火绒安全
HUORONG SECURITY

火绒终端安全管理系统
安全分析报告

报告生成时间 : 2024.01.15 11:38
报告统计周期 : 2024.01.09 - 2024.01.15

目录

一、全网安全总览 3
二、风险详情分析 5
2.1 病毒风险分析 5
2.2 网络风险分析 6
2.3 系统风险分析 7
2.4 高风险终端分析 8
三、典型风险分析及处理建议 13
Virus(感染型) 13
Worm(蠕虫) 14
Exploit(漏洞利用) 14
Rootkit(内核驱动) 15
Backdoor(后门) 15
TrojanSpy(间谍木马) 16
TrojanDownloader(木马下载) 16
TrojanDropper(木马释放) 17
VirTool(代码混淆器) 17
Trojan(一般木马) 18
Adware(广告) 18
四、附录 19
4.1 常见病毒介绍 19
4.2 风险等级介绍 20
4.3 安全建议 20

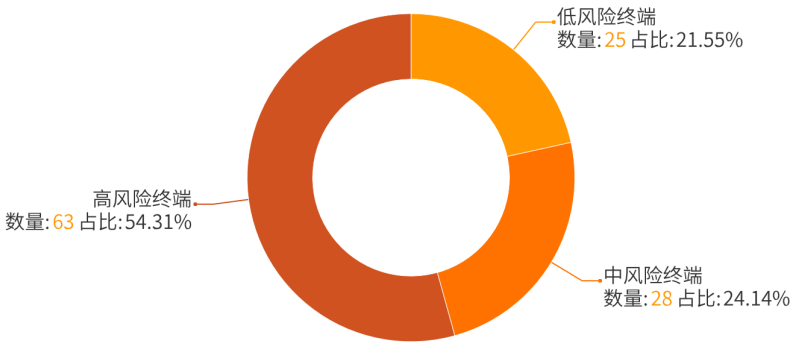
一、全网安全总览

统计周期 2024.01.09 - 2024.01.15

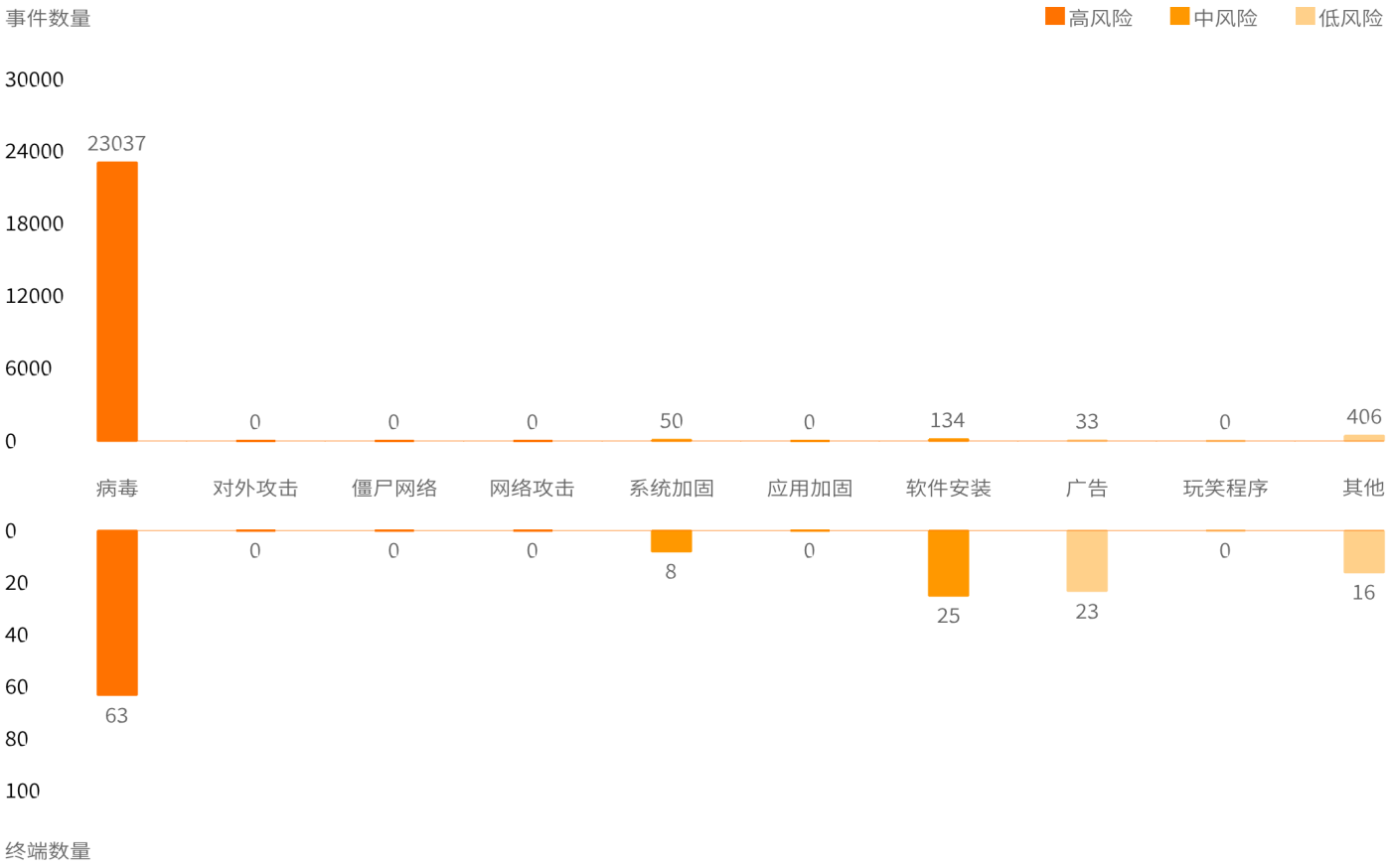
全网累计防护终端	1035 台

风险终端累计	116 台

