışan bir yöneticinin olduğu yönündeki MIT

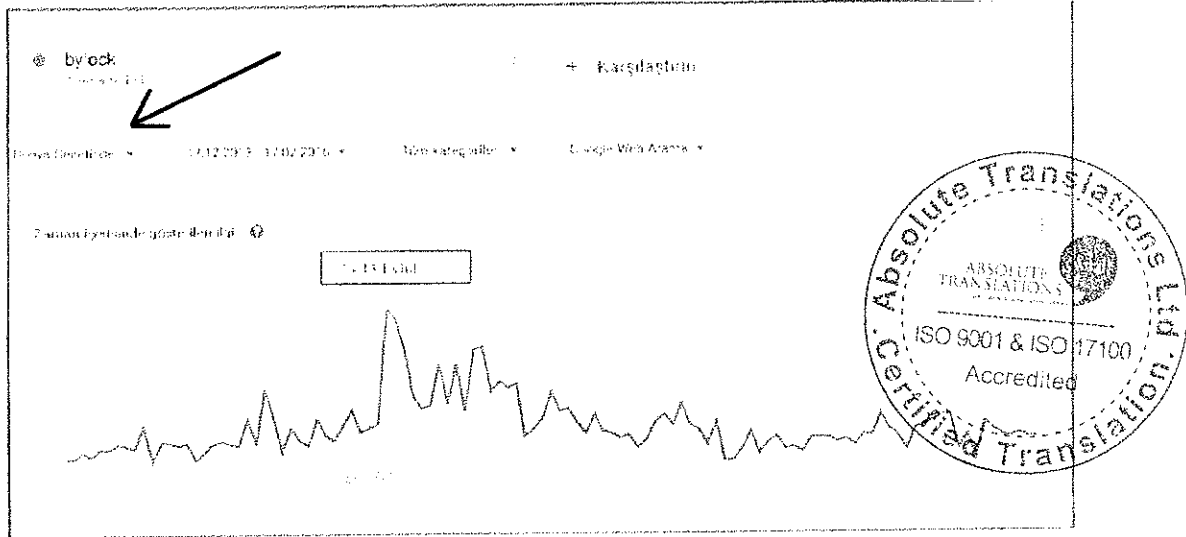
değerlendirmesini desteklememektedir.

➤ 4.1.3. Açık Kaynak Araştırması

MİT raporu Bölüm 3.3'te açıklanan soruşturmada ve sonuçlarda birden fazla sorun yer almaktadır ve bu sorunların hepsi de varılan sonuçlarla ilişkilidir.

Arama trendleri

Bölüm 3.3'teki ilk şekil, 17 Aralık 2013 ile 17 Şubat 2016 tarihleri arasındaki dünya genelinde "ByLock" arama terimi için Google Eğilim sonuçlarını göstermektedir. Ancak şeklin altındaki açıklamada "ByLock arama istatistikleri (Türkiye)" yer almaktadır. Bu da şu soruyu gündeme getirmektedir: Bu metin hangi istatistiğe atıf yapmaktadır?



"ByLock" Arama İstatistikleri (Türkiye)

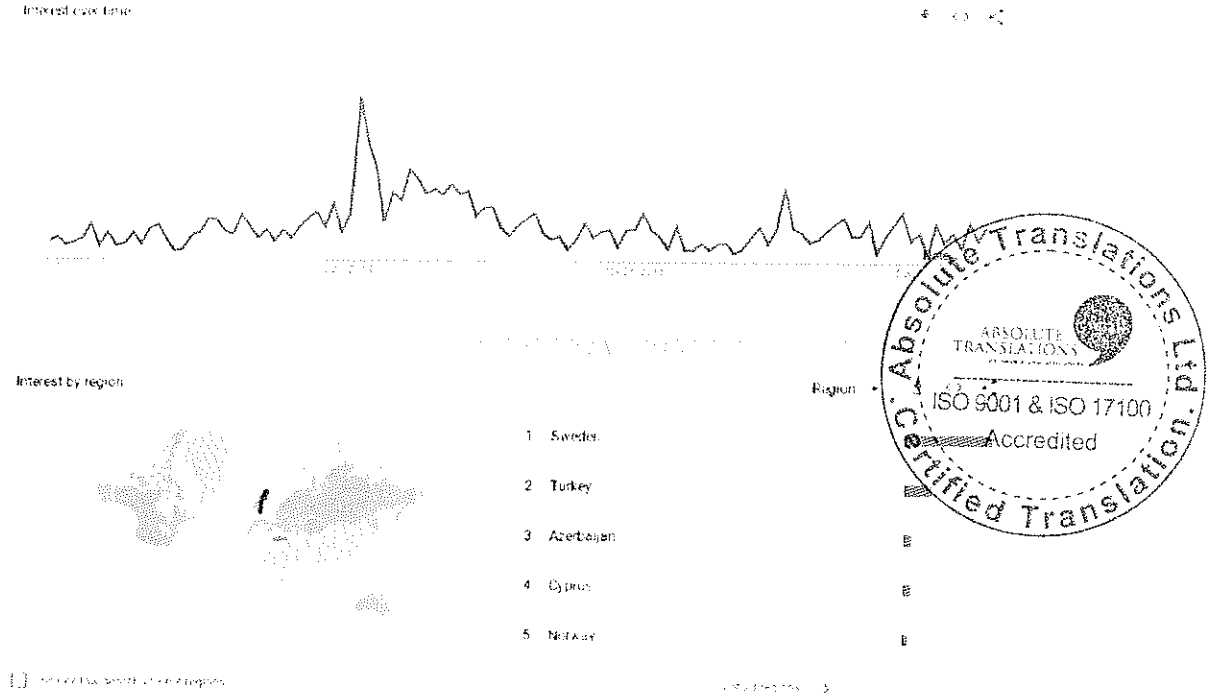
Türkiye'den Aramalar

MİT raporunun 15. sayfasında "ByLock" terimiyle yapılan aramaların çoğunlukla Fransa, İngiltere ve ABD'den yapıldığı belirtilmiştir. Sayfa 15, Google Eğilimler sonuçlarını gösteren rakamları içermektedir. Sorgu, Türkiye, ABD, Birleşik Krallık ve Fransa ülkeleri için filtrelenmiştir. Bu okuyucuyu yanlış yönlendirmektedir. Eğer daha yüksek kullanım istatistiklerine sahip başka ülkeler varsa, bu grafikte yer alamayacaktır. Çünkü söz konusu şekil yalnızca bahsi geçen dört ülkeyi göstermektedir.

Fox-IT, Google Eğilimler uygulamasında "ByLock"u arayarak Google Eğilimler sonuçlarını yeniden elde etmeye çalışmıştır. Bu sorgu 17 Ağustos 2017'de gerçekleştirilmiştir. Sorgu, Google'ın farklı ülkelerin son kullanıcılarına farklı sonuçlar gösterebileceği ihtimalini göz önünde bulundurarak, farklı ülkelerde bulunan vekil sunucular kullanılarak gerçekleştirilmiştir. Sonuçların hepsi aynıdır ve Şekil 1'de gösterilmiştir. İlk beş ülke sırasıyla (yüksekten düşüğe) İsveç, Türkiye, Azerbaycan, Kıbrıs ve Norveç'tir. Söz konusu dönem dahilinde en çok arama yapan ülkeler arasında Fransa, Birleşik Krallık ve ABD ülkeleri sırasıyla 20, 14 ve 15. olarak yer almıştır. Bu, MİT'in gözleminden farklıdır ve MİT tarafından düzenlenen raporun Bölüm 3.3 son paragrafındaki sonucu geçersiz kılmaktadır.

"...istatistikler göz önünde bulundurulduğunda diğer ülkelere kıyasla Türkiye'den kullanım değerlerinin açık farkla yüksek olması (diğer tüm ülkelerin toplamından çok daha fazla) ..."

Aramaların hangi bölümünün Türkiye'den geldiği belli olmadığından, MİT'in olgusal ifadesi geçersizdir ve yeniden ele alınmalıdır.



Sekil 1.

Bylock arama teriminin dünya genelinde Google Eğilimler sonuçları

Twitter

MİT raporunun 16. sayfasında şöyle bir ifade yer almaktadır:

"Twitter'da 15 Temmuz 2016 tarihi öncesinde ByLock uygulamasına ilişkin paylaşımlarda bulunan kullanıcıların büyük çoğunluğunun FETÖ/PYD lehine paylaşımlarda bulunduğu görülmüştür."

Bu olgunun MİT tarafından nasıl tespit edildiğine dair hiçbir açıklama yoktur. Raporda bu ifadeyi destekleyecek hiçbir Twitter verisi, istatistiği veya başka bir delil bulunmamaktadır. Bu iddia, açık olmadığından ve MİT'in vardığı sonuçları etkileyen ana bulgularından biri olduğu için sorgulanmalıdır.

Paragraf şöyle devam ediyor:

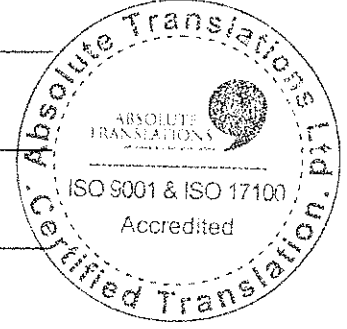
"Bu durum, kimliği tespit edilebilen hesap kullanıcılarının (...) FETÖ/PDY'ye muzahir şahıslar olduklarının kamuoyuna yansımından önce uygulamayı bildiklerinin ve yaygın şekilde kullandıklarının göstergesi olarak değerlendirilmiştir."

Bu, MİT'in ByLock uygulamasının 15 Temmuz 2016'dan önce halk tarafından bilinmediği görüşünde olduğunu yansıtmaktadır. Fox-IT bu ifadeyi mevcut istatistiklerle doğrulamaya çalışmıştır. Google Eğilimler istatistikleri, ByLock'a olan ilginin 7 Eylül ve 14 Eylül 2014 arasında en üst seviyeye gelecek şekilde en azından 2013 yılının sonundan 15 Temmuz 2016 tarihine kadar değişik seviyelerde varlığını göstermektedir. Geçmişe ait olarak Google Play Store'dan indirme ve yükleme istatistikleri⁵, ByLock yüklemelerinin en azından Nisan 2014'ten 19 Ocak 2015'e kadar 100.000 kurulumla ulaştığını

⁵ <http://choilieng.com/apk-on-pc/net.client.by.lock.apk>

göstermektedir⁶. Tablo 2'de ilgili istatistikler listelenmiştir. Bu gözlemler, halkın ByLock'u 15 Temmuz 2016'ya kadar geçen süre içerisinde bildiğini ve kullandığını göstermektedir. Mevcut bilgiler göz önüne alındığında, uygulamayı indiren ve kuran kişilerin, iddia edilen FETÖ/PDY üyesi olup olmadıklarının belirlenmesi mümkün değildir.

Date	Total installs
22 April 2014	50+
24 April 2014	100+
4 May 2014	1,000+
20 May 2014	5,000+
1 June 2014	10,000+
24 Aug 2014	50,000+
19 Jan 2015	100,000+



Tablo 2. Google Play Store ByLock uygulaması kurulum istatistikleri

Platform Sayısının Sınırlı Olması

MİT raporunun 10. sayfasında ayrıca aşağıdaki ifade yer almaktadır.

"anılan uygulamanın 15 Temmuz 2016 tarihinden önce, belirli sayıda olmak üzere, Twitter dışındaki çok az platformda yer aldığı"

Fox-IT, 15 Temmuz 2016'dan önce ByLock uygulamasının Twitter dışındaki birden çok platformda barındırıldığını gözlemlemiştir. Google Play Store, Apple Store, apk-dl.com, apkpure.com ve downloadatoz.com, ByLock'u barındıran platformların örnekleri olarak sıralanabilir. Bu platformlar, barındırılan her bir uygulama için son güncelleme tarihi ve saati sağlamaktadır. Bu tarih ve saat ByLock uygulaması için 15 Temmuz 2016'dan çok daha önce başlamıştır. Ayrıca, 15 Temmuz 2016'dan önce Google'da "ByLock" terimi aramasının, uygulamayı barındıran birçok değişik platforma yönlendiriyor olması da kuvvetle muhtemeldir. ByLock'un görünümü, Fox-IT'nin ortalama bir mesajlaşma uygulaması beklentisinden farklı değildir. Uygulama mağazalarında ve İnternet APK indirme sunucularında barındırılır ve sosyal medyada tartışılır. MİT raporundaki ifade, ortalama bir sohbet uygulaması için doğru olmadığı gibi ByLock uygulaması için de doğru değildir.

⁶ Bu tarihten sonra, kurulum sayısı daha da artmıştır. Güncellenen bir sonraki kurulum sayısı 500.000 olmuştur. Bu, son kurulum sayısının 100.000 ile 500.000 arasında olduğunu ortaya koymaktadır.

➤ 4.1.4. Ara Sonuç

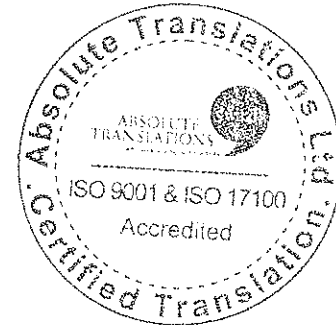
Fox-IT, ByLock soruşturmasıyla ilgili elde mevcut olan (elde edilebilen) tüm bilgilerin kapsamlı bir incelemesini gerçekleştirmiştir. Ayrıca Fox-IT, mümkün olduğu kadarı ile, MİT raporunda yer alan tüm olgu kontrollü gözlem ve olgulara da sahiptir. ByLock soruşturması ile ilgili olarak aşağıdaki sonuçlar elde edilmiştir:

1. Fox-IT, MİT raporunda soruşturma şeffaflığı konusunda genel bir eksiklik gözlemlemiştir. Ayrıca, araştırılan verilerin bütünlüğünün doğrulanmasına olanak tanıyan hiçbir bilgi bulunamamıştır. Her ne kadar soruşturma adımlarının ve veri elde etme yöntemlerin belgelendirilmesi iyi bir uygulama olsa da, bu konularda MİT raporunda çok az bilgi yer almaktadır. Bu durum, araştırılan veri kümesinin ve sonuçların; geçerli ve tam olduğunu, hiçbir ilgili verinin eksik bulunmadığını doğrulamayı imkânsız kılmaktadır.

2. Fox-IT, ByLock uygulama sunucularıyla ilgili gerçekleri ve sonuçları incelemiş ve MİT tarafından gerçekleştirilen soruşturmanın eksik ve yanlış olduğunu tespit etmiştir. Fox-IT'nin araştırması, MİT'in bylock.net alanına ilişkin sonuçlarının da yanlış olduğunu göstermiştir. Ayrıca, Fox-IT, MİT tarafından hiç soruşturulmamış ve ByLock altyapısına ait iki IP adresi (46.166.164.177 ve 46.166.164.181) tespit etmiştir.

3. MİT tarafından yapılan açık kaynak araştırması incelenmiş ve olgu kontrolleri Fox IT tarafından yapılmıştır. Fox-IT, MİT raporunda belirtilen Google Eğilimler gözlemlerinin, gerçek Google Eğilimler sonuçlarından farklı olduğunu göstermiştir. Dahası, Fox-IT, ByLock indirme ve Twitter ile ilgili iddiaların, kanıtlarla desteklenmediğini ve bazı durumlarda Fox-IT tarafından yapılan açık kaynak araştırmaları ile çeliştiğini göstermiştir.

Sonuç olarak Fox-IT, MİT tarafından yapılan soruşturmanın, birçok sorunun gündeme gelmesine sebebiyet verdiği kanaatindedir. Bu soruların cevapları ise ancak daha ayrıntılı bir soruşturmanın yapılmasını gerektirmektedir. Daha fazla rahatsız edici olan ise, birçok bulgunun yeniden çoğaltılamaz ve hatta yanlış olmasıdır. Diğer bazı bulgular ise mevcut veri eksikliği nedeniyle (örneğin, ByLock sunucusu soruşturmasından elde edilen veriler) doğrulanamamıştır. MİT'in ByLock uygulamasının iddia edilen FETÖ/PDY üyelerine münhasıran sunulmadığı olasılığını içeren alternatif senaryoyu araştırdığına dair bir bulgu bulunmamaktadır. Alternatif senaryoları incelemek, bir soruşturma için iyi bir uygulamadır. Alternatif senaryoları incelemek, araştırmacıların önceden tanımlanmış bir sonuca doğru önyargılı olmasını önlemeye yardımcı olmaktadır. Yukarıdaki zikredilen sonuçlar, MİT'in önceden belirtilen sonuca doğru önyargılı olduğunu ve MİT'in bu önyargıya karşı koymak için soruşturmalarında gerekli nesnelliği ve titizliği göstermediğini ortaya koymaktadır.



4.2 MIT'in ByLock Uygulaması Kullanan Kişileri Tespit Etme Yöntemi Ne Kadar Sağlamdır?

- 4.2.1 ByLock Hesaplarını Kişilerle İlişkilendirmek İçin Nasıl Bir Metod Kullanılmıştır ve Bu Metod Ne Kadar Güvenilirdir?

MIT raporu Bölüm 3.6.'da, ByLock veri tabanı verileriyle ilgili soruşturma sonuçlarını açıklamaktadır. Bu bölüm, bireylerin ByLock kullanıcıları olarak tanımlanmasına referans veren tek bölümdür.

MIT raporu, ByLock hesaplarının gerçek kişilerle ne şekilde ilişkilendirildiğini açıklamamaktadır. ByLock hesaplarını bireylerle ilişkilendirmeye dair referans bulunan tek bölüm MIT raporunun 3.6.2.11. bölümüdür. Bu bölümde, MIT, ByLock veri tabanının Log (Günlük) tablosundaki girdileri, kişileri tanımlamak için kullandığını açıklamaktadır. Bu kayıtlar giriş ve kayıt sırasındaki ByLock kullanıcısının IP adresini içermektedir.

MIT raporunda, bu IP adresinin bir bireyle nasıl ilişkilendirildiği açıklanmamaktadır. Bir IP adresinin genelde sadece bir bireye tahsis edilmediğinden dolayı, IP adresinin bir kişi ile ilişkilendirilmesi küçük bir ayrıntı değildir ve yanlış eşleşmeye neden olabilir. Bir IP adresinin bir kişi ile eşleştirilmesinde birçok zorluk bulunmaktadır:

İnternet servis sağlayıcısı günlüğünün tutulması. Bir IP adresi, iletişim için İnternet Protokolünü kullanan bir bilgisayar ağındaki bir aygıtın benzersiz tanımlayıcısıdır. Bilgisayar ağındaki aygıt; kişisel bilgisayar, dizüstü bilgisayar, tablet, telefon, sunucu vb. olabilir. Bir IP adresi, Bölgesel İnternet Kayıtçısı (Regional Internet Registry - RIR) tarafından verilir. Dünyanın belirli bir bölgesi için IP adreslerinin tahsis ve kayıt işlemlerini Beş RIR yönetir. Bir RIR müşterisi, bir İnternet Servis Sağlayıcı (ISS) veya son kullanıcı kuruluş olabilir. Bir IP adresini bir kayıtçıya bağlamak için RIR'dan bilgi edinilebilir. Bununla birlikte, kayıtçı bir ISS olduğunda, o ISS hangi IP'nin hangi müşteriye atandığı bilgisini tutabilir. Bu bilgiler yasal işlemlerle talep edilebilir.

