Android Stagefright Zafiyeti

written by Mert SARICA | 1 September 2015

Linkedin, Twitter gibi sosyal ağları ve medyayı yakından takip eden biri olarak son zamanlarda Linked’in üzerinden iş odaklı Whatsapp grubu kurma modası oldukça dikkatimi çekiyor. Bu modada, bir kişi Whatsapp üzerinde bir grup açıyor ve bunu Linkedin üzerinde duyuruyor ardından ilgilenen kişiler bu duyurunun altına cep telefonu numaralarını yazarak bu gruba dahil olmak istediklerini söylüyorlar. Grubun kurucusu olan kişi de ardından bu cep telefonu numaralarını teker teker gruba eklemeye başlıyor.


19:07
18%
2 g
İnsan Kaynakları Yöneticisi
İnsan Kaynakları meslektaşlarımızdan oluşan Whatsapp grubumuza katılmak isterseniz, iletişim numaranızı benimle paylaşabilirsiniz. İyi çalışmalar.
18 Beğenme
47 Yorum
+13
Eski yorumları görüntüle ...
2 g
İnsan Kaynakları Yöneticisi
Şuan ekibimiz 46 kişiden oluşuyor. Meslektaşlarımıza faydalı olacağını düşünüyorum.
2 g
İnsan Kaynakları Yöneticisi
İnsan Kaynakları çalışanlarının dışında gelen talepler için malasef olumlu geri dönüş yapamıyorum.
Yorum Yap...

19% 19:05

1 g

Human Resources Manager -

Bey Merhaba, bende gruba katılmak isterim.