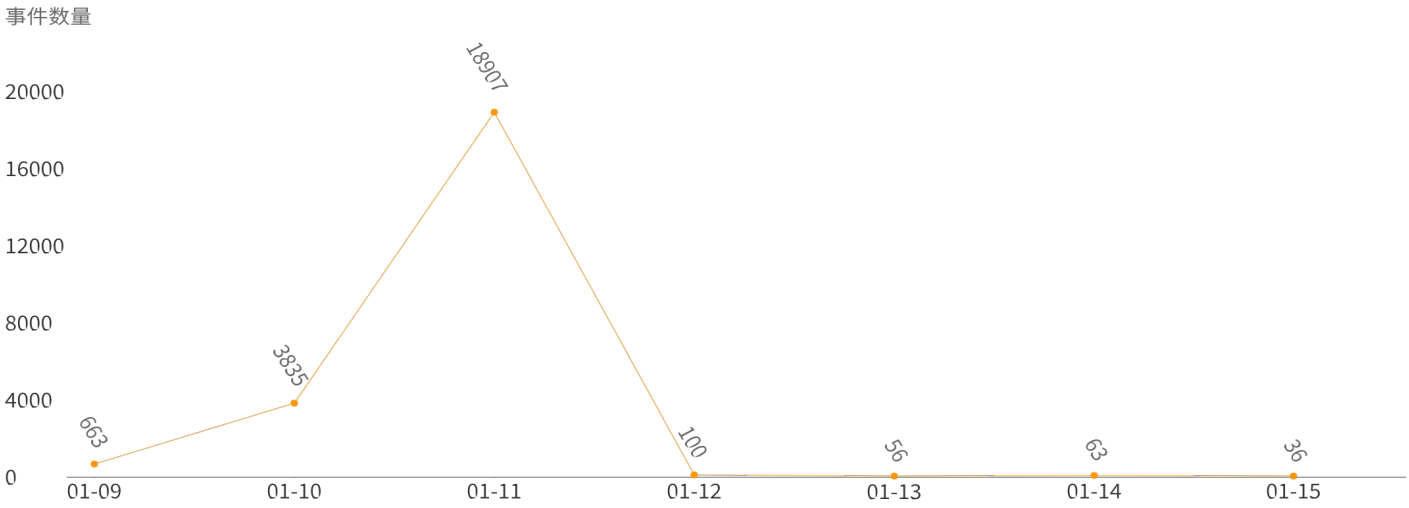
高风险终端	中风险终端	低风险终端
63 台	28 台	25 台



统计周期内检出风险事件主要分布于病毒、系统加固、软件安装、广告等风险事件类型，累计风险事件 23660 例：高风险事件 23037 例，中风险事件 184 例，低风险事件 439 例；下方对各类型风险对应的风险事件数量和涉及终端数量进行统计



统计周期内，风险事件变化趋势统计见下图：

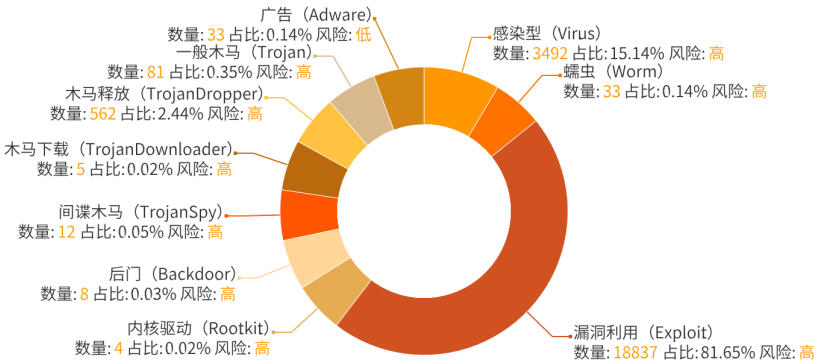


二、风险详情分析

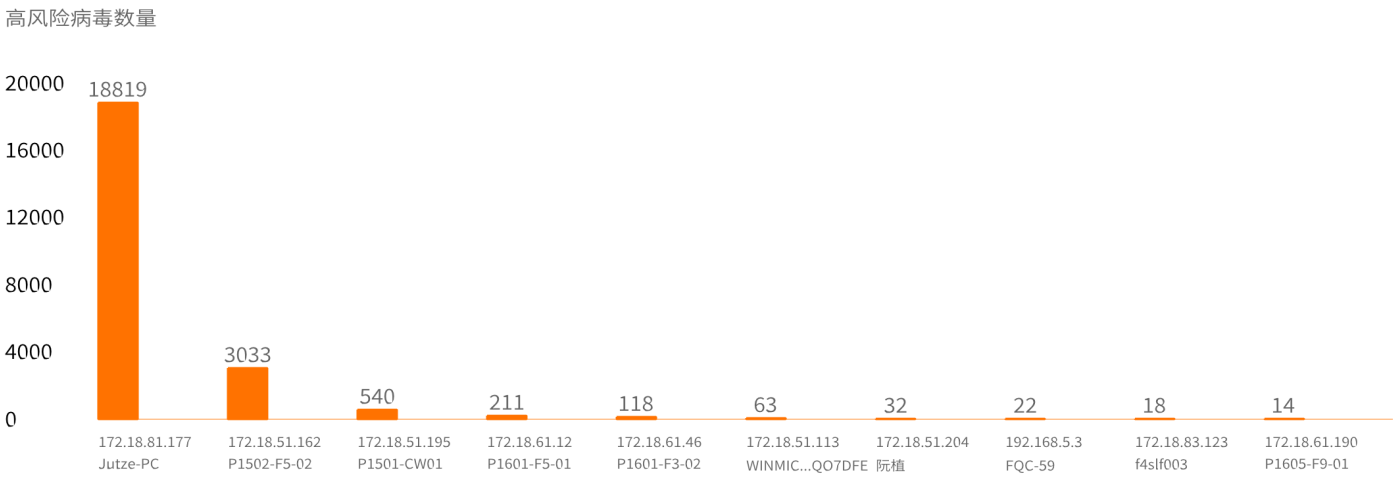
统计周期内全网病毒风险事件累计处理	系统风险事件累计处理
23070 例	184 例
网络风险事件累计处理	**受影响终端**
406 例	116 台

2.1 病毒风险分析

统计周期内全网累计处理病毒 23070 例，病毒类型分别是：感染型(Virus)、蠕虫(Worm)、漏洞利用(Exploit)、内核驱动(Rootkit)、后门(Backdoor)、间谍木马(TrojanSpy)、木马下载(TrojanDownloader)、木马释放(TrojanDropper)、代码混淆器(VirTool)、一般木马(Trojan)、广告(Adware)。下方统计了病毒类型TOP10数据：

