۱– راهنمای پاکسازی بدافزار Flame با استفاده از ابزار شناسایی و پاکسازی ارائه شده توسط مرکز ماهر

جهت استفاده از این ابزار ابتدا مطابق دستورالعمل پیوست وارد محیط Safe Mode شوید. سپس مراحل ذیل را در این محیط دنبال کنید:

۱- فقط و فقط پوشه[1] Remover را در درایو C کپی کنید. این پوشه حاوی دو فایل به نام های remover.exe و 7za.exe می باشد.

۲- سپس فایل remover.exe را اجرا نمایید (توجه داشته باشید که این فایل در صورتی به درستی اجرا خواهد شد که حتما در مسیر C:\Remover\remover.exe باشد).

۳- در صورت اجرای صحیح این ابزار، در فولدر C:\Remover سه فایل zip شده (مطابق شکل زیر) به نام های Files.zip، Temp.zip و InfFolders.zip ایجاد می گردد (فایل 7za.exe نیزکه در این پوشه قرار دارد توسط برنامه remover.exe به منظور ایجاد فایلهای zip به کار می رود و کاربرد دیگری ندارد).

Name	Date modified	Type	Size
7za.exe	11/18/2010 8:27 PM	Application	574 KB
Files.zip	5/27/2012 12:21 PM	WinRAR ZIP archive	1 KB
InfFolders.zip	5/27/2012 12:21 PM	WinRAR ZIP archive	1 KB
Remover.exe	5/27/2012 11:46 AM	Application	121 KB
Temp.zip	5/27/2012 12:21 PM	WinRAR ZIP archive	1 KB

۴- در صورتی که سیستم شما آلوده نباشد، پیغام زیر نمایش داده می شود:

```
Congratulation!
Your System Is Clean :)
Press any key to continue . . .
```

[1] Folder

۵- در صورت آلوده بودن سیستم، پیغام زیر نمایش داده خواهد شد:

```
WARNING!!!
Your System Was Infected and Now Is Clean!
Please Send Files.zip to Maher
cert@certcc.ir
www.certcc.ir
Press any key to continue . . .
```

این بدان معناست که سیستم شما آلوده به بدافزار بوده ولی در حال حاضر با اجرای این ابزار آلودگی آن برطرف شده است. با این حال به منظور اطمینان بیشتر شما بایستی فایل Files.zip را به همراه نام سازمان خود به مرکز ماهر به نشانی پست الکترونیکی cert@certcc.ir ارسال نمایید. دو فایل دیگری که با اجرای برنامه ایجاد می شوند (Temp.zip و InfFolders.zip) ممکن است حاوی اطلاعاتی در خصوص فایل های سیستم آلوده و شبکه ای که در آن قرار دارد باشد، لذا در خصوص ارسال آنها به مرکز ماهر می بایست از پیش با مدیر مربوطه و حراست هماهنگی های لازم صورت پذیرد.