1 g

SUPERVISOR /

Merhaba 0538

1 g

İnsan Kaynakları Sorumlusu -

Merhaba 0541

1 g

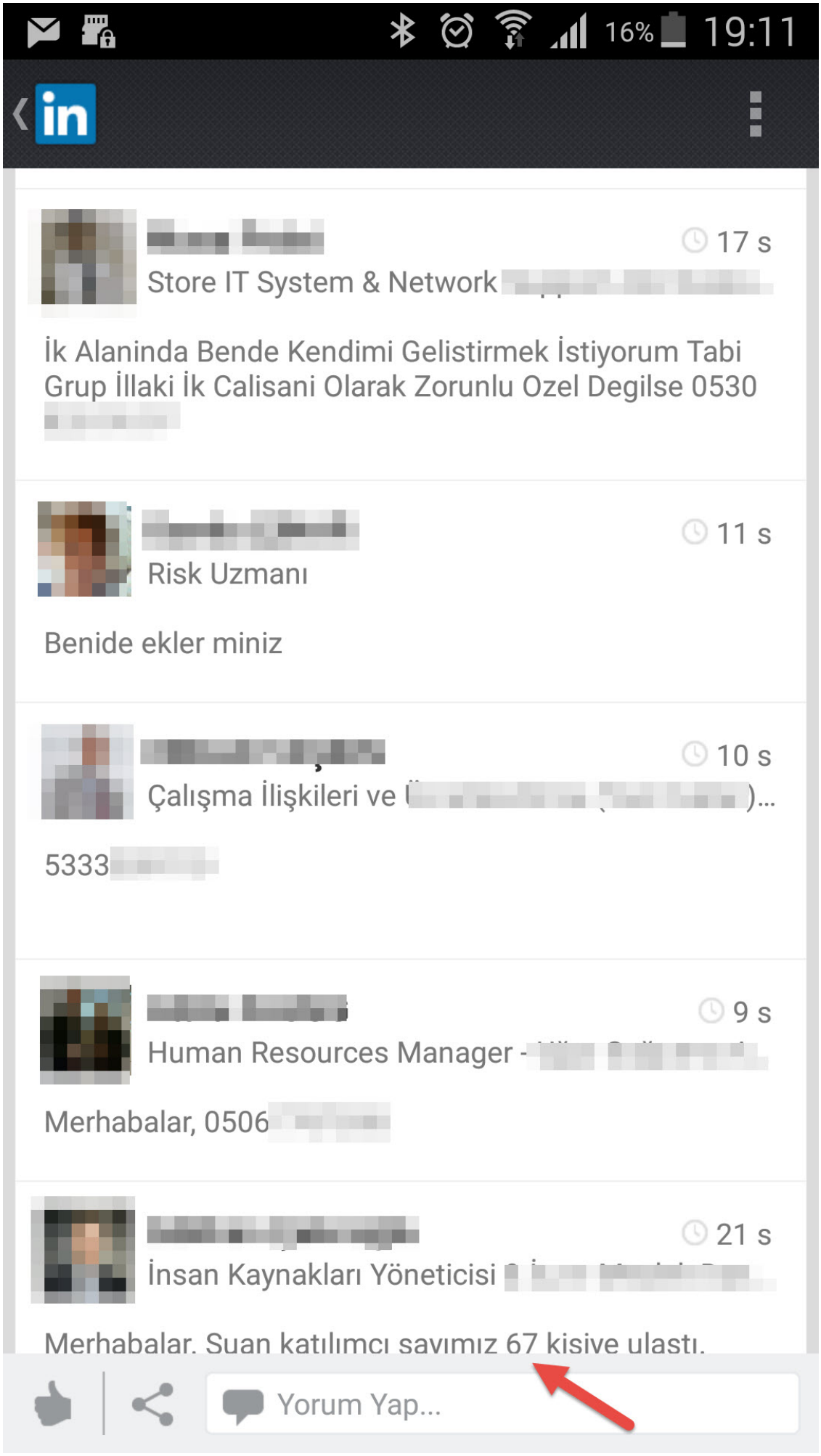
Social Media Manager at

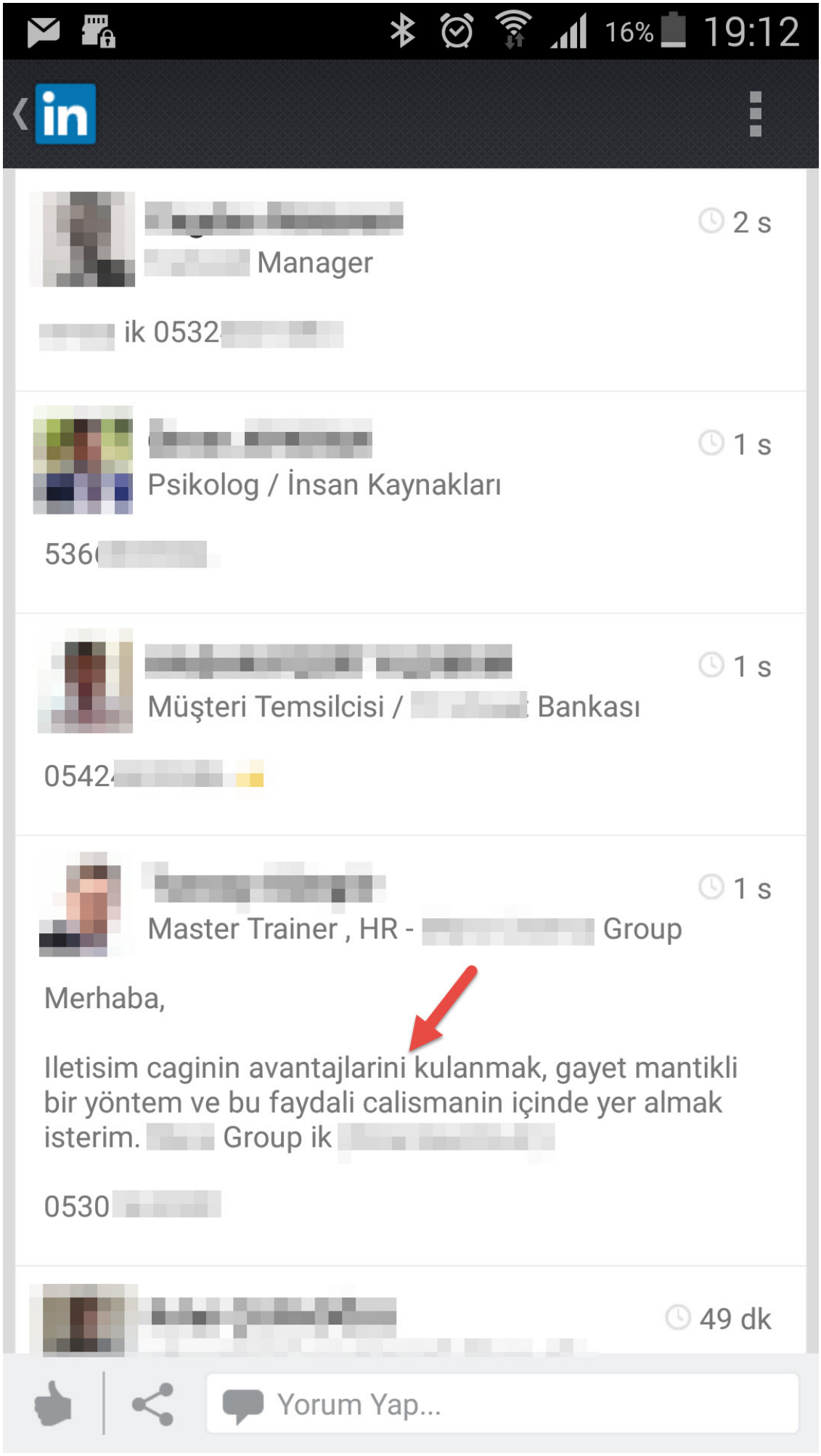
+90536

1 g

GRUBA KATILMAK İSTERİM 0 535

Yorum Yap...


16% 19:11
17 s
Store IT System & Network
İk Alaninda Bende Kendimi Gelistirmek İstiyorum Tabi Grup İllaki İk Calisani Olarak Zorunlu Ozel Degilse 0530
11 s
Risk Uzmanı
Benide ekler miniz
10 s
Çalışma İlişkileri ve
5333
9 s
Human Resources Manager -
Merhabalar, 0506
21 s
İnsan Kaynakları Yöneticisi
Merhabalar. Suan katılımcı sayımız 67 kisiye ulastı.
Yorum Yap...


16% 19:12
2 s
Manager
ik 0532
1 s
Psikolog / İnsan Kaynakları
536
1 s
Müşteri Temsilcisi / Bankası
0542
1 s
Master Trainer , HR - Group
Merhaba,
Iletisim caginin avantajlarini kulanmak, gayet mantikli bir yöntem ve bu faydali calismanin içinde yer almak isterim. Group ik
0530
49 dk
Yorum Yap...

Sorun bunun neresinde diye soracak olursanız birincisi Linkedin iş odaklı kullanılan bir sosyal ağ ve burada çalıştığınız kurumdan, pozisyonunuza kadar işiniz ve işyeriniz ile ilgili çeşitli