TEKNİK UZMAN RAPORU

ByLock Uygulaması

Gerçek Kullanıcıların Tespiti

Bu rapor ByLock Uygulamasını kullanmanın suç olup olmadığını veya ByLock Uygulaması sunucu verilerinin hukuka uygun olarak elde edilip edilmediğini tartışmaz.

Bu rapor, ByLock Uygulaması kullanıcılarının gerçek kullanıcılarının nasıl tespit edilmesi gerektiğini teknik veriler ile açıklar.

Bu raporun herhangi bir sanık dosyasına sunulmasında sakınca yoktur, ancak yargılamanın bireyselliği gereği ve sanığın dava dosyasının bütünü açısından uygun olmaması durumunda yazarlar tarafından herhangi bir sorumluluk kabul edilmemektedir.

Berker KILIÇ

Adli Bilişim Uzmanı
Veri Bilimci

Elif Eylem KINACILAR

Avukat
Adli Bilirkişi

Mesut Can TARIM

Avukat
Adli Bilirkişi

İÇİNDEKİLER

Bu rapor 4 ana bölümden oluşmaktadır.

Birinci bölümde, CGNAT konusunda açıklamalara yer verilmiştir. Bu açıklamalar, dünyanın her tarafında geçerli, hukuk sistemlerinden bağımsız, hukuken farklı şekilde yorumlanması mümkün olmayan ilgili RFC dokümanlarına ve akademik çalışmalara dayanan teknik gerçeklerdir.

İkinci bölümde, ülkemizde mahkemelerin talebi üzerine Bilgi ve İletişim Teknolojileri (BTK) tarafından sağlanan CGNAT Kayıtlarından bahsedilmiştir. İlgili RFC dokümanları ve iç mevzuattaki karşılıkları açıklanarak bir Hedef IP açısından gerçek abone tespitinde kullanılabilirliği açıklanmıştır.

Üçüncü bölümde, Litvanyada bulunan ve Milli İstihbarat Teşkilatı tarafından elde edilen ByLock Uygulaması Sunucu Veritabanı, ilgili resmi raporlar paralelinde incelenmiş ve veritabanının içerdiği kayıtlar itibariyle gerçek ByLock kullanıcılarının tespitinde kullanılabilirliği açıklanmıştır. Ayrıca bir kısım tutarsızlıklara değinilmiştir.

Dördüncü bölümde, ByLock Uygulaması veri tabanı kayıtları ile CGNAT kayıtları arasında gerçek kullanıcıların tespiti için kurulması gereken ilişki açıklanmıştır.

1. Taşıyıcı-Sınıf Ağ Adresi Çeviricisi (CGN/CGNAT-Carrier-Grade Network Address Translation)

CGNAT Nedir?

Başlangıçta, Internet mimarisi, cihazları benzersiz şekilde tanımlamak için IP adreslerini (IPv4) kullanmaktaydı. Bu yapı, eşler arası iletişimin temelini oluşturmaktaydı. Ancak zaman içerisinde IP adreslerinin kıt hale gelmesi bu mimariyi yetersiz hale getirmiştir [Richter vd., 2016 & RFC 6269].

2011 yılında, Internet İnternet Atanmış Numaralar Kurumu (IANA-Assigned Numbers Authority), kullanılabilir son IPv4 adreslerini Bölgesel İnternet Kayıtlarına (RIR-Regional Internet Registries) tahsis etmiştir [Livadariu vd., 2018].

Bu durum, Internet Servis Sağlayıcıların (ISP- Internet Service Providers), bütün abonelere aynı anda Internet hizmeti sağlayamaması anlamına gelecektir.

Bu soruna karşılık üretilen çözüm Taşıyıcı Dereceli NAT (CGN-Carrier-Grade NAT) olarak bilinen Ağ Adresi Çeviricisi (NAT-Network Address Translation) mekanizmasıdır. CGN, geleneksel NAT (NAT44) mekanizması tarafından kullanılan IPv4 adres paylaşım prensibi üzerine inşa edilmiştir [Livadariu vd., 2018].

NAT teknolojisi yeni bir teknoloji değildir. Özel ağlar (ev, küçük işletme ve birçok kurumsal ağ) uzun zamandır NAT' ları, tüm IP cihazları için özel IPv4 adresleri [RFC 1918] aracılığıyla yönetmek için kullanmaktadır.

Bu dokümanda bahsedilen Büyük Ölçekli NAT (LSN-Large Scale NAT) veya NAT444 olarak da isimlendirilen, belirli bir mesajın, kaynak aygıttan hedefine aktarılırken 3 farklı IPv4 yapısıdır.

NAT teknolojileri, İnternet Servis Sağlayıcıları tarafından herhangi bir anda internete bağlanmaya çalışan müşterilere verilecek mevcut IPv4 adreslerinin kademeli olarak yokluğunu telafi etmek için kullanılır [Fantin vd., 2019].

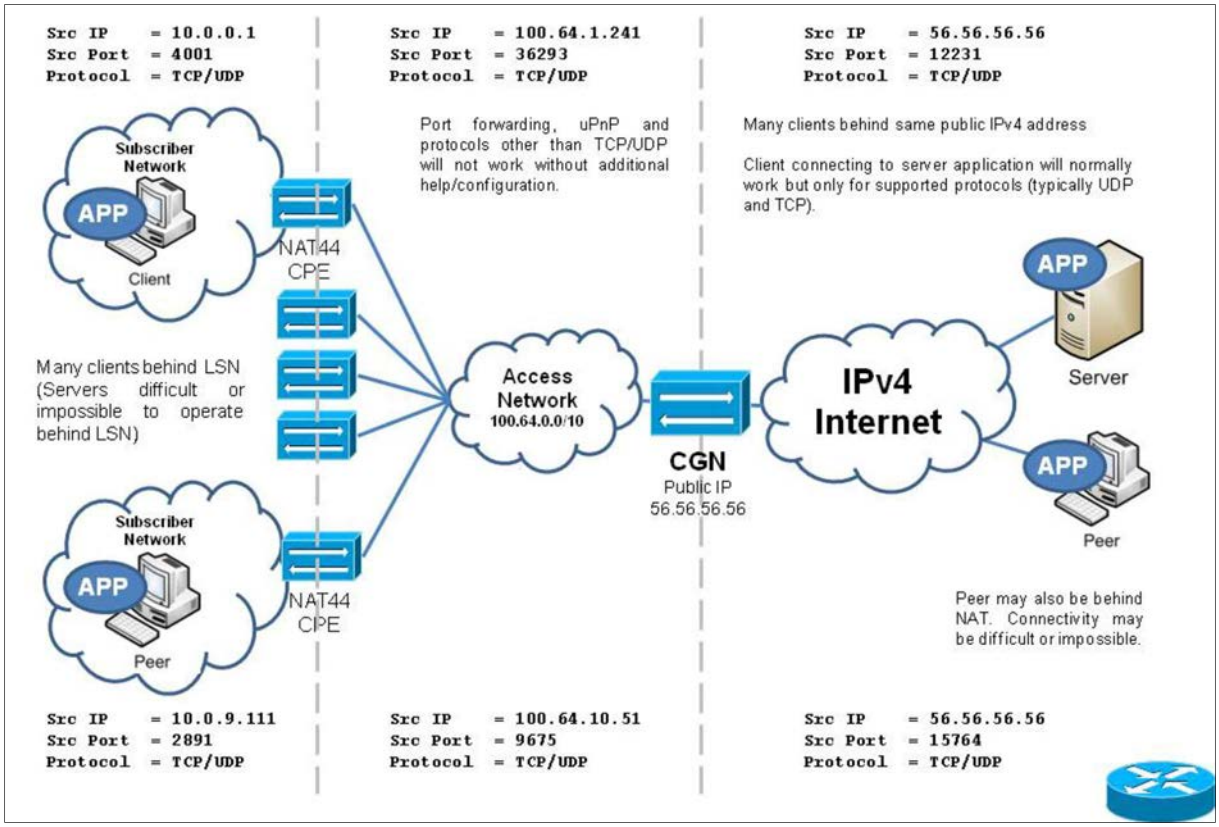
CGN, her kullanıcıya paylaşımsız IP adreslerinin atanabileceği IPv6' ya geçiş sürecinde, sınırlı sayıda ve artık yetersiz olan IPv4 adreslerinin kullanımını en üst düzeye çıkarmak için ISP' lerin abonelerine IPv4 adreslerini aboneleri arasında paylaştırmasına izin verir. [P] Yani çok sayıda IPv4 özellikli cihazın tek bir IP adresini paylaşmasına izin verir [Broadband Internet Technical Advisory Group, 2012].

Şekil 1. diyagram Abone/Müşteri Ekipmanları (CPE-Customer Premise Equipment) da dahil olmak üzere bir CGN topolojisi göstermektedir.

Her bir abone kendi NAT44 ekipmanı ile, bu ekipman kullanılan cep telefonu da olabilir, kendi ağını oluşturabilirken, aynı zamanda CGN (NAT444) ekipmanı aracılığı ile diğer abonelerle birlikte aynı IPv4 adresini üzerinden fakat her bir abone için farklı olan Portlar üzerinden Internet erişimine sahip olabilmektedir [InterConnect Communications, 2013].

Burada NAT44 olarak ifade edilen CPE aygıtı, geleneksel olarak NAT aygıtları, özel kayıt dışı adresleri olan yalıtılmış bir adres alanını, genel olarak benzersiz kayıtlı adresleri olan harici bir bölgeye bağlamak için kullanılır [RFC 2663 & RFC 1918].

ISP' nin her bir IPv4 adresini kaç aboneye tahsis edeceği, ISP' nin kendi belirleyeceği bir konudur. Teorik olarak bir IPv4 üzerinde 65.536 adet Port bulunmaktadır. Eğer operatör her bir IPv4 ile 10 adet abonesine hizmet verecekse, her bir abonesi için 6.553 Portun kullanımı mümkün olacaktır.



