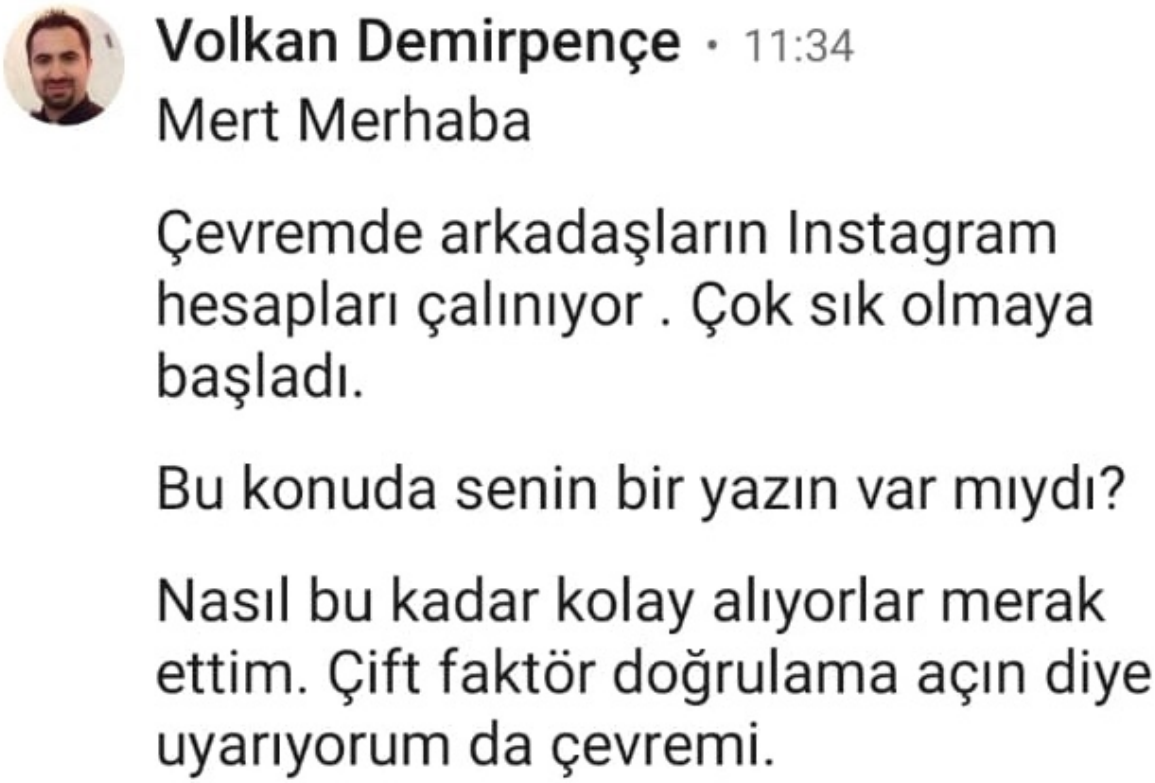
Instagram Dolandırıcıları

written by Mert SARICA | 1 December 2021
If you are looking for an English version of this article, please visit here.

Daha önce Sponsorlu Dolandırıcılık, LinkedIn Dolandırıcıları, Profilime Kim Baktı ? başlıklı blog yazılarımı okuyanlarınız, sosyal medya mecralarının dolandırıcılar tarafından etkin bir şekilde kullanıldıklarını öğrenmişti. Bu yazıları yazdıktan sonra zaman içinde beni en çok şaşırtan ise aradan neredeyse 2 yıl geçmesine rağmen özellikle LinkedIn Dolandırıcıları başlıklı blog yazıma gelen yorumlardan dolandırıcıların faaliyetlerine hala hız kesmeden devam ettiğini öğrenmem oldu.

Bu konu özelinde üç yazı yazdıktan sonra kendimi nadasa bırakmaya karar vermişken 2021 yılının Eylül ayında LinkedIn üzerinden Volkan DEMİRPENÇE'den aldığım aşağıdaki mesaj karşısında kayıtsız kalmamaya karar vererek eşe, dosta haber salıp Instagram üzerinden aldıkları şüpheli mesajları benimle paylaşmalarını rica ettim.



Gel zaman, git zaman, elime ulaşan oltalama mesajlarını inceleyip, Instagram

hesaplarını nasıl hacklediklerini öğrendikten sonra Volkan gibi arkadaşlar için bu konuyu farkındalık yaratma adına kaleme almaya karar verdim.

Oltalamala mesajlarından birinde dolandırıcı, Facebook üzerinden Messenger ile Telif Hakları isimli hesap üzerinden Instagram kullanıcısına mesaj atarak telif hakkı ihlali yapıldığını belirterek kullanıcının hesabını doğrulaması için paylaşımlı 116[.]202[.]53[.]12 ip adresine sahip userhelpconfirm[.]site-tr[.]site web adresini ziyaret etmesini ve bir form doldurmasını talep ediyordu.

Telif Hakları
Bugün aktif

Telif Hakları
Facebook

Profili Gör

Dün 22:24

İnstagram telif hak ihlali !

Güvenliğiniz bizim sorumluluğumuz.

Hesap incelendi ve telif ihlali gerçekleştirdiği anlaşıldı.

Hesabınızı doğrulamadığınız taktirde 24 saat içinde hesabınız tarafımızca askıya alınacaktır. Ortaklığımızı devam ettire bilmemiz için hesabın kullanıcısı olduğunuzu doğrulamamız gerekmektedir.

Hesabınız bu şartlar yerine getirildikten sonra , bir doğrulama kodu gönderilerek güvenli hale getirilecektir. Verilen formda gerekli bilgileri doldurarak ortaklığınızı devam ettirebilirsiniz. Doğrulama kodunuz, formu doldurduktan sonraki 24 saat içinde hesabınıza tarafımızca gönderilecektir.

Form: **https://userhelpconfirm .site-tr.site/**

© Instagram. Facebook Inc., 1601 Willow Road, Menlo Park, CA # 94025
- [ ]



Verified Badges | Help Center
Merhaba, Hesabınız telif haklarını ihlal ettiği gerekçesiyle 24 saat içinde Kapatılacaktır. Bunun Bir Hata Olduğunu Düşünüyorsanız İ...

Ara

Telif Hakları

Arkadaşı Ekle | Mesaj | ...

