Hack 4 Career - 2021

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

Hack 4 Career - 2021

HTTPS://WWW.MERTSARICA.COM

MERTSARICA

İçindekiler

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

Giriş

2009 yılında "Bilgi güçtür ve paylaşıldıkça artar" mottosuyla oluşturduğum blogumda, bilgi güvenliği farkındalığını arttırma adına çok sayıda teknik yazıya yer vermeye çalıştım. Yıllar içinde okurlarımdan aldığım olumlu geri dönüşler sonucunda, yazılarımı yıllar bazında e-kitap olarak derlemeye ve siber güvenlik meraklıları ile paylaşmaya karar verdim.

Emek, zaman ve kaynak ayırarak yaptığım araştırmalar sonucunda yazdığım bu yazıların, siber güvenlik alanında kendini geliştirmek isteyenler için faydalı olması dileklerimle...

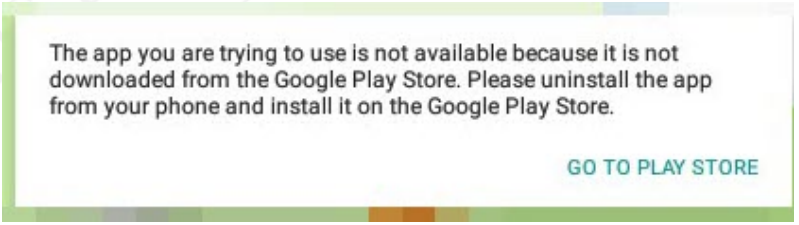
Android'de Kanca Atmak

Konumuz Android dünyası olsa da kanca atma denilince nedense aklıma ilk olarak enerji nakil hattına kanca atılarak hanelere çekilen kaçak elektrik gelir. Android dünyasında da aslında uygulamaları dinamik olarak analiz etmek veya müdahale etmek istediğimizde de benzer bir yöntem izleriz. Peki buna neden ihtiyaç duyarız ? Kimi zaman Android uygulamaları ile ilgili bir güvenlik araştırması yapmak istediğimizde veya sızma testi esnasında güvenlik zafiyeti bulmak için hedef Android uygulamasını analiz etme ihtiyacı duyarız. Bunun için genellikle ilk olarak hedef Android uygulamasını kaynak koduna çevirip statik kod analizi yapmakla işe başlarız. Fakat günümüzde çoğu Android uygulamasında kodlar gizlenerek (obfuscation) anlaşılması güçleştirildiği için uygulamayı Genymotion gibi öykünücüler (emulator) üzerinde dinamik olarak analiz etmeye çalışırız. Çalışırız dememin bir sebebi ise yine günümüzde Snapchat gibi mobil uygulamaların statik analizin yanı sıra dinamik analizi de engelleme adına çok sayıda yönteme başvurduğu görülebilmektedir.

2019 yılının Aralık ayında gerçekleştirdiğim Stockholm seyahatim esnasında şehri gezerken etrafımdan şık şıkırdım insanların vızır vızır elektrikli scooterlar ile geçip gittiğini gördüm. Avrupa'da kullanımının son derece yaygın olması sebebiyle

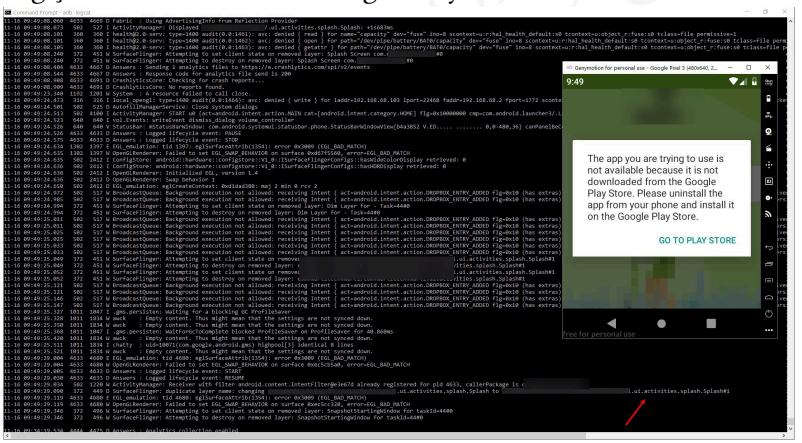
elektrikli scooter uygulamalarının zaman içinde güvenlik araştırmacılarının radarına girmesi ile bazılarında güvenlik zafiyetlerinin tespit edildiğini hatırladım. Ülkemizde de yaygınlaşmaya başlayan elektrikli scooterları ve uygulamalarını kullanmaya başlamadan önce Android uygulamalarından bir tanesinin haberleşmesini, merakımı gidermek amacıyla güvenlik araştırmacısı gözüyle incelemeye karar verdim. Tabii ki her zaman olduğu gibi evdeki hesap çarşıya uymadı ve karşıma çıkan engeller sayesinde ortaya bu blog yazısı çıkmış oldu. ?

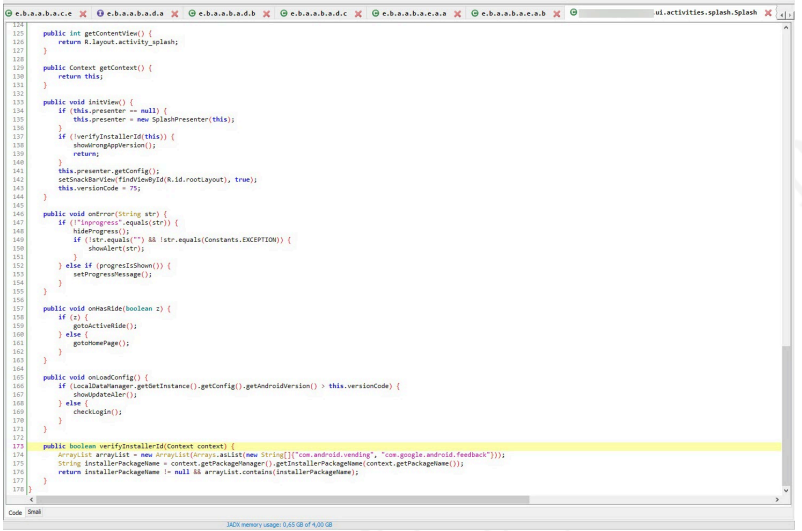
Zamanı kısıtlı bir güvenlik araştırmacısı olarak statik kod analizi ile vakit kaybetmek istemediğim için APK dosyasını APK Downloader web uygulaması ile indirip Geny Motion öykünücüsüne yükledim. Uygulamayı çalıştırdıktan sonra karşıma APK dosyasının Google Play üzerinden indirilmemesi sebebiyle sürpriz bir uyarı mesajı çıktı. ?

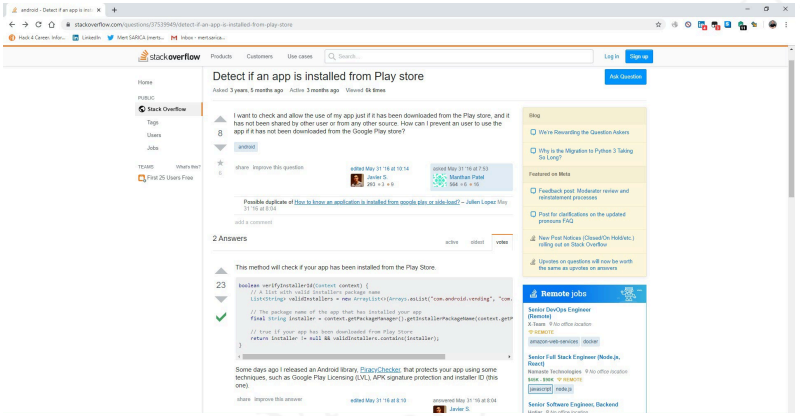


Bunun üzerine gözü kapalı statik kaynak kodu analizine girmeden önce komut satırında sistem mesajlarını görüntülemek için **adb logcat** komutunu çalıştırıp ardından da uygulamayı tekrar çalıştırdım. Mesajlar arasından ekrana gelen uyarı mesajı ile ilişkili olduğunu düşündüğüm fonksiyonu bulmak için jadx aracı ile APK dosyasını kaynak koduna çevirdikten sonra **activities.splash.Splash** dosyasını incelemeye başladım. Dosyanın sonunda yer alan **verifyInstallerId** fonksiyonu hemen dikkatimi çekti. Bu fonksiyon adını Google arama motorunda arattığımda benzer bir fonksiyonun tam da bu amaçla

kullanıldığını gördüm. Bu fonksiyon ile Android'in **getInstallerPackageName** fonksiyonundan faydalanarak uygulamayı Android'e yükleyen uygulamanın Google Play olup olmadığı kontrol ediliyordu. Şayet uygulama Google Play tarafından işletim sistemine yüklendiyse **installerPackagename** değişkeni sıfırdan farklı bir değer oluyordu.





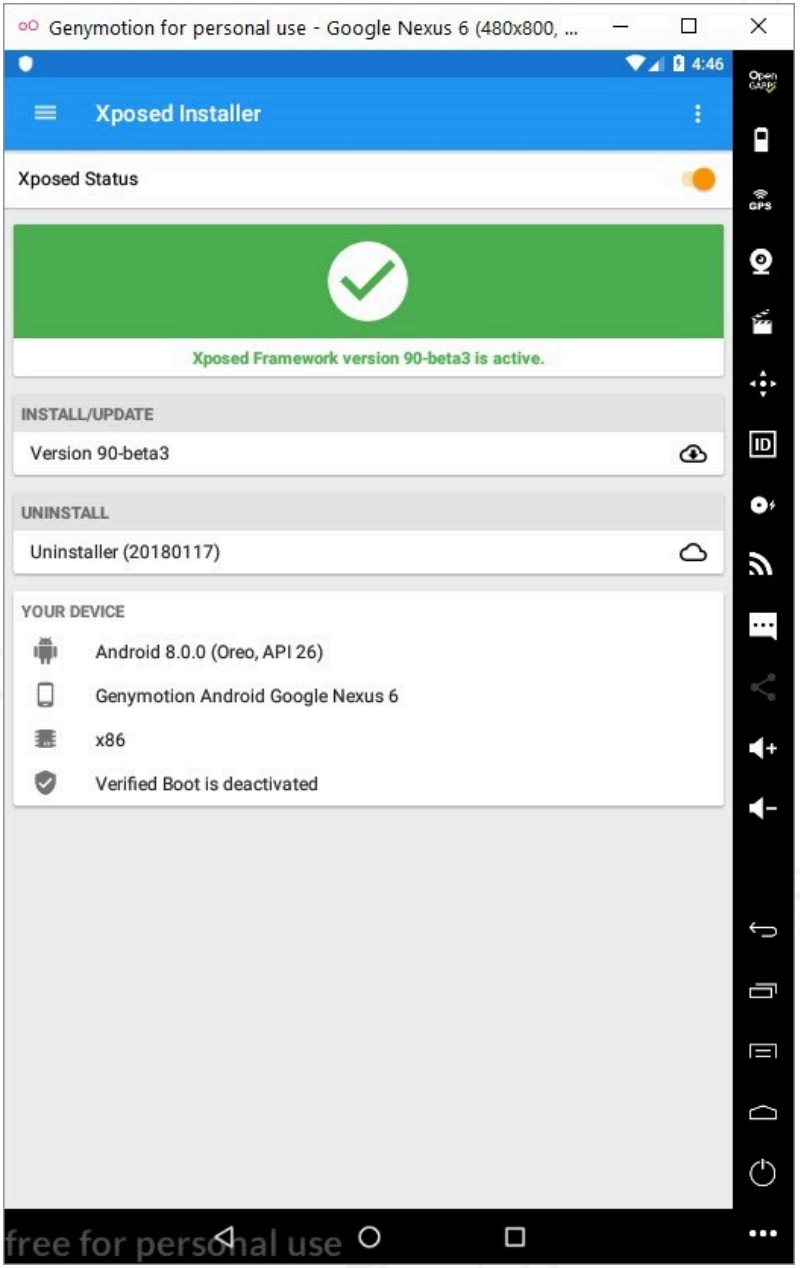


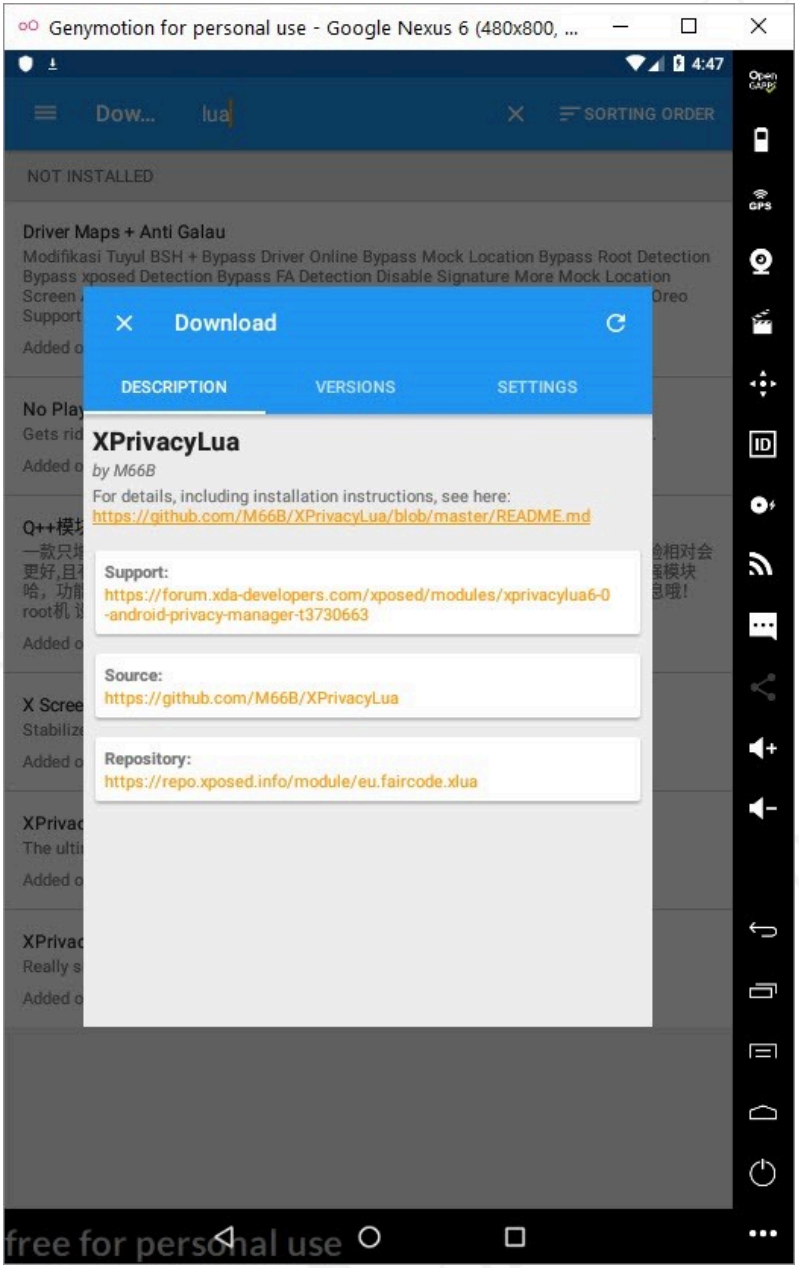
Bu fonksiyona kaynak kodu seviyesinde müdahale edip, **installerPackagename** değişkenini sıfırdan farklı bir değer yapıp ardından derleyip Android işletim sistemi üzerinde çalıştırabilirdim fakat Bill Gates'in bir röportajında dediği gibi "Her zaman en tembel insanları işe alırım çünkü tembeller çok karışık işleri bile en kısa yoldan yaparlar" ben de tembellik yapıp kısa bir yol aramaya karar verdim. ?

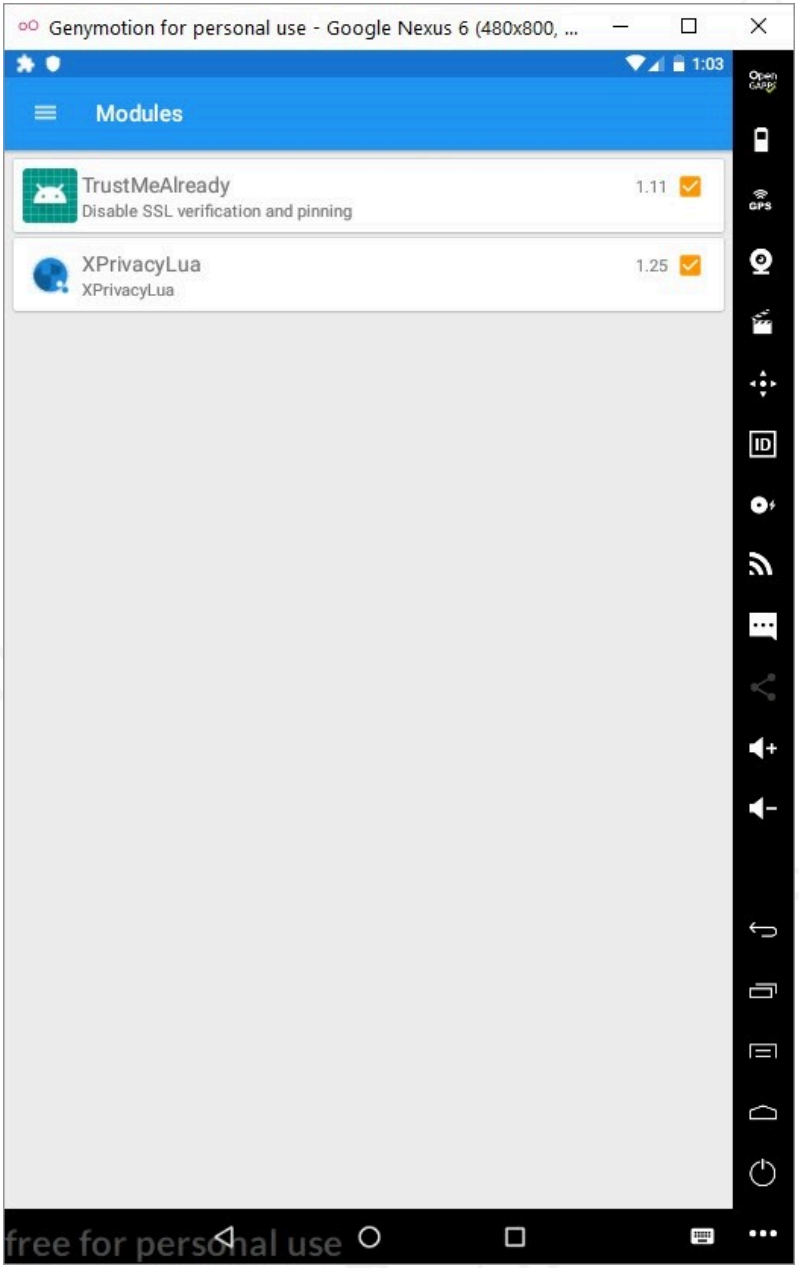
Eminim bu gibi bir durumla karşılaşan güvenlik araştırmacılarının çoğu Frida araç kiti ile ilerlemeyi tercih ederler fakat hayatın Frida'dan ibaret olmaması gerektiğine inanarak Frida'ya alternatif bir araç, farklı bir yol aramaya karar verdim. Google arama motorunda kısa bir araştırma yaptıktan sonra daha önce sızma testlerinde özellikle SSL Pinning'i atlatmak için kullandığım ve 1400'den fazla eklentiye sahip olan **Xposed Framework** aklıma geldi.

