Bilgisayar Korsanları Bugüne Kadar ki En Cüretkâr Cep Telefonu Ağına Sızma Olayını Nasıl Gerçekleştirdiler?

ATİNA OLAYI*

Vassilis Prevelakis, Diomidis Spinellis

38 yaşındaki Costas Tsalikidis isimli Yunanistanlı elektrik mühendisi 9 Mart 2005'te Atina'daki çatı katı dairesinde asılı olarak bulundu, olay bir intihar görünümündeydi. Bu haber, Yunanistan'ı aylar boyunca meşgul edecek bir skandala ait ilk haberdi. Ertesi gün, Yunanistan Başbakanı'na, Atina Valisi ve içlerinde ABD Büyükelçiliği çalışanı bir kişinin de yer aldığı yüksek mevki sahibi 100 kişi gibi, kendisinin de telefonunun dinlendiği bilgisi verildi.

Dinleme olayına maruz kalan kurbanlar genellikle Vodafone Yunanistan olarak da bilinen, ülkenin en büyük cep telefonu servis sağlayıcısı olan Atina merkezli Vodafone-Panafon'un müşterileriydi; Tsalikidis ise şirketin ağ planlamasından sorumlu olan kişiydi ve açık bir bağlantı bulunmaktaydı. Bu dinlemelerdeki insanların listesi ve pozisyonları dikkate alındığında olayın ortaya çıkmasıyla birlikte hassas, politik ve diplomatik tartışmaların, büyük meblağlarda iş görüşmelerinin ve hatta sıklıkla duyulabilecek olan evlilik tartışmalarının bile kayıt edilmiş olduğu düşünüldü.

Tsalikidis'in ölümünden önce bile, araştırmacılar Vodafone Yunanistan telefon ağına bilinmeyen taraflarca kötü niyetli yazılımlar yüklendiğini buldular. İnanılmaz derecede bilgi sahibi bazı insanlar ya ağa dışarıdan sızmıştı, ya da bir ajan veya köstebek yardımıyla içeriden çökertmek istemişti. Her iki durumda da araştırmacıların sonradan keşfettiği, telefon sisteminin kalbindeki yazılım, şimdiye kadar ender görülmüş bir şekilde bir ustalık ve incelikle yeniden programlanmıştı.

Büyük bir cep telefonu servis sağlayıcısının başına gelen bu en garip ve utandırıcı skandal olan Atina Olayı üzerinde çalışmak, şebekelerin bilgisayar korsanları ve köstebeklere karşı ne yapabilecekleri ve yapmaları gerektiğine ışık tutmaktadır.

Bu durum ayrıca en anlaşılması zor siber suçlara göz atmak için de nadir bir imkan yaratmıştır. Büyük şebekelere girilmesi çok ender olarak görülmektedir. Bunu yapmak ne kadar zorsa, yapanları araştırmak da bir o kadar zordur.

Büyük kriminal sızma olayları arasında bile Atina Olayı devlet sırlarını içermesi ve bireyleri hedef alması ile öne çıkmaktadır. Bu çapta bir olay daha önce su yüzüne çıkartılmamıştır. Devlet sırlarını tehlikeye atan en şöhretli sızma girişimi, 1986 yılında gerçekleşmiştir. O dönemde Alman bir programcı sızma girişiminde bulunarak ABD Stratejik Savunma Girişimi'nin (Yıldız Savaşları) sırlarını Sovyet KGB'sine satmıştır. Sızma girişiminde bulunan Alman programcının izini ise başarılı bir biçimde süren kurnaz şebeke yöneticisi bunu "Guguk Kuşu Yumurtası" olarak adlandırılmıştır.

Guguk Kuşu Yumurtası'ndan farklı olarak Atina Olayı'nda belirli, yüksek rütbeli devlet ve ordu görevlileri hedef alınmıştı. Ortaya çıkan sızma yönteminin görüşmelerin kaydedilmesini oldukça kolaylaştırması sebebi ile kayıt altına alınmış oldukları tahmin edilmektedir. Fakat kimse kayıtlara ulaşamamıştır. Faillerin kaç görüşmeyi kaydettiği veya dinlediği bilinmemektedir. Aktivitenin kapsamı büyük oranda bilinmiyor olsa da, şimdiye kadar ki hiçbir bilgisayar suçunda devlet sırrı sayılan bu kadar çok bilginin kayıt altına alınmış olma ihtimalinin bulunmadığı belirtilmektedir.

Her ne kadar bu durum cep telefonlarını hedeflese de, çevrilen bu dolap kablosuz ağ yapısına bağımlı değildir. Temel olarak korsanlar bir telefon şebekesine girmiş ve şebekenin dahili telefon dinleme özelliklerini kendi amaçları için kullanmışlardır. Bu başka bir telefon şebekesini de hedef almış olabilirdi. Yine de, Vodafone Yunanistan'ın sisteminin suçun işlenebilmesine olanak sağlayan çok önemli eksiklikleri vardır.

Hala bu suçu kimin işlediğini bilinmemektedir. Bunun önemli bir sebebi, Birleşik Krallık temelli ve dünyadaki en büyük kablosuz iletişim servis sağlayıcılarından biri sayılan Vodafone Grubu'nun önemli kayıt dosyalarının saklanması işini ellerine yüzlerine bulaştırmalarıdır. Şirket ayrıca kaçak yazılımın çalışmasına izin vermek yerine refleks olarak yazılımı sistemden çıkarmış ve faillere sızma girişimlerinin fark edildiğinin sinyalini vererek kaçmaları için şans yaratmıştır. 2006'nın Aralık ayında şirket, 76 milyon ceza ödemiştir.

* IEEE Spectrum Dergisi'nin Temmuz 2007 Sayısı'ndan çevrilmiştir.

Olayı anlayabilmek için Yunanistan Parlamentosu'na yapılan bilgi edinme özgürlüğü başvurusu aracılığı ile olayı araştıran Yunan Parlamento Komitesi tarafından alınan yüzlerce yeminli ifade incelenmiştir. Ayrıca vaka ile ilişkili bağımsız uzman ve kaynakların topluma açık bilgileri ve görüşmelerini içeren yüzlerce sayfalık doküman ve diğer kayıtlar da incelenmiştir. Sebeplerinin ne olduğu belirgin olmasa da teknik detaylara bakılarak şeytanca zeki ve karmaşık bir bilgisayar sızması tablosu ortaya çıkmıştır.