Şekil 1. CGN Ağ Topolojisi

CGNAT Abone Kayıtları

Geçmişte, abonelere dinamik IP adresleri verilse dahi, trafik kaynağını, yani aboneyi tanımlamak için dinamik IP adresi ile abone eşleşmesinin günlüğe kaydedilmesi yeterliydi.

Günümüzde ise IP adreslerinin her bir abone için yetersiz olması ve aynı IP adresinin birden fazla abone tarafından paylaşılarak kullanıldığı CGN teknolojisinde, CGN kullanımı tarafından etkinleştirilen IP adresi paylaşımında bir abone cihazını yalnızca kaynak IP adresi üzerinden benzersiz bir şekilde tanımlama yeteneği kaybedilir [Broadband Internet Technical Advisory Group, 2012 & RFC 6269].

Bunun nedeni, IP adreslerinin birçok abonede paylaşılmasıdır. CGN' in arkasında belirli bir aboneyi tanımlamak için, ISP abonenin dahili kaynak IP adresini ve dahili kaynak portunu, abone tarafından kullanılan her oturum için CGN' nin harici kaynak IP adresine ve harici kaynak portuna eşleyebilmesi ve bunu günlüğe kaydetmesi gerekir [InterConnect Communications, 2013].

İnternet trafiğinin kaynağını belirlemek, trafiğine kanuni olarak müdahale edilebilmesi ve kanuni yaptırım uygulanabilmesi için yasal bir gerekliliktir [InterConnect Communications, 2013].

Bu durumda, kolluk kuvvetlerinin veya diğer yetkili kurumların abonenin kimliğini talep edebilmeleri için, ISP' ye kaynak IP adresini ve kaynak portunu ve bir olayın gerçekleştiği zamanı sunabilmeleri gerekir.

CGN kayıtlarında her bir bağlantı oturumu için ISP tarafında günlüğe kaydedilmesi gereken bilgiler tarih, saat, dahili IP adresi (Özel IP), dahili port numarası (Özel Port), harici IP adresi (Genel IP), harici Port numarası (Genel Port), hedef tarafında ise günlüğe kaydedilmesi gereken bilgiler tarih, saat, kaynak IP ve kaynak Port numaralarıdır [InterConnect Communications, 2013, RFC 6269 & RFC 6888]. Ne var ki ISP'lerden erişim günlüklerinin de talep edilmesi nedeni ile ISP' ler de hedef IP ve hedef Port numarasını kaydetmektedirler. Elbette hedef IP ve hedef Port numarası kayıtlarını da günlükte ilgili abone bilgileri ile birlikte kaydetmektedirler. Bu sayede ise ISP' ler ilgili kurumlardan kendilerine gelen erişim taleplerine yanıt verebilmektedirler.

CGNAT Kayılarının Delil Olarak Kullanılması

Teknoloji sayesinde her şey yeni, daha hızlı ve daha kolay bir biçimde, nasıl iletişim kurduğumuz, çalıştığımız ve verilerle nasıl uğraştığımız. Teknoloji her şeyi değiştiriyor. Suç, bildiğimiz gibi, teknolojiyi sürece entegre etmekle birlikte değişiyor. Değerli varlıklar dijital forma dönüştükten sonra bu doğal bir sonuçtur [Shaabana vd.].

Adli Bilişim, bilgisayar suçu ile ilgili kanıtların veri bütünlüğünün korunarak sunulmasını amaçlar. Ali Bilişimin nihai amacı 5N1K sorularının cevaplanabileceği kanıtlar elde etmektir. Yani, Ne, Ne zaman, Nerede, Nasıl, Neden ve Kim sorularının cevapları aranır. Bu soruları cevaplamak, bir olayın iddialarını doğrulamaya veya reddetmeye yol açar. [Dimitriadis, 2020]

İnternet Mühendisliği Görev Gücü (IETF-Internet Engineering Task Force), ISP' nin kayıtlarındaki belirli bir aboneyi IPv4 adresi temelinde benzersiz bir şekilde tanımlayabilmek için 1) Kaynak IP adres, 2) Kaynak Port Numarası ve 3) IP adresi ve Port numarasının kullanıldığı zamanı tam olarak sağlamasını önerir. Ancak, Internet sunucuları ve uygulamalar genellikle gelen bağlantıların Kaynak IP adresini ve bağlantı süresini kaydetmektedirler. David O'Reilly buna "CGN bilgi boşluğu" demektedir [Wilson, 2019].

Kolluk kuvvetleri ve adli makamlar için bu somut olarak CGN'nin cezai soruşturmaları çok daha zor ve uzun hale getirdiği anlamına gelir, çünkü sadece kamu IPv4 adresini ve bir zaman damgasını kullanırken bir aboneyi tanımlamak artık İSS'ler için neredeyse imkansızdır. operatörler araştırmacılara aynı hizmete aynı anda bağlı olan ve aynı IP adresini kullanarak tüm abonelerin tam listesini verebilir ve bu liste binlerce isim içerebilir. Bu listede soruşturulacak ve gereksiz şekilde ceza yargılamalarına karışacak binlerce kişinin mağduriyeti endişe kaynağı olmalıdır [Wilson, 2019 & RFC 6269].

Ancak, 2019 Europol Cyber Security Perspectives isimli raporda yer alan bu ifade, aynı hizmete aynı anda aynı IP adresini kullanarak bağlantı kuran aboneler için geçerlidir.

Bu durum, Facebook, Twitter ve benzeri milyarlarca kişinin kullandığı uygulamalar için geçerli olabilir ancak ziyaretçi sayısı veya kullanıcı sayısı görece az olan uygulamalar için geçerli olmayacaktır.

Çünkü her ne kadar aynı IP adresi farklı Port numaraları aracılığı ile onlarca fazla aboneye tahsis edilmiş olsa da bu aboneler arsından yalnızca bir veya birkaç tanesi, aynı anda kullanıcı sayısı görece az olan bu uygulamayı kullanıyor olacaktır.

Burada kullanıcı sayısının görece az olması nedeni ile sunucu hizmeti verilen IP adresinin başkaca bir uygulama için kullanılmadığı varsayılmıştır.

Ancak elbetteki bir IP adresinin birden fazla uygulamanın sunumu amaçlı kullanılması mümkündür ve bu durumda sunucu tarafında yalnızca ilgili uygulamanın kaydında bulunan Kaynak IP adresi bilinen bir kullanıcı ile ISP tarafı Hedef IP adresi bilinen abonenin eşleştirmesi yapılarak gerçek kişilere ulaşılması mümkün olabilecektir.

Burada göz ardı edilmemesi gereken husus, bir IP adresinin mutlak suretle bir alan adı (DomainName) ile birlikte kullanılmasının gerekmediğidir. Alan adlarının belirli bir IP adresi üzerinden kullanım geçmişleri çeşitli sorgularla elde edilebilir bir bilgidir. Ancak, doğrudan IP adresini kullanan sunucu/istemci mimarisini kullanan uygulamalar için geriye dönük olarak sunucu IP adreslerinin aktif olarak kullanıldıkları zaman aralığını belirlemek mümkün değildir.

Aynı IP adresi üzerindeki diğer uygulamaların da var olabilmesi nedeni ile yalnızca ISP tarafı Hedef IP adresi bilgisi, belirli bir abonenin belirli bir sunucu üzerinde belirli bir uygulamaya eriştiğine dair kesin bir tespitte bulunabilmek mümkün olmayacaktır.

Yan, belirli bir IP adresi üzerinde çalışan belirli bir sunucu üzerinde, birden fazla uygulamanın var olabileceği de göz önünde bulundurularak, ISP tarafında bu sunucu IP' sinin Hedef IP olarak kaydedildiği her abone sunucu üzerindeki farklı uygulamaları kullanmış olabilir, ancak, sunucu üzerindeki belirli bir uygulamanın kullanıcılarına ait Kaynak IP adresleri de mevcutsa, bu Kaynak IP adresleri ile ISP tarafından sağlanan Hedef IP adresine bağlı abone bilgileri tek bir gerçek kişiyi gösterdiği sürece, sunucu üzerindeki belirli bir uygulamayı kullanan gerçek kişinin tespit edilebilir olacağı açıktır.

Özet

ISP' tarafı CGNAT kayıtları, aboneleri IP adresi, Port numarası ve zaman damgası ile tekil olarak birbirinden ayırt edebilecek niteliktedir.

Bu abonelerin belirli bir IP adresine erişimleri/erişim talepleri, ISP' nin Hedef IP ve Hedef Port bilgisini de kayıt altına almaları sayesinde tespit edilebilir bir veridir.

Ancak bu abonenin Hedef IP üzerinde yalnızca tek bir uygulamayı kullanabilir olmaları durumunda abonenin bu uygulamayı kullandığını tespiti sağlayacaktır.

Eğer sunucu tarafında aynı IP adresi üzerinden birden fazla uygulama bulunuyor ise, bu durumda ISP' nin CGNAT kayıtları abonenin Hedef IP üzerindeki belirli bir uygulamayı kullandığına dair kesin bir tespitin yapılamamasına neden olacaktır.

Sunucu tarafında, uygulamaya ait kullanıcı erişim kayıtlarının mevcut olması durumunda, kullanıcı erişim kayıtları ile ISP' nin CGNAT kayıtları karşılaştırılmak suretiyle abonenin Hedef IP üzerindeki belirli bir uygulamayı kullandığına dair tespitte bulunulabilecektir.

Sunucu tarafındaki uygulamanın kullanıcılarının belirli kimlik ve erişim bilgileri ile kayıt altına aldığı bir durumda ise ISP' nin CGNAT kayıtları ile yapılan karşılaştırmada uygulama kullanıcısı ile abone arasındaki kesin bir eşleşme ile sonuçlanacaktır.

Kaynakça

A. Dimitriadis, N. Ivezic, B. Kulvatunyou & I. Mavridis, (2020), **D4I - Digital Forensics Framework For Reviewing and İnvestigating Cyber Attacks**, Array, 5, doi: 10.1016/j.array.2019.100015.

