

SAYIN YETKİLİ;

Bilindiği gibi teknolojik gelişimleri ve özellikle de iletişim ve teknolojisi ve dijital teknolojinin gelişimini müteakiben bu teknolojilerin farklı amaçlı kişiler tarafından kötü amaçlı kullanımı da artmıştır.

Bahsedilen kötü amaçlı kullanımların başında da kişi ya da kurumların kendi izinleri ya da bilgileri olmadan ses veya görüntü elde yolu ile kayıt altına alınmaları, bu şekilde hassas bilgilere ulaşımı gelmektedir.

Mikrochiplerin kullanıma başlamasından sonra, hepimizin şahit olduğu gibi, önceden büyük boyutlu imal edilen birçok ses ve görüntü kaydedici cihaz son derece küçük ve hatta mikroskobik boyutlara gelmiştir. Küçük bir güç kaynağı ile uzun süreli kayıt yapabilen bu tür cihazlar; küçüklükleri nedeni ile de hemen hemen her yere gizlenebilmekte ve bazen başka bir işe yarayan herhangi bir eşya ya da aksesuar gibi üretilebilmektedirler. Öyle ki bu cihazlar bir kalemin, bir saatin içine, gözlük çerçevesine vs. yerleştirilebilir duruma gelmişlerdir. Karşımızda duran ve fark edemediğimiz bir düğme, bir saat, bir uzatma kablosu ve benzeri çok sayıda ürün vasıtası ile dinmemizde ya da görüntümüzün alınmasında bir engel yoktur.

Dinleme işlemleri sadece yakın mesafeden yapılmamakta, uzun mesafelerden de hiç mekana girilmeden yapılabilmektedir. Ofis ya da ikamet camına dışarıdan yansıtılan gözle görünmez bir lazer ışını vasıtası ile camdan alınan ses titreşimlerinin sese dönüştürülmesi tekniği bu durum hakkında fikir verecektir.

Cep telefonları ise çok daha yaygın ve kolay bir dinleme ortamı sunmaktadır. Elimizde taşıdığımız akıllı cep telefonlarından internete bağlanmış olmamız, veri alışverişini açık bırakmış olmamız, konum servislerine izin vermiş olmamız vs. gibi durumlar bizi tamamen anonim bir duruma getirmektedir. Öyle ki bilişim teknolojisinden bir parça anlayan birisi bile bu amaçla kullanılan ve internetten uygulama olarak indirebileceği casus programlar vasıtası ile telefonumuzun hoparlörünü ve kamerasını rahatlıkla kayıt cihazı olarak kullanabilir. Herhangi bir masum linki tıkladığımızda bizim haberimiz olmadan cihazımıza yüklenen casus programlar, tüm yazılı mesajlarımızı, sesli görüşme kopyalarımızı, Viber, Whats'up, facebook gibi sosyal iletişim mesajlarını bizi dinleme gayretinde olan kişilere aktarabilir. Tabi ki bütün bunlar olurken bizim hiçbir şey fark etmeyeceğimiz, bizi kaydetmeye başlayan telefonumuzun açıldığını bile görmeyeceğimiz ortadadır



Plusecon bu amaçla değerli müşterilerinde teknik, elektronik ve dijital izleme ve dinleme yöntemlerine karşı koyma, mevcutta yerleştirilmiş bulunan bu tür "böcek" olarak adlandırılan cihazları tespit etme amacı ile "böcek arama" kelimesinin tam karşılığı olan "Debugging" çalışmaları yapmaktadır.

Debugging çalışmaları evde, işyerinde, araçta, özel uçakta, toplantı odalarında, kısaca dinlenme riski altında olan kişilere ait her mekanda yapılabilmektedir. Bir kez böcek temizliği yaptırmış olmak bile, bundan sonra artık bu riskten uzak olunduğu anlamına gelmemektedir. İzniniz dışı ya da dahilinde, hatta misafir olarak bile size ait bir mekana gelen bir şahıs çok kısa süre içinde mekana bir dinleme cihazı yerleştirebilir ya da internete bağlı veya bluetooth ve wi-fi özelliği açık her türlü cihazınıza sızıp illegal dinleme ve izleme programları yükleyebilir. Bu sebeple, debugging çalışmalarının sıklıkla tekrarlanmasının yanı sıra, şahısların kendilerinin ve güvendikleri personellerinin de bu tür girişimlere engel olma ya da tespit yöntemlerini bilmeleri gerekmektedir.

