2月政企终端安全态势分析报告



2019 年 3 月 11 日

目 录

[报告说明 1](#_Toc3203916)

[第一章 病毒攻击政企整体分析 2](#_Toc3203917)

[一、 攻击整体态势 2](#_Toc3203918)

[二、 被攻击终端分析 3](#_Toc3203919)

[三、 被攻击单位分析 4](#_Toc3203920)

[第二章 勒索病毒攻击政企分析 6](#_Toc3203921)

[一、 攻击整体态势 6](#_Toc3203922)

[二、 被攻击终端分析 7](#_Toc3203923)

[三、 被攻击单位分析 8](#_Toc3203924)

[第三章 漏洞利用病毒攻击政企分析 10](#_Toc3203925)

[一、 攻击整体态势 10](#_Toc3203926)

[二、 被攻击终端分析 11](#_Toc3203927)

[三、 被攻击单位分析 12](#_Toc3203928)

[第四章 蠕虫病毒攻击政企分析 14](#_Toc3203929)

[一、 攻击整体态势 14](#_Toc3203930)

[二、 被攻击终端分析 15](#_Toc3203931)

[三、 被攻击单位分析 16](#_Toc3203932)

[第五章 2月热点病毒事件关注 18](#_Toc3203933)

[第六章 政企终端安全建议 19](#_Toc3203934)

[关于360终端安全实验室 21](#_Toc3203935)

[关于360天擎新一代终端安全管理系统 21](#_Toc3203936)

[关于360天擎终端安全响应系统 22](#_Toc3203937)

# 报告说明

终端是政企内部网络不可或缺的组成部分，其安全状况与组织内每个成员息息相关。在很多情况下，终端也是内部网络和外部网络的连接点，是外部恶意程序进入内部网络常见的入口节点。终端一旦失守，整个办公或生产网络就有可能沦陷，给政企单位带来巨额损失。

《政企终端安全态势分析报告》是“360终端安全实验室”定期发布的针对政企网络终端的安全态势分析报告。报告数据来自 360 企业安全公有云安全监测数据。报告以勒索病毒、漏洞利用病毒、蠕虫病毒为主要研究对象，以每日感染病毒的终端为基本单位，通过对政企终端感染病毒情况的分析，帮助客户更清晰地看见风险态势，为安全决策提供更有力的参考依据。

监测数据表示360企业级终端安全产品对特定威胁的云查杀主动请求数量，对于本地已经可以查杀的病毒，不在统计之列。这些数据可以在一定程度上反映出相关机构遭到特定类型**活跃恶意程序**攻击的数量和强度。

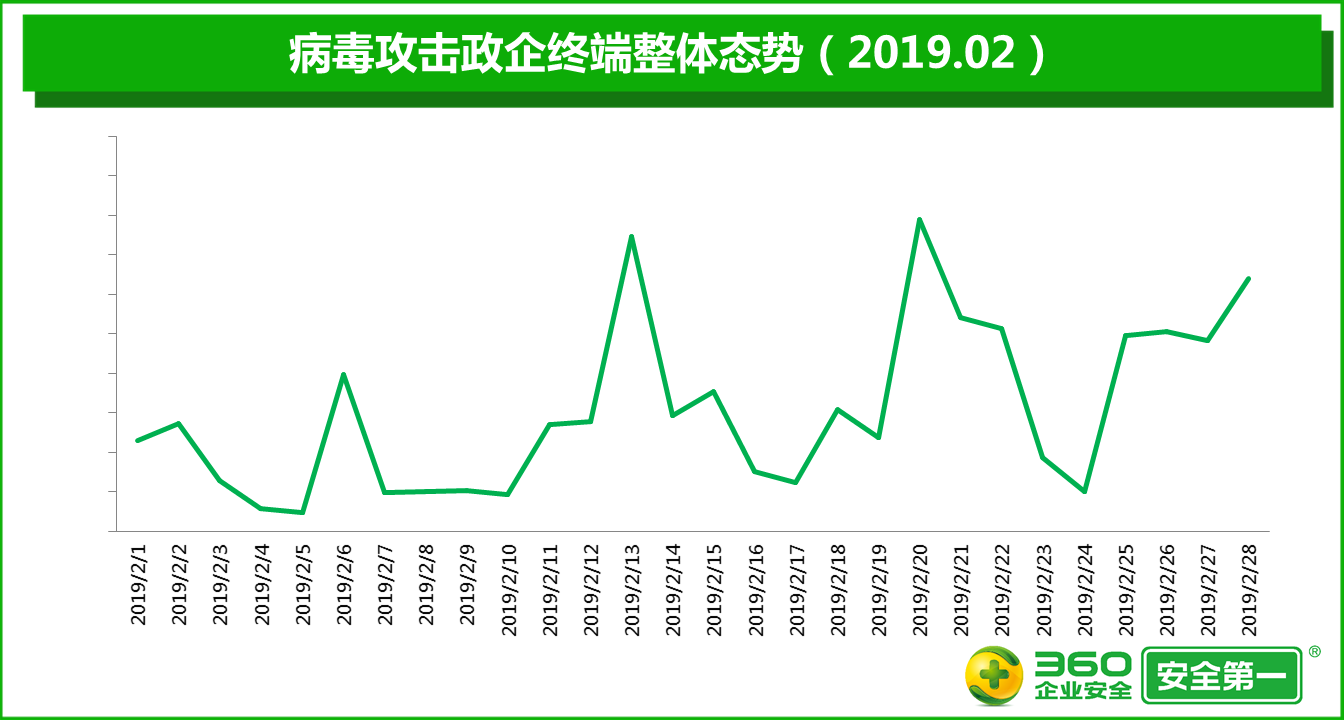
本期报告的监测时间为 **2019 年 2 月 1 日 ~ 2 月 28 日**。

# 病毒攻击政企整体分析

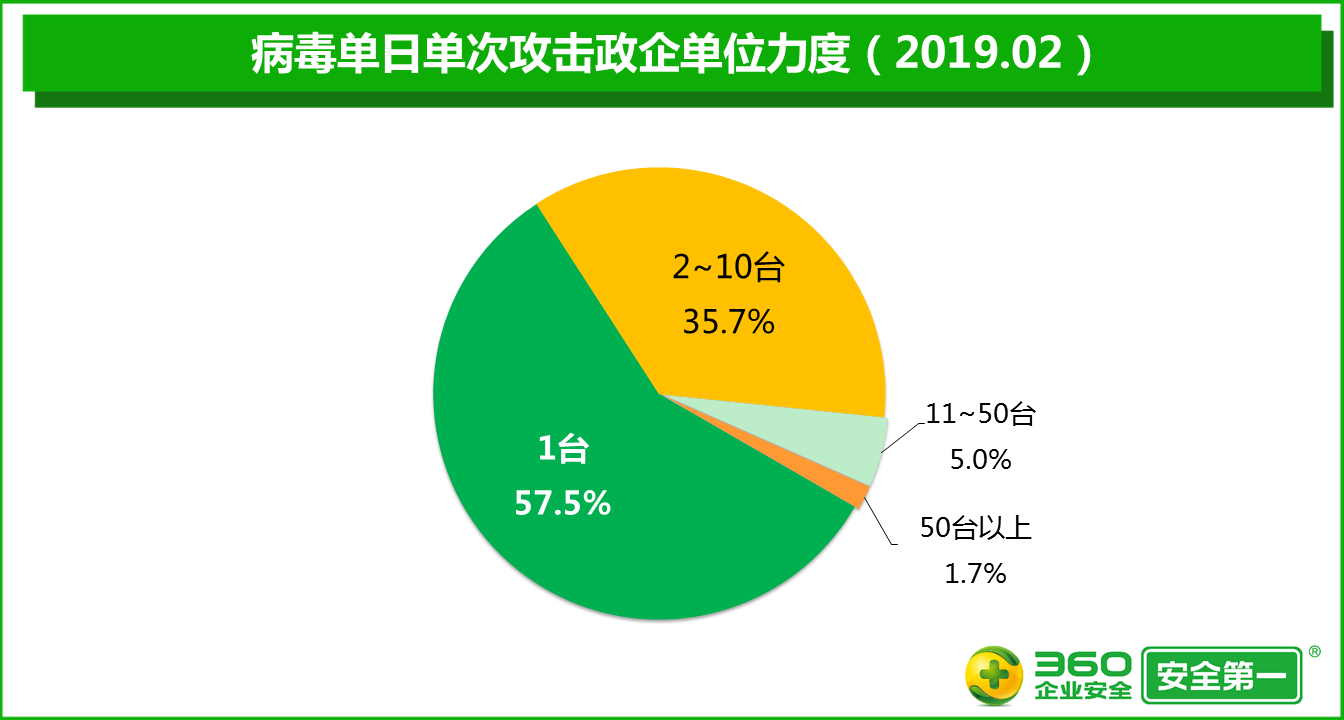
360终端安全实验室监测数据显示，2019年2月，政企单位被各类病毒攻击的事件数量比1月减少28.6%，被病毒攻击的政企终端的累计数量比1月减少13.3%，被病毒攻击的政企单位的绝对数量比1月减少19.6%。

## 攻击整体态势

2019年2月，病毒攻击的最高峰出现在**2月20日（星期三）**，最低谷则出现在**2月5日（星期二）**。

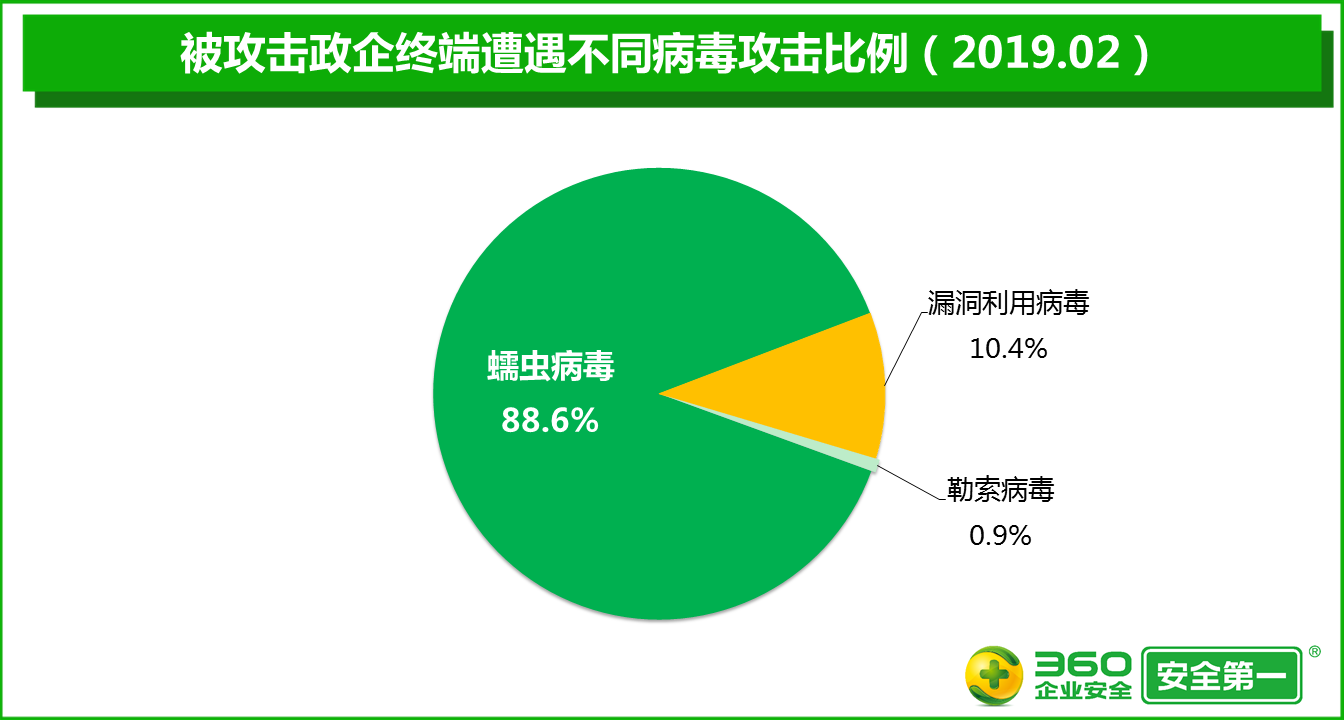


2019年2月，被病毒攻击的事件数量比1月减少28.6%。其中，病毒单日单次攻击政企单位的终端数仅为1台的事件比1月减少26.2%，占2月攻击事件总数的57.5%；单日单次攻击终端数为2~10台的事件比1月减少31.7%，占2月攻击事件总数的35.7%；单日单次攻击终端数为11~50台的事件比1月减少40.0%，占2月攻击事件总数的5.0%；单日单次攻击50台以上终端的事件比1月**增加18.8%**，占2月攻击事件总数的1.7%。

