

E-Mailleriniz Başkaları Tarafından Okunabilir mi?



Mustafa Serhat Dünder

Genel Bakış

- Yapabileceklerinizin hayal gücünüzle sınırlı olduğu internet dünyasında bu sorunun cevabı; “Evet, uygun şartlar sağlanılırsa istenildiği zaman herkesin e-mailleri okunabilir.”
- E-Maillerinize erişimdeki güvenlik zaafları kullanıcı taraflı olabileceği gibi, sunucu ve köprü taraflı da olabilir.
- Genel olarak zaaf kullanıcı kaynaklıdır.
- Nasıl saldırıldığını bilmeden asla nasıl korunacağınızı bilemezsiniz...

E-Maillerim Okunsa Ne Olur?

- E-Mail hesabınızda özel hayatınızla ilgili yazışmalar bulunuyor olabilir.
- Web uygulamalarında kullanılan parola sıfırlama özelliği ile üye olduğunuz tüm sitelerdeki hesaplarınız hacklenebilir !
- E-Mail adresiniz üzerine kayıtlı herhangi bir domain-hosting hizmeti varsa web uygulamanız hacklenebilir !
- Sizin adresiniz ile; kişisel veya yasal olarak zor durumda kalacağınız şeyler yapılabilir.
-
-

Tamamen saldırganın hayal gücü ile sınırlı.

Temel Saldırı Senaryoları

- Gizlilik Adımındaki Eksiklik
- Brute Force
- Fake Mail
- Phishing
- Keylogger-Trojan
- Şifre Politikaları
- Uygulama Zaafları
- Sosyal Mühendislik

