

Phishing

سحر رجبی
زیبا امیدوار
محمد غفاری فر
صادق حایری

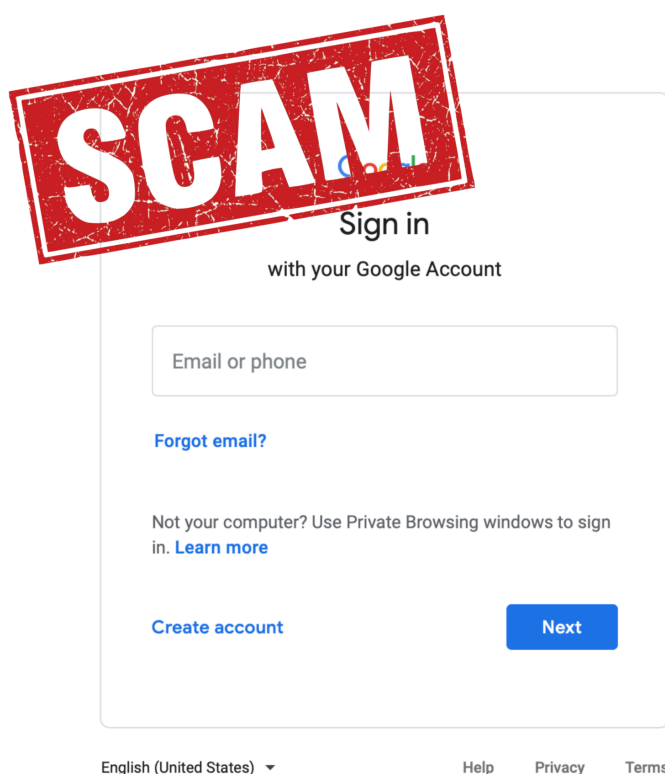
استاد: دکتر صیاد
پاییز ۹۷

فهرست

3	مقدمه
3	DNS Hijacking
3	نحوه‌ی کار DNS server
4	استفاده از DNS Server ها برای حمله‌ی Phishing
4	بدخواه بودن DNS Server
4	استفاده از DNS Hijacking
4	Public Wifi
4	Arp Spoofing
4	آشنایی با بسته‌های Arp
5	حمله‌ی Arp spoofing
5	Site Cloning
6	SSL Strip
7	روش جلوگیری از حمله:
8	Link Manipulation
8	Hiding the URL
8	Typosquatting
9	ابزار DNSTWIST
9	Homograph Attacks
10	Email Phishing
11	روش‌های مقابله
11	SPF
11	DKIM
11	DMARC
12	Demo
12	Site Cloning
12	Link Manipulation
12	SSL
12	Email Spoofing
13	نتایج
13	منابع

مقدمه

این نوع حمله، به حملاتی اطلاق می‌شود که در آن فرد بدخواه، تلاش می‌کند با فریب کاربران، و مخصوصاً استفاده از تصاویر آشنای کاربر، مثلاً فرم ورود به حساب کاربری گوگل، فیسبوک و غیره، اطلاعات محرمانه‌ای مانند نام کاربری و رمز عبور، و یا اطلاعات کارت‌های بانکی را بدست آورد. حمله کننده سپس می‌تواند با استفاده از این اطلاعات بدست آمده، با ورود به حساب‌های کاربری، و یا سواستفاده‌های دیگر حملات دیگری صورت دهد و یا حتی به سایر کاربران سیستم آسیب برساند. در ادامه‌ی این گزارش، به معرفی انواعی از راه‌های انجام این حمله، و همچنین روش‌هایی برای مقابله با آن خواهیم پرداخت.



DNS Hijacking

نحوه‌ی کار DNS server

یک کاربر اینترنت، برای اینکه بتواند به سرویس‌های موجود در یک وبسایت دسترسی داشته‌باشد، باید آدرس IP آن را بدست آورد؛ در واقع وظیفه‌ی DNS Server ها همین است. نحوه‌ی کار به این صورت است. که زمانی که کاربر می‌خواهد به سایتی با دامنه‌ی مثلا www.google.com متصل شود، درخواستی برای این سرور ارسال می‌کند که در آن ذکر شده که به آدرس IP این وبسایت احتیاج دارد. در پاسخ، DNS Server در صورتی که آدرس متناظر به این دامنه را در حافظه‌ی خود داشته‌باشد، آن را برای کاربر ارسال می‌کند. در غیر این صورت، به سراغ DNS Server های دیگر رفته و نهایتاً بعد از به دست آوردن پاسخ آن را به دست فرد می‌رساند.

