

# 百科内容引用说明文档

V0.92

百科研发小组

变更日期	变更内容
2024/01/09	补充第 3 章，引用路径设计规范、引用案例：中英文链接地址
2024/02/23	调整接口引用规范章节，简化引用方式。将拼接路径的工作从客户侧变更为由百科集中提供服务。

# 1 系统概述

计算机病毒百科系统，是一款面向公众开放的知识查询平台。通过集中维护并输出结构化、规范化的安全领域知识信息，加强公众对威胁知识的认知理解，提高公众计算机安全的意识；同时能够形成面向恶意代码技术研究的学术资源体系，促进知识分享、推动安全技术的创新与发展，以应对未来不断演化和复杂化的计算机病毒威胁。

目前我们已收录 5 万余条病毒家族词条，病毒家族词条（在已知病毒家族范围）覆盖率在 99% 以上。约 10000 余条信息安全相关词汇，词条的补充以及内容生产，90% 以上实现由赛博超脑自动化处理完成。同时我们面向广大用户采取众筹运营机制，形成取之于公众，服务于公众的运营闭环。

# 2 服务地址

<https://www.virusview.net/>

# 3 病毒名规范

## 安天历史命名规范结构

安天旧病毒名规范，恶意代码采用四段式命名：<分类名称[核心行为]>/<环境前缀>.<家族名称>.<变种号>。

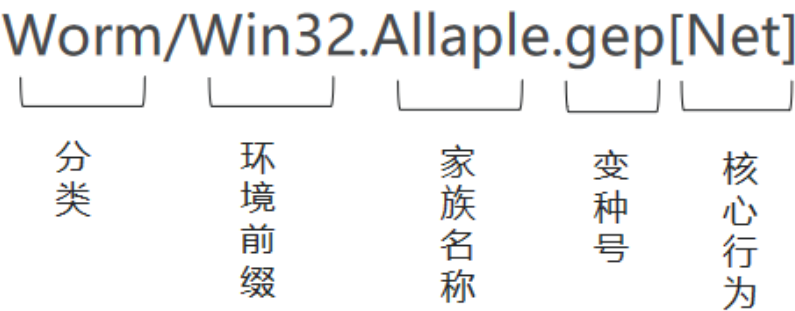


分类名称与后面的描述信息以/符号分隔，其余各段以.符号分隔

- 1) 分类名称：用于区分病毒的种族分类，不同种类的病毒，其病毒前缀应有对应的划分，如木马的前缀为 Trojan、感染式的前缀为 Virus 等。
- 2) 核心行为：恶意代码核心行为是定义恶意代码传播手段、攻击方式、攻击对象等恶意行为的描述信息，对于行为在恶意代码名称的描述中，应描述其核心的行为。
- 3) 环境前缀：是指恶意代码运行环境，包括恶意代码运行所依赖的操作系统、脚本环境、宿主格式等信息。
- 4) 家族名称：用于区别不同恶意代码同源性的的重要依据，通过家族的定义可划分出恶意代码隶属于哪个种群。
- 5) 变种号：用于区别隶属于同一家族但不同版本的恶意代码。

## 病毒百科及安天新病毒名命名规范

根据 2023/09/18《关于恶意代码分类命名规范的强制应用要求》，“新版的命名结构严格遵循了我司八大分类命名框架，并在恶意代码输出命名节的排序上有所调整：原本位于分类前缀和环境前缀之间的“核心行为标签”统一后置到整个命名之后。”病毒百科已按照新标准设置病毒名结构如下：



## 4 路径设计规范

目录路径设计体现百科网站的层次结构，方便用户产品可以直接引用，让搜索引擎可以收录增加网站的传播效率。百科的目录路径除去服务地址、词条类型，其剩余部分顺序完全依据安天新病毒名命名规则，我们将病毒名中的 “/”和“[]”符号全部转换为“/”。同时在行为后追加补充后缀参数字段。