XSRF-CSRF-XSS

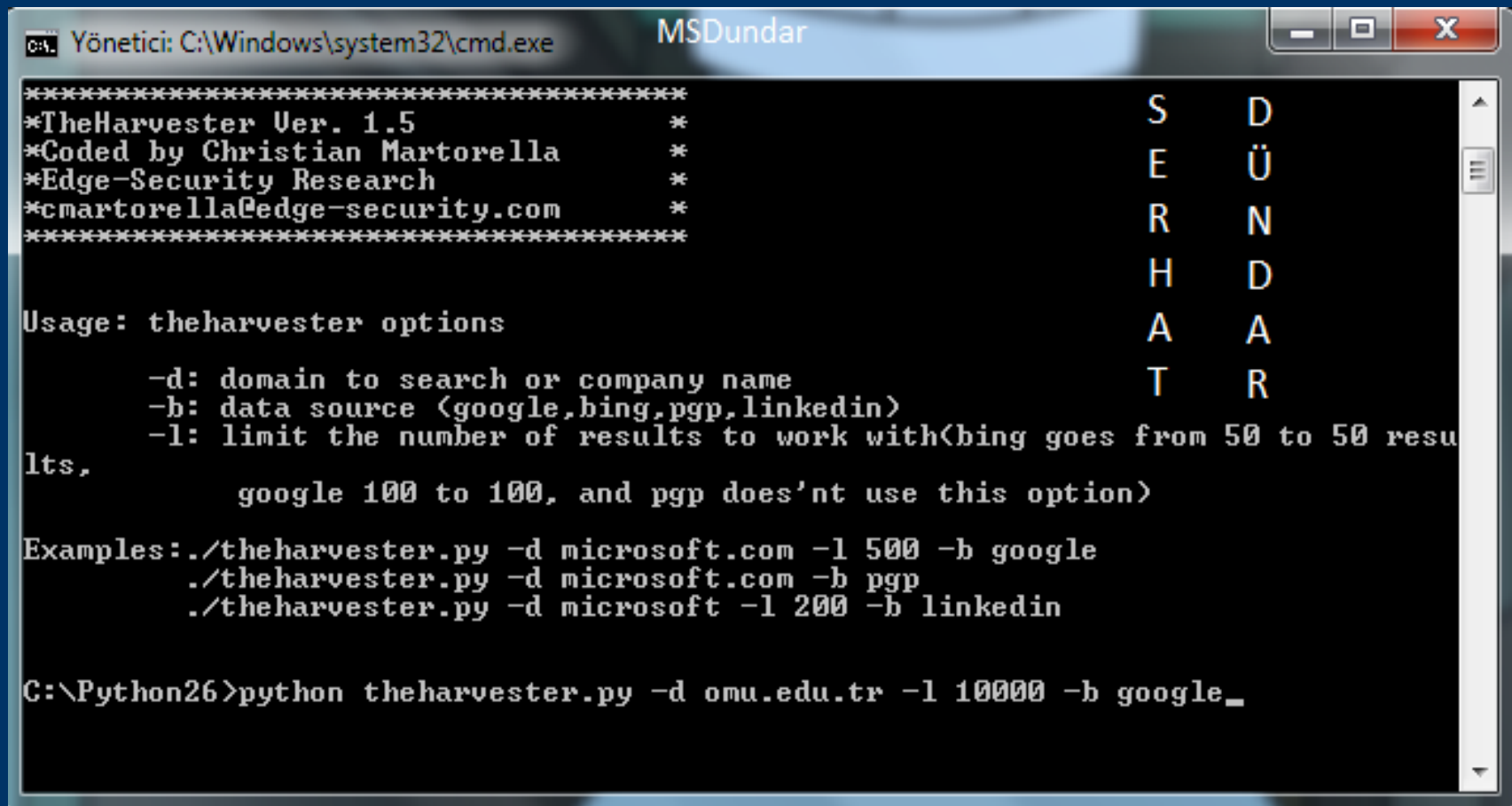
- Clickjacking
-
-

Gizlilik Adımındaki Eksiklik

- Başkaları tarafından ele geçirilmesini istemediğiniz mail adresinizi asla herhangi bir yere üye olmak için kullanmayınız !
 - Herhangi bir web sayfasına üye olduğunuz anda o sayfanın arama motorlarının robotları tarafından indexlenmesi sonucunda mail adresiniz “bulunabilir” olacaktır. Diğer bir ihtimal ise üyelik profilinizden adresinizin okunabilmesidir.
 - Arama motoru kayıtlarına mail adresiniz girdiği anda spam listelerine de girdiniz demektir, brute force ile saldırı yapanlarında “tesadüfen” saldırı listesine dahil olabilirsiniz.
 - Üye olduğunuz web uygulamasının veri tabanı hacklendiği zaman büyük bir ihtimalle üyelik için kullandığınız şifre de ele geçirilecektir. Genel olarak kullanıcıların birçok yerde aynı şifreyi kullandığını düşünürsek bu ciddi bir durum.
-
-

Gizlilik Adımındaki Eksiklik - 2

- Arama motorları robotlarınca adresiniz tanındığı zaman, saldırgana basit bir python uygulaması olan harvester gibi yazılımları kullanmak düşer.



```
Yönetici: C:\Windows\system32\cmd.exe    MSDundar

*****
*TheHarvester Ver. 1.5                    *
*Coded by Christian Martorella           *
*Edge-Security Research                   *
*cmartorella@edge-security.com            *
*****

Usage: theharvester options

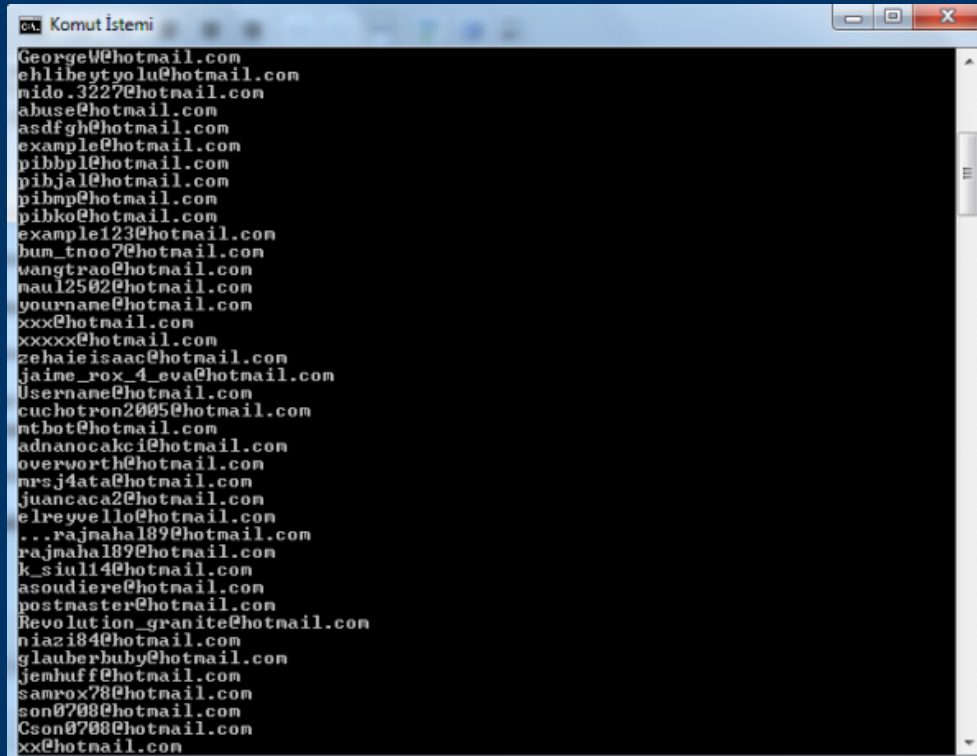
      -d: domain to search or company name
      -b: data source (google,bing,pgp,linkedin)
      -l: limit the number of results to work with(bing goes from 50 to 50 results,
           google 100 to 100, and pgp does'nt use this option)

Examples: ./theharvester.py -d microsoft.com -l 500 -b google
          ./theharvester.py -d microsoft.com -b pgp
          ./theharvester.py -d microsoft -l 200 -b linkedin

C:\Python26>python theharvester.py -d omu.edu.tr -l 10000 -b google_
```

Gizlilik Adımındaki Eksiklik - 3

- Harvester spam listesi hazırlamakta da kullanılabilir..
- Hotmail uzantısına sahip, google arama motoru ile bulunabilen tam 13 milyon mail adresi var şuan. Aslında daha da çoğu var ancak google belli bir sayfa sayısından sonra listeleme yapmıyor güvenlik açısından. Geri kalanını bing ve linkedin'den aratıp liste genişletilebilir.