14 Temmuz 2012'de yayınlanan Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi Ve Gizliliğinin Korunması Hakkında Yönetmelik, telekomünikasyon ve altyapı sağlayıcılarının günlük kaydetmeleri konusundaki kuralları içermektedir. Kanun hem telekomünikasyon hem de altyapı sağlayıcılarının, en az 1 yıl boyunca iletişim meta verilerini muhafaza etmesi gerektiğini belirtmektedir⁷.

ByLock günlüklerine kayıt olarak oturum açan bir abonenin tanımlanmasında, MIT'in servis sağlayıcıdan gelen günlük bilgilerini dayanak almış olması muhtemeldir. ByLock sunucusunda günlüğe kaydedilen IP adresleri, bir aboneye belirli bir saatte atanan NAT⁸ adresi veya dinamik adres olabilir. Her iki durumda da, IP adresini bir kişiye atamak için günlük verileri gereklidir.

ByLock soruşturmasının MIT tarafından ne zaman yapıldığı bilinmemektedir (bu bilgi raporda yoktur), ancak 2016'nın sonu olarak tahmin edilmektedir. Bu, 2015'in sonundan önceki iletişim meta verilerinin mevcut olup olmadığı sorusunun ortaya atılmasına neden olmaktadır. Ve eğer bu bilgi mevcut değilse, ByLock IP adreslerini kullanan aboneler nasıl güvenilir şekilde tanımlanabilmiştir?

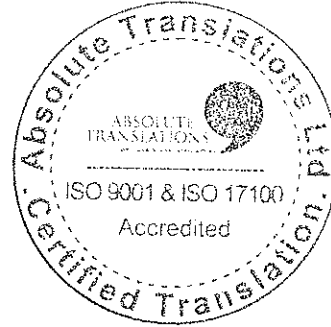
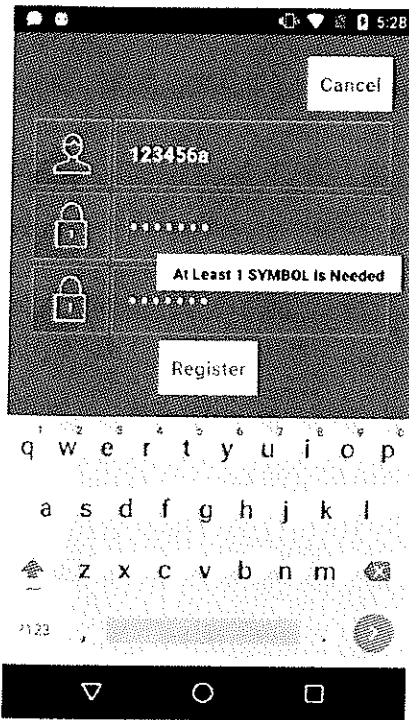
⁷ Telekom yasa ve yönetmelikleri el kitabı, Cilt 1 Stratejik Bilgiler ve Yönetmelikler ISBN-978-1-3291-6456-7.

⁸ Ağ Adresi Çevirimi (Network Address Translation - NAT), ağ adresi bir trafik yönlendirme cihazından geçerken, IP adres alanındaki bilginin değiştirilmesi ile bir IP adresinin diğer bir IP adresi ile değiştirilmesi için kullanılan bir metottur. IP maskelenmesi yöntemini kullanan daha gelişmiş Ağ Adresi Çevirimi uygulamalarında, bir özel ağ için NAT ağ geçidinin bir IP adresini paylaşarak IPv4 adres tükenmesi problemiyle karşı karşıya kalan genel adres alanı tahsislerini koruma konusunu popüler ve gerekli bir araç haline gelmiştir.

Yukarıda belirtilen üç senaryodan herhangi biri bir IP adresinin yanlış bir kişi ile eşleştirilmesine veya bir IP adresinin bir kişi ile eşleştirilmesini imkânsız hale getirmesine neden olabilir. Bireylerin belirlenmesinde bu önemli bir adım olduğundan, bu yöntem ayrıntılı biçimde incelenmelidir. Şu anda MIT, yönteminin incelenmesine imkân veren hiçbir bilgi sağlamamaktadır.

➤ 4.2.2. ByLock Hesapları Nasıl Bir Yolla Oluşturulmuştur ve Başka Kişiler ile İlişkilendirilebilecek Hesaplar Ekleme Mümkün Müdür?

Daha önce belirtildiği gibi Fox-IT, ByLock uygulamasının 1.1.6 ve 1.1.7 sürümlerini analiz etmiştir. Her iki sürümde de kullanıcı, bir kullanıcı adı ve bir şifre girerek kaydolabilmektedir. Şekil 3, ByLock 1.1.7 kayıt ekranını göstermektedir. Bir hesap oluştururken e-posta adresi, telefon numarası veya diğer kişisel kimlik bilgileri istenmemektedir. Fox-IT, ByLock uygulamasının ters mühendisliğiyle, ByLock sunucularına telefon veya kullanıcının başka hiçbir bilgisi gönderilmediğini doğrulamıştır.



Şekil 3. ByLock hesabi kayıt ekranı görüntüsü

Gevşek kayıt düzeni (herhangi bir kişisel bilgi istenmemesi), keyfi hesapların oluşturulmasına izin vermektedir, Çünkü:

- Kullanım koşulu olarak belirli bir grup üyeliği gerektiren hiçbir kısıtlama bulunmamaktadır;
- Uygulama tarafından telefon numarası veya e-posta adresinin doğrulanması yoktur;
- Kayıt sırasında seçilen kullanıcı adında biçim kısıtlaması yoktur. Bu durum, keyfi metin girilmesine izin vermektedir (e-posta adresi, telefon numarası, takma ad v.b.)
- Bir hesabı kaydetmek için davete gerek yoktur. ByLock uygulamasına erişimi olan herkes bir hesabı kaydedebilir.

Bu durum, ByLock hesabının varlığından habersiz olan bir kişi için bile, o şahsa ait ad veya diğer tanımlayıcıyı (örneğin e-posta adresi veya telefon numarası) içeren bir hesabı kaydetmeye ve kullanmaya olanak sağlamaktadır.

➤ 4.2.3. Bir ByLock Kullanıcısının Gerçekten Aktif Olduğunu Tespit Etmek İçin Nasıl Bir Metod Kullanılmıştır ve Bu Metod Ne Kadar Güvenilirdir?

Bölüm 4.2.2'de, keyfi ByLock kullanıcı hesaplarının ByLock uygulamasına erişimi olan herhangi biri tarafından kaydedilebileceği gösterilmiştir. Bu, MİT'in yalnızca ByLock'a kayıtlı olan ve oturum açmış olan kullanıcılar ile ByLock'u gerçekten iletişim kurmak için kullanmış olan kullanıcılar arasındaki farkı nasıl anlayabildiği konusunun gündeme gelmesine neden olmaktadır. Raporda, MİT'in ByLock kullanıcılarının fiili etkinliğini tespit edip etmediği ve eğer tespit etti ise nasıl tespit ettiği konusu açıkça belirtilmemiştir. Bu nedenle, ByLock soruşturmasında belirlenen kişilerin aslında ByLock kullanarak iletişim kurup kurmadığı tam açıklığa kavuşmamıştır.

➤ 4.2.4 Ara Sonuçlar

Fox-IT, ByLock kullanan kişileri tanımlamak için MİT'in kullandığı yöntemleri incelemiştir. Bu incelemenin amacı, yöntemlerin kalitesini belirlemek ve daha sonra tanımlamanın güvenilirliği hakkında sonuca varmaktır. Bu incelemede aşağıdaki sonuçlara ulaşılmıştır:

1. ByLock kullanıcısı olarak kaydolmak için tanımlayıcı hiçbir bilgi (ör. e-posta adresi veya telefon numarası) gerekli değildir. Sonuç olarak, bir ByLock hesabı oluştururken, kendisinden başka birini ima edecek biçimde takma ad kullanarak, kendisinden başka bir kişiyi taklit etmek kolaydır.

2. MİT raporu, ByLock veri tabanındaki IP adreslerinin ByLock kullanan kişileri tanımlamak için kullanıldığını bildirmektedir. Bununla birlikte, rapor, IP adreslerini kişilere ilişkilendirmek için kullanılan yöntemden söz etmemektedir. Bir IP adresinin birey ile eşleştirilmesi önemsiz bir ayrıntı değildir ve yanlış eşleştirmelere yol açabilir. Fox-IT, bir IP adresinin yanlış bir kişi ile eşleştirilmesine ya da hiçbir birey ile eşleştirilememesine neden olabilecek bazı sorunları tespit etmiştir. ByLock kullanan kişilerin belirlenmesinde, bir kaynak IP adresinin bir kişi ile ilişkilendirilmesi önemli bir adım olduğundan, bu yöntemi incelemek mümkün olmalıdır. MİT raporunda, bir kaynak IP adresinin bir kişi ile ilişkilendirilmesi işleminin güvenilir olup olmadığının doğrulamasına imkan veren hiçbir bilgi bulunmamaktadır.

3. MİT raporunda, MİT'in etkin olarak iletişim kuran kullanıcı hesapları ile yalnızca kayıt yapmış ve oturum açmış kullanıcı hesapları arasındaki farkın nasıl belirlendiğinden hiç bahsedilmemektedir. Bu nedenle, ByLock soruşturmasında tespit edilen kişilerin aslında ByLock'u kullanarak iletişim kurup kurmadığı belirsizdir.

Genel olarak, MİT raporu kişilerin tespit edilmesi hakkında çok sınırlı bilgi içermektedir. Fox-IT, ByLock kullanıcı hesaplarının bir birey ile ilişkilendirilmesindeki zorlukları göstermiştir.



4.3 MİT'in, İddia Edilen FETÖ/PDY ile ByLock Kullanıcıları Arasında Bağlantı Bulunduğuna İlişkin Varmış olduğu Sonuç Ne Derecede Güvenilir?

➤ 4.3.1. ByLock Uygulamasının Sadece İddia Edilen FETÖ/PDY Tarafından Kullanıldığı Hükmüne Nasıl Varılmıştır?

Fox-IT, MİT raporunda sunulan argümanları ve sonuçları, Fox-IT'nin yorumladığı şekilde aşağıda özetlemiştir.

MİT, ByLock uygulamasının münhasıran iddia edilen FETÖ/PDY tarafından kullanıldığı hükmüne aşağıdaki bulgulara dayalı olarak varmıştır:

1. ByLock uygulaması, her mesajın bir kript anahtarı ile gönderilmesine izin veren güçlü bir şifreleme sistemi kullanarak internet üzerinden iletişim kurmak üzere tasarlanmıştır. Fox-IT, MİT'in mesajlarda gerçek kript grafik anahtarın kendisini göndermek yerine, mesajların bir şifreleme anahtarı kullanarak şifrelenebileceğini ifade etmeye çalıştığını varsaymaktadır.

2. a. MİT, ByLock'un geliştiricisi hakkında çok sayıda gözlem ve bulguyu ifade etmekte ve geliştiricinin kurumsal veya ticari nitelik taşımadığı sonucuna varmaktadır.

2. b. MİT, ByLock ve Türk dili ve kullanıcıları bakımından bazı gözlemleri belirtmektedir. Ardından MİT, ByLock'un, küresel bir uygulama görüntüsü altında münhasıran iddia edilen FETÖ/PDY terör örgütü mensuplarının kullanımına sunulduğu sonucuna varmıştır. Listelenen argümanlardan bazıları şöyledir:

- Yönetici, Türkiye menşeli IP adreslerini engellemiştir.
- Kullanıcılar kimliklerini gizlemek için VPN kullanmaya zorlanmıştır.
- Google'da "bylock" arama terimi için yapılan aramaların hemen hemen tümü Türkiye'den yapılmıştır ve Türk IP adreslerinden uygulamaya ulaşım engellendiği tarihten itibaren "bylock" arama teriminde önemli bir artış yaşanmıştır.

- ByLock'la ilgili yayınlar, çoğunlukla sahte ve içeriğinin iddia edilen FETÖ/PDY'nin lehine olduğu hesaplar aracılığıyla gönderilmiştir.

- 15 Temmuz 2016'daki darbe girişiminden önce ByLock uygulaması Türk kamuoyunda veya Türkiye dışında bilinmemekteydi.

3. Kullanıcı kimliği ve iletişimi için en üst düzey güvenlik seviyesini sağlamak, ByLock uygulamasının bir amacı olmuştur. Başvuru işlemi sırasında kişisel bilgi gerektirmemesinin ve bir doğrulama sistemi bulunmamasının nedeni de anonimliği sağlamaktır.

4. Uygulama geliştiricisi, doğrulanmış SSL sertifikaları yerine kendisinin oluşturup imzaladığı bir SSL sertifikasını kullanmıştır. Fox-IT, kişisel olarak geliştirilmiş SSL sertifikası terimiyle MİT'in kendinden imzalı sertifikaya atıfta bulunduğunu varsaymaktadır. MİT, burada gözlem ve geliştiricinin niyetleri üzerinden sonuçlara varmaya devam etmektedir. MİT, geliştiricinin kendine ait olmayan sunuculara bilgi akışını engellemek için kendisinin oluşturup imzaladığı bir sertifikanın seçildiğine inanmaktadır.

5. Başka bir kayıtlı kullanıcıyla iletişim kurabilmek için, her iki tarafın karşılıklı olarak birbirinin kullanıcı adını ve kodunu eklemesi gerekmektedir. Bu nedenle, uygulamanın "hücre yapılanmasına" uygun iletişimi sağlayacak şekilde tasarlandığı kabul edilmiştir.

6. Uygulama tüm örgütsel iletişim ihtiyaçlarını karşılamaktadır ve uygulama yöneticisi tarafından kontrol edilerek denetlenmektedir.

7. Manuel müdahale olmaksızın belirli bir süre sonra mesajların cihazdan otomatik olarak silinmesi, sistemin cihazın yasal bir şekilde el konulması durumunda iletişim verisine ve ayrıntılara erişimi engelleyecek şekilde tasarlandığını göstermektedir.

8. MİT, aşağıdaki gözlemlere dayanarak kullanıcıların kimliğini gizleme niyetinde olduğu çıkarımını yapmaktadır:

- Kullanıcılar uzun şifreler oluşturmaktadırlar.

-Kullanıcılar, uygulamayı Android Market veya Apple Appstore yerine APK sitelerinden indirmektedirler.

- Kullanıcılar kayıt sırasında gerçek adlarını kullanıcı kimliği olarak kullanmamışlardır.

- Kullanıcılar irtibat listelerinde ve iletişimlerinde gerçek kimlikler yerine kurumlar arası kod adlarını kullanmışlardır.

Dahası, MİT, şifresi çözülmüş mesajların içeriğinin 'neredeyse hepsi'nin, iddia edilen FETÖ/PDY örgütünün iletişim ve etkinliklerinden oluştuğunu ve kuruluşun jargonuyla eşleştirildiğini belirtmektedir.

9. İddia edilen FETÖ/PDY tarafından yürütülen 15 Temmuz 2016 darbe girişimi sonrasında adli kontrol tedbirlerine tabi tutulan örgüt üyeleri, ByLock'un iddia edilen FETÖ/PDY üyeleri tarafından örgüt içi iletişim aracı olarak kullanıldığını belirtmişlerdir.

Yukarıdakilere dayanarak MİT, ByLock'un sözde terör örgütü FETÖ/PDY'nin üyelerinin münhasır kullanımına sunulduğu sonucuna varmaktadır.

➤ 4.3.2. İfade Edilen Bulgular ve Varılan Sonuçlara İlişkin Fox-IT'nin Görüşü nedir?

Fox-IT, varılan hükmün yukarıda belirtilen MİT bulgularıyla oluşturulamayacağı görüşündedir. Bu bölümde, her bir argüman doğruluk, kesinlik ve sağlamlık tespiti yapmak üzere analiz edilmiştir. Son olarak Fox-IT, genel sonuçlar hakkında bir görüş sunacaktır.

1. Güçlü şifreleme. MİT, ByLock uygulamasının güçlü bir şifreleme algoritması kullandığını belirtmektedir. Güçlü görece bir terimdir ve Fox-IT, ByLock şifrelemesini bilinen diğer sohbet uygulamalarından daha güçlü görmemektedir. Son yıllarda iletişimde kriptografi kullanımı yaygın bir uygulama haline almıştır. WhatsApp ve Facebook gibi kitleler için sohbet uygulamaları, iletişimi güvenli hale getirmek için gelişmiş şifreleme protokollerini içeren Sinyal Protokolünü kullanmaktadır^{10,11}. ByLock uygulamasında kullanılan şifreleme, var olan Java Uygulama Programlama Ara yüzleri (API) kullanılarak kolayca elde edilebilir. ByLock, uygulamanın kullanıcıları arasında şifrelenmiş iletişim sağlamak için standart ve açık Java kütüphanelerini kullanmıştır. Kullanılan kütüphaneler java.security ve javax.crypto'de¹² bulunmaktadır ve gayet iyi belgelenmiştir^{13,14}. Bölüm 4.3.3, ByLock ve diğer uygulamaları arasında güvenlik önlemleri açısından bir karşılaştırmayı daha ayrıntılı bir şekilde sunmaktadır.

2a. Ticari niteliği olmayışı. Yazılımın ticaret özelliklerinin değerlendirilmesi Fox-IT'nin uzmanlığının dışındadır ve bu nedenle Fox-IT bu noktaya değinmemektedir.

2b. Genel uygulamayı gizleme. Bu paragrafta belirtilen sonuç, MİT raporu Bölüm 3.3 ve 3.5'teki bulgulara dayanmaktadır. Fox-IT, bu raporun 6.1. Bölümünde, ilgili bulguların kanıtlarla desteklenmediğini, şüpheli veya yanlış olduğunu göstermiştir. Madde 5, 6, 7 ve 8'de tanımlanan bulguların geçersiz olduğu gösterilmiştir. Bu bulgular olmaksızın, ilgili sonuca ulaşamamaktadır.

3. Güvenlik ve anonimliğin hedeflenmesi. Fox-IT, geliştiricinin, uygulamanın adsız kullanılmasına izin veren güvenli bir iletişim uygulaması oluşturma konusuna odaklanmış olmasının muhtemel olduğunu düşünmektedir. Gizliliğin çok önemli olduğu bir dünyada Fox-IT, ByLock uygulamasının gizliliğin amaçlanması yasadışı faaliyetlerde kullanılması için bir amaç taşımadığı görüşündedir. Benzer amaçlara sahip çok sayıda iyi bilinen ücretsiz uygulama bulunmaktadır. Örneğin, TOR

¹⁰ https://fbnewsroomus.files.wordpress.com/2016/07/secret_conversations_whitepaper-1.pdf

¹¹ <https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf>

¹² <https://docs.oracle.com/javase/7/docs/api/javax/crypto/package-summary.html>

¹³ <https://docs.oracle.com/javase/7/docs/technotes/guides/security/crypto/CryptoSpec.html>

¹⁴ <http://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html>



project¹⁵, internette gizliliği ve güvenliği artıran tanınmış bir anonim tarayıcıdır. Gazetecilerin yanı sıra devlete ait IP adreslerini terk etmeden web sitelerini denetlemek maksadıyla ABD Deniz Kuvvetleri de TOR'u kullanmaktadır¹⁶. Bölüm 4.3.3, ByLock ve diğer uygulamaların güvenlik önlemleri açısından karşılaştırmasını daha ayrıntılı bir şekilde sunmaktadır.