... Telif'in Hakkında Bilgilerini Gör

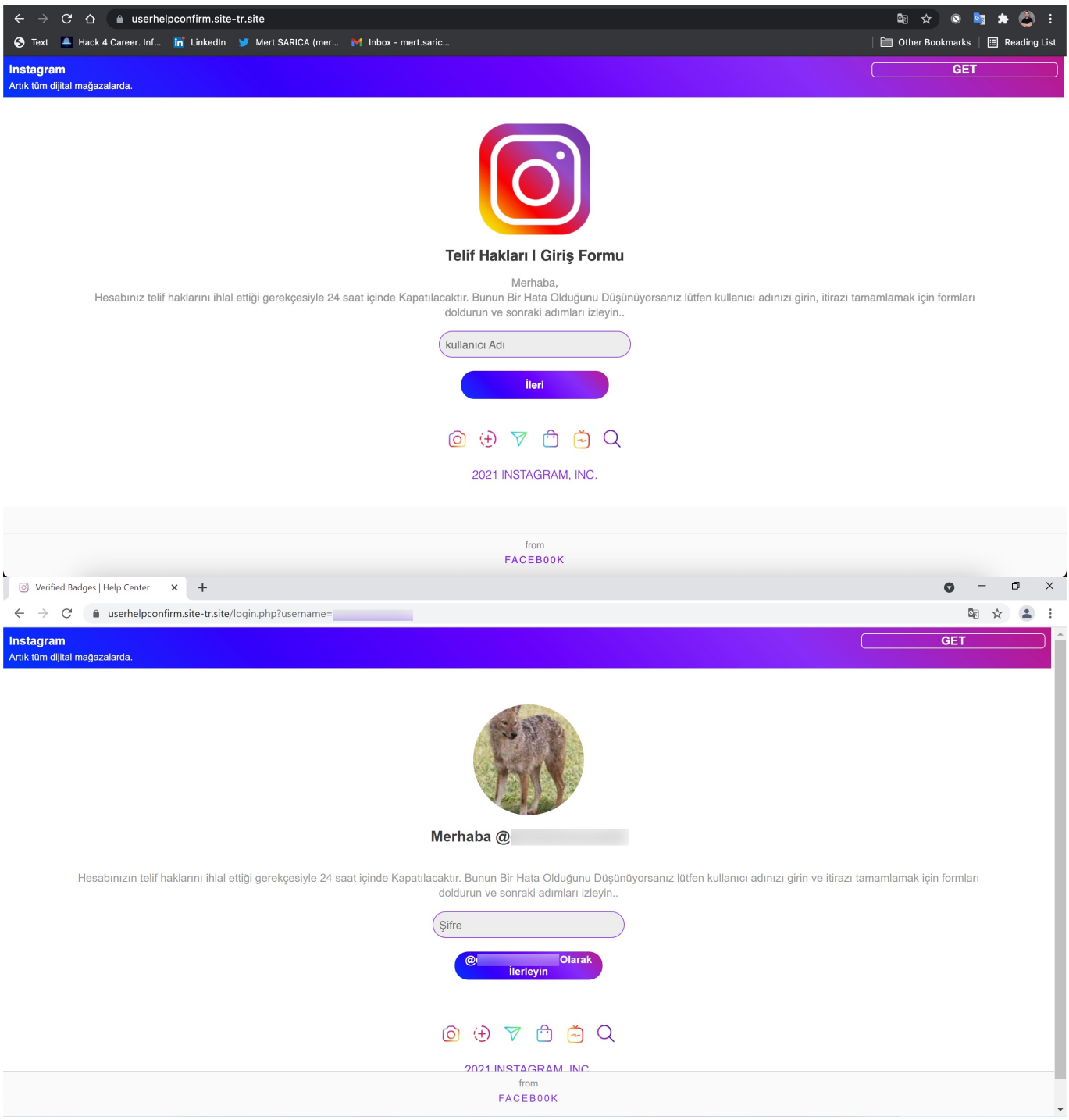
Arkadaşlar

Gönderiler

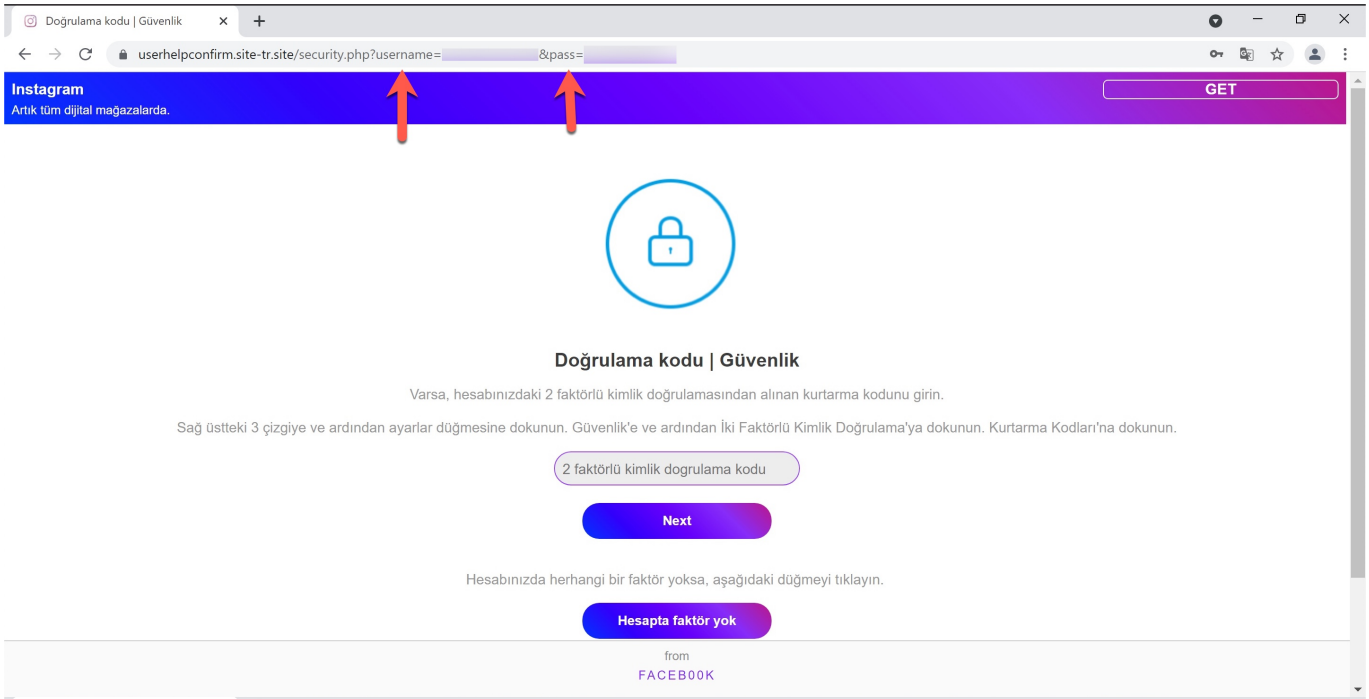
Fotoğraflar

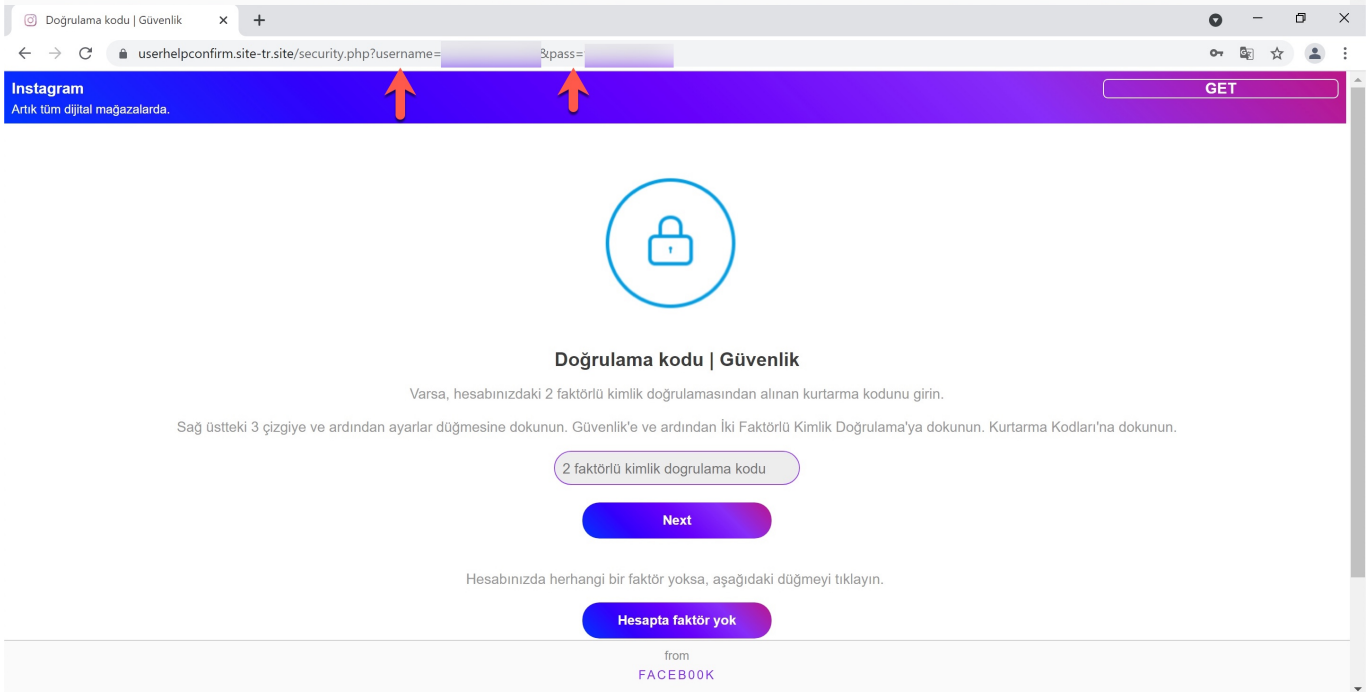
Telif Hakları profil resmini güncelledi.
31 Ağu, 23:08 •