Geny Motion üzerinde bulunan Android Oreo işletim sistemine Xposed Framework'u kurduktan sonra eklentilerine göz atmaya başladım. Eklentiler arasında XPrivaclyLua isimli eklenti hemen dikkatimi çekti. Adından da anlaşılabileceği üzere bu eklenti, Android üzerinde yüklü olan uygulamaları sahte bilgilerle (sahte konum bilgisi gibi) besleyerek mahremiyetinizi korumaya

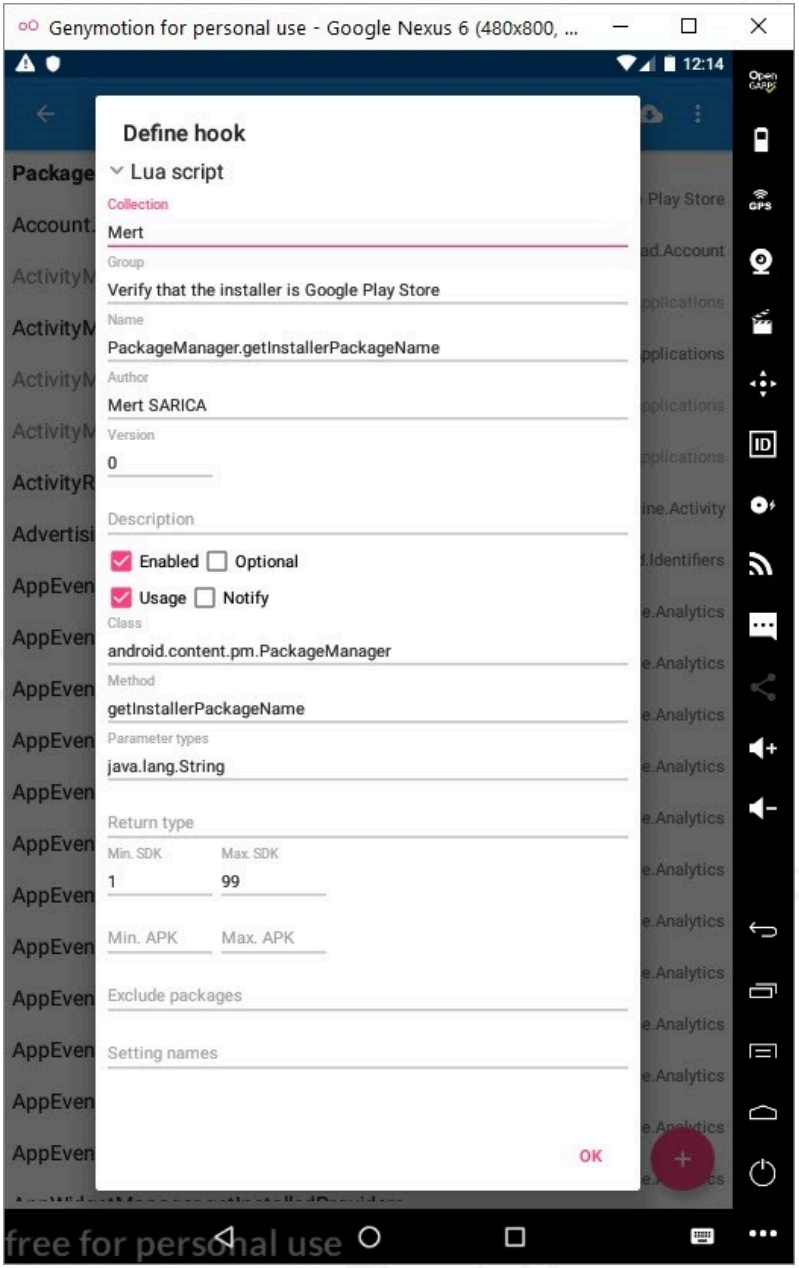
yardımcı olmaktadır. Çalışma yöntemi olarak kabaca bu bilgileri toplamaya çalışan fonksiyonlara kanca atarak gerçek bilgiler yerine sahte bilgiler vermektedir. Eklentiyi ihtiyaçlarınız doğrultusunda şekillendirmek için ise Pro sürümünü yükleyerek Lua programlama dili ile betikler oluşturmanız gerekmektedir.

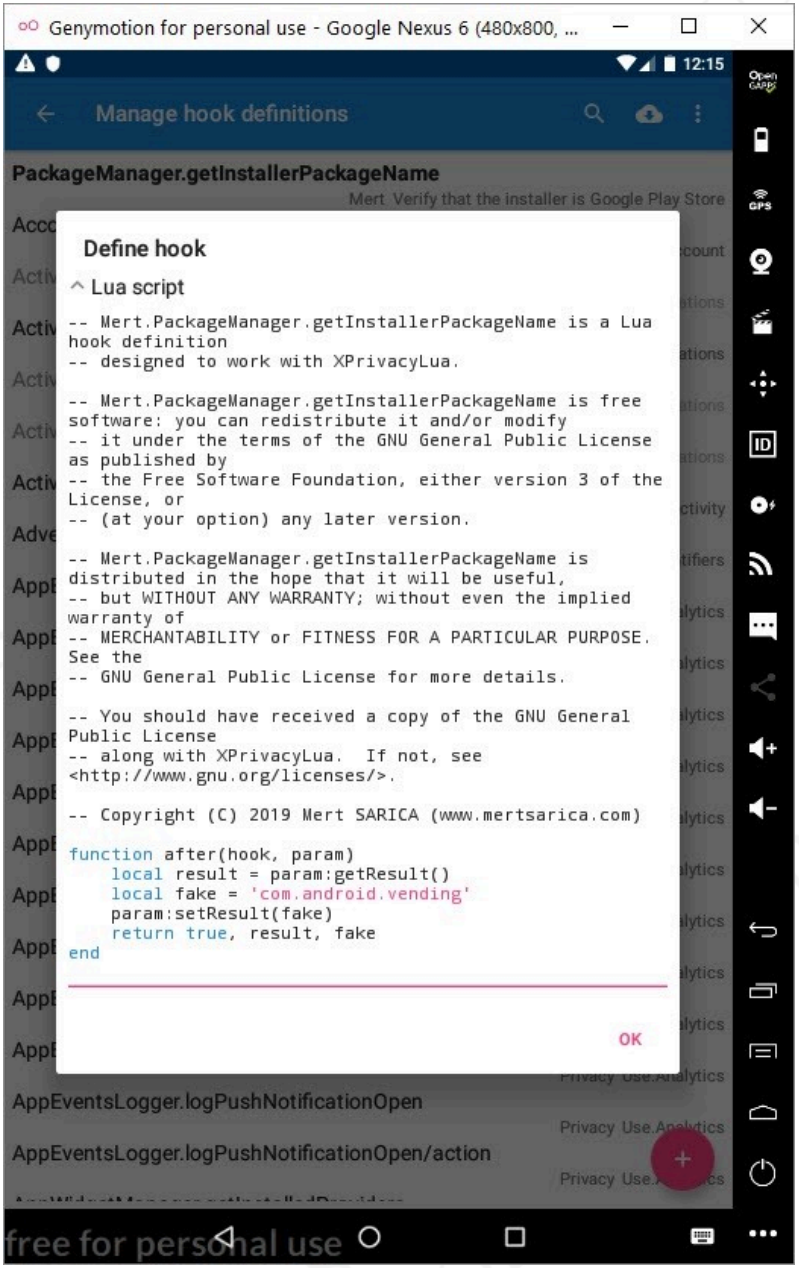

Genymotion for personal use - Google Nexus 6 (480x800, ...
4:46
Xposed Installer
Xposed Status
Xposed Framework version 90-beta3 is active.
INSTALL/UPDATE
Version 90-beta3
UNINSTALL
Uninstaller (20180117)
YOUR DEVICE
Android 8.0.0 (Oreo, API 26)
Genymotion Android Google Nexus 6
x86
Verified Boot is deactivated
free for personal use

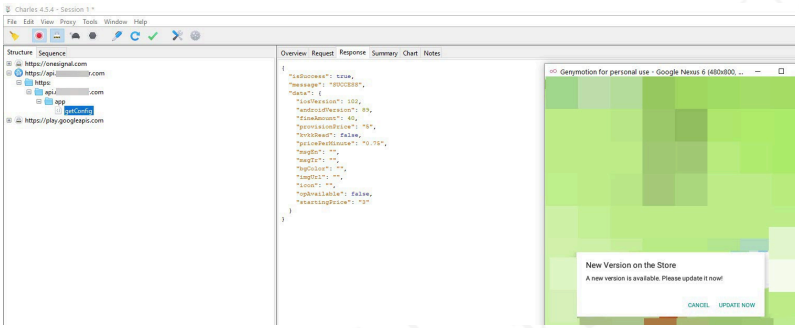

Genymotion for personal use - Google Nexus 6 (480x800, ...
4:47
Dow...
lua
SORTING ORDER
NOT INSTALLED
Driver Maps + Anti Galau
Modifikasi Tuyul BSH + Bypass Driver Online Bypass Mock Location Bypass Root Detection Bypass xposed Detection Bypass FA Detection Disable Signature More Mock Location
Download
DESCRIPTION
VERSIONS
SETTINGS
XPrivacyLua
by M66B
For details, including installation instructions, see here:
https://github.com/M66B/XPrivacyLua/blob/master/README.md
Support:
https://forum.xda-developers.com/xposed/modules/xprivacylua6-0-android-privacy-manager-t3730663
Source:
https://github.com/M66B/XPrivacyLua
Repository:
https://repo.xposed.info/module/eu.faircode.xlua
free for personal use


Genymotion for personal use - Google Nexus 6 (480x800, ...
1:03
Modules
TrustMeAlready
Disable SSL verification and pinning
1.11
XPrivacyLua
XPrivacyLua
1.25
free for personal use

Lua ile **installerPackagename** değişkenini değiştiren ufak bir betik hazırlayıp aktif hale getirdikten sonra uygulamayı çalıştırdığımda uygulamanın artık daha önceki uyarı mesajını çıkarmadığını ve Charles Proxy ile web trafiğini görüntüleyebildiğimi görerek mutlu sona ulaşmış oldum.


Genymotion for personal use - Google Nexus 6 (480x800, ...
12:14
Define hook
Lua script
Collection
Mert
Group
Verify that the installer is Google Play Store
Name
PackageManager.getInstallerPackageName
Author
Mert SARICA
Version
0
Description
Enabled
Optional
Usage
Notify
Class
android.content.pm.PackageManager
Method
getInstallerPackageName
Parameter types
java.lang.String
Return type
Min. SDK
Max. SDK
1
99
Min. APK
Max. APK
Exclude packages
Setting names
OK
free for personal use


Genymotion for personal use - Google Nexus 6 (480x800, ...
12:15
Manage hook definitions
PackageManager.getInstallerPackageName
Mert: Verify that the installer is Google Play Store
Define hook
Lua script
-- Mert.PackageManager.getInstallerPackageName is a Lua hook definition
-- designed to work with XPrivacyLua.
-- Mert.PackageManager.getInstallerPackageName is free software: you can redistribute it and/or modify
-- it under the terms of the GNU General Public License as published by
-- the Free Software Foundation, either version 3 of the License, or
-- (at your option) any later version.
-- Mert.PackageManager.getInstallerPackageName is distributed in the hope that it will be useful,
-- but WITHOUT ANY WARRANTY; without even the implied warranty of
-- MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
-- GNU General Public License for more details.
-- You should have received a copy of the GNU General Public License
-- along with XPrivacyLua. If not, see <http://www.gnu.org/licenses/>.
-- Copyright (C) 2019 Mert SARICA (www.mertsarica.com)
function after(hook, param)
local result = param:getResult()
local fake = 'com.android.vending'
param:setResult(fake)
return true, result, fake
end
OK
AppEventsLogger.logPushNotificationOpen
AppEventsLogger.logPushNotificationOpen/action
free for personal use



Bu yazının güvenlik araştırmalarında Frida'ya alternatif araç ve yöntem arayanlara ışık tutacağını ümit ederek bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

SIM Kart Dolandırıcılığı ile Mücadele

Günümüzde, kullandığımız e-posta hesabından sosyal medya hesabına, internet bankacılığı hesabından geliştirdiğimiz yazılımın kaynak kodunu barındırdığımız hesaba kadar giriş (login) esnasında güvenliğimiz için iki faktörlü kimlik doğrulama kullanıyoruz veya kullanmaya zorlanıyoruz. İki faktörlü kimlik doğrulama denildiğinde son yıllarda geniş kitleler tarafından sıklıkla kullanılması sebebiyle çoğumuzun aklına tek kullanımlık parola, OTP olarak SMS doğrulama kodu gelse de, tek kullanımlık parola üreten aygıtlar, uygulamalar hala hayatımızda fazlasıyla yer edinmektedir.

Yakın geçmişte yabancı basında SIM kartı değişikliği ile yapılan dolandırıcılık haberlerine sıkça rastlamaya başladık. Bu dolandırıcılıkların başarıyla ulaşmasının en büyük nedeni ise kullanıcıların doğrulama adına bir aygıt kullanmaması veya tek kullanımlık parola üreten bir aygıt, uygulama kullanmak yerine SMS doğrulama kodu kullanmalarıdır. Bu sayede telefon hattını üzerine geçiren bir dolandırıcı bundan sonra bankacılıktan sosyal medya hesaplarına kadar hedef kişinin giriş esnasında cep telefonununa gönderilen tek kullanımlık SMS doğrulama kodunu ele geçirerek kötü emellerine ulaşabilmektedir. Türkiye'de bu

şekilde gerçekleştirilen dolandırıcılıklar ile yıllar yıllar önce karşılaşılmaya başlandığı için bugün GSM operatörleri ile finans kurumları arasında etkin bir işbirliği yapılması ile SIM kartı değişikliği ile gerçekleştirilmeye çalışılan internet/mobil bankacılığı dolandırıcılıkları önlenebilmektedir. Son zamanlarda ise zorlu hedeflerle uğraşmak yerine kolay olanları tercih eden dolandırıcıların SIM kartı değişikliği ile kripto para borsalarında hesabı olan kullanıcıları, yatırımcıları hedef aldığını görebilmekteyiz.

Kendi hesaplarım için olabildiğince Google Authenticator gibi tek kullanımlık parola üreten uygulamalar kullansam da APT41 gibi telekomünikasyon firmalarını hedef alıp SMS meajlarına göz diken devlet destekli hacker grupları, casusa dönüşme potansiyeli git gide artan akıllı telefonlar derken telefonumu doğrulama amacıyla kullanmak bir siber güvenlik araştırmacısı olarak pek güvende hissettirmemeye başlamıştı. Bir de bağlantılarımdan "Hocam peki sen kendi hesaplarının güvenliğini nasıl sağlıyorsun ?" vb. sorular ile de zaman içinde karşılaşmaya başladıkça bu yazı ile bilfiil hesaplarımın güvenliğini nasıl sağladığımı kısaca açıklamaya karar verdim.