Cep telefonlarının dinlenmesi olayının başlangıç tarihi Atina'daki Olimpiyat Oyunları'nın olduğu 2004 Ağustos'una denk gelmektedir. Vodafone'un telefon santrallarından birinin, başka bir operatöre ait metin mesajlarının iletilmediğine dair hata mesajları ürettiği, 24 Ocak 2005 tarihine kadar ortaya çıkmamıştır. Bu santralla, iki telefon hattını birbirine bağlayarak, telefon görüşmesini tamamlayan bir telefon ağı bilgisayarla kontrol edilmiştir. Çok nadir ortaya çıkan fakat o anda zararsız görünen bu hataların anlaşılabilmesi için Vodafone santralların üreticisi olan İsveçli telekomünikasyon şirketi Ericsson ile iletişime geçmiştir.

Şimdi biliyoruz ki illegal olarak yerleştirilen yazılım, Vodafone Yunanistan'ın toplam 4 santralında bulunmuştur. Yazılım, dinlenen telefonlar için dijital seslerin aktarıldığı paralel akışlar oluşturmuştur. İlk akış birbirini arayan iki kişi arasında gerçekleştirilmiştir. Diğer akış ise bir öncekinin tam bir kopyası olarak, diğer cep telefonlarına yönlendirilerek ve büyük ihtimalle kayıt edilmiştir. Bu yazılım ayrıca aramalarla ilgili yer ve diğer bilgileri de gölge telefonlara otomatik metin mesajları olarak yönlendirmiştir.

İlk mesajlaşma hatasından 5 hafta sonra, 4 Mart 2005 tarihinde Ericsson, Vodafone'u merkez ofislerinden iki tanesine izinsiz yazılım kurulması dolayısıyla uyarmıştır. Üç gün sonra Vodafone teknikerleri yabancı kodu izole etmişlerdir. Ertesi gün 8 Mart'ta, Vodafone Yunanistan Genel Müdürü Giorgos Koronias, teknikerlere yazılımı kaldırmaları talimatını vermiştir.

Bu andan itibaren olaylar ölümcül bir hal almıştır. 9 Mart'ta, 3 ay içerisinde evlenmeyi planlayan Tsalikidis, apartmanında asılmış olarak bulunmuştur. Kimse intiharının vaka ile ilişkili olup olmadığını bilmemekle birlikte birçok gözlemci bu yönde yorumda bulunmuştur.

Tsalikidis'in cesedi bulunduktan sonraki gün, Koronias, Yunan Başbakanı'nın ofis yöneticisi Yiannis Angelou ve Kamu Düzeni Bakanı Giorgos Voulgarakis ile buluşmuştur. Koronias, kaçak yazılımın Vodafone'un kanuni hat dinleme mekanizmasını kullanarak dijital santrallar üzerinden 100 telefonu dinlediğini anlatarak, dinlenen numaraların listesini vermiştir. Başbakan ve eşi de dahil olmak üzere numaraların savunma, dışişleri ve adalet bakanlarına, Atina Valisi'ne, Avrupa Birliği Yunanistan Komiseri'ne ait oldukları ortaya çıkmıştır. Diğer numaralar sivil toplum kuruluşlarına, barış aktivistlerine ve küreselleşme karşıtı gruplara, Ulusal Savunma, Kamu Düzeni, Deniz Ticareti, Dışişleri bakanlıklarındaki üst düzey çalışanlara, Yeni Demokrasi Partisi'ne, Yunan Donanması generallerine ve Atina ABD Büyükelçiliği'ndeki Yunan asıllı bir çalışana ait olduğu saptanmıştır.

Telekulak olayının ortaya çıkmasını takip eden haftalarda, Yunan Hükümeti ve bağımsız otoriteler beş farklı soruşturma başlatarak şu sorulara yanıt aramışlardır: Dinleme operasyonundan kim sorumlu idi? Tsalikidis'in ölümü skandal ile ilişkili miydi? Failler bu cüretkar operasyonu nasıl gerçekleştirmişlerdi?

Yunanistan'ın üst düzey yetkililerinin görüşmelerinin gizlice nasıl dinlendiğini anlayabilmek için buna izin veren alt yapının nasıl olduğuna bakmak gerekmektedir.

Öncelikle sizin veya bir başbakanın telefon aramasının nasıl gerçekleştiğine bakmak gerekmektedir. Siz telefonunuzda bir numarayı çevirmeye başlamadan çok önce bile telefonunuz yakındaki hücresel baz istasyonları ile iletişim halindedir. Bu istasyonlardan biri, ki bu genelde en yakındaki olur, telefonunuz ile ağ arasındaki aracı olur. Telefonunuzun ahizesi kelimelerinizi dijital veri akışına çevirerek baz istasyonundaki alıcıya gönderir.

Baz istasyonu faaliyetleri, istasyon içindeki radyo kanallarını ayıran ve kendi kontrolündeki vericiler arasında konuşma geçişlerini koordine etmeye yarayan özel amaçlı bir bilgisayar olan baz istasyonu kontrolörü tarafından yönetilir.

Bu kontrolör sırasıyla, telefon aramalarını alan mobil anahtarlama merkezi ile iletişim kurar ve bu aramaları aynı anahtarlama merkezinde, şirketin diğer anahtarlama merkezlerinde ya da yabancı şebekelere ağ geçidi olarak çalışan özel santrallarda diğer telefon şebekelerine (mobil ya da sabit) yönlendirerek alıcılara bağlar. Mobil anahtarlama merkezleri, Atina Olayı için önemlidir çünkü dinlemeler, kötü niyetli yazılımı bulunduran bu merkezler aracılığıyla yapılmıştır. Mantıklı seçimlerdir, çünkü ağın kalbinde yer almışlardır. Korsanlar saldırı için yalnızca bir kaçını ele geçirmeye ihtiyaç duymuştur.