bilgiler paylaşıyorsunuz. Kurumları hacklemek isteyen art niyetli kişilerin, istihbarat servislerinin, kurum çalışanlarını hedef aldığını biliyoruz. En yakın örnek olarak Edward Snowden tarafından sızdırılan belgelerde, ABD istihbarat servisi NSA ile İngiliz siber istihbarat servisi GCHQ'nun, 2010 yılında sim kart şifreleme anahtarlarını çalmak için sim kart üreticisi Gemalto firmasının çalışanlarının e-posta ve Facebook hesaplarına sızdıkları anlaşılmıştı. 2015 yılında neler yaptıklarını hayal bile edememekle birlikte, istihbarat servisleri dışında art niyetli kişilerin de akıllı telefonları hatta ve hatta akıllı saatleri bile hedef aldığını görüyoruz.

Eskiden olsaydı, telefon numaranızı internette ve/veya herhangi bir ortamda paylaştığınızda başınıza gelebilecek en kötü şey olsa olsa gecenin köründe sizi rahatsız eden bir telefon sapığı olurdu. Ancak bu çağda başınıza gelebilecek en kötü şey, telefonunuzu hackleyen (Evil Pi başlıklı yazımda zafiyet barındıran Android telefonların nasıl istismar edilebileceğini simüle etmiştim.) ve tüm kişisel verilerinizi çalan bir art niyetli kişi olabilir.