4. Kendinden imzalı sertifika. MIT raporunun, bu konuda ByLock sunucularındaki (HTTPS için) SSL sertifikalarını mı yoksa ByLock uygulaması içerisindeki SSL sertifikalarını mı kastettiği bilinmemektedir. Her iki durumda da, SSL sertifikalarının kimin tarafından imzalandığı MIT raporunun belirttiği gibi "bilgi akışını" etkilemez. SSL sertifikasının HTTPS için olması durumunda, bir otoritenin imzaladığı sertifika, sertifikayı imzalayan otoritenin veriye ulaşmasına izin vermemektedir. Çünkü oluşturulan özel anahtar otorite ile paylaşılmamaktadır. Bu noktada MIT tarafından yürütülen mantık çok net değildir ve MIT raporunu yazanın açık anahtar altyapısı ve SSL sertifikaları hakkında yanlış bilgiye sahip olduğunu düşündürmektedir.

Fox-IT, geliştiricinin kendinden imzalı sertifika kullanmasının amacının kendi sunucuları dışındaki yerlere veri akışını engellemek için olmasını pek olası görmemektedir. Genel olarak, kendinden imzalı sertifikanın uygulanması daha kolaydır ve maliyetsizdir. Bu durumun, kendinden imzalı sertifikanın kullanması için bir teşvik unsuru olması daha akla yatkındır.

5. İletişimin yalnızca hücre yapılanmasına uygun bir şekilde olması. Bu bağlamda hücre yapılanması terimi tanımlanmamış ve belirsizdir. Fox-IT, burada iddia edilen FETÖ/PDY'nin örgütlenme biçimini ifade ettiğini varsaymaktadır. Örgütsel yapılar Fox-IT'nin uzmanlığının dışındadır.

Kayıt işlemi ile ilgili olarak, oturum bilgilerini paylaşmak için yüz yüze görüşme veya arabulucu ile bilgi alışverişinin sağlanmasının farkının konu ile ilgili olduğu düşünülmektedir. Rapor, ByLock ayrıntılarının bant dışından değiş tokuşunun yapıldığı daha muhtemel üçüncü bir senaryoyu tanımlamamıştır: Başka bir iletişim yöntemini (örneğin, telefon görüşmesi, WhatsApp, Facebook, Skype) kullanmak. İki kişinin WhatsApp üzerinden iletişim kurduğunu varsayarsak (MIT raporu iki kişinin WhatsApp üzerinde bir araya geldiğini incelememiştir), bu kişiler WhatsApp üzerinden kendi ByLock ayrıntı bilgilerini değiş tokuş edebilir ve ardından ByLock üzerinden iletişime geçebilirler.

6. Örgütsel iletişim ihtiyaçları. Örgütün iletişim ihtiyaçlarının değerlendirilmesi Fox-IT'nin uzmanlığı dışındadır ve bu nedenle Fox-IT bu konuyla ilgili değerlendirme yapmamıştır.

7. Yasal soruşturma durumunda erişimin engellenmesi. Fox-IT, bu argümana ilişkin MIT raporuna katılmak ya da katılmamak için geliştiricilerin niyetleri hakkında yetersiz bilgi olduğu yönünde bir kanaat edinmiştir. Fox-IT, eğer MIT'in sonuçlarını doğrulayan daha fazla bilgi mevcut değilse, MIT'in raporda belirtilen gözlemlere dayanarak geliştiricinin niyetine ilişkin yeteri kadar bilgi edinmeksizin doğrudan karara vardığını düşünmektedir. İletilerin otomatik olarak silinmesi SnapChat¹⁷ gibi popüler sosyal medya uygulamalarında da kullanılmaktadır. Bölüm 4.3.3, ByLock ve diğer uygulamaların güvenlik önlemleri açısından karşılaştırılmasını daha ayrıntılı bir şekilde sunmaktadır.

8. Kimlik gizleme. Fox-IT, kullanıcıları özellikle kimlik gizleme amaçlı olmadığı görüşündedir:

- Uzun şifreler oluşturma

ByLock'da bir şifre seçmenin minimum gereksinimi altı karakter artı en az bir sembol seçimidir. MIT, şifresi çözülmüş parolaların 38 karakter uzunluğundaki parolaları içerdiğini ve bunların yarısının en az 9 karakter uzunluğunda olduğunu bildirmektedir. Güçlü bir şifre kullanımı güvenlik nedenleriyle önemlidir ve kimliğinizi saklamanın bir yolu olarak görülemez. Şifreniz ne kadar güçlüyse, hackerlar

¹⁵ <https://www.torproject.org/>

¹⁶ <https://www.torproject.org/about/torusers.html.en>

¹⁷ <https://www.snapchat.com/>



tarafından şifrenin kırılması o kadar zor olur¹⁸. Haziran 2017'da yayınlanan Ulusal Standartlar ve Teknoloji Enstitüsü yeni yönergelerine göre¹⁹, şifrelerde en az 8 karakter kullanılması önerilir ve uygulamalar en fazla 64 karakter uzunluğa izin vermelidir.

- Uygulamanın APK web sitelerinden manuel olarak indirilmesi.

Google Play Store'dan bir uygulama başlatmak için uygulamanın çeşitli gereksinimleri^{20, 21} karşılaması gerekir. Bu, kullanıcı beklentilerinin karşılanması için garanti altına alınması maksadıyla, Google'ın yaptığı bir uygulamadır. Bazı geliştiriciler, uygulamalarını kullanım kolaylığı için diğer APK web sitelerinde sunmayı tercih etmektedir. Bununla birlikte, geliştiricinin niyeti doğrulanamamıştır.

- Kayıt sırasında kullanıcı adı olarak başka bir ad kullanılması.

Mesajlaşma uygulamalarının çoğu (WhatsApp ve SnapChat gibi) kullanıcının gerçek adının kullanılmasını gerektirmez. Aslında, kullanıcı kimliği olarak başka bir ad kullanmak da oldukça yaygındır. Bu, sohbet uygulamalarının genel kullanımı, sosyal medya platformları ve genel internet hizmetleri için de geçerlidir.

9. ByLock'in, darbe girişimi sırasında kullanılması. Fox-IT, ByLock'un iddia edilen FETÖ/PDY tarafından kullanıldığına dair ifadeyi doğrulayamamaktadır. Bununla birlikte her durumda, bu argüman, istatistiklerdeki temel oran yenilgisi nedeniyle geçersizdir²². Aşağıdaki ifade, yanlış algıyı göstermektedir:

Bir terör örgütünün tüm üyeleri ByLock'u kullanmaktadır, bu nedenle ByLock kullanıcıları terör örgütünün üyesidirler.

Bu mantık sıklıkla yapılan bir hatadır. Bu akıl yürütmeye çok basit ve sezgisel bir benzetme aşağıda verilmiştir:

Bütün balıklar yüzer, bu nedenle yüzen her şey bir balıktır.

Bu ifade açıkça yanlıştır. Bununla birlikte bu ifadenin yaklaşık olarak gerçekliği açıkladığı izlenimi edinilebilir (neredeyse yüzen her şey balıktır). Bununla ilgili olarak, aşağıdaki örneği göz önüne alalım:

10,000 kişide 1 kişi çevrimiçi suçlusudur

1000 kişiden 1 kişi TOR kullanmaktadır

Tüm suçlular TOR ağını iletişim için kullanmaktadır

Kaç tane TOR kullanıcısı suçludur?

Cevap sadece 10'da 1'dir. Dolayısıyla, tüm suçlular TOR'u kullanıyor olsa da, TOR kullanıcılarının sadece 10'undan 1'i suçludur²³.

Aslında, iddia edilen tüm FETÖ/PDY üyelerinin ByLock'u kullandıklarını varsayarsak (pek mümkün olmasa da), iddia edilen FETÖ/PDY'ye üye olmayan çok sayıda ByLock kullanıcısı olacaktır. Tam sayı, gerçek FETÖ/PDY üyelerinin taban oranı ile belirlenir.

Fox-IT, yukarıda açıklanan analizlere dayanarak, MIT tarafından sunulan bulguların, ByLock'un sadece iddia edilen FETÖ/PDY üyeleri tarafından örgütler arası bir iletişim ortamı olarak kullanıldığı²⁴ sonucunu desteklemediği görüşündedir.

➤ 4.3.3. Güvenlik Açısından, ByLock Uygulaması, Diğer Benzeri Mesajlaşma Uygulamaları ile Nasıl İlişkilidir?

Bu bölümde, Fox-IT, ByLock uygulaması ile diğer bilinen iletişim uygulamaları arasındaki

¹⁸ https://en.wikipedia.org/wiki/Brute-force_attack

¹⁹ <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf>

²⁰ <https://developer.android.com/distribute/best-practices/launch/launch-checklist.html>

²¹ <http://r-stylelab.com/company/blog/mobile-technologies/how-to-meet-google-play-requirements>

²² https://en.wikipedia.org/wiki/Base_rate_fallacy

²³ Bu durum Bayes teorisi kullanılarak hesaplanabilir: $P(\text{suçlu} | \text{Tor}) = P(\text{Tor} | \text{suçlu}) * P(\text{suçlu}) / P(\text{Tor})$

²⁴ MIT raporunda "münhasıran kullanıma sunulması" ifadesi geçmektedir. Fox-IT bunu kullanmak olarak yorumlamıştır.



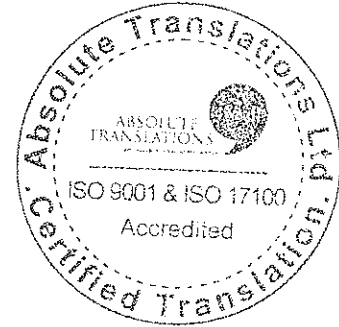
karşılaştırma ayrıntılarıyla ele alınacaktır. MIT raporunu yazarlar, ByLock'un güvenlik özelliklerinin (MIT rapor Bölümü 4.1, 4.3, 4.7), iddia edilen FETÖ/PDY terör örgütü mensuplarının münhasır kullanımına sunulduğu sonucuna varmak için argümanlar taşıdığını ileri sürmektedir. Bu araştırmanın amacı, ByLock'un güvenlik özelliklerini diğer mesajlaşma uygulamaları bağlamında karşılaştırmak ve güvenlik özelliklerinin ByLock'u diğer sohbet uygulamalarından ne derece ayırt ettiğini belirlemektir.

Şifreleme

Paragraf 4.3.1'de belirtildiği gibi, şifreleme kullanımı son yıllarda iletişimde yaygın bir uygulama haline gelmiştir. Fox-IT tarafından yapılan soruşturma sonucunda ByLock uygulamasında kullanılan şifreleme, varsayılan Java Uygulama Programlama Arabirimi (API) kullanılarak sağlanan standart ve genel kullanıma açık Java kütüphaneleri vasıtasıyla oluşturulmuştur. Bununla birlikte, diğer sohbet uygulamalarında daha karmaşık şifreleme teknikleri vardır. Electronic Frontier Foundation (EFF), 6 Kasım 2014 tarihinde, uygulamaların şifreleme özelliklerine genel bakış sunan bir puan kartı²⁵ uygulaması başlatmıştır (Şekil 4). Bu skor kartı son olarak 4 Mayıs 2016'da güncellenmiştir. Bu şekilde, WhatsApp'ın en güvenli sohbet uygulamalarından biri olduğu görülmektedir. Ayrıca, son kaynaklara göre^{26, 27} araştırılan sohbet uygulamaları arasında, WhatsApp en güvenli iletişim uygulamasıdır ve Temmuz 2017 itibarıyla 1,3 milyar kullanıcıya sahiptir²⁸. Bu, genel olarak kullanıcılar için şifrelemenin ve dolayısıyla güvenli mesajlaşma özelliğinin önemini göstermektedir.

Şekil 4, sohbet uygulamalarını güvenlik konusunda puanlamak için EFF tarafından kullanılan güvenlik özelliklerini listelemiştir. Bu özelliklerin arasında, ByLock uygulamasında sadece iki özellik bulunduğu Fox-IT tarafından doğrulanmıştır:

1. Gönderim anında şifreleme;
2. Uygulama sahibi tarafından okunamayacak şekilde şifreleme.



²⁵ <https://www.eff.org/node/82654>

²⁶ <http://www.techworld.com/security/best-secure-mobile-messaging-apps-3629914/>

²⁷ <http://www.techradar.com/news/top-10-best-secure-messaging-apps-of-2017>

²⁸ <https://www.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users/>

	Encrypted in transit?	Encrypted in the provider can't read it?	Can provider's contacts' identities?	Are text contents secure if sent here are stolen?	Is the code open to independent review?	Is security design properly documented?	Has there been any recent code audit?
WhatsApp	✓	✗	✗	✗	✗	✗	✗
Facebook chat	✓	✗	✗	✗	✗	✗	✓
Google Hangouts/Chat/Text for Android	✓	✗	✗	✗	✗	✗	✓
Skype	✓	✓	✗	✓	✗	✓	✓
Line Chat	✓	✓	✓	✓	✓	✓	✗
On The Border Messaging for Android/iOS/Apple	✓	✓	✓	✓	✓	✓	✗
On The Border Messaging for Android/iOS/Apple	✓	✓	✓	✓	✓	✓	✓
Viber	✓	✗	✗	✗	✗	✗	✗
Telegram	✓	✗	✗	✗	✗	✗	✓
Signal	✓	✓	✓	✓	✓	✓	✓
BlackBerry	✓	✓	✓	✓	✗	✓	✓

Sekil4. EFF tarafından hazırlanan güvenli mesajlaşma skor kartı.

Mesajın Kendisini Yok Etmesi

ByLock'un dışında, Snapchat, kendini yok eden bir mesaj özelliğiyle tanınmış ve popüler bir mesajlaşma uygulamasıdır. Snapchat 2011'de ilk defa sürülmüştür ve 173 milyon kullanıcıya sahiptir²⁹. Ayrıca, 800 milyon kullanıcısıyla Viber sohbet uygulaması da kendini imha özelliğini eklemiştir³⁰.



²⁹ <https://www.statista.com/statistics/545967/snapchat-app-dau/>

³⁰ <https://www.theverge.com/2017/3/10/14879986/viber-secret-chats-self-destructing-encryption>

Kullanıcı tarafından oluşturulan içeriğin ve mesajların belirli bir süre sonra kendiliğinden silindiği diğer sohbet uygulamaları aşağıda sunulmuştur:

- Telegram³¹
- Bleep³²
- Wickr³³
- Confide³⁴
- SpeakOn³⁵

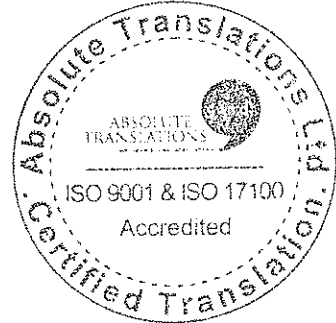
Bu araştırma, milyonlarca kullanıcının katıldığı çok sayıda Android uygulamasının bu güvenlik özelliğini uyguladığını göstermektedir. Bu nedenle, ByLock istisnai derecede güvenli görünmemektedir.

➤ 4.3.4. Ara Sonuçlar

Fox-IT, MIT raporunu, sonuca varırken kullandığı mantık kalitesini belirlemek için incelemiştir. Sonuç olarak, MIT, ByLock'un güvenlik önlemlerine ve geliştiricinin iddia edilen amaçlarına büyük önem atfetmektedir. Bu nedenle Fox-IT, ByLock'un güvenlik özelliklerini mevcut diğer sohbet uygulamaları bağlamına taşımak için diğer sohbet uygulamalarıyla karşılaştırma yapmıştır.

Bu karşılaştırmada Fox-IT, ByLock'ta uygulanan güvenlik önlemlerinin olağanüstü olmadığını ve aslında yaygın olarak kullanılan sohbet uygulamaları ile eşit seviyede olduğu sonucuna ulaşmıştır. Veri iletiminde veri güvenliği ve şifrelerin karılması için herkesçe bilinen şifreleme protokolleri ve kendini imha eden mesajlar milyonlarca kullanıcı tarafından kullanılan diğer haberleşme uygulamalarında da kullanılmaktadır. Dolayısıyla, MIT raporunun 1, 3 ve 7. maddelerdeki sonuçlarında belirtilen özellikler, ByLock'un belirli bir kullanıcı grubuna ait olduğunu (FETÖ/PDY olduğu iddia edilmektedir) veya güvenli iletişim kurmak dışında başka bir amacı olduğunu göstermez.

MIT raporunun sonuçları Fox-IT tarafından ayrıntılı biçimde incelenmiş ve değerlendirilmiştir. Öne sürülen argümanların ciddi biçimde kusurlu olduğu ve belirtilen dokuz argümandan yedisinin geçersiz veya şüpheli olduğu gösterilmiştir. Bu yargı, Bölüm 4.1'de açıklanan Fox-IT bulgularına dayanmaktadır. Geriye kalan argümanlar ise, MIT'in sonuçlarını desteklemek için tek başına yeterli değildir. Sonuç olarak, MIT raporunda yer alan "ByLock, münhasıran iddia edilen FETÖ/PDY terör örgütünün üyelerinin kullanımına sunuldu" hükmü sağlam değildir.



³¹ <https://telegram.org/>

³² <https://n0where.net/chat-privately-bleep/>

³³ <https://www.wickr.com/>

³⁴ <https://getconfide.com/>

³⁵ <https://www.crunchbase.com/organization/speakon#/entity>

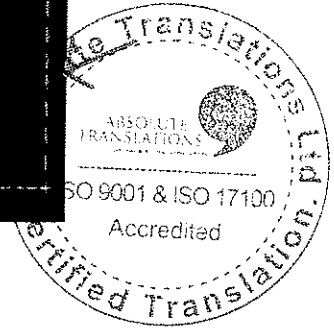
4.4. ByLock Soruşturması ile İlgili Olarak Fox-IT Tarafından Tespit Edilen Başka Hususlar Var mıdır?

➤ 4.4.1. Dikkat Çekici Tutarsızlıklar

MİT raporunun Bölüm 3.6.2.4'teki Şekil 5 (SQL çıktısının ekran görüntüsü) ve Bölüm 3.6.2.15'teki Şekil 15 (başka bir ekran görüntüsü) dikkat çekicidir. Ekran görüntüleri, satırları ve toplam satır sayısını gösteren bir SQL sorgusunun çıktısını göstermektedir. Toplam satır sayısı, gösterilen satırların gerçek sayısı ile eşleşmemektedir. Ayrıca, sıralarda ince bir aralık farkı vardır. Bu, ekran görüntüsünün veya çıktısının manipüle edilmiş olmasını akla getirmektedir. Şekil 5 tutarsızlığı göz önüne sermektedir.

3.6.2.4"chat" table:

Field	Type	Null	Key	Default	Extra
id	int(11)	NO	PRI	NULL	
fromUserId	int(11)	NO	MUL	NULL	
toUserId	int(11)	NO	MUL	NULL	
ciphertext	text	NO		NULL	
signature	varchar(512)	NO		NULL	
sentTime	timestamp	NO		CURRENT_TIMESTAMP	
receivedTime	timestamp	NO		0000-00-00 00:00:00	
8 rows in set (0.00 sec)					



Sekil 5. SQL çıktısının ekran görüntüsündeki tutarsızlık.

Fox-IT, MİT raporu Bölüm 3.6.2.15'deki aşağıdaki durumu da belirlemiştir:

Kullanıcı tablosunda depolanan, şifresi çözülmüş verilere örnekler aşağıda gösterilmiştir:

("Kullanıcı Adı" tabiri, kullanıcı adı / kodunu ve "düz" ise yapılan çalışmalar sonucu şifresi çözülmüş kullanıcı şifresini belirtir.)