Hem baz istasyonu kontrolörleri, hem de anahtarlama merkezleri, santral adıyla bilinen büyük bilgisayarlar etrafına kurulmuşlardır. Santrallar, kendi ağı içindeki telefonlar arasında iletişim yolları yaratırlar ve prensipte dünyada bulunan diğer telefonlarla da bu iletişim ağı kurulur. Santrallar, güçlü bilgisayarların odaları doldurduğu yıllar olan 1970'lerden kalmadır ve özel donanım ve yazılım etrafına inşa edilmişlerdir. Bu bilgisayarlar günümüzde çok daha küçük olsa da, sistemin temel mimarisi çoğunlukla değişmeden kalmıştır.

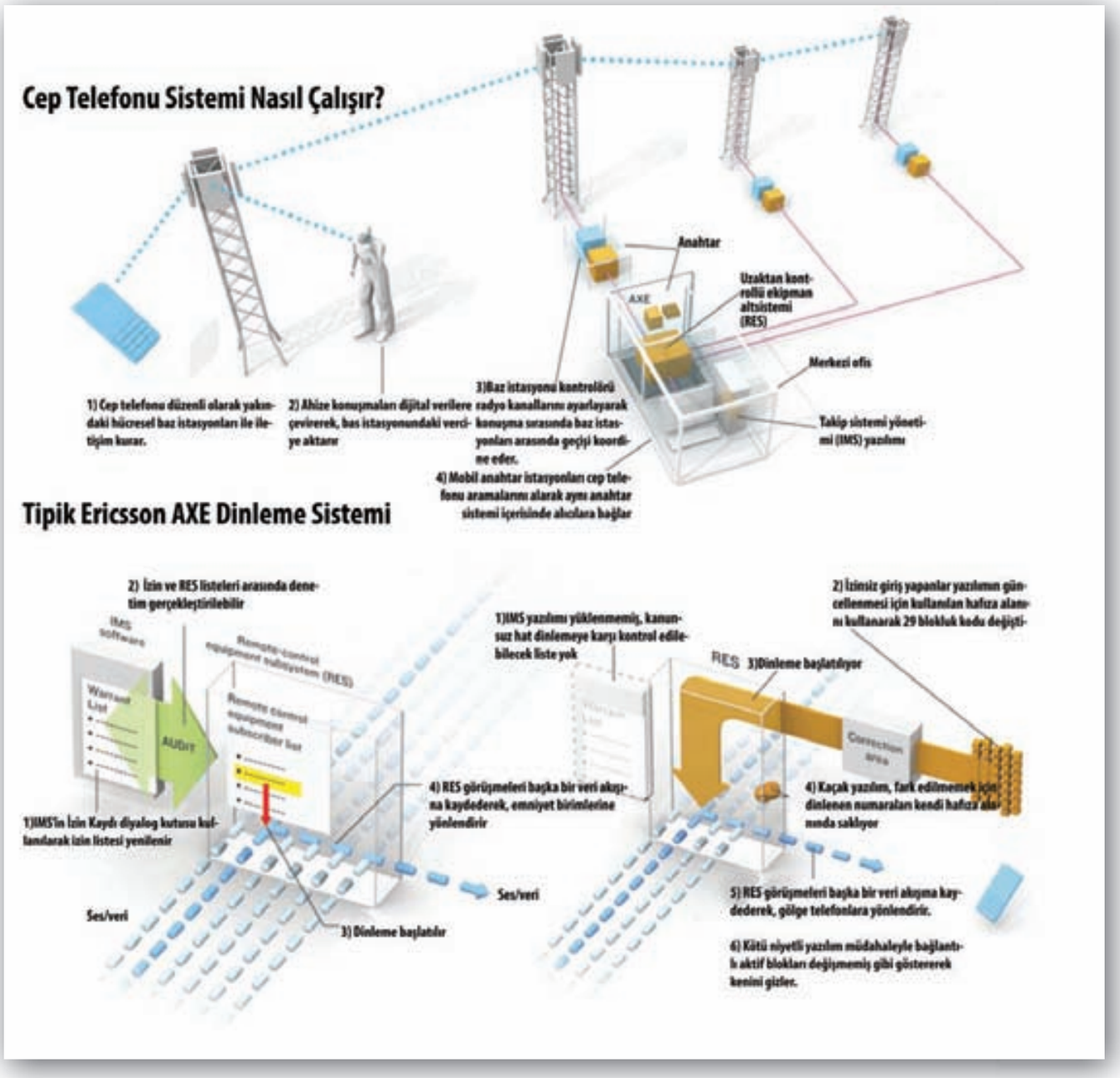
Çoğu telefon firması gibi, Vodafone Yunanistan, kendi mobil anahtarlama merkezi ve baz istasyonu kontrolörü için Ericsson'un AXE modelini kullanmıştır. Bu sistemde merkezi bir işlemci santralın operasyonunu koordine eder ve santralı bir telefondan diğerine veri yolu kurabilmesi için yönlendirir. Ağ aktivite kayıtları ve faturalandırma bilgisi, yönetim işlemcisi adı verilen farklı bir ünitede bulunan disk üzerinde saklanır.

Atina Olayı'nın kalbinde bulunan sızmayı anlamanın yolu Ericsson AXE'nin hukuki dinlemelere nasıl izin verdiğini bilmekten geçmektedir. Detaylar ülkeden ülkeye değişiklik gösterse de, Yunanistan'da, birçok yerde olduğu gibi, kolluk kuvvetleri mahkemeye başvurarak izin alır Daha sonra bu dinleme izni dinlenecek olan kişinin müşterisi olduğu telefon şirketine iletilmektedir

Bugünlerde, bütün hukuki dinlemeler merkez ofiste gerçekleştirilmektedir. AXE santrallında uzaktan kontrollü ekipman alt sistemi (RES), konuşma ve veri akışını izleyerek dinlemeyi gerçekleştirir. RES, dinleme için kullanılan ve sadece kolluk kuvvetlerinin erişmine açık olması gereken bir yazılımdır. Dinleme kararı bulunan bir telefondan arama yapıldığında, RES bütün konuşmayı ikinci bir veri akışına kopyalar ve bu kopyayı kolluk kuvvetlerinin dinlemeyi gerçekleştirdiği hatta aktarır.

