恶意代码检测 虚拟机脱壳. Rootkit检测 木马检测 window._wpemojiSettings =

u(e,t,n){switch(t){case"flag":return n(e,"\ud83c\udff3\ufe0f\u200d\u26a7\ufe0f","\ud83c\udff3\ufe0f\u200b\u26a7\ufe0f")?!1:!n(e,"\ud83c\uddfa\ud83c\uddf3","\ud83c\uddfa\u200b\ud83c\uddf3")&&!n(e,"\ud83c\udff4\udb40\udc67\udb40 f(e,t,n){var r="undefined"!=typeof WorkerGlobalScope&&self instanceof WorkerGlobalScope?new OffscreenCanvas(300,150):i.createElement("canvas"),a=r.getContext("2d", {willReadFrequently:!0}),o=(a.textBaseline="top",a.font="600 32px Arial",{});return e.forEach(function(e){o[e]=t(a,e,n)}),o}function t(e){var t=i.createElement("script");t.src=e,t.defer=!0,i.head.appendChild(t)}"undefined"!=typeof Promise&&(o="wpEmojiSettingsSupports",s=["flag","emoji"],n.supports= {everything:!0,everythingExceptFlag:!0},e=new Promise(function(e){i.addEventListener("DOMContentLoaded",e,{once:!0})}),new Promise(function(t){var n=function(){try{var e=JSON.parse(sessionStorage.getItem(o));if("object"==typeof e&&"number"==typeof e.timestamp&&(new Date).valueOf()

```
img.wp-smiley, img.emoji { display: inline !important; border: none !important; box-shadow: none !important; height: 1em !important; width: 1em !important; margin: 0 0.07em !important; vertical-align: -0.1em !important; background: none !important; padding: 0 !important; }
/*! This file is auto-generated */ .wp-block-button__link{color:#fff;background-color:#32373c;border-radius:9999px;box-shadow:none;text-decoration:none;padding:calc(.667em + 2px) calc(1.333em + 2px);font-size:1.125em}.wp-block-file__button{background:#32373c;color:#fff;text-decoration:none}
body{--wp--preset--color--black: #000000;--wp--preset--color--cyan-bluish-gray: #abb8c3;--wp--preset--color--white: #ffffff;--wp--preset--color--pale-pink: #f78da7;--wp--preset--color--vivid-red: #cf2e2e;--wp--preset--color--luminous-vivid-orange: #ff6900;--wp--preset--color--luminous-vivid-amber: #fcb900;--wp--preset--color--light-green-cyan: #7bdcb5;--wp--preset--color--vivid-green-cyan: #00d084;--wp--preset--color--pale-cyan-blue: #8ed1fc;--wp--preset--color--vivid-cyan-blue: #0693e3;--wp--preset--color--vivid-purple: #9b51e0;--wp--preset--gradient--vivid-cyan-blue-to-vivid-purple: linear-gradient(135deg,rgba(6,147,227,1) 0%,rgb(155,81,224) 100%);--wp--preset--gradient--light-green-cyan-to-vivid-green-cyan: linear-gradient(135deg,rgb(122,220,180) 0%,rgb(0,208,130) 100%);--wp--preset--gradient--luminous-vivid-amber-to-luminous-vivid-orange: linear-gradient(135deg,rgba(252,185,0,1) 0%,rgba(255,105,0,1) 100%);--wp--preset--gradient--luminous-vivid-orange-to-vivid-red: linear-gradient(135deg,rgba(255,105,0,1) 0%,rgb(207,46,46) 100%);--wp--preset--gradient--very-light-gray-to-cyan-bluish-gray: linear-gradient(135deg,rgb(238,238,238) 0%,rgb(169,184,195) 100%);--wp--preset--gradient--cool-to-warm-spectrum: linear-gradient(135deg,rgb(74,234,220) 0%,rgb(151,120,209) 20%,rgb(207,42,186) 40%,rgb(238,44,130) 60%,rgb(251,105,98) 80%,rgb(254,248,76) 100%);--wp--preset--gradient--blush-light-purple: linear-gradient(135deg,rgb(255,206,236) 0%,rgb(152,150,240) 100%);--wp--preset--gradient--blush-bordeaux: linear-gradient(135deg,rgb(254,205,165) 0%,rgb(254,45,45) 50%,rgb(107,0,62) 100%);--wp--preset--gradient--luminous-dusk: linear-gradient(135deg,rgb(255,203,112) 0%,rgb(199,81,192) 50%,rgb(65,88,208) 100%);--wp--preset--gradient--pale-ocean: linear-gradient(135deg,rgb(255,245,203) 0%,rgb(182,227,212) 50%,rgb(51,167,181) 100%);--wp--preset--gradient--electric-grass: linear-gradient(135deg,rgb(202,248,128) 0%,rgb(113,206,126) 100%);--wp--preset--gradient--midnight: linear-gradient(135deg,rgb(2,3,129) 0%,rgb(40,116,252) 100%);--wp--preset--font-size--small: 13px;--wp--preset--font-size--medium: 20px;--wp--preset--font-size--large: 36px;--wp--preset--font-size--x-large: 42px;--wp--preset--spacing--20: 