A. Shaabana, & N. Abdelbakia, (2018), **Comparison Study of Digital Forensics Analysis Techniques; Findings versus Resources**, Procedia Computer Science, 141, 545–551, doi: 10.1016/j.procs.2018.10.128.

Broadband Internet Technical Advisory Group, (2012), **Implications of Large Scale Network Address Translation (NAT)**.

O. Maennel, R. Bush, L. Cittadini & S.M. Bellovin, (2008), **A Better Approach than CarrierGradeNAT**, Columbia University Technical Report, CUCS-041-08.

I. Livadariu, K. Benson, A. Elmokashfi, A. Dhamdhere & A. Dainotti, (2018), **Inferring Carrier-Grade NAT Deployment in the Wild**, IEEE Conference on Computer Communications (IEEE INFOCOM), doi: 10.1109/infocom.2018.8486223.

InterConnect Communications, (2013), **MC/159 Report on the Implications of Carrier Grade Network Address Translators**.

P. Richter, F. Wohlfart, N. Vallina-Rodriguez, M. Allman, R. Bush, A. Feldmann, C. Kreibich, N. Weaver & V. Paxson, (2016), **A Multi-perspective Analysis of Carrier-Grade NAT Deployment**, ACM Internet Measurement Conference (IMC), 215-279, doi: 10.1145/2987443.2987474.

RFC 1918, **Özel Ağlar İçin Adres Tahsisi**, (Address Allocation for Private Internets)

RFC 2663, **IP Ağ Adresi Çevirmeni (NAT) Terminolojisi ve Dikkat Edilmesi Gerekenler**, (IP Network Address Translator (NAT) Terminology and Considerations)

RFC 6269, **IP Adresi Paylaşmayla İlgili Sorunlar**, (Issues with IP Address Sharing)

RFC 6888, **Taşıyıcı Sınıfı NAT'lar (CGN'ler) için Genel Gereksinimler**, (Common Requirements for Carrier-Grade NATs (CGNs))

S. Fantin, G. Specchio & P. Valcke, (2019), **Modern Issues in Cyber Forensics and Digital Intelligence: A Critical, Case-Studies-Based Overview in Light of the Announced Legislative Reforms**, Rivista Italiana Di Informatica E Diritto (RIID), 1(2), doi: 10.32091/RIID0011.

S. Wilson, (2019), **The Dark Side of Address Translation Mechanisms (CGNAT)**, European Cyber Security Perspectives 2019, 10-13.

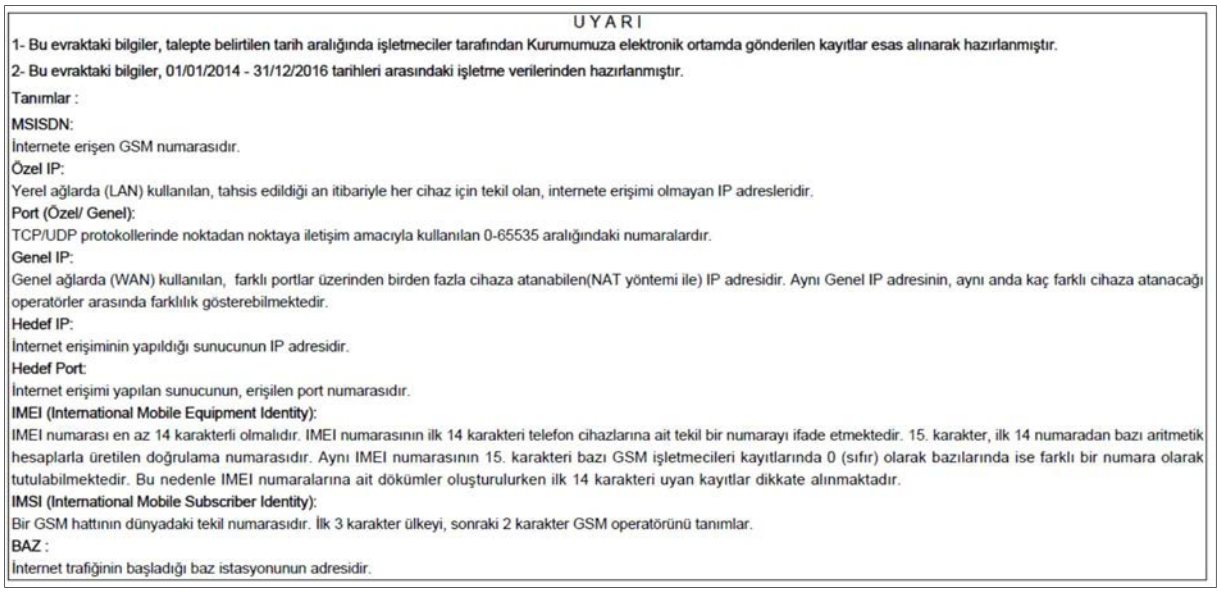
2. BTK Tarafından Sağlanan CGNAT Kayıtları

Türkiye' de ISP abonelerine ait CGNAT kayıtları Bilgi ve İletişim Teknolojileri Kurum (BTK) tarafından merkezi olarak depolanmakta ve yetkili kurumların talebi ile sağlanmaktadır.

BTK tarafından sağlanan CGNAT kayıtlarının ilk sayfasında UYARI başlığı altında Şekil-2' deki açıklamalar yer almaktadır.

Bu açıklamalarda sıra numaralı olarak yer alan 2 açıklama dikkat çekmektedir.

Bunlardan birincisi, BTK tarafından sağlanan bilgilerin, işletmeciler tarafından elektronik ortamda BTK' ya gönderilen bilgilerden ibaret olduğu ikincisi ise BTK' nın elinki mevcut CGNAT verilerinin 01/01/2014 ile 31/12/2016 tarihlere ait olduğudur.



UYARI

1- Bu evraktaki bilgiler, talepte belirtilen tarih aralığında işletmeciler tarafından Kurumumuza elektronik ortamda gönderilen kayıtlar esas alınarak hazırlanmıştır.

2- Bu evraktaki bilgiler, 01/01/2014 - 31/12/2016 tarihleri arasındaki işletme verilerinden hazırlanmıştır.

Tanımlar :

MSISDN:
İnternete erişen GSM numarasıdır.

Özel IP:
Yerel ağlarda (LAN) kullanılan, tahsis edildiği an itibariyle her cihaz için tekil olan, internete erişimi olmayan IP adresleridir.

Port (Özel/ Genel):
TCP/UDP protokollerinde noktadan noktaya iletişim amacıyla kullanılan 0-65535 aralığındaki numaralardır.

Genel IP:
Genel ağlarda (WAN) kullanılan, farklı portlar üzerinden birden fazla cihaza atanabilen(NAT yöntemi ile) IP adresidir. Aynı Genel IP adresinin, aynı anda kaç farklı cihaza atanacağı operatörler arasında farklılık gösterebilmektedir.

Hedef IP:
İnternet erişiminin yapıldığı sunucunun IP adresidir.

Hedef Port:
İnternet erişimi yapılan sunucunun, erişilen port numarasıdır.

IMEI (International Mobile Equipment Identity):
IMEI numarası en az 14 karakterli olmalıdır. IMEI numarasının ilk 14 karakteri telefon cihazlarına ait tekil bir numarayı ifade etmektedir. 15. karakter, ilk 14 numaradan bazı aritmetik hesaplarla üretilen doğrulama numarasıdır. Aynı IMEI numarasının 15. karakteri bazı GSM işletmecileri kayıtlarında 0 (sıfır) olarak bazılarında ise farklı bir numara olarak tutulabilmektedir. Bu nedenle IMEI numaralarına ait dökümler oluşturulurken ilk 14 karakteri uyan kayıtlar dikkate alınmaktadır.

IMSI (International Mobile Subscriber Identity):
Bir GSM hattının dünyadaki tekil numarasıdır. İlk 3 karakter ülkeyi, sonraki 2 karakter GSM operatörünü tanımlar.

BAZ :
İnternet trafiğinin başladığı baz istasyonunun adresidir.

Şekil 2. BTK Tarafından Sağlanan CGNAT Kayıtları Açıklamaları

Şekil-2' de yer alan diğer açıklamalar "Tanımlar" yan başlığı altında sıralanmıştır. Bu tanımlar şunlardır:

MSISDN: Internete erişen GSM numarasıdır.

Özel IP: Yerel ağlarda (LAN) kullanılan, tahsis edildiği an itibariyle her cihaz için tekil olan, internete erişimi olmayan IP adresleridir.

Port (Özel/Genel): TCP/UDP protokollerinde noktadan noktaya iletişim amacıyla kullanılan 0-65535 aralığındaki numaralardır.

Genel IP: Genel ağlarda (WAN) kullanılan, farklı portlar üzerinden birden fazla cihaza atanabilen (NAT yöntemi ile) IP adresidir. Aynı Genel IP adresinin, aynı anda kaç farklı cihaza atanacağı operatörler arasında farklılık gösterebilmektedir.

Hedef IP: Internet erişiminin yapıldığı sunucunun IP adresidir.

Hedef Port: Internet erişimi yapılan sunucunun, erişilen port numarasıdır.

IMEI (International Mobile Equipment Identity): IMEI numarası en az 14 karakterli olmalıdır. IMEI numarasının ilk 14 karakteri telefon cihazlarına ait tekil bir numarayı ifade

etmektedir. 15. karakter, ilk 14 numaradan bazı aritmetik hesaplarla üretilen doğrulama numarasıdır. Aynı IMEI numarasının 15. karakteri bazı GSM işletmecileri kayıtlarında 0 (sıfır) olarak bazılarında ise farklı bir numara olarak tutulabilmektedir. Bu nedenle IMEI numaralarına ait dökümler oluşturulurken ilk 14 karakteri uyan kayıtlar dikkate alınmaktadır.

IMSI (International Mobile Subscriber Identity): Bir GSM hattının dünyadaki tekil numarasıdır. Ilk 3 karakter ülkeyi, sonraki 2 karakter GSM operatörünü tanımlar.

BAZ: Internet trafiğinin başladığı baz istasyonunun adresidir.

