吾爱破解论坛

[LCG]

[LSG]

立足软件安全和病毒分析最前端，丰富的技术版块交相辉映，由无数加密解密及反病毒爱好者共同维护，留给世界一抹值得百年回眸的惊艳，沉淀百年来计算机应用之精华与优雅，信息线条与生活质感淡定交融，任岁月流转，低调而奢华的技术交流与研究却是亘古不变。

标题：Win32.Virut.ce 不完整报告

作者：roxiel

来源:byxxdrls　文件为被感染的 sreng 可执行文件
MD5: 0xD96C28619A2BBA73C8B439039E1B5419
大小: 2,232,320 bytes

HOSTS 文件被修改
127.0.0.1 jL.chura.pl
#.0.0.1 www.powernum123.com
127.0.0.1 www.powernum123.com.cn
127.0.0.1 powernum123.com
127.0.0.1 powernum123.com.cn
127.0.0.1 www.chebl.com
127.0.0.1 www.chebl.cn
127.0.0.1 www.chebl.com.cn
127.0.0.1 chebl.com
127.0.0.1 chebl.com.cn
127.0.0.1 chebl.cn
127.0.0.1 www.chebuluo.com.cn
127.0.0.1 www.chebuluo.com
127.0.0.1 www.chebuluo.cn
127.0.0.1 chebuluo.com.cn
127.0.0.1 chebuluo.com
127.0.0.1 chebuluo.cn
127.0.0.1 www.17sp.com
127.0.0.1 www.17sp.com.cn
127.0.0.1 17sp.com
127.0.0.1 17sp.com.cn
127.0.0.1 www.feikong.com
127.0.0.1 www.feikong.com.cn
127.0.0.1 www.feikong.cn
127.0.0.1 feikong.com
127.0.0.1 feikong.com.cn
127.0.0.1 feikong.cn
127.0.0.1 www.hacong.com
127.0.0.1 hacong.com
127.0.0.1 www.xbxbxbxb.com
127.0.0.1 www.sobt.com
127.0.0.1 www.sobt.com.cn
127.0.0.1 www.sobt.cn
127.0.0.1 www.sobt.net
127.0.0.1 sobt.com
127.0.0.1 sobt.com.cn
127.0.0.1 sobt.cn
127.0.0.1 sobt.net

感染文件：（？ 和*为通配符,*为 0 个或多个字符，?这里指系统盘。 Progra~1=Program Files）
c:\contacts.html
c:\Inetpub\wwwroot\index.html
share\msinfo32.exe
share\sapisvr.exe
share\Blank.htm
share\Citrus Punch.htm
share\Clear Day.htm
share\Fiesta.htm
share\Glacier.htm
share\Ivy.htm
share\Leaves.htm
share\Maize.htm
share\Nature.htm
share\Network Blitz.htm
share\Pie Charts.htm
share\Sunflower.htm
share\Sweets.htm
share\Technical.htm
SHARE\msinfo32.exe
SHARE\sapisvr.exe
?:\Progra~1\Common Files\System\ado\MDACReadme.htm
?:\Progra~1\Internet Explorer\Connection Wizard\icwconn1.exe
?:\Progra~1\Internet Explorer\Connection Wizard\icwconn2.exe
?:\Progra~1\Internet Explorer\Connection Wizard\icwrmind.exe
?:\Progra~1\Internet Explorer\Connection Wizard\icwtutor.exe
?:\Progra~1\Internet Explorer\Connection Wizard\inetwiz.exe
?:\Progra~1\Internet Explorer\Connection Wizard\isignup.exe
?:\Progra~1\Internet Explorer\iedw.exe
?:\Progra~1\Internet Explorer\IEXPLORE.EXE
?:\Progra~1\MSN\MSNIA\msniasvc.exe
?:\Progra~1\MSN\MSNIA\prestp.exe
?:\Progra~1\MSN\MsnInstaller\msninst.exe
?:\Progra~1\NetMeeting\cb32.exe
?:\Progra~1\NetMeeting\conf.exe
?:\Progra~1\NetMeeting\wb32.exe
?:\Progra~1\Outlook Express\msimn.exe
?:\Progra~1\Outlook Express\oemig50.exe
?:\Progra~1\Outlook Express\setup50.exe
?:\Progra~1\Outlook Express\wab.exe
?:\Progra~1\Outlook Express\wabmig.exe
?:\Progra~1\Web Publish\WPWIZ.EXE
?:\Progra~1\Windows Media Player\migrate.exe