Yukarıdaki "düz" sütununun analiz için MİT tarafından kullanıcı tablosuna eklendiğini göstermektedir.

Ayrıca, MİT raporu Bölüm 3.5.5, komut satırı çıktısı olduğunu düşündüren bir liste içermektedir. Liste şunları göstermektedir:

```
root@hst-46-166-160-137:~#  
iptables -N LOGGING  
iptables -A INPUT -s 5.2.80.0/21 -j LOGGING  
...
```

Bu liste iptables komutunun çıktısını göstermektedir. Bununla birlikte, komutun kendisi listede görünmemektedir. Komut satırı öneki (root@hst-46-166-160-137:~#) görünür olduğundan, bu beklenmedik bir durumdur. Bu, komutun bu girişten kaldırıldığını göstermektedir. Sonuç olarak, hangi komutun girildiği bilinmemekte ve okuyucu, çıktının temsil ettiği şeyi doğrulayamamaktadır.

MİT raporu Bölüm 3.6.2.11 şekil 11'de başka bir tutarsızlık bulunmuştur. Resimde "log" tablosu okunurken gösterilen sorgu komutu olarak "select * log2 liMiT 50" kullanılmıştır. Halbuki başlıkta "log" tablosu yer almaktadır. Bu, analistlerin bir tablo ekledikleri veya değiştirdikleri ve log2 olarak

adlandırdıklarını akla getirmektedir. Tablodaki diğer bilgilerin eklenip eklenmediği, kaldırıldığı veya değiştirilip değiştirilmediği açık değildir.

Yukarıdaki tutarsızlıklar, açıklama yapılmaksızın veri tabanı sonuçlarının veya ekran görüntülerinin tahrif edilip değiştirildiğini gösterdiğinden ötürü sorunludur. Sonuç olarak, rapordaki bilgilerin hangisinin orijinal veri olduğu ve hangi bilgilerin, hangi amaçla MİT tarafından değiştirildiği açık değildir. Bu durum, sunum öncesinde nelerin değiştirildiğinin, niçin değiştirildiğinin ve tam olarak neyin dışarıda bırakıldığının sorgulanmasına neden olmaktadır. Bilgileri kanıt olarak sunarken, şeffaflık, orijinal veriler (gerçek kanıtlar) ile analist tarafından eklenen veya değiştirilen veriler arasındaki ayrımın yapılması çok önemlidir.

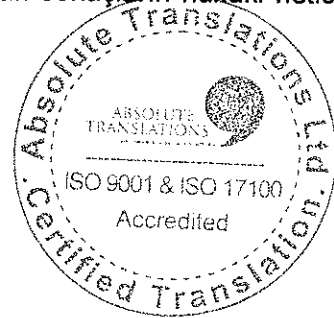
➤ 4.4.2 Raporlama Biçimi ve Okunabilirlik

Genel olarak Fox-IT, MİT raporunu üstü kapalı, iyi yapılandırılmamış ve temel ayrıntılardan yoksun bulmaktadır. Bu sadece bir biçimlendirme sorunu değildir. Önemli ayrıntıları atlayan, okunamayan bir rapor yazmak, okuyucunun soruşturmayı inceleme imkânını azaltır. Bir rapor ciddi hukuki sonuçların temeli olarak kullanıldığında, yazar soruşturma ile ilgili hiçbir soru bırakmamak için raporda kusursuz ve özenli olmalıdır.

Aşağıdaki örnekler bu sorunu göstermektedir:

- Yazma tarihi ve sürüm yönetimi gibi temel belge yönetimi bilgileri eksiktir.
- Fiili soruşturma soruları hakkında hiçbir açıklama yapılmamıştır. Soruları ortaya koymak, okuyucuya, atılan adımları izlemek için bağlam bilgisi sağlar ve araştırmacıların soruşturma için tarafsız bir başlangıç noktası olduğunu gösterir. Sonuçlar, bundan sonra soruşturma sorularıyla ilgili olarak değerlendirilebilir.
- MİT raporunun 4. bölümündeki 2. maddede yazar, ByLock'ın geliştiricisi ve niyeti ile ilgili altı "sonuç ve değerlendirme"yi açıklamaktadır. Bu maddeler çok açık ve belirgin olmadıkları gibi raporun içinde de açıklanmamıştır. Ayrıca, gerçek yada bulgu olarak sunulduklarından raporda bu maddelerin ilk bahsedildiği yerin sonuçlar olmaması gerekir.
- Bu bölümdeki 2. maddenin sonuç kısmında "... uygulamanın global bir uygulama maskesi altında FETÖ/PDY üyeleri tarafından kullanıma sunulduğu" sonucuna varmaktadır. Bununla birlikte, bölüm 4, daha fazla argüman listesi yapmaya devam etmekte ve daha sonra yine bir benzer sonuca varmaktadır. Bu sonuçların birbirleriyle nasıl ilişkili olduğu ve nihai sonucun dayandığı argümanlarının ne olduğu açık değildir.

Fox-IT son 15 yılda birçok dijital soruşturma raporu okumuş ve yazmıştır. Bu tecrübeye dayanarak, Fox-IT MİT raporunun kalitesini, özellikle raporda varılan sonuçların hukuki neticeleri göz önüne alındığında, çok düşük bulmaktadır.



5 - SONUÇLAR

Bu bölüm, bu bilirkişi raporunda Fox-IT tarafından ele alınan konuların her biriyle ilgili varılan sonuçları sunmaktadır. Fox-IT soruşturma yaklaşımının ve sonuçlarının daha ayrıntılı bir dokümantasyon bu raporun 3. ve 4. bölümlerinde bulunabilir.



5.1. ByLock Soruşturmasında MİT Tarafından Kullanılan Soruşturma Metodu Hakkında Fox-IT'nin Düşünceleri Nelerdir?

MİT soruşturmasındaki birçok temel bulgu, Fox-IT tarafından yapılan açık kaynak araştırmasıyla çelişkilidir ve diğer bulguların ise MİT tarafından sunulan kanıtlarla desteklenmediği görülmüştür. Dahası, MİT soruşturması şeffaflıktan yoksundur. Delil ve analiz adımları çoğu durumda MİT raporunda atlanmıştır. Birçok bulgunun (doğrulanabilir olanlar) yanlış olduğu görülmüştür. Bu durum, doğrulanma olasılığı bulunmayan bulgulardan birçoğunun da doğrulanabilir olması durumunda, yanlış ya da tutarsız olduğunun kanıtlanabileceği izlenimini bırakmaktadır.

MİT'in alternatif başka bir senaryoyu (ByLock'un münhasıran iddia edilen FETÖ/PDY üyelerinin kullanıma sunulmadığı senaryosu) oluşturduğu yönünde bir gösterge bulunmadığından, Fox-IT, MİT soruşturmasının nesnellikte eksik olduğu sonucuna varmaktadır. Bir soruşturmada alternatif senaryoların araştırılması iyi bir uygulamadır. Alternatif senaryo, araştırmacıların önceden tanımlanmış bir sonuca doğru, peşin hükümlü şekilde, dar bir bakış açısı ile sınırlandırılmasının önlenmesine yardımcı olur. Fox-IT'nin MİT soruşturması üzerine yaptığı incelemede, MİT'in önceden belirtilen sonuca doğru önyargılı olduğu ve MİT'in bu önyargıya karşı koymak için soruşturmalarında gerekli nesnelliği ve titizliği göstermediği gözlemlenmiştir.

Fox-IT, MİT raporunda tanımlanan MİT soruşturmasının, bu raporun 3. bölümünde özet halinde verilen adli ilkelere bağlı kalmadığını ve bu nedenle adli soruşturma olarak görülmemesi gerektiği sonucuna varmıştır. Soruşturma, çelişkili ve asılsız bulguları, nesnellikten ve şeffaflıktan uzak olması nedeniyle temelden kusurludur. Fox-IT, ByLock hakkında daha kapsamlı, objektif ve şeffaf bir adli soruşturma yürütülmesini önermektedir.

5.2 MİT'in ByLock uygulaması Kullanan Kişileri tespit etme yöntemi Ne kadar Geçerlidir?

MİT raporu, kişilerin tespiti hakkında çok sınırlı bilgi içermektedir. Fox-IT, ByLock kullanıcı hesaplarının tek başına bir birey ile ilişkilendirilmesinin zor olduğunu göstermiştir. ByLock hesabı oluştururken, diğer bireylerin kimliğine bürünmek kolaydır ve MİT, kişilerin tespit edilmesinde ByLock sunucu günlüğünde bulunan IP adresi bilgisinden başka bir bilgiye sahip değildir. Bu IP adresini gerçek kişilerle ilişkilendirmek basit değildir ve hataya açık bir işlemdir. Bu nedenle yanlış kişilerin ByLock kullanıcıları olarak tanımlanmasına yol açabilir.

MİT raporu bu yöntem hakkında bilgi vermediğinden, Fox-IT, tanımlama yönteminin sağlamlığını değerlendirememiştir. Bu metodun açıklanmasının ihmal edilmesi rahatsızlık vericidir. Yöntemdeki hatalar ortaya konulamamaktadır ve okuyucunun MİT'in hata yapmadığını varsayması beklenmektedir. Şeffaflık adli tıp araştırmalarının temel ilkelerinden biri olsa da soruşturmanın bu kritik kısmı şeffaflıktan tamamen uzaktır.

5.3. MİT'in, FETÖ/PDY ile ByLock Arasında İlişki Olduğu Hükmünün Sağlamlık Niteliği Nedir?

MİT raporunun sonuçları ve bulguları Fox-IT tarafından incelenmiştir. Değerlendirme safhasının ciddi şekilde kusurlu olduğu ve belirtilen dokuz argümanın yedisinin yanlış veya şüpheli olduğu

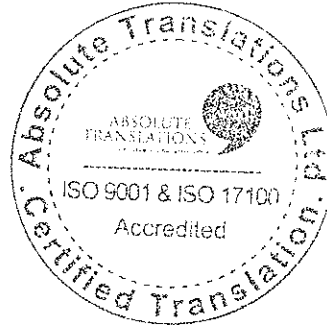
gösterilmiştir (bkz. Sonuç 6.1). Geriye kalan iki argüman kendi başına, MİT'in sonuçlarını desteklemek için yeterli değildir. Sonuç olarak, MİT raporunun çıkarsaması olarak ortaya konulan "ByLock, münhasıran FETÖ/PDY terör örgütünün üyelerinin kullanımına sunuldu" hükmü, sağlam bir hüküm değildir.

5.4. Fox-IT Tarafından Tespit Edilen ByLock Soruşturması ile İlgili Başka Hususlar Var mıdır?

Fox-IT, MİT raporunda sonuçların ve/veya ekran görüntülerinin MİT tarafından tahrif edildiğini gösteren tutarsızlıklarla karşılaşmıştır. Rapordaki bilgilerin hangisinin orijinal veriden kaynaklandığı ve hangi bilgilerin MİT tarafından (hangi maksatla) değiştirildiği belli olmadığından, bu durum oldukça sorunludur. Bu, MİT'in mevcut bilgilerin hangi bölümünü sunulmadan önce değiştirdiği, niçin değiştirildiği ve tam olarak hangi kısımların dışarıda bırakıldığı veya değiştirildiği sorularını gündeme getirmektedir. Bilgileri kanıt olarak sunarken, orijinal veriler (gerçek kanıtlar) ile analist tarafından eklenen veya değiştirilen veriler arasındaki ayrımın yapılması, şeffaflık açısından çok önemlidir.

Dahası, Fox-IT, MİT raporunu örtülü, kapalı, iyi yapılandırılmamış ve önemli detaylardan yoksun olarak değerlendirmektedir. Kötü raporlama yalnızca bir biçimlendirme sorunu değildir. Önemli ayrıntıları atlayan ve okunamayan bir rapor yazmak, okuyucunun sonuçlara götüren soruşturmayı detaylı inceleme imkânını azaltır. Bir rapor ciddi hukuki sonuçların temeli olarak kullanıldığında, yazar soruşturma ile ilgili hiçbir soru bırakmayacak biçimde kapsamlı ve öz olmalıdır.

Fox-IT son 15 yılda birçok dijital soruşturma raporu okumuş ve yazmıştır. Bu tecrübeye dayanarak, Fox-IT MİT raporunun kalitesini, özellikle varılan hükümlerin hukuki sonuçları göz önüne alındığında, çok düşük bulmaktadır.



6 - İNCELENEN BELGELER ve VERİLER

Soruşturma sırasında Fox-IT tarafından aşağıdaki belgeler incelenmiştir:

1. ByLock uygulaması teknik raporu. MİT'in raporu, yeminli bir tercüman tarafından Türkçe'den Hollandaca'ya çevrilmiştir. Hollandaca rapor, İngilizce dil için yeminli tercüman tarafından Hollandaca'dan İngilizce'ye çevrilmiştir. Türkçe, tercüme edilen İngilizce ve Hollandaca dokümanlar 19 Temmuz 2017'de Müvekkil tarafından Fox-IT'ye fiziksel dokümanlar olarak teslim edilmiştir.

Fox-IT, bu soruşturma sırasında halka açık olan ByLock uygulaması sürümlerini analiz etmiştir. ByLock Android uygulamasının aşağıdaki sürümlerinin halen mevcut olduğu tespit edilmiş ve incelenmiştir.

2. Android için ByLock 1.1.6. Uygulama, http://downloadapk.net/down_ByLock-Secure-Chat-amp-Talk.601634.html adresinden bir APK dosyası olarak indirilmiştir. Dosya 20 Temmuz 2017 tarihinde indirilmiştir. Fox-IT, dosyanın kriptografik özet fonksiyonu değerlerini aşağıdaki gibi hesaplamıştır:

MD5 karma³⁶ b43eeb3fed4c20061e0c87f4d371508d

SHA1 karma aeb4256fa23d0d5090c5506e2d647f8d6a63f4af

3. Android için ByLock 1.1.7. Uygulama, <https://m.downloadatoz.com/bylock-secure-chat-talk/net.client.by.lock/bylock-secure-chat-talk,v1.1.7-download.html> adresinden bir APK dosyası olarak indirilmiştir. Dosya 20 Temmuz 2017 tarihinde indirilmiştir. Fox-IT, dosyanın kriptografik özet fonksiyonu değerlerini aşağıdaki gibi hesaplamıştır:

MD5 karma 84fddf10a23f4f25b5212232b73cd557

SHA1 karma cac87620162e211b4fb02719a244b8127610cb7e

Aşağıdaki sürümler MİT raporunda belirtilmiştir, ancak analiz etmek için kamuya açık çevrimiçi kaynaklarda artık bu sürümlerin mevcut olmadığı tespit edilmiştir:

ByLock for Android 1.1.3

Android 2.0 için ByLock (ByLock ++)



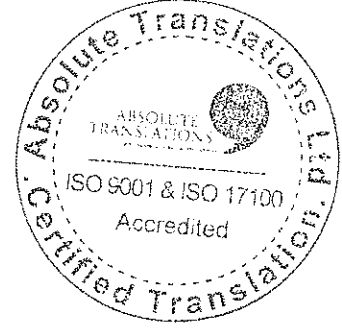
³⁶ Bir kriptografik özet fonksiyon değeri, bir algoritma kullanarak hesaplanmış matematiksel bir ifadenin sonucudur. Hesaplama yalnızca bir yönde çalışır, yani orijinal veriyi belirlemek için karma değer kullanılamaz. Bir kriptografik özet fonksiyon değeri, verinin dijital parmak izini temsil eder ve bir dizi sayıdan (sabit uzunlukta) oluşur. Genellikle, adli olarak sağlam bir kopyanın oluşturulması sırasında bir kriptografik özet fonksiyon değeri kaydedilir. Böylece kopyanın bütünlüğü, karma değerini tekrar hesaplayarak ve orijinal olarak kaydedilen kriptografik özet fonksiyon değeri ile karşılaştırarak kontrol edilebilir. Bilinen ve yaygın olarak kullanılan kriptografik özet fonksiyon algoritmaları MD5, SHA1 ve SHA256'dır.

7 - EKLER

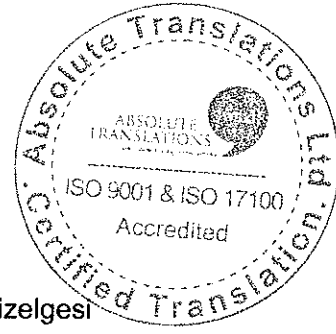
7.1. ByLock.net Zaman Cizelgesi

Aşağıdaki tabloda, zaman içinde bylock.net alan adı tarafından başvuru mülkiyet bilgilerindeki ve IP adreslerindeki değişiklikleri listelenmiştir.

[SAYFA 31 VE 32'DE BULUNAN TABLO]



[SAYFA 31 VE 32'DE BULUNAN TABLO]



Tablo 3: Bylock.net zaman çizelgesi

7.2. Teknik Terimlerler Sözlüğü

Android Paket Kiti

Android işletim sistemi tarafından mobil uygulamalar ile ara katman yazılımlarının dağıtımı ve kurulumu için kullanılan paket dosya biçimi.

APK

bakınız, Android Paket Kit

Kaynak Koda Dönüştürme

Çalıştırılabilir bilgisayar kodunun kaynak koda (geri) dönüştürmek için kullanılan bir teknik. Genellikle bir programın çalışmasını analiz ederken kullanılmaktadır.

DNS

bakınız, Alan Adı Sistemi

Alan Adı Sistemi

İnternet'e veya bir özel ağı bağlı bilgisayarlar, hizmetler veya diğer kaynaklar için hiyerarşik dağıtık bir adlandırma sistemi. Katılımcı varlıkların her birine atanan alan adları ile çeşitli bilgileri ilişkilendirir. En yaygın olarak, daha kolay bir şekilde ezberlenen alan adlarını, bilgisayar servislerini ve cihazları bulmak ve tanımlamak için gereken sayısal IP adreslerine çevirir.

HTTPS (Güvenli HTTP)

Güvenli HTTP, İnternet'te yaygın olarak kullanılan ve bilgisayar ağı üzerinden güvenli iletişim amacıyla kullanılan bir iletişim protokolüdür. HTTPS, Taşıma Katmanı Güvenliği veya onun bir öncesinde yer alan Güvenli Soket Katmanı tarafından şifrelenmiş bir bağlantı ile çalışan, Köprü Metni Aktarım Protokolü (HTTP) üzerinden kurulmuş iletişimden oluşur. HTTPS için ana motivasyon, ziyaret edilen ağ kaynaklarının kimliğini doğrulamak ile alınan/verilen verilerin gizliliğini ve bütünlüğünü korumaktır.

Java

Eşzamanlı, sınıf tabanlı, nesne yönelimli ve mümkün olduğunca az uygulama bağımlılığına sahip olacak şekilde tasarlanmış genel amaçlı bir bilgisayar programlama dili.

Vekil sunucusu

Diğer sunuculardan kaynak isteyen istemcilerin istekleri için aracılık yapan bir sunucu (bilgisayar sistemi veya uygulama). Bir istemci, bir dosya, bağlantı, web sayfası veya farklı bir sunucudan erişilebilen diğer kaynaklar gibi bazı hizmetleri talep edenler vekil sunucusuna bağlanır. İstenen kaynak daha sonra hizmetin bulunduğu esas sunucudan alınır veya olası bir önbellekten ulaşılır.