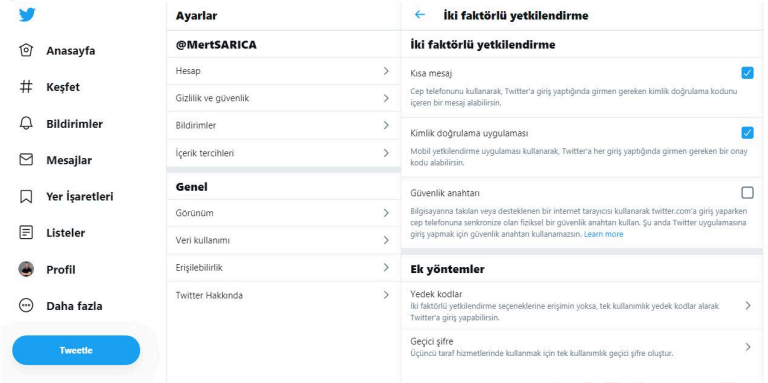
SMS doğrulama koduna (something you have) kıyasla doğrulama faktörü olarak daha güvenli ne kullanabilirim diye kısa bir araştırma yaptığımda Google'ın Gelişmiş Güvenlik Programı'nda da yer alan güvenlik anahtarı üreticisi Yubico'nun web sayfasını incelemeye karar verdim. YubiKey NFC 5 anahtarını almaya karar verdikten sonra maalesef YubiKey'in bilinen e-ticaret mağazalarında satılmadığını öğrendim. Amazon.com üzerinde 45$'a satılan bu anahtara bir o kadar da kargo bedeli üzerine bir de vergi ödememek için ne yapmalı ne etmeli diye kara kara düşünürken imdadıma o esnada FireEye etkinliği için ABD'ye uçacak olan FireEye Türkiye Kıdemli Satış Mühendisi Ökkeş

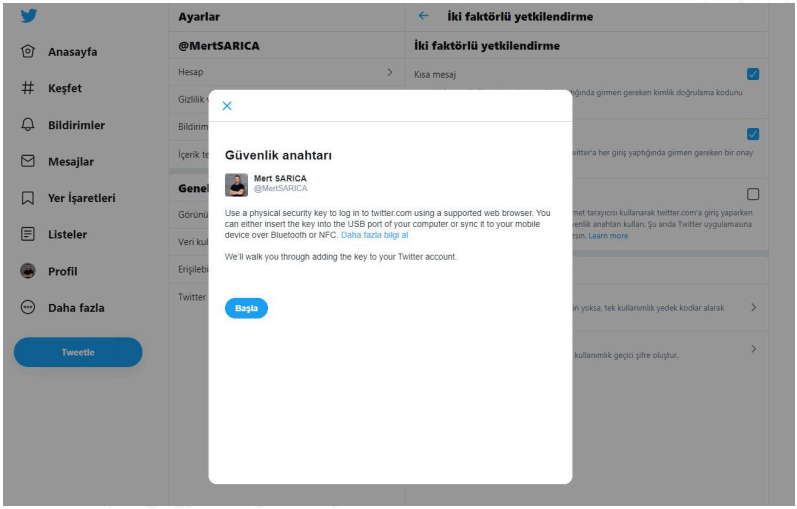
ÖZDEMİR koştu ve sağolsun dertsiz, tasasız bu güvenlik anahtarına sahip olabildim.

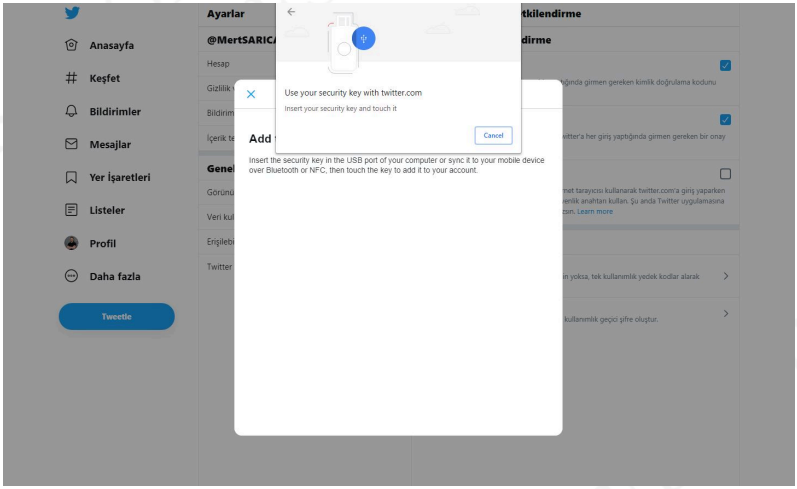
Anahtarı alır almaz http://yubico.com/start adresini ziyaret edip kurulum ile ilgili yönergeleri okuduktan sonra ilk iş olarak siber güvenlik ile ilgili haberleri takip etmek için çok sık kullandığım Twitter hesabımı güvenli hale getirmeye karar verdim. Twitter'a

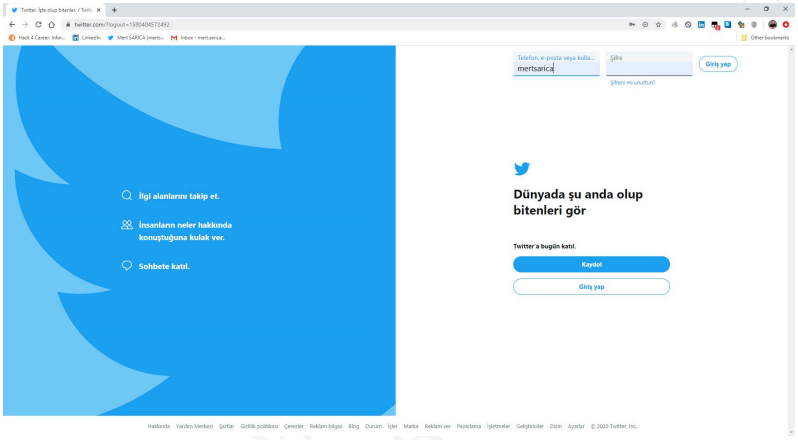
giriş yaptıktan sonra **iki faktörlü yetkilendirme** sayfasında **kısa mesaj** opsiyonunu devre dışı bıraktım. Ardından **güvenlik anahtarı** opsiyonunu aktif hale getirip yönergeleri takip ederek USB güvenlik anahtarımı Twitter'a başarıyla tanıtarak SMS doğrulama kodu ile girişten kurtulmayı başardım. WordPress yönetim sayfasına girişte de bu anahtarı kullanabilir miyim acaba diye araştırma yaparken Two-Factor WordPress eklentisi ile de karşılaşmak beni oldukça mutlu etti.

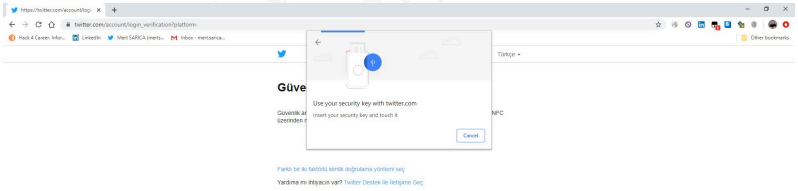
> Yeri gelmişken güvenlik anahtarı ile doğrulamayı desteklemeyen platformlar için ise Yubico tarafından geliştirilmiş olan Google Authenticator muadili, NFC destekli Yubico Authenticator uygulaması sayesinde güvenlik anahtarınızı telefonunuza NFC üzerinden okutarak tek kullanımlık parola oluşturabileceğinizi de belirtmiş olayım.

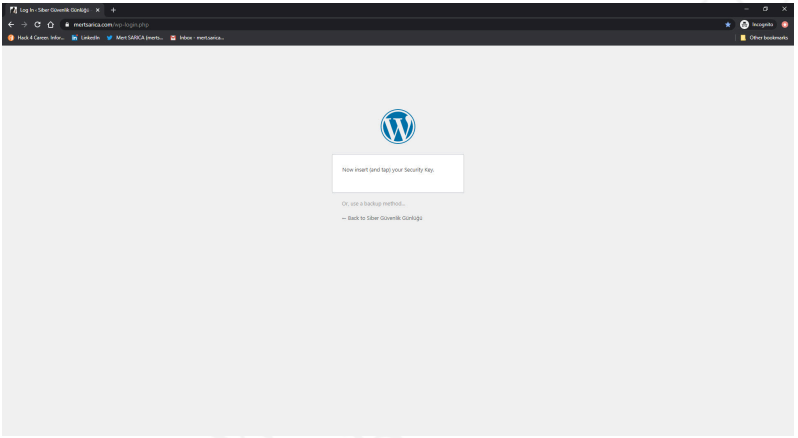












Son olarak Google'ın Gelişmiş Güvenlik Programı'na da dahil olup tüm Google hesaplarımı da güvenlik anahtarı destekleyen platformlarda olduğu gibi güvenli hale getirdikten sonra kendini bir nebze daha güvenli hisseden bir siber güvenlik araştırmacısı olarak mutlu sona ulaşmış oldum.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

Excel 4.0 Makro (XLM) Analizi

2017 yılında başlayan DDE tabanlı oltalama saldırıları, 2020 yılı itibariyle yerini Excel 4.0 Makro (XLM) oltalama saldırılarına bıraktı. Ufak bir araştırma yaptığınızda XLM makrolarının hayatımıza girişinin 1992 yılında Microsoft Excel 4.0'ın yayınlanması ile olduğunu görebilirsiniz. Tehdit aktörleri tarafından sıklıkla kötüye kullanılan VBA makroları ise Excel 5.0 ile duyurulması ile hayatımıza girmiş ve günümüzde de en güncel Microsoft Office sürümünde hala desteklenmektedir.

Yanlış anımsamıyorsam XLM makroları ile ilgili ofansif güvenlik üzerine okuduğum ilk teknik makale Outflank firmasına ait bu blog yazısıydı. XLM makrolarını VBA makroları gibi tespit edip, analiz etmenin pek de kolay olmadığı XLM makrolarına yönelik yapılan güvenlik araştırmaları ile ortaya çıkmaya başladıktan sonra her zaman olduğu gibi ofansif güvenlik uzmanlarının yanı sıra tehdit aktörlerinin de dikkatini çekmeye başladı. Aradan çok zaman geçmeden de kurumlar XLM makro içeren oltalama saldırıları ile karşılaşmaya başladılar.

XLM makro içeren bir Office dosyasını analiz etmenin zorluğu, Microsoft Office Makro Analizi başlıklı blog yazımda belirttiğimin aksine Office'nin arayüzünden kolaylıkla görüntülenememesinden (view macro) kaynaklanmaktadır. Durum böyle olunca da zararlı XLM makro içeren Office dosyalarının tecrübesiz siber güvenlik

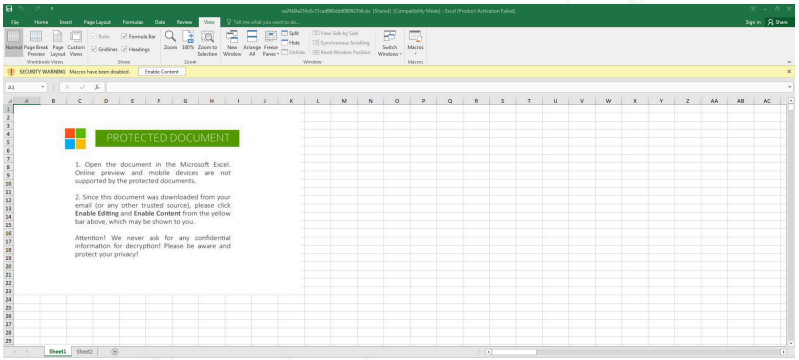
uzmanlarının dikkatinden kaçma ihtimali (“Bu Office dosyası bozuk”, “Makro içermiyor” gibi) artmaktadır. Ben de hem siber güvenlik analisletlerine XLM makro içeren Microsoft Office dosyalarının nasıl analiz edilebileceğini göstermek hem de XLM makro içeren Microsoft Office dosyalarına karşı farkındalık yaratmak adına gerçek bir olaydan yola çıkarak bir blog yazısı yazmaya karar verdim.

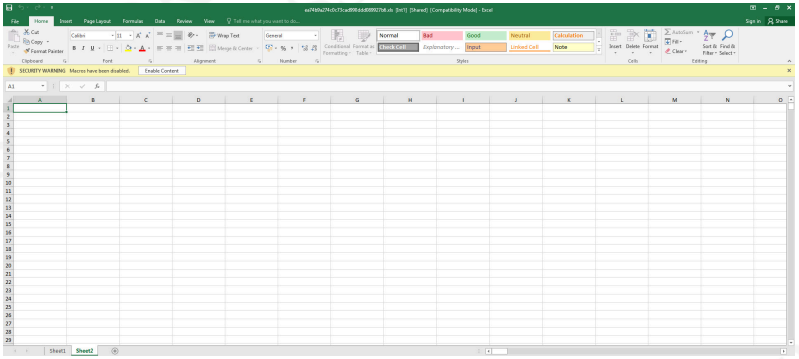
2020 yılının Mayıs ayında çok sayıda SMTP ip adresinden gönderilen ve gönderici adresi @wp.pl uzantılı olan yüzlerce e-posta için güvenlik sistemlerinde engellendiğine dair alarmlar üremeye başladı. E-postalar incelendiğinde eklerinde rastgele isimle oluşturulmuş XLS uzantılı Excel dosyaları bulunuyordu. Bu gibi durumlarda siber güvenlik analistlerinin yapması gereken en önemli adımlardan biri zararlı doküman içinde yer alan komuta kontrol merkezine ait adreslerini tespit etmek, web trafiği kayıtlarında aramak ve kurum genelinde erişimi engellemektedir.

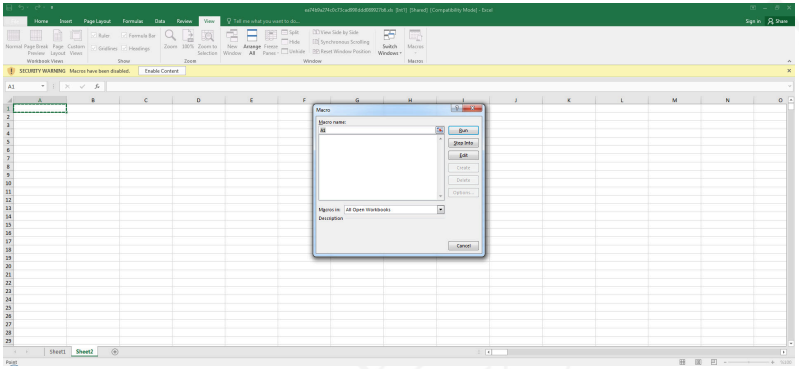
Tabii mevzu bahis XLM makro içeren Office dosyası olduğunda statik ve dinamik analiz yapan kum havuzu (sandbox) sistemlerinin anti kum havuzu yöntemleri karşısında yetersiz kaldığı durumlar söz konusu (Örnek: Kum Havuzu Tespiti) olabilmektedir. Alarma konu olan zararlı Excel dosyası da tam da bu şekilde kum havuzunda çalıştığını anlamaya yönelik kontroller gerçekleştirdiği için komuta kontrol merkezinin adresi bu analizler (VirusTotal, Hybrid-Analysis) esnasında ortaya çıkmamaktadır. Bu durumda siber güvenlik analistinin yapması gereken iş bu zararlı Excel dosyasını alıp zararlı yazılımı analizi amacıyla oluşturduğu sanal sistemine kopyalamak ve orada analiz etmek olmalıdır.

Excel dosyasını sanal sistemde çalıştırdığımızda karşımıza iki tane sayfa (Sheet1 & Sheet2) çıkmaktadır. Birinci sayfada kötü emellerini gerçekleştirebilmek için makroyu aktif hale getirmemiz gerektiğini belirten sahte bir resim/mesaj, ikinci sayfada ise bomboş hücreler (aslında boş değil :)) karşımıza çıkmaktadır. Her

ne kadar Excel bize bu dosyada makro olduğuna dair uyarı verse de dosyada yer alan makroyu görüntülediğimizde içinin boş olduğu görünmektedir.

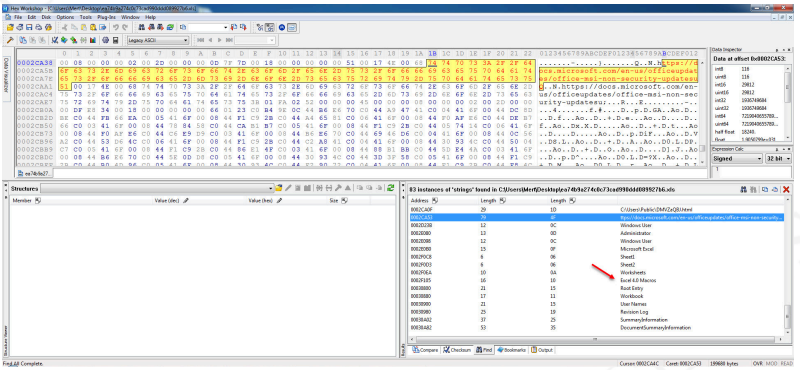


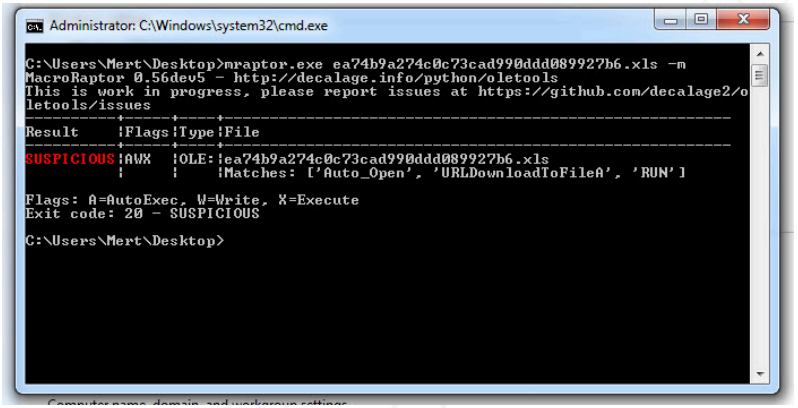


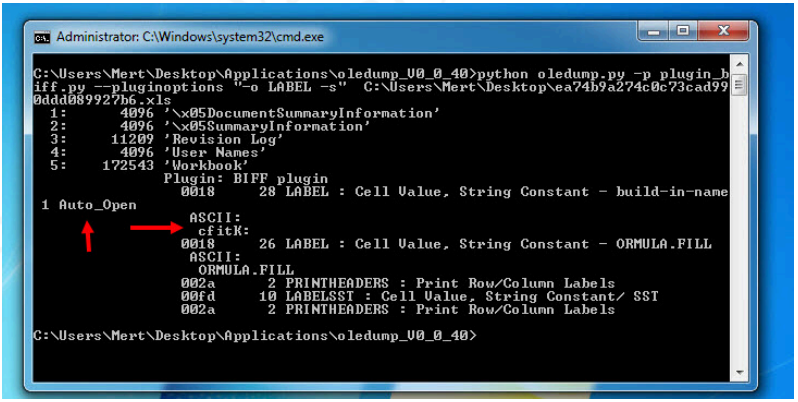


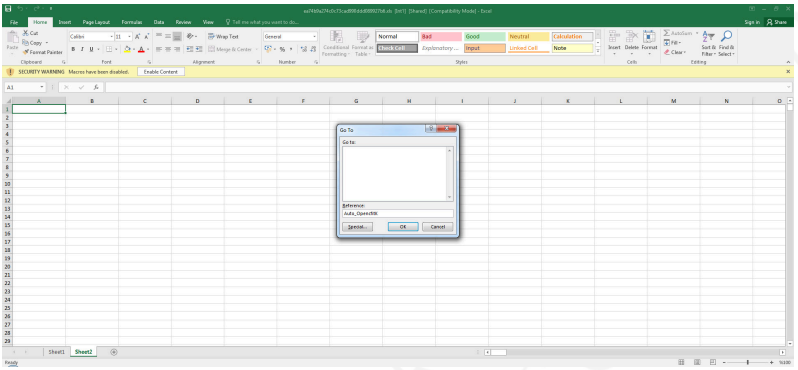
Dosyayı herhangi bir hex editörü ile açıp içinde yer alan karakter

dizilerine (strings) baktığımızda **Excel 4.0 Macros** dizisinden şüphe ettiğimiz gibi bunun XLM makrosu içerdiğini görebiliyoruz. Dosyanın içinde makro olduğundan emin olmak için dosyayı mraptor aracı ile analiz ettiğimizde dosyada makro olduğu ve otomatik olarak çalışabilmesi adına Auto_Open isminde (VBA makrosundaki AutoOpen() fonksiyonu gibi) bir hücreye (cell) sahip olduğu anlaşılıyordu. Bu hücrenin adını öğrenip görüntülemek ve analiz etmek için ise Didier STEVENS'ın oledump aracından faydalanarak (**oledump.py -p plugin_biff.py –pluginoptions "-o LABEL -s" C:\Users\Mert\Desktop\ea74b9a274c0c73cad990ddd089927b6.xls**) ilk çalıştırılan hücrenin **Auto_OpencfitK** adına sahip olduğunu gördüm. Analistin Excel üzerinden **Go To (CTRL-G)** ile Auto_Open ismine sahip hücreye giderek analize başlayacağını bilen zararlı kod geliştiricisi akıllılık yaparak adını bu hücrenin adını **Auto_OpencfitK** olarak değiştirmiştir.