0.44rem;--wp--preset--spacing--30: 0.67rem;--wp--preset--spacing--40: 1rem;--wp--preset--spacing--50: 1.5rem;--wp--preset--spacing--60: 2.25rem;--wp--preset--spacing--70: 3.38rem;--wp--preset--spacing--80: 5.06rem;--wp--preset--shadow--natural: 6px 6px 9px rgba(0, 0, 0, 0.2);--wp--preset--shadow--deep: 12px 12px 50px rgba(0, 0, 0, 0.4);--wp--preset--shadow--sharp: 6px 6px 0px rgba(0, 0, 0, 0.2);--wp--preset--shadow--outlined: 6px 6px 0px -3px rgba(255, 255, 255, 1), 6px 6px rgba(0, 0, 0, 1);--wp--preset--shadow--crisp: 6px 6px 0px rgba(0, 0, 0, 1);}:where(.is-layout-flex){gap: 0.5em;}:where(.is-layout-grid){gap: 0.5em;}body .is-layout-flow > .alignleft{float: left;margin-inline-start: 0;margin-inline-end: 2em;}body .is-layout-flow > .alignright{float: right;margin-inline-start: 2em;margin-inline-end: 0;}body .is-layout-flow > .aligncenter{margin-left: auto !important;margin-right: auto !important;}body .is-layout-constrained > .alignleft{float: left;margin-inline-start: 0;margin-inline-end: 2em;}body .is-layout-constrained > .alignright{float: right;margin-inline-start: 2em;margin-inline-end: 0;}body .is-layout-constrained > .aligncenter{margin-left: auto !important;margin-right: auto !important;}body .is-layout-constrained > :where(:not(.alignleft):not(.alignright):not(.alignfull)){max-width: var(--wp--style--global--content-size);margin-left: auto !important;margin-right: auto !important;}body .is-layout-constrained > .alignwide{max-width: var(--wp--style--global--wide-size);}body .is-layout-flex{display: flex;}body .is-layout-flex{flex-wrap: wrap;align-items: center;}body .is-layout-flex > *{margin: 0;}body .is-layout-grid{display: grid;}body .is-layout-grid > *{margin: 0;}:where(.wp-block-columns.is-layout-flex){gap: 2em;}:where(.wp-block-columns.is-layout-grid){gap: 2em;}:where(.wp-block-post-template.is-layout-flex){gap: 1.25em;}:where(.wp-block-post-template.is-layout-grid){gap: 1.25em;}.has-black-color{color: var(--wp--preset--color--black) !important;}.has-cyan-bluish-gray-color{color: var(--wp--preset--color--cyan-bluish-gray) !important;}.has-white-color{color: var(--wp--preset--color--white) !important;}.has-pale-pink-color{color: var(--wp--preset--color--pale-pink) !important;}.has-vivid-red-color{color: var(--wp--preset--color--vivid-red) !important;}.has-luminous-vivid-orange-color{color: var(--wp--preset--color--luminous-vivid-orange) !important;}.has-luminous-vivid-amber-color{color: var(--wp--preset--color--luminous-vivid-amber) !important;}.has-light-green-cyan-color{color: var(--wp--preset--color--light-green-cyan) !important;}.has-vivid-green-cyan-color{color: var(--wp--preset--color--vivid-green-cyan) !important;}.has-pale-cyan-blue-color{color: var(--wp--preset--color--pale-cyan-blue) !important;}.has-vivid-cyan-blue-color{color: var(--wp--preset--color--vivid-cyan-blue) !important;}.has-vivid-purple-color{color: var(--wp--preset--color--vivid-purple) !important;}.has-black-background-color{background-color: var(--wp--preset--color--black) !important;}.has-cyan-bluish-gray-background-color{background-color: var(--wp--preset--color--cyan-bluish-gray) !important;}.has-white-background-color{background-color: var(--wp--preset--color--white) !important;}.has-pale-pink-background-color{background-color: var(--wp--preset--color--pale-pink) !important;}.has-vivid-red-background-color{background-color: var(--wp--preset--color--vivid-red) !important;}.has-luminous-vivid-orange-background-color{background-color: var(--wp--preset--color--luminous-vivid-orange) !important;}.has-luminous-vivid-amber-background-color{background-color: var(--wp--preset--color--luminous-vivid-amber) !important;}.has-light-green-cyan-background-color{background-color: var(--wp--preset--color--light-green-cyan) !important;}.has-vivid-green-cyan-background-color{background-color: var(--wp--preset--color--vivid-green-cyan) !important;}.has-pale-cyan-blue-background-color{background-color: var(--wp--preset--color--pale-cyan-blue) !important;}.has-vivid-cyan-blue-background-color{background-color: var(--wp--preset--color--vivid-cyan-blue) !important;}.has-vivid-purple-background-color{background-color: var(--wp--preset--color--vivid-purple) !important;}.has-black-border-color{border-color: var(--wp--preset--color--black) !important;}.has-cyan-bluish-gray-border-color{border-color: var(--wp--preset--color--cyan-bluish-gray) !important;}.has-white-border-color{border-color: var(--wp--preset--color--white) !important;}.has-pale-pink-border-color{border-color: var(--wp--preset--color--pale-pink) !important;}.has-vivid-red-border-color{border-color: var(--wp--preset--color--vivid-red) !important;}.has-luminous-vivid-orange-border-color{border-color: var(--wp--preset--color--luminous-vivid-orange) !important;}.has-luminous-vivid-amber-border-color{border-color: var(--wp--preset--color--luminous-vivid-amber) !important;}.has-light-green-cyan-border-color{border-color: var(--wp--preset--color--light-green-cyan) !important;}.has-vivid-green-cyan-border-color{border-color: var(--wp--preset--color--vivid-green-cyan) !important;}.has-pale-cyan-blue-border-color{border-color: var(--wp--preset--color--pale-cyan-blue) !important;}.has-vivid-cyan-blue-border-color{border-color: var(--wp--preset--color--vivid-cyan-blue) !important;}.has-vivid-purple-border-color{border-color: var(--wp--preset--color--vivid-purple) !important;}.has-vivid-cyan-blue-to-vivid-purple-gradient-background{background: var(--wp--preset--gradient--vivid-cyan-blue-to-vivid-purple) !important;}.has-light-green-cyan-to-vivid-green-cyan-gradient-background{background: var(--wp--preset--gradient--light-green-cyan-to-vivid-green-cyan) !important;}.has-luminous-vivid-amber-to-luminous-vivid-orange-gradient-background{background: var(--wp--preset--gradient--luminous-vivid-amber-to-luminous-vivid-orange) !important;}.has-luminous-vivid-orange-to-vivid-red-gradient-background{background: var(--wp--preset--gradient--luminous-vivid-orange-to-vivid-red) !important;}.has-very-light-gray-to-cyan-bluish-gray-gradient-background{background: var(--wp--preset--gradient--very-light-gray-to-cyan-bluish-gray) !important;}.has-cool-to-warm-spectrum-gradient-background{background: var(--wp--preset--gradient--cool-to-warm-spectrum) !important;}.has-blush-light-purple-gradient-background{background: var(--wp--preset--gradient--blush-light-purple) !important;}.has-blush-bordeaux-gradient-background{background: var(--wp--preset--gradient--blush-bordeaux) !important;}.has-luminous-dusk-gradient-background{background: var(--wp--preset--gradient--luminous-dusk) !important;}.has-pale-ocean-gradient-background{background: var(--wp--preset--gradient--pale-ocean) !important;}.has-electric-grass-gradient-background{background: var(--wp--preset--gradient--electric-grass) !important;}.has-midnight-gradient-background{background: var(--wp--preset--gradient--midnight) !important;}.has-small-font-size{font-size: var(--wp--preset--font-size--small) !important;}.has-medium-font-size{font-size: var(--wp--preset--font-size--medium) !important;}.has-large-font-size{font-size: var(--wp--preset--font-size--large) !important;}.has-x-large-font-size{font-size: var(--wp--preset--font-size--x-large) !important;}
.wp-block-navigation a:where(:not(.wp-element-button)){color: inherit;}
:where(.wp-block-post-template.is-layout-flex){gap: 1.25em;}:where(.wp-block-post-template.is-layout-grid){gap: 1.25em;}
:where(.wp-block-columns.is-layout-flex){gap: 2em;}:where(.wp-block-columns.is-layout-grid){gap: 2em;}
.wp-block-pullquote{font-size: 1.5em;line-height: 1.6;}
.recentcomments a{display:inline
```