***توضیح ۱ : تمامی مراحل بایستی در safemode و با کاربری با سطح دسترسی administrator انجام گیرد.**

***توضیح ۲ : این ابزار قابلیت اجرا تحت domain را دارد ولی هیچگونه تستی بر روی آن صورت نگرفته است.**

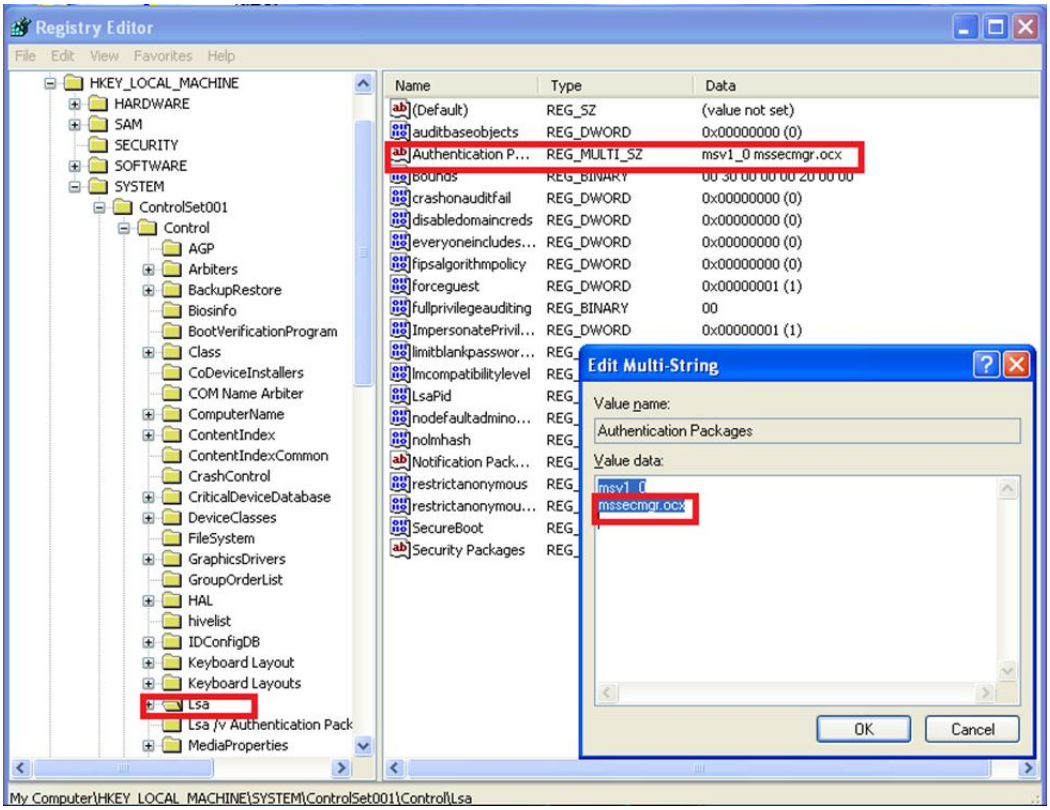
۱- راهنمای پاکسازی بدافزار Flame به صورت دستی

برای این کار ابتدا مطابق دستورالعمل پیوست وارد محیط Safe Mode شوید. سپس مراحل ذیل را در این محیط دنبال کنید:

۱- با دستور regedit وارد محیط رجیستری شده و در مسیر زیر مقدار رجیستری[2] Authentication package را یافته و کلید modify را بزنید. داده mssecmgr.ocx را از این مقدار رجیستری پاک کنید.

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa

[2] Registry Value



۲- در مسیر c:\windows\system32 کلیه فایل های زیر را برداشته (cut) و سپس در یک فولدر با نام مشخص کپی و zip کنید.

- mssecmgr.ocx
- ccalc32.sys
- msglu32.ocx
- boot32drv.sys
- ntep32.ocx
- soapr32.ocx
- advnetcfg.ocx
- to961.tmp
- sstab*.dat

۳- در مسیر c:\windows فایل EF_trace.log را برداشته (cut) و سپس در یک فولدر با نام مشخص کپی و zip کنید.

۴- در مسیر C:\Program Files\Common Files\Microsoft Shared چنانچه پوشه هایی با نام های MssecurityMgr و MsAudio وجود دارد از این مسیر حذف به در یک پوشه جدا کپی و zip گردد.

۵- در مسیر C:\windows\temp فایل های زیر را پیدا کرده و در یک پوشه جدا کپی و zip کنید.