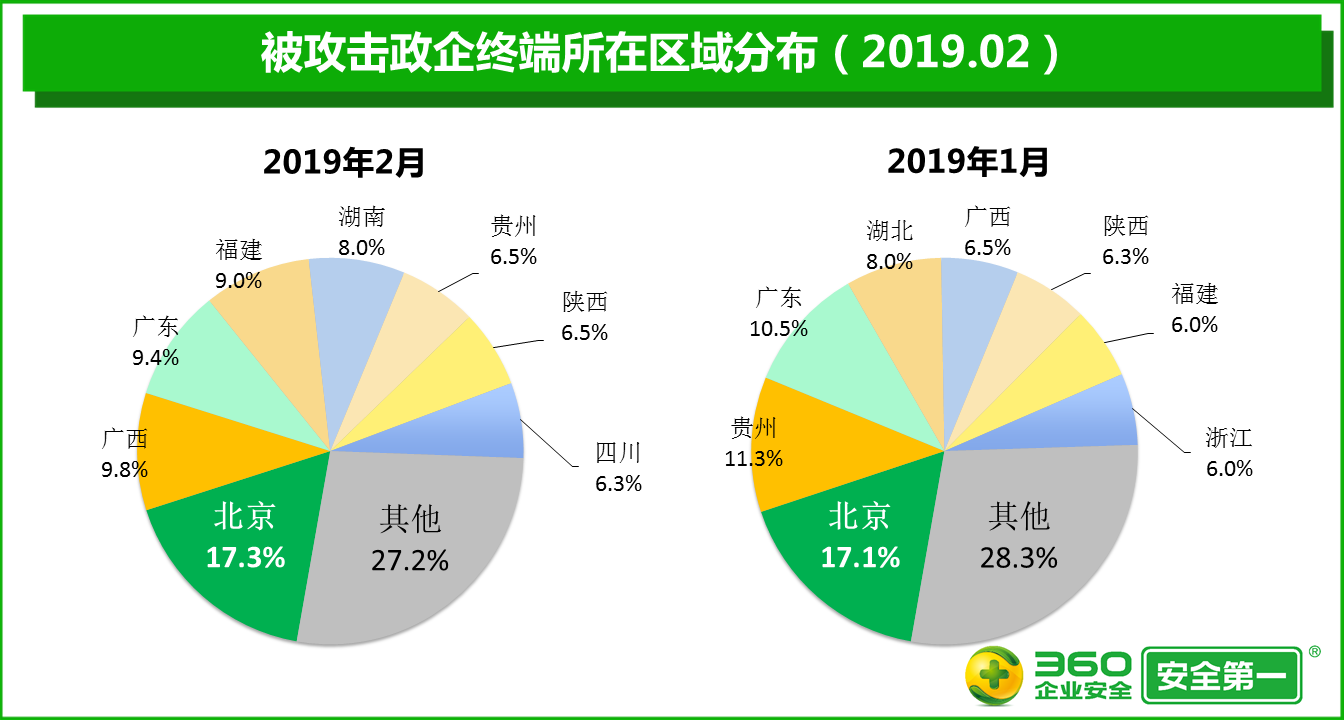


## 被攻击终端分析

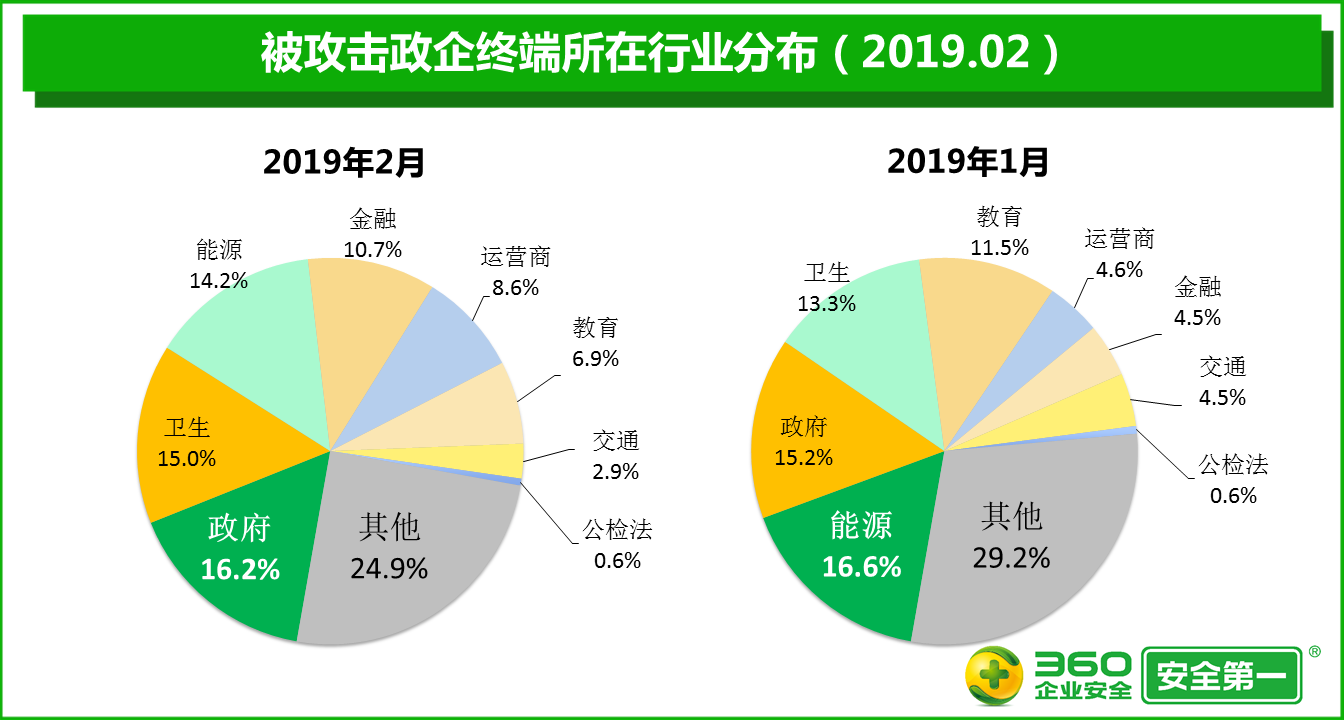
2019年2月，被病毒攻击的政企终端的累计数量比1月减少13.3%。其中，遭遇蠕虫病毒攻击的政企终端的累计数量比1月减少9.0%，占被攻击政企终端的88.6%；遭遇漏洞利用病毒攻击的政企终端的累计数量比1月减少32.9%，占被攻击政企终端的10.4%；遭遇勒索病毒攻击的累计数量比1月减少32.5%，占被攻击政企终端的0.9%。



在被病毒攻击的政企终端中，北京地区最多，占比高达17.3%，被攻击终端的累计数量比1月减少12.5%；其次是广西，占比为9.8%，被攻击终端的累计数量比1月**增加31.8%**；广东排在第三位，占比为9.4%，被攻击终端的累计数量比1月减少22.5%。



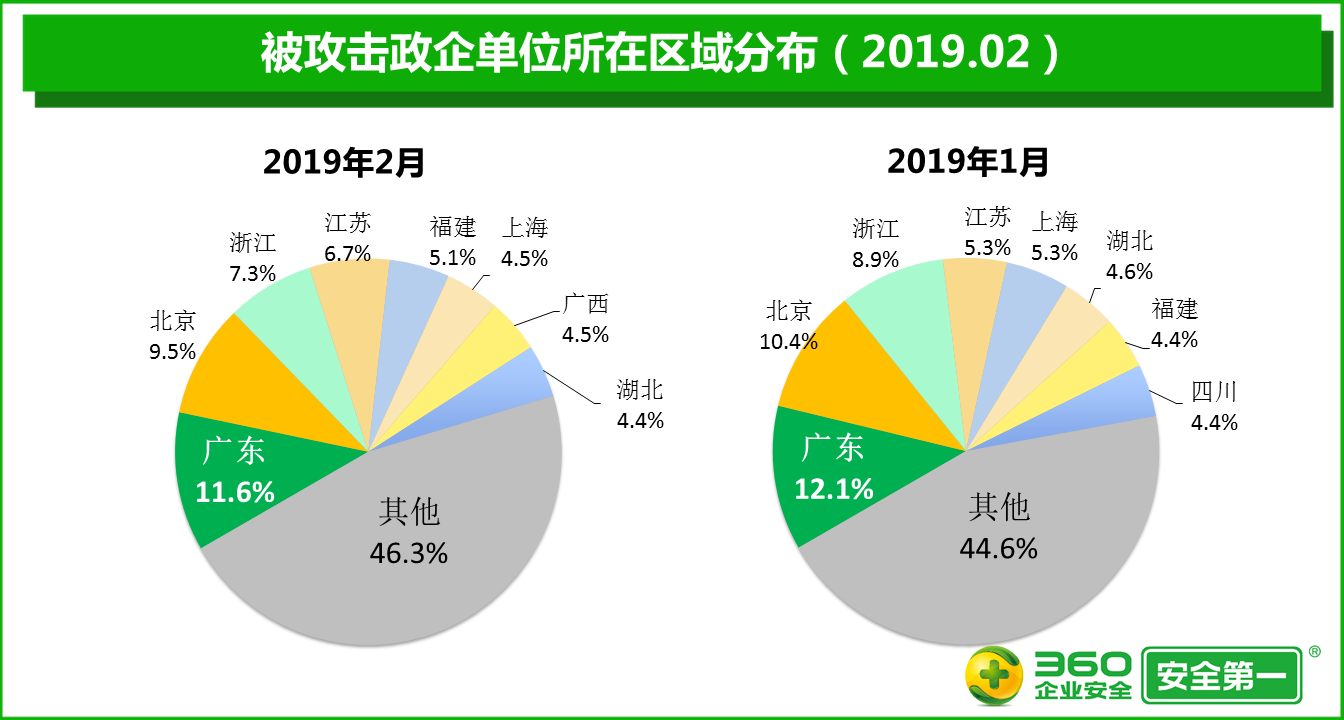
在被病毒攻击的政企终端中，政府行业最多，占比高达16.2%，被攻击终端的累积数量比1月减少7.7%；其次是卫生行业，占比为15.0%，被攻击终端的累积数量比1月减少2.2%；能源行业排在第三位，占比为14.2%，被攻击终端的累积数量比1月减少25.9%。