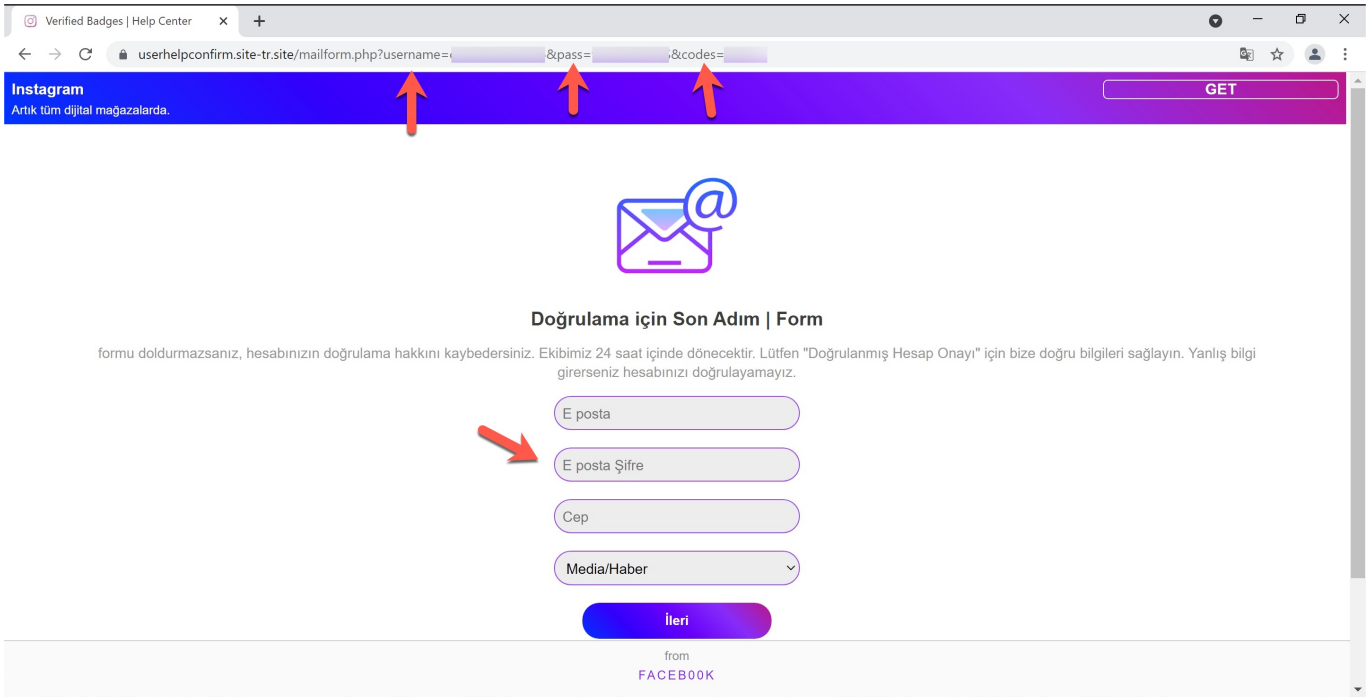
Web sayfasına Instagram kullanıcı adı girildiği anda inandırıcılığı arttırmak için parola istenen sayfada dumpor.com web sitesi üzerinden kullanıcının profil resmi de arka planda indirilip, gösteriliyordu.



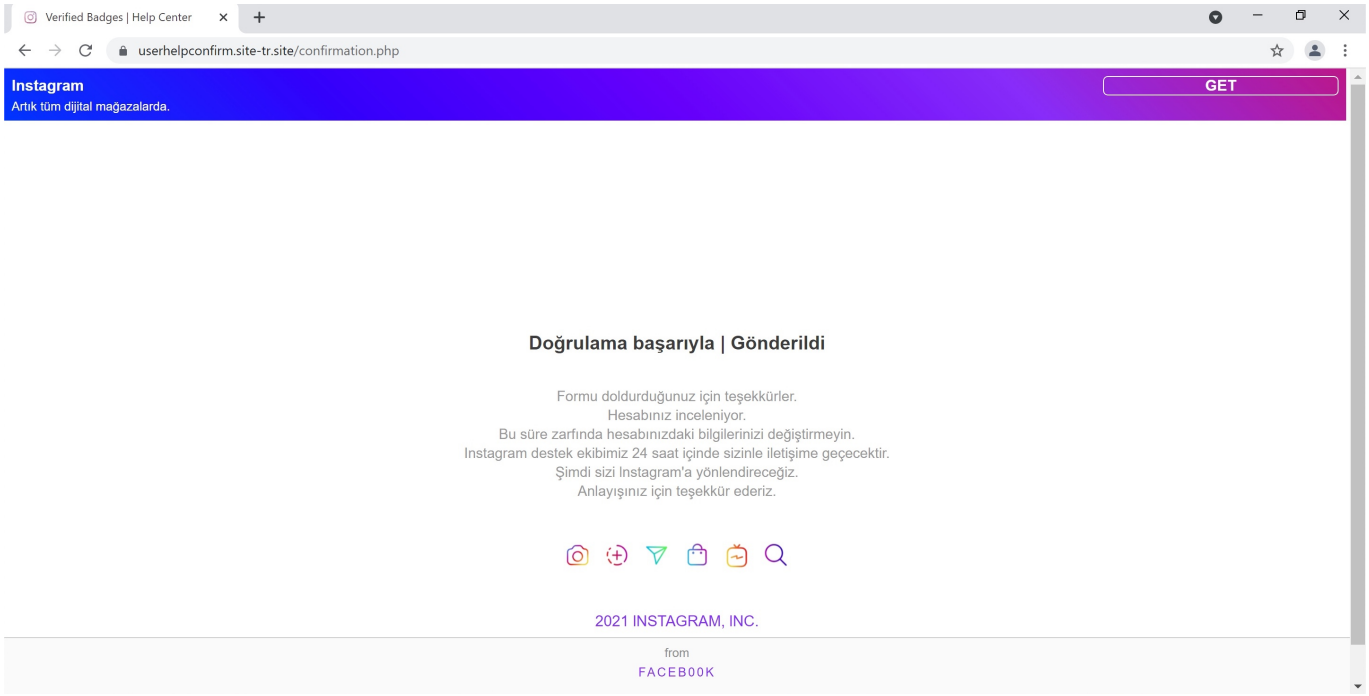
Şayet hesap iki faktörlü kimlik doğrulaması ile korunuyorsa (kullanmanızı şiddetle tavsiye ediyorum), oltalama sayfası doğru parola girildikten hemen sonra kullanıcıdan doğrulama kodunu (sms veya giriş kodu) ve yetmezmiş gibi bir de üzerine e-posta adresini ve parolasını girmesini istiyordu.


Doğrulama kodu | Güvenlik
userhelpconfirm.site-tr.site/security.php?username=&pass=
Instagram
Artık tüm dijital mağazalarda.
GET
Doğrulama kodu | Güvenlik
Varsa, hesabınızdaki 2 faktörlü kimlik doğrulamasından alınan kurtarma kodunu girin.
Sağ üstteki 3 çizgiye ve ardından ayarlar düğmesine dokunun. Güvenlik'e ve ardından İki Faktörlü Kimlik Doğrulama'ya dokunun. Kurtarma Kodları'na dokunun.
2 faktörlü kimlik dogrulama kodu
Next
Hesabınızda herhangi bir faktör yoksa, aşağıdaki düğmeyi tıklayın.
Hesapta faktör yok
from
FACEB00K


Doğrulama kodu | Güvenlik
userhelpconfirm.site-tr.site/security.php?username=&pass=
Instagram
Artık tüm dijital mağazalarda.
GET
Doğrulama kodu | Güvenlik
Varsa, hesabınızdaki 2 faktörlü kimlik doğrulamasından alınan kurtarma kodunu girin.
Sağ üstteki 3 çizgiye ve ardından ayarlar düğmesine dokunun. Güvenlik'e ve ardından İki Faktörlü Kimlik Doğrulama'ya dokunun. Kurtarma Kodları'na dokunun.
2 faktörlü kimlik dogrulama kodu
Next
Hesabınızda herhangi bir faktör yoksa, aşağıdaki düğmeyi tıklayın.
Hesapta faktör yok
from
FACEB00K



Tüm bilgiler girildikten sonra ise dolandırıcılar Instagram hesabını ele geçirmek ve kötü emellerini gerçekleştirmek için tüm bilgileri elde etmiş oluyordu. Bundan sonra yapabilecekleri artık hayal gücümüz ile sınırlı olsa da tam olarak niyetlerini anlamak ve dolandırıcılar tarafından kullanılan sistemin IP adresleri elde etmek için sahte bir Instagram hesabı oluşturup bilgilerimi bu sayfaya girip hesabımı hacklemelerini beklemeye başladım ancak büyük ihtimalle takipçi sayımın az olması sebebiyle ilgilerini çekmeyi başaramadığım için hesabıma giriş yapmalarını sağlayamadım.