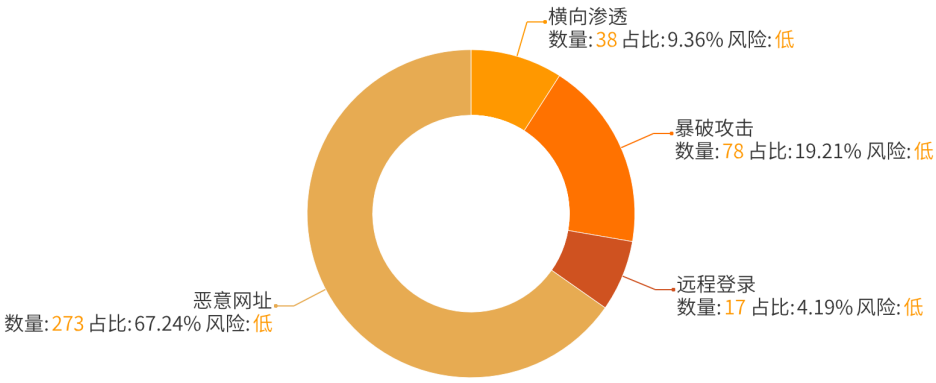


统计周期内受高风险病毒影响终端累计 63 台，下方统计了检出高风险病毒最多的终端TOP10数据：

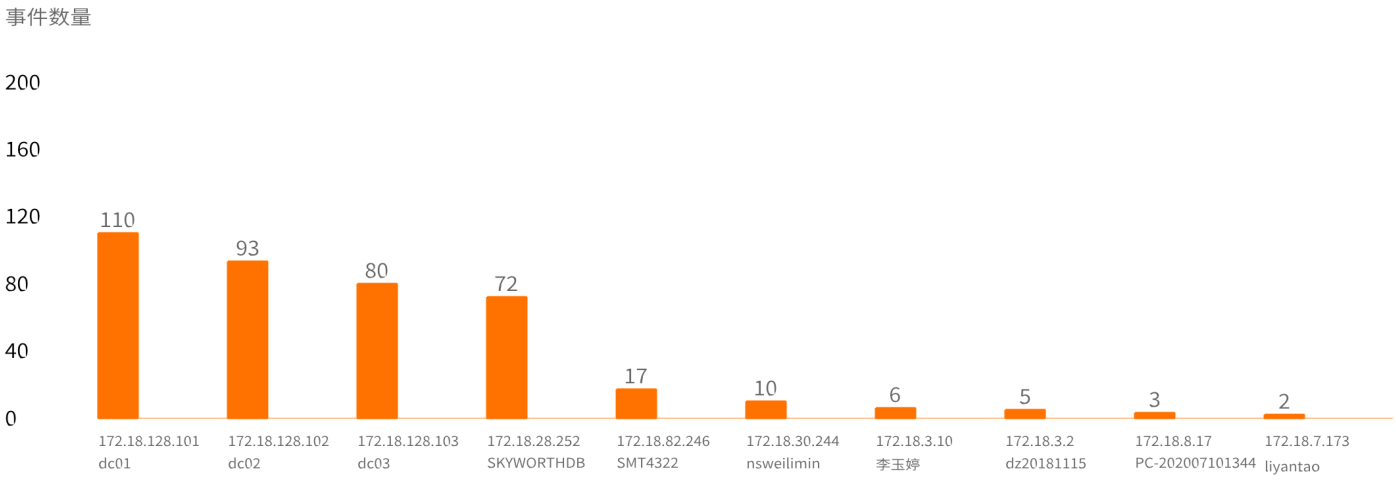


2.2 网络风险分析

统计周期内全网累计处理网络风险事件 406 例，风险类型分别是：横向渗透、暴破攻击、远程登录、恶意网址

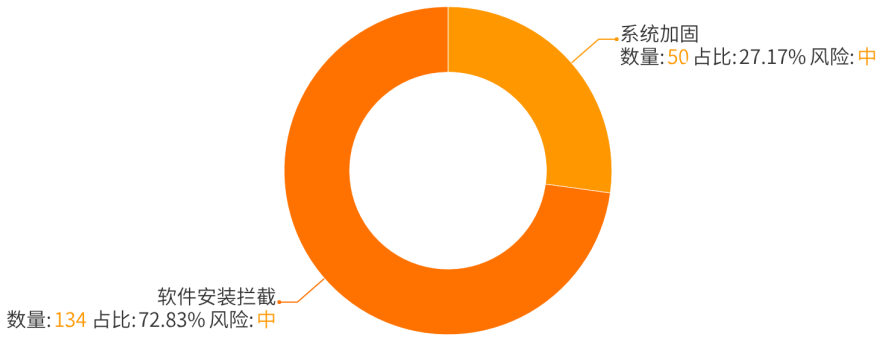


统计周期内受网络风险影响终端累计 16 台，下方统计出受网络风险事件影响最多的终端TOP10数据：

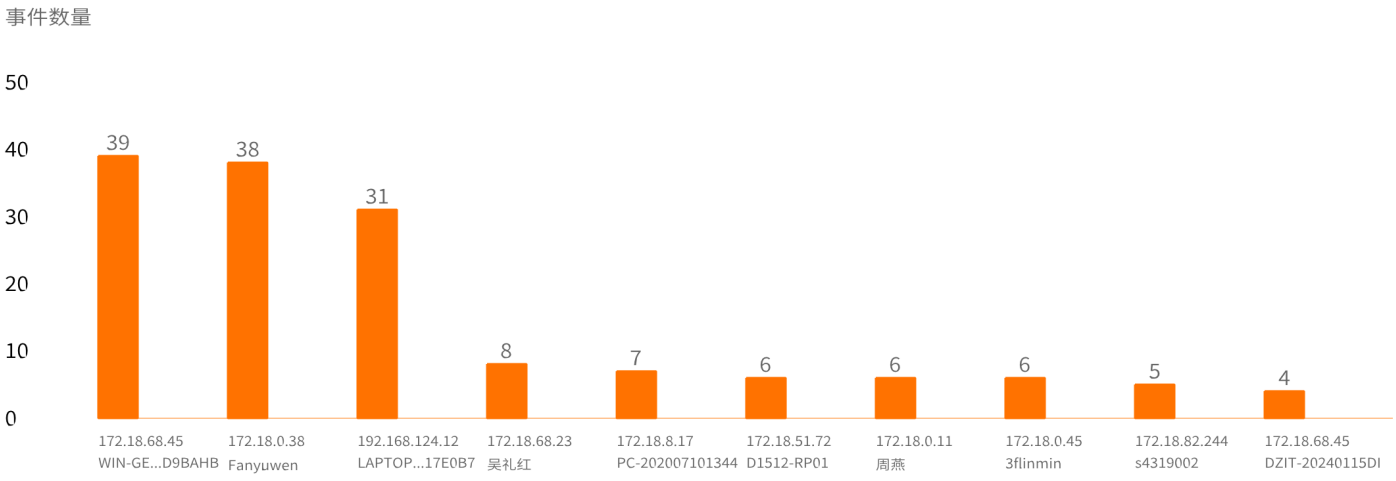


2.3 系统风险分析

统计周期内全网累计处理系统风险事件 184 例，风险类型分别是：系统加固、软件安装拦截



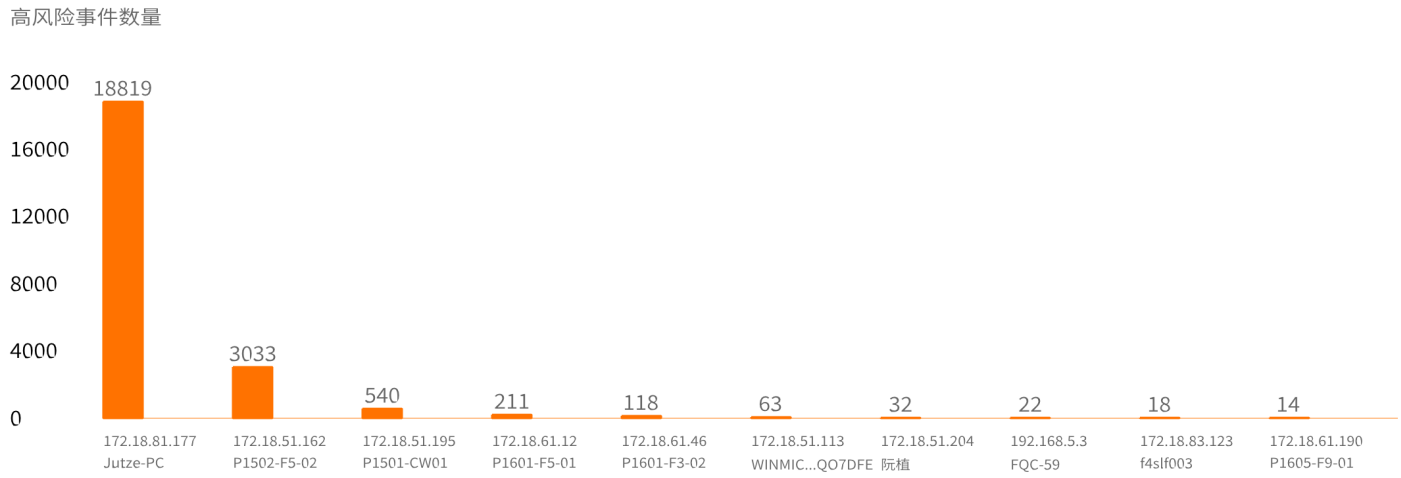
统计周期内受系统风险影响终端累计 31 台，下方统计出受系统风险事件影响最多的终端TOP10数据：



2.4 高风险终端分析

统计周期内全网高风险终端累计 63 台，下方对高风险终端进行分析统计

高风险终端TOP10统计



高风险终端风险详情（TOP10）

终端	典型风险	风险详情TOP10
阮植（172.18.51.204）	感染型 蠕虫	主机在2024/01/09 09:26检出感染型病毒Virus/Injexplorer
		主机在2024/01/09 09:26检出感染型病毒Virus/Sality.c
		主机在2024/01/09 09:26检出蠕虫病毒HEUR:Worm/FakeFolder.b
FQC-59（192.168.5.3）	感染型 木马释放 代码混淆器	主机在2024/01/11 11:18检出感染型病毒Virus/Sality.c
		主机在2024/01/11 11:18检出感染型病毒Virus/Injexplorer
		主机在2024/01/10 14:49检出感染型病毒Virus/Sality.c
		主机在2024/01/11 11:18检出木马释放病毒TrojanDropper/Ramnit.h
		主机在2024/01/10 14:49检出代码混淆器病毒HEUR:VirTool/Obfuscator.gen!C
P1502-F5-02（172.18.51.162）	感染型 代码混淆器	主机在2024/01/11 17:02检出感染型病毒Virus/Parite.b
		主机在2024/01/10 21:59检出感染型病毒Virus/Parite.b
		主机在2024/01/10 04:51检出感染型病毒Virus/Parite.b
		主机在2024/01/10 04:51检出感染型病毒Virus/Parite.bb!dll
		主机在2024/01/10 04:51检出感染型病毒Virus/Virut.e
		主机在2024/01/10 04:51检出感染型病毒Virus/Injexplorer
		主机在2024/01/10 04:51检出代码混淆器病毒HEUR:VirTool/Obfuscator.gen!B
P1501-CW01（172.18.51.195）	感染型 木马释放	主机在2024/01/10 11:11检出感染型病毒Virus/Ramnit.ep
		主机在2024/01/10 11:11检出木马释放病毒TrojanDropper/Ramnit.h
		主机在2024/01/10 11:11检出木马释放病毒TrojanDropper/Ramnit.a

终端	典型风险	风险详情TOP10
P1601-F5-01（172.18.61.12）	感染型 蠕虫 一般木马	主机在2024/01/10 19:52检出感染型病毒Virus/Virut.q!dam
		主机在2024/01/10 19:52检出感染型病毒Virus/Virut.r!dam
		主机在2024/01/09 17:39检出感染型病毒Virus/Virut.q!dam