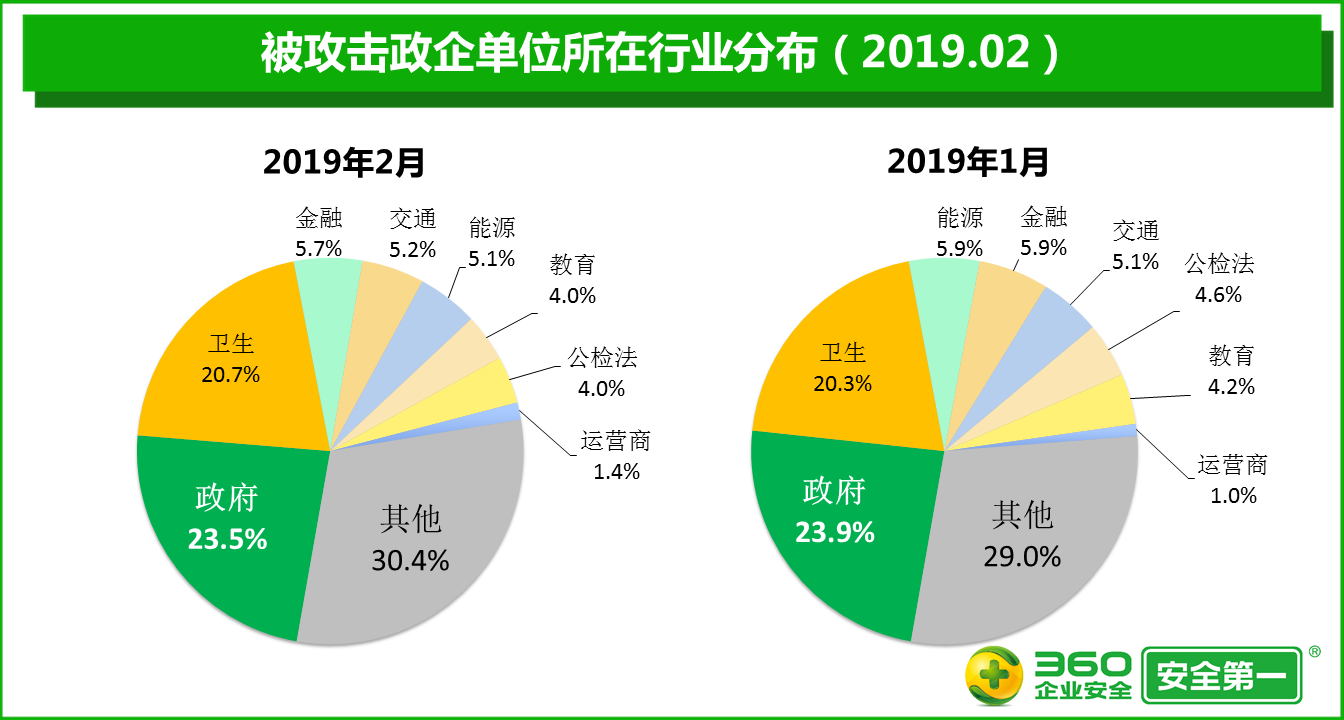
## 被攻击单位分析

2019年2月，被病毒攻击的政企单位的绝对数量比1月减少19.6%。在受到病毒攻击的政企单位中，87.9%的单位遭到蠕虫病毒的攻击，绝对数量比1月减少22.9%；26.1%的单位遭到漏洞利用病毒的攻击，绝对数量比1月减少12.3%；5.9%的单位遭到勒索病毒的攻击，绝对数量比1月减少7.5%。

在被病毒攻击的政企单位中，广东地区最多，占比高达11.6%，被攻击单位的绝对数量比1月减少20.7%；其次是北京，占比为9.5%，被攻击单位的绝对数量比1月减少25.0%；浙江排在第三位，占比为7.3%，被攻击单位的绝对数量比1月减少31.8%。



在被病毒攻击的政企单位中，政府行业最多，占比高达23.5%，被攻击单位的绝对数量比1月减少20.9%；其次是卫生行业，占比为20.7%，被攻击单位的绝对数量比1月减少18.2%；金融行业排在第三位，占比为5.7%，被攻击单位的绝对数量比1月减少21.7%。

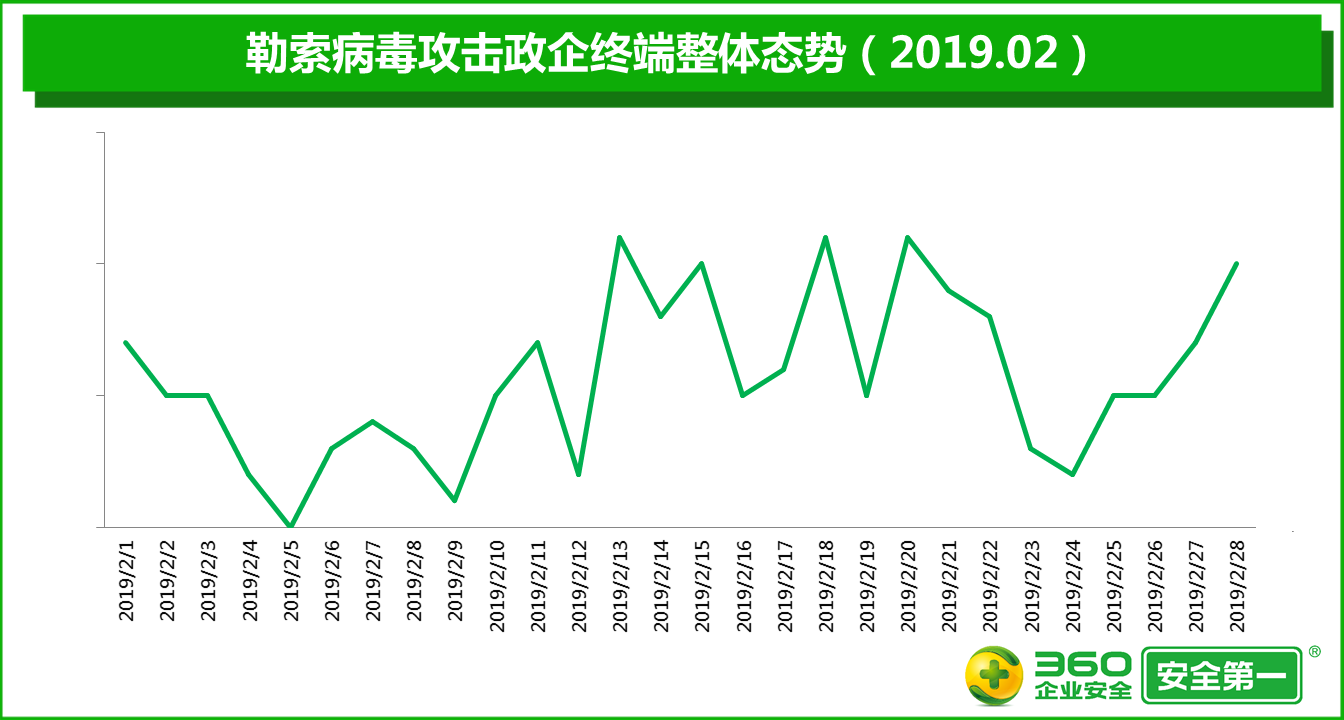


# 勒索病毒攻击政企分析

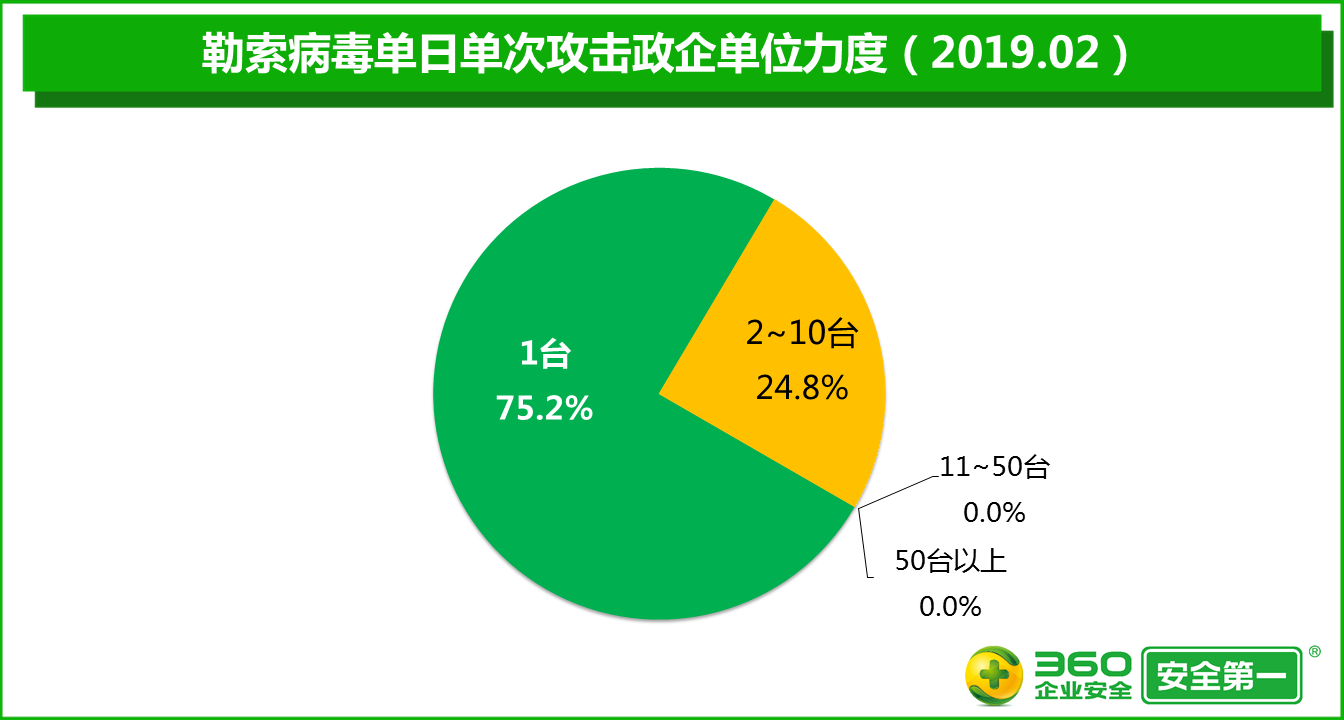
360终端安全实验室监测数据显示，2019年2月，政企单位被勒索病毒攻击的事件数量比1月减少16.6%，被勒索病毒攻击的政企终端的累计数量比1月减少32.5%，被勒索病毒攻击的政企单位的绝对数量比1月减少7.5%。

## 攻击整体态势

2019年2月，勒索病毒攻击的最高峰出现在**2月18日（星期三）**，最低谷则出现在**2月5日（星期二）**。



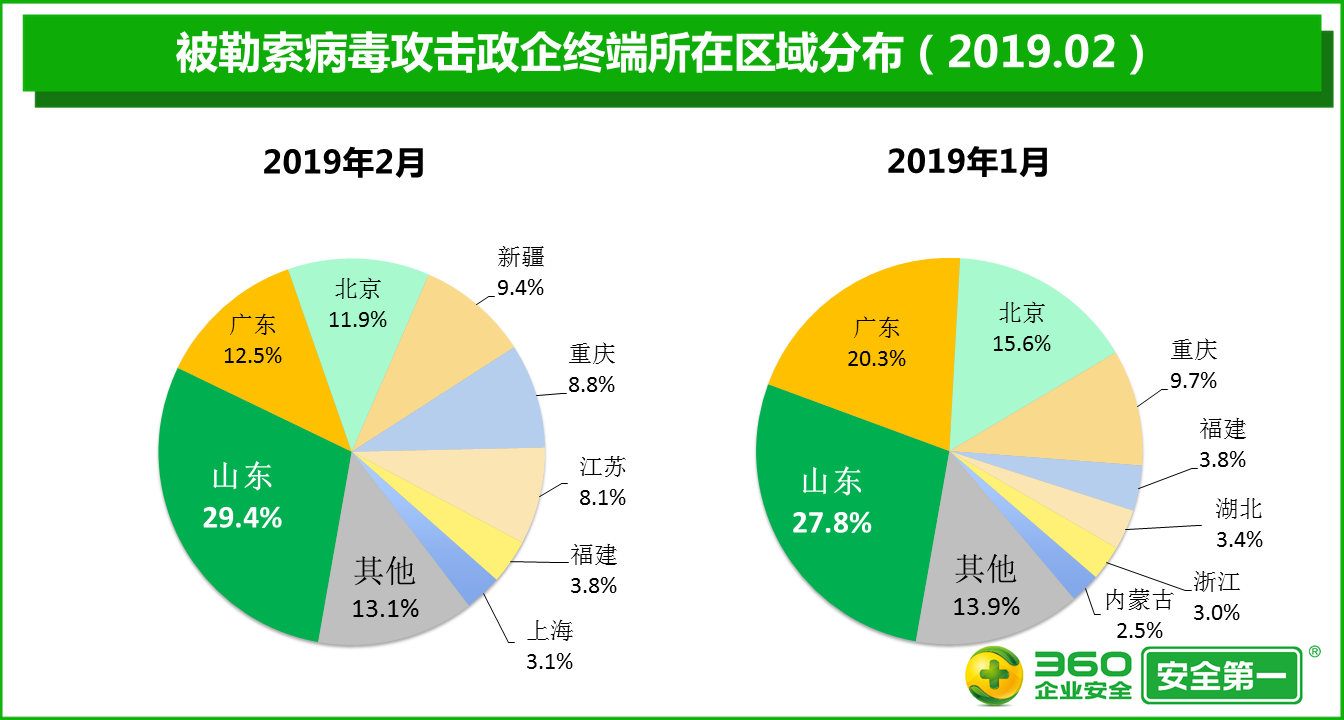
2019年2月，被勒索病毒攻击的事件数量比1月减少16.6%。其中，单日单次攻击政企单位的终端数仅为1台的事件比1月减少9. 9%，占2月勒索病毒攻击事件总数的75.2%；单日单次攻击终端数为2~10台的事件比1月减少28.6%，占2月勒索病毒攻击事件总数的24.8%；没有监测到单日单次攻击终端数超过10台以上的事件。