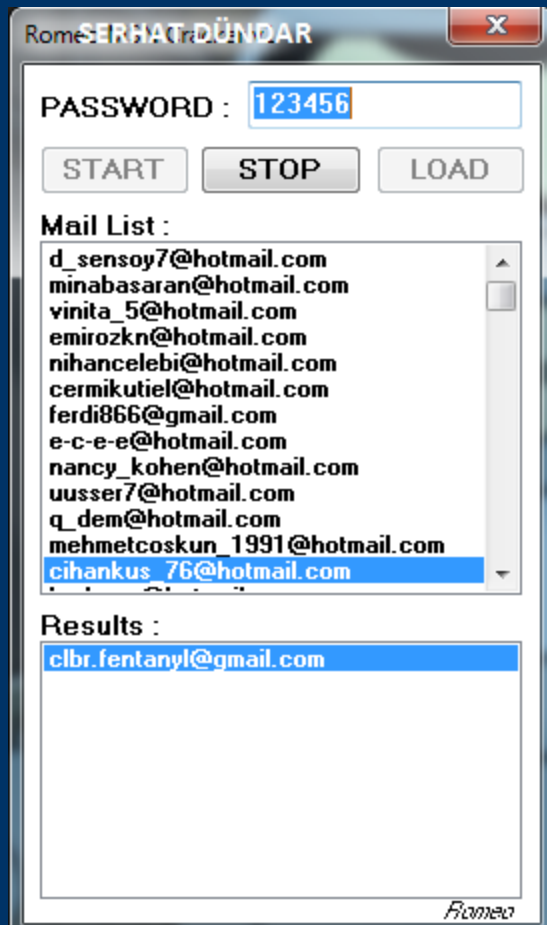
```
Komut İstemi
GeorgeW@hotmail.com
ehlibeytyolu@hotmail.com
mido.3227@hotmail.com
abuse@hotmail.com
asdfgh@hotmail.com
example@hotmail.com
pibbpl@hotmail.com
pibjal@hotmail.com
pibmp@hotmail.com
pibko@hotmail.com
example123@hotmail.com
bum_tnoo7@hotmail.com
wangtrao@hotmail.com
maul2502@hotmail.com
yourname@hotmail.com
xxx@hotmail.com
xxxxx@hotmail.com
zehaieisaac@hotmail.com
jaime_rox_4_eva@hotmail.com
Username@hotmail.com
cuchotron2005@hotmail.com
ntbot@hotmail.com
adnanocakci@hotmail.com
overvorth@hotmail.com
nrsj4ata@hotmail.com
juancaca2@hotmail.com
elreyvello@hotmail.com
...rajmahal89@hotmail.com
rajmahal89@hotmail.com
k_siull14@hotmail.com
asoudiere@hotmail.com
postmaster@hotmail.com
Revolution_granite@hotmail.com
niazi84@hotmail.com
glauberbuby@hotmail.com
jenhuff@hotmail.com
samrox78@hotmail.com
son0708@hotmail.com
Cson0708@hotmail.com
xx@hotmail.com
```

Brute-Force (Kaba Kuvvet)

- Kimi yazılımlar wordlistleri (kelime listeleri), kimi yazılımlar rainbow tablolarını (daha çok kriptolu şifrelerin kırılmasında) kullanarak bu işlemi yapar. Tabi ki başka methodlarda vardır ancak genel olarak özelliği deneme-yanılma yöntemini kullanmasıdır.
- Kesin hedefi olmayan, rastgele saldıran kişilerce de kullanılabilir.
Örn: RMC
- RMC nedir kısaca tanımlayalım; RMC belirlenen şifreyi kullanan mail adreslerini, yoğun bir maillistesini kullanarak dener. Bu mail listesi harvester gibi yazılımlarla oluşturulabilir.
- Her adrese 1 deneme yaptığından sunucular tarafından saldırı girişiminizin tespit edilmesi zordur. Ayrıca saldırgan kişi proxy'de kullanılabilir.

Brute-Force (Kaba Kuvvet) -2

- Yazılımı test etmek için mail şifremi 123456 yaptım :



