3月政企终端安全态势分析报告

2019 年 4 月 8 日

目　　录

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。

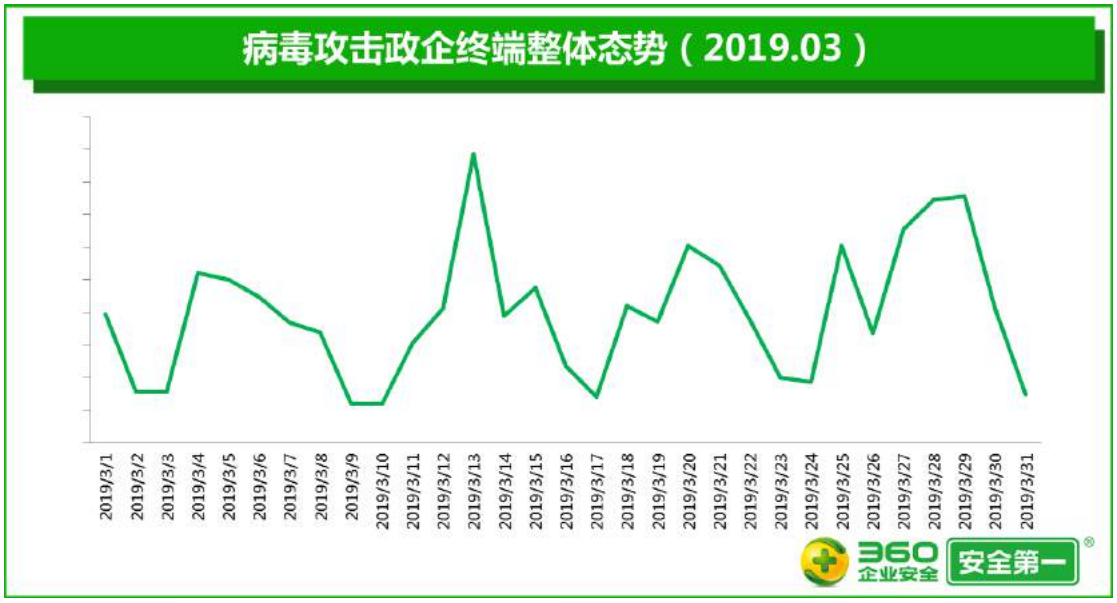
本期报告的监测时间为 **2019 年 3 月 1 日 ~ 3 月 31 日**。

第一章　病毒攻击政企整体分析

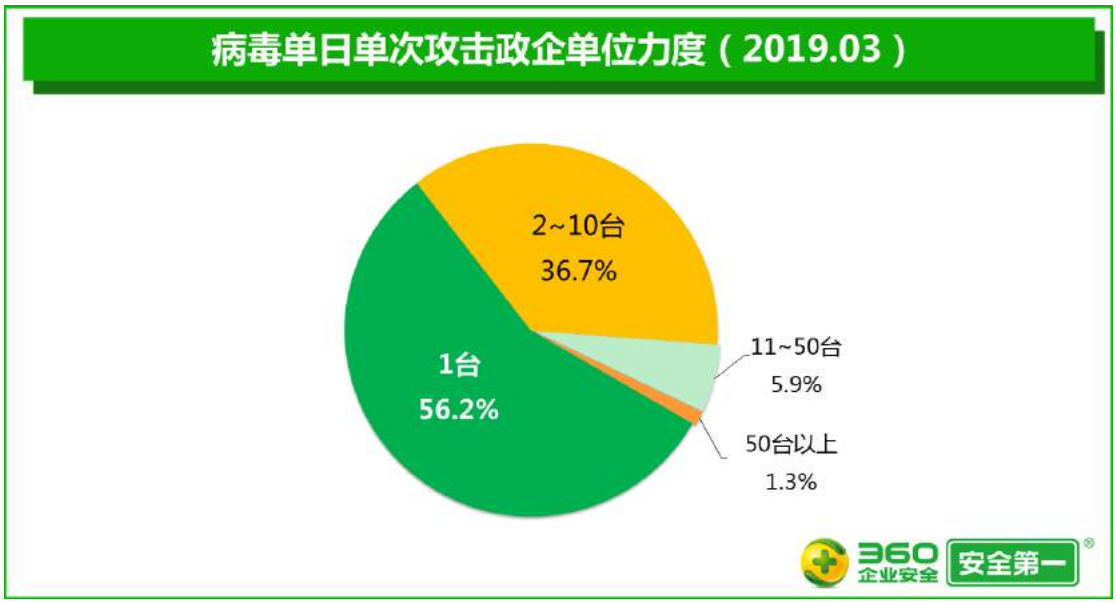
360 终端安全实验室监测数据显示，2019 年 3 月，政企单位被各类病毒攻击的事件数量比 2 月**增加 61.3%**，被病毒攻击的政企终端的累计数量比 2 月**增加 44.3%**，被病毒攻击的政企单位的绝对数量比 2 月**增加 44.7%**。