استفاده از DNS Server ها برای حمله‌ی Phishing

بدخواه بودن DNS Server

در صورتی که این سرور بدخواه باشد؛ یا کنترل آن موقتاً به دست افراد بدخواه افتاده باشد؛ پس از دریافت درخواست کاربر مبنی بر نیاز به گرفتن آدرس یک دامنه، سرور می‌تواند در صورتی که این دامنه، همان دامنه‌ی هدف برای جمع‌آوری اطلاعات کاربران آن باشد، آدرس وبسایتی جعلی، که تنها طراحی آن مشابه با سایت اصلی است را به کاربر ارسال کند. در ادامه، کاربر با دریافت این پاسخ به صفحه‌ی آلوده منتقل می‌شود و در صورت عدم توجه کافی، و یا مکانیزم‌های تشخیص حمله‌ی phishing اطلاعات خود را در اختیار حمله کننده قرار می‌دهد.

استفاده از DNS Hijacking

در یک حالت دیگر ممکن است DNS Server به سلامت مشغول انجام کار خود باشد؛ اما حمله کننده مانع از رسیدن درخواست کاربر به آن شده، و خودش این درخواست را دریافت کند. سپس مشابه حالت قبل، فرد بدخواه می‌تواند در پاسخ به جای آدرس دامنه‌ی درخواستی، آدرس سرور جعلی که کنترل آن در دست خودش است را برای کاربر ارسال کند و با انجام این کار به سادگی فرد را به صفحه‌ی آلوده‌ی خود منتقل کند.

Public Wifi

استفاده از Wifi‌های عمومی هم می‌تواند ما را در معرض حمله‌ی phishing قرار دهد. یک wifi در واقع routerای است که بسته‌های ما را دریافت و یا ارسال می‌کند. فرد حمله کننده، می‌تواند با استفاده از یک wifi عمومی، بسته‌های رد و بدل شده‌ی کاربران - در صورت رمز شده نبودن آن‌ها - را دریافت کند. تحت این شرایط، زمانی که یک کاربر می‌خواهد به وبسایت خاصی متصل شود؛ فرد بدخواه بسته‌ی او را دریافت می‌کند. در صورت مطابقت با دامنه‌ای که قصد انجام حمله‌ی phishing به کاربران آن را دارند، پاسخ را از سمت سرور خودش که در دست فرد بدخواه است به کاربر ارسال می‌کند. باز هم کاربر در صورت عدم توجه کافی - مثلاً به آدرس دامنه‌ی نمایش داده شده و یا امنیت سایت - می‌تواند فریب بخورد و اطلاعات خود را به سادگی در اختیار افراد بدخواه قرار دهد. همچنین یک حمله کننده می‌تواند Access point ای مشابه یکی از Access point های مورد اعتماد کاربران در یک مکان ایجاد کند و افراد سهواً به آن متصل شوند با تصور اینکه از طریق کانالی امن در حال تبادل اطلاعات خود هستند.

Arp Spoofing

آشنایی با بسته‌های Arp

زمانی که یک دستگاه‌ها در یک شبکه‌ی محلی بخواهند با یکدیگر ارتباط برقرار کنند، نیاز دارند که MAC Address یکدیگر را بدانند. برای این کار، زمانی که یک دستگاه با دستگاه دیگر با IP مشخص کار دارد، بسته‌های Arp را در کل شبکه broadcast می‌کند. این بسته‌ها در واقع بیان می‌کنند که یک دستگاه با یک MAC Address و IP مشخص، با دستگاه دیگری که IP آن در پیام این بسته قرار می‌گیرد کار دارد. زمانی که دستگاه مقصد این بسته را دریافت کند، پاسخ آن را به دستگاه درخواست کننده ارسال می‌کند و از این به بعد می‌توان با آن ارتباط برقرار کرد. آدرس MAC سایر دستگاه‌ها در یک شبکه‌ی محلی در داخل هر گره cache می‌شود.

همچنین با وارد کردن دستور زیر در ترمینال می‌توان cache موجود در این لحظه را دریافت کرد:

arp -a

```
2. fish /Users/sadegh/Desktop (fish)
~/Desktop ➤ arp -a
? (172.30.48.1) at f0:b2:e5:90:f2:e1 on en0 ifscope [ethernet]
? (172.30.48.69) at ac:bc:32:83:92:c3 on en0 ifscope [ethernet]
? (172.30.48.218) at 7c:4:d0:82:a6:ad on en0 ifscope [ethernet]
? (172.30.48.221) at 3c:2e:f9:4b:68:3d on en0 ifscope [ethernet]
? (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
? (239.255.255.250) at 1:0:5e:7f:ff:fa on en0 ifscope permanent [ethernet]
```

همان‌طور که مشاهده می‌شود لیست نگاشت‌های ip به mac در تصویر قابل مشاهده است.

حمله‌ی Arp spoofing

از آنجایی که مکانیزم پرسش و پاسخ بسته‌های Arp به صورت stateless صورت می‌گیرد، حمله‌کننده در صورتی که موفق شود به شبکه‌ی محلی متصل شود، می‌تواند شروع به ارسال پاسخ بسته‌های Arp به گره‌های شبکه‌ی محلی کند و با استفاده از IP spoofing خود را به عنوان دستگاه هدف معرفی کند. و با توجه به stateless بودن این فرآیند سایر دستگاه‌ها با دریافت پاسخ بسته‌ی Arp، اقدام به بروزرسانی cache خودشان می‌کنند. برای مثال اگر فرد بدخواه، خودش را به عنوان router به شبکه معرفی کند، می‌تواند همه‌ی بسته‌های موجود را دریافت و شنود کند.