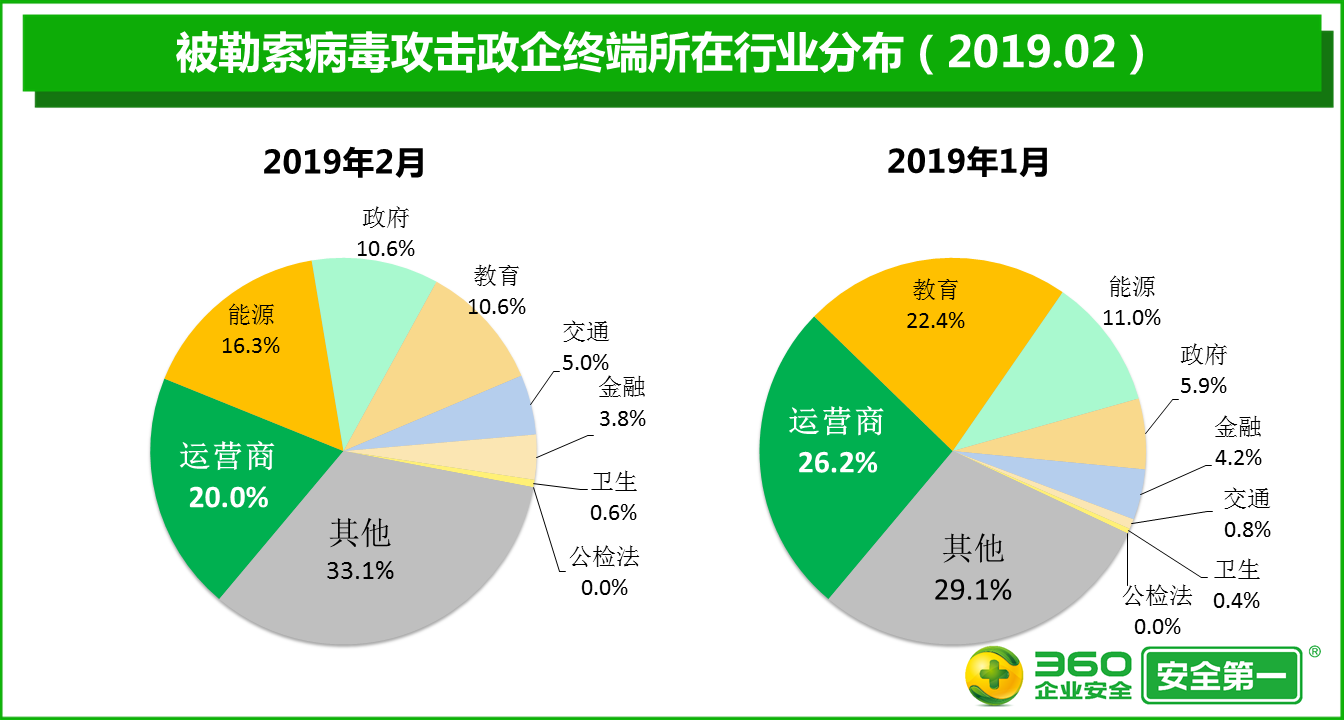
## 被攻击终端分析

2019年2月，被勒索病毒攻击的政企终端的累计数量比1月减少32.5%。

在被勒索病毒攻击的政企终端中，山东地区最多，占比高达29.4%，被攻击终端的累计数量比1月减少22.8%；其次是广东，占比为12.5%，被攻击终端的累计数量比1月减少58.3%；北京排在第三位，占比为11.9%，被攻击终端的累计数量比1月减少48.6%。



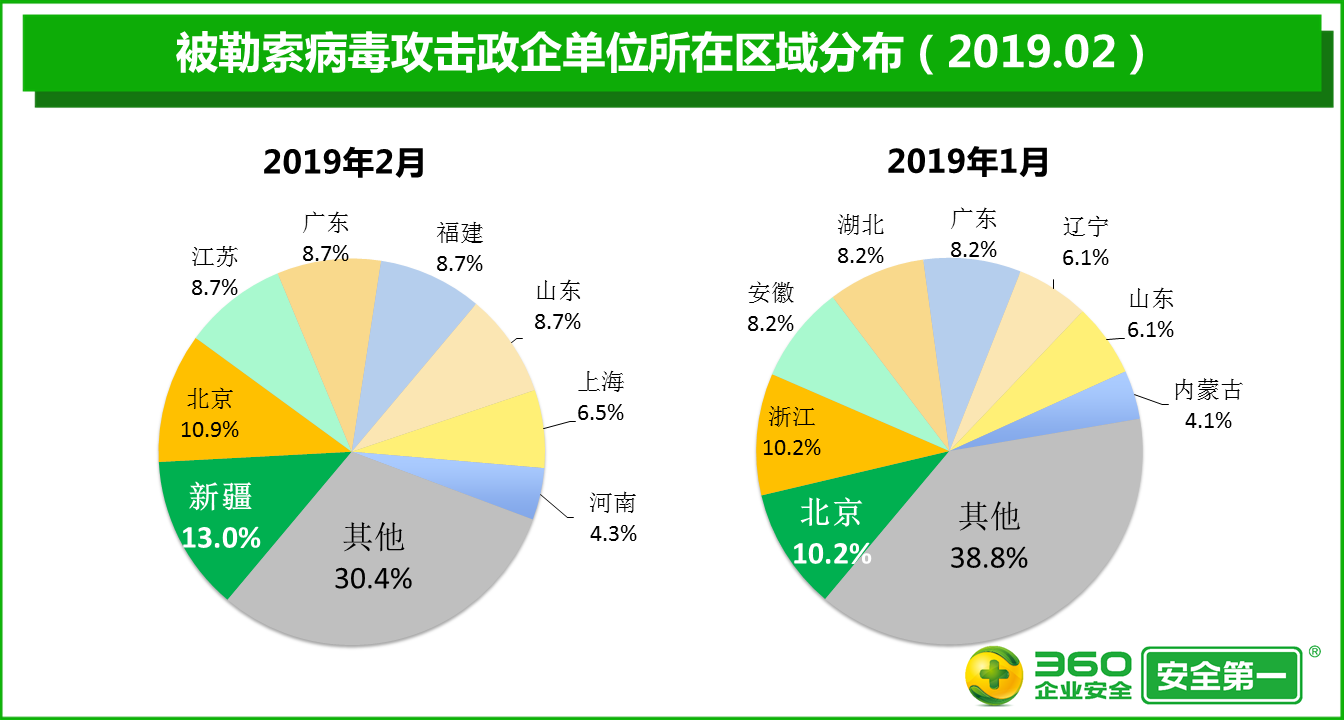
在被勒索病毒攻击的政企终端中，运营商行业最多，占比高达20.0%，被攻击终端的累计数量比1月减少48.4%；其次是能源行业，占比为16.3%，被攻击终端的累计数量和1月持平；政府行业排在第三位，占比为10.6%，被攻击终端的累计数量比1月**增加21.4%**。



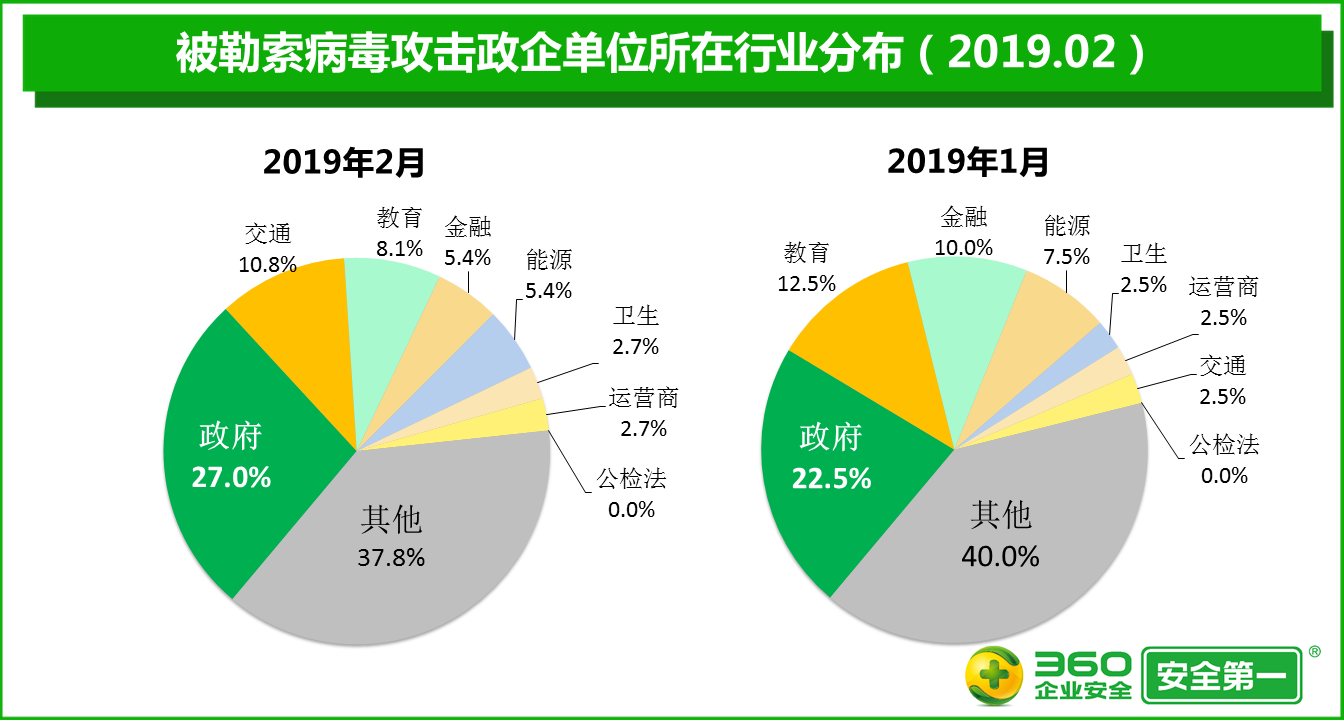
## 被攻击单位分析

2019年2月，被勒索病毒攻击的政企单位的绝对数量比1月减少7.5%。

在被勒索病毒攻击的政企单位中，新疆地区最多，占比高达13.0%；其次是北京和江苏，占比分别是10.9%、8.7%。



在被勒索病毒攻击的政企单位中，政府行业最多，占比高达27.0%，被攻击单位的绝对数量比1月**增加11.1%**；其次是交通行业，占比为10.8%，被攻击单位的绝对数量比1月**增加300%**；教育行业排在第三位，占比为8.1%，被攻击单位的绝对数量比1月减少40.0%。