		主机在2024/01/09 17:39检出感染型病毒Virus/Virut.r
		主机在2024/01/09 17:39检出感染型病毒Virus/Virut.n
		主机在2024/01/09 17:39检出感染型病毒Virus/Virut.q
		主机在2024/01/09 17:39检出感染型病毒Virus/Virut.r!dam
		主机在2024/01/09 17:39检出感染型病毒Virus/Sality.c
		主机在2024/01/09 17:39检出感染型病毒Virus/HTML.Virut
		主机在2024/01/09 17:39检出蠕虫病毒Worm/Autorun.fy
f4slf003（172.18.83.123）	蠕虫	主机在2024/01/13 21:50检出蠕虫病毒HEUR:Worm/FakeFolder.b
		主机在2024/01/13 21:28检出蠕虫病毒HEUR:Worm/FakeFolder.b
		主机在2024/01/13 20:16检出蠕虫病毒HEUR:Worm/FakeFolder.b
		主机在2024/01/12 20:06检出蠕虫病毒HEUR:Worm/FakeFolder.b
		主机在2024/01/09 21:54检出蠕虫病毒HEUR:Worm/FakeFolder.b

终端	典型风险	风险详情TOP10
P1605-F9-01（172.18.61.190）	感染型 后门 间谍木马 一般木马	主机在2024/01/10 09:07检出感染型病毒Virus/Injexplorer
		主机在2024/01/10 09:07检出后门病毒Backdoor/Agent.kv
		主机在2024/01/10 09:07检出间谍木马病毒TrojanSpy/Bzub.c
		主机在2024/01/10 09:07检出间谍木马病毒TrojanSpy/Bzub.b
		主机在2024/01/10 09:07检出一般木马病毒Trojan/Generic!65172AB1AEBDE007
		主机在2024/01/10 09:07检出一般木马病毒Trojan/AutoIT.Injector.h
		主机在2024/01/10 09:07检出一般木马病毒Trojan/Generic!8F5017C6663F46FD
		主机在2024/01/10 09:07检出一般木马病毒Trojan/Generic!EC8FBA2E62311269
P1601-F3-02（172.18.61.46）	感染型 一般木马	主机在2024/01/09 14:11检出感染型病毒Virus/Parite.b
		主机在2024/01/09 14:11检出感染型病毒Virus/Parite.bb!dll
		主机在2024/01/09 14:11检出一般木马病毒Trojan/Generic!65172AB1AEBDE007
WINMICR-FQO7DFE（172.18.51.113）	感染型 蠕虫 后门 间谍木马 木马释放 一般木马	主机在2024/01/10 14:54检出感染型病毒Virus/Injexplorer
		主机在2024/01/10 14:54检出感染型病毒Virus/Sality.c
		主机在2024/01/09 21:26检出感染型病毒Virus/Injexplorer
		主机在2024/01/09 21:26检出感染型病毒Virus/Ramnit.ep
		主机在2024/01/09 21:26检出感染型病毒Virus/Sality.c
		主机在2024/01/09 21:26检出蠕虫病毒Worm/Ramnit.e
		主机在2024/01/09 21:26检出后门病毒Backdoor/Agent.kv
		主机在2024/01/09 21:26检出间谍木马病毒TrojanSpy/Bzub.b
		主机在2024/01/09 21:26检出间谍木马病毒TrojanSpy/Bzub.c
		主机在2024/01/09 21:26检出木马释放病毒TrojanDropper/Ramnit.h