یکی از راه‌های ساده‌ی جلوگیری از انجام این حمله، ذخیره کردن آدرس MAC دستگاه‌ها به صورت static است. این کار با دستور زیر قابل انجام است:

arp -s <ip address> <mac address>

```
2. fish /Users/sadegh/Desktop (fish)
~/Desktop ➤ arp -a
? (172.30.48.1) at f0:b2:e5:90:f2:e1 on en0 permanent [ethernet]
? (172.30.48.47) at 7c:1:91:aa:56:2a on en0 ifscope [ethernet]
? (172.30.48.151) at 3c:2e:f9:4b:68:3d on en0 ifscope [ethernet]
? (172.30.49.26) at f4:5c:89:93:9d:f7 on en0 ifscope [ethernet]
? (172.30.49.112) at 38:ca:da:ce:8e:3e on en0 ifscope [ethernet]
? (172.30.49.137) at ac:bc:32:83:92:c3 on en0 ifscope [ethernet]
```

بعد از آن در صورتی که مجدداً دستور arp -a را وارد کنیم، می‌توانیم این آدرس‌ها را با کلیدواژه‌ی permanent مشاهده کنیم.

Site Cloning

site cloning به معنای کپی کردن اسکریپت‌ها و فرمت‌های یک سایت است. معمولاً برای بیشتر حملات phishing به site cloning نیاز داریم. این اقدام می‌تواند برای ایجاد یک وب سایت جدید با استفاده از اسکریپت‌ها و فرمت‌های سایت‌های دیگر مفید باشد. همچنین با استفاده از این روش می‌توانیم به صورت آفلاین در اطلاعات سایتی که آن را clone کردیم؛ جستجو انجام دهیم و به اطلاعاتی مثل ایمیل، password‌های فایل‌های پنهان و... دست پیدا کنیم.

