

بسم الله الرحمن الرحيم

نویسنده و گردآورنده : علی انصاری

ایمیل : Ansari1375@gmail.com

کتابخانه الکترونیکی ویکیو : <http://ebook.veyq.ir>

فهرست مطالب

3	مقدمه
4	از چه راه هایی هک میشود؟
5	تروجان ها
6	لینک هایی که آی پی شما را به هکر میدهد
7	صفحات تقلبی(Fake Page)
8	روش کار صفحات تقلبی
9	برنامه های تقلبی(Fake Program)
10	کیلاگر ها
11	کرکر ها
12	مهندسی اجتماعی

با سلام، تقریباً چندین سال است که چت با ابزارهایی نظیر یاھو مسنجر ارتباط سریع و ساده میان ایرانیان را فراهم ساخته است. اخیراً نیز شبکه‌های اجتماعی نظیر فیسبوک و گوگل پلاس پدید آمده اند که نسبت به یاھو از امکانات بیشتری بهره‌مند هستند. نقطه مشترک میان آنها مسئله امنیت است. شاید برای شما هم پیش آمده باشد که در فضای اینترنت هک شده باشید و احتمالاً بعد از آن از شما اخاذی شده باشد. احساس امنیت در اینترنت هم ممکن است. فقط باید راه‌های نفوذ را شناسایی و آنها را برطرف نماییم. در این کتاب متدائل ترین روش‌ها توضیح داده شده و همچنین بهترین روش‌های جلوگیری هم بیان شده است. پس دیگر نگران امنیت خود نباشید!

با تشکر، علی انصاری

امنیت هنگام چت و صحبت کردن در فضای اینترنت از چه راه هایی هک میشود؟

1-تروجان ها و کیلرگر ها

2-صفحاتی که آیپی شما را به هکر میدهند

3-صفحات تقلبی

4-کرکر ها

5-مهندسی اجتماعی!!!

این پنج روش از متدائل ترین روش های هک کردن کاربران فضای مجازی است. هر کدام از اینها به راحتی قابل جلوگیری است به جز روش پنجم که کاملا به خودتان بستگی دارد. در ادامه بیشتر توضیح خواهیم داد.

تعریف: تروجان یک فایل جاسوسی میباشد که توسط هکر با توجه به نیاز به اطلاعات قربانی آماده میشود و برای قربانی فرستاده میشود.

به عنوان مثال هکر به تروجان یا همان فایل جاسوسی دستور میدهد که برود و از مکان مشخصی از کامپیوتر شما پسورد های ذخیره شده را بدزد و برای ایمیل هکر بفرستد که اگر با موقوفیت همراه باشد زیان های جبران ناپذیری به بار می آورد. از جمله نرم افزار های ساخت تروجان Magic Ps است که هکر های زیادی از آن بعنوان یک تروجان ساز معحبوب یاد میکنند.

معمولًا تروجانها به دو قسمت تقسیم میشوند:

- 1-کلابینت: که تنظیمات را انجام داده و آن را با توجه به نیازهایی که بیان کردیم تنظیم مینمایند.
- 2-سرور: که بعد از تنظیمات باید این سرور برای قربانی فرستاده شود تا قربانی بعد از دریافت آن را اجرا کند.

با پیشرفت تروجان ها این امکانات به آنها اضافه شد.

- 1-فرستاده شدن اکانت اینترنت شما برای هکر
- 2-فرستاده شدن نام کامپیوتر شما همراه با پسورد ویندوز برای هکر
- 3-محدود کردن کارهای شما با کامپیوتر(قفل شدن Task Manager) کامپیوتر شما توسط هکر
- 4-از کار انداختن ویروس کش و فایروال کامپیوتر شما
- 5-در اختیار داشتن هارد شما توسط هکر(پاک کردن فایل از کامپیوتر شما و یا اضافه کردن فایل توسط هکر)

یک تروجان میتواند به صورت فایل اجرایی (exe) برای شما ارسال شود یا یک فایل صوتی یا تصویری با تروجان ادغام شود(Bind). در صورت دوم شما متوجه نمیشوید که این یک تروجان است.