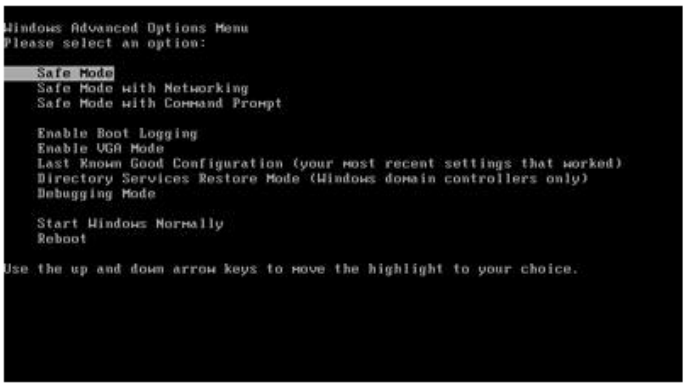
- ~KWI*.tmp
- ~KLV*.tmp
- ~ZFF*.tmp
- ~dra*.tmp
- ~DEB.tmp
- ~DFL*.tmp
- ~DFA*.tmp
- ~rei*.tmp
- ~TFL*.tmp

پیوست الف) طریقه وارد شدن به محیط Safe Mode

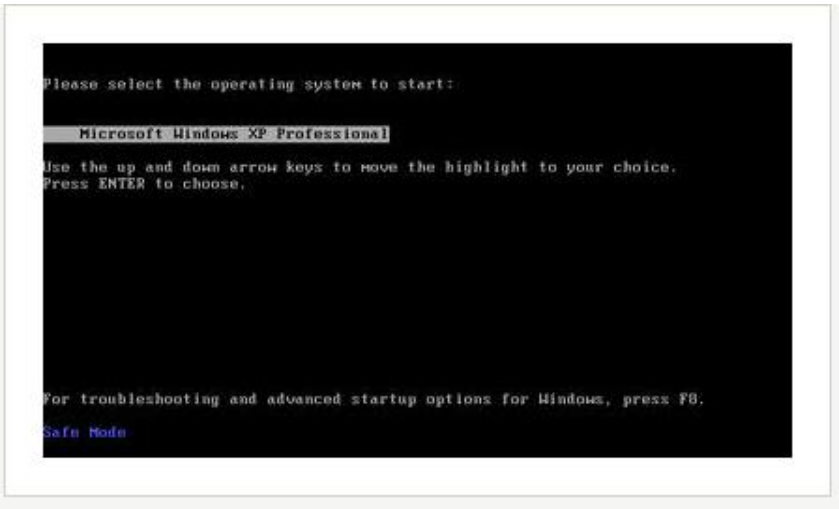
در ادامه شرح وارد شدن به محیط Safe Mode در ویندوزهای XP، Vista و 7 به تفصیل بیان شده است.

ویندوز XP:

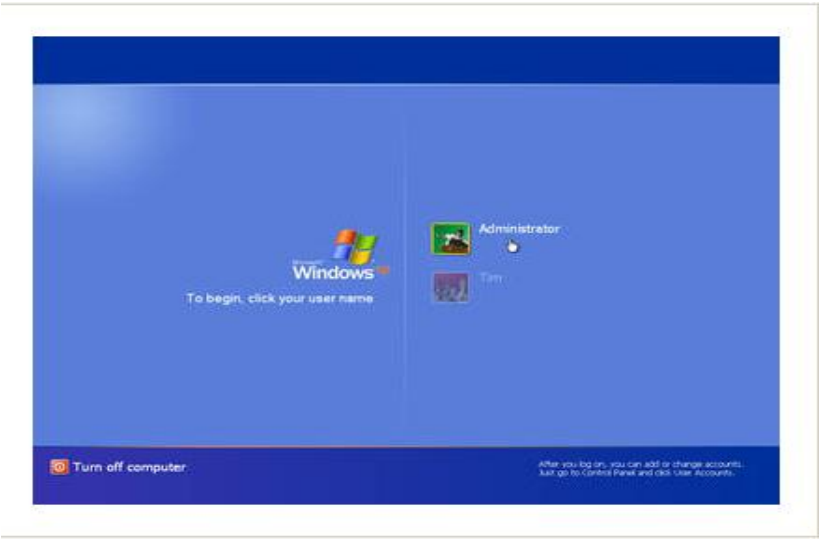
۱- شما باید پیش از مشاهده لوگوی ویندوز مرتب کلید F8 را فشار دهید تا صفحه ای مطابق شکل زیر مشاهده نمایید.