ابزار هایی مثل HTtrack و Setoolkit برای این کار وجود دارد که کار با آن ها راحت است و نیاز به دانش خاصی ندارد.

```
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing: 192.168.171.179
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone https://www.facebook.com
[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

Site cloning با استفاده از ابزار setoolkit در سیستم عامل کالی

این کار با استفاده از ابزار setoolkit در سیستم عامل kali برای جلوگیری از این حمله باید امنیت کد خود را بالا ببریم و کد های رمزگذاری شده و لایه های اضافی از امنیت داشته باشیم. یا به script هایمان چیزهایی اضافه کنیم که امکان کپی شدن آن ها وجود نداشته باشد.

SSL Strip

در ssl strip (که در واقع نوعی حمله ی man in the middle است) تمام ترافیک از سیستم قربانی از طریق یک پراکسی که توسط مهاجم ایجاد شده است، عبور می کند. در این روش یک attacker که روی آن یک ssl strip در حال اجراست، بین قربانی و سرور قرار میگیرد و ارتباط مستقیمی بین سرور و قربانی وجود ندارد. فرض کنیم که قربانی A می خواهد پولی را از حسابش از طریق بانکداری آنلاین منتقل کند و url مورد نظر را وارد میکند؛ در این شرایط browser قربانی که به سیستم مهاجم متصل است، منتظر جواب از طرف سرور می ماند. مهاجم درخواست قربانی را به سرور ارسال می کند و منتظر پاسخ از طریق سرور می ماند. ترافیک بین مهاجم و سرور امن است زیرا از طریق ssl با هم ارتباط برقرار می کنند. سرور بانک صفحه ی login را به عنوان پاسخ می فرستد. در این مرحله مهاجم به این صفحه ی login دسترسی دارد و پاسخی که از طرف سرور آمده است را دستکاری می کند و پاسخ را که به شکل https است به http تبدیل می کند و سپس آن را برای قربانی ارسال می کند.



در واقع قربانی به صفحه ی login بانک با یک ارتباط نا امن دسترسی پیدا میکند و اطلاعات درخواست قربانی به صورت plain text برای مهاجم ارسال می شود. (این اطلاعات می تواند شامل username و password کاربر باشد). attacker می تواند این اطلاعات را شنود کند. سرور فکر میکند که ارتباط با کاربر به درستی برقرار شده است و ارتباط امن است. کاربر نیز فکر می کند ارتباط او با بانک امن بوده است در حالی که بدون این که دو طرف متوجه شوند؛ attacker اطلاعات را شنود کرده است. . این حمله http-downgrading attacks هم خوانده می شود چون ارتباطی که از طریق browser قربانی صورت می گیرد از https به http ، downgrade می شود.

روش جلوگیری از حمله:

HSTS (HTTP Strict Transfer Security) یک پروتکل است که به کاهش حملات sslstrip کمک می کند. هر بار که یک کاربر یک اتصال https را به یک سایت ایجاد می کند، سایت یک پیام هدر را ارسال می کند که از حالا تا مدت زمان مشخصی اتصال به این سایت فقط از طریق https صورت می گیرد. این اطلاعات توسط مرورگر کاربر ذخیره می شود و اگر در آینده مرورگر ببیند که درخواست کاربر از نوع http است، آن را به https تبدیل می کند. باید دقت داشت تمام وب سایت هایی که از https پشتیبانی می کنند، شامل هدرهای پاسخ HSTS نیستند. افزون بر بالا رفتن ضریب ایمنی، وجود HSTS با حذف یکی از مراحل پردازش بارگیری وب سایت، سبب افزایش سرعت بالا آمدن سایت خواهد شد. مراحل زیر را در نظر بگیرید:

- یک کاربر آدرس google.com را در نوار آدرس مرورگر خود تایپ می کند.
- به صورت پیش فرض مرورگر تلاش می کند ابتدا آدرس http://google.com را بارگذاری نماید.
- مدیر سایت google.com به طور دائمی آن آدرس را به آدرس امن https://google.com هدایت کرده است.