Opsiyonel olarak Ericsson Dinleme Yönetim Sistemi (IMS) de sunmaktadır. Bu sistemle birlikte, yasal dinlemeler düzenlenir ve yönetilir. Mahkeme kararı şirkete ibraz edildikten sonra, operatörler IMS yazılımındaki bir formu doldurarak dinlemeyi başlatır. Operatör arayüzündeki opsiyonel IMS ve santraldaki RES dinlenen numaraların listesini içerir. IMS'de dinleme istekleri ve RES'te dinleme numaraları bulunur. Sadece IMS ile başlatılmış olan dinlemeler RES'te aktif olmaktadır, böylece RES'teki bir dinleme IMS'te dinleme isteği olmaksızın oluşmuş ise yetkili olmayan bir dinlemenin oluştuğunun iyi bir kanıtıdır. Bu iki sistem arasındaki farkları tespit etmek için bir denetleme prosedürü kullanılabilir.

İllegal dinlemeler sırasında, Vodafone'un dinleme opsiyonunu satın almamış olduğu ve IMS yazılımının Vodafone sistemlerinde kurulmamış olduğu ortaya çıkmıştır. Fakat 2003 başlarında Vodafone Yunanistan teknisyenleri santrallarındaki AXE için kullanılan yazılım paketini R9.1 sürümüne yükseltmişlerdir. Bu yükseltme, RES yazılımını da içermektedir. Dolayısıyla yükseltme işleminden sonra, Vodafone'un sistemi, RES'i kullanarak, konuşmaları dinlemek için gerekli olan yazılım kodlarını da içerir hale gelmiştir. Ancak IMS'de dinleme işlemlerinde kullanılan arayüze sahip değildir.



Bu hoş olmayan durumun, Atina korsanlarının illegal olarak konuşmaları dinlemelerine ve aylarca fark edilmemelerine sebebiyet verdiği anlaşılmıştır.

Vodafone'un mobil anahtarlama merkezlerinde yasal dinleme fonksiyonlarını manipüle etmek için ciddi bir programlama bilgisi gerekmektedir. Saldırganların işi karmaşıktır çünkü dinleme yazılımını kurma ve çalıştırma işlemlerini Vodafone ya da Ericson'un sistem yöneticilerine yakalanmadan yapmak zorundadırlar. Zaman zaman saldırganların izlenen numaraların ve gölge telefonların listesini güncellemek için yazılıma giriş yapmaları gerekmektedir. Bu aktiviteler, rutin bakım aktivitelerini yerine getiren sistem yöneticilerine görünmeyerek, kayıt dışı tutulmalıdır. Saldırganlar bunları yerine getirmeyi başarmıştır.

Saldırganlar, AXE'nin sistemi yeniden başlatmaya gerek olmadan yeni yazılım yüklenmesine izin veren fonksiyonundan yararlanmışlardır. Sistemdeki bir kesintinin telefon görüşmelerini keseceği, kısa mesajlarda veri kaybına yol açacağı ve acil güvenlik servislerini ulaşılamaz kılacağı dikkate alındığında bu önemli bir özelliktir. AXE santrallının on yıllarca kesintisiz olarak işlemesine izin verebilmek için, birçoklarının yaptığı gibi Ericsson'un yazılımları hatalarla başa çıkmak ve santralın yazılımına ara vermeden güncelleme yapmak için bir kaç teknik kullanmaktadır. Bu teknikler merkezi işlemcide yüklü olan kodu doğrudan güncellemeye izin vermektedir, ki bu güncelleme işleyen sistemi çalışır durumdayken etkilemektedir.

Modern GSM sistemleri, Vodafone gibi, kablosuz bağlantıları karmaşık şifreleme mekanizmalarıyla güven altına almaktadır. Bir cep telefonuna başka bir telefondan yapılan bir arama uzak cep telefonu ve en yakın baz istasyonu arasında yeniden şifrelenecektir. Fakat servis sağlayıcının çekirdek ağından geçerken korunmaz. Bu sebeple -aramaları izleme kolaylığı için- failler Vodafone ağının çekirdek anahtarlarına saldırmışlardır. Zincirin başından sonuna iletişimi şifreleme -bankaların yaptığı gibi- yasal dinlemelerin uygulanmasını çok zorlaştırmaktadır.

AXE'nin kendi merkezi işlemcisinde çalışan yazılımı doğrudan güncellemek için detaylı kurallar bulunmaktadır. AXE'nin var olan kodu, merkez işlemci hafızasında saklanan bağımsız bloklar (ya da program modülleri) etrafında yapılandırılmıştır. 2004'te kullanılmakta olan sürüm yaklaşık 1760 bloktan oluşmaktadır. Her bir blok güncelleme sırasında kullanılan küçük bir "düzeltme alanına" da sahiptir.

Örneğin, hali hazırda farklı bir fonksiyonu (Y), yerine getiren bilgisayarı yeni bir fonksiyon (Z), yerine getirmesi için kod içine yama yapılır. Sonuç olarak orijinal yazılım "eğer X ise Y" komutuna sahipken, bunun etkisiyle yamalı yazılım "Eğer X ise düzeltme alanı L'ye git" komutuna sahip olur. Yazılım lokasyon L'ye gider ve orada karşılaştığı komutları yerine getirir ki bu da Z'dir. Diğer bir değişle, yazılım yaması kod alanındaki düzeltilecek olan komutu, programı kodun yeni sürümünü içeren düzeltme alanındaki hafıza lokasyonuna çevirecek olan komutla değiştirir.

Saldırganların karşılaşacağı zorluk, RES'in arama akışı verisini, IMS'deki arayüz olan form kutusunu kullanmadan; dolayısıyla aktivite kaydı tutulmadan kopyalamak ve yönlendirmek olacaktır. Saldırganlar, dinlemeyi araştıran Yunan Parlemento Komitesi karşısında ifade veren Ericsson çalışanlarına göre, 29 farklı kod bloğuna yama serisi yükleyerek bunu gerçekleştirmişlerdir. Bu kötü niyetli yazılım, merkezi işlemcideki yazılımı doğrudan dinleme başlatarak RES'in özelliklerini kullanabilecek şekilde değiştirmiştir. Onlar için en iyisi, dinlemelerin operatörlere IMS kullanıcı ara yüzleri kullanılmadığı için görünmemiş olmasıdır.

