



- 门户
- 首页
- 论坛
- 资讯
- 安全
- 软件
- 硬件
- 休闲
- 搜索
- 帖子
- 伯乐榜
- 勋章
- 帮助

论坛 > 安全区 > 病毒样本 分享&分析区 > 银狐/FakeApp/CW等国产样本 样本测试 9X

发帖

返回列表 1 2 3 2 / 3页 下一页

楼主: wwwab

[病毒样本] 银狐/FakeApp/CW等国产样本 样本测试 9X [复制链接]

wowocock

发表于 2025-12-30 13:45:29

11楼



[https://www.virustotal.com/gui/f ... 381cbfb7ee0568e7a8b](https://www.virustotal.com/gui/f...381cbfb7ee0568e7a8b) ,  
 目前都没入库, 不知道木马作者怎么找到的。  
 银狐换了个新的漏洞驱动来杀杀软。可能来自于这里  
[https://help.eset.com/protect\\_cl ... etica\\_software.html](https://help.eset.com/protect_cl...etica_software.html)

case 0xB822200C:

```

v10 = *(_DWORD *)(IrpSp + 16) < 8u;
ProcessHandle = 0i64;
if ( !v10 )
{
  ClientId.UniqueProcess = *(HANDLE **)(Irp + 24);
  ClientId.UniqueThread = 0i64;
  ObjectAttributes.Length = 48;
  memset(&ObjectAttributes.RootDirectory, 0, 20);
  *(_OWORD *)&ObjectAttributes.SecurityDescriptor = 0i64;
  v7 = ZwOpenProcess(&ProcessHandle, 0x1FFFFFFu, &ObjectAttributes, &ClientId);
  if ( v7 >= 0 )
  {
    v7 = ZwTerminateProcess(ProcessHandle, 0);
    ZwClose(ProcessHandle);
  }
  break;
}

```

回复

举报

wowocock

发表于 2025-12-30 13:54:32

12楼



中毒后用火绒恶意木马专杀查杀即可。

**本帖子中包含更多资源**  
 您需要 登录 才可以下载或查看, 没有帐号? 快速注册 [用QQ帐号登录](#)

回复

举报

LeeHS


发表于 2025-12-30 14:05:34

13楼



cortex 解压杀剩下4个, 剩下双击杀

**本帖子中包含更多资源**



您需要 [登录](#) 才可以下载或查看，没有帐号？[快速注册](#)  [用QQ帐号登录](#)

 回复  举报

post88 发表于 2025-12-30 16:07:46 | 14楼

本帖最后由 post88 于 2025-12-30 16:10 编辑

AVAST 扫描8X 剩下一个双击杀衍生物DLL

 **本帖子中包含更多资源**  
 您需要 [登录](#) 才可以下载或查看，没有帐号？[快速注册](#)  [用QQ帐号登录](#)

 回复  举报

hansyu 发表于 2025-12-30 16:28:13 | 15楼

McAfee 扫描清空

 回复  举报

LingGao 发表于 2025-12-30 19:29:58 | 16楼

“ [LingGao 发表于 2025-12-30 10:54](#)  
 Microsoft Defender  
 Specification9.exe - Trojan:MSIL/PureLogStealer.ZYI!MTB ”

ams.865301004.exe - **Trojan:Win32/Malgent!MSR**  
 款式-尺码.exe - **Trojan:Win32/Malgent!MSR**  
 yinhu.exe - **不符合 Microsoft 对恶意软件的判定标准**


力竭了

**评分**

参与人数 **1** 人气 **+3** 理由 [收起](#) ▲

 Loyisa **+3** 版区有你更精彩：)

[查看全部评分](#)

 回复  举报

bbszy 发表于 2025-12-30 19:34:01 | 17楼

“ [hansyu 发表于 2025-12-30 16:28](#)  
 McAfee 扫描清空 ”

咖啡拉黑还是算快

回复

举报

hansyu

发表于 2025-12-30 22:14:25 |

18楼



“ bbszy 发表于 2025-12-30 19:34 咖啡拉黑还是算快 ”

这也算是咖啡在国内还算能用的理由。

回复

举报

inhh1

发表于 2025-12-30 22:52:45 |

19楼



sesc扫描余2 执行杀衍生=kill all

**本帖子中包含更多资源**

您需要 [登录](#) 才可以下载或查看, 没有帐号? [快速注册](#) [用QQ帐号登录](#)

回复

举报

Renascence

发表于 2025-12-31 08:58:31 |

20楼



SESC清空

回复

举报

下一页 »

发帖

返回列表 1 2 3 2 / 3页 下一页

B A [icons] 高级模式

您需要登录后才可以回帖 登录 | 快速注册 [用QQ帐号登录](#)

发表回复  回帖后跳转到最后一页

本版积分规则

手机版 | 杀毒软件 | 软件论坛 | 卡饭论坛

Copyright © KaFan KaFan.cn All Rights Reserved.

Powered by Discuz! X3.4 (沪ICP备2020031077号-2) GMT+8, 2026-4-17 22:22, Processed in 0.088490 second(s), 3 queries, Redis On.

卡饭网所发布的一切软件、样本、工具、文章等仅限于学习和研究, 不得将上述内容用于商业或者其他非法用途, 否则产生的一切后果自负, 本站信息来自网络, 版权争议问题与本站无关, 您必须在下载后的24小时之内从您的电脑中彻底删除上述信息, 如有问题请通过邮件与我们联系。