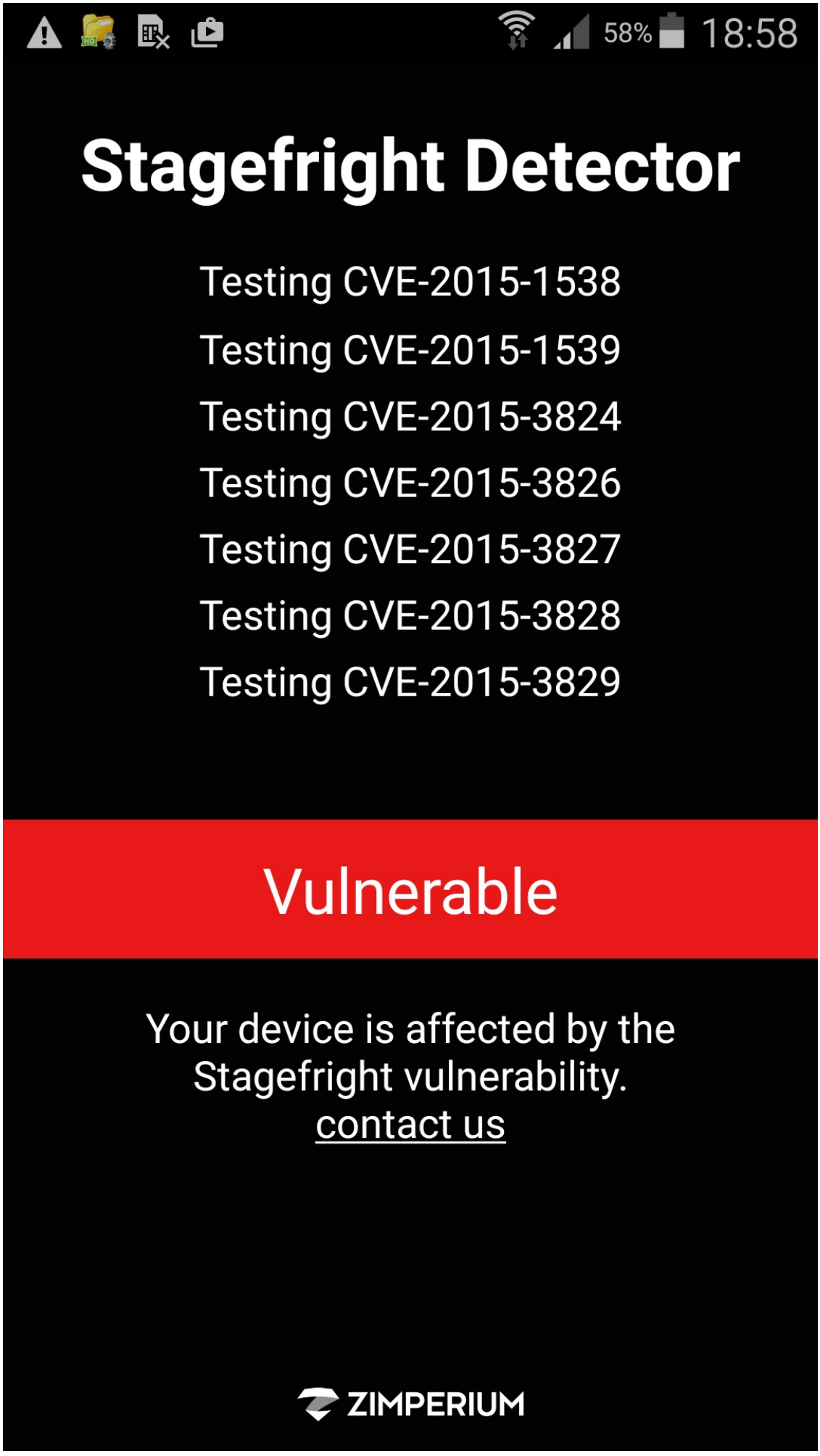
5 Ağustos 2015 tarihinde gerçekleştirilen Black Hat bilgi güvenliği konferansında, Joshua Drake (@jduck) tarafından 950 milyon Android cihazı etkileyen bir zafiyetin detaylarına yer verildi. Bu zafiyeti istismar etmek (cep telefonunu/tableti hacklemek) için hedef kişinin cep telefonunu bilmek ve istismar kodu içeren bir multimedya mesaj veya mp4 formatına sahip bir video dosyasının bağlantı adresini göndermek yeterli oluyor.