一、　攻击整体态势

2019 年 3 月，病毒攻击的最高峰出现在 **3 月 13 日（星期三）**，最低谷则出现在 **3 月 9 日（星期六）**。

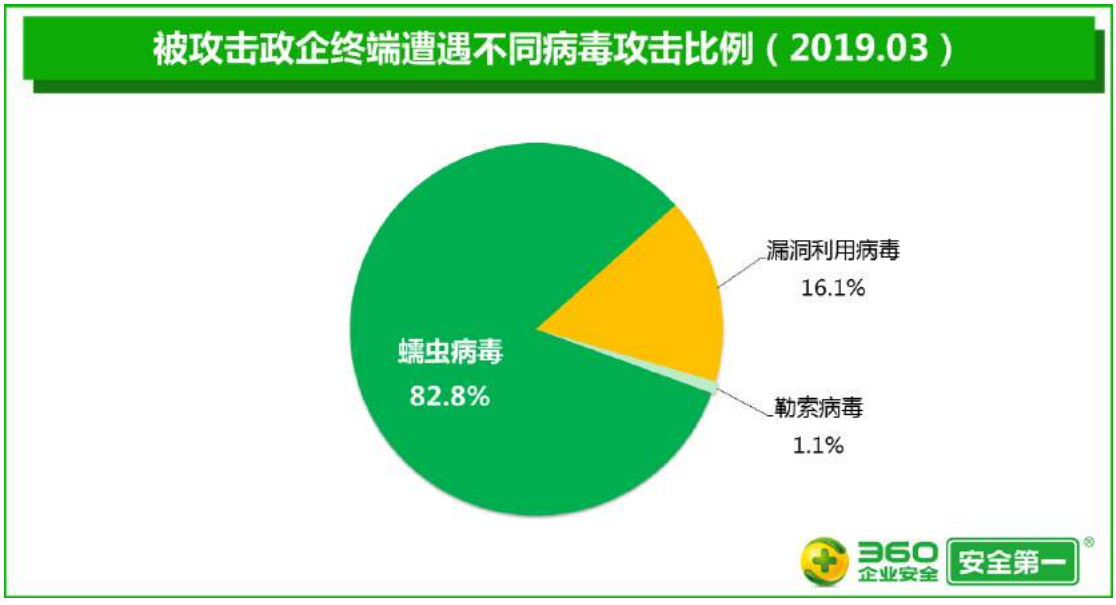


2019 年 3 月，被病毒攻击的事件数量比 2 月增加 61.3%。其中，病毒单日单次攻击政企单位的终端数仅为 1 台的事件比 2 月增加 57.5%，占 3 月攻击事件总数的 56.2%；单日单次攻击终端数为 2~10 台的事件比 2 月增加 65.4%，占 3 月攻击事件总数的 36.7%；单日单次攻击终端数为 11~50 台的事件比 2 月增加 91.5%，占 3 月攻击事件总数的 5.9%；单日单次攻击 50 台以上终端的事件比 2 月增加 17.5%，占 3 月攻击事件总数的 1.3%。