- مرورگر دایرکت را یافته و این بار به جای آن آدرس https://google.com را بارگذاری می نماید.

ولی با استفاده از ssl strip، هکر می تواند از فرصت بدست آمده در بین مرحله 3 و 4 برای مسدود کردن فرمان دایرکت و متوقف کردن مرورگر به منظور بارگذاری نسخه امن https وب سایت استفاده نماید. در این شرایط همچنان به یک نسخه بدون رمزگذاری و ناامن دسترسی دارید و به سادگی تمام اطلاعات شما قابل سرقت خواهد بود. هکر حتی می تواند شما را به وبسایتی کاملاً مشابه با سایت مورد نظر هدایت کرده و تمامی اطلاعاتی که شما وارد می کنید (از جمله شماره حساب بانکی و رمز اینترنتی آن و ...) را بدست آورد بدون آنکه شما متوجه ناامن بودن سایت جعلی شوید.

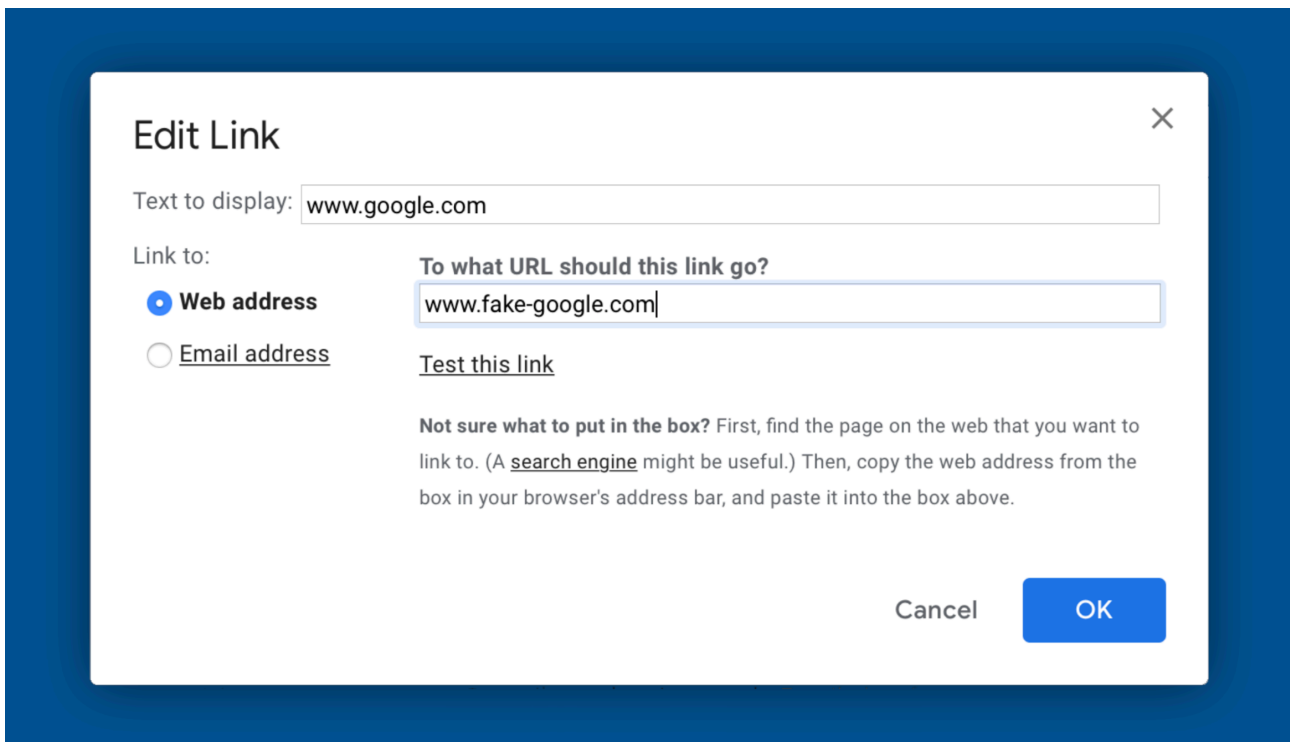
فعال کردن HSTS مرورگر را مجبور می کند نسخه ایمن یک وبسایت را بارگیری نماید و هرگونه ریدایرکت و تماس دیگری را برای باز کردن اتصال http نادیده بگیرد و مشکل آسیب پذیری فرایند ریدایرکت را که با هدایت کدهای 301 و 302 وجود دارد، برطرف کند. با این حال نکته ناخوشایند ماجرا در استفاده از HSTS این است که مرورگر مورد استفاده کاربر، باید حداقل یک بار قبل از به کارگیری همیشگی از این ویژگی، واکنش و فرمان HSTS را دیده باشد. این بدین معناست که حداقل یک بار باید وب سایت فرایند ریدایرکت http به https را انجام دهد. به همین علت حتی در وب سایت های مجهز به HSTS نیز برای بار اولین این آسیب پذیری وجود دارد. برای مقابله با این تهدید بالقوه، مرورگر کروم لیستی از وبسایت هایی که دارای HSTS فعال هستند را در اختیار دارد و پیش از بارگذاری نسبت به اعمال این مورد اقدام می نماید. به علاوه کاربران حرفه ای که دارای دانش فنی کافی در این زمینه هستند نیز خودشان می توانند وبسایت های مجهز به HSTS فعال را به این لیست بیافزایند.

Link Manipulation

Link manipulation به معنای دستکاری و تغییر در لینک ها برای یک حمله ی phishing است. این مساله روش های مختلفی دارد که می توان به موارد زیر اشاره کرد:

Hiding the URL

در این روش یک لینک که مورد درخواست کاربر است؛ نمایش داده می شود ولی با کلیک بر روی آن به لینک طراحی شده توسط کاربر ارجاع داده می شود. به عنوان مثال لینکی که برای کاربر نمایش داده می شود www.google.com است اما با کلیک بر روی آن کاربر به آدرس www.fake-google.com هدایت می شود.



Edit Link [X]

Text to display:

Link to:

☒ **Web address**

☐ Email address

To what URL should this link go?

[Test this link](#)

Not sure what to put in the box? First, find the page on the web that you want to link to. (A [search engine](#) might be useful.) Then, copy the web address from the box in your browser's address bar, and paste it into the box above.

Cancel

نمونه تکنیک پنهان کردن آدرس وبسایت مخرب

Typosquatting

در این روش attacker از اشتباهات رایج کاربر در وارد کردن url درخواستی استفاده کرده و صفحه ی phishing خود را متناسب با این آدرس ها طراحی می کند تا در صورت رخ دادن اشتباهات رایج توسط کاربر، کاربر وارد این صفحات شده و attacker بتواند سوءاستفاده ی خود را انجام دهد.

انواع typosquatting های مختلف عبارتند از :

- **common misspelling**: یک حرف به اشتباه تایپ شود: exemple.com
- **misspelling based on typos**: مثلاً یک حرف جابجا تایپ شود: example.com
- **different top level domain**: نام top level domain به اشتباه نوشته شود: example.org