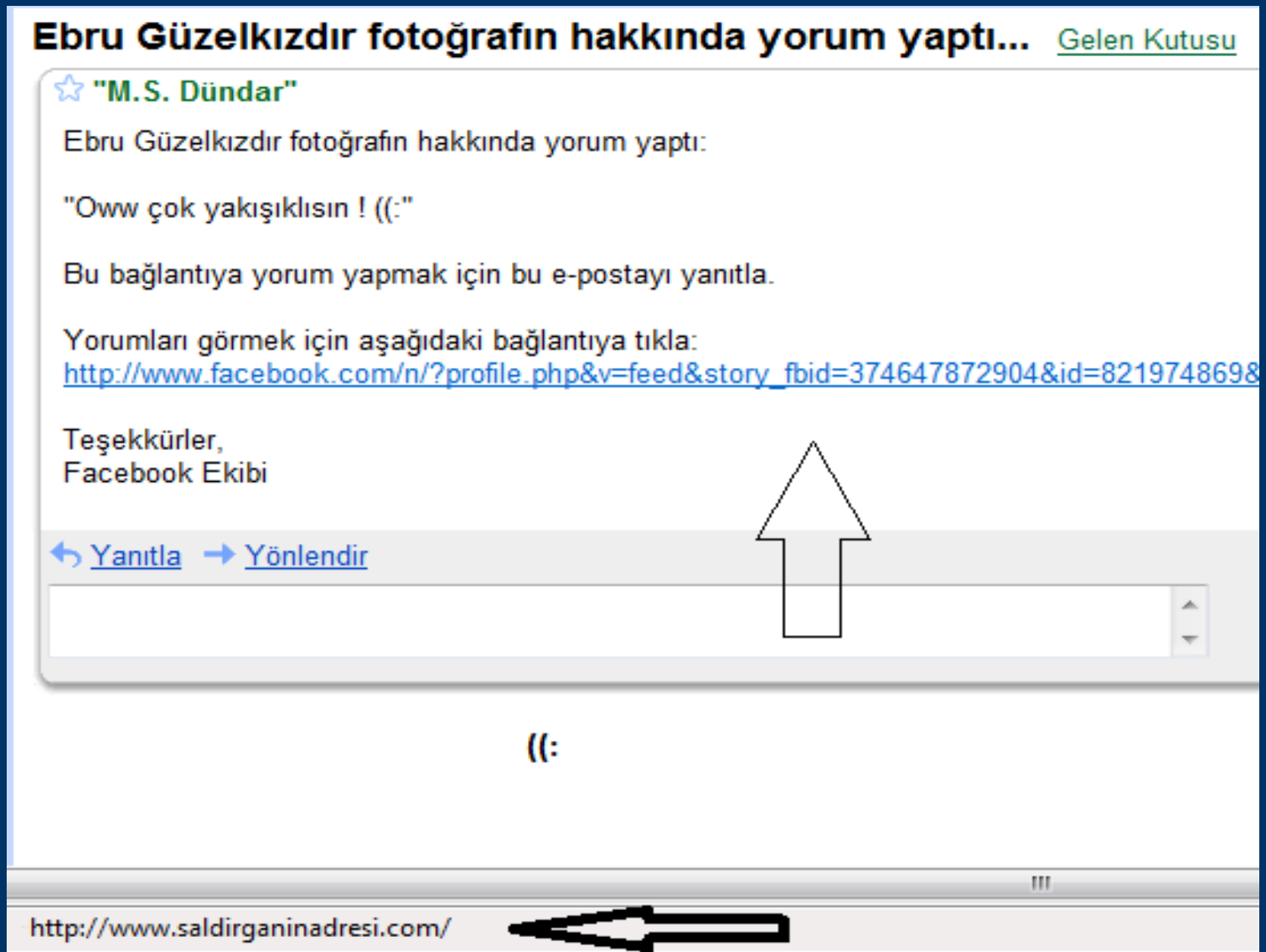
Bir milyon kişilik bir mail listesinde en azından binlerce kişinin mail şifresi 123456'dır...

Bunun gibi çok kullanılan kelimeleri ve sayıları deneyerek saldırı yapılabilir.

Fake Mail (Sahte Mail)

- Bir Phishing türü olarakta düşünülebilir.
- Posta kutunuza giriş yaptığınız sayfanın veya herhangi bir web sayfasının fake'inin (sahte) basit html kodları ve formmail ile hazırlanmış halidir. Kullanıcıyı bu adrese bir mail yardımı ile çekmeye çalışmak ve bu sahte giriş panelinden giriş yapmasını sağlatmaya çalışma işlemidir.
- Dikkatli kullanıcılar adres çubuğunu takip ederek şifrelerini girdikleri yerleri denetleyebilirler.
- Bazı mail servislerinin ajax denetimleri hedef adresin görünmesini engellediği için “temel html görünümü” özelliğinde kullanılması önerilir !
- <http://facebookmails.somee.com/> Adresi örnek bir saldırgan adresidir. Kullanıcının dikkatini çekmeyecek adresler tehlikeyi ciddileştirir. www.facebookx.com Gibi.
- Örnek bir fake mail görelim :

Fake Mail (Sahte Mail) - 2

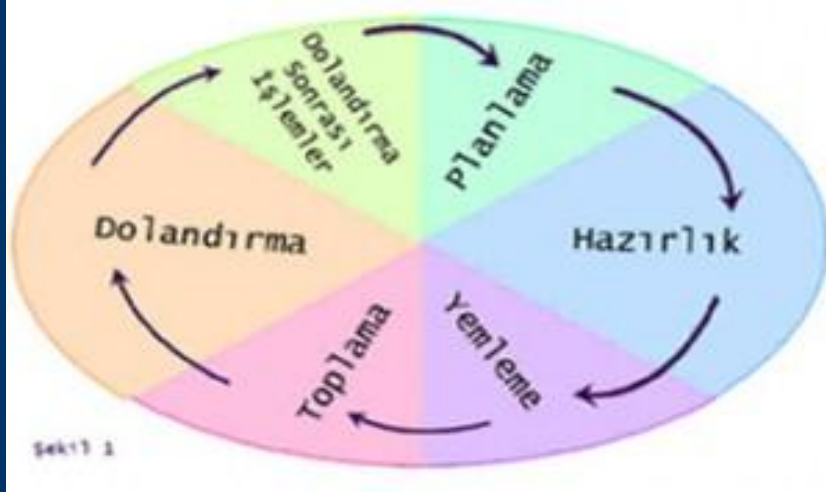


Phishing

- “Sosyal Mühendislik” teknikleri kullanılarak, kurbanın Kredi, Debit/ATM Kart Numaraları/CVV2, Şifreler ve Parolalar, Hesap Numaraları, İnternet Bankacılığına Girişte Kullanılan Kullanıcı Kodu ve Şifreleri gibi büyük önem arz eden ve çok iyi korunması gereken bilgilerini, kurbanı aldatarak elde etme yöntemi olarak tanımlanabilir. Başka bir ifadeyle Phishing; kişileri, yasal bir şirket, ajans veya organizasyon olduğuna inandırarak, kişisel ve finansal bilgilerini ele geçirme yöntemidir.
- Mail'i gönderen kişinin adresine aşına olmanız, bu mailin gerçekten o kişi tarafından yollandığı anlamına gelmez ! Gönderen kısmında yazan adres saldırgan tarafından istediği gibi değiştirilebilir. Örneğin iletisim@akbank.com.tr adresinden gelen bir mail ile hesap numaranız/şifreniz sorulabilir veya asayis@emniyet.gov.tr gibi çeşitli adresler saldırılarda kullanılabilir. İstedığınız mail adresinden mail göndermek oldukça basittir.