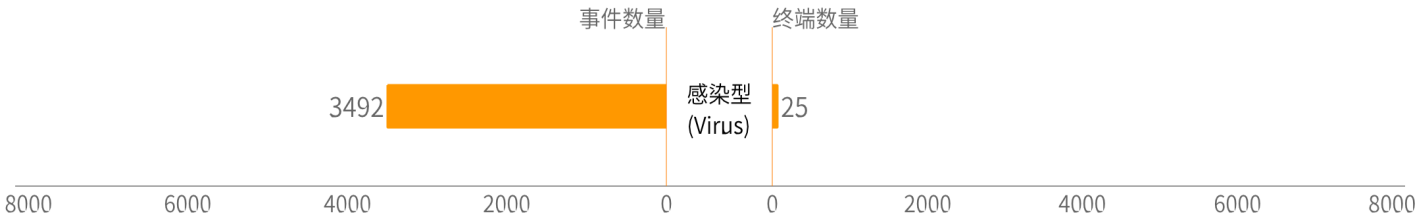
终端	典型风险	风险详情TOP10
Jutze-PC（172.18.81.177）	漏洞利用	主机在2024/01/11 11:10检出漏洞利用病毒Exploit/CVE-2010-2568.gen
		主机在2024/01/11 00:10检出漏洞利用病毒Exploit/CVE-2010-2568.gen
		主机在2024/01/11 00:09检出漏洞利用病毒Exploit/CVE-2010-2568.gen

三、典型风险分析及处理建议

统计周期内，全网发现典型风险 11 个，分别是：感染型(Virus)、蠕虫(Worm)、漏洞利用(Exploit)、内核驱动(Rootkit)、后门(Backdoor)、间谍木马(TrojanSpy)、木马下载(TrojanDownloader)、木马释放(TrojanDropper)、代码混淆器(VirTool)、一般木马(Trojan)、广告(Adware)；下方针对典型风险项进行分析并给出处理建议；

Virus(感染型)

统计周期内检出您的环境内存在Virus(感染型)，总计检出 3492 例，涉及终端总计 25 台



风险分析：

感染型病毒(Virus)，多会通过依附在其他可执行程序(.exe\.dll)上运行。此类病毒在感染正常的程序后，会利用该程序的自启动项，或用户正常使用等方式获得运行机会。除感染可执行文件外，还会利用如企业共享，漏洞利用等方式进行传播。终端感染此类病毒后，多会有数据被盗取、磁盘空间被额外占用、系统配置被修改、程序无法正常运行等问题。

处理建议：

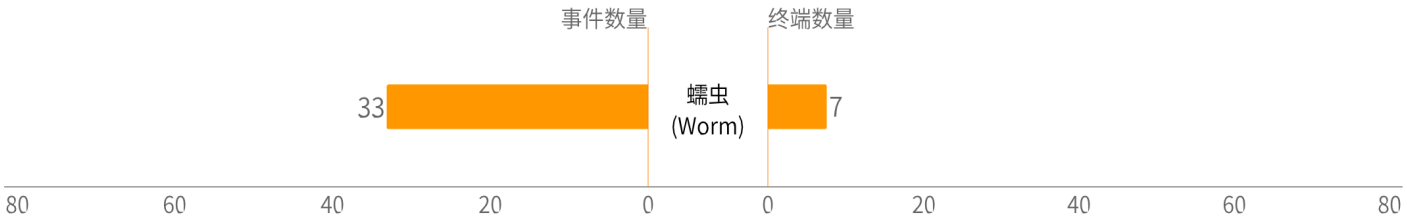
1.允许的话暂时停止使用共享文件，暂时禁用445端口。

2.调整文件实时监控级别为中高级别，清空中心和终端信任区，全盘扫描，处理后重启终端，再快速扫描确定是否有残留。

3.如遇到以上操作后仍然报毒情况可将终端日志提交给火绒进行分析。

Worm(蠕虫)

统计周期内检出您的环境内存在Worm(蠕虫)，总计检出 33 例，涉及终端总计 7 台



风险分析：

蠕虫病毒(Worm)，存在自我复制并有传播行为的病毒，常会利用系统漏洞、文件共享、可移动设备等多种方式进行传播。此类病毒除自身包含传播、修改系统配置等恶意行为外，多会与其他病毒模块结合使用，如挖矿病毒利用自身的蠕虫模块，在企业内进行传播。蠕虫病毒多使用火绒全盘查杀，查杀完毕后重启即可解决。企业内特殊场景(如共享目录查杀)的病毒处理方法，可按照此文档内提到的查杀方式解决。

处理建议：

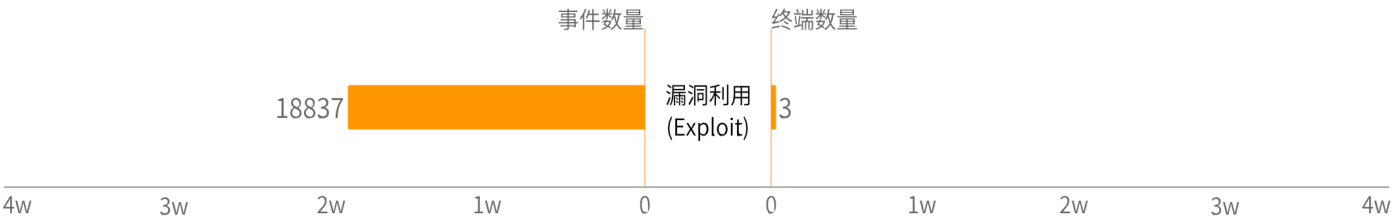
1.允许的话暂时停止使用共享文件，暂时禁用445端口。

2.调整文件实时监控级别为中高级别，清空中心和终端信任区，全盘扫描，处理后重启终端，再快速扫描确定是否有残留。

3.如遇到以上操作后仍然报毒情况可将终端日志提交给火绒进行分析。

Exploit(漏洞利用)