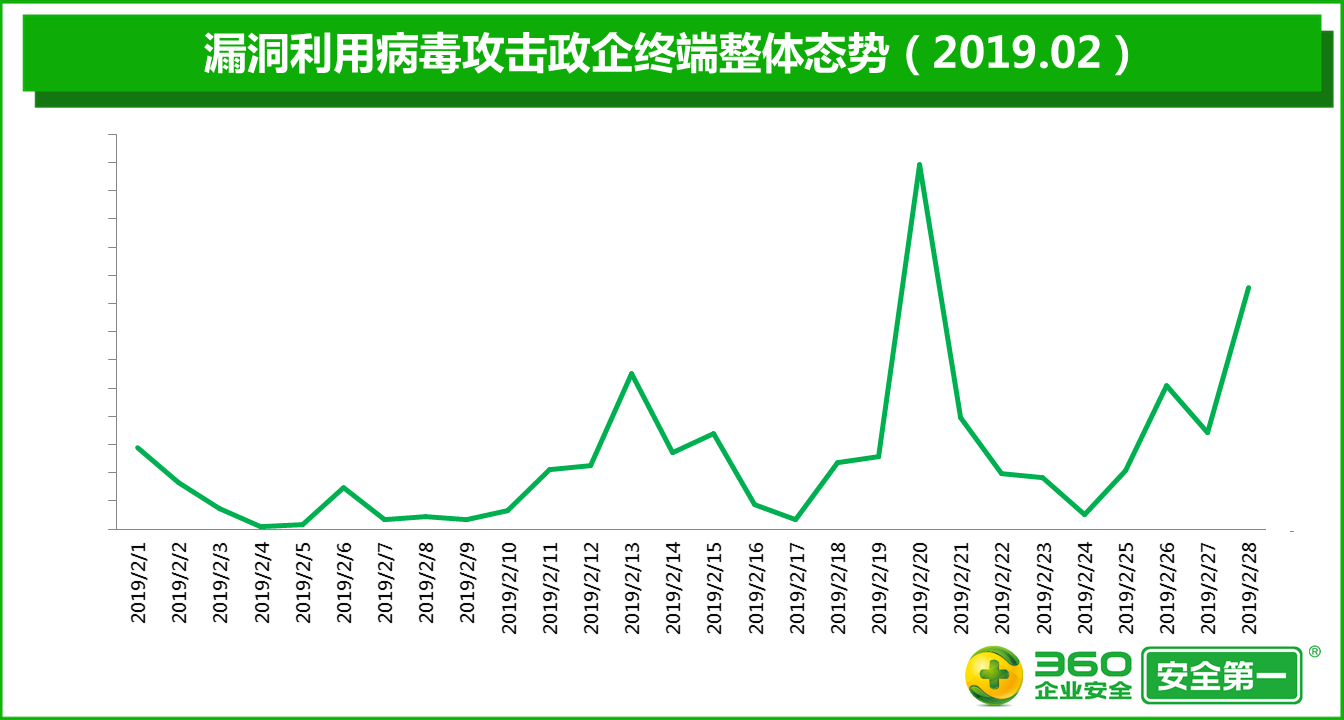


# 漏洞利用病毒攻击政企分析

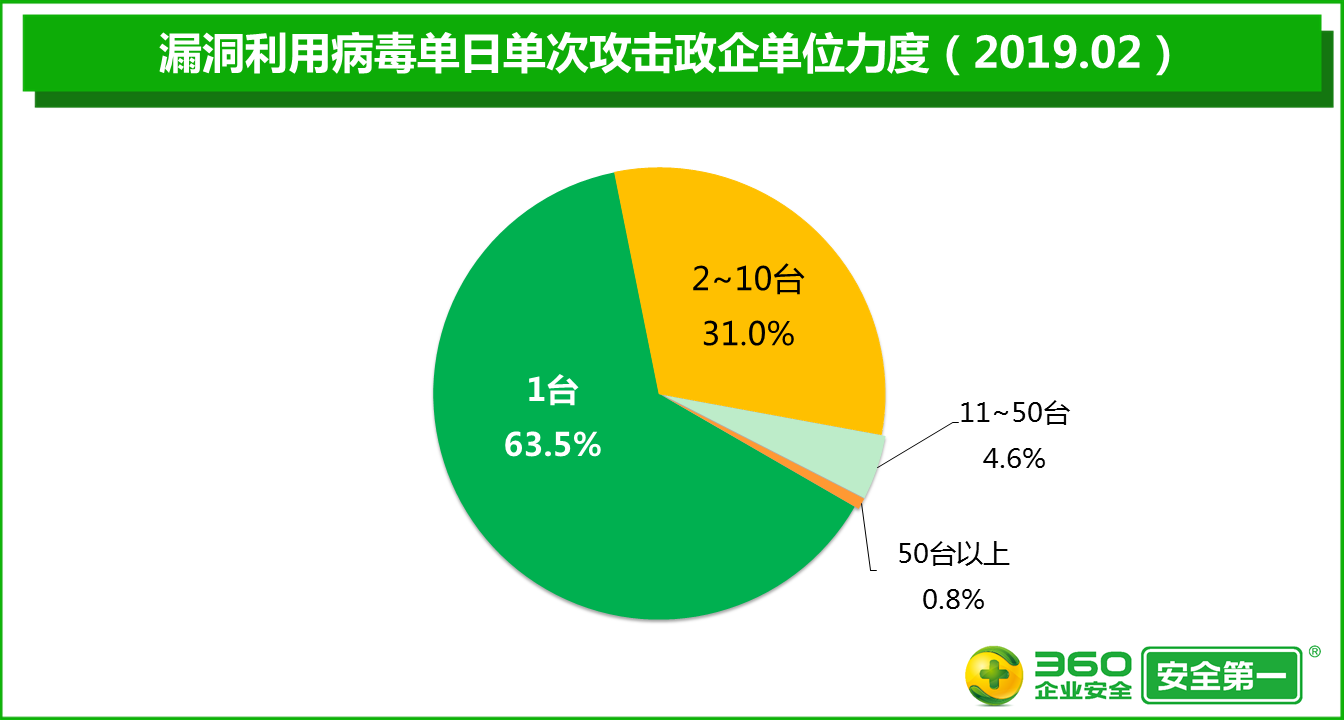
360终端安全实验室监测数据显示，2019年2月，政企单位被漏洞利用病毒攻击的事件数量比1月减少24.3%，被漏洞利用病毒攻击的政企终端的累计数量比1月减少32.9%，被漏洞利用病毒攻击的政企单位的绝对数量比1月减少12.3%。

## 攻击整体态势

2019年2月，漏洞利用病毒攻击的最高峰出现在**2月20日（星期三）**，最低谷则出现在**2月4日（星期一）**。



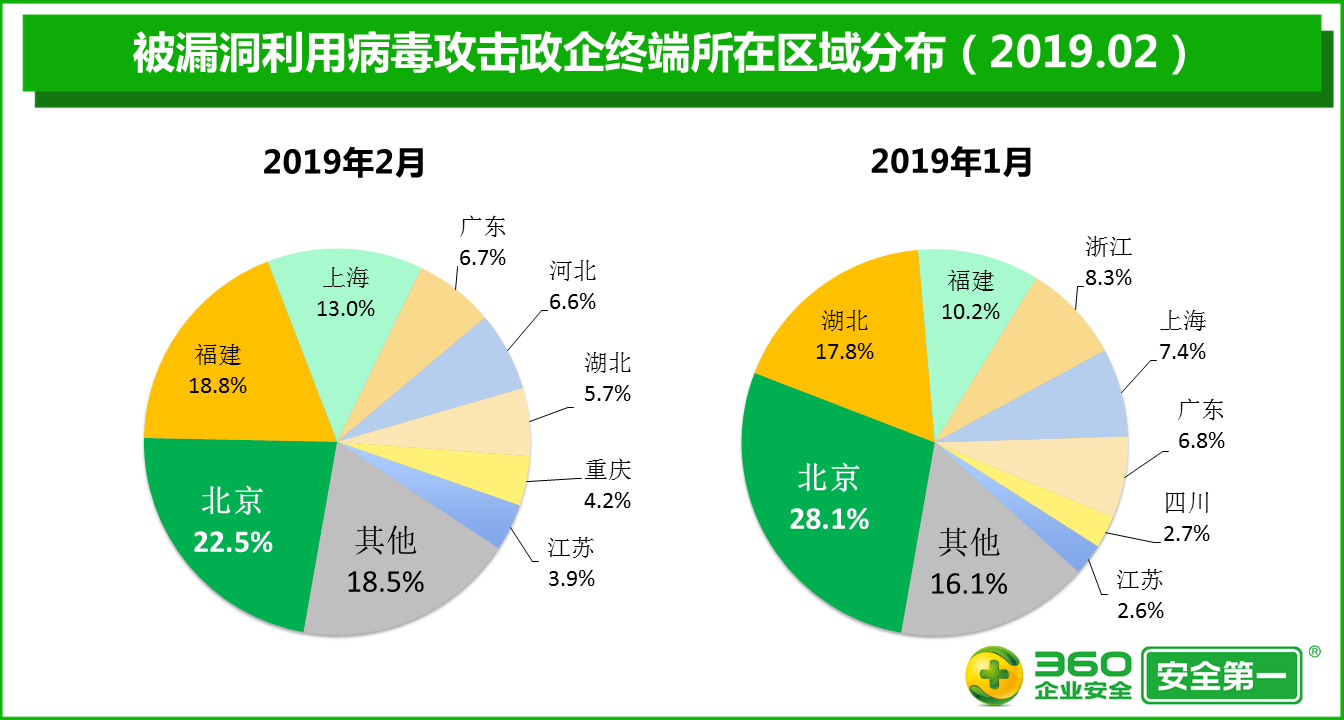
2019年2月，被漏洞利用病毒攻击的事件数量比1月减少24.3%。其中，单日单次攻击政企单位的终端数仅为1台的事件比1月减少13.0%，占2月漏洞利用病毒攻击事件总数的63.5%；单日单次攻击终端数为2~10台的事件比1月减少35.8%，占2月漏洞利用病毒攻击事件总数的31.0%；单日单次攻击终端数为11~50台的事件比1减少48.9%，占2月漏洞利用病毒攻击事件总数的4.6%；单日单次攻击50台以上终端的事件比1月减少50.0%，占2月漏洞利用病毒攻击事件总数的0.8%。



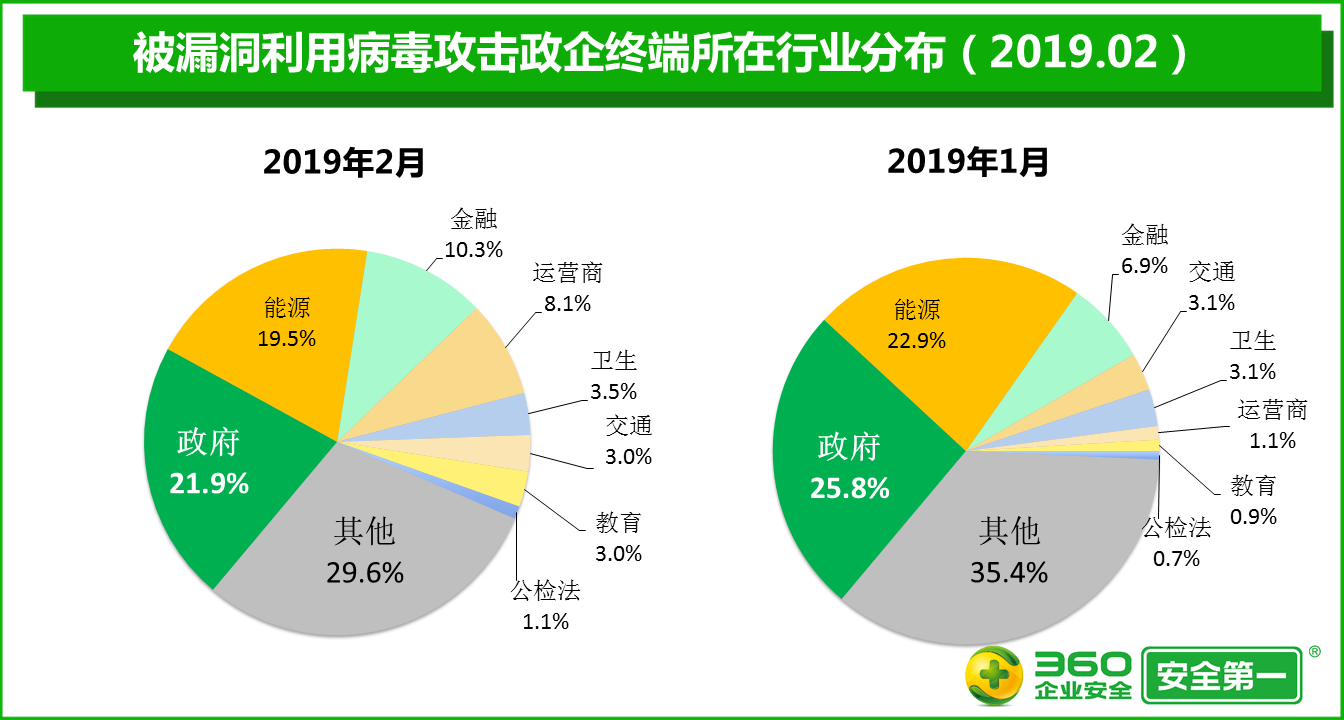
## 被攻击终端分析

2019年2月，被漏洞利用病毒攻击的政企终端的累计数量比1月减少32.9%。

在被漏洞利用病毒攻击的政企终端中，北京地区最多，占比高达22.5%，被攻击终端的累计数量比1月**减少46.2%**；其次是福建，占比为18.8%，被攻击终端的累计数量比1月**增加24.1%**；上海排在第三位，占比为13.0%，被攻击终端的累计数量比1月**增加18.4%**。