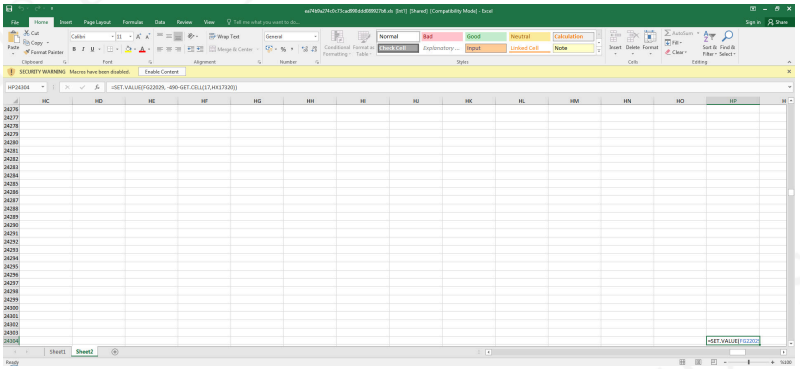


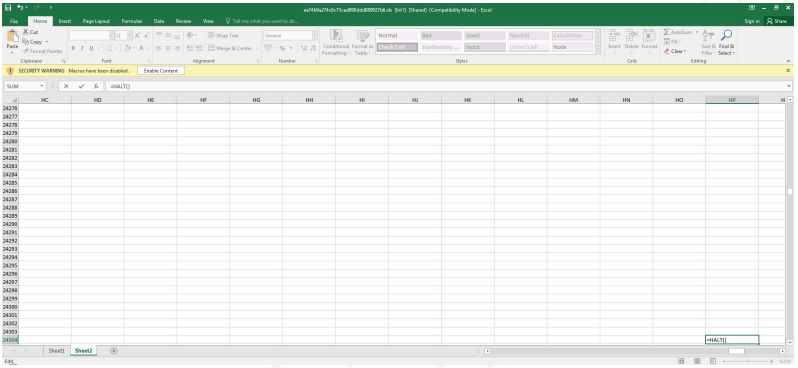




Başlangıç hücresine gittikten ve dosya genelinde 42 tane FORMULA ifadesi ve CHAR fonksiyonundan oluşan gizlenmiş

(obfuscated) bir makro olduğunu öğrendikten sonra her birini teker teker çözmek ve analiz etmek bir hayli zaman alacağı için hata ayıklaması (debugging) ile ilerlemeye karar verdim. **Auto_OpencfitK** hücresine gidip ALT + F8 kısa yoluna bastıktan sonra **Step Into** butonuna bastığımda haliylen Excel beni devam etmek için makro çalıştırmaya izin vermemi ve ardından dosyayı kapatıp açmamı istedi. Dosyayı açar açmaz Excel hızlıca **Auto_OpencfitK** hücresinden ilerleyeceği için bu adımı kaçırmamak için bu hücrede yer alan **=SET.VALUE(FG22029, -490-GET.CELL(17,HX17320))** formülünü **=HALT()** ile değiştirerek makronun sonlanmasını sağladım. Ardından **=HALT()** formülünü **=SET.VALUE(FG22029, -490-GET.CELL(17,HX17320))** ile değiştirip bu hücre üzerinde ALT + F8 kısa yoluna bastığımda sorunsuz bir şekilde ilk hücreden makroyu dinamik olarak analiz etmeye başlayabildim.



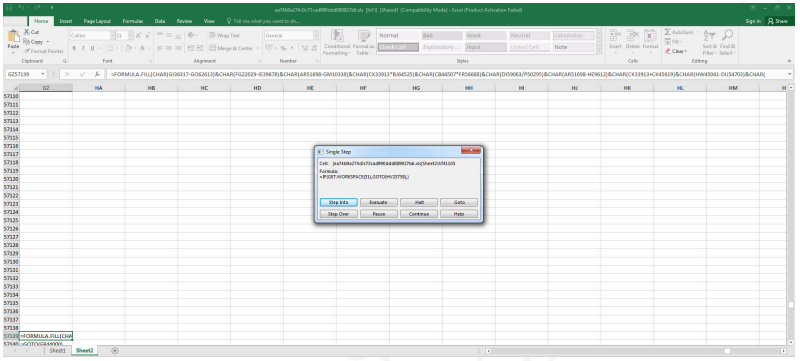


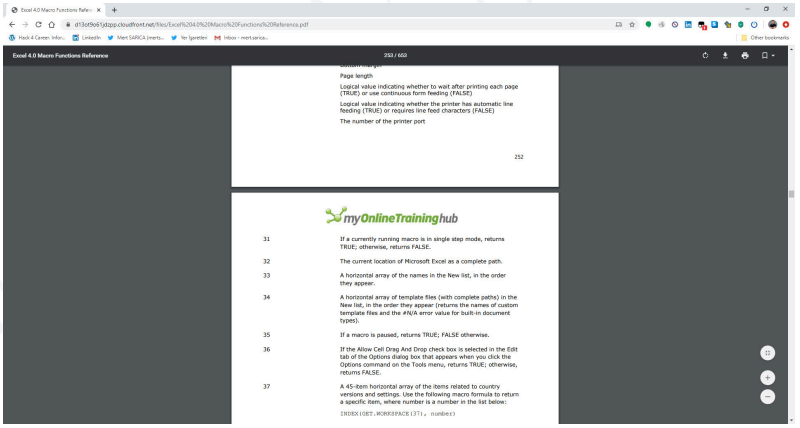
Step Into ve **Evaluate** butonlarından faydalanarak gizlenmiş hücrelerin çözülmesi ile analize devam ettikçe Excel 4.0 Macro Functions Reference belgesinden faydalanarak makronun hata ayıklamaya ve kum havuzuna karşı çeşitli kontroller gerçekleştirdiğini gördüm. Hata ayıklama kontrolü yapan AT41104 hücresine geldiğimde bu kontrolü atlatmak için hata ayıklama tespit edilememesi durumunda devam ettiği hücredeki **=GOTO(AY23948)** değerini **AT41104** hücresine kopyaladım.

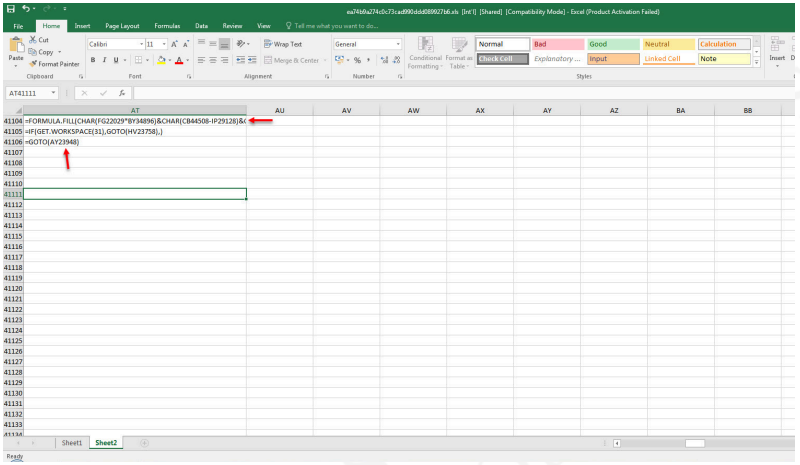
=IF(GET.WORKSPACE(31),GOTO(HV23758),) Makro hata ayıklama modunda mı ? (Anti-debugging)

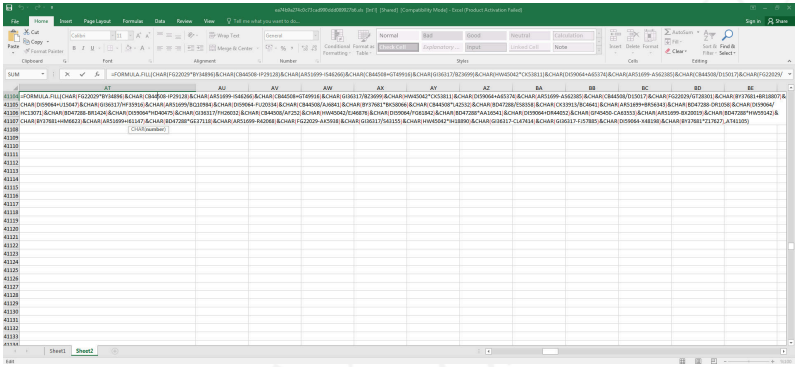
=IF(GET.WORKSPACE(19),,GOTO(HV23758),) Sistemde fare var mı ? (Anti-sandbox)

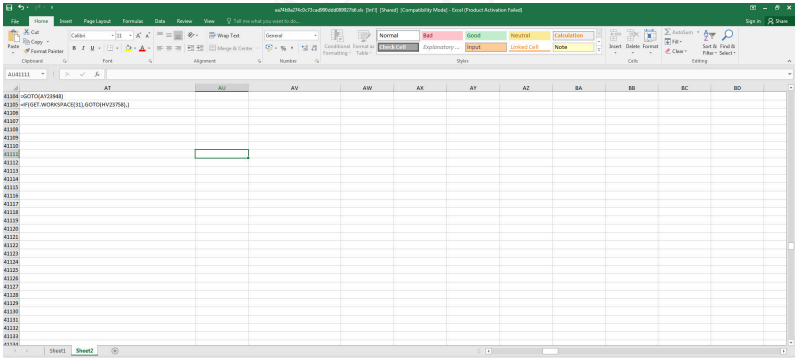
=IF(GET.WORKSPACE(42),,GOTO(HV23758),) Ses dosyası çalınabiliyor mu ? (Anti-sandbox)

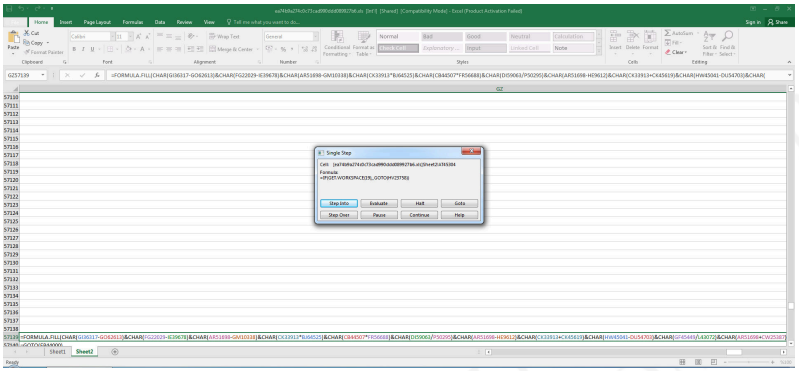

Single Step
Step Into
Evaluate
Halt
Goto
Step Over
Pause
Continue
Help
=FORMULA.FILL(CHA

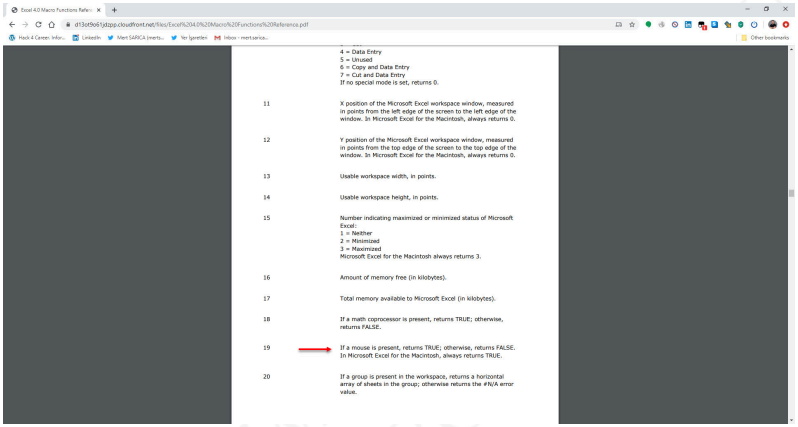

Excel 4.0 Macro Functions Reference
253 / 603
Page length
Logical value indicating whether to wait after printing each page (TRUE) or use continuous form feeding (FALSE)
Logical value indicating whether the printer has automatic line feeding (TRUE) or requires line feed characters (FALSE)
The number of the printer port
252
myOnlineTraininghub
31
If a currently running macro is in single step mode, returns TRUE; otherwise, returns FALSE.
32
The current location of Microsoft Excel as a complete path.
33
A horizontal array of the names in the New list, in the order they appear.
34
A horizontal array of template files (with complete paths) in the New list, in the order they appear (returns the names of custom template files and the #N/A error value for built-in document types).
35
If a macro is paused, returns TRUE; FALSE otherwise.
36
If the Allow Cell Drag And Drop check box is selected in the Edit tab of the Options dialog box that appears when you click the Options command on the Tools menu, returns TRUE; otherwise, returns FALSE.
37
A 45-item horizontal array of the items related to country versions and settings. Use the following macro formula to return a specific item, where number is a number in the list below:
INDEX(GET.WORKSPACE(37), number)

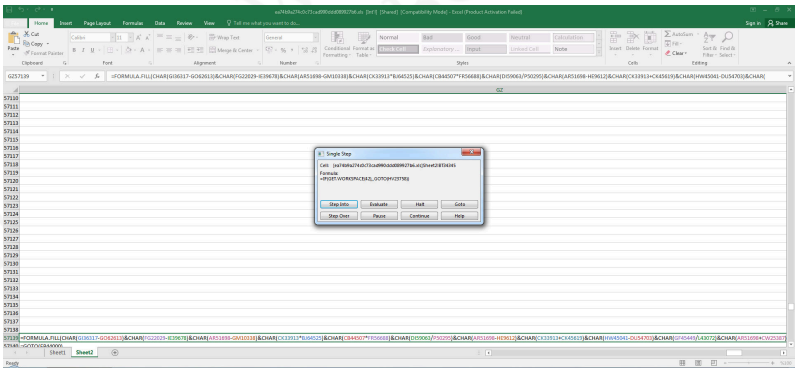

=FORMULA.FILL(CHAR(FG22029*BY34896)&CHAR(CB44508-IP29128)&<
=IF(GET.WORKSPACE(31),GOTO(HV23758),)
=GOTO(AY23948)
Sheet1
Sheet2
Ready