统计周期内检出您的环境内存在Exploit(漏洞利用)，总计检出 18837 例，涉及终端总计 3 台



风险分析：

漏洞利用(Exploit)，指利用程序中的某些漏洞，使恶意代码穿越过具有漏洞的程序的限制，得到计算机的控制权，以达到攻击者的非法目的。漏洞是在硬件、软件、协议的具体实现或操作系统安全策略上存在的缺陷，从而使攻击者能够在未经授权的情况下访问或者破坏系统。漏洞利用通常为本地\远程入侵，该类入侵方式也常被其他病毒利用，如挖矿、蠕虫、木马等，火绒均可防御本地\远程的入侵攻击。

处理建议：

1.允许的话暂时停止使用共享文件，暂时禁用445端口。

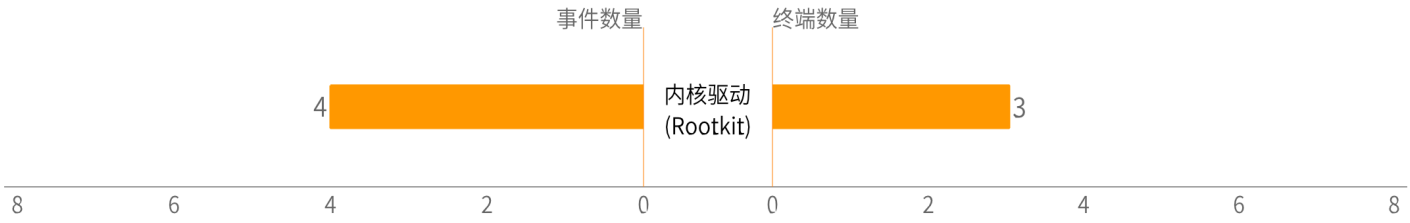
2.调整文件实时监控级别为中高级别，清空中心和终端信任区，全盘扫描，处理后重启终端，再快速扫描确定是否有残留。

3.及时使用漏洞修复小工具安装最新补丁。

4.如遇到以上操作后仍然报毒情况可将终端日志提交给火绒进行分析。

Rootkit(内核驱动)

统计周期内检出您的环境内存在Rootkit(内核驱动)，总计检出 4 例，涉及终端总计 3 台



风险分析：

Rootkit，指一种系统内核级病毒，其进入内核模块后能获取到操作系统高级权限，从而使用各种底层技术隐藏和保护自身，绕开安全软件的检测和查杀，达到收集用户信息、隐藏其他恶意工具、篡改用户数据等目的。该病毒一般都和木马、后门等其他恶意程序结合使用，或通过“白加黑”的方式释放，运行后常会有安全软件无法打开、安全服务异常和病毒模块反复被查杀但无法根除的情况。火绒可针对内核驱动病毒的释放进行实时查杀，并针对已经中毒终端用专杀工具进行清除。

处理建议：

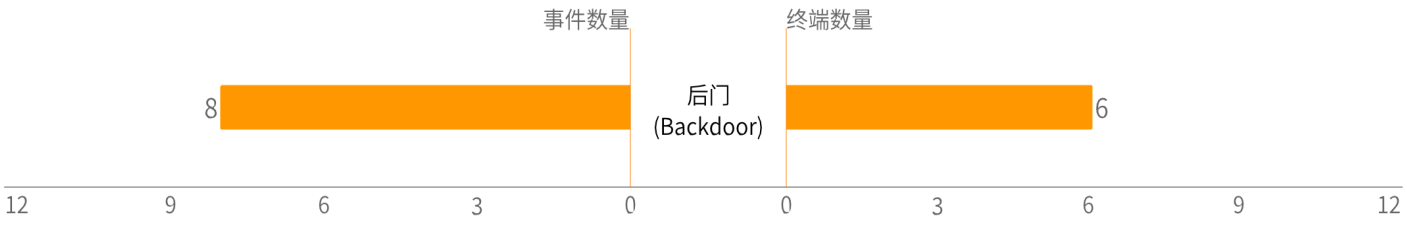
1.下载火绒专杀工具，扫描后处理病毒。

2.调整文件实时监控级别为中高级别，清空中心和终端信任区，全盘扫描，处理后重启终端，再快速扫描确定是否有残留。

3.如遇到以上操作后仍然报毒情况可将终端日志提交给火绒进行分析。

Backdoor(后门)

统计周期内检出您的环境内存在Backdoor(后门)，总计检出 8 例，涉及终端总计 6 台



风险分析：

后门(Backdoor)，指用户不知道也不允许的情况下，在终端上以隐蔽的方式运行，以达到远程控制、盗取用户数据、破坏用户系统等目的。后门病毒主要依靠漏洞、流氓软件等方式传播，常利用白加黑、注入、加壳等方式达到免杀、常驻的效果。

处理建议：

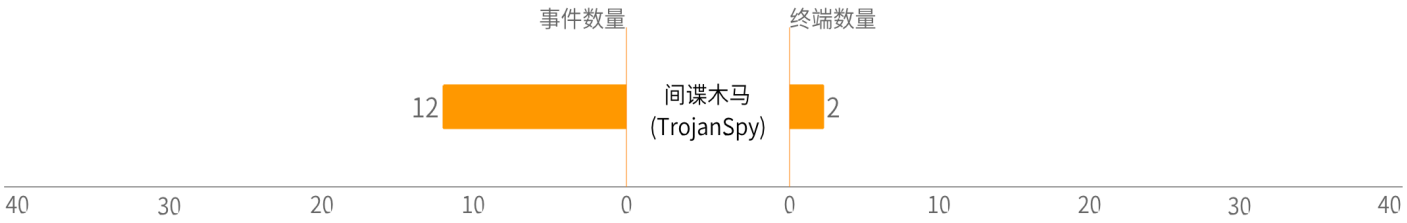
1.下载火绒专杀工具，扫描后处理病毒。

2.调整文件实时监控级别为中高级别，清空中心和终端信任区，全盘扫描，处理后重启终端，再快速扫描确定是否有残留。

3.如遇到以上操作后仍然报毒情况可将终端日志提交给火绒进行分析。

TrojanSpy(间谍木马)

统计周期内检出您的环境内存在TrojanSpy(间谍木马)，总计检出 12 例，涉及终端总计 2 台



风险分析：

间谍木马(TrojanSpy)，指通过将自身伪装吸引用户下载执行，向施种木马这提供打开被种者电脑的门户，使施种者可以任意破坏、窃取被种着的文件，甚至远程操控被种着的电脑。该病毒多通过第三方下载器、流氓软件、外挂程序、银行木马等传播，被感染终端多会有一个或几个端口被打开，使黑客利用控制器远程控制该终端，进行盗取数据、破坏终端等操作。