۲- اکنون گزینه Safe Mode را مطابق شکل فوق انتخاب کنید. حال صفحه دیگری مطابق شکل زیر نمایش داده خواهد شد که از شما می خواهد سیستم عامل مورد نظر خود را انتخاب کنید.



۳- پس از انتخاب گزینه مورد نظر ویندوز بوت شده و صفحه login نمایش داده می شود. اکنون شما بایستی با کاربری که دسترسی کاربر ارشد (Administrator) دارد، login کنید. سپس وارد محیط safe mode می شوید.



در صورتی که موفق به انجام این کار نشدید می توانید از دستور msconfig که در آخرین صفحه این راهنما توضیح داده شده است استفاده نمایید

ویندوز VISTA:

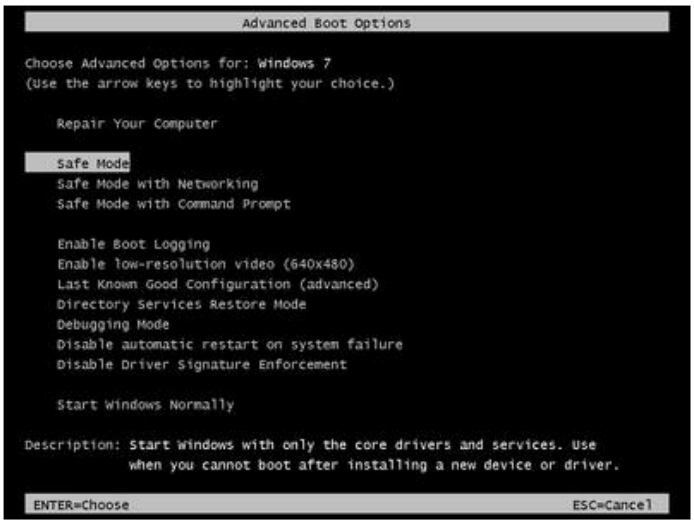
۱- شما باید پیش از مشاهده لوگوی ویندوز مرتب کلید F8 را فشار دهید تا صفحه ای مطابق شکل زیر مشاهده نمایید.

۲- اکنون گزینه Safe Mode را مطابق شکل فوق انتخاب کنید. حال صفحه login نمایش داده می شود. اکنون شما باید با کاربری که دسترسی کاربر ارشد (Administrator) دارد، login کنید. سپس وارد محیط safe mode می شوید.

در صورتی که موفق به انجام این کار نشدید می توانید از دستور msconfig که در آخرین صفحه این راهنما توضیح داده شده است استفاده نمایید

ویندوز 7:

۱- شما باید پیش از مشاهده لوگوی ویندوز مرتب کلید F8 را فشار دهید تا صفحه ای مطابق شکل زیر مشاهده نمایید.

