



- 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 1 / 3 页 下一页

查看: 3462 | 回复: 21 [病毒样本] 银狐/FakeApp/CW等国产样本 样本测试 9X [复制链接]

wwwab

发表于 2025-12-30 00:18:07 | 1楼 电梯直达



3 download links:
 下载1: <https://pan.huang1111.cn/s/zMmzGUM>
 下载2: <https://qfile.qq.com/q/A5P3mE3k0a> (14days)
 下载3: <https://c.wss.ink/f/itkzvctg085> (24h)

解压密码 infected
 压缩包 SHA-256: 41b2b36d264d154bd27bf82cdf3ed1f70cc4a29cefd74edea430682ec0164b0d

收藏 淘帖

回复 举报

心醉咖啡

发表于 2025-12-30 00:21:23 | 2楼



360

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

Myrenaser

发表于 2025-12-30 01:05:25 | 3楼




比特焚德清除36udhea_x64.2.1.exe、Installlke.exe、wpfhsrfhsrsej.exe衍生物的.dll, 仅有弹窗但无记录。

其余均触发ATD

样式.exe扫描报毒

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](#)

superLYT




回复

举报

发表于 2025-12-30 01:09:59 |

4楼


ams.865301004双击kill大量释放文件，Installlke双击kill潜在和释放文件，yinhuh双击kill释放的文件，有意思的是，双击后的报毒名基本重复，而且出现了罕见的ML机学和rootkit

 **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

xjwzq




发表于 2025-12-30 09:08:47 |

5楼

本帖最后由 xjwzq 于 2025-12-30 09:10 编辑


奇安信扫描5，改名后拦截3，余下一个Specification9因被ESET拦截不得知

 **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

小蚂蚁



发表于 2025-12-30 09:12:30 |

6楼

本帖最后由 小蚂蚁 于 2025-12-30 09:42 编辑

kes扫描删8个，360zip.exe miss

 **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](#)

评分

参与人数 1	人气 +3	理由	收起 ▲
---------------	--------------	----	----------------------

 dongwenqi	+3	版区有你更精彩：)
---	-----------	-----------

[查看全部评分](#)

回复

举报

微微的笑



发表于 2025-12-30 09:22:04 |

7楼

扫描kill6x，双击kill2x，剩余一个wps报错


 **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](#)

dd2006

 发表于 2025-12-30 09:41:03 |

8楼



红伞 杀6个
华为 杀2个
瑞星 杀4个
sep 杀5个



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](#)

猥琐大叔

 发表于 2025-12-30 10:52:10 |

9楼



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](#)

LingGao

 发表于 2025-12-30 10:54:38 |

10楼



Microsoft Defender

Specification9.exe - **Trojan:MSIL/PureLogStealer.ZY!MTB**
2025年第二季度违规内职人员名单信息公示.exe - **Trojan:Win32/Wacatac.F!ml**
InstalIike.exe - **Trojan:Win32/Wacatac.F!ml**
360zip.exe - **Trojan:Win32/Wacatac.C!ml**
36udhea_x64.2.1.exe - **Trojan:Win32/Etset!rfn**
wpfhsrfhsrjsej.exe - **Trojan:Win32/Wacatac.F!ml**

ams.865301004.exe - **MISS**
款式-尺码.exe - **MISS**

yinhu.exe - **MISS**

正在排队分析。

○ 评分

参与人数 **1** 人气 **+2** 理由

收起 ▲

 scottxzt + 2

[查看全部评分](#)

 回复


[举报](#)

下一页 »

发帖

◀ 返回列表 **1** 2 3 1 / 3 页 下一页 ▶

B  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 23:52, Processed in 0.068209 second(s), 2 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。