در صورتی که کامپیوتر شما این مشخصات را دارد بگویم متسافانه کامپیوتر شما آلوده به تروجان است.

- 1-در صورت از کار افتادن Msconfig و Task Manager
- 2-از کار افتادن ویروس کش
- 3-تغییر در شکل نوپی پسورد در مسنجر ویا سیو نشدن آن
- 4-در صورت دیدن علائم مشکوک در مسنجر(باز و بسته شدن یک پنجره پی ام)
- 5-فعال بودن نرم افزار های مشکوک مثل Msconfig و Task Manager
- 6-خوانده شدن ایمیل های که ما آنها را قبلاً نخوانده ایم

برای جلوگیری از آلوده شدن به تروجان این موارد را رعایت کنید:

- 1-از هر فرد ناشناسی فایل دریافت نکنید
 - 2-همیشه Task Manager و Msconfig خود را چک کنید اگر چیزی مشکوک دیدید مثل Windows/system32 sender.exe در درایو ویندوز پوشش دنباله چنین فایلی باشید که مشکوک بود و آن را پاک کنید.
 - 3-آنتی ویروس خود را همیشه به روز نگه دارید.
- برای از بین بردن تروجان ها از Anti Trojan Elite استفاده کنید.

لینک هایی که آپی شما را به هکر میدهند

آپی یک نشانی چهار قسمتی است که هر قسمت شامل یک عدد بین 0 تا 255 میباشد. شما وقتی به اینترنت متصل میشوید دارای یک آپی مثل آپی زیر هستید:

0.1.2.3

اگر کسی که مقاصد بدی دارد(هکر) آپی شما را بداند با آنلایز کردن پورت های باز شما به راحتی به سیستم شما دسترسی پیدا میکند.

سایت myspy.ir این خدمت را برای هکر ها انجام میدهد!!!

این سایت یک لینک به هکر میدهد و هکر هم آنرا به شما میدهد. آپی، سیستم عامل، مرورگر، سایت هایی که دیده اید و اطلاعات حساس دیگری با باز شدن این لینک توسط شما به هکر داده میشود.

این قشر از لینک ها قابل شناسایی نیست. تنها راهی که میتوانید از شر این روش آسوده باشید این است که هوشیار باشید و هر لینکی را از هر ناشناسی که به شما میدهد باز نکنید.

نصب یک فایروال خوب نیز میتواند بسیار موثر باشد. چون فایروال ها معمولاً آپی این جور سایت ها را بلاک میکنند و به شما اجازه ورود نمیدهند.

صفحات تقلیبی

صفحات تقلیبی یا Fake Page از محبوب ترین روش ها نزد هکر ها است. صفحات تقلیبی دقیقاً شبیه بعنوان مثل یاهو میل است. نوشه ها، سایر ها و همه چیز دقیقاً مثل صفحه اصلی یاهو میل است. با وارد کردن ایمیل و پسورد شما هردو در جایی ذخیره میشوند و هکر بعداً به سراغ آنها خواهد رفت و احتمالاً عواقب مخربی خواهد داشت.

راه های شناسایی صفحه تقلیبی یا فیک پیچ

1- اصولی ترین راه نگاه کردن به آدرس است. بعنوان مثال آدرس یاهو میل اینچنین است:

<http://yahoomail.com>

اما آدرس فیک پیچ ممکن است شبیه آدرس بالا باشد اما هیچوقت خود این آدرس نیست پس با کمی دقت میتوانید بفهمید که این صفحه واقعی است یا تقلیبی.
مثال آدرس فیک پیچ:

<http://yahoomail.felan.com>

2- برای شناسایی صفحه تقلیبی میتوان به کد صفحه نیز توجه کرد. برای این کار روی صفحه راست کلیک کنید و View Source را انتخاب کنید. اکنون کد html صفحه برای شما نمایان میشود.
حالا دنبال واژه action بگردید.
چیزی شبیه به این خواهد دید:

```
<form method="post" action="https://login.yahoo.com/config/login?">
```

یک آدرس جلوی action وجود دارد. میبینید که آدرس مربوط به سایت یاهو میباشد پس این صفحه نمیتواند تقلیبی باشد.