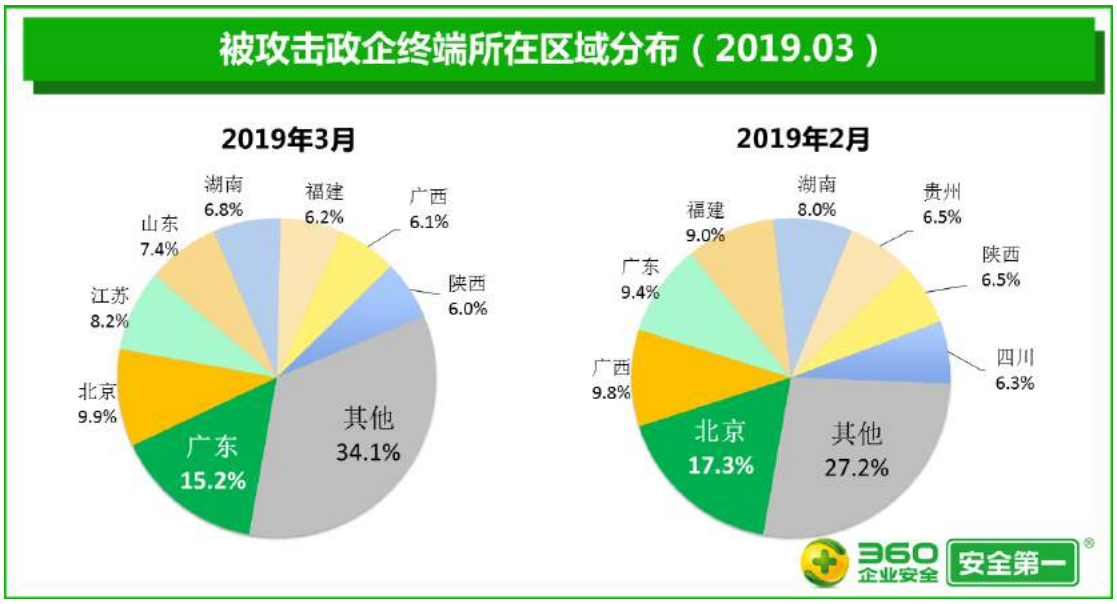


二、 被攻击终端分析

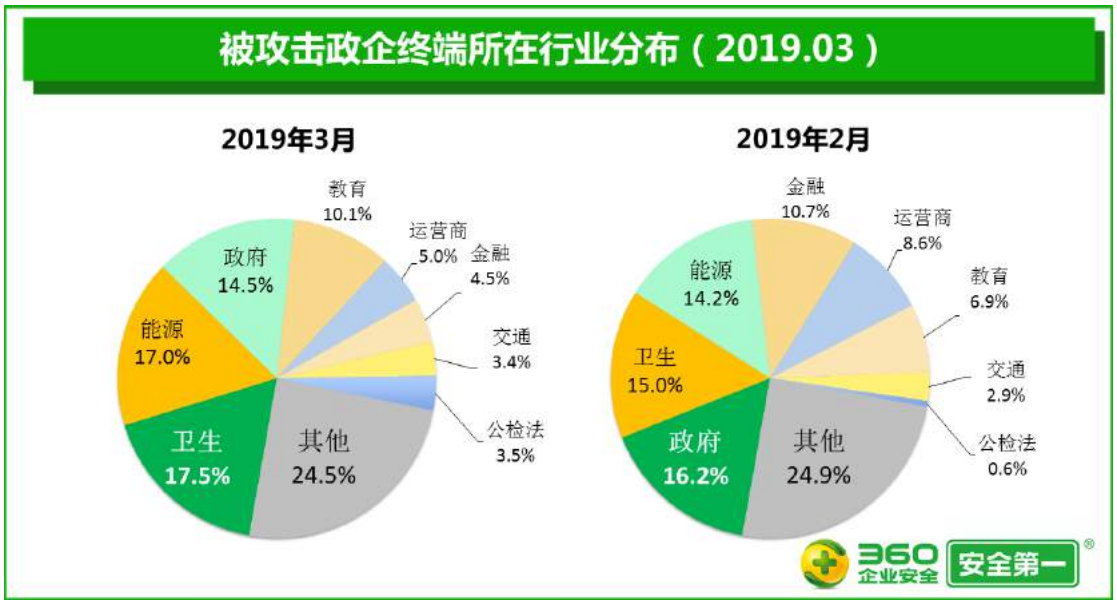
2019 年 3 月，被病毒攻击的政企终端的累计数量比 2 月增加 44.3%。其中，遭遇蠕虫病毒攻击的政企终端的累计数量比 2 月增加 34.9%，占 3 月被攻击政企终端的 82.8%；遭遇漏洞利用病毒攻击的政企终端的累计数量比 2 月**增加 122.4%**，占 3 月被攻击政企终端的 16.1%；遭遇勒索病毒攻击的累计数量比 2 月增加 61.9%，占 3 月被攻击政企终端的 1.1%。



在被病毒攻击的政企终端中，广东地区最多，占比高达 15.2%，被攻击终端的累计数量比 2 月**增加 134.5%**；其次是北京，占比为 9.9%，被攻击终端的累计数量比 2 月**减少 17.6%**；江苏排在第三位，占比为 8.2%，被攻击终端的累计数量比 2 月**增加 236.5%**。