BTK tarafından sağlanan CGNAT kayıtlarında yer alan tanımlar, ilgili RFC dokümanları açısından değerlendirildiğinde, RFC 6888 Taşıyıcı Sınıfı NAT'lar (CGN'ler) için Genel Gereksinimler ve 6269 IP Adresi Paylaşmayla İlgili Sorunlar ile uyumlu oldukları görülmektedir.

BTK tarafından sağlanan CGNAT kayıtları içerisinde yer alan Özel IP, Özel Port bilgileri abonenin ISP tarafından oluşturulan ve aynı IPv4 adresini paylaşan aboneler grubu içerisinde belirlenebilmesini sağlarken, Genel IP ve Genel Port bilgileri ise aboneler tarafından paylaşılan IPv4 adresini ve bu IP adresi içerisinde aboneye tahsis edilen iletişim portunun belirlenebilmesini sağlamaktadır.

RFC 6888 içerisinde Gereksinim-12' de "Bir CGN, idari nedenlerle gerekmedikçe, hedef adresleri veya bağlantı noktalarını günlüğe kaydetmemelidir" ifadesi yer almaktadır.

Bu gereksinimin gerekçesi ise RFC 6888' de şu şekilde açıklanmaktadır: "CGN' de hedef IP kaydı, gizlilik sorunları yaratır. Ayrıca, okuyucular Internet sunucuları [RFC 6302] için günlüğe kaydetme önerilerinin farkında olmalıdır. Uyumlu sunucularla, hedef adresin ve bağlantı noktasının CGN tarafından günlüğe kaydedilmesi gerekmez. Bu, günlüğe kaydetme miktarını azaltmaya yardımcı olabilir."

Yani bu gereksinim, abonelerin iletişim gizliliğinin sağlanabilmesi için kaydedilmemesi gerektiği düşünülmektedir. Ancak yine RFC 6888' in bir sonraki paragrafında bağlantı kurulan sunucunun RFC 6302 ile uyumlu şekilde kayıt tutmuyor olabileceğinin göz önünde bulundurularak karar verilmesi önerilmektedir.

Türkiye mevzuatına bakıldığında ISP' lerin kayıt tutma zorunluluğu, "5651 Sayılı Internet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" ve bu kanuna dayanak alan "İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik" ile düzenlenmiştir.

Yönetmeliğin "Tanımlar" başlığı altında kaydı tutulacak veriler "Madde-3/ö) Vekil sunucu trafik bilgisi: İnternet ortamında erişim sağlayıcı tarafından kullanılan vekil sunucu hizmetine ilişkin talebi yapan kaynak IP adresi ve port numarası, erişim talep edilen hedef IP adresi ve port numarası, protokol tipi, URL adresi, bağlantı tarih ve saati ile bağlantı kesilme tarih ve saati bilgisi gibi bilgileri" olarak tanımlanmıştır.

Aynı yönetmeliğin "Erişim sağlayıcının yükümlülükleri" başlığı altında ise "Madde-8/e) Kullanıcılarına vekil sunucu hizmeti sunuyor ise; vekil sunucu trafik bilgisini bir yıl saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü oluşan verilerin dosya bütünlük değerlerini zaman damgası ile birlikte muhafaza etmek ve gizliliğini temin etmekle" ISP' leri yükümlülük altına sokmaktadır.

BTK tarafından sağlanan CGNAT kayıtları içerisinde yer alan Hedef IP ve Hedef Port bilgilerinin abone ile ilişkili olarak kayıt altına alınmış olması da bu durumda Hedef IP adresinde bulunan sunucunun, yurtdışı kaynaklı bir sunucu olması durumunda, RFC 6302 ile uyumlu olarak Kaynak IP ve Kaynak Port bilgilerini kaydedip kaydetmediği bilinmemesi ve günlük kayıtlarının temin edilmesinin mümkün görülmemesi nedeni ile yerel mevzuat açısından, suça ilişkin bir abone tespitinin yapılabilmesi için gerekli olacaktır.

Yurtiçi sunucular açısından bu durum aynı yönetmeliğin yine "Tanımlar" bölümü altında "Madde-3/ş) Yer sağlayıcı trafik bilgisi: İnternet ortamındaki her türlü yer sağlamaya ilişkin olarak; kaynak IP adresi, hedef IP adresi, bağlantı tarih ve saat bilgisi, istenen sayfa adresi, işlem bilgisi (GET, POST komut detayları) ve sonuç bilgileri gibi bilgileri" şeklinde tanımlanmış ve "Yer sağlayıcının yükümlülükleri" başlığı altında "Madde-7/c) Yer sağlayıcı trafik bilgisini altı ay saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü oluşan verilerin dosya bütünlük değerlerini zaman damgası ile birlikte saklamak ve gizliliğini temin etmekle," yer sağlayıcıları yükümlülük altına sokmaktadır.

Özet

BTK tarafından sağlanan CGNAT kayıtlarında yer alan Özel IP, Özel Port, Genel IP, Genel Port ve Oturum Başlama Tarihi (Zaman Damgası) bilgilerinin kaydedilmesi, RFC 6269 ve 6888 ile uyumludur. Bu durum ilgili kanun ve yönetmelik ile ISP' ler açısından bir zorunluluk olarak görülmüştür.

BTK tarafından sağlanan CGNAT kayıtlarında yer alan Hedef IP ve Hedef Port bilgilerinin kaydedilmesi RFC 6888 ile uyumludur. RFC dokümanında abonelerin gizliliği gereksinimin göz önünde bulundurulması gerektiği ifade edilmiştir. Hedef IP adresinde yer alan yurtdışı sunucunun RFC 6302' ye göre kullanıcının Kaynak IP ve Kaynak Port bilgisini kaydedip kaydetmediği bilinmemesi ve günlük kayıtlarının temin edilmesinin mümkün görülmemesi nedeni ile ISP' ler açısından bir zorunluluk olarak görülmüştür. Yurtiçi sunucular için Hedef IP ve Hedef Port bilgilerinin kaydedilmesi ilgili kanun ve yönetmelik ile yer sağlayıcılar açısından bir zorunluluk olarak görülmüştür.

Bu durumda, ISP' ler tarafından BTK' ya gönderilen CGNAT kayıtları aracılığı ile bir abonenin herhangi bir IP adresine erişim veya erişim talebi kesin bir şekilde belirlenebilecektir. Ancak, Hedef IP adresinde bulunan sunucunun birden fazla uygulamayı barındırması durumunda, bu uygulamalardan hangisine erişim sağlandığı veya erişim sağlanmaya çalışıldığı kesin bir şekilde tespit edilemeyecektir.

3. ByLock Uygulama Sunucusu, Veritabanı Kayıtları

ByLock Uygulamasının incelenmesine ilişkin 2 önemli rapor mevcuttur.

Bunlardan birincisi 12/07/2017 tarihli ByLock Uygulaması Veritabanının incelendiği Bilirkişi Raporu, ikincisi ise Milli İstihbarat Teşkilatı (MİT) tarafından hazırlandığı bilinen ByLock Uygulaması Teknik Raporudur.

ByLock Uygulama Sunucusu Veritabanı Bilirkişi Raporu

Ankara Cumhuriyet Başsavcılığının 2016/104109 Soruşturma numaralı dosyası kapsamında 27/09/2016 tarihli görevlendirme ile 12/07/2017 tarihli Bilirkişi Raporu yazılmıştır.

Bilirkişilerden ByLock Uygulaması hakkında bir takım bilgilerin ve ByLock Veritabanı dosyasına ait İmaj kopyasının bulunduğu sabit diskin incelenerek dosya içeriklerinin raporlanması talep edilmiştir.

Bu raporun konusu ByLock Uygulamasının ne olduğu değildir, bu raporun konusu önceki bölümlerde izah edilen bilgilere ek olarak ByLock Uygulaması Veritabanından elde edilen bilgiler ile bir ByLock kullanıcısının gerçek kimliğinin nasıl tespit edilebileceğidir. Bu nedenle, Bilirkişi Raporunun veritabanı incelemesi yapılan kısımlarından bahsedilmiştir.

ByLock Uygulaması Veritabanının 26/10/2016 tarihinde adli imajının alındığı ve HASH değerlerinin hesaplanmış olduğu Bilirkişi Raporunun 25' nci sayfasında (Şekil 3.) görülmüştür.

3.2.1. YAPILAN İNCELEME SONUCU

Sony Hard Drive 4691832C10F3 olarak etiketlenen diske ait Imaj verilerinin doğrulaması yapılmış, HASH değerlerinin doğrulandığı, Diskin içerisinde ibdata1 ve md5checksum.txt olarak iki adet dosyanın yer aldığı görülmüştür.

Ad	Değiştirme tarihi	Tür	Boyut
md5checksum.txt	26.10.2016 15:19	Metin Belgesi	1 KB
ibdata1	26.10.2016 15:13	Dosya	113.789.140 KB

Şekil 3.2.1.1 (Sony Hard Drive 4691832C10F3 seri nolu Harddisk İçeriği)

Dosya Adı	**ibdata1**
Mantıksal Boyutu	116.520.079.360
Son Erişim Tarihi	26/10/2016 15:18:49
Son Yazma Tarihi	26/10/2016 15:13:22
MD5	1173d7a09195cf0274ce24f0d69ede96
SHA1	e8cae63538d7a20ddfcb4c4ec49e552f4342e75c
Dosya Yolu	SONY_MARKA_bBW3DEK69121056_IBARELI_HARICI_HDD\media/e5a15e1f-844d-4b49-a747-c64ae055ead1\ibdata1

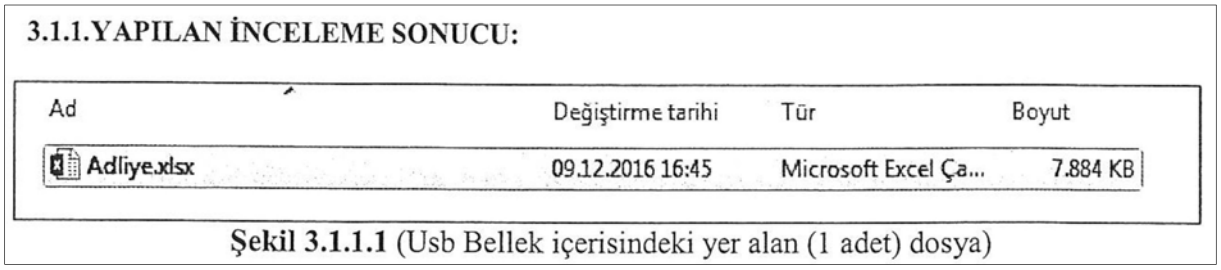
Şekil 3.2.1.2 (Sony Hard Drive 4691832C10F3 seri nolu Harddisk İçeriği)

Şekil 3. ByLock Uygulaması Veritabanı Adli İmaj Bilgileri (Bilirkişi Raporu s.25)

Şekil 3.' de görüleceği üzere, adli imajın 26/10/2016 tarihinde alınmış olması itibariyle, herhangi bir ByLock kullanıcısının gerçek kimliğinin bu tarihten önce tespit edilemez olduğu anlaşılmaktadır.