SSL Sertifikası

Güvenli (SSL) bir bağlantı için kullanılan bir açık anahtar sertifikasıdır. Açık anahtar sertifikası, açık anahtarın sahipliğini kanıtlamak için kullanılan elektronik bir belgedir. Sertifika, anahtara ait, anahtarın sahibinin kimliğine (özne denir) ait ve sertifikanın içeriğini doğrulayan bir varlığın (imzalayan olarak anılır) dijital imzasına ait bilgi içerir. İmza geçerli ise ve sertifikayı inceleyen yazılım imzalayana güveniyorsa, sertifikanın öznesiyle güvenli bir şekilde iletişim kurmak için bu anahtarı kullanabilir. Taşıma Katmanı Güvenliğinde (TLS) sertifikanın öznesi genellikle bir bilgisayar veya başka bir aygıttır, ancak TLS sertifikaları, aygıtları tanımlamadaki temel rollerine ek olarak kuruluşları veya kişileri de tanımlayabilir. Bazen eski adı olan Güvenli Soket Katmanı (SSL) olarak da adlandırılan TLS, İnternette güvenli dolaşabilmek için kullanılan bir protokol olan HTTPS'in parçası olarak bilinir.

SQL

Yapısal Sorgulama Dili (SQL), ilişkisel veri tabanı yönetim sisteminde (RDBMS) veya ilişkisel veri akış yönetimi sisteminde (RDSMS) tutulan veriler için tasarlanmış, programlamada kullanılan alana özgü bir dildir.

Sanal Özel Ağ

Tünel protokolü üzerinden ağ trafiğini tünellemek için kullanılan bir teknoloji. Kanalın güvenliğini sağlamak ve VPN istemcisinin kimliğini gizlemek için şifreleme teknikleri uygulayarak internete güvenli ve anonim erişim sağlamak amacıyla da kullanılmaktadır.

VPN

bakınız, Sanal Özel Ağ



ByLock Sorusturmasi Hakkinda Bilirkisi Raporu

13 Eylul 2017

Versiyon:1.0

Durum: Son

Sayfa Sayisi: 33

Yazar: Fox-IT

Gizlilik Derecesi: Acik

ACIK

Bu dokumanin gizlilik derecesi ACIK olarak siniflandirilmistir.

Fox-IT BV

Olof Palmestraat 6
2616 LM Delft
Postbus 638
2600 AP Delft
Hollanda
Telefon: +31 (0)15 284 7999
Fax: +31 (0)15 284 7990
E-mail: fox@fox-it.com
Internet: www.fox-it.com
Telif Hakkı © 2017 Fox-IT BV

Her hakkı saklıdır. Bu belgenin hiçbir kısmı Fox-IT'nin yazılı izni olmaksızın çoğaltılamaz, bir geri çağrı sisteminde saklanamaz veya herhangi bir yolla iletilemez. İhlaller, ilgili kanunlarca kovuşturulacaktır. Fox-IT B.V.'nin genel hizmet koşulları bu dokümantasyon için geçerlidir.

Marka

Fox-IT ve Fox-IT logosu Fox-IT B.V'nin ticari markalarıdır.
Bu belgede adı geçen diğer tüm ticari markalar, belirtilen organ veya kuruluşlara aittir.



Dokuman Yonetimi

Versiyon Yonetimi

Proje Adi: BREEZEWOOD

Konu: ByLock Sorusturmasi Hakkinda Bilirkisi Raporu

Tarih: 13 Eylul 2017

Versiyon:1.0

Durum: Son

Yazar: Fox-IT

Bu versiyon tum onceki versiyonlari yerine gecir. Lutfen onceki versiyonlari hepsini yok ediniz.





FOX IT
an nccgroup

Expert Witness Report on ByLock Investigation

13 September 2017

Version: 1.0

Status: Final

Pages: 33



Author: Fox-IT

Classification: **PUBLIC**



PUBLIC

This document is classified as PUBLIC.

Fox-IT BV

Olof Palmestraat 6
2616 LM Delft
Postbus 638
2600 AP Delft
Nederland



Telephone: +31 (0)15 284 7999
Fax: +31 (0)15 284 7990
E-mail: fox@fox-it.com
Internet: www.fox-it.com

Copyright © 2017 Fox-IT BV

All rights reserved. No part of this document shall be reproduced, stored in a retrieval system or transmitted by any means without written permission from Fox-IT. Violations will be prosecuted by applicable law. The general service conditions of Fox-IT B.V. apply to this documentation.

Trademark

Fox-IT and the Fox-IT logo are trademarks of Fox-IT B.V.

All other trademarks mentioned in this document are owned by the mentioned legacy body or organization.

for a more secure society

FOX-IT BV	T +31 (0)15 284 79 95
Olof Palmestraat 6, Delft	F +31 (0)15 284 79 90
Postbus 638, 2600 AP Delft	ABN AMRO 554697041
	r.v.v. Haaglanden 27301624

DOCUMENT MANAGEMENT

Version Management

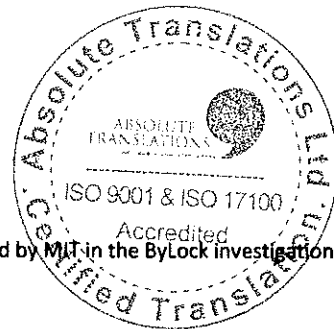
Project name : BREEZEWOOD
Subject : Expert witness report on ByLock investigation
Date : 13 September 2017
Version : 1.0
Status : Final
Authors : Fox-IT

This version replaces all previous versions of this document. Please destroy all previous copies!



TABLE OF CONTENTS

1	Introduction	5
2	Issues Addressed	6
3	Approach	7
3.1	Analysis of MIT investigation and report	7
3.2	Fact-checking	7
4	Findings	8
4.1	What is Fox-IT's opinion on the investigation methodology used by MIT in the ByLock investigation?	8
4.1.1	Transparency and evidence authenticity	8
4.1.2	Application servers and the ByLock.net domain	9
4.1.3	Open-source research	10
4.1.4	Sub-conclusions	14
4.2	How sound is MIT's identification of individuals that have used the ByLock application?	15
4.2.1	Which method was used to link ByLock accounts to individuals and how reliable is this method?	15
4.2.2	In what way were ByLock accounts created, and was it possible to add accounts that are linked to another individual?	17
4.2.3	Which method was used to determine that a ByLock user was actually active on ByLock and how reliable is this method?	17
4.2.4	Sub-Conclusions	18
4.3	What is the qualification of soundness on MIT's conclusion regarding the relation between ByLock and the alleged FTÖ/PDY?	19
4.3.1	How is it concluded that the ByLock application is used exclusively by the alleged FTÖ/PDY?	19
4.3.2	What is Fox-IT's opinion on the stated findings and the resulting conclusion?	20
4.3.3	How does the ByLock application relate to other similar chat applications available with respect to security?	22
4.3.4	Sub-Conclusions	25
4.4	Are there any other issues identified by Fox-IT that are relevant to the ByLock investigation?	26
4.4.1	Notable inconsistencies	26
4.4.2	Reporting style and readability	27
5	Conclusions	28
5.1	What is Fox-IT's opinion on the investigation methodology used by MIT in the ByLock investigation?	28
5.2	How sound is MIT's identification of individuals that have used the ByLock application?	28
5.3	What is the qualification of soundness on MIT's conclusion regarding the relation between ByLock and the alleged FTÖ/PDY?	28
5.4	Are there any other issues identified by Fox-IT that are relevant to the ByLock investigation?	29
6	Documents and Data Examined	30
7	Appendix	31
7.1	ByLock.net timeline	31
7.2	Glossary of technical terms	33



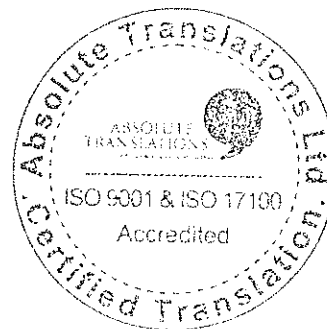
1 INTRODUCTION

Fox-IT was engaged with a request for an expert witness report in ongoing legal proceedings in Turkey. This request was done by a Turkish lawyer (hereafter: Principal) representing clients in custody. Principal is requesting an expert opinion on the following matter.

The Turkish government is currently actively pursuing the prosecution of members of the alleged¹ terrorist organization *fethullahçı terör örgütü/paralel devlet yapılanması (FTÖ/PDY)*. To this end, the Turkish Intelligence organization MIT (Millî İstihbarat Teşkilatı) has investigated the relation of the chat application *ByLock* to FTÖ/PDY. MIT has written a report on this investigation describing the *ByLock* application and MIT's findings regarding the relation of the *ByLock* users to the alleged FTÖ/PDY. This report (hereafter: the MIT report) was distributed to the main prosecutor's office in Ankara.

According to Principal, the report is used by Turkish prosecutors to identify a large number of people as members of the alleged FTÖ/PDY and to place people in preliminary custody based on the fact that they have used *ByLock*. The findings and conclusions of the MIT report are, according to Principal, not sufficiently scrutinized and incorrect. Therefore, Principal requests Fox-IT to review the report and provide its expert opinion on the soundness of the methodology, findings and conclusions.

Fox-IT has received MIT's report in Turkish and two translated copies titled "*ByLock* Application Technical Report". The first translated report is a sworn translation from Turkish to Dutch. The second translated report is a sworn translation from Dutch to English released on 19 July 2017. The latter report was reviewed by Fox-IT for this expert witness report.



¹ The name *FTÖ/PDY* refers to a social movement in Turkey, also referred to as the *Hizmet* movement. The name *FTÖ/PDY* implies a terrorist organization. According to Principal, the movement is not generally recognized as a terrorist organization outside the Turkish government. This discussion is outside the area of expertise of Fox-IT. To prevent the impression of bias, this report will therefore refer to the organization as *alleged FTÖ/PDY*.

2 ISSUES ADDRESSED

This section describes the issues addressed in the expert witness review described in this report. The issues are posed by Principal and formulated by Fox-IT in collaboration with Principal. The following issues are addressed in this report by Fox-IT:

1. What is Fox-IT's opinion on the investigation methodology used by MIT in the ByLock investigation?
2. How sound is MIT's identification of individuals that have used the ByLock application?
 - a. Which method was used to link ByLock accounts to individuals and how reliable is this method?
 - b. In what way were ByLock accounts created, and was it possible to add accounts that are linked to another individual?
 - c. Which method was used to determine that a ByLock user was actually active on ByLock and how reliable is this method?
3. What is the qualification of soundness on MIT's conclusion regarding the relation between ByLock and the alleged FTÖ/PDY?
 - a. How is it concluded that the ByLock application is used exclusively by the alleged FTÖ/PDY?
 - b. What is Fox-IT's opinion on the stated findings and the resulting conclusion?
 - c. How does the ByLock application relate to other similar chat applications available with respect to security?
4. Are there any other issues identified by Fox-IT that are relevant to the ByLock investigation?



3 APPROACH

This section described the approach used by Fox-IT to conduct the investigation required for this expert witness report. The approach can be subdivided in two parts: analysis of the MIT report and analysis of source data to verify stated facts and observations from the MIT report. Both parts are described in the following subsections.

3.1 Analysis of MIT investigation and report

During this research, Fox-IT analyzed the MIT report regarding the soundness of the digital investigation process used by MIT in their investigation. Specifically, the methodology, argumentation, findings and conclusions of the MIT investigation were assessed. Since results from the ByLock investigation are submitted as evidence in legal procedures, the investigation is evaluated as a forensic investigation. Multiple relevant articles and books are written and cited on the principles of forensic evidence and forensic investigation. Fox-IT adheres to the following principles when conducting investigations which are well-described in the book *Digital Evidence and Computer Crime*²:

1. **Objectivity.** The interpretation and presentation of evidence should be free of bias to provide decision with clearest possible view of the facts. All possible hypotheses should be analyzed and evaluated in order to make sure that the investigator has no tunnel vision and is unbiased in his/her investigation.
2. **Evidence authenticity.** Authentication of evidence is the process to determine that the evidence is what the proponents claim it is. This includes demonstrating that presented evidence is the same as when it was collected, but also the date and location of where the evidence was collected. A chain of custody document is important in demonstrating who handled the evidence and why.
3. **Evidence integrity.** Integrity checking is required to verify that evidence is not altered since it was collected, thus supporting evidence authentication. The verification process of digital data is usually based on calculating cryptographic hash functions. The hash functions produce a (nearly) unique fingerprint of data. This fingerprint can be used at any time to verify that data is unchanged from when the hash was calculated.
4. **Transparency/Repeatability.** It should be possible to independently examine and verify the digital forensic process in its entirety. A key element of verification is the ability to reproduce the forensic process under the same conditions with a consistent level of quality being observed each time the process is run. Sources for all hypotheses should be included.

These principles were applied as criteria to evaluate the MIT investigation and report.

3.2 Fact-checking

Fox-IT attempted to verify the facts and observations relevant to the conclusions of the MIT report. To this end, open and closed sources were researched and data from ByLock was analyzed to the extent that this was available at the time of this research. Analysis was also performed by decompilation of the ByLock Android application and static analysis of the decompiled code. Section 5 describes which ByLock application data was examined by Fox-IT.

Furthermore, online open sources were researched to verify observations described by MIT related to Google searches, Twitter and other online platforms.

Data from the ByLock servers was not available for analysis by Fox-IT. Therefore, the observations and facts stated by MIT with respect to the ByLock server data were not checked.

Various observations and facts (presented by Fox-IT and MIT) have been plotted in a timeline to create a clear overview of the various events. Since the MIT report appears to use the attempted coup on 15 July 2016 in Turkey as an important point in time, this date is mentioned on multiple occasions in this report as a reference point in time.

² Digital Evidence and Computer Crime, 3rd edition. 2014. Eoghan Casey.

4 FINDINGS

4.1 What is Fox-IT's opinion on the investigation methodology used by MIT in the ByLock investigation?

The ByLock application and the corresponding communicating servers were subjected to technical examination by MIT. In the MIT report, the methodology is not described explicitly. Fox-IT has attempted to deduce the investigation performed by MIT and summarized the content of each section of the MIT report as follows:

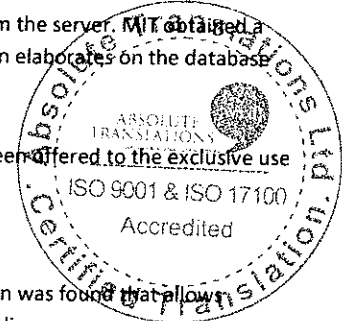
- Section 2 provides general information on the ByLock application.
- Section 3.1 describes the legal grounds for, and methods used, in obtaining data stored in the ByLock application servers.
- Section 3.2 describes an analysis performed by MIT of IP addresses and domain names related to ByLock. Through analysis of the different versions of the application and open-source investigation, MIT makes observations and draws conclusions on the application infrastructure.
- Section 3.3 describes results from an open-source research on ByLock performed by MIT. MIT compared the searches made from Turkey and worldwide for the word "ByLock" in search engines. Based on their observations, MIT draws conclusions with respect to the usage and goals of the ByLock application.
- Section 3.4 describes results from analysis of cryptographic protocols used by ByLock and reverse engineering performed by MIT.
- Section 3.5 describes results from an analysis of a ByLock server performed by MIT. It explains the ByLock infrastructure and describes observations about the supposed administrator of the ByLock server and the server itself. Conclusions are drawn based on these observations with respect to intentions of the administrator.
- Section 3.6 describes the results of the examination of database files derived from the server. MIT obtained a database file of 109GB where the ByLock application data was stored. This section elaborates on the database model and the content.
- Section 3.7 describes statistical data of the ByLock server analyzed by MIT.
- Section 4 holds the assessment and conclusion. MIT concludes that ByLock has been offered to the exclusive use of the members of the alleged terrorist organization of FTÖ/PDY.

4.1.1 Transparency and evidence authenticity

Fox-IT noticed a general lack of transparency in the MIT report. Furthermore, no information was found that allows verification of integrity of the investigated data. This section will elaborate on these two findings.

Based on the MIT report available, Fox-IT is unable to verify that the evidence has not been affected during handling of the ByLock data. Calculating cryptographic hashes of an acquired dataset is the accepted method to fingerprint forensic data for later verification of integrity. It is good practice to document the hashes and generate an audit trail, such that at a later stage, it is possible to independently verify that the meaning of the evidence has not been altered during the digital forensic process. No hashes and no audit trail have been included within the MIT report. Especially for the ByLock database data it is essential that an audit trail and hashes are available, since essential findings have been derived from that dataset.

The MIT report describes multiple findings and conclusions, but the report lacks a description of the analysis steps taken leading to most of the findings. This makes it difficult for the readers to scrutinize the investigation method(s) used. Transparency is in the interest of natural justice: it should be possible to verify that the investigation was reliable and accurate. The most notable section in the MIT report where this fails is section 3.6. This section describes a crucial part of the ByLock investigation: outcomes of the investigation on the ByLock server. The section contains screenshots that contain inconsistencies in itself or are inconsistent with the surrounding text, suggesting manipulation of either the source data or the screenshot (or both). Section 4.4.1 of this report elaborates on this. If the report would have detailed the steps taken by the analyst leading to the screenshot, it may have clarified the inconsistencies. This is not the case. Fox-IT finds this a serious issue, since it raises questions regarding the integrity of the results and provides no means to examine the methods and verify results.



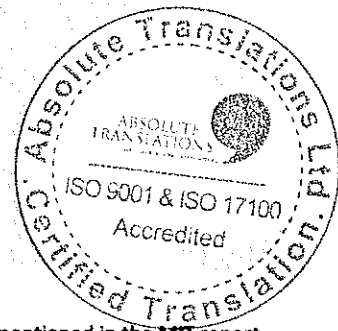
Furthermore, it is good forensic practice to document in what way and on which location the investigated data has been acquired and which specific techniques were used. The MIT report contains no documentation on the data acquisition. This makes it impossible to verify whether the data set is complete and that no relevant data is missing.

4.1.2 Application servers and the ByLock.net domain

The first finding that MIT presents in section 3.2 is that only IP address 46.166.160.137 had been used for bylock.net in the period from 1 September 2015 to 9 October 2016. MIT identified nine different IP addresses by work conducted in connection with a self-signed SSL certificate issued in the name of "David Keynes". Fox-IT performed research on the IP addresses and domain names used by ByLock in order to verify the findings.

Fox-IT has performed a search for IP addresses that hosted an SSL certificate with common name "David Keynes" using PassiveTotal³. This resulted in the following 10 IP addresses:

46.166.160.137
 46.166.164.176
 46.166.164.177
 46.166.164.178
 46.166.164.179
 46.166.164.180
 46.166.164.181
 46.166.164.182
 46.166.164.183
 69.64.56.133



The first nine IP addresses are mentioned in MIT's report. The last IP address was not mentioned in the MIT report. Bylock.net resolved to this IP address from April 2014 to August 2014, so it is possible this was the first ByLock application server. It is unclear why this is not mentioned in the MIT report.

Fox-IT performed an open-source investigation on the domain bylock.net and IP address 46.166.160.137 to determine the ownership information and IP addresses referenced by this domain name. The changes in this information over time are listed in appendix 7.1. It was observed that the domain bylock.net resolved to 46.166.164.137 only from August 2014 to March 2016. This contradicts the statement in the MIT report, stating that bylock.net resolved to that IP address from 1 September 2015 to 9 October 2016. Fox-IT concludes that the bylock.net domain was active only until March 2016 and could not have been used in the period from April 2016 leading up to 15 July 2016. Table 1 includes a timeline on the ByLock versions.