Yazılımın tam sürümü, santral içinde resmi kayıt ile dinlenmekte olan telefon numaralarını kaydedebilirdi. Ve daha önce belirttiğimiz gibi, inceleme santral tarafından izlenen numaraların ve IMS'de aktif olan izinler arasındaki farklılıkları bulabilirdi. Ama kötü niyetli yazılım IMS'yi atlatmıştır. Onun yerine, dinlenecek numaraları kötü niyetli yazılımın, santralın hafızası içerisinde bulunmakla birlikte izole olan ve santral yazılımı tarafından fark edilmeyen, kendi hafıza alanında bulunan iki veri bölümünde saklamıştır.

Bu durum kötü niyetli yazılıma tespit edilmeden çalışması için büyük avantaj sağlamıştır. Fakat suçlular kendi izlerini aynı zamanda farklı teknikler kullanarak saklamışlardır. Vodafone teknisyenlerinin AXE yazılım bloklarında olan değişiklikleri fark edebilecekleri bazı durumlar vardır. Örneğin, Microsoft Windows'taki görev yöneticisi ya da Unix'deki işlem durumuna (PS) benzer bir şekilde blokların listeleyebilirlerdi ki bu da AXE içinde çalışmakta olan bütün aktif işlemleri gösterirdi. Böylece, aktif olmamaları gerektiği halde aktif olan bazı işlemleri görebilirlerdi. Fakat kötü niyetli yazılımın, aktif blokları listeleyen komutları, dinlemelerle ilgili olan blokları bu tür listelerin dışında bırakacak şekilde değiştirdiği anlaşılmıştır.

Ek olarak kötü niyetli yazılım, güncelleme sırasında ya da Vodafone teknisyenleri küçük bir yama yaparken bile keşfedilmiş olabilirdi. Telekomünikasyon endüstrisinde teknisyenlerin var olan blok içeriklerini güncelleme ya da yama yapmadan önce doğrulamaları standart bir uygulamadır. Kötü niyetli yazılımın neden bu yolla keşfedilemediğini bilmiyoruz. Fakat yazılımın aynı zamanda sağlama için kullanılan komutun (mevcut blokların bütünlüğünün doğrulanması için bir çeşit imza yaratan kodlar) da işleyişini değiştirmiş olabileceğinden şüphelenilmiştir. Bir şekilde, bloklar operatörlere değişmemiş görünmüşlerdir.

Son olarak, yazılım suçluların gelecekte kontrol edebilmesi için bir arka kapı da içermektedir. Bu da, tespit edilmeyi önleyecek şekilde oluşturulmuştur. Yunanistan Bilgi ve İletişim Güvenliği ve Gizliliği Başkanlığı (ADAE) tarafından hazırlanmış olan rapora göre, kötü niyetli yazılım, santralın komut ayrıştırıcısını (sistem yöneticisi statüsündeki kişiler tarafından kullanılabilen bir prosedür) değiştirmiştir. Bu değişiklik sayesinde, zararsız komutlardan sonra gelen 6 boşluk karakteri santralda işlem kaydı tutulmasını devre dışı bırakmakta, devre dışı bırakıldığında oluşması gereken alarmı da durdurmakta ve yasal dinleme alt sistemiyle ilgili komutların çalışmasını sağlamaktadır. Sonuç olarak, dinleme ile ilgili operasyonlara izin veren fakat iz bırakmayan bir komut olarak işlev görmüştür. Ayrıca yeni bir kullanıcı adı ve şifresini sisteme eklemiş ve bunlar santralla giriş için kullanılmıştır.

Sadece işleyen sistem kodunu değiştirmekle kalmayıp, kendi izlerini yok eden yazılımlara "rootkit" adı verilmiştir. Bu terim halk tarafından bir plakçılık markası olan Sony BMG Music Entertainment'ın 2005'de çıkan bazı müzik CD'lerinin eklediği rootkit adlı bir yazılım eklemesiyle gerçekleşmiştir. Sony rootkit, CD'lerin kopyalanmasını

sınırlamıştır: CD Windows İşletim Sistemi'nden çalıştırıldığında varlığını, sahibinden saklamaya yönelik bir yazılım çalıştırmaktadır. (Sony, rootkit kullanmayı genel istek üzerine kaldırmıştır.) Gizlilik uzmanları, genel amaçla kullanılan işletim sistemleri için de diğer rootkitleri de keşfetmişlerdir. Bu işletim sistemlerine örnek olarak Linux, Windows ve Solaris verilebilir. Fakat bildiğimiz kadarıyla, rootkitin özel amaçlı bir sistem üzerinde, yani Ericsson'un telefon santrallı üzerinde bulunmasına ilk kez rastlanmıştır.

Peki bütün bu karmaşık çalışma yöntemine rağmen, kötü amaçlı yazılım nasıl fark edildi? 24 Ocak 2005 tarihinde failler yüklemiş oldukları yazılımı güncellemişlerdir. Bu güncelleme bazı kısa mesajların iletilmesini etkileyerek, onların ulaşmamasına yol açmıştır. Ulaşmayan kısa mesajlar, otomatik bir hata raporu oluşturulmasını tetiklemiştir.

Bu noktada, korsanlar AXE yazılım paketine yaptıkları değişiklikleri gizli tutma şanslarını yitirmişlerdir, zaten başka birinin siteminde bir işlemi gizli tutmak neredeyse imkansızdır.

AXE, diğer büyük yazılım sistemleri gibi, bütün ağ aktivitelerinin kaydını tutmaktadır. Sistem yöneticileri bu kayıt dosyalarını inceleyebilir ve sıradan kullanım olmadığını belirledikleri herhangi bir olay araştırılabilir.