处理建议：

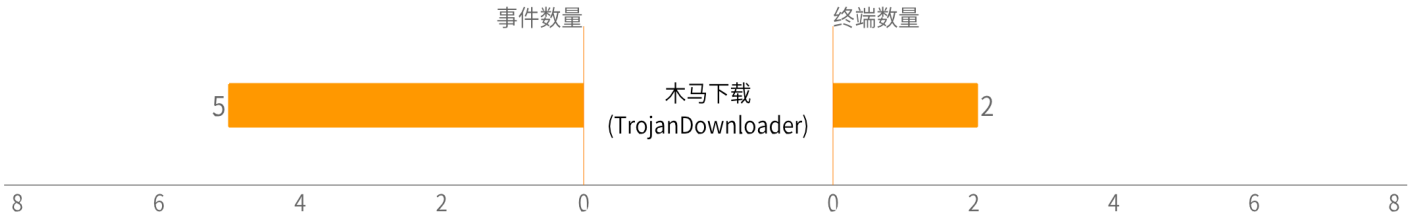
1.允许的话暂时停止使用共享文件，暂时禁用445端口。

2.调整文件实时监控级别为中高级别，清空中心和终端信任区，全盘扫描，处理后重启终端，再快速扫描确定是否有残留。

3.如遇到以上操作后仍然报毒情况可将终端日志提交给火绒进行分析。

TrojanDownloader(木马下载)

统计周期内检出您的环境内存在TrojanDownloader(木马下载)，总计检出 5 例，涉及终端总计 2 台



风险分析：

木马下载(TrojanDownloader)，指通过用户的计算机从其指定的C&C服务器下载一个或多个病毒文件并在本地运行，多为病毒内的下载组件。该病毒多依赖第三方下载器、流氓软件、外挂程序、挖矿木马、感染型病毒等传播，部分下载器还拥有对抗杀软、穿透防火墙、映像劫持、浏览器劫持等功能。

处理建议：

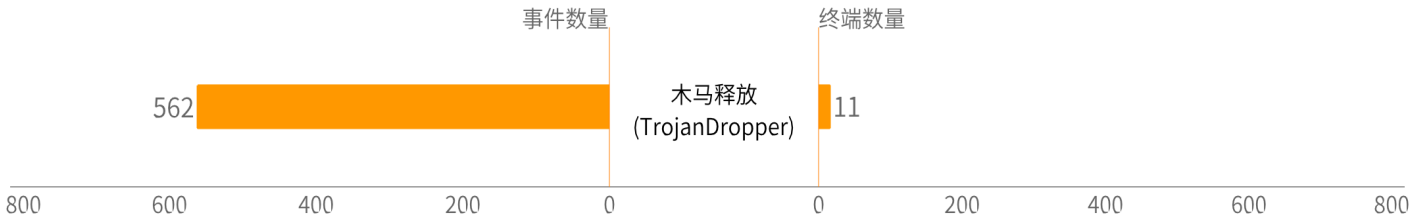
1.允许的话暂时停止使用共享文件，暂时禁用445端口。

2.调整文件实时监控级别为中高级别，清空中心和终端信任区，全盘扫描，处理后重启终端，再快速扫描确定是否有残留。

3.如遇到以上操作后仍然报毒情况可将终端日志提交给火绒进行分析。

TrojanDropper(木马释放)

统计周期内检出您的环境内存在TrojanDropper(木马释放)，总计检出 562 例，涉及终端总计 11 台



风险分析：

木马释放(TrojanDropper)，指启动后会从体内资源部分释放出病毒文件，多为病毒内的释放组件。该病毒多依赖第三方下载器、流氓软件、外挂程序、挖矿木马、感染型病毒等传播。因其多为“白加黑”进程或加壳进程，会具有一定的免杀作用。

处理建议：

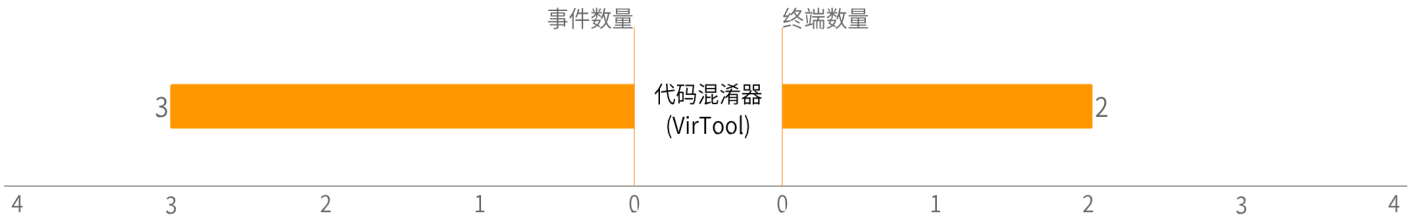
1.允许的话暂时停止使用共享文件，暂时禁用445端口。

2.调整文件实时监控级别为中高级别，清空中心和终端信任区，全盘扫描，处理后重启终端，再快速扫描确定是否有残留。

3.如遇到以上操作后仍然报毒情况可将终端日志提交给火绒进行分析。

VirTool(代码混淆器)

统计周期内检出您的环境内存在VirTool(代码混淆器)，总计检出 3 例，涉及终端总计 2 台



风险分析：

代码混淆器(VirTool)，指对发布出去的进程进行重新阻止和处理，使得处理后的代码与处理前代码完成相同的功能，而混淆后的代码很难被反编译，并且具有一定的免杀功能。该类多为对抗杀软查杀的方法之一，针对已报毒病毒重新加入代码混淆，使杀软无法根据以往查杀逻辑查杀该病毒。

处理建议：

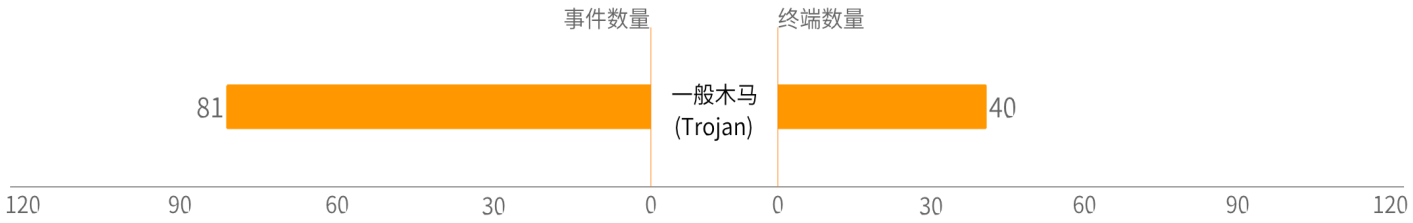
1.允许的话暂时停止使用共享文件，暂时禁用445端口。

2.调整文件实时监控级别为中高级别，清空中心和终端信任区，全盘扫描，处理后重启终端，再快速扫描确定是否有残留。

3.如遇到以上操作后仍然报毒情况可将终端日志提交给火绒进行分析。

Trojan(一般木马)