Date	Description	Source
April 2014	ByLock.net domain resolving 69.64.56.133	PassiveTotal
11 July 2014	Android ByLock 1.1.3 uploaded to downloadatoz	downloadatoz.com
13 July 2014	Android ByLock 1.1.3 uploaded to Google Play Store	web.archive.org
10 August 2014	ByLock.net domain resolving to 46.166.160.137	PassiveTotal

³ PassiveTotal from RiskIQ provides intelligence on internet data sets like passive DNS, WHOIS, SSL certificate data, web trackers, and more.

⁴ <https://community.riskiq.com/search/certificate/issuerCommonName/David%20Keynes>

22 August 2014	iOS ByLock 1.1.3 uploaded to Apple App Store	sensortower.com
23 August 2014	Android ByLock 1.1.4 uploaded to downloadatoz	downloadatoz.com
24 August 2014	Email confirmation from baltic servers that IP range 46.166.164.176/29 is ready for use	MIT report, page 14
4 September 2014	Android ByLock 1.1.6 uploaded to downloadatoz	downloadatoz.com
15 November 2014	Blog announcement re blocking of IP addresses	MIT report, page 17
24 Dec 2014	Android ByLock 1.1.7 uploaded to downloadatoz	downloadatoz.com
26 Dec 2014	Android ByLock 1.1.7 uploaded to Google Play Store	web.archive.org
March 2016	ByLock.net domain deactivated	PassiveTotal
15 July 2016	Attempted coup	Various

Table 1: Timeline of ByLock versions and domain records for bylock.net.

Next, Fox-IT examined the ByLock application for Android version 1.1.6 and 1.1.7 to determine the application server addresses used in those versions. It was observed that ByLock 1.1.6 uses the hardcoded IP address 46.166.164.177 and version 1.1.7 uses IP address 46.166.164.181. Both IP addresses are part of the IP addresses listed by the MIT report. ByLock version 1.1.6 was available as an upgrade from 4 September 2014. As a result, after 4 September 2014, upgraded or newly installed ByLock application would connect to one of these two IP addresses instead of the server at bylock.net. The two servers have been an active part of the ByLock infrastructure as either:

1. A ByLock application server or
2. A proxy server to a ByLock application server.

The MIT report does not mention anything related to investigation of these servers. This raises relevant questions:

- How were these two servers used in the ByLock infrastructure and why is investigation of these servers not included in the MIT report?
- If they were actually proxy servers, how does this relate to the statements on page 17 of the MIT report regarding the blocking of IP addresses from Turkey? MIT states that "it is clear that by blocking access of IP addresses [...]. It is believed that this was another fictitious measure to prevent identification of individuals using the application". Since ByLock versions 1.1.6 and 1.1.7 do not contact 46.166.160.137, the mentioned firewall blocking on that server would not apply to those (v1.1.6 and v1.1.7) ByLock clients. This observation does not support MIT's assessment of the developer attempting to force users through VPN connections.

4.1.3 Open-source research

There are multiple problems in the investigation and results described in section 3.3 of the MIT report. All of them are relevant for the conclusion.

Search trend incline

The first figure in section 3.3 depicts the Google Trends results for search term "ByLock" for the worldwide scope from December 17, 2013 to February 17, 2016. However, the subscription says "ByLock search statistics (Turkey)". This raises the question: to which statistic is the text referring?

Searches from Turkey

Page 10 of the MIT report states that the searches on the term “ByLock” were made mostly from France, the United Kingdom (UK) and the United States of America (USA). Page 10 contains a figure depicting Google Trends results from a query filtered on the countries Turkey, USA, UK and France. This is misleading to the reader: if other countries would have higher scores, then it would not be shown in that graph, because it only shows the four mentioned countries.

Fox-IT attempted to reproduce the Google Trends result by searching on “ByLock” in the Google Trends web application. This query was performed on 17 Aug 2017. The query was also performed using proxy servers from different countries to account for the possibility that Google would show different results to end-users from different countries: the results are the same. The result is depicted in Figure 1. The top five countries are respectively (from high to low score): Sweden, Turkey, Azerbaijan, Cyprus and Norway. The countries France, UK and USA are actually respectively placed 20th, 14th and 15th of countries with relative most searches on ByLock during the period. This is different from MIT’s observation and invalidates the conclusion in the last paragraph of section 3.3 MIT:

“In light of the statistics, the fact that its usage in Turkey was considerably higher (more users in Turkey than in all other countries combined) ...”

Since it is unclear what part of the searches originate from Turkey, MIT’s factual statement is invalid and should be reconsidered.

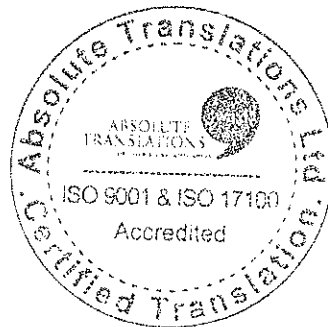




Figure 1. Google Trends results for search term "ByLock" worldwide

Twitter

On page 10 of the MIT report, the author states:

"It has become apparent that of the Twitter users who posted content via "ByLock" before July 15, 2016, the vast majority appear to have been posting content in support of the FETO/PDY."

There is no explanation on how this fact was established by MIT. There is no Twitter data, statistics or other evidence in the document that supports this statement. This claim should be questioned since it is not evident and functions as one of the key findings for MIT's conclusion.

The paragraph goes further:

"This is seen as an indication that users who could be identified ([...]) are those who are actually affiliated with the FETO/PDY, and that they were aware of the application and widely used it before it was known to the public."

This suggest that MIT considers the ByLock application unknown to the public before 15 July 2016. Fox-IT has attempted to verify this statement with available statistics. The Google Trends statistics suggest varying interest in ByLock from at least the end of 2013 up until the 15 July 2016, peaking between 7 September and 14 September 2014. Historical download and install statistics from Google Play store⁵ indicate ByLock installations from at least April 2014 and reaching 100,000 installation on 19 January 2015⁶. Table 2 lists the statistics. These observations suggest that a public has actually known and used ByLock in the years leading up to 15 July 2016. Given the available information, it is not possible to determine whether the individuals that installed the application were members of alleged FTO/PDY or not.

Date	Total installs
22 April 2014	50+
24 April 2014	100+
4 May 2014	1,000+
20 May 2014	5,000+
1 June 2014	10,000+
24 Aug 2014	50,000+
19 Jan 2015	100,000+

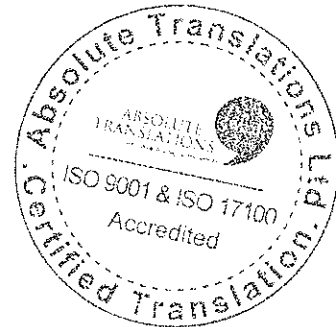


Table 2. Google Play Store installation statistics on ByLock application

Limited number of platforms

On page 10 of the MIT report, the author further states:

“before 15 July 2016 the app appeared on a limited number of platforms apart from Twitter”

Fox-IT has observed that before 15 July 2016, the ByLock application was hosted on multiple platforms other than Twitter. Examples of the platforms that hosted ByLock are *Google Play Store*, *Apple Store*, *apk-dl.com*, *apkpure.com* and *downloadatoz.com*. These platforms provide a date and time of last update for each hosted application. This date and time was well before 15 July 2016 for the ByLock application. Also, it is very likely that before 15 July 2016 a Google search on the term “ByLock” would lead to multiple platforms hosting the application. The appearance of ByLock is no different than Fox-IT would expect from an average chat application: it is hosted on the app stores and internet APK download servers and it is discussed in social media. The statement of MIT is no more true for ByLock than it is for an average chat application.

⁵ <http://choilieng.com/apk-on-pc/net.client.by.lock.apk>

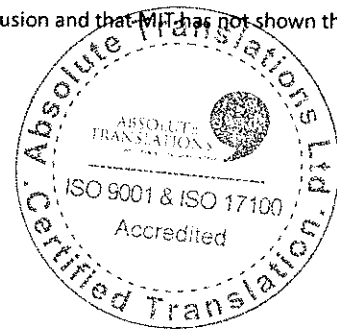
⁶ After this date, the installation number has very likely risen further. The next installation number logged would be 500,000. This suggests that the final number of installations is between 100,000 and 500,000.

4.1.4 Sub-conclusions

Fox-IT has performed a thorough examination of the information relating to the ByLock investigation to the extent that the information was (made) available. Furthermore, Fox-IT has, where possible, fact-checked observation and facts stated in the MIT report. This resulted in the following conclusions regarding the ByLock investigation:

1. Fox-IT noticed a general lack of investigative transparency in the MIT report. Furthermore, no information has been found which allows verification of integrity of the investigated data. Although it is good practice to document investigation steps and the data acquisition process, the MIT report contains very little information on these matters. This makes it impossible to verify whether the investigated data set and results are valid, complete and no relevant data is missing.
2. Fox-IT examined the facts and results related to the ByLock application servers and found that the documented investigation performed by MIT is incomplete and incorrect. Investigation by Fox-IT has shown that MIT's conclusions with respect to the bylock .net domain were incorrect. Also, Fox-IT has identified two relevant IP addresses (46.166.164.177 and 46.166.164.181) belonging to the ByLock infrastructure, which apparently were not investigated.
3. The open-source investigation performed by MIT was examined and fact-checked. Fox-IT has shown that stated Google Trends observations were fundamentally different from actual Google Trends results. Furthermore, Fox-IT has shown that claims related to ByLock downloads and Twitter are not supported by evidence and in some cases contradicted by observations from open-source research performed by Fox-IT.

Overall, Fox-IT is of the opinion that, as far as the report goes, the investigation performed by MIT raises many questions which require a more thorough investigation for a definite answer. More troubling is the fact that multiple findings appear to be non-reproducible or even incorrect. Other findings could not be verified due to lack of available data (e.g. from the ByLock server investigation). There is no indication of MIT investigating the alternative scenario: that ByLock has not exclusively been offered to members of the alleged FTÖ/PDY. Investigating existing alternate scenarios is good practice in an investigation. It helps prevent tunnel vision where investigators are biased towards a predefined outcome. The conclusions above suggest that MIT was, in advance, biased towards the stated conclusion and that MIT has not shown the required objectivity and thoroughness in their investigation to counter this bias.



4.2 How sound is MIT's identification of individuals that have used the ByLock application?

4.2.1 Which method was used to link ByLock accounts to individuals and how reliable is this method?

Section 3.6 of the MIT report describes the results of the investigation into the ByLock database data. This is the only section containing a reference to identification of individuals as ByLock users.

The MIT report does not describe in what way ByLock accounts are linked to actual individuals. The only reference found in the report to identify the individual linked to an account is mentioned in section 3.6.2.11 of the MIT report. In that section, MIT describes that entries in the *Log* table of the ByLock database have been used to identify individuals. These entries contain the IP address of the ByLock user during login and registration.

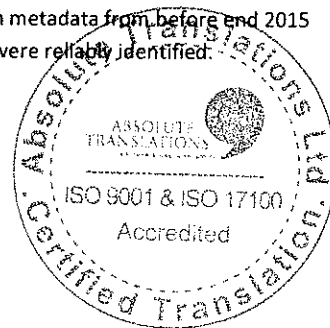
The MIT report does not describe how this IP address is linked to an individual. However, this attribution of IP address to individual is not trivial and can be prone to mismatching, since an IP address is usually not strictly assigned to one individual. There are multiple challenges with attributing an IP address to an individual:

Internet service provider log retention. An IP address is a unique identifier of a device in a computer network that uses the Internet Protocol for communication. A device can be a personal computer, laptop, tablet, phone, server, etc. An IP address is issued by a Regional Internet Registry (RIR). Five RIRs manage the allocation and registration of IP addresses each for a particular region of the world. The customers of a RIR could be either an Internet Service Provider (ISP) or end-user organization. In order to link an IP address to a registrar, information from the RIR can be obtained. However, when the registrar is an ISP, the ISP holds the information about which IP address has been assigned to which customer. This information can be requested in legal proceedings.

The Turkish regulation on the process and the protection of Personal Data in Telecommunication Sector published 14 July 2012 contains the regulation with respect to log retention by telecom- and infrastructure providers. The law states that both telecom- and infrastructure providers must retain communication metadata for at least 1 year⁷.

When identifying the subscriber using the IP address that logged on to ByLock, it is likely that MIT relied on log information from the service provider to identify individuals. IP addresses logged on the ByLock server may be NAT⁸ addresses or dynamic addresses assigned to a subscriber at a certain time. In both cases, log data is necessary to attribute the IP address to an individual.

It is unknown when the ByLock investigation was conducted by MIT (this information is not in the report), but the estimate is end of 2016. This leaves the question whether the communication metadata from before end 2015 was available. And if not, how the subscribers using the ByLock IP addresses were reliably identified.



⁷ Telecom laws and regulations handbook. Volume 1 strategic information and regulations. ISBN-978-1-3291-6456-7

⁸ Network Address Translation is a method of remapping one IP address space into another by modifying network address information in IP traffic while it is in transit across a traffic routing device. In more advanced NAT implementations featuring IP masquerading, it has become a popular and essential tool in conserving global address space allocations in face of IPv4 address exhaustion by sharing one Internet-routable IP address of a NAT gateway for an entire private network.

Shared Wi-Fi access points. One scenario where an individual accesses ByLock is by connecting their smartphone to the internet over a Wi-Fi connection. Wi-Fi access points allow multiple devices to access the same internet connection at the same time. It is not uncommon for access point in people's homes to be unsecured or an owner sharing their Wi-Fi password and thus allowing other (unknown) people to access the same internet connection. In this scenario, when an IP address found in logs on the ByLock server is investigated it will be linked to an internet subscription number. This subscription is registered on the name of the individual that owns the service contract. However, as shown above, that individual may be just one of the users using the Wi-Fi connection and not the ByLock user the investigation suggests.

VPN⁹ or other anonymizing technology. Nowadays, it is not uncommon to use a VPN server to keep web browsing secure and private. Many VPN services are available on the internet for this purpose. According to the MIT report, section 3.5.5, ByLock users from Turkey were forced to use such VPN services to access the ByLock servers due to firewall blocking on the ByLock server. Consider the scenario where a ByLock user connects to ByLock through a VPN session (see Figure 2 for an illustration).

Now, the source IP address found in the Log table on the ByLock server would belong to the VPN server's pool of IP addresses. Thus hiding the IP address of the ByLock user's internet connection. To retrieve the user's home IP-address, the investigator would likely need access to information stored on the VPN server, since the VPN provider holds the information on which client IP address relates to which VPN session (and corresponding VPN IP address seen in the ByLock log). Often this information is not available on the VPN server due to protection of the user data on those servers or it will not be provided upon request. It is possible to use multiple VPN connections, which means that for each VPN server, the investigators needs to overcome the same challenge.

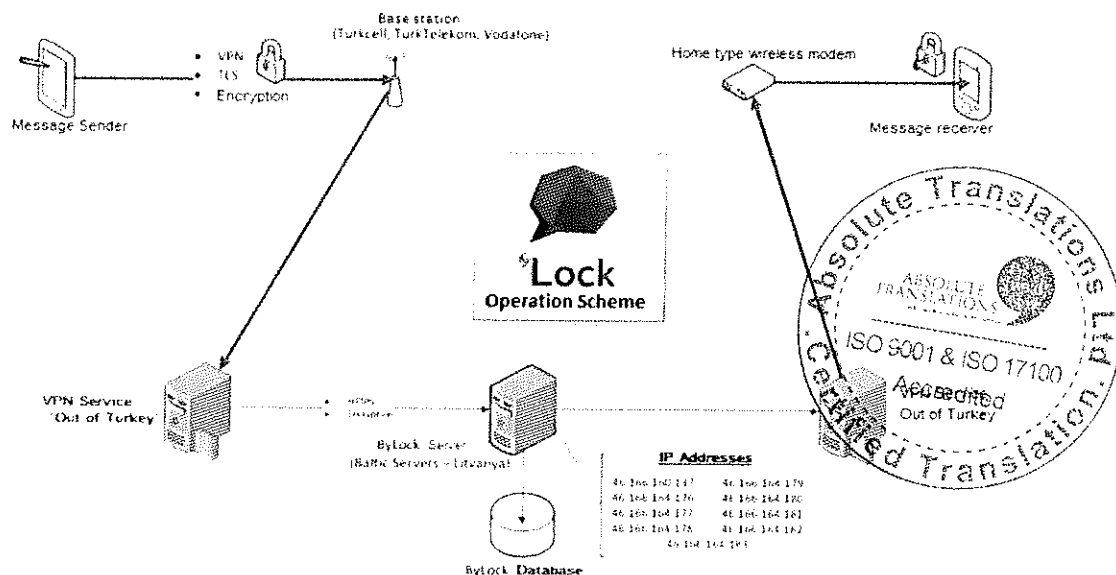


Figure 2: ByLock over VPN connection (from MIT report)

Any of the abovementioned three issues may lead to incorrect attribution or impossible attribution of an IP address to an individual. Since this is a crucial step in identifying the individuals, this method should be scrutinized. Currently, MIT does not provide any information that allows the examination of their method.

⁹ Virtual Private Network. A technology used to tunnel network traffic over a secure network channel. It is also used to provide secure and anonymous access to the internet.

4.2.2 In what way were ByLock accounts created, and was it possible to add accounts that are linked to another individual?

As mentioned, Fox-IT analyzed versions 1.1.6 and 1.1.7 of the ByLock application. In both versions, a user can register by creating a username and entering a password. Figure 3 depicts the registration screen of ByLock 1.1.7. No email address, phone number or other personal identifying information is required when creating an account. Fox-IT has confirmed, by reverse engineering of the ByLock application that no other information of the phone or user is sent to ByLock servers.

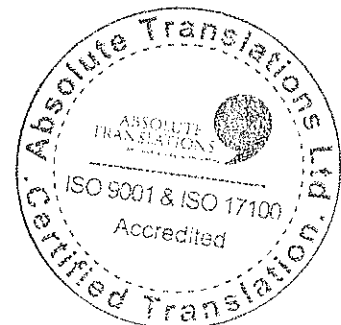
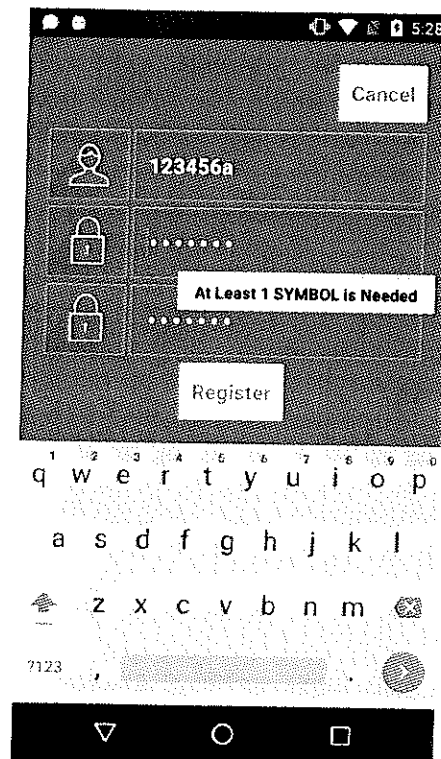


Figure 3: Screenshot of registration for a ByLock account.

The loose registration scheme allows creation of arbitrary accounts, since:

- There are no restrictions found that require a specific group membership as a condition of use;
- There is no verification of phone number or email address by the application;
- There are no format restrictions in the username chosen during registration. This allows entering arbitrary text like email address, phone number, nickname, etc.
- No invitation is required to register an account. Anyone having access to a ByLock application can register an account.