Kayıt tutma işlemi çok önemlidir. Örneğin, 1986'da Guguk Kuşu Yumurtası vakasında, ağ yöneticisi Clifford Stoll'dan 75 dolar sentlik hesaplama hatasını bulması istenmiştir. Stoll, Kaliforniya'daki nükleer silah laboratuvarı olan Lawrence Livermore Ulusal Laboratuvarı ağlarının çok derinlerine girmiş olan korsanı bulmak için 10 ay harcamıştır. Bu zamanın çoğu kayıt rapor sayfalarına bakarak geçmiştir.

AXE, günümüzdeki çoğu gelişmiş sistem gibi, operatöre, yarattığı çok miktarda kayıtların arasından kullanışlı bilginin kaynağını bulmasında yardımcı olur. Kendi anormal aktivitelerini hata ya da başarısızlık raporu olarak kaydetmek için programlanmıştır. Ek olarak, düzenli aralıklarla anahtarlama merkezi kendisinin bellek kopyasını, yani bütün program ve verilerinin bir kopya ya da dökümünü alır.

Dökümler sıklıkla kurtarma ve tanı koyma amacıyla kullanılır. Fakat güvenlik araştırmalarında da kullanılabilirler. Sonuç olarak teslim edilmeyen yazılı mesajlar yüzünden Ericsson'un araştırmacıları çağrıldığında, baktıkları ilk şey periyodik dökümler olmuştur. İzlenmiş olan telefon numaralarının tutulduğu iki alan bulmuşlardır ve listelerini almayı başarmışlardır.

Araştırmacılar dökümleri daha özenli bir şekilde incelemişlerdir ve kötü niyetli programları bulmuşlardır. Buna rağmen, buldukları yürütülebilir kodlar halindedir, diğer bir deyişle kodlar mikroişlemcilerin doğrudan yürüttüğü ikili dildedir. Yürütülebilir kod, kaynak kod (AXE için PLEX dilinde yazılan programlar) bilgisayar işlemcisinin yürüttüğü ikili makina koduna dönüştürüldüğünde oluşan koddur. Dolayısıyla, araştırmacılar, titizlikle saldırganların oluşturduğu orijinal PLEX kaynak kodlarına yakın bir dosya oluşturmuşlardır. Bu dosyanın, şaşırtıcı bir şekilde yazılımın azımsanmayacak bir parçasını oluşturan 6500 kod satırından oluştuğu ortaya çıkmıştır.

Araştırmacılar, modüllerin nasıl çalıştığını daha iyi anlamak için modülleri simülasyon ortamında çalıştırmışlardır. Bütün bu araştırmanın sonucunda dinlenmiş olan numaraların tutulduğu veri alanına ve yakın zamandaki dinlemelerin zaman damgalarına ulaşılmıştır.

Eldeki bütün bu bilgiyle, araştırmacılar önceki dökümlere bakıp dinlemelerin olduğu zaman aralıklarını belirleyerek dinlenen numaraların tam listesine ve arama verisine (kimin kimi ne zaman aradığı ve aramaların ne kadar sürdüğü) ulaşmışlardır. (Konuşmaların içerikleri kayıtlarda tutulmamaktadır.)

Sızma yöntemi karmaşık olsa da, dinleme işlemi daha basittir. Örneğin, Başbakan cep telefonundan bir arama başlatır ya da alırsa santral, yasal bir dinlemede kullanılan bağlantının aynısını konuşmanın dinlenmesi amacıyla bir gölge numarayla kurmaktadır.

Kötü niyetli yazılım yaratmak ve böylece algılanmadan saklanmasını sağlamak, AXE kodu yazımı için az rastlanan bir uzmanlık gerektirmektedir. Ericsson yazılımının AXE için geliştirilen büyük bir bölümü son 15 yıldır Atina kökenli Intracom Holding'in bünyesindeki Intracom Telekom'la birlikte yapılmıştır. Intracom'da göreve yapan ve geçmişte görev alan bir çok yazılım geliştiricisi, bu işi yapmak için gerekli bilgiye sahipti. Dolayısıyla gerçekleştirilen sızma, yazılımı geliştirenlerden biri tarafından yapılmış olabilir mi?

Sızmanın ilk aşamasının Vodafone içinden olan birinin yardımıyla gerçekleştirilmesi çok daha kolay olabilirdi. Fakat bu senaryoyu destekleyebilecek bir kanıt mevcut değildir. Sızma uzaktan yapılmış olabilir hatta resmi bir rapora göre, gerçekleşme zamanı bilinen metin mesajı hatasından hemen önce, santrala en son erişen kişi için bir ziyaretçi kartı düzenlenmiştir.

Benzer bir şekilde, Tsalikidis'in dinlemelerle ilgisi olup olmadığını da bilemeyiz. Çoğu gözlemci ölümünün zamanlamasını düşündürücü bulmaktadır. Fakat bu güne kadar herhangi bir bağlantı açıklanamamıştır. Gözlemciler sızan kişilerin güdüleri hakkında spekülasyon yapmaktan öteye gidememektedir.

Atina Olayı'nın arkasında kimin olduğunu ve amaçlarının ne olduğunu kesinlikle bilemeyeceğimiz gibi, onların saldırılarını yaparken izledikleri yol hakkında da ancak tahmin yürütebiliyoruz. Çünkü kritik bilgiler ya bir şekilde kayboldu ya da hiç bir zaman toplanmadı. Örneğin, Haziran 2005'te soruşturmanın sürdüğü sırada Vodafone, santral yönetim sistemine giriş için kullanılan üç sunucunun ikisini yükseltmiştir. Bu yükseltme sırasında giriş kayıtları silinmiş ve şirket politikasına zıt olarak yedekler tutulmamıştır. Bir süre sonra, ziyaretçi giriş kayıtlarının 6 aylık tutulma süresi sona ermiş, Vodafone kötü niyetli yazılımın değiştirilerek metin mesajı hatalarının oluştuğu döneme ait olan kayıtları yok etmiştir.