Bir yandan bazı okurlarımın “E peki Mert, bu oltalama mesajlarına kim inanır

ki ?” dediğini duyar gibiyim. Ben de aynı şekilde bu soruyu kendi kendime sorup yanıtını bulmak için oltalama mesajlarını bir süre daha incelemeye devam ettim.

Bir diğer oltalama saldırısında ise bu defa oltalama sitesinin güvenlik kontrollerine yakalanmaması için çok daha temkinli olan, ikna adına tatlı dil kullanmaktan çekinmeyen ve bir o kadar da şeytani emellerini gerçekleştirmek için “Kadına Şiddete Hayır” gibi toplumun oldukça hassas olduğu bir konuyu senaryosunda kullanmaktan imtina etmeyen soğuk kanlı bir dolandırıcı ile karşılaştım.

21 Ekim tarihinde sahte isim, soyad ve profil fotoğrafı ile gamzedemirel.avk hesabının arkasına gizlenip hedef kullanıcı ile iletişime geçen avukat kılığına girmiş olan dolandırıcı, kadınlara ve çocuklara uygulanan şiddete karşı sonsuz bir mücadele içinde olduğunu ve 2 dakika görüşmek istediğini belirtmekteydi.

gamzedemirel.avk



Gamze Demirel

gamzedemirel.avk · Instagram

4,5 B takipçi · 52 gönderi

Seni takip ediyor

Profili Gör

21 Eki 11:24

[redacted] merhaba iyi günler rahatsızlık vermiyorum umarım

21 Eki 16:17

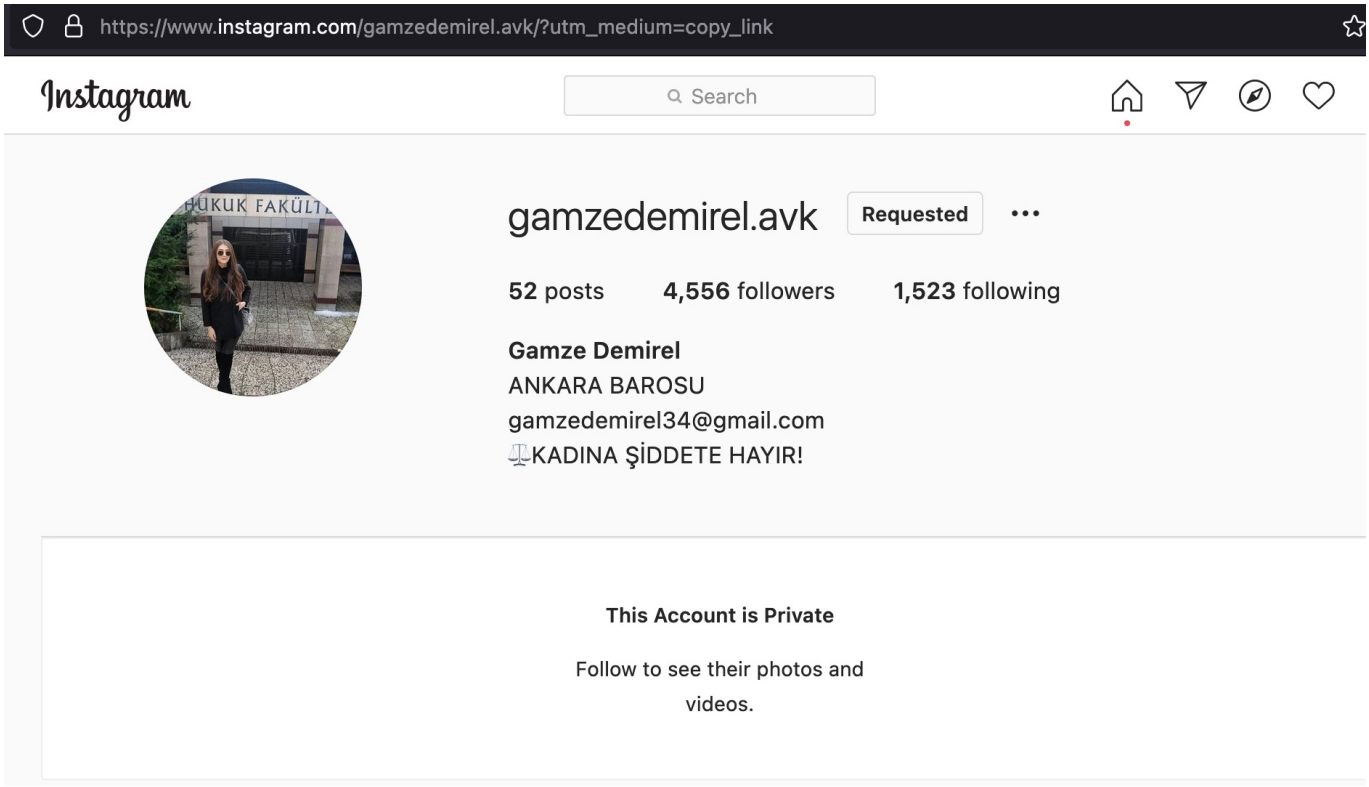
[redacted]

Türkiyede son dönemlerde kadınların ve çocukların hedef olduğu şiddet olaylarını haberlerde izliyorsunuzdur mutlaka, bu durumlara farkındalık yaratmak için devlet kadınlarımız ve çocuklarımızın yanında olmak adına bir destek platformu oluşturduk. Sizde katılıp destek verirseniz en azından manevi anlamda yanımızda durursanız bizi çok mutlu edersiniz. Kadınlara ve çocuklara uygulanan şiddetin her türlüsüne karşı bir avukat olarak sonsuz bir mücadele içindeyim adı geçen her failin en yüksek cezayı almasi için elimden gelen gayreti göstermekteyim. Sizden ricam sadece birkaç dakikanızı ayırmanız

[redacted]

Duyarlı olduğunuz için minnettarım size,duyarlı olmak,bilinçi olmak, hayvana, kadına şiddete her türlü şiddete dur demek ve bunu yapanlara en yüksek mertebeden cezalar vermek için mücadelemiz 2 dk vaktinizi ayıracağınız için çok teşekkür ederim 🙏🥰

21 Eki 18:25



Aradan 6 gün geçtikten sonra hedef kullanıcıdan yanıt almadığını farkeden dolandırıcı, 26 Ekim tarihinde tekrar iletişime geçip destek verenler arasında hedef kullanıcının adını göremediğini ve destek için Cloudflare arkasına gizlenen kadinlaradestek[.]com/home.php web sitesi üzerinden destek istediğini paylaşmaktaydı.

gamzedemirel.avk

teşekkür ederim 🙏🥰

21 Eki 18:25

🙏

Bugün 11:19

https://www.kadinlaradestek.com/home.php



Kadın Şiddetine Hayır

Kadına şiddet insanlık suçudur! Kadına yönelik her türlü şiddetin karşısında, şiddet mağduru kadınlarımızın da her zaman yanı...