Hatta, Bilirkişi Rapor tarihinin 12/07/2017 olduğu göz önünde bulundurulacak olursa, bilirkişilerin raporlarını tamamlamadan ve teslim etmeden önce veritabanından elde ettikleri bilgileri ilgili kurumlar ile paylaşmaksızın 12/07/2017 tarihinden önce herhangi bir ByLock kullanıcısının gerçek kimliğinin bu tarihten önce tespit edilemez olduğu anlaşılmaktadır.

Bu durum sanıklar ve müdafiler açısından şüpheye değer olmakla birlikte, Bilirkişi Raporunun 24' ncü sayfasında (Şekil 4.) içerisinde Adliye.xlsx isimli bir dosyanın bulunduğu bir Flash Diskin de mevcut olduğu görülmüştür.


3.1.1.YAPILAN İNCELEME SONUCU:

Ad	Değiştirme tarihi	Tür	Boyut
Adliye.xlsx	09.12.2016 16:45	Microsoft Excel Ça...	7.884 KB

Şekil 3.1.1.1 (Usb Bellek içerisindeki yer alan (1 adet) dosya)

USB Belleğin alınan Imaj bilgilerinin doğrulaması yapılmış, hash değerlerinin Imaj kopyası ile doğrulandığı görülmüştür. USB Bellek içerisinde yer alan **"Adliye.xlsx"** isimli dosyanın şifrelenmiş olduğu görülmüş, dosya içeriğinin bylock listelerinin olduğu bildirildiğinden dolayı söz konusu dosya ile ilgili herhangi bir çalışma yapılmamıştır.

Şekil 4. ByLock Kullanıcılarının Bulunduğu Excel Dosyası (Bilirkişi Raporu s.24)

Şekil 4.' de görüleceği üzere bu Excel dosyasının son değiştirilme tarihi 09/12/2016 tarihidir. Devamında yer alan paragrafta ise "dosya içeriğinin bylock listelerinin olduğu bilindiğinden" ifadesi yer almaktadır.

Bilirkişilerin görevlendirilme tarihi 27/09/2016 ve Rapor tarihi 12/07/2017' dir. ByLock Uygulamasına ait Veritabanı imajı ise 26/10/2016 tarihlidir. İçerisinde ByLock listeleri bulunduğu ifade edilen Excel dosyası ise 09/12/2016 tarihlidir.

Bu tarihsel tutarsızlık, Bilirkişi Raporunun 26' ncı sayfasında yer alan ifadelerle daha tutarsız hale gelmektedir.

ibdata1 dosyası içerisindeki verilere erişim sağlanabilmesi ve bu verilerin tablolar halinde kurtarılması için **Linux Centos ve Debian** işletim sistemleri üzerinde "**Percona Data Recovery (percona-data-recovery-tool-for-innodb)**" https://www.percona.com/ ve "**TwinDB Data Recovery (undrop-for-innodb)**" araçları kullanılmıştır. https://recovery.twindb.com/

Şekil 5. Veritabanı İlk İncelemesinin Bilirkişiler Tarafından Yapıldığı (Bilirkişi Raporu s.26)

Şekil 5.' de görüleceği üzere, adli imaj üzerinde veritabanı ilk kez Bilirkişiler tarafından incelenmiştir.

Bu durumda, Bilirkişilere incelenmek üzere verilen imajlar arasında 09/12/2016 tarihli Excel dosyası içerisinde ByLock listelerinin bulunmasının ne şekilde gerçekleştiği sanık ve müdafiler açısından şüphelidir.

Bilirkişi Raporunun 26' ncı sayfasından 38' nci sayfasına kadar veritabanı yapısı ve tabloları açıklanmaktadır (Şekil 6.).

İlgili araçlar ile yapılan işlemler sonucunda **"ibdata1"** içeresinde toplam **(28)** adet tablonun bulunduğu **"appDb"** ve **"wordpress"** isimli iki ayrı veri tabanının yer aldığı, abbDb içerisinde toplam **(15)** adet tablonun bulunduğu, wordpress veri tabanında **(11)** adet tablonun yer aldığı görülmüştür. "**byLock**" veri tabanına ait "**appDb**" detaylı olarak incelenmiştir.

```
mysql> select * from SYS_TABLES;
+--------------------------------+----+------------+------+--------+---------+--------------+-------+
| NAME                           | ID | N_COLS     | TYPE | MIX_ID | MIX_LEN | CLUSTER_NAME | SPACE |
+--------------------------------+----+------------+------+--------+---------+--------------+-------+
| appDb/action                   | 13 |          7 |    1 |      0 |       0 |              |     0 |
| appDb/attachment               | 41 |          7 |    1 |      0 |       0 |              |     0 |
| appDb/call_history             | 15 |          7 |    1 |      0 |       0 |              |     0 |
| appDb/chat                     | 40 |          7 |    1 |      0 |       0 |              |     0 |
| appDb/client                   | 17 |          6 |    1 |      0 |       0 |              |     0 |
| appDb/exception                | 18 |          5 |    1 |      0 |       0 |              |     0 |
| appDb/file                     | 43 |          3 |    1 |      0 |       0 |              |     0 |
| appDb/file_transfer            | 42 |         10 |    1 |      0 |       0 |              |     0 |
| appDb/group_member             | 21 |          2 |    1 |      0 |       0 |              |     0 |
| appDb/log                      | 45 |         10 |    1 |      0 |       0 |              |     0 |
| appDb/mail                     | 44 |          9 |    1 |      0 |       0 |              |     0 |
| appDb/roster                   | 24 |          4 |    1 |      0 |       0 |              |     0 |
| appDb/setting                  | 25 |          2 |    1 |      0 |       0 |              |     0 |
| appDb/user                     | 26 |         10 |    1 |      0 |       0 |              |     0 |
| appDb/user_group               | 27 |          3 |    1 |      0 |       0 |              |     0 |
```

Şekil 6. ByLock Uygulaması Veritabanında Yer Alan Tablolar (Bilirkişi Raporu s.26)

Veritabanı içerisinde kullanıcıların birbirleri ile etkileşimlerinden bağımsız olarak 3 önemli tablo bulunmaktadır. Bunlar Actions, User ve Log isimli tablolardır.

Action isimli tablo içerisinde ByLock kullanıcılarının uygulama içerisindeki gerçekleştirilebilir kullanıcı eylemleri tanımlanmıştır (Şekil 7.).

a) **Action Tablosu**

```
+------------+-------------+------+-----+---------+-------+
| Field      | Type        | Null | Key | Default | Extra |
+------------+-------------+------+-----+---------+-------+
| id         | int(11)     | NO   | PRI | NULL    |       |
| name       | varchar(64) | NO   |     | NULL    |       |
| parameter1 | varchar(64) | NO   |     | NULL    |       |
| parameter2 | varchar(64) | NO   |     | NULL    |       |
| parameter3 | varchar(64) | NO   |     | NULL    |       |
| parameter4 | varchar(64) | NO   |     | NULL    |       |
| parameter5 | varchar(64) | NO   |     | NULL    |       |
+------------+-------------+------+-----+---------+-------+
```

Şekil 3.2.1.1.3 (Action tablo yapısı)

Şekil 7. Action Tablosu Veri Yapısı (Bilirkişi Raporu s.27)

User isimli tabloda, kullanıcıların, kullanıcı hesaplarını oluştururken belirledikleri bilgiler yer almaktadır (Şekil 8.).

n) user Tablosu

```
ysql> mysql> desc user;
+-----------------+--------------+------+-----+---------------------+-----------------------------+
| Field           | Type         | Null | Key | Default             | Extra                       |
+-----------------+--------------+------+-----+---------------------+-----------------------------+
| id              | int(11)      | NO   | PRI | NULL                |                             |
| username        | varchar(32)  | NO   |     | NULL                |                             |
| psw             | varchar(32)  | NO   |     | NULL                |                             |
| admin           | int(11)      | NO   |     | NULL                |                             |
| publicMessage   | varchar(64)  | YES  |     | NULL                |                             |
| privateExponent | varchar(512) | YES  |     | NULL                |                             |
| modulus         | varchar(512) | YES  |     | NULL                |                             |
| name            | varchar(32)  | YES  |     | NULL                |                             |
| creationTime    | timestamp    | NO   |     | CURRENT_TIMESTAMP   | on update CURRENT_TIMESTAMP |
| lastOnlineTime  | timestamp    | NO   |     | 0000-00-00 00:00:00 |                             |
+-----------------+--------------+------+-----+---------------------+-----------------------------+
0 rows in set (0,00 sec)
```

Şekil 3.2.1.1.26 (user tablo yapısı)

Şekil 8. User Tablosu Veri Yapısı (Bilirkişi Raporu s.37)

Log isimli tabloda ise hangi kullanıcının hangi eylemi hangi diğer kullanıcı ile etkileşim halinde gerçekleştirdiği günlük kayıtları yer almaktadır (Şekil 9.).

j) "log" Tablosu

```
ysql> desc log;
+------------+--------------+------+-----+---------------------+-----------------------------+
| Field      | Type         | Null | Key | Default             | Extra                       |
+------------+--------------+------+-----+---------------------+-----------------------------+
| id         | int(11)      | NO   | PRI | NULL                |                             |
| userId     | int(11)      | NO   |     | NULL                |                             |
| actionId   | int(11)      | NO   |     | NULL                |                             |
| sessionId  | varchar(128) | NO   |     | NULL                |                             |
| eventTime  | timestamp    | NO   |     | CURRENT_TIMESTAMP   | on update CURRENT_TIMESTAMP |
| parameter1 | varchar(64)  | YES  |     | NULL                |                             |
| parameter2 | varchar(64)  | YES  |     | NULL                |                             |
| parameter3 | varchar(64)  | YES  |     | NULL                |                             |
| parameter4 | varchar(64)  | YES  |     | NULL                |                             |
| parameter5 | varchar(64)  | YES  |     | NULL                |                             |
+------------+--------------+------+-----+---------------------+-----------------------------+
0 rows in set (0,24 sec)
```

Şekil 3.2.1.1.16 ("log" tablo yapısı)

Şekil 9. Log Tablosu Veri Yapısı (Bilirkişi Raporu s.32)

Bu tabloların kullanıcıların tespitinde kullanılabilirliğine tekrar değinilecektir.