?:\Progra~1\Windows Media Player\mplayer2.exe
?:\Progra~1\Windows Media Player\setup_wm.exe
?:\Progra~1\Windows Media Player\wmplayer.exe
?:\Progra~1\Windows NT\Accessories\wordpad.exe
?:\Progra~1\Windows NT\dialer.exe
?:\Progra~1\Windows NT\hypertrm.exe
?:\Progra~1\Windows NT\Pinball\PINBALL.EXE
?:\windows\hh.exe
?:\windows\inf\unregmp2.exe
?:\windows\Installer\{350C97B0-3D7C-4EE8-BAA9-00BCB3D54227}\places.exe
?:\windows\Microsoft.NET\Framework\NETFXSBS10.exe
?:\windows\Microsoft.NET\Framework\v2.0.50727\aspnet_compiler.exe
?:\windows\Microsoft.NET\Framework\v2.0.50727\aspnet_regbrowsers.exe
?:\windows\Microsoft.NET\Framework\v2.0.50727\aspnet_regsql.exe
?:\windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
?:\windows\Microsoft.NET\Framework\v2.0.50727\dfsvc.exe
?:\windows\Microsoft.NET\Framework\v2.0.50727\IEExec.exe
?:\windows\Microsoft.NET\Framework\v2.0.50727\InstallUtil.exe
?:\windows\Microsoft.NET\Framework\v2.0.50727\jsc.exe
?:\windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
?:\windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
?:\windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
?:\windows\msagent\agentsvr.exe
?:\windows\mui\muisetup.exe
?:\windows\NOTEPAD.EXE
?:\windows\pchealth\helpctr\binaries\HelpCtr.exe
?:\windows\pchealth\helpctr\binaries\HelpHost.exe
?:\windows\pchealth\helpctr\binaries\HelpSvc.exe
?:\windows\pchealth\helpctr\binaries\HscUpd.exe
?:\windows\pchealth\helpctr\binaries\msconfig.exe
?:\windows\pchealth\helpctr\binaries\notiflag.exe
?:\windows\pchealth\UploadLB\Binaries\UploadM.exe
?:\windows\pchealth\helpctr\System\blurbs\about_support.htm
?:\windows\pchealth\helpctr\System\blurbs\Favorites.htm
?:\windows\pchealth\helpctr\System\blurbs\ftshelp.htm
?:\windows\pchealth\helpctr\System\blurbs\History.htm
?:\windows\pchealth\helpctr\System\blurbs\Index.htm
?:\windows\pchealth\helpctr\System\blurbs\isupport.htm
?:\windows\pchealth\helpctr\System\blurbs\keywordhelp.htm
?:\windows\pchealth\helpctr\System\blurbs\options.htm
?:\windows\pchealth\helpctr\System\blurbs\searchblurb.htm
?:\windows\pchealth\helpctr\System\blurbs\searchtips.htm
?:\windows\pchealth\helpctr\System\blurbs\tools.htm
?:\windows\pchealth\helpctr\System\blurbs\windows_newsgroups.htm