Kötü niyetli yazılımın yüklenmesinin izleri santralın işlem kayıtlarına geçmiş olabilir. Ancak, santral yönetim sistemindeki depolama alanının yetersizliği sebebiyle, sadece 5 günlük kayıtlar tutulmuştur. Çünkü Vodafone aynı yerde depolanmakta olan faturalama verisine çok daha fazla önem vermektedir. En önemlisi, Vodafone'un kötü niyetli yazılımı 7 Mart 2005'te kullanım dışına almış olması neredeyse kesin olarak komploculari alarma geçirmiş ve gölge telefonları kapatmaları için onlara şans tanımıştır. Sonuç olarak yetkililerin gölge telefonların yerlerini belirleme ve zanlıları yakalama şansı kalmamıştır.

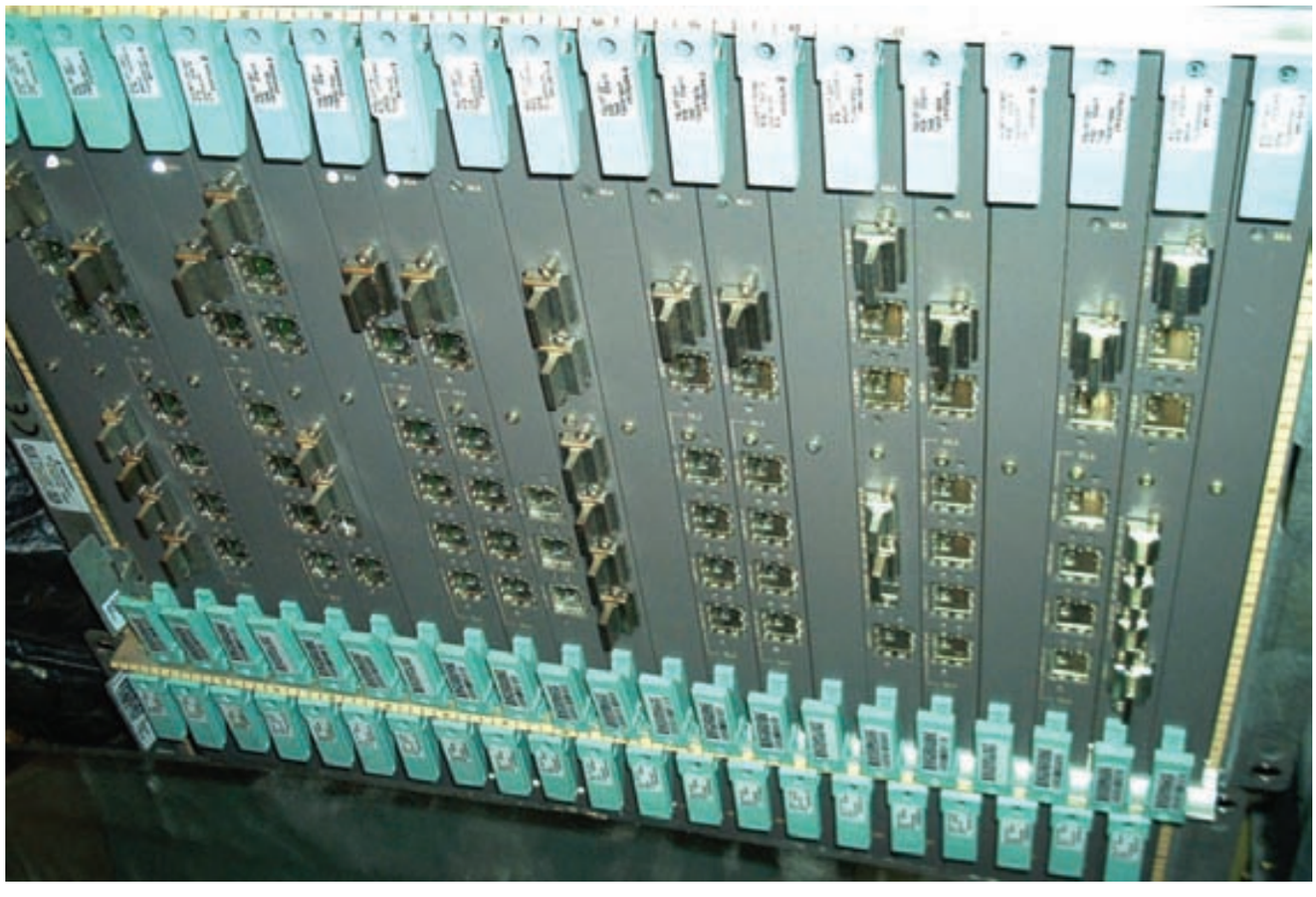
Bu olay bize telefon ağlarımızı korumakla ilgili olarak ne öğretebilir?

Bir kere sızma keşfedildiğinde, Vodafone devam etmekte olan ağ işletimini kesintiye uğratmadan suçluların takibini kolaylaştırması gerekiyordu. Maalesef hem Vodafone'un, hem de Yunanistan kolluk kuvvetlerinin tepkileri yetersiz kalmıştır. Vodafone'un hamleleriyle, hem kritik veriler yok olmuş ya da imha edilmiştir; hem de suçlular fark edildiklerine dair sinyal almış ve ortadan kaybolmak için yeterli zamanı kazanmışlardır.

Telekomünikasyon endüstrisinde geçerli uygulamalar operatör politikalarının, virüs saldırısı gibi sızmalara karşı tüm veriyi tutmak, sistemin sızılan bölümünü mümkün olduğunca izole etmek ve kolluk kuvvetleriyle işbirliği yapmak için gerekli işlemleri içermesini zorunlu kılmaktadır.

Yunanistan telekom mevzuatında operatörlerin ağ kullanıcılarının ve iletişimin gizliliğini temin edecek ölçütleri detaylandıracak güvenlik politikası olması zorunluluğu bulunmaktadır. Buna rağmen, Vodafone'un uygulamaları, eğer varsa bile böyle politikaların yok sayıldığını göstermektedir. Basın toplantıları ve kamu araştırmaları için değilse bile, kolluk kuvvetleri gölge cep telefonlarını izleyebilirlerdi. Fiziksel ziyaret kayıtları kaybedilmiştir ve veri kayıtları imha edilmiştir. Ek olarak, ne kolluk kuvvetleri ne de ADAE ile doğrudan iletişime geçilmiştir. Onun yerine Vodafone Yunanistan politik bir kanaldan, Başbakanlık ile iletişim kurmayı tercih etmiştir. Şu belirtilmelidir ki ADAE 2003'te kurulan ve nispeten yeni bir kuruluştur.