Android işletim sistemi için yamalar bildiğiniz üzere Google tarafından hemen yayınlansa da, telefonunuza indirilebilmeniz için cihaz üreticisi (misal Samsung) tarafından güncelleme yazılımının hazırlanması gerekiyor. Durum böyle olunca da Google ilgili zafiyeti ortadan kaldıran yamayı zafiyetin tespitinden bir gün sonra yayınlasa bile üreticinin de elini çabuk tutması gerekiyor.

Her ne kadar Google ilgili yamayı yayınlasa da bu defa da yamanın aslında zafiyeti ortadan kaldırılmadığı Exodus firmasının yaptığı bir araştırma ile

ortaya çıktı. En iyi ihtimalle Eylül ayından önce bu yamayı Android cihazımıza yükleyemeyeceğiz gibi görünüyor.

Peki elimizi kolumuzu bağlayıp bekleyecek miyiz ? Hayır. İlk olarak Android cihazımızın bu zafiyetten etkilenip etkilenmediğini StageFright Detector aracı ile öğrenebiliriz.


58% 18:58
Stagefright Detector
Testing CVE-2015-1538
Testing CVE-2015-1539
Testing CVE-2015-3824
Testing CVE-2015-3826
Testing CVE-2015-3827
Testing CVE-2015-3828
Testing CVE-2015-3829
Vulnerable
Your device is affected by the Stagefright vulnerability.
contact us
ZIMPERIUM

İkinci olarak her ne kadar MMS, atak vektörlerinden sadece biri de olsa, en kolay istismar edilebileceği için buradan gelecek bir saldırıyı engellemek için size gönderilen MMS'in Android cihazınız tarafından otomatik olarak almasını engellemek isteyebilirsiniz. (Bunu devre dışı bıraksanız bile, manuel olarak gelen MMS'i alıp görüntülediğiniz taktirde cihazınızın hacklenebileceğini unutmayın!)

MMS'in otomatik alması ve gösterilmesini devre dışı bırakmak için aşağıdaki adımları izleyebilirsiniz.

Android için; Ayarlar -> Mesaj -> Multimedya mesajları -> Otomatik al
Google Hangout için; Hangout -> Ayarlar -> SMS -> MMS'leri otomatik al

Samsung kullanıcısı iseniz MMS'i devre dışı bırakmak için Samsung tarafından yayınlanan MMS control uygulamasını da yükleyebilirsiniz.

Yukarıdaki adımlar bir yama gibi bu zafiyeti tamamiyle ortadan kaldırmayacağı için ve Google firması Android 4.0 "Ice Cream Sandwich" ile gelen ASLR (address space layout randomization) güvenlik önlemi sayesinde bu zafiyetin çok sayıda cihazda istismar edilmesinin zor olduğunu söylese de, yama çıkana kadar dikkatli olmakta fayda var.

Sonuç itibariyle, akıllı cihazlarda ortaya çıkan zafiyetleri istismar etmek için kimi zaman sadece cep telefonu numarasının yeterli olması, kurumlara sızmak isteyen art niyetli kişilerin kurum çalışanlarını hedef alması ile sonuçlanabiliyor bu nedenle cep telefonu numaranızı paylaşırken bile temkinli olmakta fayda olduğunu asla unutmayın.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Güncelleme: 09.09.2015 tarihi ile cve-2015-1538 zafiyeti için istismar kodu yayınlanmıştır.