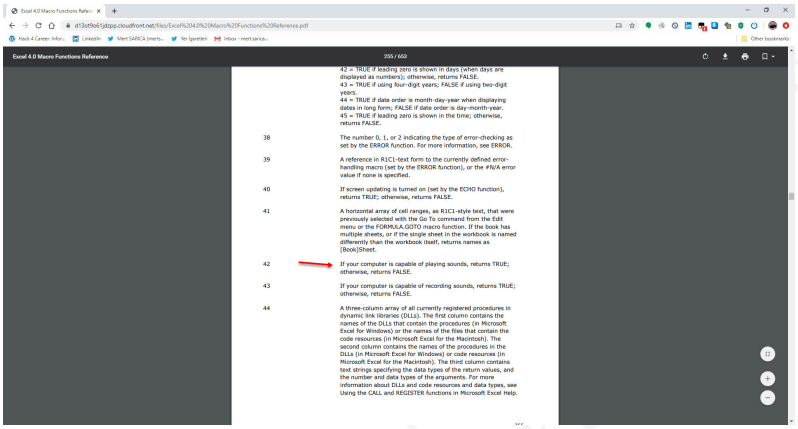






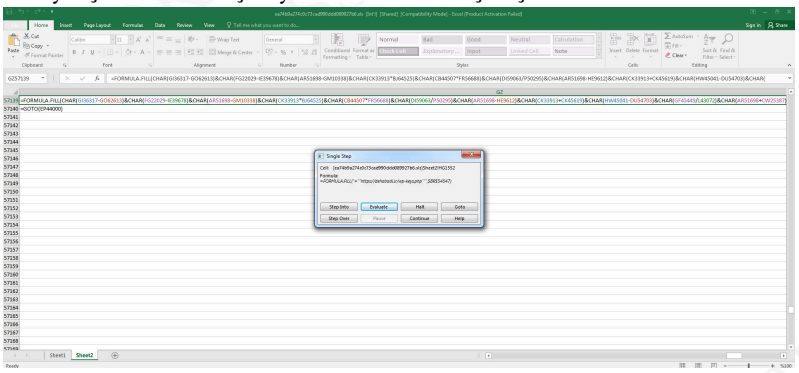


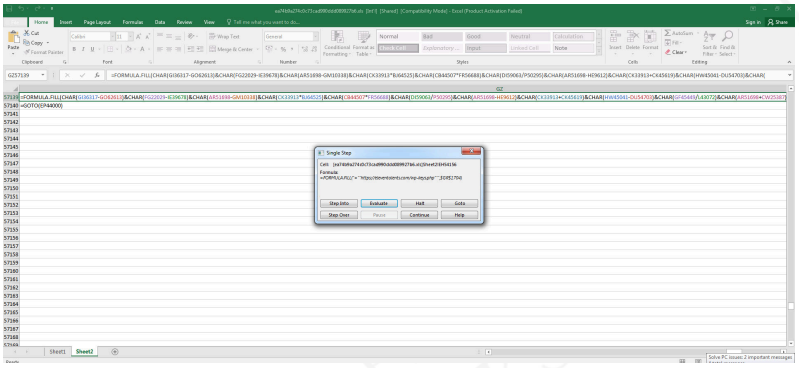




Hata ayıklamaya devam ettiğimde internet bağlantısını kontrol

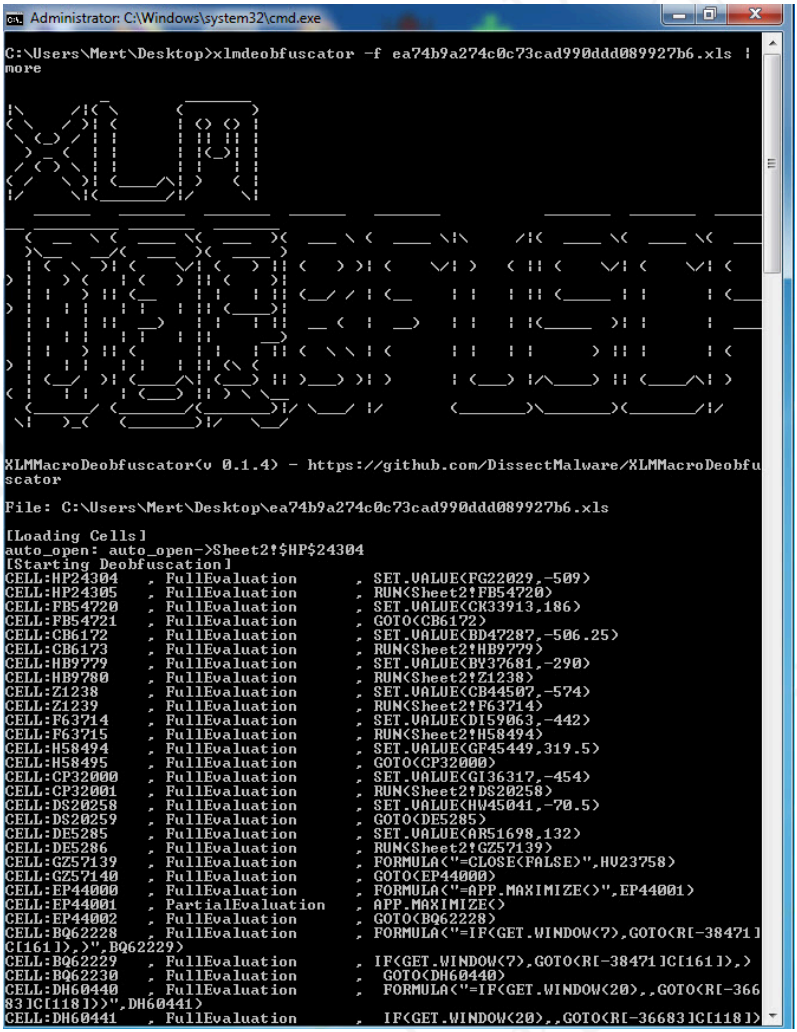
etmek için **https://docs.microsoft.com/en-us/officeupdates/office-msi-non-security-updates** web adresine bağlandığını ve hata alması durumunda çalışmayı durdurduğunu farkettim. Kayıt defteri (registery) üzerinden sistemde makro kullanımına izin verilip verilmediğini de kontrol ettikten sonra **https://dehabadi[.]ir/wp-keys[.]php** ve **https://eleventalents[.]com/wp-keys[.]php** adresleri ile iletişim kurmaya çalıştığını gördüm. Analiz esnasında bu iki adres de aktif olmadığı için analize devam edememiş olsam da yapmış olduğum araştırmalar sonucunda Zloader zararlı yazılımına ait komuta kontrol merkezleri olduğunu tahmin ettiğim bu adresleri ortaya çıkararak başarıyla amacıma ulaşmış oldum.

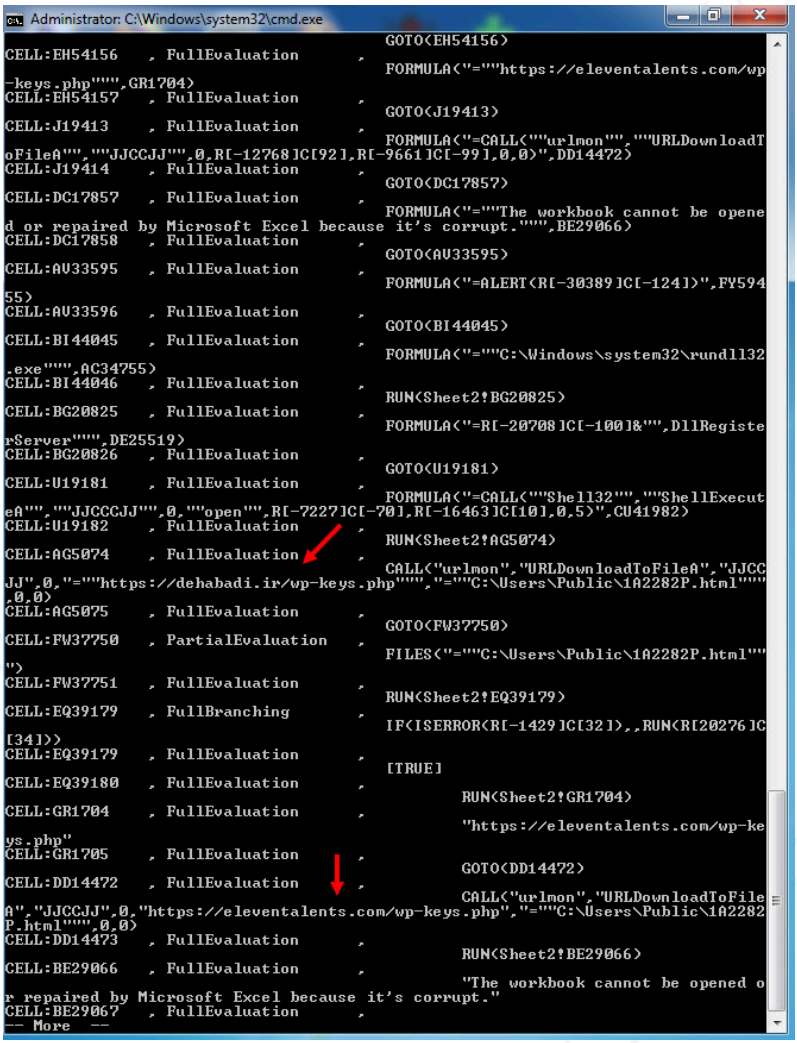




Bu yazı ile işin temelini öğrendiğinize göre bundan sonra

XLMMacroDeobfuscator gibi bir araç ile gizlenmiş XLM makroyu hızlıca çözebilir ve zamandan tasarruf edebilirsiniz. ? Bu yazının XLM makro analizi yapmak isteyen analistlere ışık tutacağını ümit ederek bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.



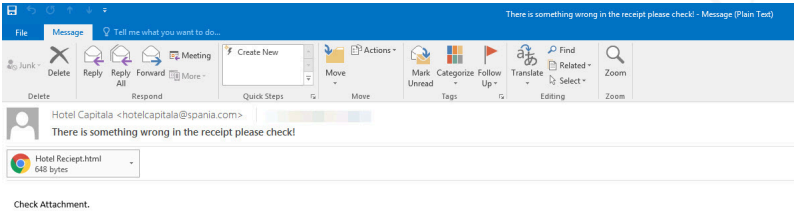


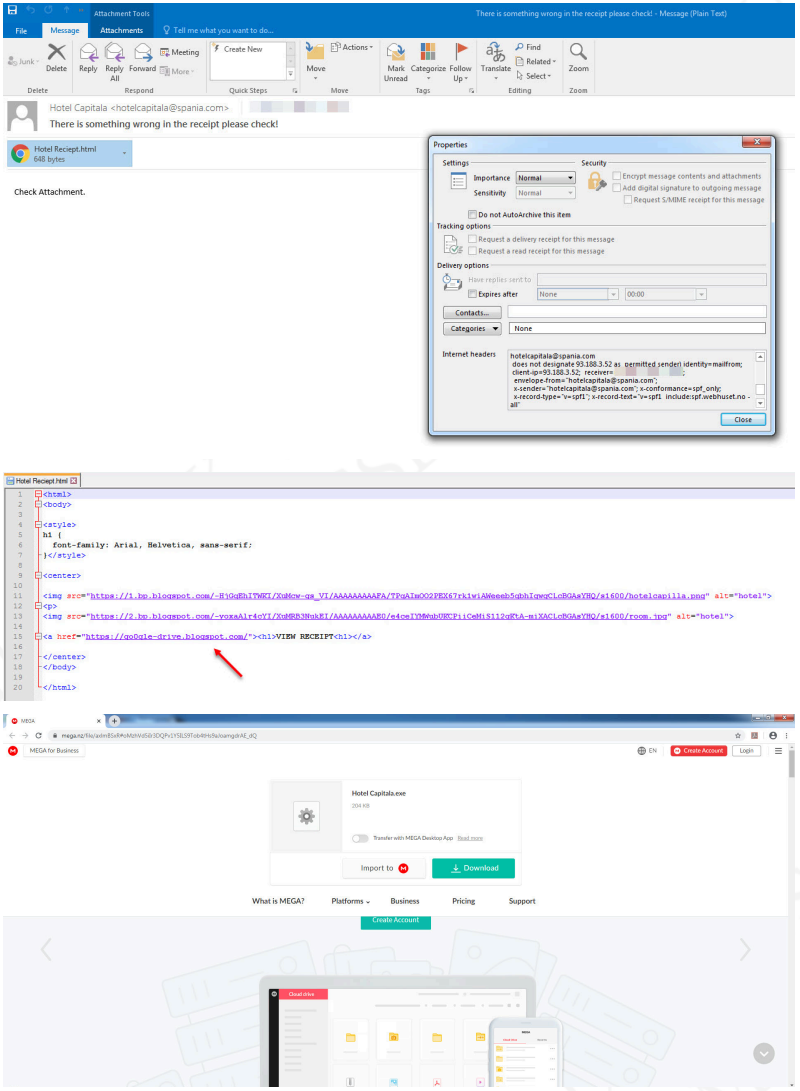
Not: XLM makro analizine dair daha fazla kaynak arayanlara şu yazılara da (#1, #2, #3, #4, #5) göz atmalarını tavsiye edebilirim.

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

Kaçabilirsin ama Saklanamazsın

Evvel zaman içinde, kalbur saman içinde; pireler berber, develer tellal iken bir tehdit aktörü varmış. Bu tehdit aktörü hedef aldığı kurumlardaki üst düzey çalışanlara ekinde bir HTML dosyası bulunan bir e-posta göndermiş. Bu HTML dosyası açılır ve içindeki bağlantı adresi (**https://go0gle-drive[.]blogspot[.]com**) takip edilirse, hedef alınan kişi mega.nz isimli dosya saklama ve paylaşım sitesindeki bir adrese (**https://mega[.]nz/file/axlmBSxR**) yönlendiriliyormuş. Bu dosya indirilip çalıştırılırsa, tehdit aktörü tarafından hedef sistem uzaktan yönetilerek ses, görüntü, tuş kaydı da dahil olmak üzere her türlü kötülük yapılabiliyormuş. Rivayete göre de ağ tabanlı kum havuzu sistemlerinden bazıları, tehdit aktörü tarafından gönderilen bu HTML dosyasında yer alan bağlantı adresini analiz edemiyormuş.

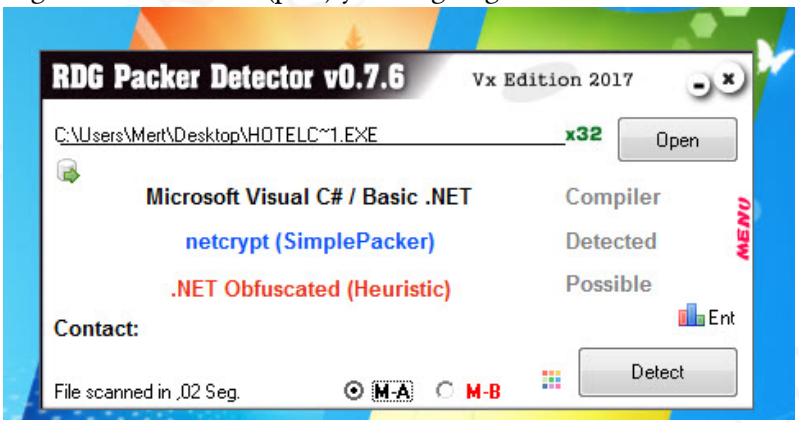


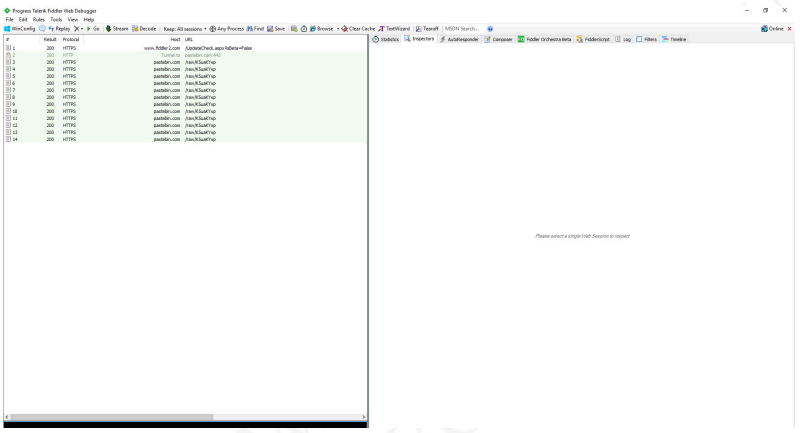


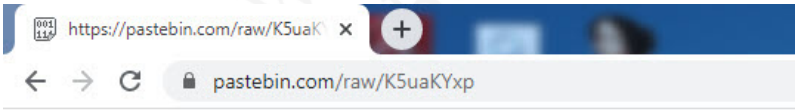
Bir kurum yukardaki gibi bir senaryo ile karşılaştığında, saldırı girişimi başarıya ulaşmasa da konuyu büyük bir dikkatle ele almalıdır çünkü bu öncü bir sarsıntı olup ardından gelecek büyük depremin işaretçisi olabilir dolayısıyla bu girişimin hedefli (Spear

Phishing), organize mi (APT) yoksa çok sayıda kullanıcıya gerçekleştirilen genel bir kampanyanın parçası mı sorularına da arka planda yanıt araması gerekir. Tabii bu soruların yanıtlarını bulması kimi zaman mümkün olmasa da yapılan analizler sayesinde bir fikir elde edilebilir. Ben de bu yazı ile bu sorulara yanıt aramaya koyuldum.

İlk olarak statik analiz ile dosyanın C# ile geliştirilip, paketlenmiş olduğunu gördüm. Dosyayı sanal bir sistem üzerinde çalıştırıp dinamik olarak analiz ettiğimde zararlı yazılımın Pastebin sitesindeki bir adrese eriştiğini öğrendim. Bu web adresini ziyaret ettiğimde sayfada bir ip adresi (**193.161.193.99**) ve bağlantı numarasının (port) yer aldığını gördüm.