目录路径范式如下：

<https://hostname/entry type/threat type/platform/family/behavior?source=XXX>

表 1 目录范式释义

域值	域名称	含义	示例
hostname	服务地址	标识网站的地址	<a href="http://www.virusview.net">www.virusview.net</a>
entry_type	词条类型	标识词条的分类	malware:病毒名称词条 百科暂时仅提供这一种类型服务
threat type	病毒名类型	标识词条病毒名分类	Trojan
platform	运行平台	病毒运行平台	Win32
family	家族名	病毒家族	DownloaderGuide
behavior	行为信息	病毒核心行为	Downloader
?source=XXX	后缀参数	服务的参数	?source=IEP-A。标识请求者来自 IEP 的 A 模块。通过英文-向下分级。百科系统会将其用于统计计量数据。
&language=en	后缀补充参数（可缺省，缺省时默认 cn）	切换引用百科的英文： &language=en， 或中文版本： &language=cn，	?source=IEP-A&language=cn. 表示 IEP-A 请求的中文百科内容。  ?source=IEP-A&language=en. 表示 IEP-A 请求的英文百科内容。

## 5 接口引用规范

### 接口说明

用户调用该接口提供给我们病毒名，由百科生成引用链接路径，并输出结果页面。输入参数包括：病毒名，语种 CN/EN，请求来源。返回：拆解后的链接。包括：病毒结构，来源，中文/英文版。

### 接口地址

<https://www.virusview.net/base/v1/api/organization/sourceBox>

# HTTP 方法

GET

## 输入参数

参数	类型	是否必须	示例
name	string	是	如 Trojan/Win32.RecordBreaker[Spy] : 同时支持卡巴命名、微软命名、ESET-NOD32 命名, 以及安天旧命名, 持续增加类型。
Source	string	是	如: CERT-boyin
Language	string	否 (默认 CN)	如: cn (中文)、en (英文)

## 引用示例 (路径不区分大小写)

新标准命名查询示例:  
[https://www.virusview.net/base/v1/api/organization/sourceBox?name=Trojan/Win32.RecordBreaker\[Spy\]&language=cn&source= CERT](https://www.virusview.net/base/v1/api/organization/sourceBox?name=Trojan/Win32.RecordBreaker[Spy]&language=cn&source= CERT)

卡巴命名查询示例:  
<https://www.virusview.net/base/v1/api/organization/sourceBox?name=Trojan/Spy.Win32.Zbot.gen&language=cn&source= CERT>

微软命名查询示例:  
<https://www.virusview.net/base/v1/api/organization/sourceBox?name=PWS:Win32/Zbot&language=cn&source= CERT>

ESET-NOD32 命名查询示例:  
<https://www.virusview.net/base/v1/api/organization/sourceBox?name=Win32/Spy.Zbot.JF&language=cn&source= CERT>

旧标准命名查询示例  
[https://www.virusview.net/base/v1/api/organization/sourceBox?name=Trojan\[Backdoor\]/PHP.Li mmet&language=cn&source= CERT](https://www.virusview.net/base/v1/api/organization/sourceBox?name=Trojan[Backdoor]/PHP.Li mmet&language=cn&source= CERT)

输出格式：

查询有结果

返回百科详情页面，如下

首页 > 分类索引 > 列表 > Trojan/PHP.Limmet[Backdoor]

Trojan/PHP.Limmet[Backdoor]

安全AVL威胁检测引擎可查杀

Trojan/PHP.Limmet[Backdoor]的首个样本在2013年03月被安天捕获。它属于特洛伊木马，是一类以严重侵害运行系统的可用性、完整性、保密性为目的，或运行后能达到同类效果的恶意代码。该特洛伊木马关联样本主要运行或者载体为PHP。它的主要行为是以隐藏、欺骗的方式打开安全漏洞或绕过身份验证机制，从而给攻击者提供对受感染计算机的远程访问权限。后门行为通常由黑客或恶意软件开发利用，用于悄悄地远程控制受害者的计算机，执行未经授权的操作或者窃取敏感信息。目前Trojan/PHP.Limmet[Backdoor]存在文本、脚本文件等3种模式的样本，文本占绝大部分。除安天外，基于样本的命名对比分析，当前共有1个安全厂商对其进行命名，安全厂商对其行为分析较为清晰，检测的方式基本一致，对该特洛伊木马形成相同命名。

目录

收起

1 病毒行为

2 样本格式分布

3 其他厂商命名


4 典型变种

5 典型样本

6 解决方案

7 关联报告

Trojan/PHP.Limmet[Backdoor]