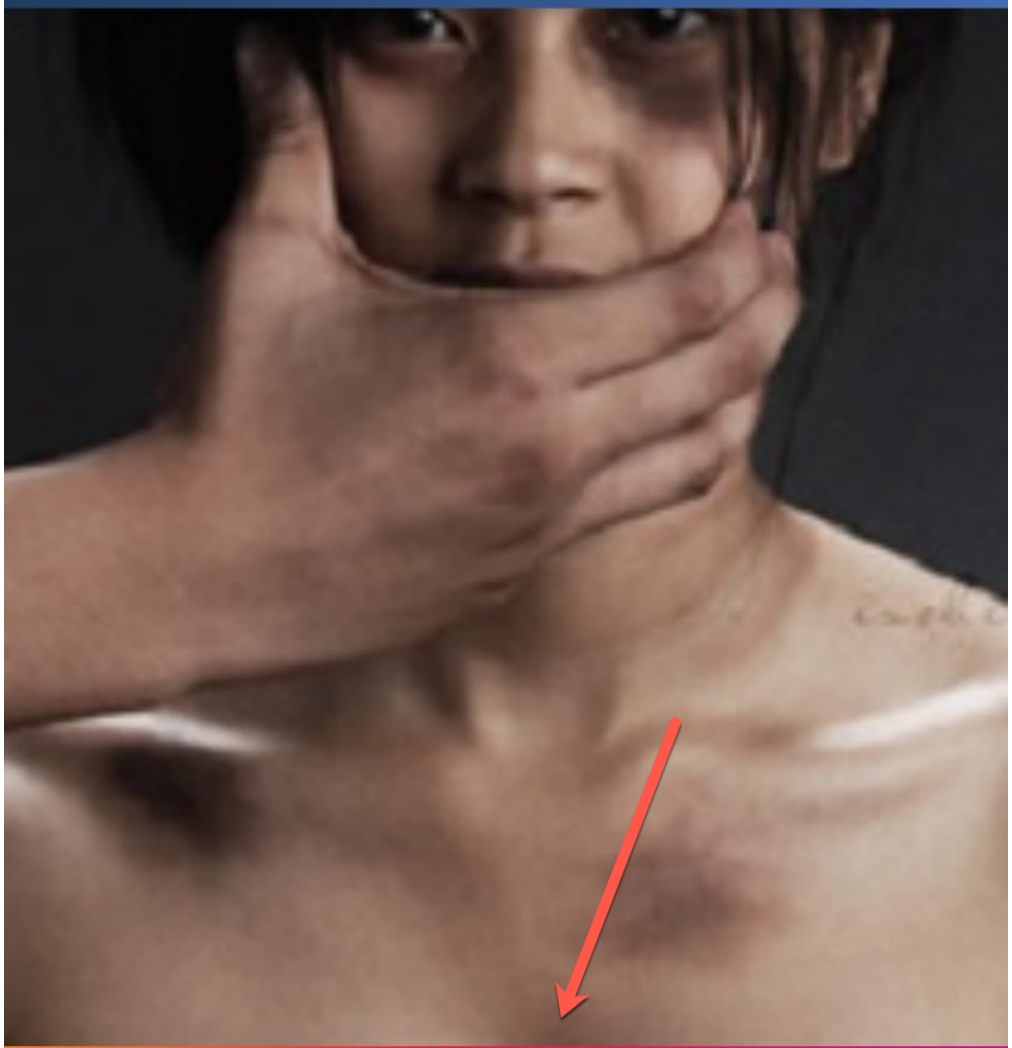
Merhaba iyi günler efendim listede adınızı göremedim destek olmamışsınız da, umarım bu duruma duyarsız kalmayıp desteğinizi gerçekleştirirsiniz. Kampanyamızın süresinin dolmasına çok az bir süre kaldı😊🙏

kadinlaradestek.com/ho

30

KADINA ŞİDDETE DUR!

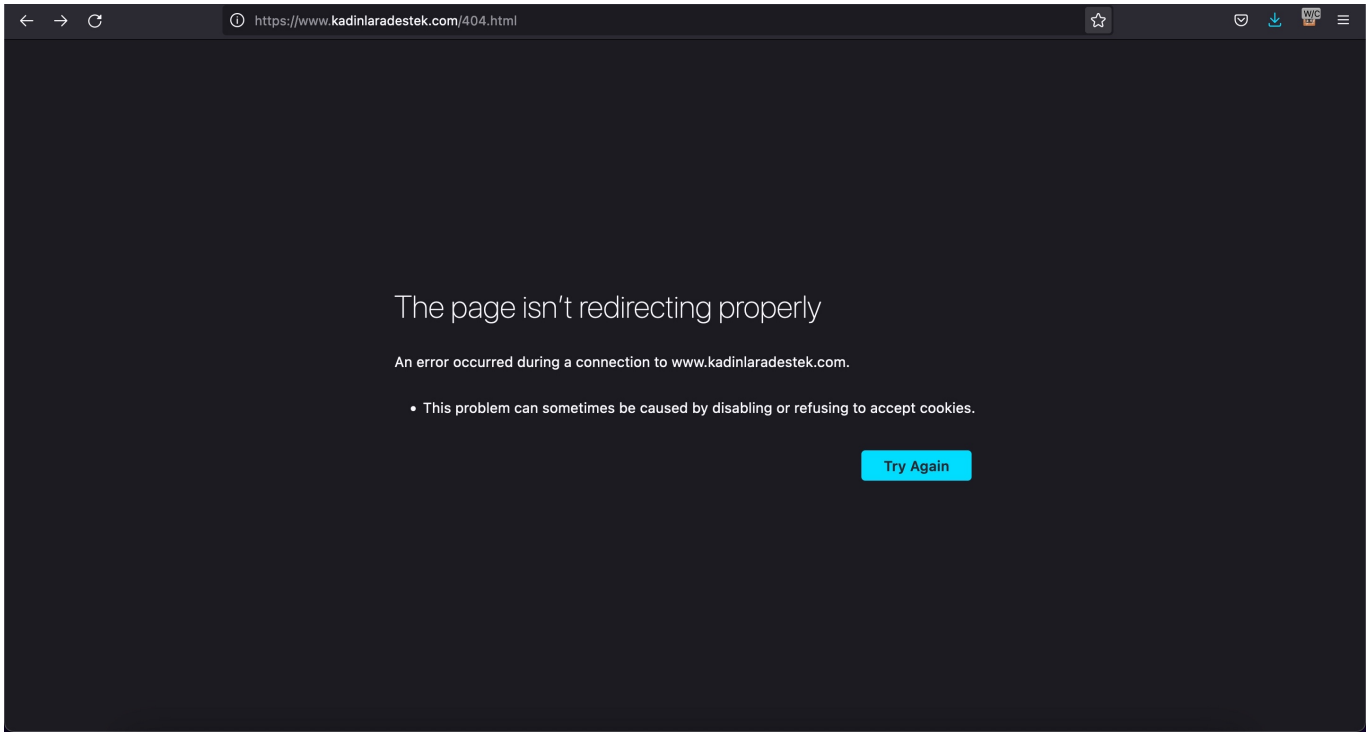
Kadına şiddet insanlık suçudur! Kadına yönelik her türlü şiddetin karşısında, şiddet mağduru kadınlarımızın da her zaman yanındayız. Destek olarak bizlere katıl!