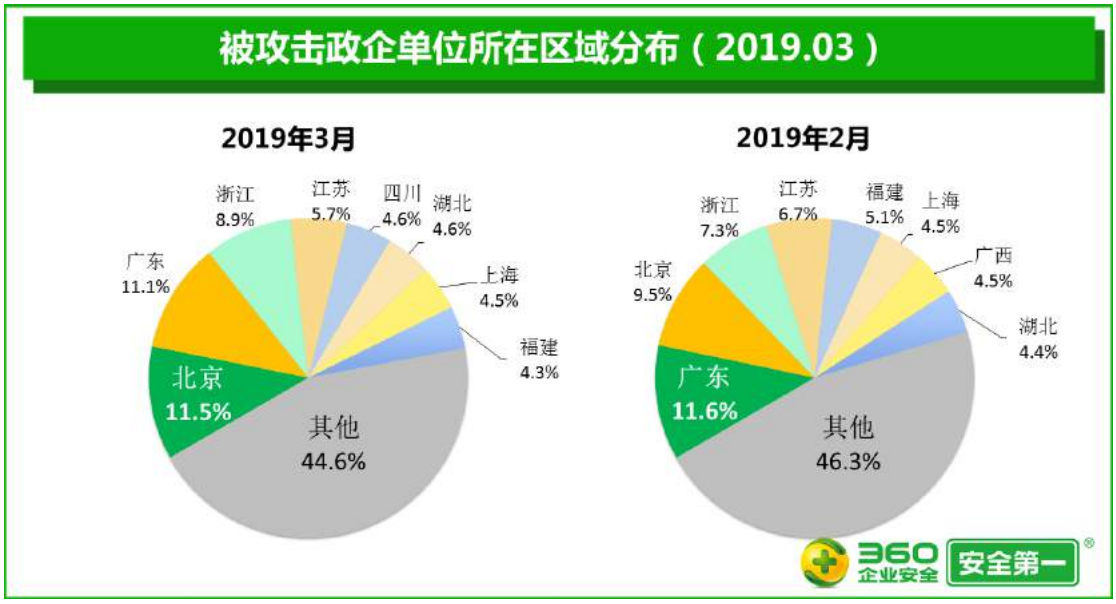
在被病毒攻击的政企终端中，卫生行业最多，占比高达 17.5%，被攻击终端的累积数量比 2 月增加 67.6%；其次是能源行业，占比为 17.0%，被攻击终端的累积数量比 2 月增加 73.7%；政府行业排在第三位，占比为 14.5%，被攻击终端的累积数量比 2 月增加 29.2%。



