2FA ATLATMA YOLLARI

Hangi Yöntemleri Öğreneceğiz

E-mail Phishing

En yaygın yoldur. Fakat insanların bilinçlenip, E-mail filtrelerinin gelişmesiyle birlikte hackerların işi zorlaşmıştır.
SMTP Spoofing gibi yeni yöntemler türetilmiştir.
Kuzey Kore temelli “Lazarus Group” hala bu yöntemi aktif olarak kullanmaktadır

SMS Cloning

Akla ilk gelen ve en çok kullanılan 2fa yöntemi olmasından dolayı piyasada çok fazla spyware vardır.
Genellikle masum görünen bir uygulama yoluyla yada uzaktan erişim sağlanarak kullanılır.
2016 yılında duyulan “Pegasus” casus yazılımı buna bir örnektir.

Cookie Hijacking

Son dönemlerde ele geçirilen büyük sosyal medya hesaplarıyla ismini sıkça duyurmuştur. Genellikle E-mail Phishingin devamında kullanıcıya bir dosya yükletilmesiyle gerçekleştirilir.

En etkili ve uzun süreli yöntemdir.

E-MAIL PHISHING

Kullanılan alt yöntem vardır

01

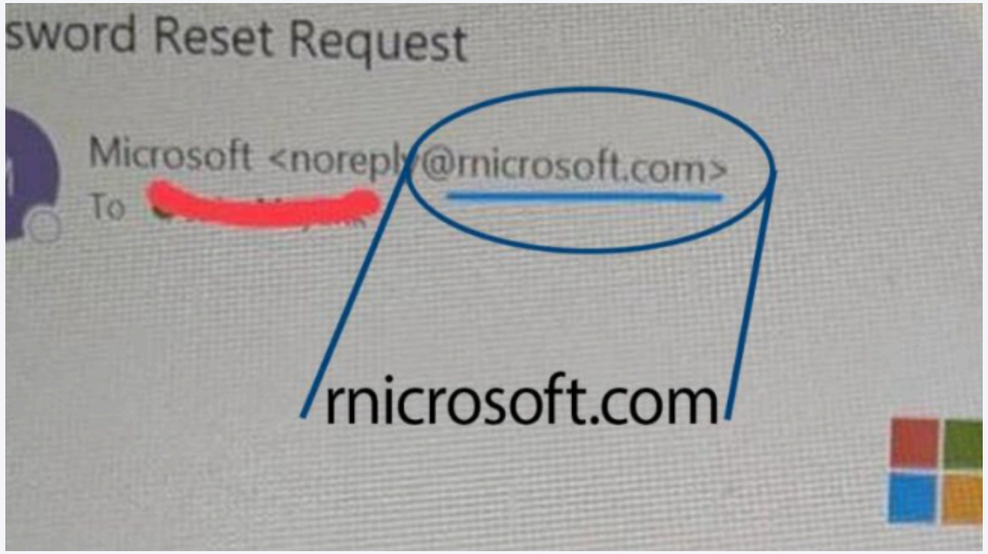
Benzer Domain kullanımı

02

SMTP Spoofing

BUNLAR GERÇEK MI?

Sistemin en zayıf halkası her zaman insanlar ve onların dikkatidir



SMTP SPOOFING

Saldırganların, kendi kurduğu bir sunucudan maili atarken teknik kısma kendi adresini yazsa bile, "Header" kısmına elinde hiçbir yetki olmasa dahi google.com yazabilmesidir.

```
mail from: dude1@domain1.com
rcpt to: dude2@domain2.com
data
```

Envelope

```
From: Dude1 <dude1@domain1.com>
Subject: Nice To Meet You!
Date: February 13, 2018 3:30:58 PM PDT
To: dude1 <dude1@domain1.com>
Reply-To: dude2 <dude2@domain2.com>


Hi Dude1,

It's nice to meet you!
```