<https://login.yahoo.com/config/login?>

3- روش سوم شناسایی فیک پیچ ها وارد شدن با ایمیل و پسورد بی ارزش است. بدین منظور یک ایمیل تازه بسازید و با آن ایمیل و پسورد وارد شوید. اگر پیغام خطأ داد بدین معنی است که این یک صفحه تقلیبی است. اما صفحات تقلیبی گاهها پس از ورود به صفحه اصلی یاهو منتقلتان میکنند که شک نکنید. این هم با نگاه کردن به آدرس و دیدن تغییرات قابل شناسایی است.

روش کار صفحات تقلیبی

برای اینکه روش کار صفحات تقلیبی را بدانیم ابتدا لازم است کمی از زبان های برنامه نویسی زیر سررشنط داشته باشیم.

Html,PHP

هکر ها ابتدا کد صفحه اصلی یا هو میل را ذخیره میکنند. سپس با تغییر دادن آدرس جلوی اکشن صفحه را منحرف میکنند و به یک فایل پی اچ پی انتقال میدهند. فایل پی اچ پی اطلاعات به دست آمده از صفحه تقلیبی را تحلیل میکند و آن را در یک فایل متند ذخیره میکند.

نمونه کدنویسی صفحه تقلیبی:

```
<form method="post" action="hacker.php"
```

نمونه فایل پی اچ پی هکر:

```
<?php  
header ('Location: /error.php ');\n$handle = fopen("Hacker.txt", "a");\nforeach($_POST as $variable => $value) {\n    fwrite($handle, $variable);\n    fwrite($handle, "=");\n    fwrite($handle, $value);\n    fwrite($handle, "\r\n");\n}\nfwrite($handle, "\r\n");\nfclose($handle);\nexit;\n?>
```

Hacker.txt

این برنامه پی اچ پی اطلاعات شما را در فایلی با نام زیر ذخیره میکند:

برنامه های تقلبی (Fake Program)

این روش خیلی خطرناک هست. چون شما نمیتوانید به همین راحتی متوجه بشوید. هکر یک فایل مخرب را برای شما میفرستد. باز کردن آن فایل بعنوان مثال یاهو مسنجر شما آلوود خواهد شد. این الودگی به شکل ظاهری خودش را نشان نمیدهد. شما اکنون در کامپیوتر خود یک برنامه تقلبی دارید که آن هم یاهو مسنجر میباشد!!!

در این حال اگر با آیدی و پسورد خود وارد شوید بلافاصله آیدی و پسورد شما برای هکر ارسال میشود. زیرا ایندفعه تروجان در قلب یاهو مسنجر شما نفوذ کرده است.

راه های جلوگیری از این روش

1- آنتی ویروس خود را بروز نگه دارید.

2- همیشه جدید ترین نسخه یاهو مسنجر را نصب کنید.

3- یاهو مسنجر خود را از سایت های معتر دانلود کنید.

کیلاگر ها

کار کیلاگر ها بسیار ساده و همچنان بسیار مخرب است. کیلاگر ها در ابتدا فقط کلید های زده شده روی کیبورد را برای هکر میفرستند. اما با پیشرفت علم هکینگ کیلاگر ها دارای امکاناتی نظیر عکس گرفتن از صفحه و فرستادن برای هکر شدند.

کیلاگر ها اطلاعات رو به ایمیل هکر یا یک سرور اف تی پی میفرستند که در هر دو صورت یکی از مشخصه ها کاهش ناگهانی سرعت اینترنت و بازگشت به حالت عادی است.