İzlenme ve dinlenme risklerinin detaylı açılımı ve kullanılan Cihazlar

Akıllı Cep Telefonları vasıtası ile

A-Resmi kurumlar vasıtası ile

Yasal dinlemelerde yetkili kurum Telekomünikasyon İletişim Başkanlığıdır. (TİB). Üç GSM şirketi ve sabit hat hizmeti veren Türk Telekom TİB'in Gölbaşı'ndaki merkezine fiber optik ağla bağlı durumda. Mahkeme, savcılık veya kolluk amiri yasal bir dinleme kararını TİB'e ve dinlemeyi yapacak kurumlara bildiriyor.

Dinlemeyi yapabilecek kurumlar ise MİT, Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığı. TİB dinleme yapmıyor, dinlenecek hattı, talebi yapan birime yönlendiriyor. Telefon operatörleri dinlenecek numarayı kesinlikle bilmiyor. Bu dinlenen kişinin haberdar olmaması için alınan bir güvenlik önlemi.

MİT, Emniyet Genel Müdürlüğü veya Jandarma bilgisayar sistemleri üzerinden dinleme işlemini gerçekleştiriyor.

Bu konuda yetkili resmi kurumların cep telefonları ile yapabildiği sadece anlık dinleme ile sınırlı değil. İstenildiği takdirde konum bilgileri açık telefonlardan anlık konuma ulaşılabilir gibi, konum bilgileri kapalı olsa da cihazın sinyal aldığı baz istasyonlarından ortalama konumuna ulaşılabilir. Tüm SMS ve MMS'ler izlenebilir ve kaydedilebilir. IP numaranıza göre her türlü internet geçmişiniz öğrenilebilir.

Not: Telefon dışında yasal olarak ilgili kurumlar teknolojik aletlerle ortam dinlemesi başta olmak üzere farklı dinleme teknikleri de kullanabilir.

B-Gayri resmi kişi veya vasıtası ile

Gayri resmi kişi ve kurumların GSM operatörleri vasıtası ile, varolan bir altyapıyı kullanarak cep telefonlarınızı dinlemeleri veya içeriğine ulaşabilmeleri mümkün değil. Ancak bu, yapılamadığı

anlamına gelmiyor. Sağlanması gereken tek şart, telefonunuza bir şekilde ulaşıp, içine sizin fark etmeyeceğiniz bir casus program yerleştirmek. İnternette şöyle bir araştırma yapacak olursanız, bu hizmeti cüzi fiyatlarla verme iddiasında olan veya casus program satan birçok sanal şirket olduğunu göreceksiniz. Bu da her isteyen bu tür bir beceriye sahip olabileceği anlamına geliyor. Aşağıda yerleştirilmiş görsel bu amaçla kurulmuş bir web sayfasından resim görüntüsü olarak alınmıştır. Taahhütlere bakıldığında ne demek istediğimiz anlaşılacaktır.



Casus Mesajlaşma Takip

Telefona gelen ve giden SMS içeriklerini tarih saat bilgisi ile göre bilirsiniz



Görüşme Dinleme Yazılımı

Takip edilen casus telefonda yapılan telefon görüşmelerini ses kaydı olarak dinleye bilirsiniz.



Telefon Rehber Takibi

Casus telefonundaki kayıtlı bütün rehber bilgilerini isimleri de dahil olmak üzere tamamını görüntüleyebilirsiniz.



Online Resim Görme

İstedğiniz aralıklarla telefonun ortamdaki resimleri alabilirsiniz



GPS Konum izleme

Takip edilen telefonun bulunduğu konumu bilgisini verir.



Mikrofon açmak

Takip edilen telefonu artık uzaktan online kontrol edebilirsiniz.

Casus programlar nasıl yerleştirilir.?

Bir casus programın telefonunuza yerleştirilebilmesi için uygulanan en yaygın yöntem telefonunuza ya da Whatsup, wiber, facebook Messenger, twitter vs. gibi kullanmakta olduğunuz mesajlaşma programlarına, muhtemelen açmanızı istedikleri bir dosya ya da resim linki göndermektir. Bunu açtığınızda dosya ya da resmi görerseniz bile casus program siz fark etmeden telefonunuza kurulacaktır. Linki size gönderen kişi çok iyi tanıdığınız biri olsa da, güvenilirlikten emin olunamaz. Genelde casus yazılım yollayanlar önce bazı kişilerin yazışma programlarını hack yöntemi ile ele geçirir ve adres defterlerindeki rastgele ya da belirli kişileri hedef seçerler. Link yollama yöntemi aynı zamanda hesaplarınızın ele geçirilmesine yarayan bir casus yazılım gönderme amaçlı da kullanılabilir.

Bir diğer casus program yerleştirme yöntemi de, telefonunuzun bluetooth ya da Wi-fi özelliği açık olduğunda başarı ile kullanılabilir. Telefonun sahibinin haberi bile olmadan kısa mesafeden bluetooth ya da wi-fi ile telefona casus yazılım yüklenebilir.