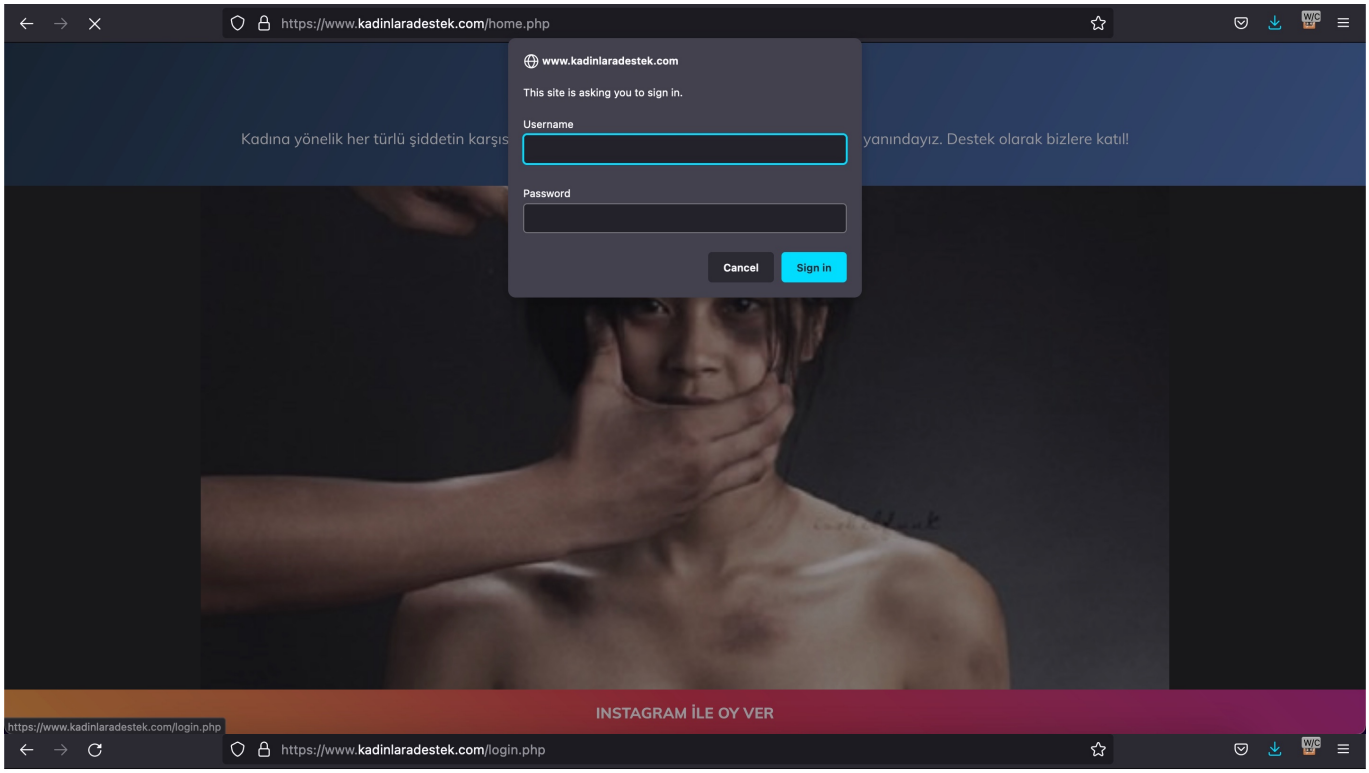


INSTAGRAM İLE OY VER

Web sitesini ziyaret ettiğimde, dolandırıcının uzun bir süre operasyonuna devam edebilmek için çeşitli teknik tedbirler aldığını farkettim. İlk olarak https://kadinlaradestek[.]com adresine direkt gitmeye çalıştığımda web sitesi 404 (sayfa bulunamadı) hata döngüsüne girerek açılmamaktaydı. Siteye ulaşabilmek için direkt https://kadinlaradestek[.]com/home.php adresini ziyaret etmek gerekiyordu.

Dikkatimi çeken bir diğer nokta ise Instagram özel mesajı üzerinden siteye gittiğinizde sayfanın altında yer alan INSTAGRAM İLE OY VER butonuna bastığınızda bilgilerinizi https://kadinlaradestek[.]com/login.php sayfası üzerinden çalan bir form ile karşılaşıyordunuz ancak bunun aksine https://kadinlaradestek[.]com/login.php adresine direkt internet tarayıcısı üzerinden gitmeye çalıştığınızda bu defa form yerine kullanıcı adı ve parola isteyen bir kutucukla karşılaşıyor, CANCEL butonuna bastığınızda ise sahte bir hata sayfası ile karşılaşıyordunuz. Kısaca dolandırıcı bu tür oltalama sitelerinin siber güvenlik firmaları tarafından tarama araçları ile tespit edilmesini engellemek için çeşitli tedbirler aldığı net olarak görülüyordu.





{ "error": { "message": "You did not provide an API key. You need to provide your API key in the Authorization header, using Bearer auth (e.g. "Authorization: Bearer YOUR_SECRET_KEY"). See https://stripe.com /docs/api#authentication for details, or we can help at https://support.stripe.com/.", "type": "invalid_request_error" } }

Avına odaklanmış bir aslan misali hedef aldığı kullanıcının bilgilerini çalıp çalamadığını yakından takip eden dolandırıcı 28 Ekim ve 1 Kasım tarihlerinde tekrar iletişime geçmişti.

Per 11:07

Merhabalar, zamanınız olmadı galiba

Per 12:18



Tamam efendim

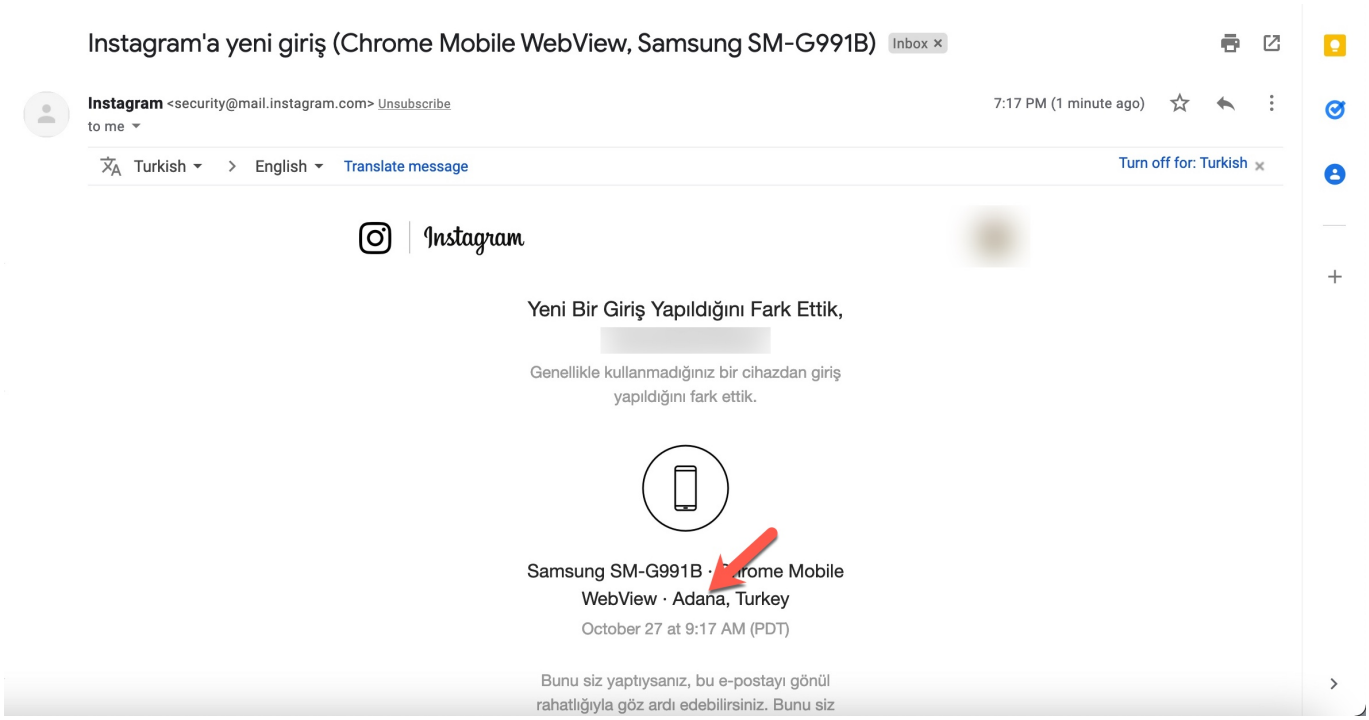
Bugün 15:09

Sizi rahatsız ediyorum sürekli kusura bakmayın

Müsaitliğiniz sağlanmadı galiba

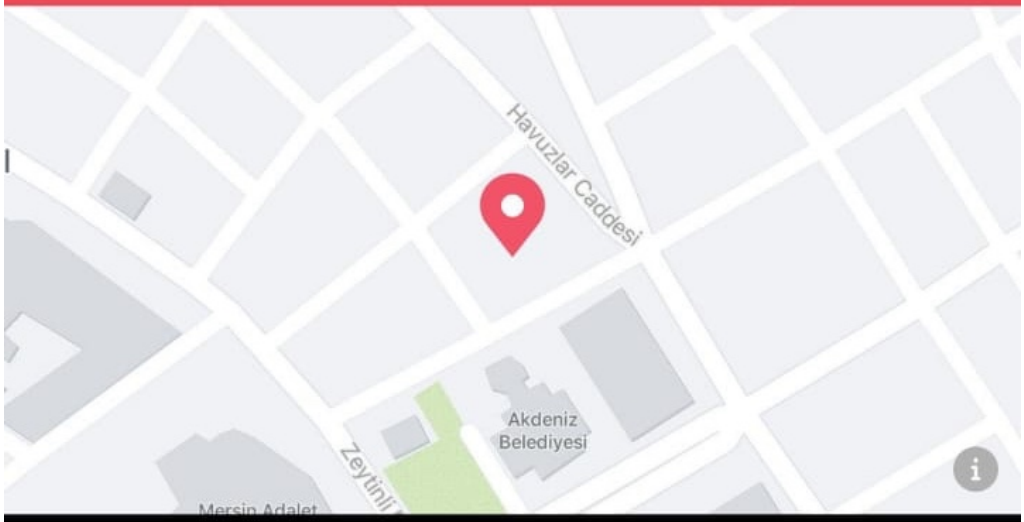
Mesaj...