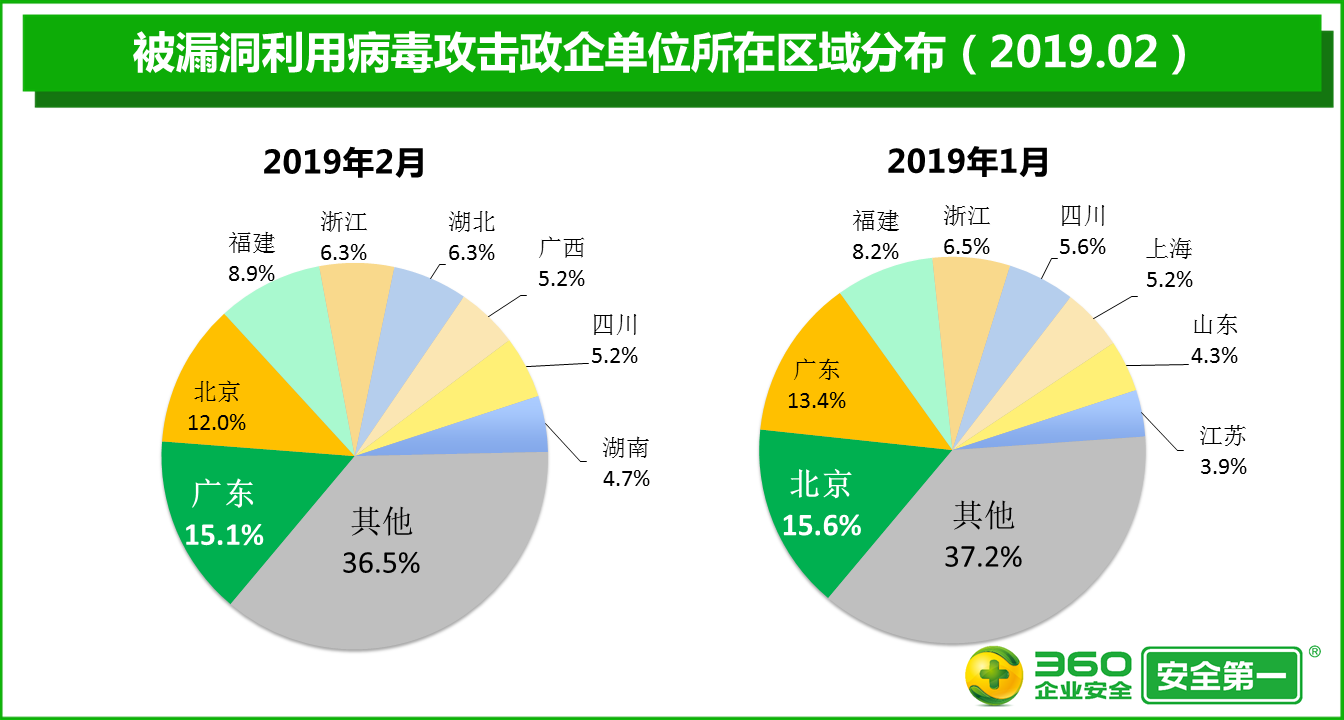
在被漏洞利用病毒攻击的政企终端中，政府行业最多，占比高达21.9%，被攻击终端的累计数量比1月减少43.1%；其次是能源行业，占比为19.5%，被攻击终端的累计数量比1月减少42.8%；金融行业排在第三位，占比为10.3%，被攻击终端的累计数量和1月基本持平。



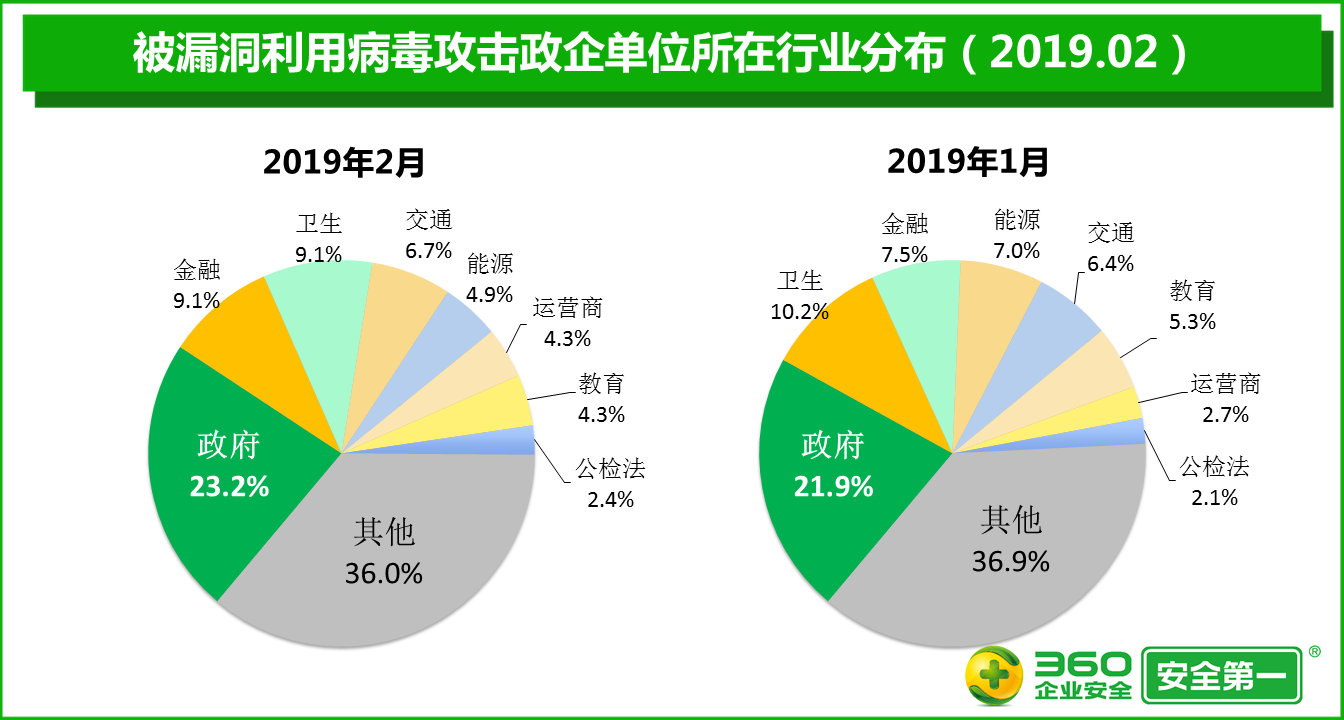
## 被攻击单位分析

2019年2月，被漏洞利用病毒攻击的政企单位的绝对数量比1月减少12.3%。

在被漏洞利用病毒攻击的政企单位中，广东地区最多，占比高达15.1%，被攻击单位的绝对数量比1月减少6.5%；其次是北京，占比为12.0%，被攻击单位的绝对数量比1月减少36.1%；福建排在第三位，占比为8.9%，被攻击单位的绝对数量比1月减少10.5%。



在被漏洞利用病毒攻击的政企单位中，政府行业最多，占比高达23.2%，被攻击单位的绝对数量比1月减少7.3%；其次是金融、卫生行业，占比均为9.1%，但金融行业被攻击单位的绝对数量比1月**增加7.1%**，而卫生行业被攻击单位的绝对数量比1月减少21.1%。