This scheme allows for creation of suggestive accounts by registering and using an account with a name or other identifier (e.g. email address or phone number) related to a real individual while that individual is unaware of the existence of that ByLock account.

4.2.3 Which method was used to determine that a ByLock user was actually active on ByLock and how reliable is this method?

Section 4.2.2 of this report describes that arbitrary ByLock user accounts may be registered by anyone having access to the ByLock application. This leads to the question how MIT has differentiated between users that have only been registered and logged on to ByLock and users that have actually used ByLock to communicate.

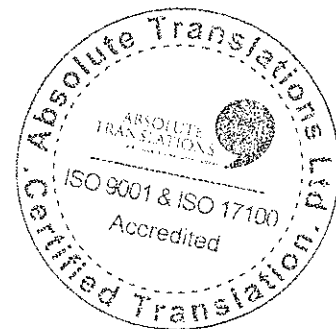
In the report it is not explicitly described if and how MIT determined the actual activity of the ByLock users. It is therefore unclear whether the individuals identified by the ByLock investigations have actually been communicating using ByLock.

4.2.4 Sub-Conclusions

Fox-IT has examined the methods used by MIT to identify individuals that have used ByLock. The goal of this examination was to determine the quality of the methods and then conclude on the soundness of the identification. This examination resulted in the following conclusions:

1. No identifying information (e.g. email address or phone number) is required to register as a ByLock user. As a result, it is easy to impersonate other individuals when creating a ByLock account by using a suggestive nickname.
2. The MIT report states that IP addresses from the ByLock database are used for identifying individuals using ByLock. However, the report omits the method used to attribute the IP addresses to individuals. Attribution of an IP address to individual is not trivial and prone to incorrect attributions. Fox-IT identified multiple issues that may lead to incorrect attribution or impossible attribution of a source IP address to an individual. Since attribution of a source IP address to an individual is a crucial step in identifying the individuals using ByLock, it should be possible to scrutinize this method. In the MIT report no information is provided that allows the reader to verify whether the attribution of an IP address to an individual is reliable.
3. The MIT report does not mention how MIT has differentiated between user accounts that were actively communicating and user accounts that have only registered and logged on. It is therefore unclear whether the individuals identified by the ByLock investigation have actually been communicating using ByLock.

Overall, the MIT report contains very limited information on the identification of individuals. Fox-IT has shown that ByLock user accounts are on their own difficult to attribute to an individual.



4.3 What is the qualification of soundness on MIT's conclusion regarding the relation between ByLock and the alleged FTÖ/PDY?

4.3.1 How is it concluded that the ByLock application is used exclusively by the alleged FTÖ/PDY?

Below, Fox-IT has summarized the arguments and conclusions as described in the MIT report and as interpreted by Fox-IT.

MIT concludes that the ByLock application is used exclusively by the alleged FTÖ/PDY based on the following:

1. The ByLock application is designed to communicate over the internet using a strong cryptographic system, which allows sending each message with a *crypto key*. Fox-IT assumes MIT intends to describe that the messages can be encrypted using a cryptographic key instead of sending the actual cryptographic key itself.
2.
 - a. MIT states multiple observations and findings about the developer of ByLock and concludes that the developer does not have any corporate or commercial nature.
 - b. MIT states multiple observations with respect to ByLock and Turkish language and users. Then MIT continues to conclude that ByLock was meant to be used by the members of the alleged FTÖ/PDY under the disguise of a global application. Some of the arguments listed are:
 - The administrator blocked IP addresses with origin Turkey.
 - Users were forced to use VPN in order to hide their identities.
 - Almost all searches on Google for the search term "bylock" were made from Turkey and significantly increased as of the date access to the application from Turkish IP addresses were blocked.
 - Publications related to ByLock have mostly been posted through fake accounts and in which the content was in favor of the alleged FTÖ/PDY.
 - Before the coup attempt on 15 July 2016, the ByLock application was not known to Turkish public or known outside of Turkey.
3. Utmost security of user id and communication was an aim of the ByLock application. Also, the reason why the application does not require personal information during sign up and does not have a verification system is to ensure anonymity.
4. The application developer used personally "developed" SSL certificates instead of verified SSL certificates. Fox-IT assumes that with the term personally developed SSL certificate, MIT means to refer to a self-signed certificate. MIT continues to conclude on that observation and on the intentions of the developer, MIT believes that a self-signed certificate was chosen to prevent the flow of information to servers other than his own.
5. In order to be able to communicate with another registered user, both parties need to mutually add each other's username/code. The application is therefore considered to have been designed to allow communication suitable to "the cell structure".
6. The application meets all organizational communication needs and are controlled and supervised by the application administrator.
7. The automatic deletion of messages from the device after a certain period without manual intervention indicates that the system is designed to prevent access to communication data and details in the event of a possible legal confiscation of the device.
8. MIT makes an inference of the users intention to hide their identity, based on the following observations:
 - Users create long passwords.
 - Users manually download the application on APK websites instead of Android Market or Apple Appstore.
 - Users did not use the real name as user ID during sign up.
 - Users used inter-organizational code names instead of real identities in their contact lists and communication.

Furthermore, MIT states that 'almost all' of the content of the decrypted messages are of communications and activities of alleged FTÖ/PDY and matched the organization's jargon.

9. Members of the organization who were subjected to judicial control measures following the coup attempt of 15 July 2016 conducted by the alleged FTÖ/PDY have stated that ByLock had been used as an inter-organizational communication medium by the member of the alleged FTÖ/PDY.

Based on the above, the MIT concludes that ByLock has been offered to the exclusive use of the members of the alleged terrorist organization of FTÖ/PDY.

4.3.2 What is Fox-IT's opinion on the stated findings and the resulting conclusion?

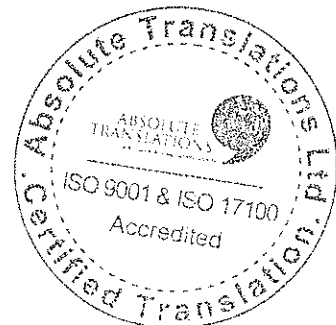
Fox-IT is of opinion that the resulting conclusion is not founded by the stated findings of MIT above. In this section each of the arguments is analyzed to determine the accuracy, correctness and soundness. Finally, Fox-IT will provide an opinion on the overall conclusion.

1. Strong cryptography. MIT states that the ByLock application makes use of a strong cryptographic algorithm. Strong is a relative term and Fox-IT does not regard the ByLock cryptography stronger than other known chat applications. The use of cryptography has become common practice in communications in recent years. Chat applications for the masses like WhatsApp and Facebook use the Signal Protocol which implements sophisticated cryptographic protocols for securing communications^{10,11}. The encryption used in the ByLock application is readily available using the default Java Application Programming Interface (API). ByLock used standard, publicly available Java libraries to provide encrypted communication between users of the application. Those are included in `java.security` and `javax.crypto`¹² and are well-documented^{13,14}. Section 4.3.3 further elaborates on the comparison between ByLock and other applications in light of the security measures discussed.

2a. Lack of commercial nature. Assessment of commercial nature of software is outside the expertise of Fox-IT and therefore Fox-IT will not address this point.

2b. Disguise of global application. The conclusion mentioned in this paragraph is based on findings from section 3.3 and 3.5 from the MIT report. Fox-IT has shown in section 6.1 of this report that relevant findings are not backed by evidence, questionable or incorrect. The findings described in bullets 5, 6, 7 and 8 were shown to be invalid. Without those findings as arguments, the conclusion does not hold true.

3. Aim at security and anonymity. Fox-IT finds it likely that the developer had a focus on creating a secure communication application allowing anonymous use of the application. In a world where privacy is of high importance, Fox-IT is of the opinion that the ByLock application's anonymity aim does not imply an intent for use in illegal activities. There are numerous well-known free applications that have similar goals. For example, the Tor project¹⁵ is a well-known anonymity browser that improve privacy and security on the internet. Journalists use Tor, as well as the U.S. Navy, for surveilling websites without leaving government IP addresses¹⁶. Section 4.3.3 further elaborates on the comparison between ByLock and other applications in light of the security measures discussed.



¹⁰ https://fbnewsroomus.files.wordpress.com/2016/07/secret_conversations_whitepaper-1.pdf

¹¹ <https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf>

¹² <https://docs.oracle.com/javase/7/docs/api/javax/crypto/package-summary.html>

¹³ <https://docs.oracle.com/javase/7/docs/technotes/guides/security/crypto/CryptoSpec.html>

¹⁴ <http://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html>

¹⁵ <https://www.torproject.org/>

¹⁶ <https://www.torproject.org/about/torusers.html.en>

4. Self-signed certificate. It is unclear whether the MIT author is referring to SSL certificates on the ByLock servers (for HTTPS) or SSL certificates on the application. In both cases, the SSL signing party does not impact the 'flow of information' as the MIT author states it. In case of SSL certificates for HTTPS, having a certificate authority sign the certificate does not give the authority access to the data, since the private key is not shared with the authority. The reasoning on this point by MIT is very unclear and suggests a misunderstanding of public key infrastructures and SSL certificates on the part of the MIT author.

Fox-IT finds it unlikely that the self-signed certificate was implemented by the developer to prevent data flowing to servers other than its own. In general, self-signed certificates are easier to implement and are free of cost. It is possible that this was an incentive for the developer to use self-signed certificates.

5. Communication only in a way suitable to the cell structure. The term cell structure is undefined and ambiguous in this context. Fox-IT assumes here that it refers to the way the alleged FTÖ/PDY is organized. Organizational structures are outside the expertise of Fox-IT.

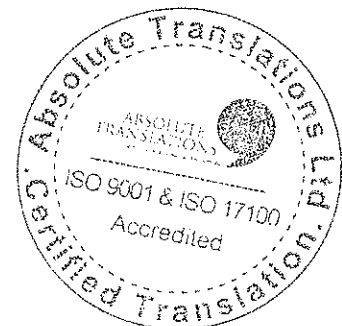
With respect to the registration procedure, it is relevant to nuance the requirement to meet face-to-face or by intermediary to exchange login details. The author fails to identify a third, more likely scenario to exchange ByLock details out of band: use of another communication method (e.g. phone call, WhatsApp, Facebook, Skype). Assuming two individuals are in contact by WhatsApp (the MIT author does not seem to scrutinize how two individuals meet on WhatsApp), they could exchange their ByLock details and then switch to communication by ByLock.

6. Organizational communication needs. Assessment of communication needs of organization is outside the expertise of Fox-IT and therefore Fox-IT will not address this point.

7. Prevent access in case of legal confiscation. Fox-IT is of the opinion that insufficient knowledge of the developers intention is available to agree or disagree with the MIT report on this argument. Following, Fox-IT is of the opinion that MIT is jumping to conclusions on the intent of the developer based on the observations stated in the report, unless more information is available to MIT corroborating their conclusion. Automatic deletion of messages is also used in popular social media applications like SnapChat¹⁷. Section 4.3.3 further elaborates on the comparison between ByLock and other applications in light of the security measures discussed.

8. Identity hiding. Fox-IT is of opinion that users do not explicitly hide their identity by:

- **Creating long passwords**
The minimum requirement of choosing a password in ByLock is six characters plus at least one symbol. MIT states that the decrypted passwords included passwords of 38 characters long and half of them were at least 9 characters long. The usage of a strong password is important for security reasons and not considered as a manner of hiding your identity. The stronger your password, the harder it is to crack the password by hackers (brute-force attack¹⁸). According to the new guidelines of the National Institute of Standards and Technology published in June 2017¹⁹, a minimum of 8 characters is advised and applications should allow a maximum length of at least 64 characters.
- **Manually download the application from APK websites**



¹⁷ <https://www.snapchat.com/>

¹⁸ https://en.wikipedia.org/wiki/Brute-force_attack

¹⁹ <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf>

In order to launch an application from Google Play Store, the application should meet a number of requirements²⁰²¹. This is in order for Google to give some guarantee to the users that an application is as expected. Some developers choose to make their application available on other APK websites for ease of use. However, the intention of the developer cannot be verified.

- Use another name as user ID during sign up
Most of the chat applications, like WhatsApp and SnapChat, do not require the use of the user's real name. In fact, it is not uncommon to use another name as user identification. This applies to the general usage of chat applications, social media platforms and overall internet services.

9. ByLock used during coup attempt. Fox-IT is unable to verify the statement that ByLock was used by the alleged FTÖ/PDY. However, in any case, this argument is invalid due to the base-rate fallacy in statistics²². The statement indicates the following misconception:

All members of a terrorist organization use ByLock, therefore all ByLock users are members of the terrorist organization.

This reasoning is a common mistake. A very basic and intuitive analogy to this reasoning is:

All fish swim, therefore everything that swims is a fish.

Which is obviously incorrect. One could still be of the impression that the statement does approximate reality (nearly everything that swims is a fish). Then consider the related example below:

1 in 10,000 people is an online criminal

1 in 1000 people use Tor

All criminals use the Tor network for communications

How many of TOR users are criminal?

The answer is only 1 in 10. So, even though all criminals use Tor, only 1 in 10 of the TOR users is criminal.²³

Assuming that, indeed, all alleged FTÖ/PDY members used ByLock (which is unlikely), there will be a significant number of ByLock users that are not a member of alleged FTÖ/PDY. The exact number is determined by the base-rate of the actual FTÖ/PDY members.

Based on the analysis described above, Fox-IT is of opinion that the findings presented by MIT do not support the conclusion that ByLock had been used²⁴ as an inter-organizational communication medium by the members of the alleged FTÖ/PDY.

4.3.3 How does the ByLock application relate to other similar chat applications available with respect to security?

In this section, Fox-IT will elaborate on the comparison between the ByLock application and other known communication applications. The authors of the MIT report suggest that the security features of ByLock (MIT report section 4 point 1, 3 and 7) are arguments to the conclusion that ByLock was offered to the exclusive use by alleged FTÖ/PDY. The goal of this investigation is to put the security features of ByLock into context of other chat applications and determine to what extent the security features distinguish ByLock from the other chat applications.

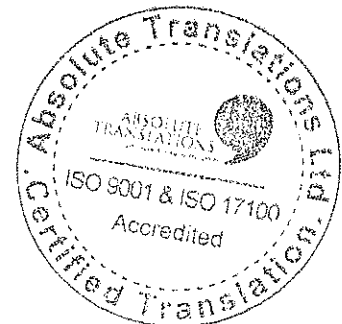
²⁰ <https://developer.android.com/distribute/best-practices/launch/launch-checklist.html>

²¹ <http://r-stylelab.com/company/blog/mobile-technologies/how-to-meet-google-play-requirements>

²² https://en.wikipedia.org/wiki/Base_rate_fallacy

²³ This can be calculated using Bayes theory: $P(\text{criminal} \mid \text{Tor}) = P(\text{Tor} \mid \text{criminal}) * P(\text{criminal}) / P(\text{Tor})$

²⁴ The MIT report states 'offered to the exclusive use', which Fox-IT has interpreted as used



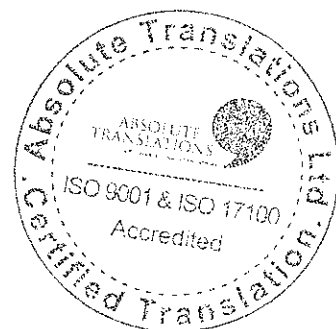
Encryption

As mentioned in paragraph 4.3.1, the use of encryption has become common practice in communications in recent years. According to the investigation performed by Fox-IT, the encryption used in the ByLock application was created using standard, publicly available Java libraries available using the default Java Application Programming Interface (API).

However, other chat applications have more sophisticated encryption techniques implemented. The Electronic Frontier Foundation (EFF) launched on 6 November 2014 a score card with an overview of encryption features per application²⁵, see Figure 4. This score card was last updated on 4 May 2016. From this Figure, it can be seen that WhatsApp is one of the most secure chat applications. Also, according to recent sources^{26,27}, of chat applications investigated, WhatsApp is the best secured chat application and has 1,3 billion users²⁸ as of July 2017. This implies, that encryption, and therefore secure messaging, is of great importance to the general user.

Figure 4 lists the security features used by EFF to score chat applications on security. Of these features, only two features were confirmed by Fox-IT to be implemented in the ByLock application:

1. Encrypted in transit;
2. Encrypted so the provider can't read it



²⁵ <https://www.eff.org/node/82654>

²⁶ <http://www.techworld.com/security/best-secure-mobile-messaging-apps-3629914/>

²⁷ <http://www.techradar.com/news/top-10-best-secure-messaging-apps-of-2017>

²⁸ <https://www.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users/>

	Encrypted in transit?	Encrypted so the provider can't read it?	Can you verify contacts' identities?	Are past comms secure if your keys are stolen?	Is the code open to independent review?	Is security design properly documented?	Has there been any recent code audit?
AIM	✓	✗	✗	✗	✗	✗	✗
Facebook chat	✓	✗	✗	✗	✗	✗	✓
Google Hangouts/Chat "off the record"	✓	✗	✗	✗	✗	✗	✓
iMessage	✓	✓	✗	✓	✗	✓	✓
iText - Oxtel	✓	✓	✓	✓	✓	✓	✗
Off-The-Record Messaging for Mac (Adium)	✓	✓	✓	✓	✓	✓	✗
Off-The-Record Messaging for Windows (Pidgin)	✓	✓	✓	✓	✓	✓	✓
Skype	✓	✗	✗	✗	✗	✗	✗
Snapchat	✓	✗	✗	✗	✗	✗	✗
TextSecure	✓	✓	✓	✓	✓	✓	✓
WhatsApp	✓	✓	✓	✓	✗	✓	✓

Figure 4: Secure Messaging Scorecard of the EFF.

Self-destruction

Other than ByLock, a well-known and popular messaging application with a self-destructing message feature is Snapchat. Snapchat was released in 2011 and has 173 million users²⁹. Also, the popular chat application Viber with 800 million users added a self-destruction feature³⁰.

²⁹ <https://www.statista.com/statistics/545967/snapchat-app-dau/>

³⁰ <https://www.theverge.com/2017/3/10/14879986/viber-secret-chats-self-destructing-encryption>

Other chat application with a similar feature where content and messages created by the user will automatically delete themselves after a period of time are:

- Telegram³¹
- Bleep³²
- Wickr³³
- Confide³⁴
- SpeakOn³⁵

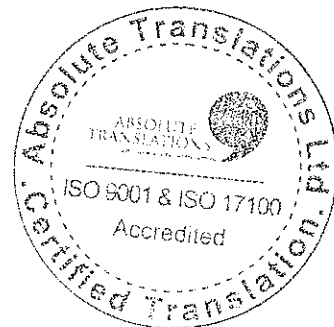
This survey has shown that multiple Android applications, totaling millions of users, implemented this security feature. Therefore, ByLock does not appear exceptionally secure.

4.3.4 Sub-Conclusions

Fox-IT has examined the MIT report to determine the quality of reasoning in the conclusion. In the conclusion, MIT puts substantial weight on ByLock's security measures and alleged goals of the developer. Therefore, Fox-IT has compared ByLock to other chat applications to put the security features of ByLock into context of the available chat applications.

From this comparison, Fox-IT concludes that the security measures implemented in ByLock are not exceptional and actually on par with widely used chat applications. The use of self-destruct messages and well-known cryptographic protocols for hashing passwords and securing data in transit has been implemented in other communication applications used by millions of users. Therefore, the features mentioned in the conclusion of the MIT report in point 1, 3 and 7 are in no way an indication that ByLock is aimed at a specific user group (alleged FTÖ/PDY) or with a specific purpose other than to communicate in a secure manner.