Yunanistan kolluk kuvvetlerinin tepkisi de olması gerekenden uzaktır. Polis Vodafone'un olayla ilişkili bütün telekomünikasyon ekipmanına el koyarak kanıtları güvence altına alabilirdi. Bunun yerine, görülmektedir ki mobil telefon ağı işletiminin zarar göreceğine yönelik endişeler yetkilileri konuyu daha hafif bir yaklaşımla ele almaya yö-



neltmiş, çalışanları sorgulamak ve Vodafone tarafından sağlanan bilgiyi almakla yetinilmiş, ve bu durum adli delillerin kaybedilmesine yol açmıştır. Sonunda polis hem operatörü (Vodafone) hem de yazılım sağlayıcısını (Ericsson) suçlayarak, mağdurları sanık konumuna düşürmüş ve iyi niyetlerini kaybetmelerine neden olmuştur. Bu durum soruşturmayı bir nebze daha aksatmıştır.

Böyle teknoloji suçlarının az görüldüğü ülkelerde, eğitimli uzmanlardan oluşan bir soruşturma takımı bulmayı ummak mantıksızdır. Yüksek teknoloji kullanılan suçlarla başa çıkmak için hızlı hareket eden bir birim kurulabilir mi? Uluslararası polis organizasyonu Interpol'ün, ülkelerin bu tür suçlar için yardım isteyeceği, bilişim suçları için bir soruşturmacı takımı oluşturmasını isteriz.

Telefon santralları yıllar içersinde yazılım tabanlı sistemlere dönüştü ve bu sebeple güvenlik açıkları için sistemleri analiz etmek çok zorlaşmıştır. Konferans, numara taşınabilirliği, arayan kişinin kimliğinin saptanması gibi veritabanı özellikleri santrallara yüklenmiş olsa da, eski yazılım yerinde durmaktadır. Alt sistemler ve barok kodlama stilleri (20 ya da 30 yıl önce yazılmış olan eski programlar) arasındaki karmaşık etkileşimler geliştiricilerin ve denetleyicilerin kafasını karıştırmaktadır.

Ancak virüslere, solucanlara ve rootkitlere karşı etkili savunma, kaynak kodunun barok heterojenliğine nüfuz edebilen derinlemesine analize bağlıdır. Örneğin, arama günlüklerinin istatistiksel analizleri, gölge numara aramaları ve izlenen numara aramaları arasında bir ilişki ortaya çıkarabilir. Telefon şirketleri, müşteri eğimlerini anlayabilmek için, bu çeşit veriler üzerine zaten detaylı analizler yapmaktadır. Ancak güvenlik perspektifinden bakıldığında, bu analizler yanlış sebeplerle (güvenliğin aksine pazarlama) ve yanlış insanlar tarafından gerçekleştirilmektedir. Güvenlik personeline bu araçların kullanımı için eğitim vererek ve onların bu verilere ulaşmalarını sağlayarak, müşteri eğilim analizleri, kötü niyetli yazılımlara karşı bir önlem haline gelebilir.

Ek ipuçları, faturalandırma ve hesap bilgileriyle santral tarafından oluşturulan arama kayıtları birleştirilerek deşifre edilebilir. Ancak böyle yapılması, telekom organizasyonu içindeki farklı öğeler tarafından oluşturulan farklı verilerin birleştirilmesini zorunlu kılmaktadır.

Bir diğer savunma, Ericsson'ın çevrimdışı dökümleri inceleyerek kötü niyetli yazılımı keşfetmesini sağlayan türden düzenli denetimdir. Ancak, bu durumda, veri analizi durumunda da olduğu gibi, kötü niyetli yazılımın, kayıtlardaki bilgileri -örneğin kendi yazılımını çalıştıran ayrı bir izleme bilgisayarı kullanarak- değiştiremeyeceğinden emin olmamız gerekir.

Dijital sistemler çok fazla miktarda bilgi oluştururlar. Vodafone'un ağına sızılmış olduğunu keşfetmek için gerekli olan bütün bilgiler, iletilemeyen bir kısa mesaj onları bakmaya yönlendirmeden önce de Ericsson ve Vodafone Yunanistan'ın gözünün önündedir. Diğer alanlarda olduğu gibi, zor olan ortaya çıkan bilgileri kullanabilmek için bir yol bulmaktır. Eğer bir şirketin teknisyenleri ve bir ülkenin polis kuvveti bu zorlu işi yerine getiremiyorsa, yapabilecek ayrı bir müdahale takımı oluşturulmalıdır.

Soruşturmayı bir cadı avına dönüştürmemek çok önemlidir. Özellikle faillerin kimliklerinin belirlenmesinin zor olduğu durumlarda, telekom operatörünü günah keçisi olarak ilan etmek genellikle siyaseten uygun olabilir. Bu sadece operatörleri ve çalışanlarını vukuatları halı altına süpürmeye ve onları kolluk kuvvetleri ile işbirliği yapmamaya yöneltir. Suçlamak (ve cezalandırmak) için birini bulmak yerine, tam olarak neyin yanlış gittiğini belirlemek ve nasıl düzeltileceğini bulmak, sadece operatör için değil aynı zamanda endüstrinin tamamı için daha iyidir.

Sadece sistem sağlayıcıların ve ağ operatörlerinin sızmalara izin vermemeleri gerektiğini söylemek hatta kanun yolu ile yükümlülük getirmek anlamsızdır, çünkü böyle bir olaydan sonra şirketlerin yapabilecekleri çok azdır. Bunun yerine, bu tarz sistemlerin geliştirildiğinden ve güvenli bir şekilde kullanıldığından emin olunması için proaktif önlemler alınmalıdır. Belki, hem uçak üreticileri hem de havayolu şirketlerinin ulusal ve uluslararası organlar tarafından yolcu güvenliğinin sağlanması için dikkatle takip edildiği havacılık güvenliği mevzuatı örnek alınabilir.