- **missing dot typos**: فراموش کردن dot در نام سایت: wwwexample.com
- **abuse of top level domain**: example.om
- **differently phrased domain name**: examples.com

با استفاده از این ابزار می توانیم نام هایی که به یک دامنه شبیه هستند و در واقع typosquatting های آن هستند را پیدا کنیم و متوجه شویم کدام یک از آن ها register شده اند. همچنین به کمک این ابزار می توانیم از بین این لیست نام دامنه ها محتوای آن هایی که می خواهیم را با دامنه ی اصلی ای که وارد کردیم، مقایسه کنیم و در صورت شبیه بودن محتوا متوجه ی رخ دادن حمله ی phishing می شویم.

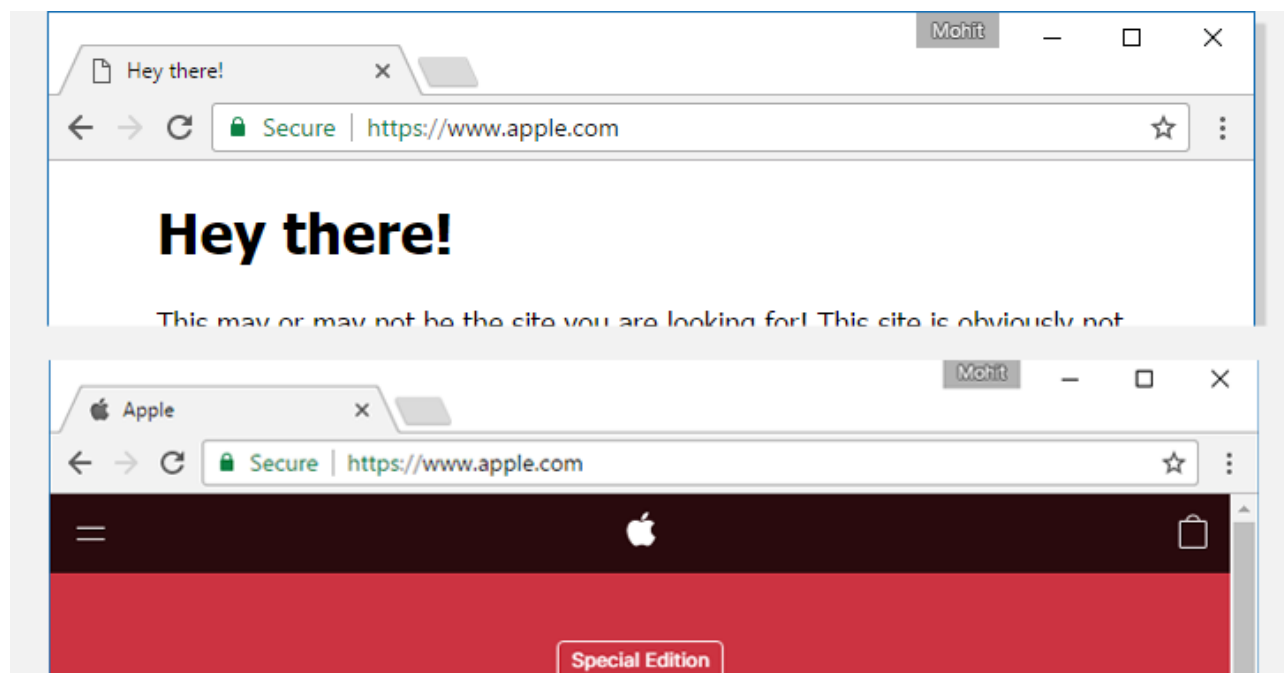
[illegible]

نمونه ای از نتایج DNSTWIST برای دامنه ی google.com

Homograph Attacks

حمله Homograph از سال ۲۰۰۱ شناخته شده است اما سازندگان مرورگرها در تلاش برای برطرف کردن آن هستند. این یک نوع حمله spoofing است که در حقیقت آدرس یک وبسایت به نظر قانونی می‌آید اما درواقع این‌طور نیست چراکه یک کاراکتر یا چند کاراکتر به‌صورت فریب‌کارانه‌ای توسط کاراکترهای Unicode جایگزین شده‌اند. بسیاری از کاراکترهای Unicode که در نام‌های دامنه بین‌المللی نمایشگر حروف الفبای یونانی، سیریلیک یا ارمنی هستند در نگاه عادی مانند حروف لاتین به نظر می‌رسند اما توسط کامپیوترها به‌گونه‌ای دیگر شناخته‌شده و آدرس‌های وب آن‌ها کاملاً متفاوت است.

برای مثال، حرف سیریلیک "а" (U+0430) و حرف لاتین "a" (U+0041) هر دو به طور متفاوتی توسط مرورگرها شناخته می‌شوند اما در نوار آدرس مرورگرها به صورت "a" نمایش داده می‌شوند.



<https://apple.com> - <https://www.xn--80ak6aa92e.com/>

Email Phishing

Email phishing به معنی ساخت و ارسال Email با هویت جعلی می باشد. به این شکل که شخصی بدون اجازه صاحب ایمیل آدرس از طرف او به دیگران ایمیل ارسال کند.

این امر به دلیل نوع معماری هسته اصلی پروتکل ایمیل که دارای هیچ مکانیزم تشخیص هویتی نیست به راحتی امکان پذیر است ، حملات جعل ایمیل (email phishing) به دلیل محدودیت های موجود در پروتکل SMTP (پروتکل انتقال ایمیل ساده) حاصل می شوند، این تکنولوژی اجازه می دهد تا ایمیل ها از فردی به فرد دیگر فرستاده شوند.

SMTP یا Simple Mail Transfer Protocol یکی از پروتکل های TCP/IP برای ارسال یا انتقال ساده ایمیل است که مانند یک دستیار عمل می کند و ایمیل را از فرستنده دریافت کرده و برای گیرنده می فرستد. SMTP، پروتکلی ساده و درعین حال مهم برای انتقال ایمیل است. این اصطلاح از آن رو به کار می رود که نسبت به سایر پروتکل های قبلی ایمیل، بسیار ساده عمل می کند. SMTP برای مسیریابی مستقیم پیغام به سمت گیرنده فقط به نام کاربری و دامنه نیاز دارد. SMTP یک پروتکل ارسال است و برای دریافت مناسب نیست، به همین دلیل برای دریافت ایمیل به جای SMTP از پروتکل های دریافت ایمیل مثل POP3 استفاده می کنند.

تنها محدودیت پروتکل SMTP در این است که اگر آدرسی در قسمت "from" ایمیل باشد، اصالت آن را بررسی نمی کند. اگر هکر خرابکاری بخواهد ایمیلی را جعل کند، تنها کاری که مجبور است انجام دهد، این است که از یکی از خدمات سرور SMTP آنلاین استفاده کند، ایمیلی بنویسد و سپس آدرس ایمیل دلخواهش را در فیلد "From" وارد کرده و بر روی گزینه ارسال کلیک کند. یا از یک برنامه مخصوص جعل ایمیل استفاده کند.