Phishing -2

- Temel olarak 6 basamaktan oluşur. Tek korunma yöntemi dikkatli ve bilinçli olmaktır.

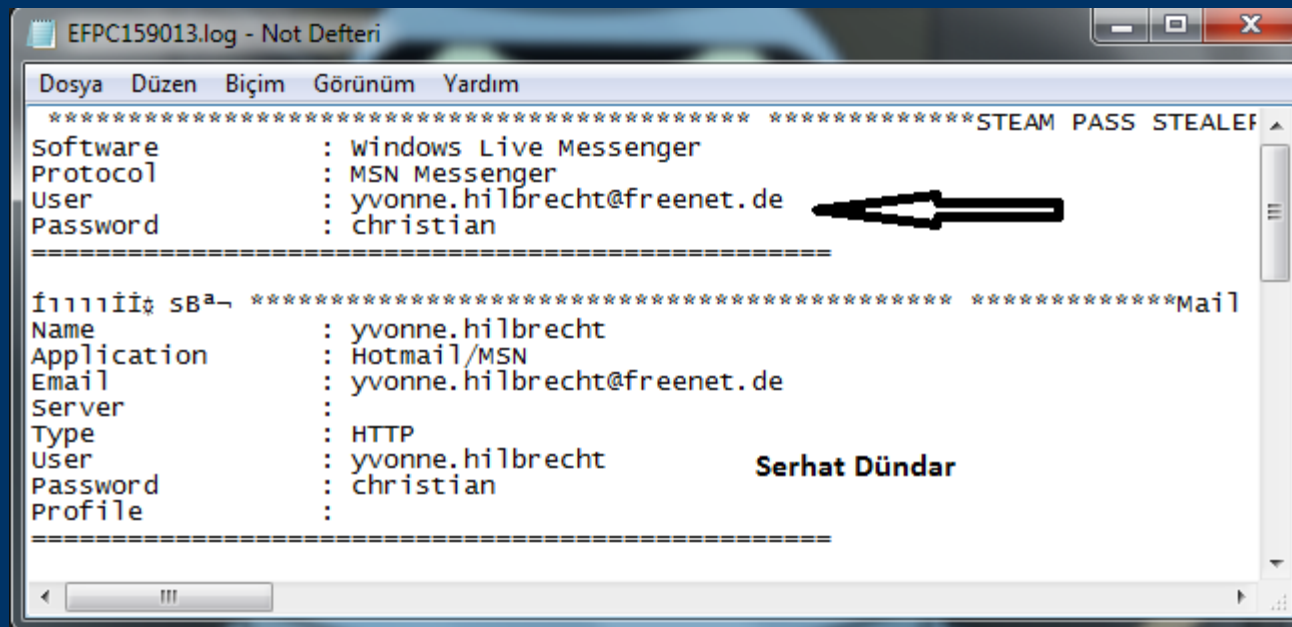


Çeşitlerini; Aldatıcı Phishing (Deceptive Phishing), Kötü Yazılım Phishingi (Malware Phishing), Sahte Website Phishingi (Faulty Website Phishing) ve İçerik Gönderme Phishingi (Content Injection Phishing) olarak sınıflandırabiliriz.

Detaylı bilgi : <http://bilisimpolisi.net/phishing-password-harvesting-fishing/>

Keylogger – Trojan

- Bir malware genellikle temel olarak 2 kısımdan oluşur. Bunlar “server” ve “client”tir. Zararlı dosya hedef kişiye çeşitli yöntemlerle kabul ettirilmeye çalıştırılmalıdır. Server dosyasını hedef kişi çalıştırdığı andan itibaren client ile hedef üzerinden veri gönderilir/alınır, ekran görüntüsü alınır, klavye vuruşları loglanır vs. Her malware farklı karakteristik özellikler barındırır.
- Bir keylogger veya trojan sayesinde hedef seçilen bilgisayarda yapılan işlemlerin logları edinilebilir. Örnek bir log dosyası :



```
EFPC159013.log - Not Defteri
Dosya Düzen Biçim Görünüm Yardım
*****STEAM PASS STEALEF
Software      : windows Live Messenger
Protocol      : MSN Messenger
User          : yvonne.hilbrecht@freenet.de
Password      : christian
=====
f11111111 SB^ *****Mail
Name          : yvonne.hilbrecht
Application   : Hotmail/MSN
Email         : yvonne.hilbrecht@freenet.de
Server        :
Type          : HTTP
User          : yvonne.hilbrecht
Password      : christian
Profile       :
=====
Serhat Dünder
```

Daha kötüsü de olabilir :

Keylogger – Trojan - 2

- Keylogger'lar sonucu başka istenmeyen şeylerde yaşanabilir..
Avusturya'dan Wenzl Thomas isimli şahsın online bankacılık yapması sonucu :