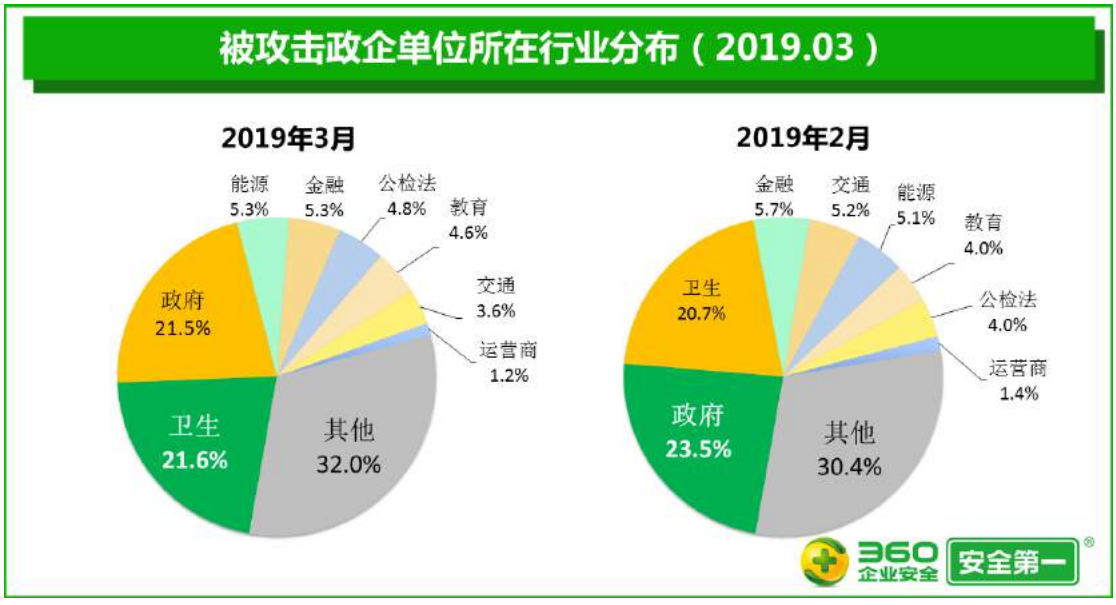
三、 被攻击单位分析

2019 年 3 月，被病毒攻击的政企单位的绝对数量比 2 月增加 44.7%。在受到病毒攻击的政企单位中，87.8%的单位遭到蠕虫病毒的攻击，绝对数量比 2 月增加 44.5%；31.3%的单位遭到漏洞利用病毒的攻击，绝对数量比 2 月**增加 73.8%**；5.4%的单位遭到勒索病毒的攻击，绝对数量比 2 月增加 32.4%。

在被病毒攻击的政企单位中，北京地区最多，占比高达 11.5%，被攻击单位的绝对数量比 2 月**增加 78.7%**；其次是广东，占比为 11.1%，被攻击单位的绝对数量比 2 月增加 41.3%；浙江排在第三位，占比为 8.9%，被攻击单位的绝对数量比 2 月**增加 79.3%**。



在被病毒攻击的政企单位中，卫生行业最多，占比高达 21.6%，被攻击单位的绝对数量比 2 月增加 51.5%；其次是政府行业，占比为 21.5%，被攻击单位的绝对数量比 2 月增加 32.4%；能源和金融行业并列第三，占比均为 5.3%，被攻击单位的绝对数量比 2 月分别增加 50.0% 和 33.3%。