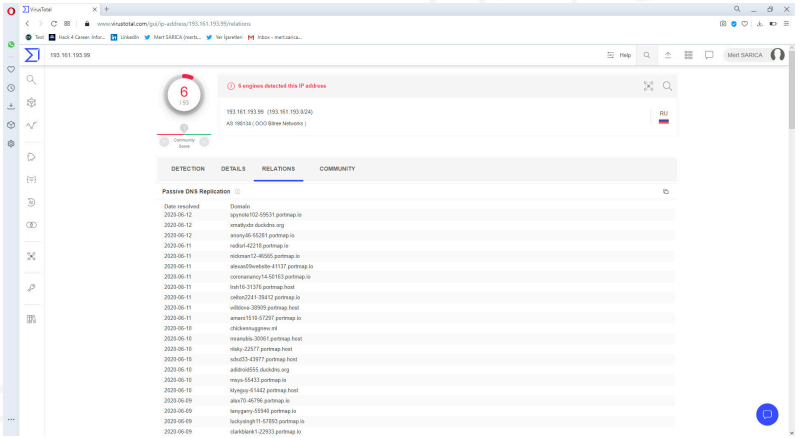

```
193.161.193.99:20614
```

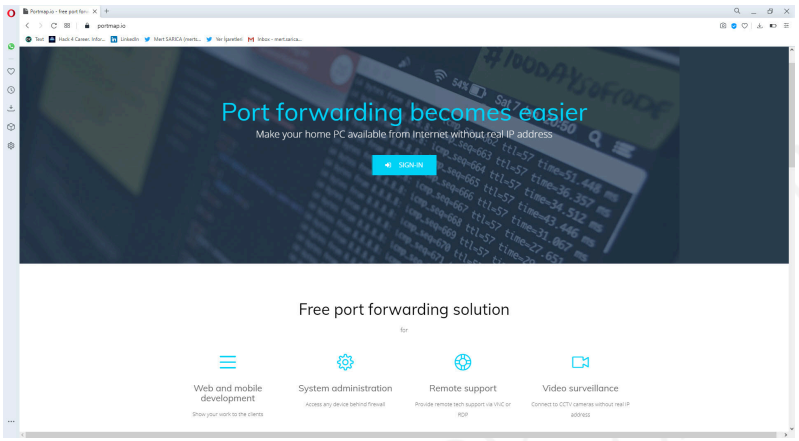
> Özellikle APT saldırılarında kullanılan zararlı yazılımlar tehdit aktörleri tarafından özel olarak geliştirildiği ve saldırıdan hemen önce derlendiği için VirusTotal'a yüklendiğinde çoğunlukla genel bir imza adı altında (Backdoor, Trojan vb) tespit edilmektedir. Bu gibi durumlarda Intezer gibi servislerden faydalanarak zararlı yazılımın kodunun başka hangi zararlı yazılımlarda kullanıldığını arayarak eşleştirme yapmanız ve tehdit aktörü konusunda bilgi edinmeniz söz konusu olabilir.

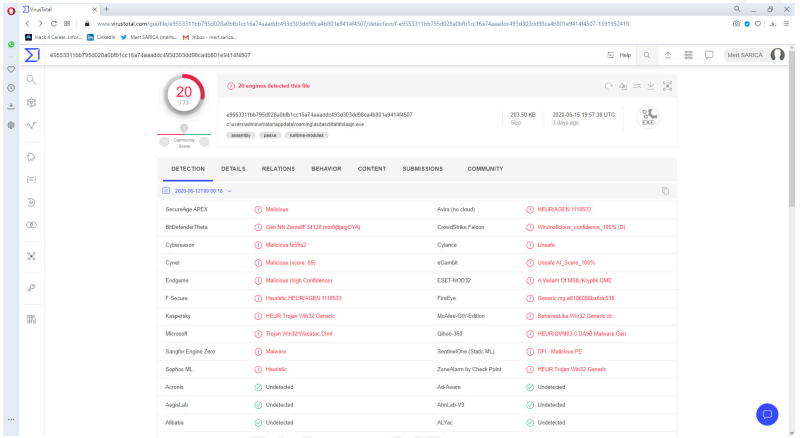
Bu zararlı yazılımı VirusTotal'a yüklediğim spesifik olarak bir zararlı yazılımla eşleştirilmediğini gördüm. Bunun üzerine Intezer

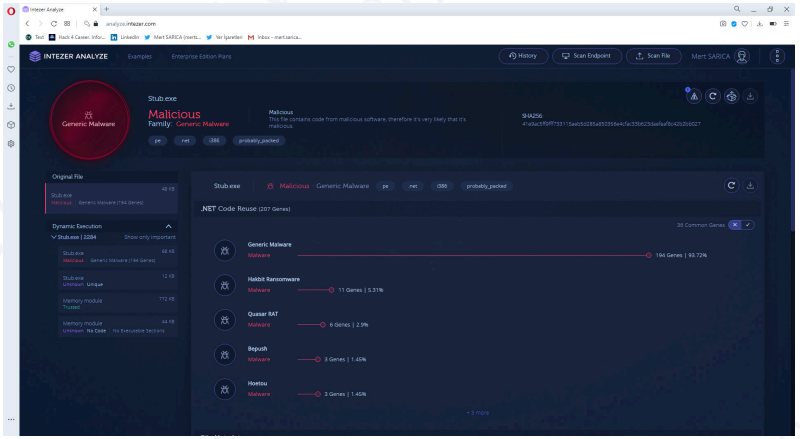
üzerinde arama yaptığımda da maalesef yine elim boş kaldı. (Generic Malware)

Pastebin.com sayfasından elde ettiğim ip adresini VirusTotal'da arattığımda bu ip adresinin bağlantı noktası yönlendirmek amacıyla hizmet veren Portmap.io servisine ait olduğunu öğrendim.

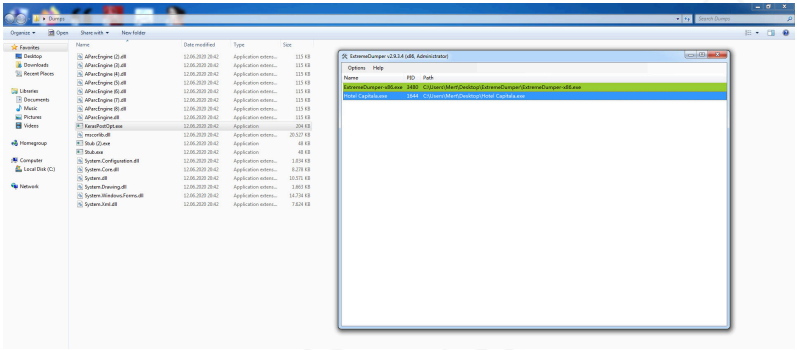




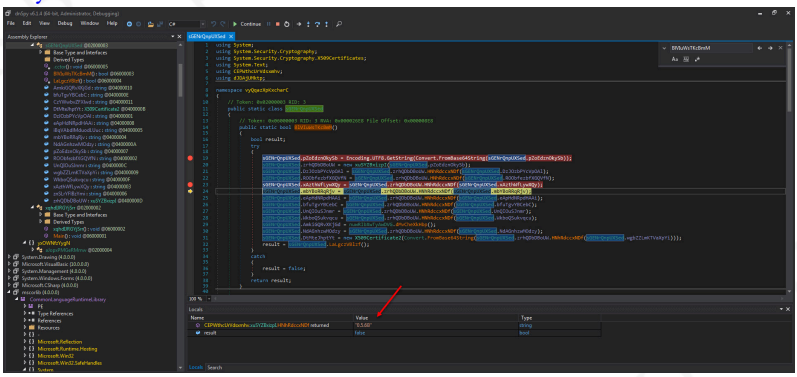


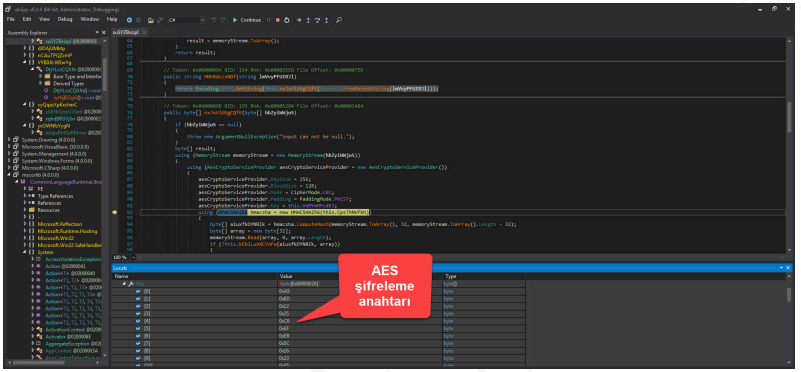


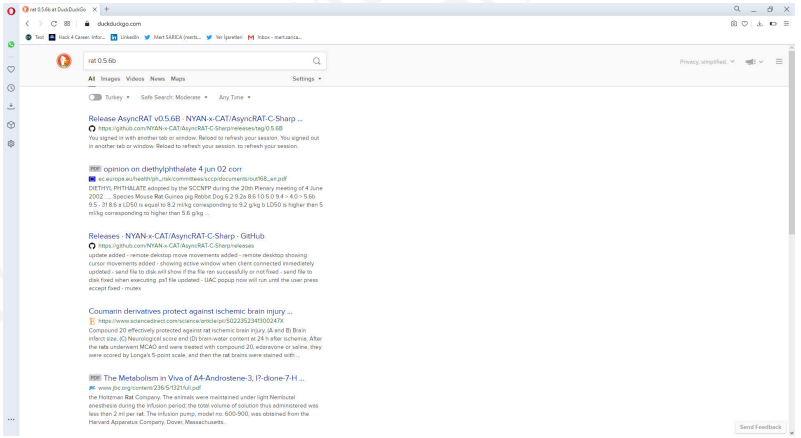
Kendisini gizlemek için elinden geleni yapan tehdit aktörünün geliştirmiş olduğu zararlı yazılımın ne olduğunu öğrenmek için araştırmaya devam ettiğimde sıra dinamik kod analizine geldi ve imdadıma OPSEC başlıklı yazımda kullandığım dnSpy hata ayıklayıcısı yetişti. dnSpy aracı ile hata ayıklamaya başlamadan önce paketlenmiş yazılımın bellekte gizlediği ana modülünü bulmak için ExtremeDumper aracını çalıştırdığımda ortaya kötülüklerin anası Stub.exe çıkmış oldu.



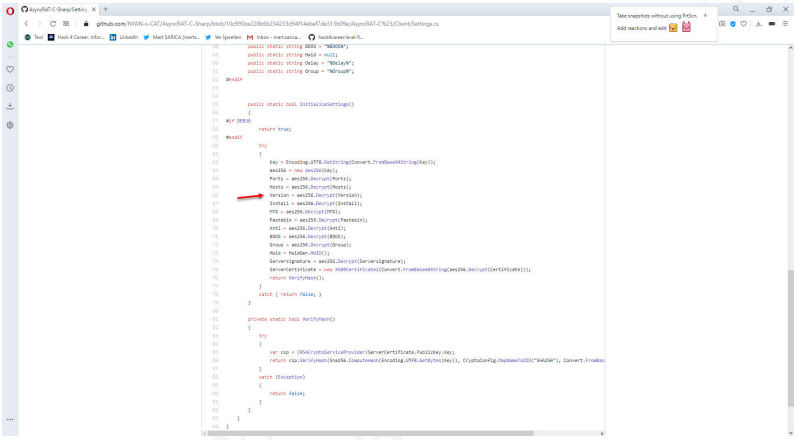
Stub.exe programını adım adım dnSpy ile analiz ettiğim bir noktada AES ile şifrelenmiş olup çözülen **0.5.6B** değeri dikkatimi çekti. Bu değeri Google'da "rat 0.5.6B" anahtar kelimeleri ile arattığımda bilin bakalım karşıma ne çıktı ? Açık kaynak kodlu AsyncRAT! ?



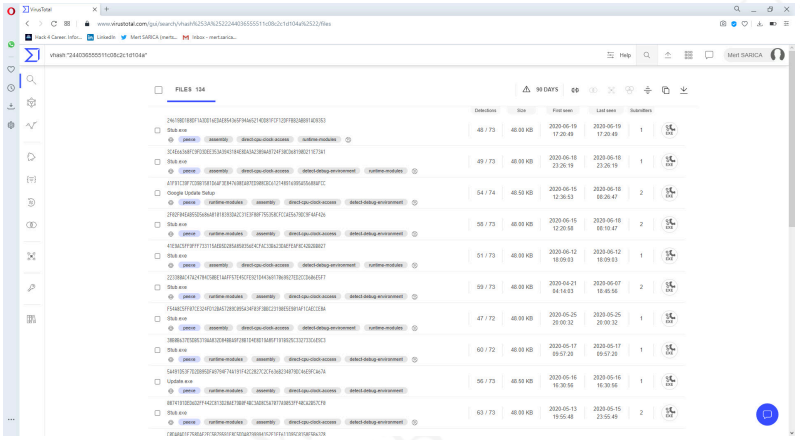




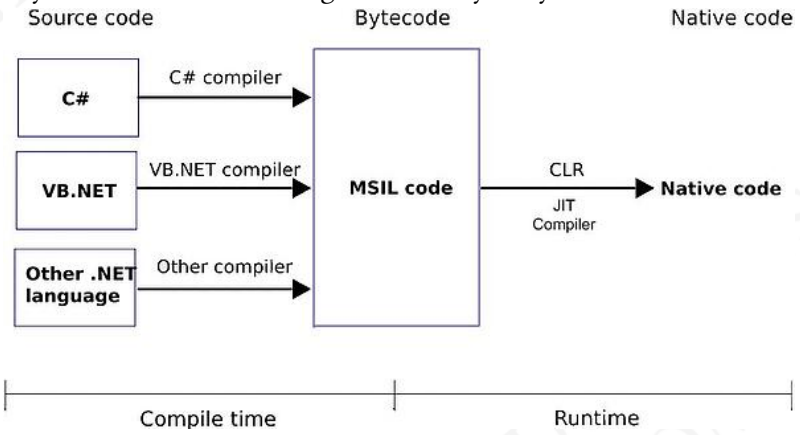
GitHub üzerinde bu projeyi detaylı bir şekilde incelediğimde analiz ettiğim zararlı yazılımın AsyncRAT olduğunu benzer kod bloklarından yola çıkarak doğrulayabildim.



Son aşamada Stub.exe dosyasının benzerlerini **vhash** ile VirusTotal üzerinde arattığımda çok sayıda örnek ile karşılaştım. Tüm bu örnekler, analiz ettiğim zararlı yazılımdaki Pastebin adresine mi sahip, ortak bir kampanyanın parçası mı diye merak içinde düşünürken ya 50'den fazla her bir örneğin analiz raporunu inceleyip bunu kontrol edecektim ya da tembellere yakışır çok kısa ve pratik bir yol bulacaktım. ? Hindi gibi düşünmeye başladıktan sonra aklıma Python ile tüm bu örnekleri statik olarak analiz ederek önce AES şifreleme anahtarını bulan ve ardından da konfigürasyon bilgilerini çıkaran bir araç hazırlama fikri geldi.

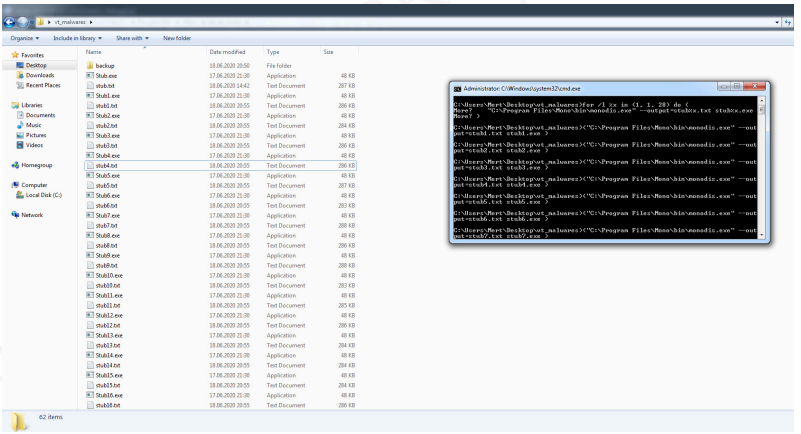


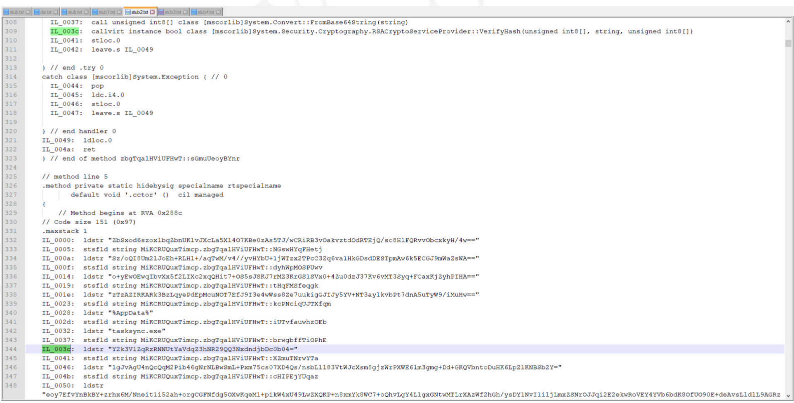
Tabii değişken isimleri her bir programda rastgele oluşturulduğu için öncelikle AES anahtarını statik bir değişkenden faydalanarak bulmam gerekiyordu. .Net ile geliştirilen programların derlendiğinde baytkoda (CIL/MSIL) çevrildiğini bildiğimiz için baytkod üzerinde statik değerler aramaya koyuldum.