统计周期内检出您的环境内存在Trojan(一般木马)，总计检出 81 例，涉及终端总计 40 台



风险分析：

一般木马(Trojan)，指隐藏在正常程序中的一段具有特殊功能的恶意代码，使具备破坏和删除文件、发送密码、记录键盘和攻击DOS等特殊功能的后门程序。该类病毒多以来第三方下载器、流氓软件、系统漏洞、垃圾邮件、网页挂马等方式传播，被感染终端通常会出现系统卡顿、文件丢失、修改图标、破坏终端安全环境、盗取用户数据等情况。

处理建议：

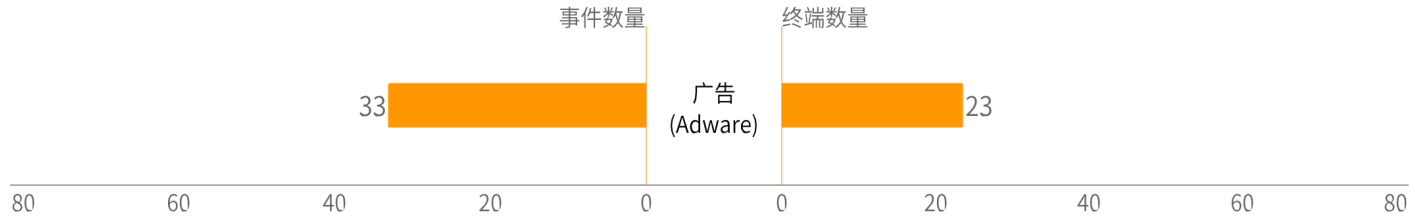
1.允许的话暂时停止使用共享文件，暂时禁用445端口。

2.调整文件实时监控级别为中高级别，清空中心和终端信任区，全盘扫描，处理后重启终端，再快速扫描确定是否有残留。

3.如遇到以上操作后仍然报毒情况可将终端日志提交给火绒进行分析。

Adware(广告)

统计周期内检出您的环境内存在Adware(广告)，总计检出 33 例，涉及终端总计 23 台



风险分析：

广告软件(Adware)，指此软件有大量广告推广行为，或此软件只包含广告推广功能，多通过"下载站下载器"、"捆绑安装"等方式进行安装，并难以完全卸载，对用户使用电脑造成影响。终端内发现此类软件，可先尝试卸载，如卸载后仍有广告弹出，可通过火绒查杀进行处理，如依旧存在问题，可联系火绒协助您进行排查。

处理建议：

1.排查终端是否被安装恶意软件，如被安装，请卸载。

2.调整文件实时监控级别为中高级别，清空中心和终端信任区，全盘扫描，处理后重启终端，再快速扫描确定是否有残留。

3.如遇到以上操作后仍然报毒情况可将终端日志提交给火绒进行分析。

四、附录

4.1 常见病毒介绍

常见病毒类型	定义
Virus(感染型)	通过感染以寄生的方式将恶意代码附着于正常程序中，并通过被感染的程序进行传播。
Worm(蠕虫)	通过可移动存储设备、网络、漏洞主动进行传播，此类病毒具有很强的扩散性。
Exploit(漏洞利用)	利用软件漏洞进行攻击的恶意代码类型。
Bootkit(磁盘主引导记录)	在操作系统启动前或启动时对操作系统内核进行劫持，通过隐藏其他病毒进程、注册表、文件相关操作等方式与安全软件进行对抗。
Rootkit(内核驱动)	对操作系统内核进行劫持，通过隐藏其他病毒进程、注册表、文件相关操作等方式与安全软件进行对抗。
Ransom(勒索)	通过对用户计算机中的数据文件进行加密、强行修改用户计算机密码、锁定用户计算机屏幕等手段来勒索用户钱财。
Backdoor(后门)	秘密开放用于远程操控的端口和权限，或主动连接黑客的控制端，持续存在在终端中造成持续安全威胁，将被感染主机变为可以被黑客控制的“肉鸡”。
Rogue(流氓程序)	通过诱导、欺骗、恐吓等手段胁迫用户，或通过篡改、劫持等手段操纵用户数据流量，以达到非法获利的目的。
TrojanSpy(间谍木马)	此类木马隐匿内在系统中，监视或记录用户主机信息等，然后将获取到的用户信息对外发送。
TrojanDownloader(木马下载)	通过下载其他病毒来间接对系统产生安全威胁，此类木马通常体积较小，并辅以诱惑性的名称和图标诱骗用户使用。
TrojanDropper(木马释放)	通过释放其他病毒来间接对系统产生安全威胁。
TrojanClicker(自动点击木马)	在后台通过访问特定网址来“刷流量”，为病毒作者获利，并会占用被感染主机的网络带宽。
TrojanProxy(代理木马)	在被感染主机上设置代理服务器，黑客可将被感染主机作为网络攻击的跳板，以躲避执法者的网络追踪。
VirTool(代码混淆器)	通过代码变形、反跟踪、反虚拟机等技术手段，专门被病毒用来与安全软件进行技术对抗的恶意代码类型。
Trojan(一般木马)	通过网络或者系统漏洞进入您的系统并隐藏，破坏系统或正常软件的安全性，向外泄露用户的隐私信息。
Omacro(Office宏病毒)	会感染您计算机上的OFFICE系列软件保存的文档，并且通过OFFICE通用模板进行传播。
HackTool(黑客工具)	可以被黑客利用，攻击用户计算机（以渗透传播为目的）或用户所在网络的工具程序。

4.2 风险等级介绍

风险等级	定义
高风险（存在失陷风险）	终端内出现高危病毒日志，或该终端有对外攻击、遭受攻击风险，需优先处理。
中风险（存在安全问题）	终端内发现异常行为，被火绒拦截，需详细确认。
低风险（风险较低）	终端内出现低危病毒日志，如广告程序，可根据需求处理。

4.3 安全建议

1.全网部署火绒，可对不同业务终端进行分类策略防护，加强内网终端安全防护，避免病毒反复传播感染。
2.定期全盘扫描，及时处理病毒问题，并对内网病毒种类进行分析，着重排查。
3.重视高危端口，针对不同业务的终端禁用端口，并定期排查终端安全日志，避免被长期暴破。
4.规范软件使用，避免使用第三方下载站、绿色版、破解版等软件的使用。
5.规范硬盘使用，针对可移动硬盘实行先查杀后使用的原则，避免传播病毒。
6.规范安全意识，针对报毒文件、软件、文档、工具等，不私自添加信任区，需将样本提取提交给火绒分析后使用。
7.安全加固建议，可根据《部署火绒后的安全加固建议》对内网进行防护部署，加强防护建设。
https://down5.huorong.cn/doc/enterprisev2/security_advice.pdf