SPF یا Sender Policy Framework یک روش برای جلوگیری از Email phishing میباشد. SPF به شما اجازه میدهد اطلاعات فرستنده یا فرستنده های اصلی ایمیل را روی دامنه خود تعریف کنید و تمام میل سرورها از روی آن اطلاعات میتوانند هویت واقعی فرستنده ایمیل را شناسایی کنند. بنابر این ایمیل های ارسال شده توسط میل سرورها بررسی میشوند اگر اطلاعات فرستنده با موارد مطرح شده در SPF مطابقت داشت ایمیل دریافت میگردد در غیر این صورت ایمیل به نام ایمیل جعلی یا اسپم شناسایی خواهد شد.

DKIM

DKIM که از ادغام دو روش اعتبارسنجی در شرکت های یاهو و سیسکو تشکیل شده است، در سال 2004 رسماً معرفی شد. سیسکو یک استاندارد احراز هویت مبتنی بر امضا و یاهو سیستمی جهت بررسی DNS های دامنه طراحی کرده بودند.

با ادغام این دو تکنولوژی پروتکل استاندارد با نام DKIM(DomainKeys Identified Mail) پدید آمد که توسط آن فرستنده ایمیل از طریق دامنه احراز هویت میشود. بدین ترتیب ایمیل های مخرب و غیر واقعی از ایمیل های صحیح و سالم تمیز داده می شوند. با استفاده از DKIM، سرویس دهنده، ایمیل ارسالی را که به یک کلید خصوصی مجهز می کند. در عین حال کلید عمومی آن در DNS Zone دامنه به عنوان یک رکورد TXT ذخیره می شود. بنابراین هنگامی که ایمیل در سرویس دهنده مقصد دریافت شد، سرویس دهنده مقصد ابتدا کلید خصوصی که همراه ایمیل آمده است را با کلید عمومی که از طریق DNS دامنه، قابل شناسایی است، تطبیق می دهد. در صورتیکه نتیجه مثبت بود، ایمیل احراز هویت شده و در صندوق دریافت مخاطب جای می گیرد. در غیر اینصورت بسته به نوع و محتوای ایمیل، یا در اسپم قرار میگیرد یا به طور کل رد و Reject می شود.

DKIM در حقیقت یک امضای دیجیتال است که اثبات می کند فرستنده ایمیل واقعا همان فردی است که نام ایمیل نشان می دهد. تکنولوژی DKIM بر پایه ی رمزگذاری نامتقارن با کلیدهای عمومی و خصوصی فعالیت می کند در نتیجه امکان انجام امضای دیجیتال نامه ی الکترونیکی بدون در اختیار داشتن کلید خصوصی برای سارقان اینترنتی امکان پذیر نخواهد بود.

DMARC

DMARC کوتاه شده عبارت Domain-based Message Authentication, Reporting and Conformance به معنای "تصدیق هویت، گزارش و مطابقت پیام بر اساس دامنه" است. این پروتکل برای ادغام بهترین های SPF و DKIM در یک پروتکل منفرد و سپس اضافه کردن کارکردهای بیشتری همچون تحت نظر داشتن ایمیل ها، قرنطینه کردن آن ها و باز پس دادن ایمیل ها در نظر گرفته شده است.

برای دموی درس ما فیشینگ سایت شناسه یکتا دانشگاه به آدرس utid.ut.ac.ir را انتخاب کردیم.

Site Cloning

برای اینکار ابتدا نیاز است تا سایت clone شود، یکی از ابزارهای مناسب برای اینکار ابزار HTTrack می‌باشد، با اجرای برنامه و انتخاب هدف و تنظیمات پایه برنامه به راحتی سایت مورد نظر را copy می‌کنیم. با تغییر فایل‌های کپی شده می‌توان آدرسی را که اطلاعات کاربر را برای سرور اصلی ارسال می‌کند به سرور جعلی خودمان تغییر داده، سپس با استفاده از یک وب‌سرور ساده اقدام به جمع‌آوری اطلاعات کاربران و در آخر کاربر را به سایت اصلی redirect کنیم.

Link Manipulation

بعد از این کار نیاز است تا آدرس جعلی شبیه به آدرس اصلی هدف را انتخاب کنیم تا بتوانیم کاربران را به دام بیندازیم. چون این حمله تنها با اهداف آموزشی انجام شده است و نیاز به هزینه نیست، از یک دامنه با آدرس utid.ut.ac.ir.cheapsi.ir (cheapsi.ir) که برای یک سرویس دیگه خریداری شده بود استفاده کردیم، دامنه‌ی utid.ut.ac.ir.cheapsi.ir را می‌توانستیم برای حمله انتخاب کنیم (فکر کنید با کمی هزینه دامین utid.ut.ac.ir را می‌توانستیم برای حمله انتخاب کنیم) دقت کنید که برای حملات نباید ردی از خود به جای گذاشت، برای همین از دامنه‌هایی که اطلاعات مالک دامنه را موقع ثبت دامنه از کاربر می‌گیرند باید اجتناب کرد و انتخاب دامنه با دامین ir خیلی منطقی به نظر نمی‌رسد. برای اینکار می‌توان از سرویس‌هایی که خرید هاست و دامین را به صورت ناشناس و به صورت Anonymous انجام دهند استفاده کرد.