!important;padding:0 !important;margin:0 !important;} jQuery(document).ready(function() { jQuery("#dropmenu ul").css({display: "none"}); // Opera Fix jQuery("#dropmenu li").hover(function(){ jQuery(this).find('ul:first').css({visibility: "visible",display: "none"}).show(268); }, function(){ jQuery(this).find('ul:first').css({visibility: "hidden"}); }); });

同时也是一个手工杀毒辅助软件。

2023年08月12日发布V1.6版本。

免费版本下载地址：本地下载(md5:0825CA3F3667D6F62F0300B39DFF1C05) 其中PCHunter32.exe是32位版本，PCHunter64.exe是64位版本。

本工具目前初步实现如下功能：

1.进程、线程、进程模块、进程窗口、进程内存信息查看，杀进程、杀线程、卸载模块等功能 2.内核驱动模块查看，支持内核驱动模块的内存拷贝 3.SSDT、Shadow SSDT、FSD、KBD、TCPIP、Classpnp、Atapi、Acpi、SCSI、IDT、GDT信息查看，并能检测和恢复ssdt hook和inline hook 4.CreateProcess、CreateThread、LoadImage、CmpCallback、BugCheckCallback、Shutdown、Lego等Notify Routine信息查看，并支持对这些Notify Routine的删除 5.端口信息查看，目前不支持2000系统 6.查看消息钩子 7.内核模块的iat、eat、inline hook、patches检测和恢复 8.磁盘、卷、键盘、网络层等过滤驱动检测，并支持删除 9.注册表编辑 10.进程iat、eat、inline hook、patches检测和恢复 11.文件系统查看，支持基本的文件操作 12.查看（编辑）IE插件、SPI、启动项、服务、Host文件、映像劫持、文件关联、系统防火墙规则、IME 13.ObjectType Hook检测和恢复 14.DPC定时器检测和删除 15.MBR Rootkit检测和修复 16.内核对象劫持检测 17.WorkerThread枚举 18.Ndis中一些回调信息枚举 19.硬件调试寄存器、调试相关API检测 20.枚举SFilter/Fltmgr的回调 21.系统用户名检测

免责声明：这只是一个免费的辅助软件，如果您使用本软件，给您直接或者间接造成损失、损害，本公司概不负责。从您使用本软件的一刻起，将视为您已经接受了本免责声明。

Posted on 2月 1, 2013 at 10:45 by admin · Permalink · 498 Comments In: 原创工具 PCHunter[2013-11-25]命令行版本 这是一个简易的PCHunter命令行版本程序，目前只提供了检测功能，未提供任何可能到系统造成修改的功能，如果您是PCHunter专业版用户，可以把专业版Key放入命令行版目录下，即可使用专业版特有的一些检测功能。本程序使用期限一年(2013.11.25~2014.11.24)，过期后会无法加载驱动。下载点我(md5:640C74AA397F3E76766AC04CDAA8A9AE)