NOT.txt - Not Defteri M.SERHAT DÜNDAR

Dosya Düzen Biçim Görünüm Yardım

Microsoft Office Professional Edition 2003 CD Key: GWH28-DGCM-P6RC4-6J4MT-3
Microsoft Office Enterprise 2007 CD Key: F2B96-XCBHY-PWFJ9-GJFP6-XGJBJ
Microsoft Office Enterprise 2007 CD Key: CMTCR-YMJWC-K6JY9-JDY7F-XFMYJ

Host : https://wwwtb.psk.co.at tn : 71425[REDACTED] pin : 72543[REDACTED]EAL4GFVUB

Kontonummer 0007144[REDACTED] EUR | Wenzl Thomas

BIC OPSK[REDACTED]W

IBAN AT50[REDACTED]00007144[REDACTED]

Kontostand 8.134,29 EUR

Verfügbare Betrag 13.034,29 EUR

Aktuelle Einkaufsreserve 4.900,00 EUR = Überziehungsrahmen

Durchschnittssaldo per 07.03.2010 8.724,58 EUR für Konto-Box

LETZTER KONTOAUSZUG

Nummer 2

Datum 11.02.2010

Saldo 9.113,16 EUR

DRUCKEN

Saldırgana kalan parayı önce paypal hesabına transfer etmek, daha sonra belirli bir kesinti karşılığı banka kartına transfer etmek olacaktır.

Şifre Politikaları

- Şifreleriniz tahmin edilebilir (isim-soyisim-futbol takımı, cep telefonu numaranız, doğum tarihiniz vs.) olmamalıdır.
- Olabildiğince farklı tip karakter barındıran şifreler kullanılmalıdır. Küçük/Büyük harf, rakam, sembol vs. Eğer izin verilmiş ise türkçe karakter (ö, ç, ş, ı, ğ) kullanmanız yabancı saldırıları kısmen engelleyecektir çünkü bir çok yazılım sadece Q klavye karakterlerini tanımakta..
- Web uygulamaları saldırıya maruz kalıp, veritabanları ele geçirildiğinde saldırgan bir çok kullanıcı adı/şifre bilgisine ulaşacaktır. Bir çok uygulamanın artık veritabanlarında MD5 şifreleme sistemini kullandığını düşünürsek uzun ve karmaşık şifrelerin önemi bir kez daha anlaşılır. Çünkü “123456” gibi bir şifrenin MD5 ile şifreli hali oldukça çabuk kırılabilirken “Sam?Sun_55&/” gibi bir şifrenin MD5'ini kırmak yüzlerce yıl sürebilir.

Yukarıda ki şifrenin Md5 ile kriptolanmış hali :

acf4f8427d0833728cf6920159cc172d

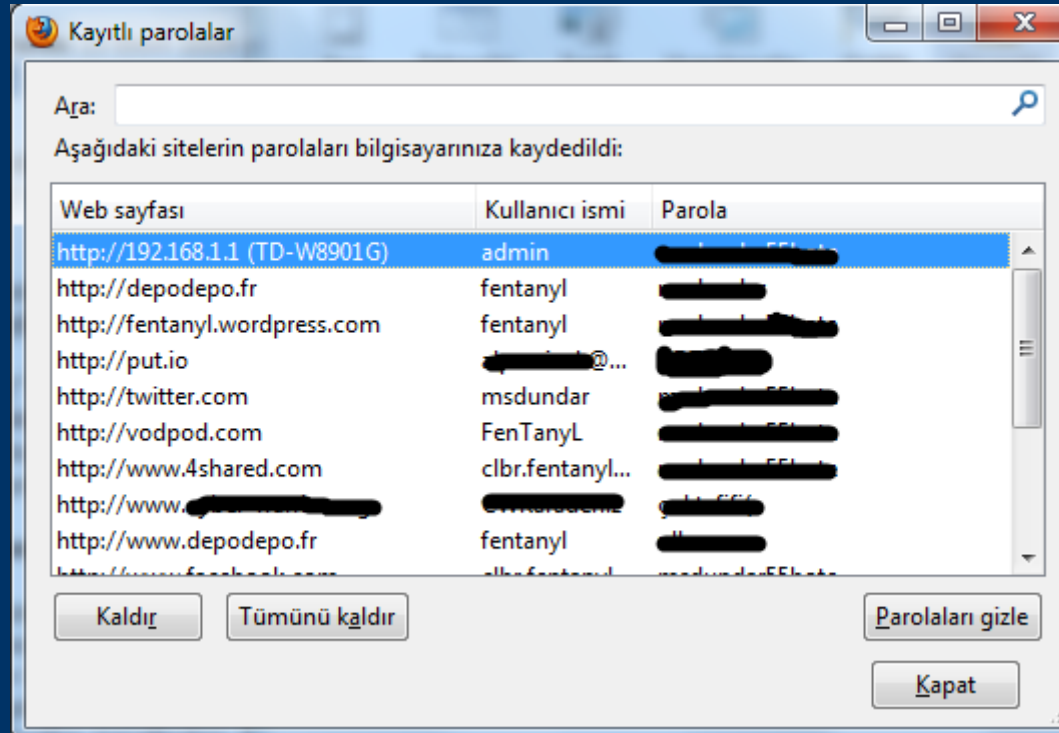
- Bir şifre 2 farklı yerde kullanılmamalıdır.