دور زدن کیلاگر ها بسیار مشکل هست چرا که قادر هستند خودشون رو مخفی کنند. اما اصلا نگران نباشید، چون همیشه یک راه حل وجود دارد.

متداول ترین راه های دور زدن کیلاگر

1- استفاده از یک آنتی ویروس بروز و پر قدرت.

2- استفاده از صفحه کلید های مجازی نظیر صفحه کلید ویندوز که از آدرس زیر قابل دسترسی هست:

Start – All Programs – Accessories - Ease of Access - On-Screen Keyboard

3- زدن کلید های متفرقه و اشتباه به هنگام وارد کردن پسورد برای سردرگم کردن هکر.

یک برنامه ضد کیلاگر:

<http://www.anti-keyloggers.com>

روش کار cracker به این صورت است که تعداد زیادی پسورد به همراه آیدی شما به برنامه cracker داده میشود و برنامه با اتصال به سرور های یاهو این پسورد ها را امتحان کرده و وقتی به پسورد درست رسید به هکر اطلاع می دهد. این روش همان روش آزمون و خطا میباشد.

در اوایل کار یاهو قانونی وضع کرد که طبق آن اگر از طرف یک آیپی تعداد زیادی لاغین انجام شود آن آیپی دیگر قادر به لاغین نخواهد بود. با این روش تا مدتی جلوی کرکرها را گرفت. اما مدتی بعد هکرهای خلاق با نصب پروکسی روی برنامه باعث شدند کرکرها را چند گاهی آیپی خود را عوض کند تا یاهو آنرا شناسایی نکند. هنوز هم این روش پروکسی کارایی دارد.

برنامه هایی هم هستند که تعداد زیادی پسورد می سازند برای کرکرها.

مهم ترین راه جلوگیری از لو رفتن پسورد توسط کرکر انتخاب یک پسورد طولانی است. گاهها گفته میشود در پسورد خود از کاراکتر های عجیب و غریب استفاده کنید. اما من به شما میگویم که استفاده از کاراکتر های عجیب و غریب کاملاً بی فایده است. چون همان برنامه های پسورد ساز میتوانند پسورد هایی شبیه پسود شما سازند.

به سایت زیر بروید:

<http://www.passwordmeter.com>

این سایت به شما میگوید پسوردتان چقدر قوی است و چقدر طول میکشد تا کرک شود.

این سایت نیز به شما کمک میکند پسوردی قوی بسازید:

<http://strongpasswordgenerator.com>

استفاده از این دو سایت به شدت توصیه میشود.

تعريف بین المللی از مهندسی اجتماعی در سایت ویکیپدیا چنین آمده است :

مهندسي اجتماعي هنر بهره برداري از رفاتهای آسيب پذير انسانها برای ايجاد شکاف امنيتی بدون هيچ ظن و گمانی از سوی قرباني است.

تمام راه هايی که در اين كتاب نوشته شده با بكار بردن مهندسی اجتماعی دو برابر آسانتر ميشود.

با يك مثال اين مسئله را توضيح ميدهم.

هکر برای فرستادن تروجان یا کیلاگر به سمت قربانی نیاز دارد تا قربانی را به این کار ترغیب کند. به این منظور از جمله های جذابی مثل "کاملا رایگان"، "عکس های فلان هنرپیشه" و... قربانی را ترغیب به دانلود فایلی میکند که آلوده به تروجان یا کیلاگر است.

1-لينک هايی که خبر های بزرگ دارد: مثل خبر مرگ یا اتفاقی بزرگ برای شخصیت های مهم.

2-جعل هویت:کسی که خود را از دوستان شما معرفی میکند.

این دو از برترین روش های مهندسی اجتماعی به شمار میروند.

نکته مهم:مهندسي اجتماعي تنها ترغیب برای دریافت فایل خاصی نیست. بلکه یک نفر ممکن است از شما بخواهد مشخصات تولد خود را به او بدهید.اما او با دانستن اینها میتواند رمز عبور شما را از یاهو دریافت کند.