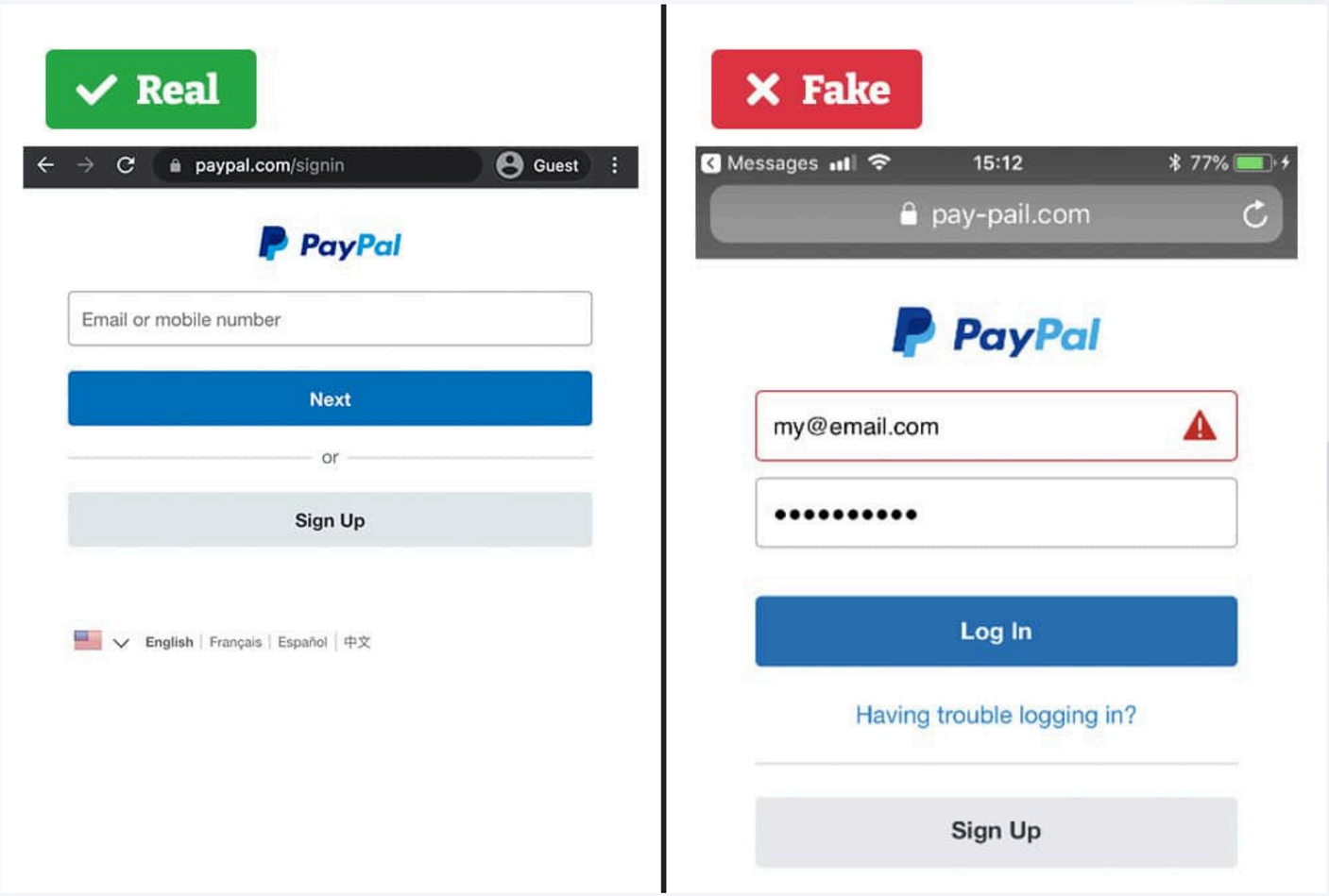
Header / Body

OLTALAMA SONRASINDA NELER OLUYOR?