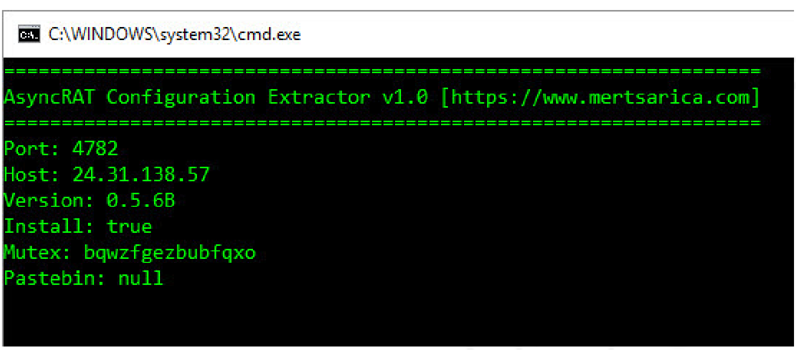


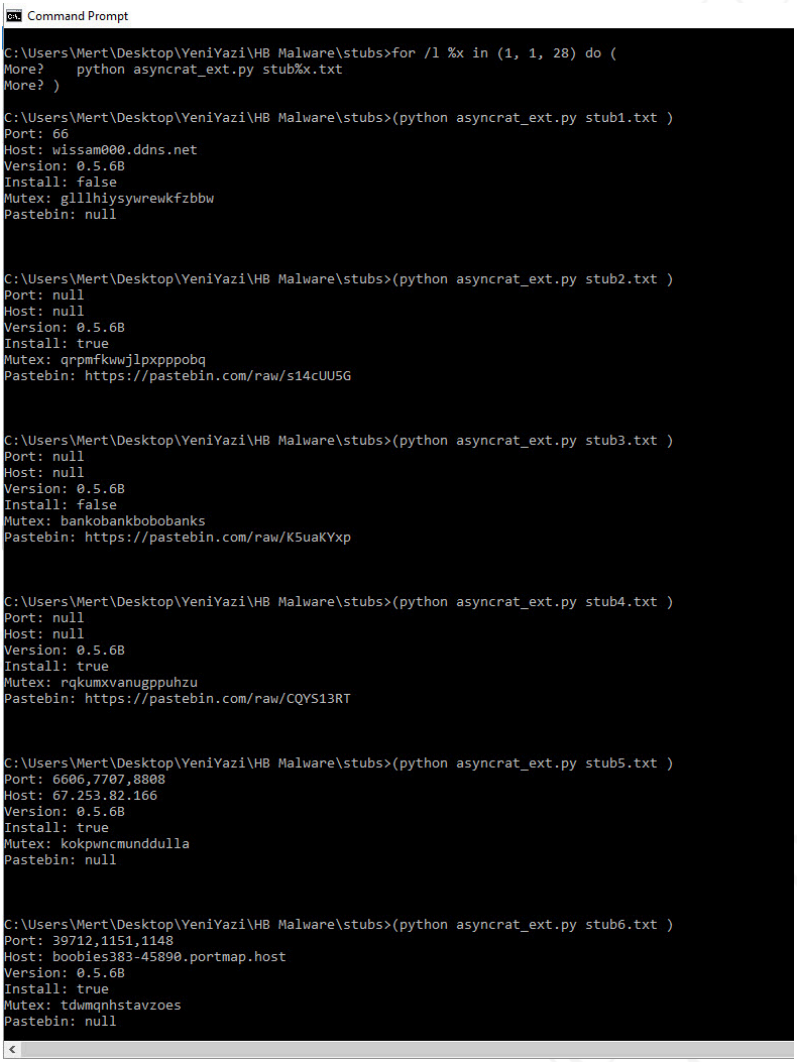
Bunun için meşhur Mono projesinde yer alan Mono Disassembler (monodis) aracından faydalanmaya karar verdim. Monodis aracı ile tüm Stub.exe örneklerini koda çevirdikten sonra AES şifreleme anahtarının her daim **0x288c** değerinden sonra gelen **IL_003c**

değerinde olduğunu tespit ettim. ve bu bilgilerden faydalanarak Python ile AsyncRAT Configuration Extractor aracını geliştirdim. Aracı tüm örnekler üzerinde çalıştırdığımda her birinin konfigürasyonunda yer alan bilgilerin, analiz ettiğim zararlı yazılımdan farklı olduğunu dolayısıyla analiz ettiğim zararlı yazılım ortak bir kampanyanın parçası olmadığını öğrenmiş oldum.






C:\WINDOWS\system32\cmd.exe
AsyncRAT Configuration Extractor v1.0 [https://www.mertsarica.com]
Port: 4782
Host: 24.31.138.57
Version: 0.5.6B
Install: true
Mutex: bqwzfgezbubfqxo
Pastebin: null



Sonuç itibariyle tüm bu bilgileri derleyip topladıktan sonra bu siber saldırı girişiminin bir APT saldırısı olmasa da hedeflenmiş bir saldırının (Spear Phishing) parçası olması terazide ağır basmış oldu. Özellikle Covid-19 salgınından sonra artan bu tür hedeflenmiş siber saldırı girişimlerine karşı kurumların ve

çalışanlarının çok dikkatli olmasını önerir bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Instagram Dolandırıcıları

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
Facebook

Profili Gör

Dün 22:24

İnstagram telif hak ihlali !

Güvenliğiniz bizim sorumluluğumuz.

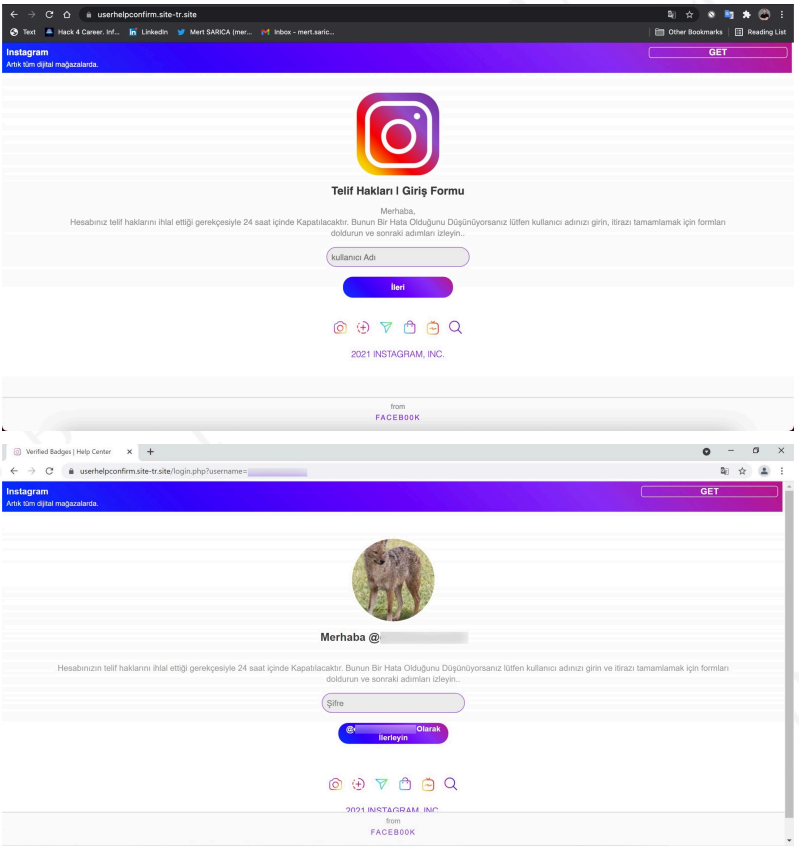
Hesap incelendi ve telif ihlali gerçekleştirdiği anlaşıldı.

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

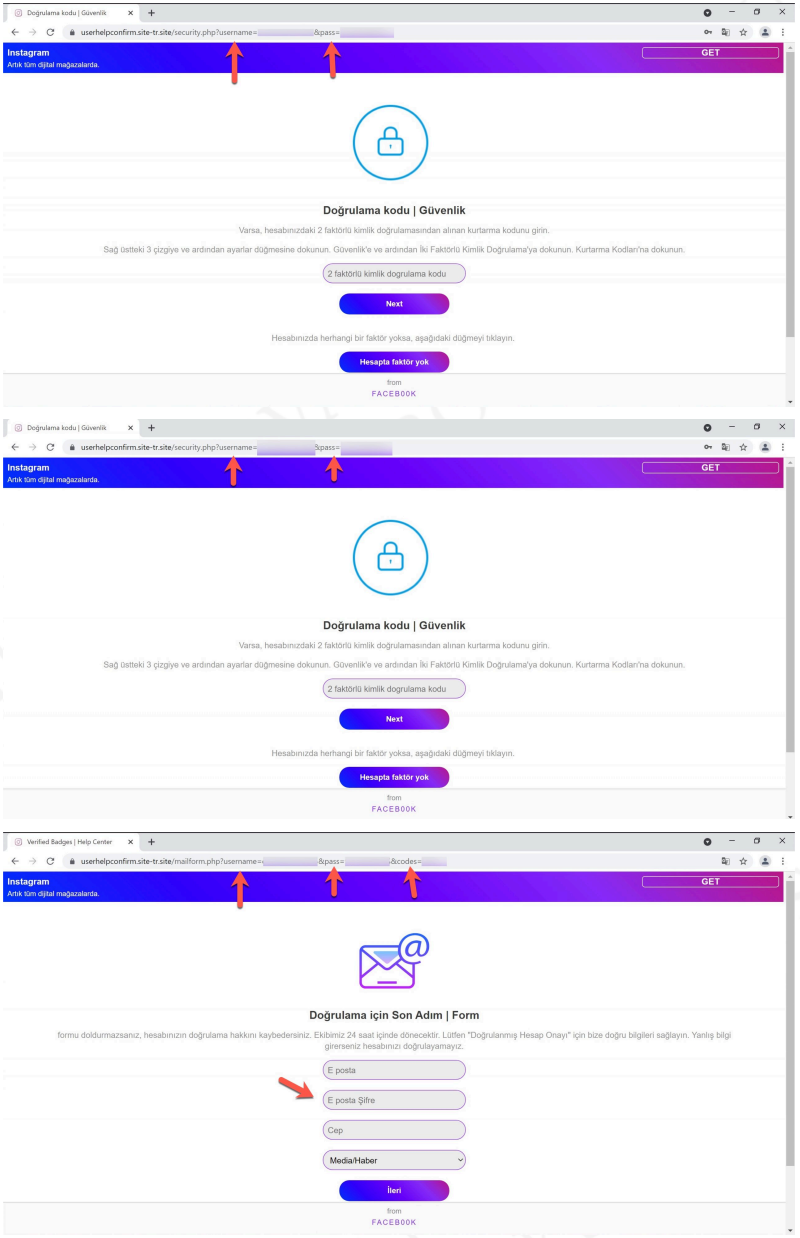
Hesabınız bu şartlar yerine getirildikten sonra , bir doğrulama kodu gönderilerek güvenli hale


Ara
Telif Hakları
Arkadaşı Ekle
Mesaj
Telif'in Hakkında Bilgilerini Gör
Arkadaşlar
Gönderiler
Fotoğraflar

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.

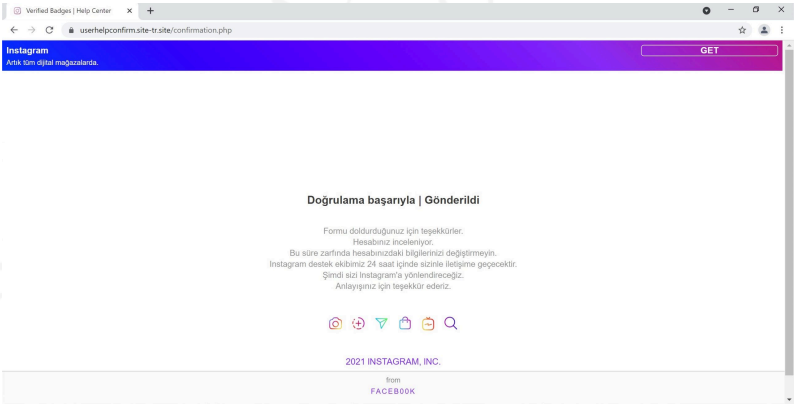


Şayet hesap iki faktörlü kimlik doğrulaması ile korunuyorsa (kullanmanızı şiddetle tavsiye ediyorum), oltalama sayfası doğru parola girildikten hemen sonra kullanıcıdan doğrulama kodunu (sms veya giriş kodu) ve yetmezmiş gibi bir de üzerine e-posta adresini ve parolasını girmesini istiyordu.



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

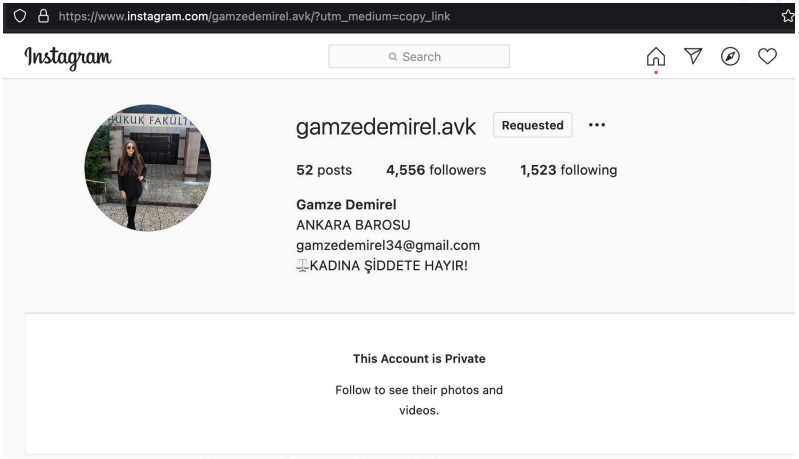
Profili Gör

21 Eki 11:24

merhaba iyi günler rahatsızlık vermiyorum umarım

21 Eki 16:17

Türkiyede son dönemlerde kadınların ve çocukların hedef olduğu şiddet olaylarını haberlerde izliyorsunuzdur mutlaka, bu durumlara farkındalık



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

🙏

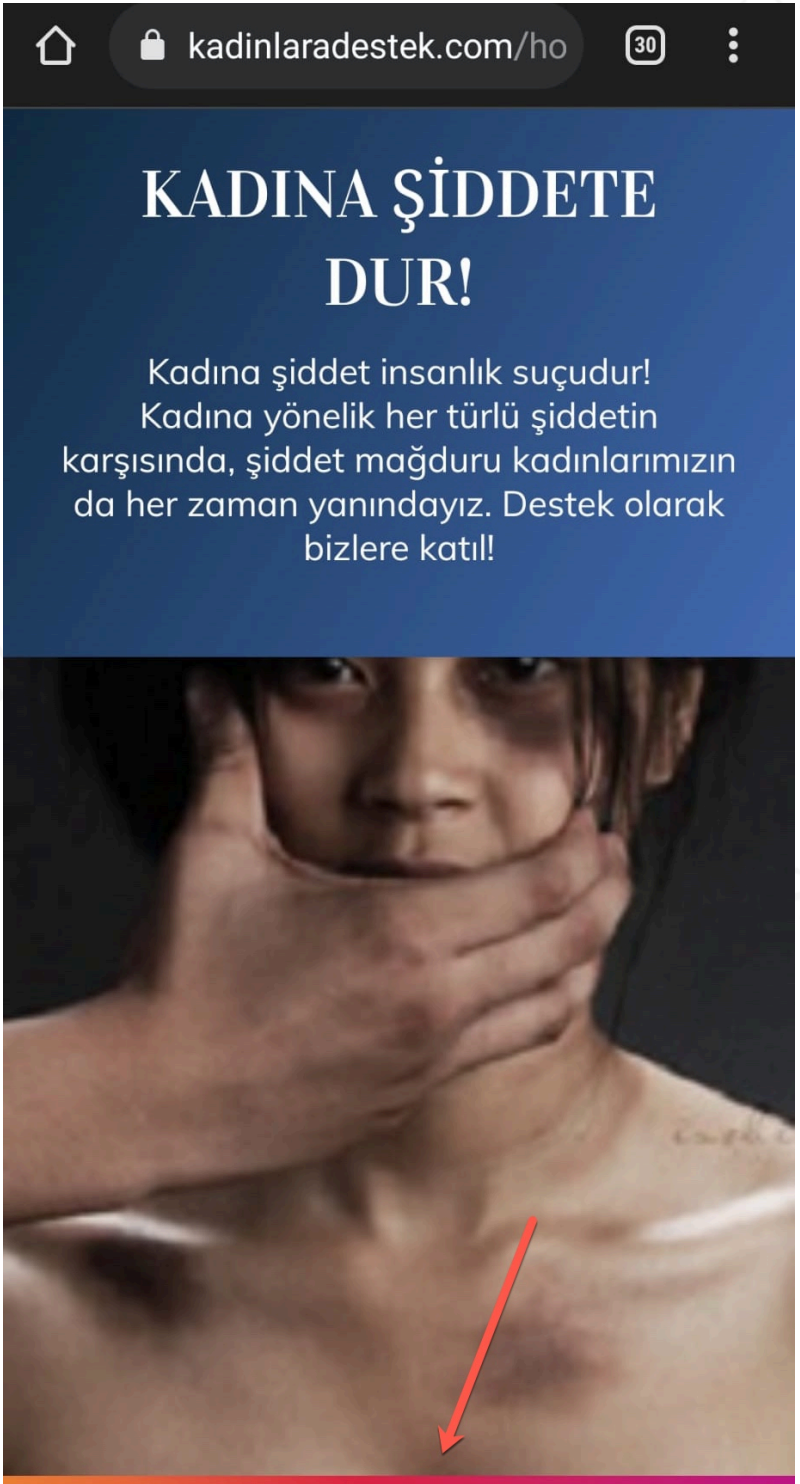
Bugün 11:19

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

Kadın Şiddetine Hayır

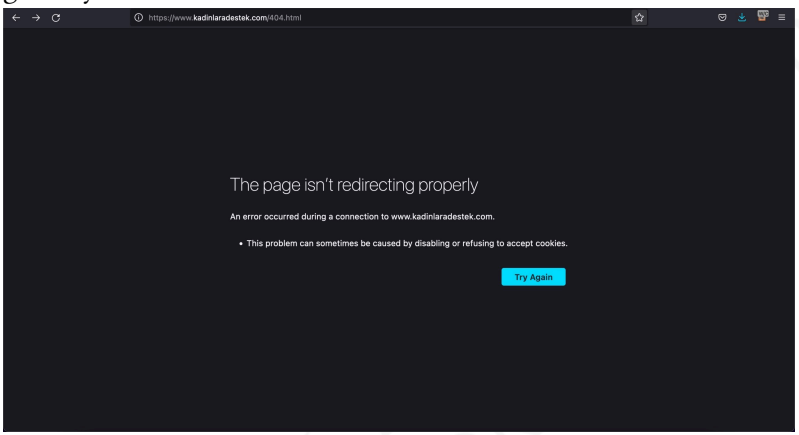
Kadına şiddet insanlık suçudur! Kadına yönelik her türlü şiddetin karşısında, şiddet mağduru kadınlarımızın da her zaman yanı...