Doğrudan yetkili servis olmayan servislerde tamir ettirilen telefonlarda da bu tür bir risk yüksektir.

Casus program yüklemesinden sonraki riskler ve olasılıklar nelerdir?

Casus bir programın yüklenmesinden sonra, programın tipine göre yapılabilecekler şunlardır.

1-Telefon sahibi açıldığını bile fark etmeden, uzak erişimle telefonun mikrofon ve kamera özelliği açılabilir. Telefonun tamamen kapalı olması bile bu durumu engellemez. Sonrasında uzaktan erişim sağlayan kişi mikrofonla ortam dinleme ve kamera ile ortam görüntü kaydı yapabilir.

2-Casus program buna yönelikse, her arandığınızda bir arama da programı uzaktan izleyen kişiye yönlendirilecektir ve kişi isterse konuşmanızı anlık olarak dinleyebilir. Aynı şekilde size

casus programının kapsadığı her türlü mesajlaşma uygulamanıza gelen mesaj, video veya görüntülerin bir kopyası yazılımı izleyen kişinin telefonunda da gidecektir.

3-İzleme ve dinleme yapan gayrı resmi kişi ve kurumlar istedikleri takdirde sadece belirledikleri bazı anahtar kelimelerinin içinde geçtiği mesaj ve e-mailleri filtreleyerek alabilirler. Tahmin edeceğimiz bazı gelişmiş ülkelerin bu yöntemleri tüm dünyadaki web ağını kullanarak kontrol altında tuttukları bilinmektedir.

4-Mesajlaşma uygulamalarına ulaşabilen kişiler, telefon sahibinin her türlü bilgisine ulaşabildikleri gibi, onun telefonundan gidiyormuş gibi mesaj ve görüntüler yollayabilirler. Bu da belirli konularda en kolay suç atma yöntemlerinden birisidir.

Cep telefonu harici diğer yöntemler?

Camdan dinleme; (Akustik Dinlemeler)

Özel üretim bir dinleme cihazı ile, uzak mesafeden içinde bulunduğunuz odanın camına yönlendirilen lazer ya da infrared ışınları, konuşmalarınızın camda yarattığı titreşimleri kopyalayarak cihaza geri gönderir. Geri alınan titreşim sinyalleri yine cihaz vasıtası ile ses titreşimlerine çevrilir.



Böcek yerleştirme,

Ortam dinleme ve izleme amaçlı kullanılan gizlenmiş cihazlara kısaca "Böcek" diyoruz. Son teknolojik gelişmeler bu tür cihazları oldukça mikroskobik hale gelmesine olanak tanıdılar. Bu da bu cihazların istenilen her şeyin içine bu böceklerin gizlenebilmesi sonucunu doğurdu. Kalemler, düğmeler, anahtarlıklar, saatler, çantalar, kitaplar, ampuller vs. gibi sayısız malzeme bunların arasında sayılabilir. Bu tür böcekler, genelde alıcı-verici ve alıcı-kaydedici olarak kullanılabilir. Alıcı-verici olarak kullanılan bir böcek radyo frekansı yayarak algıladığı ses veya görüntüyü anında iletebiliyor. Diğerleri ise kayıt amaçlı kullanılmakta. Kayıt amaçlı böcekler herhangi bir yayın (elektromanyetik veya optik) yapmadıkları için sıradan tespit cihazlarıyla bulunamazlar.

Telefon hattından dinleme

Telefon hattından veya santralden dinleme bilinen en eski yöntemlerden birisidir. Telefon Hattı Böcekleri algıladıkları ortam verilerini bağlı oldukları ve enerjilerini temin ettikleri telefon şebekesi üzerinden aktaran böceklerdir

IP tabanlı CCTV sistemlerine sızma

Lokal kablolu sistemi bulunmayıp, IP adresi vasıtası ile monitöre görüntü yollayan CCTV sistemleri bu anlamda oldukça kolay bir hedefdir.

Bilgisayarlara sızma

Cep telefonlarında olduğu gibi, kişisel bilgisayarlara da internete bağlı olmaları durumunda, wi-fi özelliğinin açık olması durumunda ve bluetooth özelliğinin açık olması durumunda rahatça sızılabilir. Cihaz sahibi casus yazılımla donatılmış bir güvenlik duvarı kullanmıyorsa fark etmeyecektir. Aynı şekilde cihaz sahibi açıldığını bile fark etmeden, uzak erişimle telefonun mikrofon ve kamera özelliği açılabilir. Cihazın tamamen kapalı olması bile bu durumu engellemez. Sonrasında uzaktan erişim

sağlayan kişi mikrofona ortam dinleme ve kamera ile ortam görüntü kaydı yapabilir, bilgisayarın her türlü şifreli ya da şifresiz içeriğine ulaşabilir ve kopyalayabilir. Bilgileri kopyalama yanında bilgisayara veri yükleme de yapabilir.