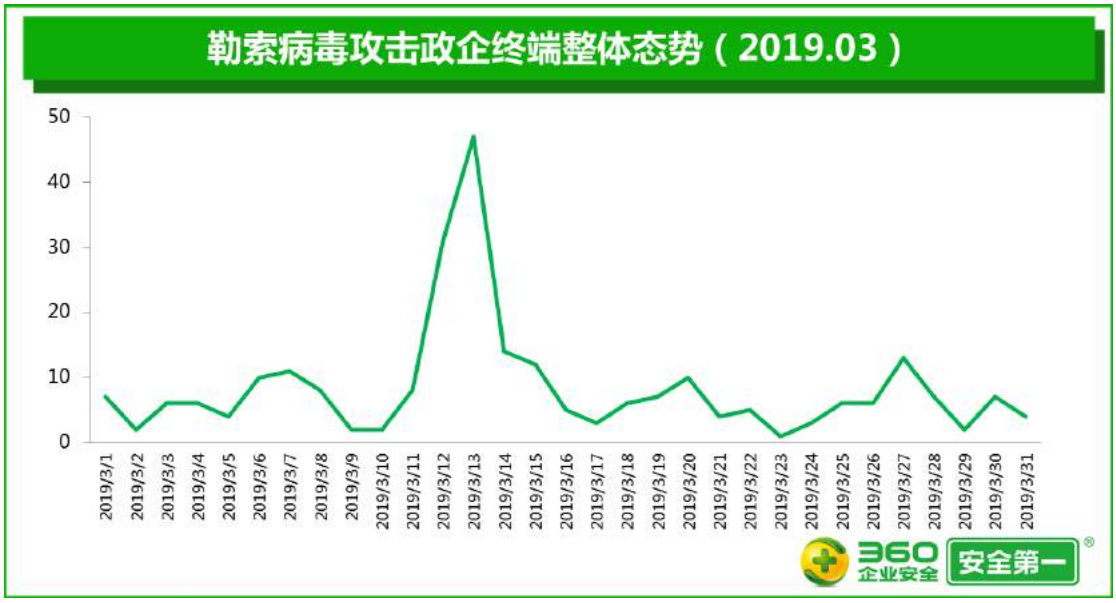


第二章　勒索病毒攻击政企分析

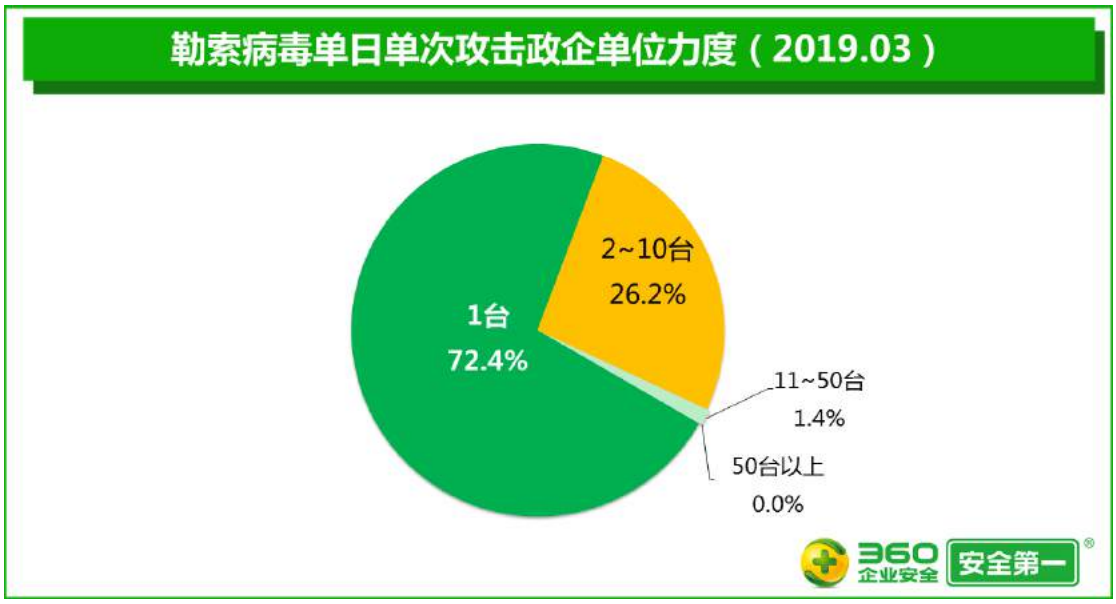
360 终端安全实验室监测数据显示，2019 年 3 月，政企单位被勒索病毒攻击的事件数量比 2 月增加 19.8%，被勒索病毒攻击的政企终端的累计数量比 2 月增加 61.9%，被勒索病毒攻击的政企单位的绝对数量比 2 月增加 32.4%。

一、　攻击整体态势

2019 年 3 月，勒索病毒攻击的最高峰出现在 **3 月 13 日（星期三）**，最低谷则出现在 **3 月 23 日（星期六）**。



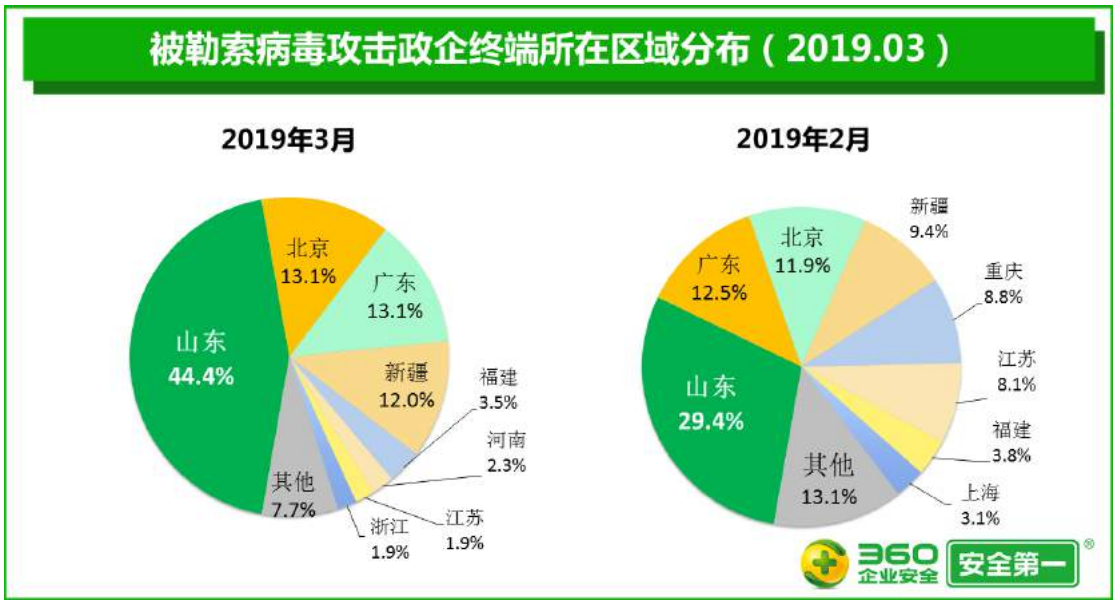
2019 年 3 月，被勒索病毒攻击的事件数量比 2 月增加 19.8%。其中，单日单次攻击政企单位的终端数仅为 1 台的事件比 2 月增加 15.4%，占 3 月勒索病毒攻击事件总数的 72.4%；单日单次攻击终端数为 2~10 台的事件比 2 月增加 26.7%，占 3 月勒索病毒攻击事件总数的 26.2%；单日单次攻击终端数为 11~50 台的事件占 3 月勒索病毒攻击事件总数的 1.4%；没有监测到单日单次攻击终端数超过 10 台以上的事件。