SSL

می‌توانیم با اضافه کردن HTTPS به سرور خود بیش از پیش اعتماد کاربران را برای وارد کردن رمز عبور خود در وب‌سایت جعلی ما جلب کنیم چرا که با توجه به آموزش‌های اشتباه به افراد، اکثر افراد گمان می‌برند که تصویر قفل سبز رنگ کنار آدرس وب‌سایت تضمین امنیت اطلاعات آن‌هاست. برای این منظور می‌توان با استفاده از سرویس‌های رایگانی مثل [let's encrypt](https://letsencrypt.org/) اقدام به گرفتن گواهی ssl کنیم، این سرویس یکی از بهترین و راحت‌ترین سرویس‌های رایگان برای این کار است.

Email Spoofing

برای اینکه کاربران هدف خود را وادار به استفاده از صفحه جعلی خود کنیم از یک ایمیل جعلی که به کاربران اخطار می‌دهد تا هرچه زودتر اطلاعات کاربری خود را در سامانه بروزرسانی کنند کمک گرفتیم، پروتکل ارسال ایمیل پروتکل قدیمی‌ای است که از امنیت پایینی برخوردار است، به سادگی می‌توان با تغییر مقدار From در سرآغاز بسته‌های ایمیل به مقدار دلخواه اقدام به email spoofing کرد، ما با ایجاد پیامی با نگارش مشابه به ایمیل‌های اصلی دانشگاه و اخطار به کاربران در مورد بروزرسانی اطلاعات کاربری‌شان در سامانه [utid](http://utid.ut.ac.ir) و با استفاده از تکنیک‌های link hiding به ارسال آن به تعدادی از کاربران هدف اقدام کردیم. (با توجه به اینکه این حمله تنها برای مقاصد آموزشی انجام شده بود تنها تعدادی از دانشجویان این درس، استاد و چیفتی‌ای هدف قرار گرفتند)

نتایج

بعد از گذشتن ۲ روز از سی نفر هدف ۱۱ نفر در دام افتاده‌اند که برای این نوع حمله درصد موفقیت بالایی به حساب می‌آید. (جامعه‌ی هدف افرادی بودند که از دانش کامپیوتری بالایی برخوردار بودند و حتی درس امنیت شبکه را گذرانده بودند، تصور کنید این هدف روی سایر دانشجویان و با دانش کمتری و به صورت حرفه‌ای‌تر انجام می‌شد، آنگاه درصد موفقیت می‌توانست خیلی بیشتر از این عدد نیز باشد.)

در این دمو ما نشان دادیم که حملات فیشینگ در عین حال که نیاز به دانش بسیار کمی دارند می‌توانند تا چه حد مخرب باشند و سیستم‌هایی حتی با بالاترین درجه امنیت را به سادگی درهم شکنند چرا که این حملات بیشتر از اینکه خود سیستم‌ها را هدف قرار دهند، کاربران ناآگاه را مورد هدف قرار می‌دهند.

در انتها می‌توانید دمو انجام این حمله را از [این آدرس](#) مشاهده کنید.

منابع

- <https://searchnetworking.techtarget.com/definition/Address-Resolution-Protocol-ARP>
- <https://www.veracode.com/security/arp-spoofing>
- https://www.webopedia.com/TERM/A/ARP_spoofing.html
- <https://blog.eccouncil.org/the-rise-of-dns-hijacking-and-how-to-avoid-it/>
- <https://blog.returnpath.com/how-to-explain-dkim-in-plain-english-2/>
- https://en.wikipedia.org/wiki/Sender_Policy_Framework
- <https://postmarkapp.com/guides>
- <https://github.com/trustedsec/social-engineer-toolkit>
- <https://www.computerweekly.com/tutorial/Social-Engineer-Toolkit-SET-tutorial>
- <https://en.wikipedia.org/wiki/Typosquatting>
- <https://securingtomorrow.mcafee.com/consumer/family-safety/what-is-typosquatting/>
- <https://github.com/elceef/dnstwist>