BÖCEK ARAMASI / DEBUGGING NASIL YAPILIR

Dinleme cihazları çeşitli yöntemlerle çalışmaktadır her yöntem için farklı tarama cihazları ve teknikleri kullanılmaktadır. Dünya standartlarında detektörlerimiz başlıca şu şekildedir.



Spectrum analiz cihazı ortamdaki frekansların analizi yapmaktadır, operatör bu sinyaller üzerinde çalışma yaparak ortamda olası frekans kaynağını tespit etmektedir.



CMP 700 Frekans analiz cihazıyla operatör tüm alanı detaylıca gezerek ederek şüpheli frekans kaynağının yerini tam olarak tespit eder.



Orion Non Liner Dedektör ortama yerleştirilmiş olan tüm elektronik cihazları tespit edebilme yeteneğine sahiptir, dinleme cihazının o anda çalışıp çalışmamasına bakmazsınız tespit edebilmektedir, aktif pasif tüm cihazları bu detektörle tespit edebilmekteyiz.



Termal kamera gizli kamera ve casus böceklerin ısısından tespit etmektedir. Herhangi bir noktaya yerleştirilmiş olan casus dinleme cihazları eğer aktif ise ısı yayacaktır ve termal kamerayla bu ısıyı algılayarak cihazın yerini tespit etmekteyiz.



Rf Tespit cihazları çeşitli frekans hassasiyetlerine sahiptir uhf-vhf gsm gibi çeşitli frekans bandında yayın yapan kablosuz cihazların yerini tespit etmekte kullanılmaktadır.



Gizli Kamera Yakalayıcı

2,4 ve 5,8 Ghz Bandında yayın yapan gizli kamera frekanslarına girerek kameranın aldığı görüntüyü operatör ekranına getirir, bu sayede ortama yerleştirilmiş olan gizli kamera tespit edilir.



Teleskopik yılan kamerayla ulaşılması mümkün olmayan yerlerde fiziksel kontrol yapılmaktadır.

Çalışma Spectrum analiz cihazıyla başlar ve ortamdaki tüm frekanslar incelenir. Tespit cihazlarımızla tüm alan detaylıca gezerek frekans yayan cihaz aranır. Çalışma yapılan ortamda olası wireless modem, telsiz telefon gibi birçok RF verici cihaz vardır. Bu tip cihazlar detaylıca kontrol edilir ve bu frekanslar içerisine kamufle edilmiş cihazlar tespit edilir. Bu noktaya kadar anlatılan yöntemler kablosuz izleme ve dinleme cihazları içindir. Eğer ortama yerleştirilen cihaz kablolu bir cihazsa veya hafızasına kayıt yapabilen bir cihazsa RF detektörlerimiz bu cihazları algılamayacaktır, bunun için non lineer detektör ile tüm alan detaylıca kontrol ederek aktif/pasif tüm cihazlar tespit edilir. Duvar içerisine gömülü dahi olsalar tespitleri mümkündür. Sonrasında termal kamerayla tüm alan detaylıca izlenerek, olası gizli kamera ve dinleme cihazları yaydıkları ısıdan tespit edilir. Bu işlemden sonra gizli kamera tespit cihazıyla olası gizli kamera kontrolü yapılır.

Telefon ve bilgisayarlarda casus yazılım tespiti ve veri kurtarımı

Tarafımızca sağlanan hizmetlerden birisi de telefon ve bilgisayarlarda casus yazılım aranması, bunların silinmesi veya telefonda ya da hard diskte bulunan verilerin kurtarılmasıdır.

Bunun yanı sıra portatif olarak kullanılabilen, cep telefonlarını bloke edecek sistemlerimiz mevcuttur. Mekandaki tüm frekans alışverişini kesmek mümkün olduğu gibi sadece cep telefonlarının mikrofonlarını bloke edecek sistemlerimiz de mevcuttur.

Talep halinde işyerleri veya ikamet personelleri, güvenlik görevlileri, VIP koruma görevlileri, güvenlik profesyonelleri v.s. gibi hedef kitlelere bu tür izleme ve dinleme yöntemleri ve bunlara engel olma konusunda bir eğitim düzenlenebilir. Bu amaçla düzenlenmesi gereken seminer en az 3 saat olmalıdır.



Telefon Analiz

CELLEBRITE-MOBILEDIT



DİNLEME ENGELLEYİCİ

JAMMERSYSTEM-BOXPLUS

Yukarıda belirtmiş olduğumuz hizmetlere ihtiyaç duymanız halinde info@plusecon.com veya **+90 554 5841844** numaralı telefonu arayarak bilgi alabilirsiniz.