二、 被攻击终端分析

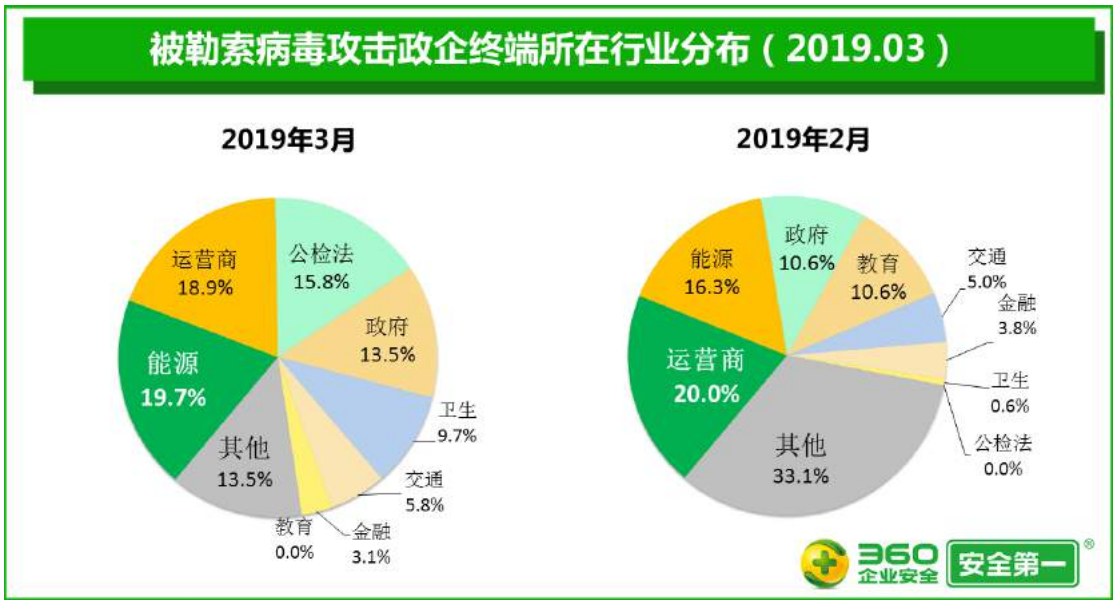
2019 年 3 月，被勒索病毒攻击的政企终端的累计数量比 2 月增加 61.9%。

在被勒索病毒攻击的政企终端中，山东地区最多，占比高达 44.4%，被攻击终端的累计数量比 2 月**增加 144.7%**；其次是北京和广东，占比均为 13.1%，被攻击终端的累计数量比 2 月分别增加 78.9%和 70.0%。



在被勒索病毒攻击的政企终端中，能源行业最多，占比高达 19.7%，而 2 月该行业只有极少量终端受到勒索病毒攻击；其次是运营商行业，占比为 18.9%，被攻击终端的累计数量比 2 月增加 88.5%；公检法行业排在第三位，占比为 15.8%，被攻击终端的累计数量比 2 月