?:\windows\pchealth\helpctr\System\CompatCtr\AboutCompat.htm
?:\windows\pchealth\helpctr\System\CompatCtr\CompatMode.htm
?:\windows\pchealth\helpctr\System\CompatCtr\CompatOffline.htm
?:\windows\pchealth\helpctr\System\CompatCtr\LearnCompat.htm
?:\windows\pchealth\helpctr\System\DVDUpgrd\dvdupgrd.htm
?:\windows\pchealth\helpctr\System\ErrMsg\ErrorMessagesOffline.htm
?:\windows\pchealth\helpctr\System\errors\badurl.htm
?:\windows\pchealth\helpctr\System\errors\connection.htm
?:\windows\pchealth\helpctr\System\errors\indexfirstlevel.htm
?:\windows\pchealth\helpctr\System\errors\notfound.htm
?:\windows\pchealth\helpctr\System\errors\offline.htm
?:\windows\pchealth\helpctr\System\errors\redirect.htm
?:\windows\pchealth\helpctr\System\errors\unreachable.htm
?:\windows\regedit.exe
?:\windows\system32\accwiz.exe
?:\windows\system32\actmovie.exe
?:\windows\system32\ahui.exe
?:\windows\system32\arp.exe
?:\windows\system32\asr_fmt.exe
?:\windows\system32\asr_ldm.exe
?:\windows\system32\asr_pfu.exe
?:\windows\system32\at.exe
?:\windows\system32\atmadm.exe
?:\windows\system32\attrib.exe
?:\windows\system32\auditusr.exe
?:\windows\system32\blastcln.exe
?:\windows\system32\bootcfg.exe
?:\windows\system32\bootok.exe
?:\windows\system32\bootvrfy.exe
?:\windows\system32\cacls.exe
?:\windows\system32\calc.exe
?:\windows\system32\charmap.exe
?:\windows\system32\chkdsk.exe
?:\windows\system32\chkntfs.exe
?:\windows\system32\cidaemon.exe
?:\windows\system32\cipher.exe
?:\windows\system32\cisvc.exe
?:\windows\system32\ckcnv.exe
?:\windows\system32\cleanmgr.exe
?:\windows\system32\clean_all.exe
?:\windows\system32\cliconfg.exe
?:\windows\system32\clipbrd.exe
?:\windows\system32\clipsrv.exe
?:\windows\system32\cmd.exe

?:\windows\system32\cmdl32.exe
?:\windows\system32\cmmon32.exe
?:\windows\system32\cmstp.exe
?:\windows\system32\Com\comrepl.exe
?:\windows\system32\Com\comrereg.exe
?:\windows\system32\comp.exe
?:\windows\system32\compact.exe
?:\windows\system32\conime.exe
?:\windows\system32\control.exe
?:\windows\system32\convert.exe
?:\windows\system32\cscript.exe
?:\windows\system32\ctfmon.exe
?:\windows\system32\dcomcnfg.exe
?:\windows\system32\ddeshare.exe
?:\windows\system32\defrag.exe

注意：这是它检测虚拟机后的结果，不能作为标准，它的感染可能具有多态性，即感染一个文件，换个特征再感染， 此文所有列表仅供参考

创建目录：
c:\System Volume Information\.
c:\System Volume Information\..
C:\WINDOWS\Backup

修改注册表
HKUSERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
--Cookies 、Cache、History

启动项：

<reader_s><?:\Documents and Settings\[USER NAME]\reader_s.exe>

服务：

[AshEvtSvc / AshEvtSvc][Running/Auto Start]
<C:\WINDOWS\System32\AshEvtSvc.exe -k netsvcs><N/A> 假冒安全软件
第二次运行的服务是：
[avast!Antivirus]<C:\WINDOWS\System32\avast!Antivirus.exe -k netsvcs><N/A>

添加映像劫持

关闭文件保护，防火墙等服务

删除安全模式

API HOOK:

ntdll.ZwCreateFile

ntdll.ZwOpenFile

ntdll.ZwCreateProcess

ntdll.ZwCreateProcessEx

ntdll.ZwQueryInformationProcess

【如何清除】
可以搜索专杀，进 PE 里使用
或者尝试 Dr.web CureIT

【如何防范】
根目录通过权限禁止创建文件夹
SYSTEM32 目录通过 NTFS 权限设置为不可新建不可修改（较极端）
安装一款安全软件，在打开网上或移动存储设备带来的东西前要扫描
平时扫描的文件类型要包含网页文件（网页是有可能被感染的，-HTM,HTML,ASP,PHP,JSP 等等）
尽量少浏览不健康网站

【如何收集感染样本】
建议将系统分区以外用权限设为不可访问，进行实机运行尝试，可行
感染后访问 virustotal 无效，浏览器直接下载 Windows 清理助手无效