İp telefonlar gerekli güvenlik önlemleri alınmadan devreye sokulduklarında hackerların saldırısına uğranmaması mucizedir. Bu gerekli tedbirler uygun güvenlik duvarı ayarları yapılandırma, ip telefon santralinin bulunduğu sabit hattın yurtdışı aramalarına engellenmesi ,kuvveti şifreler tanımlama gibi ufak önlemler aslında en büyük güvenlik açıklarını kapatmanızı sağlar.

Karel teknoloji tarafından sağlanan log dosyalarını gömülü bir işletim sistemi kullanarak açıp bu saldırıyı gerçekeştirilen kişilerin tespiti için savcılıktan dosyayı teslim aldım. Log dosyalarının tamamını açıp inceledim. Dosyaların içerisinde 2 tip farklı dosyalar ile karşılaştım. 1.si ses dosyaları . Bu dosyalar teknik format olarak “.gsm” formatında .Bu dosyaları mp3 yani bilgisayar üzerinden dinlenebilir bir formata çevirerek dinleyebildiğimde dosyaların klasik telefon santralini arandığında “Lütfen sinyal sesinden sonra mesajınızı bırakınız” yada çağrı yapan kişiyi beklerken dinletilen piyano sesi gibi dosyalar olduğu gözüktü.

İkinci tip farklı dosya ise ; İp sanral kurulurken yapılan konfigirasyon dosyaları. Konfigirasyon dosyalarının genel içeriği olarakta ; İp santral üzerinde kullanıcı tanımlama , Yurtiçi,yurtdışı, uluslararası hangi hatların santrala açık olabileceği , İp santrale erişebilmek için yönetici parolası oluşturma (Yapılan incelemede neyazıkki verilen şifrelerin çok güvensiz olduğu görüldü. ) ,voicemail denilen sesli eposta ayarları ki En çok hack maruzuna sebep olan büyük etkenlerden biriside seslimail dir. Neyazıkki konfigürasyona bakıldığı zaman sesli mail konfigürasyonunun zayıf olduğu gözlenmektedir.

Bu log dosyaları ip telefon santraline kimin yada kimlerin usulsüz bir şekilde eriştiğine dair herhangi bir bilgi içermemektedir. Sadece ip santral ile ilgili konfigirasyon dosyaları vardır.

Özellikle olayın gerçekleştiği 2012 yılında sadece Türkiye değil Tüm dünya üzerinde kullanılan güvenliği düşük ip santralli sistemlerde sayısız bu şekilde dolandırıcılık işlemi gerçekleşmiştir. Bu saldırıyı gerçekleştirenler İnternet ortamında kullandığı yazılımlar ile ip santral kullanan kişileri aratıp , bulduklarında ise yönetim paneli şifresi için 2 3 saat lik bir uğraş ile şifreyi ele geçirdikten sonra yurtdışından anlaşmalı oldukları numaraları aratıp dolandırıcılık işlemlerini gerçekleştiriyorlar .

Hackerlar kullandıkları Proxy ip(maske ip) ile gerçekten bulundukları lokasyonları gizleyip işlerini bu şekilde hallediyorlar.

Sonuç

Verilen loglar mağdurun ip santraline ait herhangi bir erişim bilgilerini içermemektedir. Sadece melodiler ve yapılandırma ayarları mevcuttur.