Daha önce olduğu gibi dolandırıcının niyetini anlamak ve IP adresini elde etmek için oluşturduğum sahte Instagram hesabının bilgilerini bu sayfada yer alan forma belli zaman aralıklarında girip hesabımı hacklemelerini beklemeye başladım. Bilgilerimi girer girmez Adana ve Mersin'den hesabıma giriş yapıldığına ve iki faktörlü kimlik doğrulamasının kapatıldığına dair Instagram'dan uyarı mesajları aldım. İşlemlerin dolandırıcılar tarafından bu kadar hızlı gerçekleştirilmesi, arka planda çalınan bilgilerin bir betik (script) yardımı ile otomatik bir şekilde gerçekleştirildiğine işaret ediyordu.



Instagram

Şüpheli Giriş Denemesi



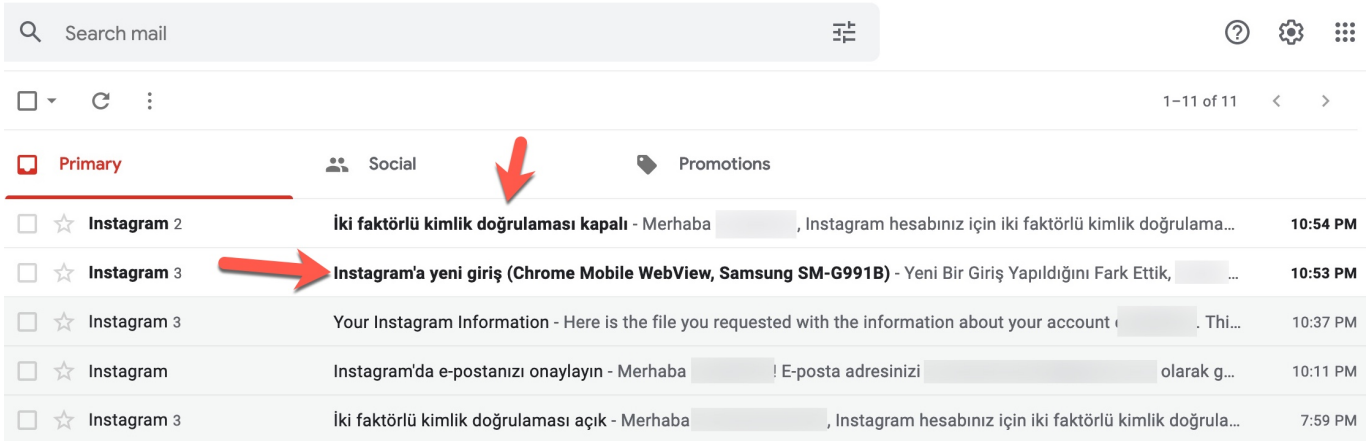
Olağandışı Bir Giriş Denemesi Saptadık

Android | 27.10.2021 22:01
Mersin

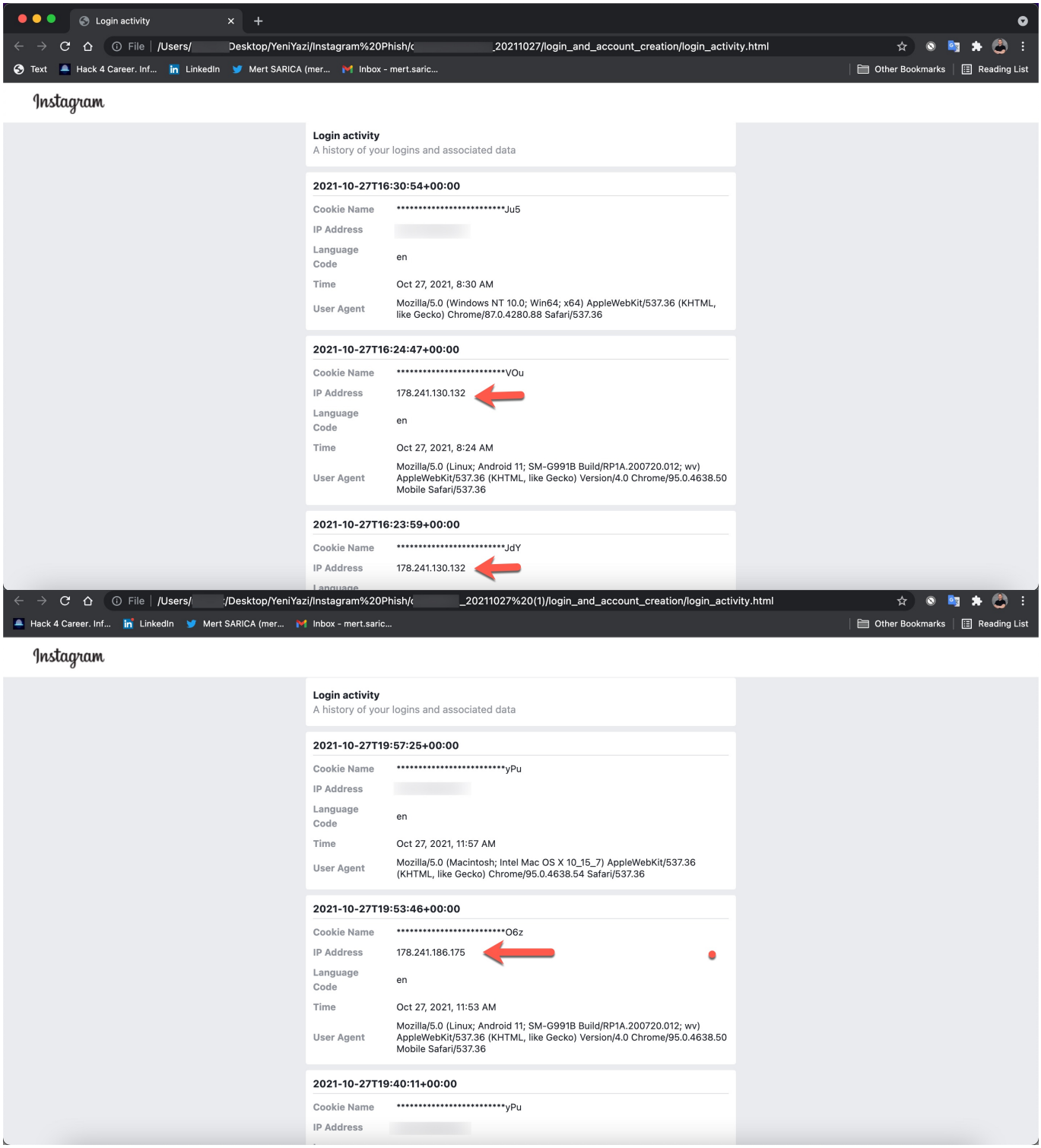
Hesabını güvene almak için bunu yapanın sen olduğunu bize bildir.