本软件加了VMProtect壳，可能有些杀毒软件会报毒……请大家放心使用，这属于杀毒软件误报。

本软件免费，但未获得作者书面授权，禁止用于商业用途；另外禁止本软件用于恶意用途（比如作为病毒木马的一部分、破解网吧收费系统等）。

如果您使用本软件，给您直接或者间接造成损失、损害，本公司概不负责。从您使用本软件的一刻起，将视为您已经接受了本免责声明。

Posted on 10月 5, 2010 at 01:41 by admin · Permalink · 13 Comments In: 原创工具 虚拟机脱壳SDK 3年前写的一个虚拟机脱壳SDK，跟linxerUnpack v0.12配套的，有需要的可以下载看看，能脱几十种简单的壳吧。下载点我(md5:F39AA981E67FB9C6AF87CAF51349CF1C)

使用前，请仔细阅读SDK包里的“说明.txt”文件，免得给你给我带来不必要的麻烦。

Posted on 6月 3, 2010 at 14:33 by admin · Permalink · One Comment In: 未分类 [2012.10.25]发布一个XueTr-火眼合作版本,详情以后在http://t.qq.com/linxer发布,欢迎收听 一个强大的手工杀毒工具，目前暂时只支持32位的2000、xp、2003、vista、2008和Win7操作系统，等忙完这阵，会购买微软的数字签名以开发支持64位和Windows8的XueTr，请大家拭目以待。 下载点我(md5:D4B3E3A5B1FEE871A610422220C0506A)

作者QQ微博：http://t.qq.com/linxer 欢迎收听，以后XueTr情况会在这里发布。

从0.44版本开始，XT中加入了捐赠信息，在此对捐赠者表示感谢。查看捐赠名单。

本工具目前实现如下功能： 1.进程、线程、进程模块、进程窗口、进程内存、定时器、热键信息查看，杀进程、杀线程、卸载模块等功能 2.内核驱动模块查看，支持内核驱动模块的内存拷贝 3.SSDT、Shadow SSDT、FSD、KBD、TCPIP、Classpnp、Atapi、Acpi、SCSI、IDT、GDT信息查看，并能检测和恢复ssdt hook和inline hook 4.CreateProcess、CreateThread、LoadImage、CmpCallback、BugCheckCallback、Shutdown、Lego等Notify Routine信息查看，并支持对这些Notify Routine的删除 5.端口信息查看，目前不支持2000系统 6.查看消息钩子 7.内核模块的iat、eat、inline hook、patches检测和恢复 8.磁盘、卷、键盘、网络层等过滤驱动检测，并支持删除 9.注册表编辑 10.进程iat、eat、inline hook、patches检测和恢复 11.文件系统查看，支持基本的文件操作 12.查看（编辑）IE插件、SPI、启动项、服务、Host文件、映像劫持、文件关联、系统防火墙规则、IME 13.ObjectType Hook检测和恢复 14.DPC定时器检测和删除 15.MBR Rootkit检测和修复 16.内核对象劫持检测 17.WorkerThread枚举

免责声明：这只是一个免费的辅助小工具，如果您使用本工具，给您直接或者间接造成损失、损害，本人概不负责。从您使用本小工具的一刻起，将视为您已经接受了本免责声明。

Posted on 12月 10, 2008 at 01:37 by admin · Permalink · 893 Comments In: 原创工具 通用基于虚拟机的脱壳机—linxerUnpacker 很早的一个东西了，参加工作一年的样子，花了3个月的业余时间写的，当时好像这类东西比较火，自己也跟风深入研究了一下，有需要的朋友可以从这里下载，这个版本是当初放在看雪论坛的版本，以后也一直没更新过了。下载点我

Posted on 11月 19, 2008 at 11:43 by admin · Permalink · 6 Comments In: 原创工具 链接 anxinsec.com 安芯网盾 kermit mtian 近期评论Jesse发表在《PCHunter[2013-11-25]命令行版本》anonymous发表在《[2012.10.25]发布一个XueTr-火眼合作版本,详情以后在http://t.qq.com/linxer发布,欢迎收听》匿名发表在《PCHunter V1.6发布无签名版，支持Win11(22621)》匿名发表在《PCHunter V1.6发布无签名版，支持Win11(22621)》匿名发表在《PCHunter[2013-11-25]命令行版本》 近期文章 PCHunter V1.6发布无签名版，支持Win11(22621) PCHunter[2013-11-25]命令行版本 虚拟机脱壳SDK [2012.10.25]发布一个XueTr-火眼合作版本,详情以后在http://t.qq.com/linxer发布,欢迎收听 通用基于虚拟机的