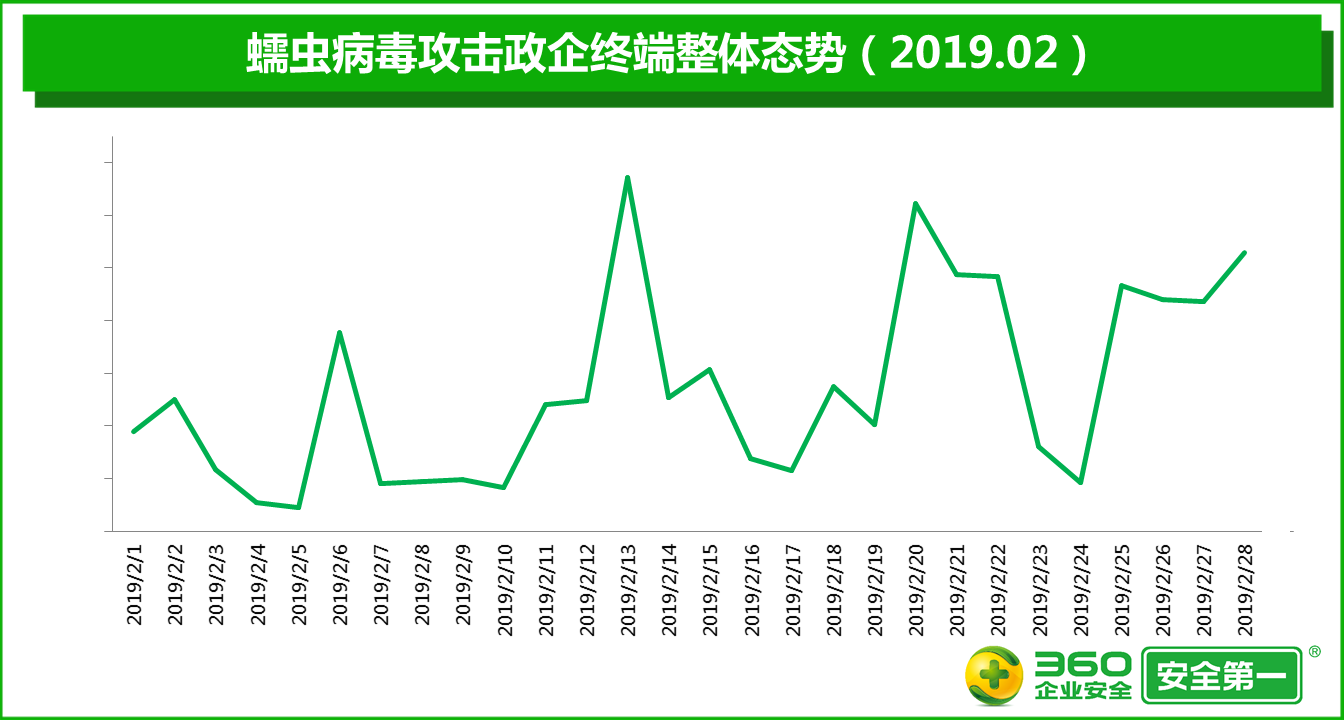


# 蠕虫病毒攻击政企分析

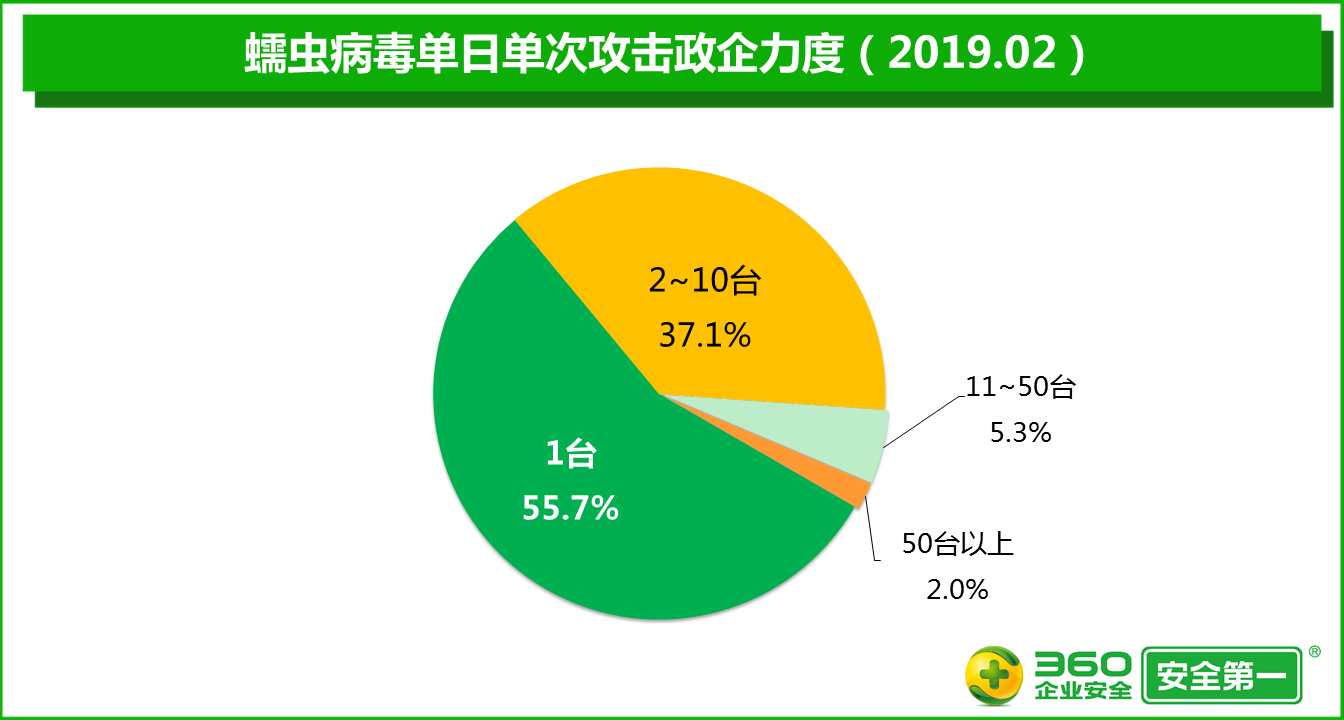
360终端安全实验室监测数据显示，2019年2月，政企单位被蠕虫病毒攻击的事件数量比1月减少29.8%，被蠕虫病毒攻击的政企终端的累计数量比1月减少9.9%，被蠕虫病毒攻击的政企单位的绝对数量比1月减少22.9%。

## 攻击整体态势

2019年2月，蠕虫病毒攻击的最高峰出现在**2月13日（星期三）**，最低谷则出现在**2月5日（星期二）**。



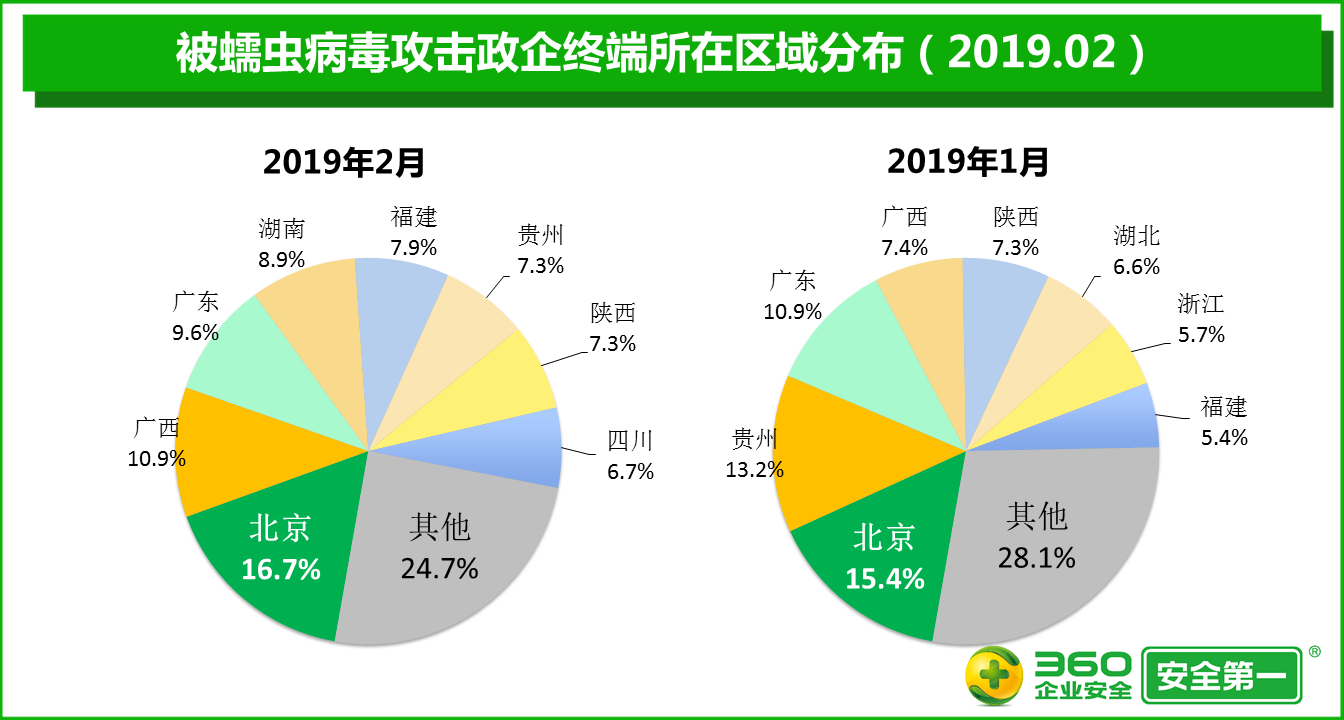
2019年2月，被蠕虫病毒攻击的事件数量比1月减少29.8%。其中，单日单次攻击政企单位的终端数仅为1台的事件比1月减少29.2%，占2月攻击事件总数的55.7%；单日单次攻击终端数为2~10台的事件比1月减少31.1%，占2月攻击事件总数的37.1%；单日单次攻击终端数为11~50台的事件比1月减少37.7%，占2月攻击事件总数的5.3%；单日单次攻击50台以上终端的事件比1月**增加32.5%**，占2月攻击事件总数的2.0%。



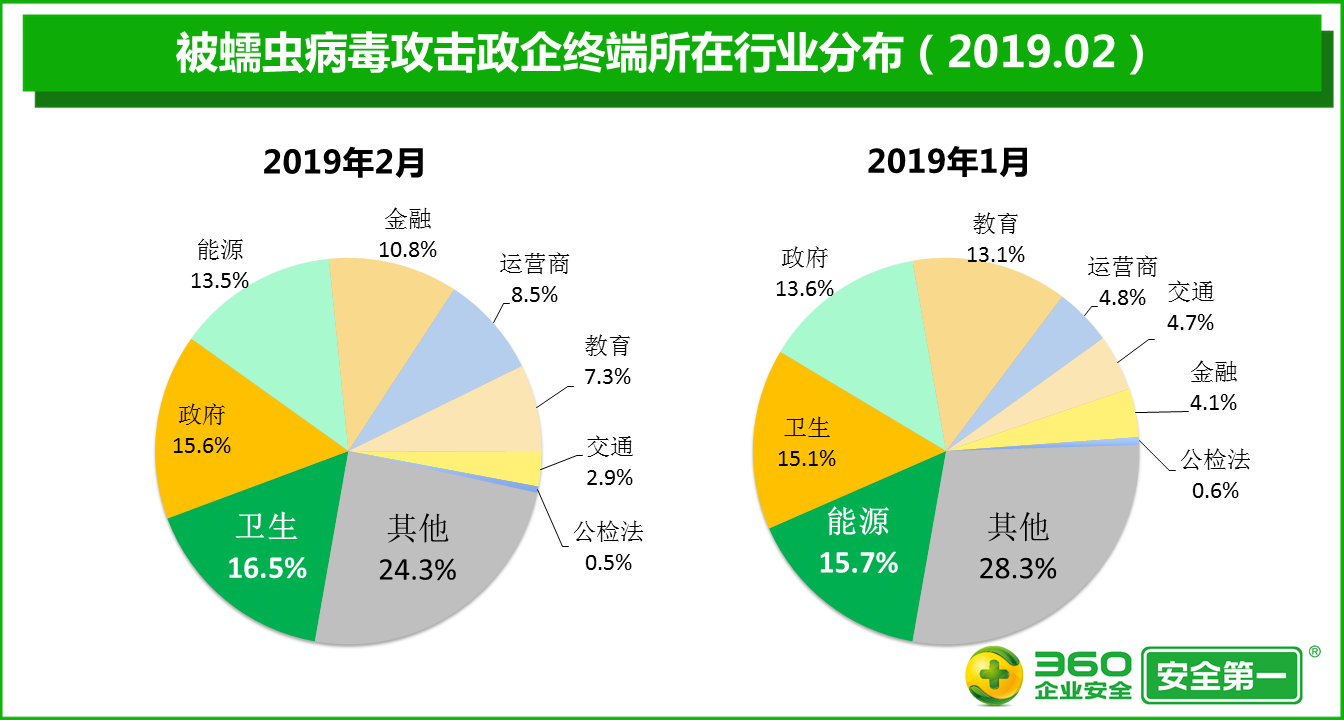
## 被攻击终端分析

2019年2月，被蠕虫病毒攻击的政企终端数量比1月减少9.9%。

在被蠕虫病毒攻击的政企终端中，北京地区最多，占比高达16.7%，被攻击终端的累计数量比1月减少2.4%；其次是广西，占比为10.9%，被攻击终端的累计数量比1月**增加31.8%**；广东排在第三位，占比为9.6%，被攻击终端的累计数量比1月减少20.4%。



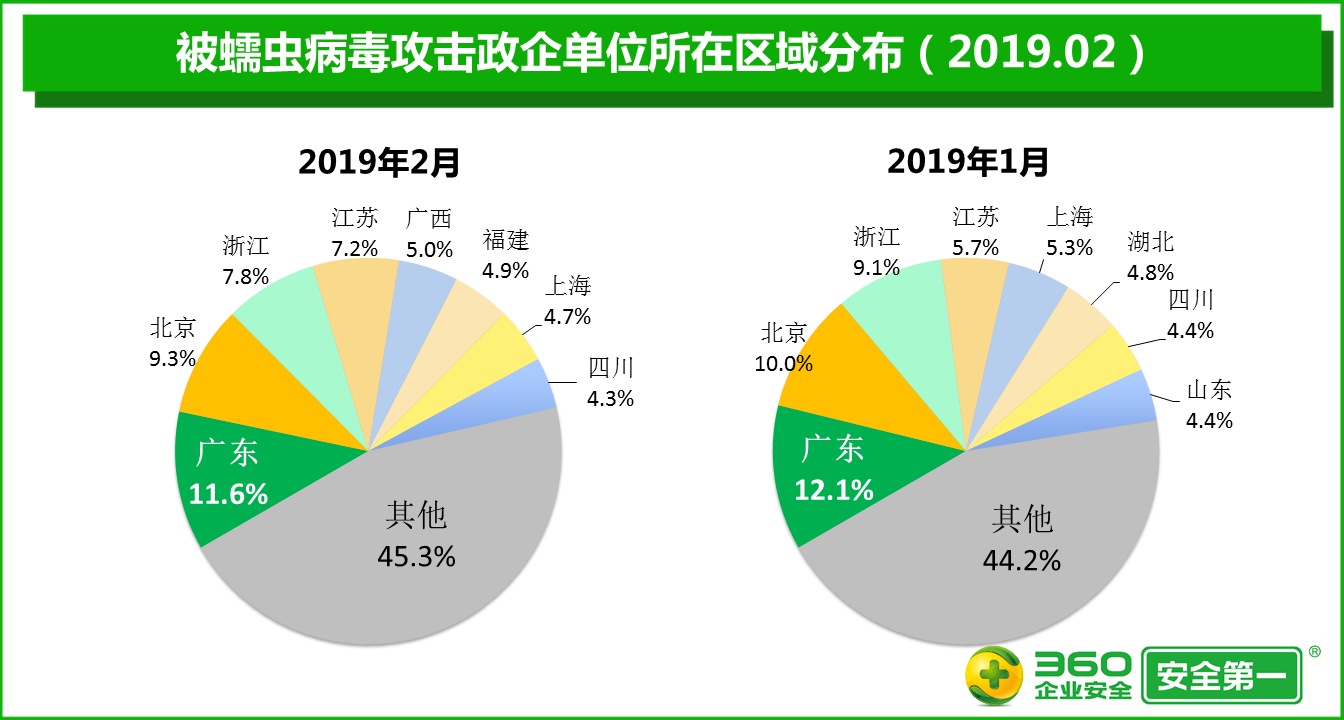
在被蠕虫病毒攻击的政企终端中，卫生行业最多，占比高达16.5%，被攻击终端的累计数量比1月减少1.5%；其次是政府行业，占比为15.6%，被攻击终端的累计数量比1月**增加2.7%**；能源行业排在第三位，占比为13.5%，被攻击终端的累计数量比1月减少22.3%。