Hem ByLock Uygulaması Veritabanının incelendiği Veritabanında hem de MIT ByLock Uygulaması Teknik Raporunda sanık ve müdafiler açısından şüpheli olarak değerlendirilebilecek bir husus daha vardır.

Bilirkişi Raporunun 35 ve 36' ncı sayfasında ByLock Uygulaması tarafından kullanılan 46.166.160.137 IP adresinin "bylock.net" alan adı tarafından 14/08/2014 ile 02/04/2016 tarihleri arasında kullanıldı gerekli açık kaynaklar kullanılarak tespit edildiği ifade edilmiştir. Yine Bilirkişi Raporunun 10 ve 11' nci sayfalarında ise bylockapp.wordpress.com blog adresinden 25/08/2014 ve 15/10/2014 tarihlerinde 2 adet açıklama metninin yayınlandığının ifade edildiği görülmüştür.

Bu konudaki bilgiler MIT ByLock Uygulaması Teknik Raporunun 13 ve 25' nci sayfalarında yer almaktadır.

ByLock Uygulamasının kendisine ait bir alan adı mevcut ve yayındayken geliştiricinin ücretsiz ve anonim bir wordpress blog hesabından uygulama ile ilgili kritik bir güncelleme bilgisini

paylaşmış olması hayatın olağan akışına uygun olarak değerlendirilemez. Ayrıca, WordPress isimli içerik yönetim yazılımının içerisinde bulunulan tarihten daha eski tarihli içerikler oluşturulmasına izin veriyor olması da sanık ve müdafiler açısından şüpheyle yaklaşılması makul bir başka noktadır.

MIT ByLock Uygulaması Teknik Raporu

Her ne kadar bu rapor tarihsiz olsa da içerisinde ByLock Uygulaması Veritabanı incelemesinin yapıldığı Bilirkişi Raporunda yer alan veritabanı yapısı ve tablolara ait bilgiler içermesi nedeni ile Bilirkişi Raporundan sonra hazırlandığı veya ByLock Uygulaması Veritabanı imajının tekrar bir incelemesinin yapılmış olabilmesi mümkündür.

Rapor tarihine ilişkin kesin bir tespit yapılamamasının sebebi, MIT Raporunda yer alan bir takım bilgilerin Bilirkişi Raporunda yer almayan bilgiler olmasıdır.

MIT Raporunda da Bilirkişi Raporunda olduğu gibi veritabanı yapısının ve tablolarının detaylı şekilde açıklandığı görülmüştür.

Bilirkişi Raporunda bahsedilen ve kullanıcıların uygulama içi eylemlerinin tanımlandığı Action tablosu içerisinde yer alan verilerin MIT Raporunun 28’ nci sayfasında açık olarak sunulduğu görülmüştür (Şekil 10.).

3.6.2.1 *"action" tablosu:*

```
MariaDB [appDb]> select * from action;
+----+-----------------------------------+-----------------+-----------------+-----------------+-----------------+
| id | name                              | parameter1      | parameter2      | parameter3      | parameter4      |
+----+-----------------------------------+-----------------+-----------------+-----------------+-----------------+
|  1 | Add Friend                        | User Id         | Nickname        |                 |                 |
|  2 | Create User                       | User Id         | Name            | is Admin?       |                 |
|  3 | Register                          | IP              | Client Edition  |                 |                 |
|  4 | Change Password                   |                 |                 |                 |                 |
|  5 | Delete File                       | File Transfer Id |                |                 |                 |
|  6 | Receive File                      | File Id         |                 |                 |                 |
|  8 | Login                             | IP              | Client Edition  | Client Version  |                 |
|  9 | Logout                            |                 |                 |                 |                 |
| 10 | Receive Chat                      | User Id         |                 |                 |                 |
| 11 | Remove Friend                     | User Id         |                 |                 |                 |
| 12 | Read Mail                         | Mail Id         |                 |                 |                 |
| 13 | Send Chat                         | User Id         |                 |                 |                 |
| 14 | Send File                         | User Id         | File Id         | File Transfer Id |                |
| 16 | Make Call                         | Call Id         | User Id         |                 |                 |
| 17 | Answer Call                       | Call Id         |                 |                 |                 |
| 18 | Reject Call                       | Call Id         |                 |                 |                 |
| 19 | Cancel Call                       | Call Id         |                 |                 |                 |
| 20 | Close Call                        | Call Id         |                 |                 |                 |
| 21 | Session Expire                    |                 |                 |                 |                 |
| 22 | Unsuccessful Login Attempt        | Username        | IP              | Client Edition  | Client Version  |
| 23 | Reset Password                    | User Id         |                 |                 |                 |
| 24 | Delete User                       | User Id         |                 |                 |                 |
| 25 | Edit User                         | User Id         | Name            | is Admin?       | Password Changed |
| 26 | Register Captcha Error            | IP              | Client Edition  | Username        |                 |
| 27 | Upload File                       | File Id         |                 |                 |                 |
| 29 | Set New Password                  |                 |                 |                 |                 |
| 30 | Session Close Due To Password Reset |               |                 |                 |                 |
| 31 | Session Close Due To User Deletion |               |                 |                 |                 |
| 32 | Send Mail                         | User Id         | Mail Id         |                 |                 |
| 33 | Delete Mail                       | Mail Id         |                 |                 |                 |
| 34 | Download Version                  | Version Id      |                 |                 |                 |
| 35 | Upload Version                    | Version Id      |                 |                 |                 |
+----+-----------------------------------+-----------------+-----------------+-----------------+-----------------+
32 rows in set (0.00 sec)
```

Şekil 3.6.2.2: Action tablosunun alan adları ve özellikleri

Şekil 10. Action Tablosu Kullanıcı Eylemleri ve Eylem Kayıt Bilgileri (MIT Raporu s.28)

Action tablosunda tanımlanan kullanıcı eylemlerinden 3 Action ID koduna sahip Register (İlk defa kayıt) ve 8 Action ID koduna sahip Login (Uygulamaya giriş) işlemlerinin parametre1 alanında kullanıcıya ait IP adresini ile kaydedilmek üzere tanımlandığı görülmüştür.

Bu eylemlerin kayıtlarının tutulduğu tablo ise Log isimli tablodur. Bu tablo, Action tablosunda tanımlanan kullanıcı eylemleri ile eylemleri gerçekleştiren kullanıcıların ilişkilendirilerek kaydedildiği bir günlük tablosudur.

Action tablosu ile birlikte MIT Raporunun 42' nci sayfasında detayları yer alan Log tablosu incelendiğinde, id, UserId, sessionId, eventTime, parameter1, parameter2, parameter3, parameter4, parameter5 sütunlarında oluştuğu görülmektedir (Şekil 11.).

Şekil 11: log tablosuna ait örnek kayıtlar

Şekil 11. Log Tablo Yapısı ve Kayıt Örnekleri

Action ve Log Tabloları birlikte incelendiğinde, herhangi bir kullanıcının (User Id) uygulamaya kayıt olurken (Register) ve uygulamaya giriş yaparken (Login) kullandığı IP adresleri ve işlemin ne zaman gerçekleştiği bilinmektedir.

User isimli tablo ByLock Uygulama Sunucusu Veritabanı inceleme Bilirkişi Raporu ile MIT ByLock Uygulaması Teknik Raporu arasında küçük fakat önemli bir farka sahiptir.

n) user Tablosu

```
ysql> mysql> desc user;
+-----------------+-------------+------+-----+---------------------+-----------------------------+
| Field           | Type        | Null | Key | Default             | Extra                       |
+-----------------+-------------+------+-----+---------------------+-----------------------------+
| id              | int(11)     | NO   | PRI | NULL                |                             |
| username        | varchar(32) | NO   |     | NULL                |                             |
| psw             | varchar(32) | NO   |     | NULL                |                             |
| admin           | int(11)     | NO   |     | NULL                |                             |
| publicMessage   | varchar(64) | YES  |     | NULL                |                             |
| privateExponent | varchar(512)| YES  |     | NULL                |                             |
| modulus         | varchar(512)| YES  |     | NULL                |                             |
| name            | varchar(32) | YES  |     | NULL                |                             |
| creationTime    | timestamp   | NO   |     | CURRENT_TIMESTAMP   | on update CURRENT_TIMESTAMP |
| lastOnlineTime  | timestamp   | NO   |     | 0000-00-00 00:00:00 |                             |
+-----------------+-------------+------+-----+---------------------+-----------------------------+
0 rows in set (0.00 sec)
```

Şekil 3.2.1.1.26 (user tablo yapısı **)**

"user" tablosunda **"id"** bylock içerisinde yer alan "UserId" no, kullanıcı adı (username), psw (md5 kriptolu olarak şifre), kullanıcı durumu admin veya user olarak, (program içerisinde 3 adet admin kullanıcısının yer aldığı diğer kullanıcıların standart user olarak görüldüğü), oluşturulma tarihi, son online tarihi gibi bilgilerin bulunduğu görülmüştür.