SAHTE SITE

Bu basit ve sık kullanılan yöntemdir. Kurban e-maildeki linkten bir websitesine yönlendirilir.

Giriş yapan kurbanın doğrulama kodu kopyalanır



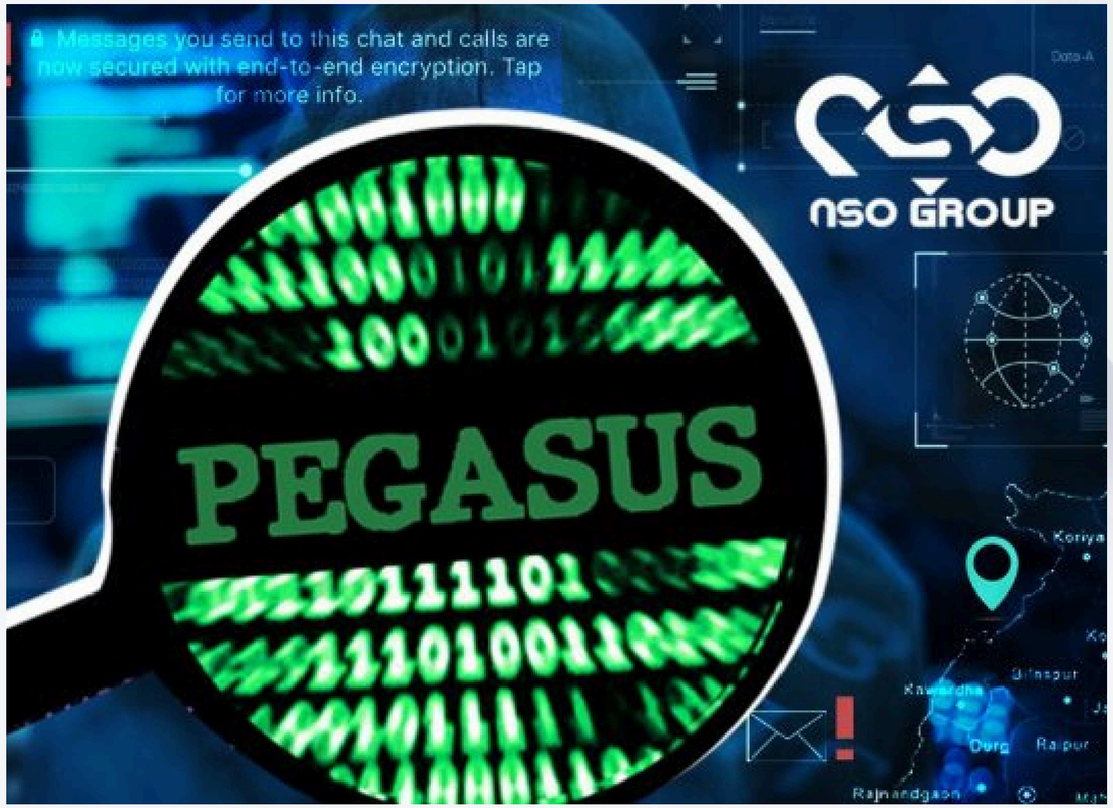
COOKIE HIJACKING

Bu en tehlikelisidir.
Hackerlar kurbanın tarayıcısına özgü cookie'leri kopyalayarak kendi tarayıcısının sanki kurbana aitmiş gibi çalışmasını sağlar.
Bu yöntemden kurtulmak zordur.

1.UYGULAMA VIDEOSU

SMS CLONING

Güncel olarak en çok kullanılan saldırıdır.
Bu saldırı SS7 ile karıştırılmamalıdır.
Pegasus en iyi örnektir.



2.UYGULAMA VIDEOSU

uygulama videoları ve kaynak kodu için: https://github.com/Yarasarda/BS439_2FA_Atlatma

HAZIRLAYANLAR

1030521228
Merve Nisa kapan

1030521224
Arda Kaan Özsoy

Bizi dinlediğiniz için Teşekkürler