安天MP网安文化工作室

威胁类型Trojan

运行环境PHP

病毒家族Limmec

威胁行为Backdoor

变种数量1

样本数量80

首次发现时间2013-03-25

病毒行为

本节内容由安天情报引擎自动化生成

屏蔽安全软件：Trojan/PHP.Limmet[Backdoor]可尝试关闭或终止安全软件进程，以防止被安全软件检测和清除。

持续控制：一旦植入目标服务器，可持续远程控制受感染服务器，监视用户活动、窃取敏感数据。

网络传播：Trojan/PHP.Limmet[Backdoor]可以通过Web漏洞、钓鱼邮件等方式扩散，并在多台服务器之间建立连接，形成僵尸网络。

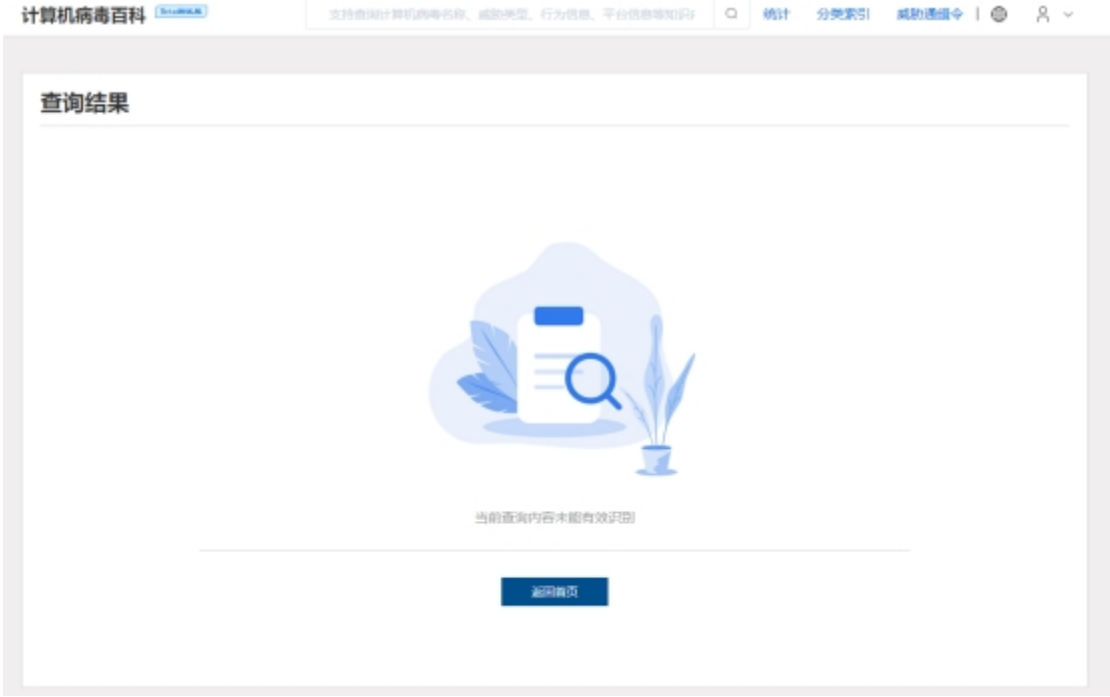
文件篡改：它可能篡改服务器文件系统，植入恶意代码，妨碍网页访问，导致用户信息泄露和网站瘫痪。

密码窃取：Trojan/PHP.Limmet[Backdoor]可通过键盘记录来窃取用户在受感染服务器上的密码和敏感信息。

防御干扰：它可识别并对抗杀毒、防火墙等安全软件，保持其对服务器的持续控制。

查询无结果

返回无结果页面，如下



## 参数错误

返回如下

```
1 {
2   "code": "A0001",
3   "data": "https://virusview.net/malware/Trojan/PHP/Limmet/Backdoor?language=cn&source=",
4   "msg": "参数不正确"
5 }
```

## 附表 1，各业务系统追加后缀名参考建议

备注：后缀名用于百科计量数据量。后缀名不区分大小写，\*\*表示按具体子系统缩写定义内容。如有自定义来源后缀，请企微联系曹琼、杨超补充，以做到及时计量。

业务系统	子系统（模块）	建议后缀名称
安天官网	AVL 反病毒引擎升级通知	?source= antiy-avl
PTD 探海	**	?source= ptd-**
IEP 智甲	**	?source= iep-**
CERT 报告	部门缩写+报告名称的英文或拼音	?source=CERT-boyin