Yapılan inceleme sonucunda toplam **246.206** adet kayıt bilgisine ulaşılmıştır.

Şekil 12. ByLock Uygulaması Sunucu Veritabanı inceleme Bilirkişi Raporunda User Tablosu (Bilirkişi Raporu s.37)

3.6.2.15 "user" tablosu:

```
MariaDB [appDb]> show columns in user;
+-----------------+-------------+------+-----+---------------------+-----------------------------+
| Field           | Type        | Null | Key | Default             | Extra                       |
+-----------------+-------------+------+-----+---------------------+-----------------------------+
| id              | int(11)     | NO   | PRI | NULL                |                             |
| username        | varchar(32) | NO   |     | NULL                |                             |
| plain           | varchar(32) | NO   | MUL | NULL                |                             |
| admin           | int(11)     | NO   |     | NULL                |                             |
| publicMessage   | varchar(64) | YES  |     | NULL                |                             |
| privateExponent | varchar(512)| YES  |     | NULL                |                             |
| modulus         | varchar(512)| YES  |     | NULL                |                             |
| name            | varchar(32) | YES  |     | NULL                |                             |
| creationTime    | timestamp   | NO   |     | CURRENT_TIMESTAMP   | on update CURRENT_TIMESTAMP |
| lastOnlineTime  | timestamp   | NO   |     | 0000-00-00 00:00:00 |                             |
+-----------------+-------------+------+-----+---------------------+-----------------------------+
12 rows in set (0.00 sec)
```

Şekil 15: user tablosunun alan adları ve özellikleri

"user" tablosunda, Kullanıcı Adı, kullanıcı şifresi (**md5 kriptografik özeti**), **RSA Sertifika bileşenleri,** kullanıcının oluşturulma tarihi ve en son giriş yapma tarihi

gibi bilgilerin tutulduğu görülmüştür. Bu tabloda aynı zamanda kullanıcının kendine özel **RSA kriptografik anahtar setinin gizli anahtarı (privateExponent)** mevcuttur. **privateExponent** bileşeninin tabloda kriptolu bir şekilde saklandığı görülmüştür.

"user" tablosunda toplam 215.092 kayıt bulunmakta olup, uygulama kullanıcılarının kullandıkları parolalar kriptolu bir şekilde saklanmıştır. Gerçekleştirilen çalışmalar neticesinde 184.298 şahsa ait parola bilgisi çözümlenmiştir. User tablosunda yer alıp deşifre edilen verilere ilişkin örneklere aşağıda verilmiştir: ("**username**" bilgisi kullanıcı adına/koduna, "**plain**" bilgisi ise yürütülen çalışmalar neticesinde çözümlenmiş kullanıcı şifresine işaret etmektedir.)

Şekil 13. MIT ByLock Uygulaması Teknik Raporu User Tablosu (MIT Raporu s.49)

Bilirkişi Raporunda User tablosunda yer alan kullanıcı şifrelerinin, şifrelenmiş halde psw isimli alanda kayıtlı olduğu ifade edilirken, MİT Raporunda şifrelenmiş haldeki kullanıcı şifrelerinin çözümlenerek plain isimli alana kaydedildiği ifade edilmiştir.

Bu noktada işlemsel olarak bir tutarsızlık olmamakla birlikte, Şekil 12. ve Şekil 13.' de yer alan User tabloları karşılaştırıldığında görüleceği üzere, psw alanının yerini plain alanı almış, yani kullanıcı şifrelerinin orijinal kayıtları silinmiştir.

Bu durumun sakıncası, sanık ve müdafilerin kendi plain şifreleri ile psw şifrelerini karşılaştırarak, şifre çözme işlemini tekrar yapmalarının yani psw' den plain' e dönüştürme işlemlerinin tekrarlanamayacak olmasıdır.

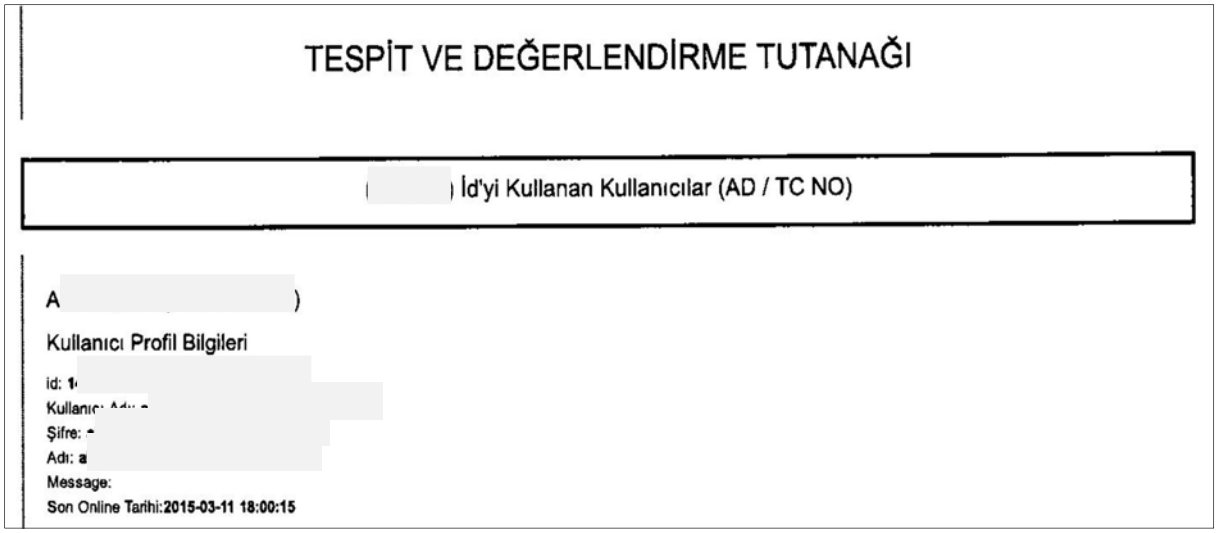
ByLock Uygulaması kullanıcılarının tespiti ile ilgili doğrudan ilgili olmayan bu noktaya yalnızca bilgilendirme amaçlı değinilmiştir.

User tablosu ile ilgili yine sanık ve müdafiler açısından dikkate alınması gereken bir başka nokta, User tablosunda yer alan creationTime ve lastOnlineTime alanları ile ilgilidir.

ByLock kullanıcılarına ait Tespit ve Değerlendirme Tutanağı ismi verilen evraklar düzenlenmekte ve mahkemelere sunulmaktadır. Bu evrakların ilk sayfasında, ilgili User ID' ye sahip kullanıcının User tablosunda yer alan bilgileri yer almaktadır (Şekil 13.).

Ancak bu bilgilerden creationTime bilgisine yer verilmemektedir.

Bu eksiklik, yine MİT Raporunun 52' nci sayfasında yer alan istatistik tablosu ile birlikte değerlendirildiğinde, "ByLock Uygulamasında En az 1 Kez Mesaj Atmış ve/veya Almış Şahıs Sayısının 60.473, Uygulamayı Sadece Sesli İletişim İçin Kullanan Şahıs Sayısının 46.799 olması ile, MIT Raporuna göre User tablosunda yer alan kullanıcı sayısı olan 215.092 ve Bilirkişi Raporunda yine User tablosunda yer alan kullanıcı sayısı olan 246.206 karşılaştırıldığında, çok büyük miktardaki kullanıcının uygulamaya yalnızca kayıt olmuş ancak kullanmamış olduğu sonucuna ulaşılabilecektir.


TESPİT VE DEĞERLENDİRME TUTANAĞI

İd'yi Kullanan Kullanıcılar (AD / TC NO)

A)

Kullanıcı Profil Bilgileri

id:

Şifre:

Adı:

Message:

Son Online Tarihi:2015-03-11 18:00:15

Şekil 13. ByLock Kullanıcılarına ait Tespit ve Değerlendirme Tutanağında Yer Alan ve User Tablosundan Alınan Bilgiler

Ayrıca, Bilirkişi Raporunda ve MIT Raporunda yer alan User tablosunda yer alan kullanıcı sayılarındaki farklılık büyük bir çelişki olarak görülmeli, esas referans alınması gereken verilerin Bilirkişi Raporunda mevcut veriler olması gerekmektedir.

ByLock Uygulaması Sunucu Veritabanı Kayıtlarının Gerçek Kullanıcı Tespitinde Kullanılabilirliği

Önceki bölümlerde ISP' ler tarafından aboneleri hakkında günlük kaydı tutulan CGNAT kayıtlarından, ilgili RFC dokümanları ve akademik literatür çerçevesinde bahsedilmiştir.

Birinci Bölümde, RFC 6269 ve RFC 6888 ISP tarafından her bir abone için tarih, saat, dahili IP (Özel IP), dahili Port numarası (Özel Port), harici IP adresi (Genel IP), harici Port numarasını bilgileri ISP' ler tarafından kaydedilmesine ilişkin bilgiler yer almaktaydı.

Birinci Bölümde ayrıca, hedef sunucu üzerinde birden fazla uygulamanın bulunması durumunda, Europol Raporunda da belirtildiği şekilde, CGNAT kayıtlarının doğru ISP abonesini tespit için yeterli olmayacağı, ancak sunucu tarafında, kullanıcına ait erişim kayıtlarının mevcut olması durumunda, CGNAT kayıtları ile karşılaştırılarak abonenin Hedef IP üzerindeki belirli bir uygulamayı kesin bir tespitte bulunulabileceği ifade edilmişti.

İkinci Bölümde ise, Türkiye de BTK tarafından sağlanan CGNAT kayıtlarının da RFC 6269 ve RFC 6888 ile uyumlu oldukları, ayrıca 5651 Sayılı Kanun ve ilgili yönetmelik çerçevesinde, ISP' ler tarafından abonelere ait belirli bir sunucuya erişim/erişim talebi kayıtlarının da mevzuata uygun olarak Hedef IP ve Hedef Port numarasının da kaydedilmesine ilişkin bilgiler yer almaktaydı.