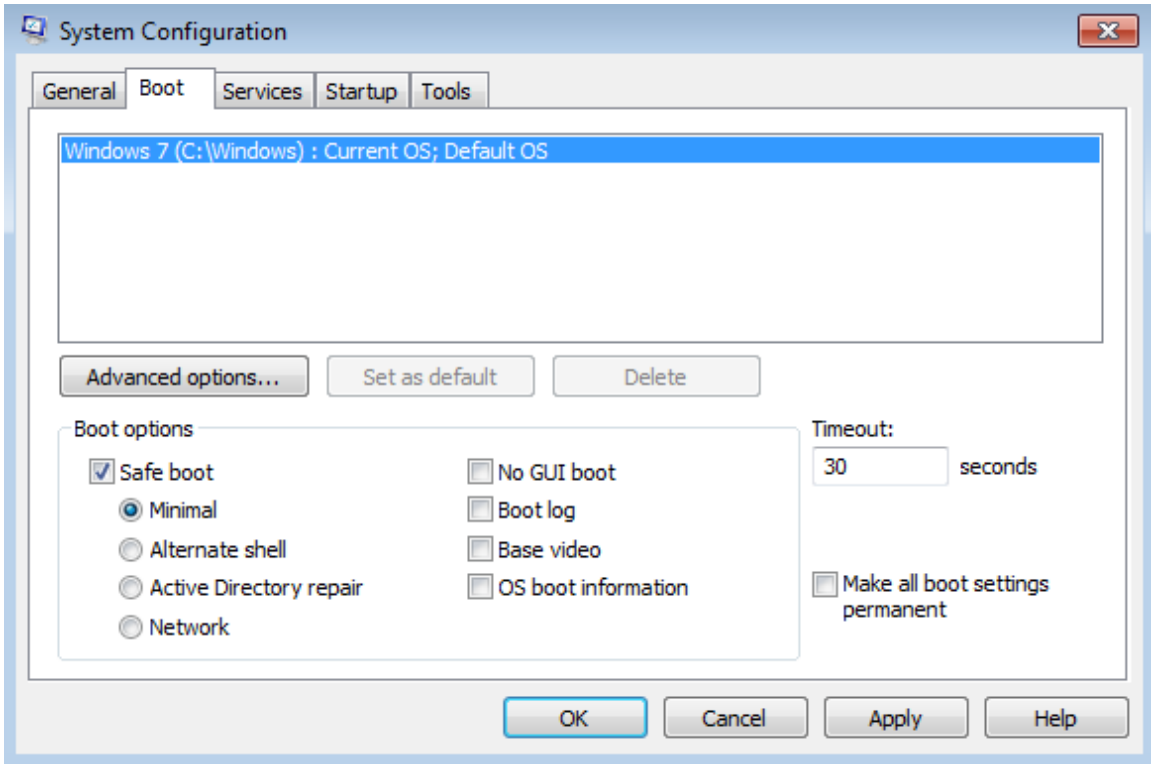


۲- اکنون گزینه Safe Mode را مطابق شکل فوق انتخاب کنید. حال صفحه login نمایش داده می شود. اکنون شما باید با کاربری که دسترسی کاربر ارشد (Administrator) دارد، login کنید. سپس وارد محیط safe mode می شوید.

در صورتی که موفق به انجام این کار نشدید می توانید از دستور msconfig که در آخرین صفحه این راهنما توضیح داده شده است استفاده نمایید

استفاده از msconfig:

جهت بوت کردن سیستم ها در شرایط safe mode می توانید از دستور msconfig.exe استفاده کنید. برای این کار در ویندوز XP از منوی start گزینه run را انتخاب کرده و در آن عبارت msconfig را تایپ کرده، کلید Enter را فشار دهید. در ویندوز 7 و Vista شما باید در قسمت search منوی start عبارت run را تایپ کرده و enter کنید. سپس در آن عبارت msconfig را تایپ کرده و ok را کلیک کنید. اکنون پنجره ای مطابق شکل زیر مشاهده خواهد شد. در لبه boot و در قسمت boot options گزینه safe boot را انتخاب کرده و تغییرات ایجاد شده را تایید کنید.



اکنون پیغامی مطابق شکل زیر به شما نمایش داده خواهد شد. اگر اکنون قصد restart کردن سیستم را دارید گزینه Restart را انتخاب کنید و در غیر این صورت گزینه Exit without restart را انتخاب نمایید. سیستم شما پس از راه اندازی مجدد در محیط safe mode بوت می شود.

*** هشدار: در صورتی که از این روش استفاده می کنید پس از اتمام کار در محیط Safe Mode تنظیمات را به حالت اولیه برگردانید. یعنی تیک قسمت safe boot را بردارید در غیر این صورت سیستم شما همواره در محیط Safe Mode بوت خواهد شد.**