Uygulama Zaafları

- Mail hesabınıza girişlerinizde browserınızın “beni hatırla” seçeneğini aktif edilmemelidir.

Böyle bir durumda browser'ın şifreleri barındırdığı dosyanın çeşitli yollarla saldırganın eline gelmesi ile mail adresiniz hacklenebilir .

Firefox'un hatırladığı şifreleri görüntüleyebilirsiniz.



Uygulama Zaafları - 2

- Outlook şifreleriniz “Protected Storage PassView” gibi yazılımlarla çalınabilir.

Outlook gibi yazılımlarda zaman zaman bulunan zaaflar ile mail güvenliğiniz tehlikeye düşebilir. Bu yüzden otomatik güncelleştirmeleri açık tutmak tavsiye edilir.

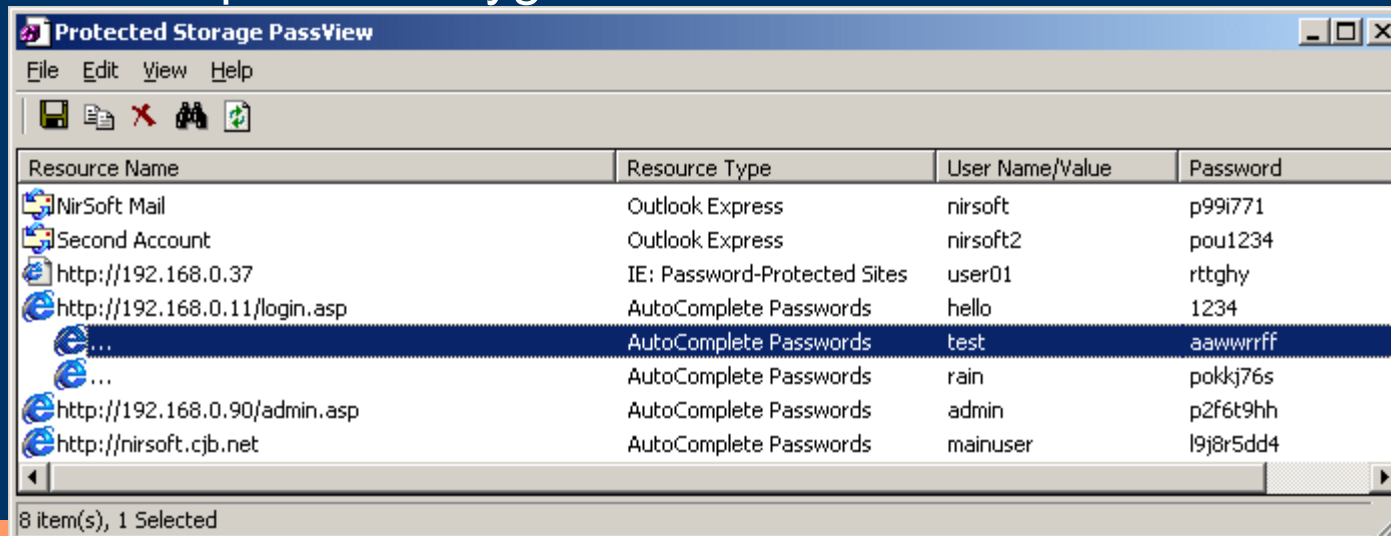
Bugtrack'lerde bulduğum 2007 tarihli bir outlook zaafı :

Makale numarası: 925938 - Son Gözden Geçirme: 30 Ocak 2007 Salı - Gözden geçirme: 2.0

MS07-003: Microsoft Outlook'taki güvenlik açıkları uzaktan kod yürütülmesine izin verebilir

[Bu makalenin geçerli olduğu ürünleri görün.](#)

Basit bir passview uygulaması :



Uygulama Zaafları - 3

- Webmail uygulamalarında, yazılımlara oranla daha çok zaaf çıkmaktadır. Örnek vermek gerekirse okulumuzun kullandığı webmail uygulaması “Squirrelmail” 1.4.7 sürümünde ciddi açıklar içermektedir. Bu uygulamanın en kısa zamanda 1.5 sürümüne yükseltilmesi gerekmektedir.
- Yanında işaret olan zaaflar okulumuzun kullandığı 1.4.7 sürümünü etkileyen zaaflardır.

SquirrelMail Vulnerabilities

The following list includes some of the most critical SquirrelMail vulneral possible.

- ✓ 1. [SquirrelMail Arbitrary Variable Overwriting](#)
- ✓ 2. [Squirrelmail compose.php Variable Overwriting](#)
3. [SquirrelMail IMAP/SMTP Injection](#)
4. [SquirrelMail Address Add Plugin XSS](#)
5. [SquirrelMail S/MIME Plugin Command Injection](#)
6. [Squirrelmail Remote and Local File Inclusion and XSS](#)
7. [SquirrelMail Cross Site Scripting in Encoded Text](#)
8. [Content-Type XSS Vulnerability in Multiple Webmail Programs](#)
9. [Squirrelmail Local Root Chpasswd Exploit](#)
- ✓ 10. [SquirrelMail Cross Scripting Attacks \(compose.php\)](#)
11. [Squirrelmail Change passwd Buffer Overflow](#)
12. [SquirrelMail XSS Vulnerabilities](#)