Bu bölümde ise, ByLock Uygulaması Sunucu Veritabanı kayıtlarının mevcut olması, bu veritabanı içerisinde 3 Action ID numarasına sahip uygulamaya kayıt (register) ve 8 Action ID numarasına sahip uygulamaya giriş (login) eylemlerinin kullanıcının kaynak IP adresi (ISP tarafından kendisine sağlanan) ile birlikte kaydedilmesi, bu verilerin, abonelerin CGNAT kayıtları içerisinde araştırılarak gerçek kullanıcıları tespit edebilmeyi sağlayacak yeterli veri oldukları görülmüştür.

Özet

ByLock Uygulama Sunucusu Veritabanı Bilirkişi Raporunda ve MİT ByLock Uygulaması Teknik Raporunda, ByLock Uygulaması Veritabanı Yapısı incelenmiştir.

Veritabanı içerisinde yer alan, uygulama kullanıcılarının uygulama içi eylemlerinin tanımlandığı Actions tablosu, kullanıcı eylemlerinin kayıtlı olduğu Log tablosu ve kullanıcı bilgilerinin kayıtlı olduğu User tablosu bulunmaktadır.

Uygulamaya ilk kayıt (register) ve uygulamaya giriş (login) eylemleri, kullanıcıların IP adresleri ile birlikte Log tablosuna kaydedilmektedir.

Birinci ve ikinci bölümlerde izah edilen RFC 6269 ve RFC 6888 ile uyumlu ISP kayıtları, RFC 6888 ve yerel mevzuata uygun hedef sunucu kayıtları ile bu bölümde izah edilen ByLock Veritabanı kayıtlarından Actions, Log ve User tablolarında yer alan kayıtların birlikte incelenmesi yoluyla gerçek kullanıcıların tespit edilebilir olduğu anlaşılmıştır.

Ayrıca, Bilirkişi Raporu ve MİT Raporunda yer alan verilerde sanık ve müdafileri tarafından şüphe ile yaklaşılması makul olan bir takım tutarsızlıklar olduğu görülmüştür:

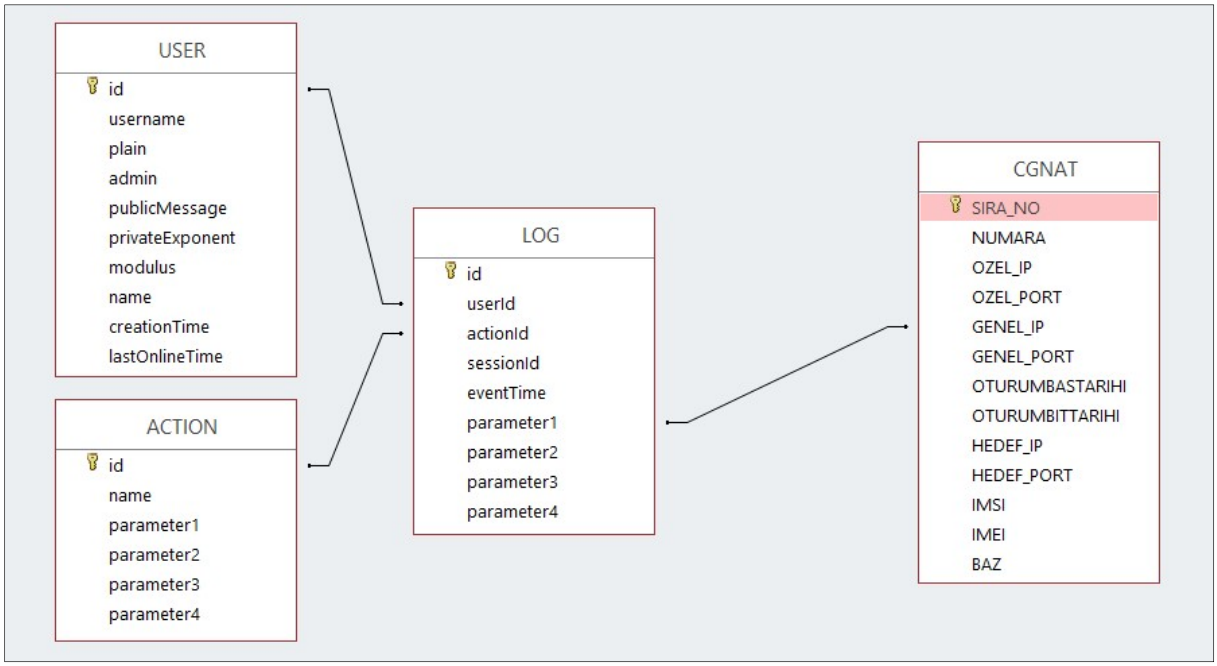
- Bilirkişi Raporu içerisinde yer alan adliye.xlsx dosyasının bilirkişi görevlendirme tarihleri ile uyumsuzluk göstermesi.
- 46.166.160.137 IP adresinin “bylock.net” alan adı tarafından 14/08/2014 ile 02/04/2016 tarihleri arasında yayında ile uygulamayla ilgili bir takım açıklamaların 25/08/2014 ve 15/10/2014 tarihlerinde bir WordPress bloğundan yayınlanmış olması.
- User tablosunda yer alan lastOnlineTime bilgisinin Tespit ve Değerlendirme Tutanaklarında yer almasına karşın kullanıcı hesabının oluşturulma tarihi olan lastOnlineTime yer almaması nedeni ile uygulamayı kurmuş fakat kullanmamış kişilerin belirlenememesi.
- Bilirkişi Raporunda User tablosunda 246.206, MİT Raporunda ise aynı tabloda 215.206 kullanıcı kaydının olması.
- Bilirkişi Raporunda User tablosunda kullanıcıların şifreleri, şifreli hali ile psw alanında kayıtlı iken MİT Raporunda bu şifrelerin plain isimli alan altına çözümlenmiş olarak kayıtlı olması nedeni ile kullanıcılara ait şifrelerin tekrar çözümlenerek teyit edilebilir olmaması.

4. Gerçek ByLock Kullanıcılarının Tespiti

ByLock Uygulama Sunucusu Veritabanı Bilirkişi Raporunda ve MİT ByLock Uygulaması Teknik Raporunda, ByLock Uygulaması veritabanı yapısı incelenmiş ve yeniden oluşturulmuştur.

Bir kullanıcı tespiti için, User tablosundaki belirli bir kullanıcıya (User ID) ait Action tablosunda tanımlanmış olan 3 Action ID numarasına sahip uygulamaya ilk kayıt (register) veya 8 Action ID numarasına sahip uygulamaya giriş (login) eylemlerinden birisinin Log tablosunda parameter1 alanında yer alan IP adresinin zaman bilgisi ile birlikte CGNAT tablosunda Genel IP alanında da tespit edilmiş olması gerekmektedir (Şekil 14.).

Bu karşılaştırmada zaman bilgisi içerisinde yer alan günün aynı olması gerekse de saat bilgisinin ISP ve veritabanı kaydı arasındaki gecikmeler nedeni ile aynı olmayabileceği göz ardı edilmemelidir.



Şekil 14. ByLock Uygulaması Veritabanı ve CGNAT Kayıtları Aracılığı İle Gerçek Kullanıcı Tespiti

Özet

ISP kayıtları ve ByLock Uygulaması Sunucu Veritabanı kayıtlarının, veritabanı Log tablosunda yer alan belirli bir kullanıcıya ait (User ID' si ile belirlenebilir), 3 ve 8 ID numaralı uygulamaya ilk kayıt (register) ve uygulamaya giriş (login) kayıtlarında yer alan IP adresinin, herhangi bir ISP abonesi için zamansal olarak uyumlu şekilde CGNAT kayıtları içerisinde tespiti gereklidir.

Bu yöntem dışında yapılacak tüm tespitler, farklı ölçülerde tespiti yapanların kanaatinden ibaret olacaktır. Bu kanaatin ByLock Uygulaması veritabanının özellikle kullanıcı adı ve şifre bilgilerine bağlı benzerliklere dayalı olması durumunda bu verilerin sanık ve müdafiler tarafından tekrar edilebilir olmadığı göz ardı edilmemelidir.

Yazarlar Hakkında

Berker KILIÇ, Adli Bilişim Uzmanı, Veri Bilimci

Adli Bilişim ve Veri Bilimi alanlarında iki yüksek lisans sahibidir.

Taraf bilirkişiliği yapmaktadır. ByLock davaları konusunda yüzlerce rapor yazmıştır.

Samsun Bilirkişilik Bölge Kuruluna kayıtlı olarak resmi bilirkişilik yapmaktadır.

Adli Bilişim ve Veri Bilimi alanlarında akademik çalışmaları mevcuttur.

berker.kilic@gmail.com , www.adlibilisimci.com

https://twitter.com/berker_kilic

Elif Eylem KINACILAR, Avukat, Adli Bilirkişi

Avukat olarak ceza hukuku, bilişim hukuku, insan hakları hukuku, idare hukuku alanlarında çalışmaktadır.

Mahkemeler nezdinde resmi bilirkişilik yapmaktadır.

Özel Hukuk alanında yüksek lisans eğitimine devam etmektedir.

eylem34@hotmail.com, www.dedeoglu.av.tr

https://twitter.com/AHargreavis

Mesut Can TARIM, Avukat, Adli Bilirkişi

Avukat olarak ceza hukuku, bilişim hukuku, insan hakları hukuku, idare hukuku alanlarında çalışmaktadır.

Ankara Bilirkişilik Bölge Kuruluna kayıtlı olarak resmi bilirkişilik yapmaktadır.

Adli Bilişim alanında yüksek lisans eğitimine devam etmektedir.

iletisim@mcthukuk.com, www.mcthukuk.com

https://twitter.com/mcthukuk

Rapor aslına https://www.adlibilisimci.com/ortak-raporlar/ adresinden ulaşılabilir.