Bunu Ben Yapmadım

Bunu Ben Yaptım

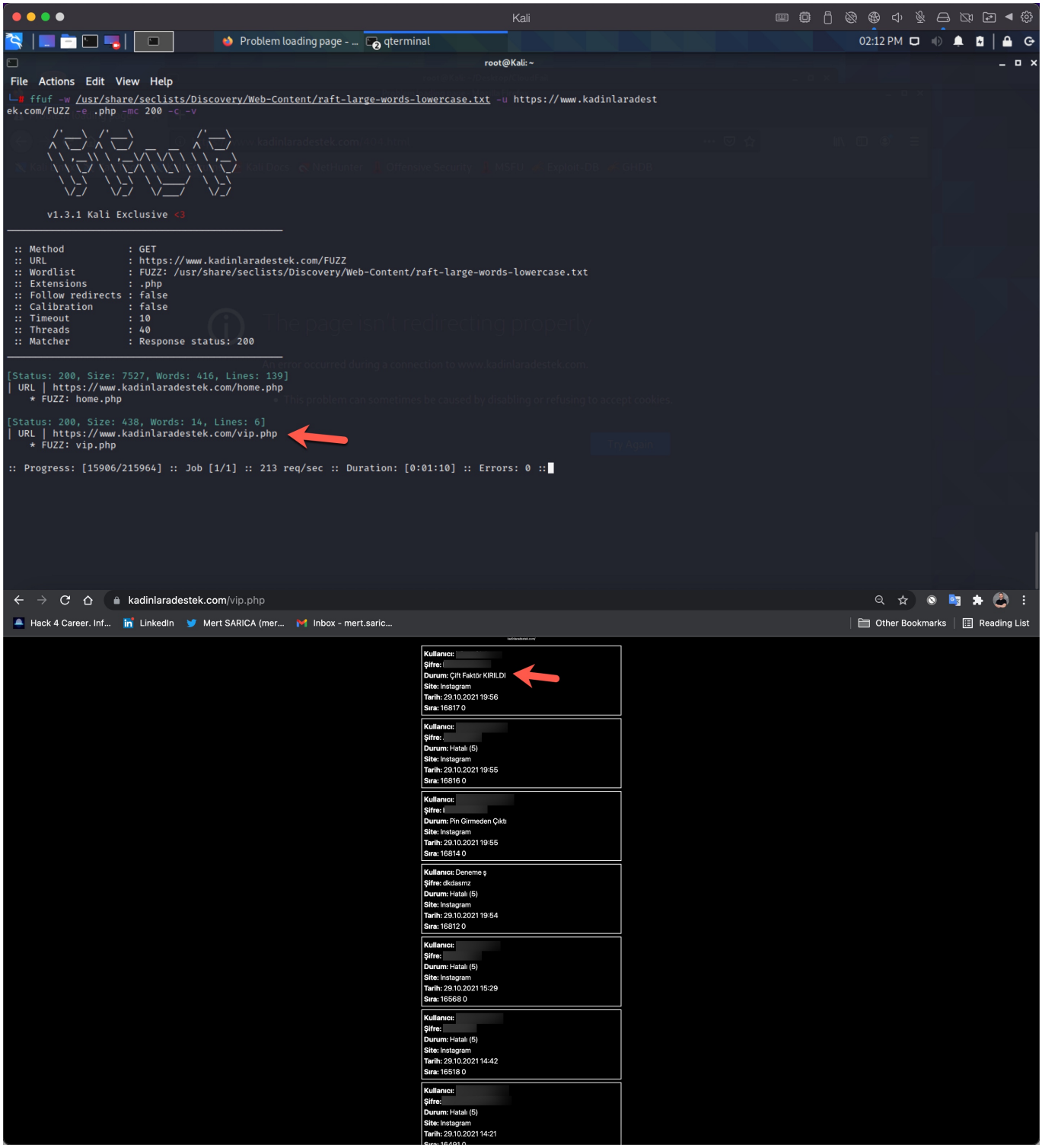


Sıra giriş yapan dolandırıcıların IP adreslerini bulmaya geldiğinde öncelikle Instagram mobil uygulamasında Ayarlar -> Güvenlik -> Verileri İndir adımlarından Instagram hesabım ile ilgili bilgileri talep etmem gerekiyordu. Bilgilerin hazır olduğuna dair Instagram'dan e-posta aldıktan sonra ilgili ZIP dosyasını indirdim. ZIP dosyasını açtıktan sonra login_and_account_creation klasöründeki login_activity.html dosyasına baktığımda dolandırıcıların her defasında Turkcell'e ait farklı, dinamik IP adresinden hesabıma eriştiğini gördüm. IP adreslerini incelediğimde 178.241.130.132 IP adresinin Diyarbakır IP havuzuna, 178.241.186.175 IP adresinin ise Kayseri IP havuzuna ait olduğunu gördüm. IP adreslerinin dinamik olup, her defasında değişiyor olması arka planda rootlanmış bir telefon, mobil cihaz üzerinden bu işlemlerin betik yardımı ile gerçekleştirildiği ihtimalini gündeme getiriyordu. Dolandırıcıların Instagram hesabına giriş yaptıktan sonra parolayı değiştirmemesi ise hackledikleri hesaplara uzun süreli erişmek ve emellerini gerçekleştirmek için kullanmak istediklerine işaret ediyordu.



Son olarak sıra bu dolandırıcıların oltasına düşen masum kullanıcıları tespit etmeye geldiğinde, ofansif güvenlik uzmanlarının da yakından bildiği ffuf aracı ile web sitesindeki PHP dosyalarını keşfetmek için işe koyuldum. Çok geçmeden ffuf aracı web sitesi üzerinde vip.php isimli bir dosya olduğunu tespit etti. Bu dosyanın bulunduğu https://kadinlaradestek[.]com/vip.php web adresini ziyaret ettiğimde ise 26 Ekim tarihinden bu yana dolandırıcılar tarafından hacklenen hesapların bir listesine ulaşmayı başardım. Listeyi incelediğimde 26 Ekim – 25 Kasım tarihleri arasında dolandırıcıların, ağlarına özel olarak hedef aldığı 70'den fazla Instagram kullanıcısını

başarıyla düşürdüğü anlaşılıyordu. Hedef alınan Instagram hesaplarının takipçi sayılarını incelediğimde ise yaklaşık 200.000 Instagram kullanıcısının hacklenen bu hesaplar üzerinden bir ortalama saldırısına veya dolandırıcılığa maruz kalma riski de ortaya çıkıyordu.



```
================================================================
Show Hacked Instragram Accounts v1.0 [https://www.mertsarica.com]
================================================================
Unfortunately 73 Instagram accounts have been hacked!

Date: 25.11.2021 12:38 Username:
Date: 23.11.2021 20:10 Username:
Date: 22.11.2021 13:32 Username:
Date: 22.11.2021 11:37 Username:
Date: 19.11.2021 21:44 Username:
Date: 19.11.2021 20:35 Username:
Date: 19.11.2021 15:54 Username:
Date: 18.11.2021 18:36 Username:
Date: 17.11.2021 18:30 Username:
Date: 16.11.2021 20:57 Username:
Date: 16.11.2021 19:58 Username:
Date: 16.11.2021 19:48 Username:
Date: 16.11.2021 16:44 Username:
Date: 16.11.2021 14:35 Username:
Date: 16.11.2021 13:28 Username:
Date: 15.11.2021 12:46 Username:
Date: 13.11.2021 15:02 Username:
Date: 13.11.2021 13:23 Username:
Date: 13.11.2021 12:01 Username:
Date: 12.11.2021 15:15 Username:
Date: 11.11.2021 12:28 Username:
Date: 11.11.2021 12:04 Username:
Date: 10.11.2021 20:07 Username:
Date: 10.11.2021 19:50 Username:
Date: 10.11.2021 11:40 Username:
Date: 10.11.2021 11:21 Username:
Date: 09.11.2021 22:32 Username:
Date: 09.11.2021 19:00 Username:
Date: 09.11.2021 17:39 Username:
Date: 09.11.2021 17:18 Username:
Date: 08.11.2021 21:11 Username:
Date: 08.11.2021 20:30 Username:
Date: 08.11.2021 19:35 Username:
Date: 08.11.2021 19:09 Username:
Date: 08.11.2021 16:48 Username:
Date: 08.11.2021 13:16 Username:
Date: 08.11.2021 12:50 Username:
Date: 08.11.2021 10:32 Username:
Date: 07.11.2021 21:22 Username:
Date: 07.11.2021 18:39 Username:
Date: 07.11.2021 09:16 Username:
Date: 06.11.2021 18:07 Username:
Date: 06.11.2021 13:14 Username:
Date: 06.11.2021 12:47 Username:
Date: 06.11.2021 11:17 Username:
Date: 06.11.2021 07:29 Username:
```



Sonuç itibariyle diğer yazılarımda da olduğu üzere tüm okurlarıma bilmedikleri kaynaklardan gelen (e-posta, SMS, özel mesaj vb.) bağlantı adreslerine (link) tıklamalarını, parolalarını, iki faktörlü doğrulama

kodlarını bilmedikleri sitelere, formlara girmemelerini, mümkün olan tüm hesaplarında iki faktörlü kimlik doğrulamasını kullanmalarını, Instagram hesaplarının güvenliğini sağlamak amacıyla bu sayfada yer alan yönergeleri takip etmelerini, Instagram hesaplarının hacklenmesi durumunda ise geri almak için Instagram'ın destek sayfasını ziyaret etmelerini ve son olarak da farkındalık adına bu yazıyı sosyal ağ/medya kullanan tanıdıkları ile paylaşmalarını öneriyorum.

Yılın son yazısı olması vesilesiyle şimdiden tüm okurlarımın yeni yılını canıgönülden kutlar, 2022 yılının herkese önce sağlık sonra mutluluk ve bol kazanç getirmesini dilerim.