The conclusions of the MIT report were thoroughly examined and assessed by Fox-IT. It was shown that the argumentation is seriously flawed and that seven out of nine stated arguments (findings) are invalid or questionable. This follows from the Fox-IT findings described in section 4.1. The remaining arguments are in itself not sufficient to support MIT's conclusion. As a result, the conclusion of the MIT report, "ByLock has been offered to the exclusive use of the members of the terrorist organization of FTÖ/PDY", is not sound.



³¹ <https://telegram.org/>

³² <https://n0where.net/chat-privately-bleep/>

³³ <https://www.wickr.com/>

³⁴ <https://getconfide.com/>

³⁵ <https://www.crunchbase.com/organization/speakon#/entity>

4.4 Are there any other issues identified by Fox-IT that are relevant to the ByLock investigation?

4.4.1 Notable inconsistencies

Figure 5 in Section 3.6.2.4 (screenshot of SQL output) and Figure 15 in section 3.6.2.15 (another screenshot) of the MIT report are remarkable. The screenshots suggest output of an SQL query, showing the rows and a total number of rows returned. The total number of rows does not match the actual number of depicted rows. Also, there is a subtle spacing difference in the rows. This suggests manipulation of the screenshot or output. Figure 5 highlights the inconsistency.

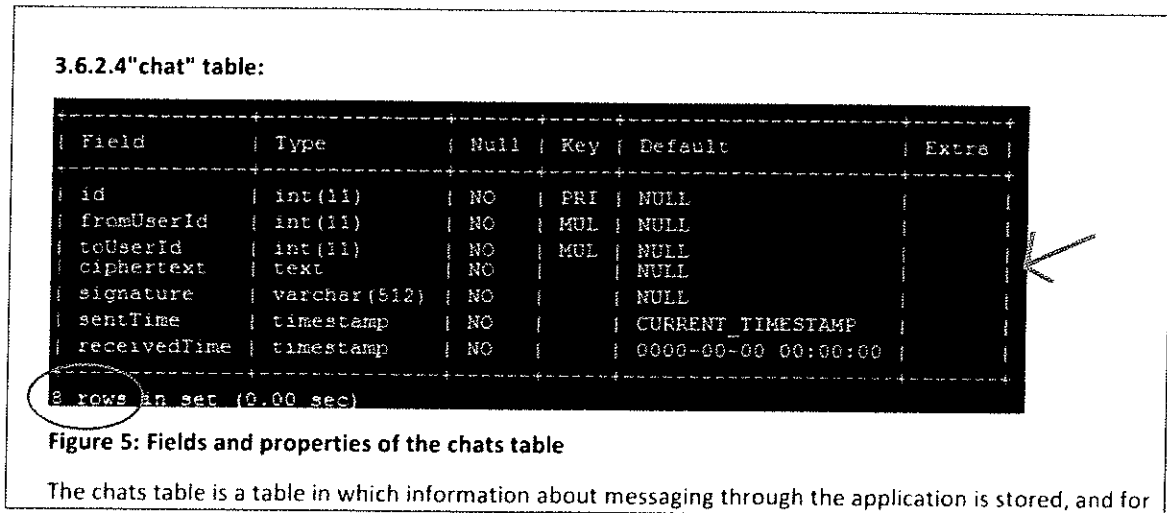


Figure 5. Inconsistency in screenshot of SQL output

Fox-IT also noted the following in section 3.6.2.15 MIT:

Examples of decrypted data stored in the user table are shown below: ("Username" indicates the user name / code for the information, and "plain" indicates the user password decrypted on the basis of the work done).

The above suggests that the column "plain" was added to the user table by MIT for analysis.

Furthermore, section 3.5.5 of the MIT report contains a listing suggesting a command line output. The listing shows:

```
root@hst-46-166-160-137:~#
iptables -N LOGGING
iptables -A INPUT -s 5.2.80.0/21 -j LOGGING
...
```

This suggests an output of the command `iptables`. However, the command itself is not visible in the listing. This is unexpected, since the command line prefix (`root@hst-46-166-160-137:~#`) is visible. This suggests that the command has been removed from this listing. As a result, it is unknown which command was entered and the reader can't verify what the output represents.

Another inconsistency is found in figure 11 (section 3.6.2.11) of the MIT report: the depicted query is `select * from log2 limit 50;`, while the title reads "*log*" table. This suggests that analysts have added or modified a table and named it `log2`. It is not clear if other information from the table was added, removed or modified.

The abovementioned inconsistencies are problematic, since it indicates manipulation of the database results or screenshots without an explanation. As a result, it is not clear which of the information in the report is from the original data and which information is modified by MIT and also to which end. This raises questions as to what more information was altered before presentation, why it was altered and what exactly was left out or changed. When presenting information as evidence, transparency is crucial in differentiating between original data (the actual evidence) and data added or modified by the analyst.

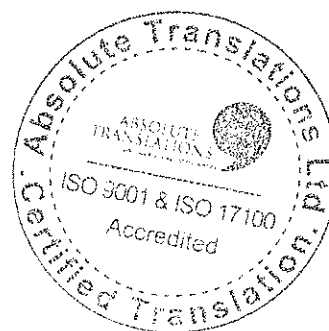
4.4.2 Reporting style and readability

Overall, Fox-IT finds the MIT report implicit, not well-structured and lacking in essential details. This is not merely a formatting issue. Writing an unreadable report that omits essential details reduces the ability for the reader to scrutinize the investigation that lead to the conclusions. When a report is used as a basis for serious legal consequences, the author should be thorough and concise in the report as to leave no questions regarding the investigation.

The following examples illustrate this problem:

- Basic document management information, such as authoring date and versioning, is missing.
- There is no description of the actual investigation question(s) that was posed. Posing the question(s) provides the reader with context information to follow the steps taken and shows that the investigators had an unbiased starting point for their investigation. The conclusions can then be merited in relation to the investigative question(s).
- In the MIT report section 4, point 2, the author describes 6 'conclusions and assessments' relating to the ByLock author and intent. These points are 1) not explained in the report (even though they are not evident) and 2) should not be first mentioned in the conclusions, since that suggests it as a fact or a finding, which was described before the conclusions.
- Point 2 in this section results in a conclusion "... that the application was meant to be used by the members of the FETO/PDY under the disguise of a global application". However, section 4 continues to list more arguments and then results in another, similar conclusion. It is unclear to the reader how these conclusions relate to each other and on which arguments the final conclusion is based.

Fox-IT has read and written many digital investigation reports over the last 15 years. Based on this experience, Fox-IT finds the quality of the MIT report very low, especially when weighed against the consequences of the conclusions.



5 CONCLUSIONS

This section provides the conclusions on each of the issues addressed by Fox-IT in this expert witness report. For a more elaborate documentation of the Fox-IT investigation approach and results, the reader is referred to section 3 and 4 of this report.

5.1 What is Fox-IT's opinion on the investigation methodology used by MIT in the ByLock investigation?

Multiple key findings from the MIT investigation were contradicted by open-source research conducted by Fox-IT and other findings were shown not to be supported by the evidence presented by MIT. Furthermore, the MIT investigation lacks in transparency: evidence and analysis steps were in many cases omitted from the MIT report. Multiple findings (that could be verified) were shown to be incorrect, which leaves the impression that more findings would prove to be incorrect or inaccurate if they could only be verified.

Fox-IT finds the MIT investigation lacking in objectivity, since there is no indication that MIT investigated the alternative scenario: namely that ByLock has not exclusively been offered to members of the alleged FTÖ/PDY. Investigating alternate scenarios is good practice in an investigation. It helps prevent tunnel vision in cases where investigators are biased towards a predefined outcome. Fox-IT's examination of the MIT investigation suggests that MIT was, in advance, biased towards the stated conclusion and that MIT has not shown the required objectivity and thoroughness in their investigation to counter this bias.

Fox-IT concludes that the MIT investigation as described in the MIT report does not adhere to the forensic principles as outlined in section 3.1 of this report and should therefore not be regarded as a forensic investigation. The investigation is fundamentally flawed due to the contradicted and unfounded findings, lack of objectivity and lack of transparency. As a result, the conclusions of the investigation are questionable. Fox-IT recommends to conduct a forensic investigation of ByLock in a more thorough, objective and transparent manner.

5.2 How sound is MIT's identification of individuals that have used the ByLock application?

The MIT report contains very limited information on the identification of individuals. Fox-IT has shown that ByLock user accounts are, on their own, difficult to attribute to an individual: it is easy to impersonate other individuals when registering a ByLock account and MIT is limited to an IP address from the ByLock server log to identify individuals. Attributing this IP address to actual individuals is not straightforward and error-prone; therefore, possibly leading to identification of the wrong individuals as ByLock users.

Fox-IT is unable to assess the soundness of the identification method, since the MIT report does not provide information on this method. The omission of a description of this method is troubling. Any errors in the method will not be discovered and the reader is left to assume MIT does not make mistakes. While transparency is one of the fundamental principles of forensic investigations, this critical part of the investigation is completely opaque.

5.3 What is the qualification of soundness on MIT's conclusion regarding the relation between ByLock and the alleged FTÖ/PDY?

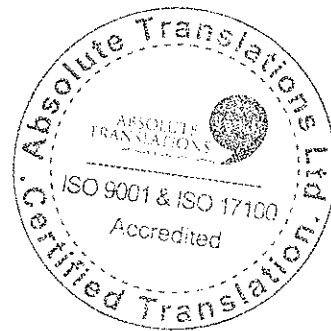
The conclusions and findings of the MIT report were examined by Fox-IT. It was shown that the argumentation is seriously flawed and that seven out of nine stated arguments are incorrect or questionable (see conclusion 6.1). The remaining two arguments are, on their own, not sufficient to support MIT's conclusion. As a result, the conclusion of the MIT report, "ByLock has been offered to the exclusive use of the members of the terrorist organization of FTÖ/PDY", is not sound.

5.4 Are there any other issues identified by Fox-IT that are relevant to the ByLock investigation?

Fox-IT encountered inconsistencies in the MIT report that indicate manipulation of results and/or screenshots by MIT. This is very problematic since it is not clear which of the information in the report stems from original data and which information was modified by MIT (and to which end). This raises questions as to what part of the information available to MIT was altered before presentation, why it was altered and what exactly was left out or changed. When presenting information as evidence, transparency is crucial in differentiating between original data (the actual evidence) and data added or modified by the analyst.

Furthermore, Fox-IT finds the MIT report implicit, not well-structured and lacking in essential details. Bad reporting is not merely a formatting issue. Writing an unreadable report that omits essential details reduces the ability for the reader to scrutinize the investigation that lead to the conclusions. When a report is used as a basis for serious legal consequences, the author should be thorough and concise in the report as to leave no questions regarding the investigation.

Fox-IT has read and written many digital investigation reports over the last 15 years. Based on this experience, Fox-IT finds the quality of the MIT report very low, especially when weighed against the consequences of the conclusions.



6 DOCUMENTS AND DATA EXAMINED

The following documents were reviewed by Fox-IT during the investigation:

1. **ByLock application technical report.**

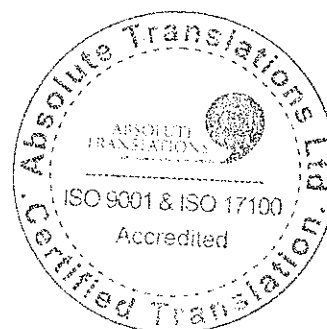
MIT's report was translated from Turkish to Dutch by a sworn translator. The Dutch report was translated from Dutch to English by a sworn translator for the English language. The Turkish, translated English and Dutch documents were delivered to Fox-IT as physical documents by Principal on 19 July 2017.

Fox-IT has analyzed versions of the ByLock application which were publicly available at the time of this investigation. The following versions of the ByLock Android application were found to be available and examined:

2. **ByLock for Android 1.1.6.** The application was downloaded as an APK file from http://downloadapk.net/down_ByLock-Secure-Chat-amp-Talk.601634.html. The file was downloaded on 20 July 2017. Fox-IT calculated hash values of the file:
- MD5 hash³⁶ b43eeb3fed4c20061e0c87f4d371508d
 - SHA1 hash aeb4256fa23d0d5090c5506e2d647f8d6a63f4af
3. **ByLock for Android 1.1.7.** The application was downloaded as an APK file from <https://m.downloadatoz.com/bylock-secure-chat-talk/net.client.by.lock/bylock-secure-chat-talk,v1.1.7-download.html>. The file was downloaded on 20 July 2017. Fox-IT calculated hash values of the file:
- MD5 hash 84fddf10a23f4f25b5212232b73cd557
 - SHA1 hash cac87620162e211b4fb02719a244b8127610cb7e

The following versions are mentioned in the MIT report, but were no longer available for analysis in online public sources:

- ByLock for Android 1.1.3
- ByLock for Android 2.0 (ByLock++)

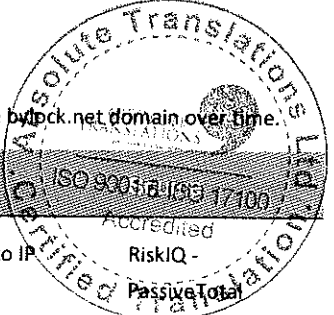


³⁶ A hash value is the result of a mathematical calculation, using an algorithm. The calculation only works in one direction, meaning that the hash value cannot be used to determine the original data. A hash value represents a digital fingerprint of the data and consists of a series of numbers (of a fixed length). Typically, a hash value is recorded during the creation of a forensically sound copy. The integrity of that copy can be checked (possibly by others) by calculating the hash value again, and checking it against the originally recorded hash value. Known and commonly used hash algorithms are MD5, SHA1 and SHA256.

7 APPENDIX

7.1 ByLock.net timeline

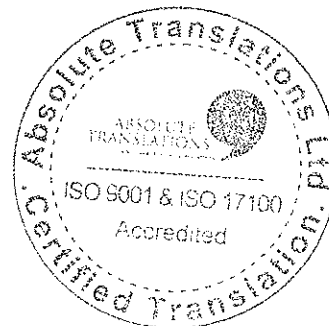
This table lists the changes in ownership information and IP addresses referenced by the ByLock.net domain over time.



Date	Event	
14 March 2014	At this date, it was observed that ByLock.net resolved to IP address 184.168.221.39 hosted by godaddy.com	
18 March 2014	At this date, it was observed that ByLock.net resolved to IP address 184.168.221.39.	DomainTools
31 March 2014	At this date, it was observed that ByLock.net resolve IP address was changed from 184.168.221.39 to 69.64.56.133	DomainTools
29 April 2014 – 10 August 2014	Between these dates, it was observed that IP address 69.64.56.133 was hosted by server4you-inc.	RiskIQ – PassiveTotal
4 August 2014	At this date, it was observed that ByLock.net was last resolved to IP address 69.64.56.133	ViewDNS
10 August 2014 – 12 March 2016	Between these dates, it was observed that IP address 46.166.160.137 was hosted by uab-cherry-servers	RiskIQ – PassiveTotal
14 August 2014	At this date, it was observed that the ByLock.net hosted on IP address 69.64.56.133 and was changed to IP-address 46.166.160.137	DomainTools
19 February 2016	At this date, the last activity was observed for IP address 46.166.160.137	VirusTotal
15 March 2016	On this date, IP address 46.166.160.137 was last resolved on this date, located in Republic of Lithuania, owned by Dedicated servers	ViewDNS
20 March 2016 – 21 April 2016	Between these dates, it was observed that IP address 184.168.221.72 was hosted by godaddy.com	RiskIQ – PassiveTotal
2 April 2016	At this date, it was observed that ByLock.net resolved to IP address 46.166.160.137 was changed to IP address 184.168.221.72	DomainTools
19 April 2016	ByLock.net hosted on IP address 184.168.221.72 was last seen on this date, located in Scottsdale - United States, hosted by GoDaddy.com, LLC	ViewDNS

4 May 2016	At this date, it was observed that the IP address 184.168.221.72 was not resolvable	DomainTools
10 August 2016	On this date, the IP address 217.70.184.38 was hosted by gandi-sas	RiskIQ – PassiveTotal
11 August 2016	At this date, it was observed that ByLock.net is resolved to a new IP address: 217.70.184.38	DomainTools
12 August 2016	At this date, it was observed that ByLock.net resolved to IP address 217.70.184.38 and was changed to IP 104.27.169.137	DomainTools
13 August 2016 – 2 August 2017	Between these dates, it was observed that IP address 104.27.169.137 was hosted by Cloudflare, Inc.	RiskIQ – PassiveTotal
24 August 2016	At this date, it was observed that ByLock.net resolved to IP address 104.27.169.137 was changed to IP address 104.27.168.137	DomainTools
13 October 2016 – 2 August 2017	Between these dates, IP address 104.27.168.137 was hosted by Cloudflare, Inc.	RiskIQ – PassiveTotal
1 August 2017	ByLock.net hosted on IP address 104.27.168.137 was last seen on this date, located in San Francisco - United States, hosted by Cloudflare, Inc.	ViewDNS
1 August 2017	ByLock.net hosted on IP address 104.27.169.137 was last seen on this date, located in San Francisco - United States, owned by Cloudflare, Inc.	ViewDNS

Table 3: Bylock.net timeline



7.2 Glossary of technical terms

Android Package Kit	The package file format used by the Android operating system for distribution and installation of mobile apps and middleware.
APK	See Android Package Kit
Decompilation	A technique to transform executable computer code (back) to source code. Commonly used when analyzing workings of a program.
DNS	See Domain Name System
Domain Name System	A hierarchical decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates more readily memorized domain names to the numerical IP addresses needed for locating and identifying computer services and devices with the underlying network protocols.
HTTPS	HTTP Secure is a communications protocol for secure communication over a computer network which is widely used on the Internet. HTTPS consists of communication over Hypertext Transfer Protocol (HTTP) within a connection encrypted by Transport Layer Security, or its predecessor, Secure Sockets Layer. The main motivation for HTTPS is authentication of visited web resources and protection of the privacy and integrity of the exchanged data.
Java	A general-purpose computer programming language that is concurrent, class-based, object-oriented and specifically designed to have as few implementation dependencies as possible.
Proxy server	A server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server. The resource requested is then fetched from the other server or retrieved from a possible cache.
SSL Certificate	A public key certificate used for a secure (SSL) connection. A public key certificate is an electronic document used to prove the ownership of a public key. The certificate includes information about the key, information about the identity of its owner (called the subject), and the digital signature of an entity that has verified the certificate's contents (called the issuer). If the signature is valid, and the software examining the certificate trusts the issuer, then it can use that key to communicate securely with the certificate's subject. In Transport Layer Security (TLS) a certificate's subject is typically a computer or other device, though TLS certificates may identify organizations or individuals in addition to their core role in identifying devices. TLS, sometimes called by its older name Secure Sockets Layer (SSL), is notable for being a part of HTTPS, a protocol for securely browsing the web.
SQL	Structured Query Language (SQL) is a domain-specific language used in programming and designed for managing data held in a relational database management system (RDBMS), or for stream processing in a relational data stream management system (RDSMS).
Virtual Private Network	A technology used to tunnel network traffic over a tunneling protocol. It is also used to provide secure and anonymous access to the internet by applying encryption techniques to secure the channel and hiding the VPN client's identity.
VPN	See Virtual Private Network