SquirrelMail
webmail
for
nuts

SquirrelMail sürüm 1.4.19
SquirrelMail Geliştirme Takımı

Ondokuz Mayıs Üniversitesi Giriş

Kullanıcı Adı:

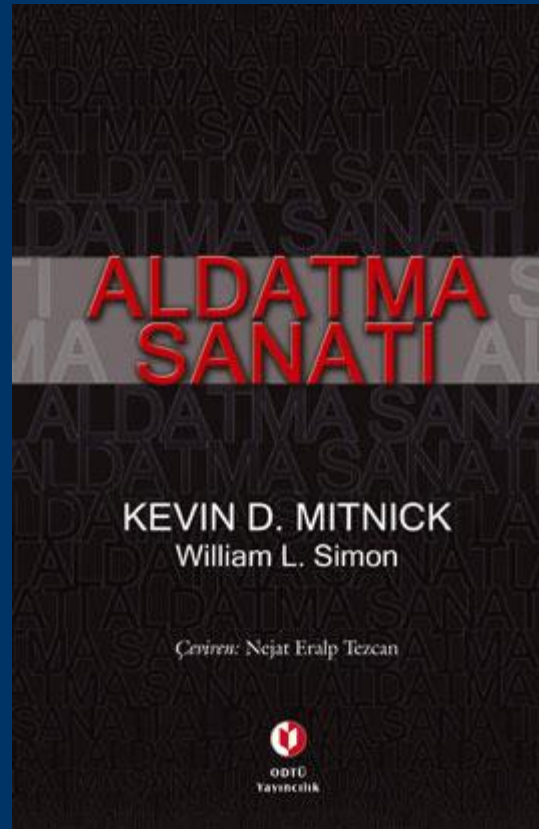
Şifre:

Sosyal Mühendislik

- Sosyal mühendislik kişileri kandırarak değerli bilgi ve parolalarını ellerinden almayı amaçlamaktadır.
- Günümüzde google, bloglar, sosyal ağlar ve daha bir çok yöntem ile hedef kişi hakkında bilgi toplanabilir.
- Hedef kişinin ilgi alanları, kişisel bilgileri, zaafları vs. keşfedilerek ön hazırlık yapıldıktan sonra saldırıya geçilir.
- Örnek vermek gerekirse mail adresinin gizli sorusu “En sevdiğim tarihi kişilik” olan birisinden bu sorunun cevabını almak için kişiyi tarihi bir forum ortamına çekmek veya arkadaşlık kurarak sorunun cevabını öğrenmek zor olmayacaktır.
- Sosyal Mühendislik sanatı kişisel iletişim ve ikna kabiliyeti gerektiren bir iştir. Karşı tarafın şüphesini çekmeden elde edilmek istenilen bilgiyi almak her zaman sanıldığı kadar kolay olmayabilir. Bu yüzden “sabır” çok önemli bir faktördür.
- Tüm teknik yöntemler tükendiğinde bazen tek yol sosyal mühendisliktir.

Sosyal Mühendislik - 2

- Dünyanın en ünlü hackerı olarak anılan Kevin Mitnick aynı zamanda sosyal mühendisliğin mucidi ve dünyanın en ünlü sosyal mühendisi olarak kabul edilir. Kendisinin “Aldatma Sanatı” isimli bir kitabı bulunmaktadır.



XSRF-CSRF-XSS

- Saldırganın çoğunlukla Java Script kodunu siteye enjekte etmesiyle ortaya çıkar. Saldırganın özel oluşturduğu bir linki kurbanı gönderdiğini düşünelim. Kurbanın linke tıklamasıyla Java Script kodu çalışmaya başlar ve kurbanın cookieleri saldırganı gider, cookieler sayesinde hedef kişinin oturumu yetkisizce çalınabilir. Hedef kişinin oturum bilgileri, saldırganın kurduğu sniffer'da toplanır.
- XSS saldırılarından korunmanın herhangi bir yolu yoktur. Tek çözüm bilmediğiniz linklere tıklamamanız ve Hex'li url'lere karşı şüpheli yaklaşmanızdır.
- Hex'li url örneği :

<http://3513587746@3563250882/d%65f.%61%73p%3F%69d=522>

- Hotmail'de bu zaaf 1 ay kadar süreyle mevcuttu ve bir çok mail adresi bu durumdan zarar gördü. Gmail ise bu zaafın ilkini 2 gün diğerini 3 gün içinde fixledi.

Clickjacking

- Bir browser güvenlik açığıdır.
- Iframe ; Bir web sayfasına zararlı bir web sayfasının (opacity(şeffaflık) değeri=0) olarak gizlenmesidir. Sayfa içinde sayfa mantığıdır.
- Click and Redirect; Normal bir link yerine tıklanış esnasında farklı bir action(yönlendirme) sağlanmış, tuzaklanmış linklerdir.
- Clickjacking ile basit bir web sayfası hazırlayıp, ufak bir sosyal mühendislik senaryosu ile bir formu submit ettirebilir, dolayısı ile XSRF saldırısı gerçekleştirebilir, HTML Downloader, Keylogger gibi yazılımlar yedirebilirsiniz.
- onmouseover="document.location='http://www.serhatdundar.net';" bu kod'dan anlayacağınız üzere hedef adrese yönlenmek için mouse'umuz ile frame'in üzerinde durmamız yetecek !

Soru-Cevap

- Sorular ?

Mustafa Serhat Dünder

clbr@grisapka.org