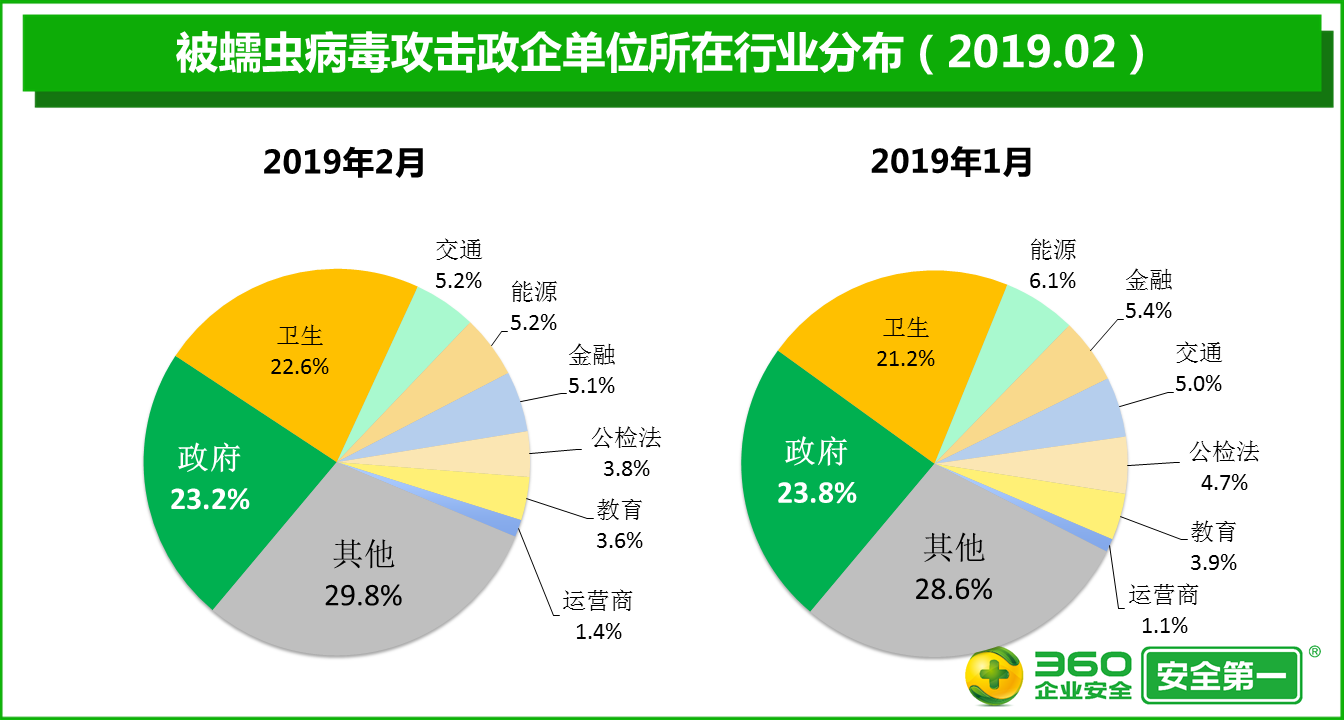
## 被攻击单位分析

2019年2月，被蠕虫病毒攻击的政企单位的绝对数量比1月减少22.9%。

在被蠕虫病毒攻击的政企单位中，广东地区最多，占比高达11.6%，被攻击单位的绝对数量比1月减少23.3%；其次是北京，占比为9.3%，被攻击单位的绝对数量比1月减少25.9%；浙江排在第三位，占比为7.8%，被攻击单位的绝对数量比1月减少31.2%。



在被蠕虫病毒攻击的政企单位中，政府行业最多，占比高达23.2%，被攻击单位的绝对数量比1月减少25.1%；其次是卫生行业，占比为22.6%，被攻击单位的绝对数量比1月减少17.8%；交通行业排在第三位，占比为5.2%，被攻击单位的绝对数量比1月减少19.4%。



# 2月热点病毒事件关注

### WinRAR爆出安全漏洞，5亿用户受到影响

近日，一款广泛使用的解压缩软件WinRAR被Check Point安全研究员Nadav Grossman爆出存在严重漏洞。这个漏洞存在一个第三方提供的用于解析ACE格式的unacev2.dll库文件中，该库文件在解压处理过程中存在一处目录穿越漏洞，允许解压过程中将文件写入启动文件夹中。攻击者可利用此漏洞构造一个恶意ACE压缩包，通过邮件、IM或网址链接欺骗或诱使受害者打开此压缩包时，在系统中植入恶意程序，使系统重启后执行恶意程序来控制受害者的计算机。该漏洞至今已经存在了近 19 年，初步评估全球有超过5亿用户受到WinRAR漏洞影响。

360天擎终端安全管理系统6.0及以上版本均未使用unacev2.dll库文件。

# 政企终端安全建议

360终端安全实验室提醒广大政企单位注意以下事项：

### 一、及时更新最新的补丁库

根据360企业安全集团终端安全多年的运营经验，病毒大规模爆发的原因大都是补丁安装不及时所致，因此及时更新补丁是安全运维工作的重中之重，但是很多政企单位由于业务的特殊性，对打补丁要求非常严格。360终端安全产品已经集成了先进的补丁管理功能，基于业界最佳的补丁管理实践，能够进行补丁编排，对补丁按照场景进行灰度发布，并且对微软更新的补丁进行了二次运营，解决了很多的兼容性问题，能够最大程度上解决补丁难打问题，帮助政企单位提升网络的安全基线。

### 二、杜绝弱口令问题

弱口令是目前主机安全入侵的第一大安全隐患，大部分大规模泛滥的病毒都内置了弱口令字典，能够轻松侵入使用弱口令的设备，应该坚决杜绝弱口令。360终端安全实验室建议登录口令尽量采用大小写、字母、数字、特殊符号混合的组合结构，且口令位数应足够长，并在登陆安全策略里限制登录失败次数、定期更换登录口令等。多台机器不使用相同或相似的口令，不使用默认的管理员名称如admin，不使用默认密码如admin、不使用简单密码如：admin123、12345678、666666等。

### 三、重要资料定期隔离备份

政企单位应尽量建立单独的文件服务器进行重要文件的存储备份，即使条件不允许也应对重要的文件进行定期隔离备份。

### 四、提高网络安全基线

掌握日常的安全配置技巧，如对共享文件夹设置访问权限，尽量采用云协作或内部搭建的wiki系统实现资料共享；尽量关闭3389、445、139、135等不用的高危端口，禁用Office宏等。如果没有这类安全经验，也可以使用360终端威胁评估产品（ETA）来对终端安全进行整体风险评估，360终端威胁评估产品（ETA）同时采用中国安全基本标准（CGDCC）和美国安全基线标准（USGCB），拥有数百种安全基线的检测能力和终端的深度安全检测能力，可以很好地帮助政企单位评估内部终端的安全。

### 五、保持软件使用的可信

平时要养成良好的安全习惯，不要点击陌生链接、来源不明的邮件附件，打开前使用安全扫描并确认安全性，尽量从官网等可信渠道下载软件，目前通过软件捆绑来传播的病毒也在逐渐增多，尤其是移动应用环境，被恶意程序二次打包的APP在普通的软件市场里非常常见。360终端安全产品家族中的软件管家，基于多年的安全软件运营经验，能够为政企单位量身定做一个可信的安全软件使用环境，避免员工任意安装软件而带来的病毒入侵风险。

### 六、选择正确的反病毒软件

随着威胁的发展，威胁开始了海量化和智能化趋势。对于海量化的威胁，就需要利用云计算的能力来对抗威胁海量化的趋势，因此在选择反病毒软件时，需要选择具备云查杀能力的反病毒软件。360终端安全的天擎基于云查杀技术和多年来威胁样本运营经验，已经具备150亿威胁样本的查杀能力，而且还首创了白名单技术，并拥有10亿量级的白名单库，而且内置云查杀、QVM、AVE、QEX、主动防御等多种引擎，能够深度解决政企网络的病毒威胁。

### 七、建立高级威胁深度分析与对抗能力

对于威胁的智能化趋势，很多智能威胁通过多种手段来躲避传统反病毒软件的查杀，这时就需要政企单位具备高级威胁深度分析和对抗能力。360终端安全响应系统基于业内公认的EDR思想，能够以终端的维度、事件的维度和时间的维度来分析网络中出现的高级威胁事件，能够为客户提供三维的立体威胁分析能力。后端利用大数据技术，能够监控终端上的所有灰文件的行为，内置AI模型，能够有效地识别传统反病毒软件识别不了的高级威胁入侵事件，帮助客户发现APT、流量、挖矿、勒索等新型威胁。

# 关于360终端安全实验室

360终端安全实验室由多名经验丰富的恶意代码研究专家组成，着力于常见病毒、木马、蠕虫、勒索软件等恶意代码的原理分析和研究，致力为中国政企客户提供快速的恶意代码预警和处置服务，在曾经流行的WannaCry、Petya、Bad Rabbit的恶意代码处置过程中表现优异，受到政企客户的广泛好评。

360终端安全实验室以360天擎新一代终端安全管理系统为依托，为政企客户提供简单有效的终端安全管理理念、完整的终端解决方案和定制化的安全服务，帮助客户解决内网安全与管理问题，保障政企终端安全。

# 关于360天擎新一代终端安全管理系统

360天擎新一代终端安全管理系统是360企业安全集团为解决政企机构终端安全问题而推出的一体化解决方案，是中国政企客户3300万终端的信赖之选。系统以功能一体化、平台一体化、数据一体化为设计理念，以安全防护为核心，以运维管控为重点，以可视化管理为支撑，以可靠服务为保障，提供了十六大基础安全能力，帮助政企客户构建终端威胁检测、终端威胁响应、终端威胁鉴定等高级威胁对抗能力，提升安全规划、战略分析和安全决策等终端安全治理能力。

特别的是，360企业安全还面向所有360天擎政企用户免费推出敲诈先赔服务：如果用户在开启了360天擎敲诈先赔功能后，仍感染了勒索软件，360企业安全将负责赔付赎金，为政企用户提供百万先赔保障，帮政企客户免除后顾之忧。



# 关于360天擎终端安全响应系统

360天擎终端安全响应系统（EDR）以行为引擎为核心，基于人工智能和大数据分析技术，对主机、网络、文件和用户等信息，进行深层次挖掘和多维度分析，结合云端优质威胁情报，将威胁进行可视化，并通过场景化和全局性的威胁追捕，对事件进行深度剖析，识别黑客/威胁意图，追踪威胁的扩散轨迹，评估威胁影响面，从而协同EPP、SOC、防火墙等安全产品，进行快速自动化的联动响应，将单次响应转化为安全策略，控制威胁蔓延，进行持续遏制，全面提升企业安全防护能力。