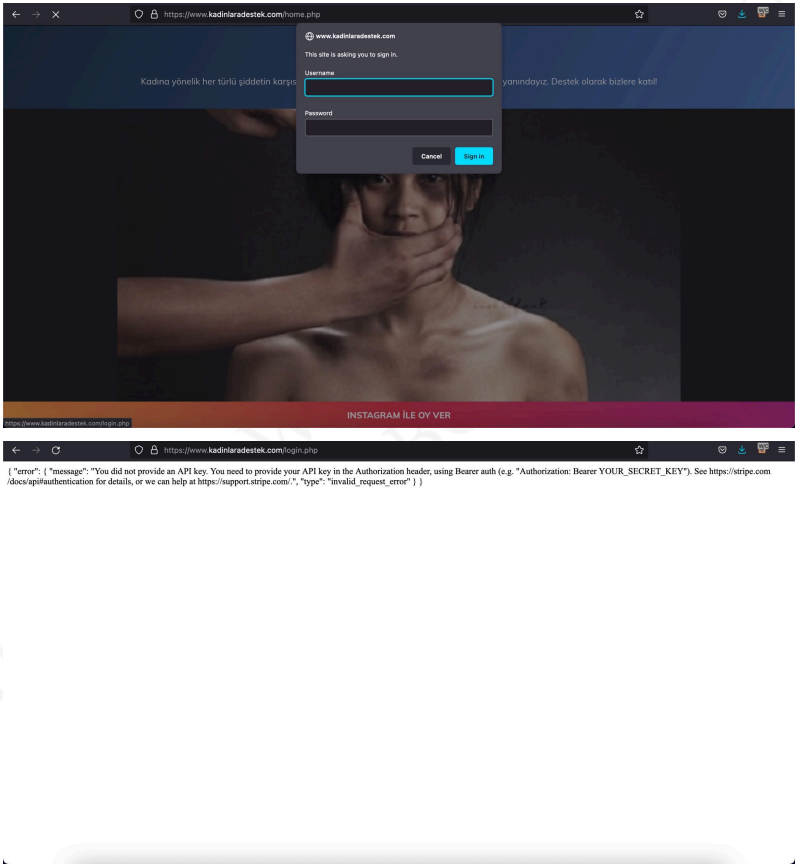
Merhaba iyi günler efendim listede adınızı göremedim destek olmamışsınız da, umarım bu duruma duyarsız kalmayıp desteğinizi gerçekleştirirsiniz. Kampanyamızın süresinin dolmasına çok az bir süre kaldı😊🙏


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!

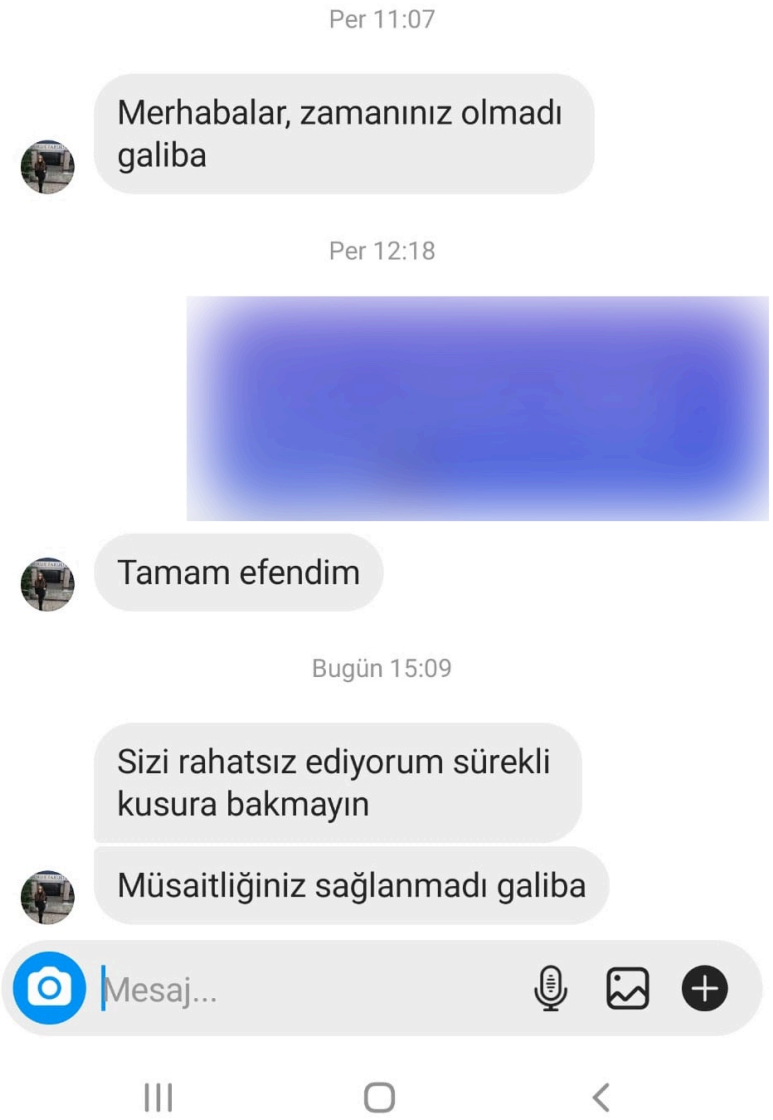
Web sitesini ziyaret ettiğimde, dolandırıcının uzun bir süre operasyonuna devam edebilmek için çeşitli teknik tedbirler aldığını farkettim. İlk olarak **https://kadinlaradestek[.]com** adresine direkt gitmeye çalıştığımda web sitesi 404 (sayfa bulunamadı) hata döngüsüne girerek açılmamaktaydı. Siteye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



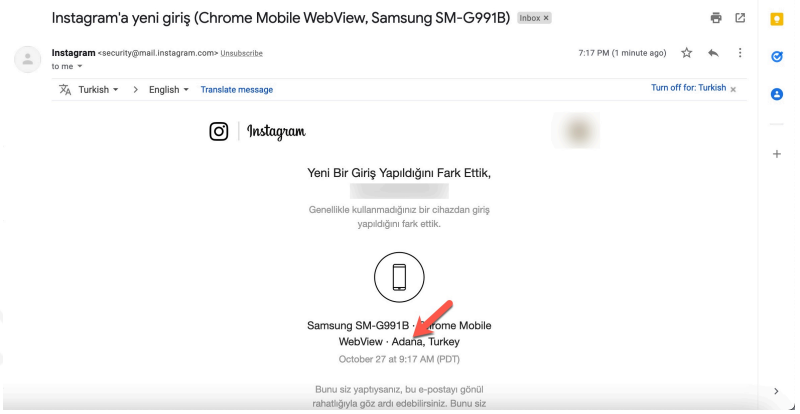


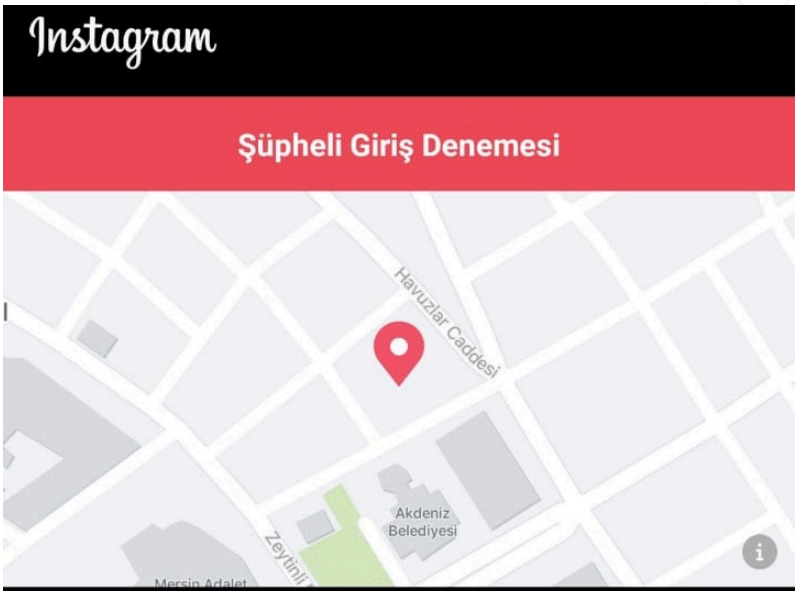
Avına odaklanmış bir aslan misali hedef aldığı kullanıcının bilgilerini çalıp çalamadığını yakından takip eden dolandırıcı 28 Ekim ve 1 Kasım tarihlerinde tekrar iletişime geçmişti.



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.



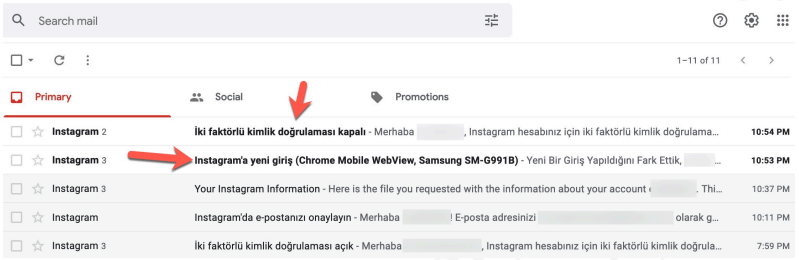


Olağandışı Bir Giriş Denemesi Saptadık

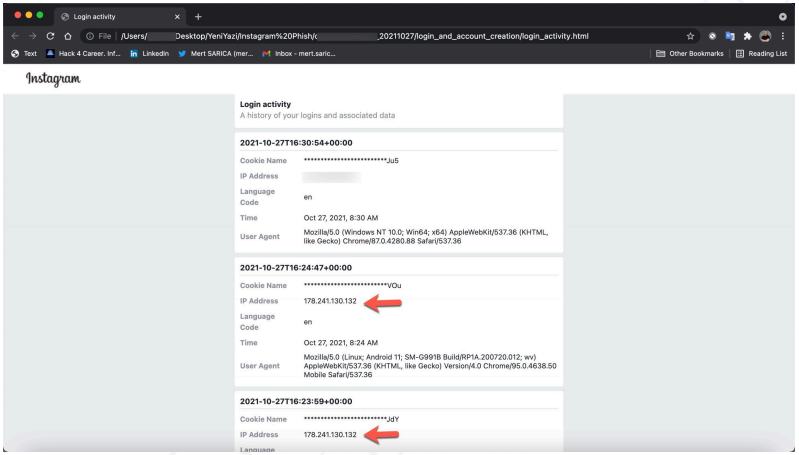
Android | 27.10.2021 22:01
Mersin

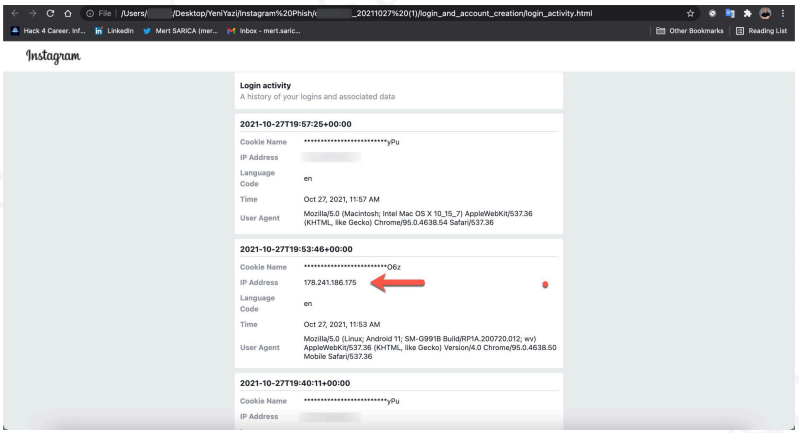
Hesabını güvene almak için bunu yapanın sen olduğunu bize bildir.

Bunu Ben Yapmadım



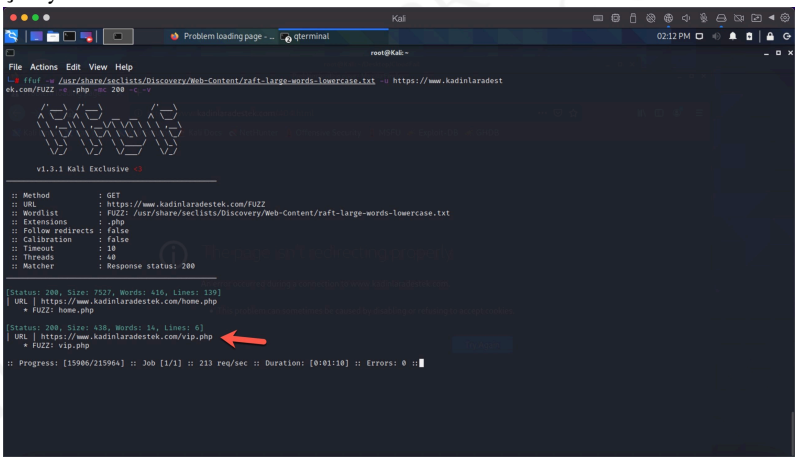
Sıra giriş yapan dolandırıcıların IP adreslerini bulmaya geldiğinde öncelikle Instagram mobil uygulamasında **Ayarlar -> Güvenlik -> Verileri İndir** adımlarından Instagram hesabım ile ilgili bilgileri talep etmem gerekiyordu. Bilgilerin hazır olduğuna dair Instagram'dan e-posta aldıktan sonra ilgili 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.

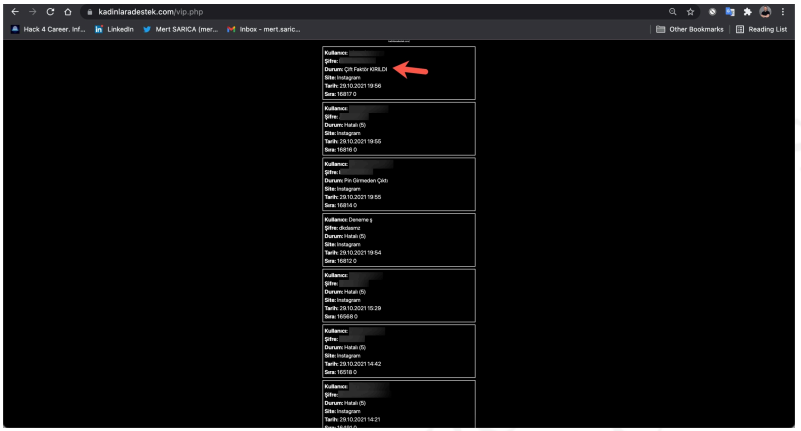


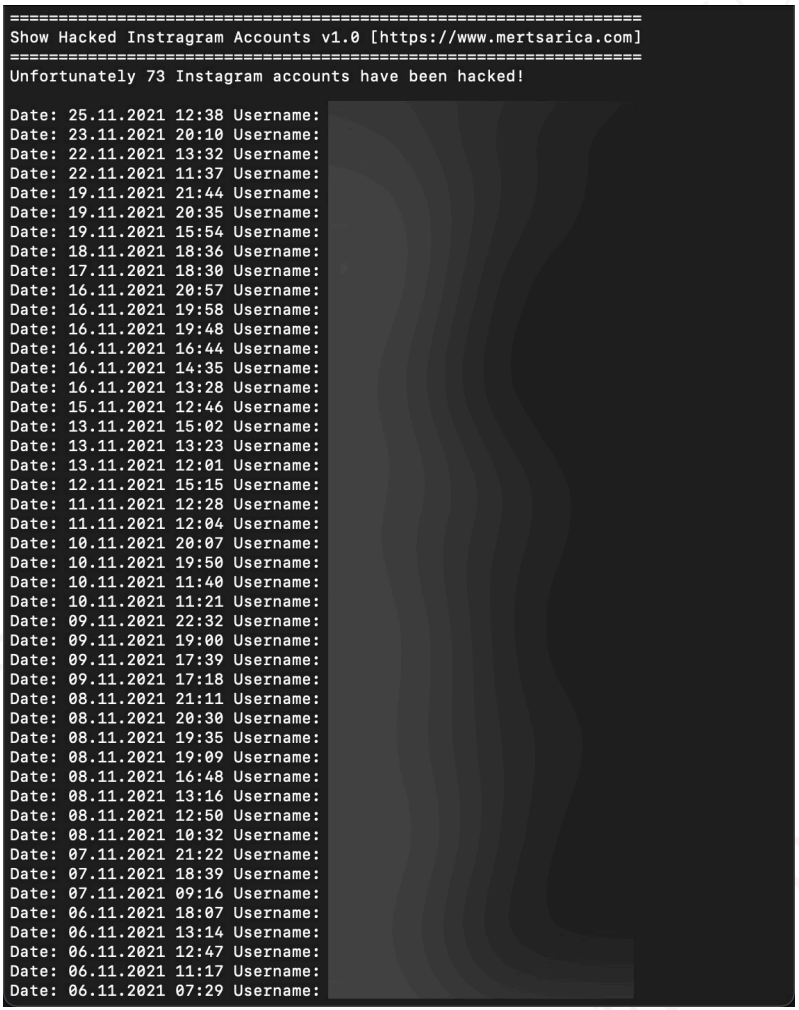


Son olarak sıra bu dolandırıcıların oltasına düşen masum kullanıcıları tespit etmeye geldiğinde, ofansif güvenlik uzmanlarının da yakından bildiği **ffuf** aracı ile web sitesindeki PHP dosyalarını keşfetmek için işe koyuldum. Çok geçmeden ffuf aracı web sitesi üzerinde **vip.php** isimli bir dosya olduğunu 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.