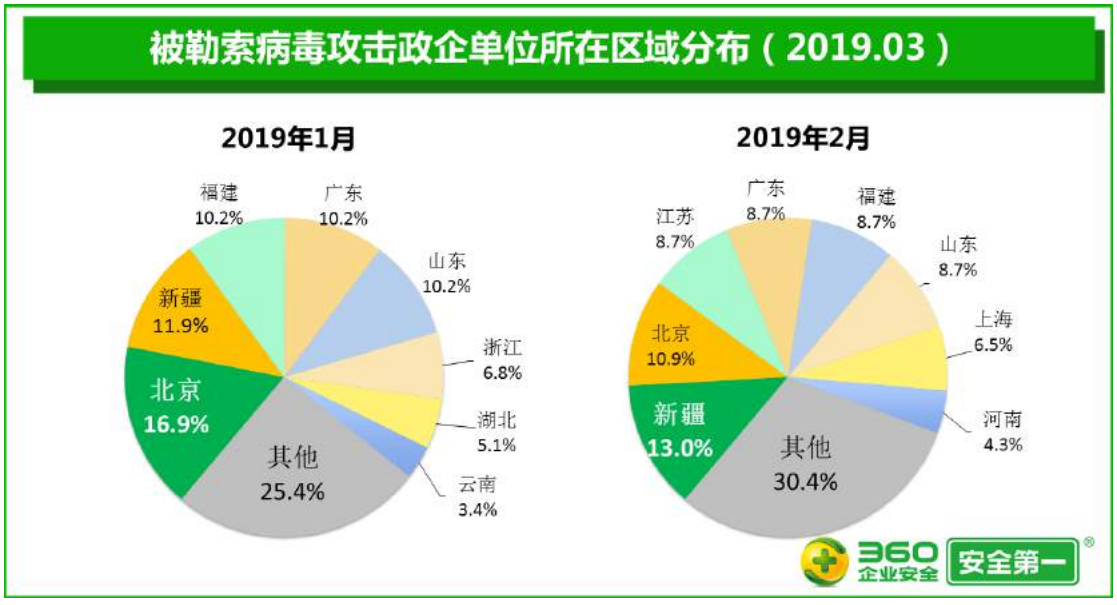
增加 28.1%。



三、 被攻击单位分析

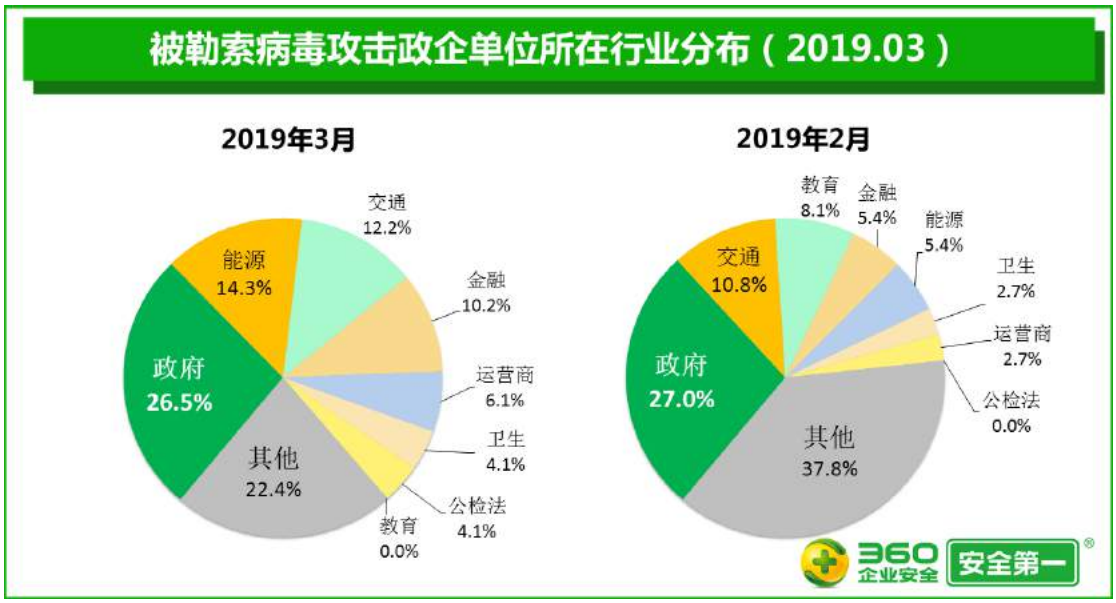
2019 年 3 月，被勒索病毒攻击的政企单位的绝对数量比 2 月增加 32.4%。

在被勒索病毒攻击的政企单位中，北京地区最多，占比高达 16.9%，被攻击单位的绝对数量比 2 月**增加 100%**；其次是新疆，占比为 11.9%，被攻击单位的绝对数量比 2 月增加 16.7%；福建、广东、山东并列第三，占比均为 10.2%。



在被勒索病毒攻击的政企单位中，政府行业最多，占比高达 26.5%，被攻击单位的绝对

数量比 2 月增加 30.0%；其次是能源行业，占比为 14.3%，被攻击单位的绝对数量比 2 月**增加 250.0%**；交通行业排在第三位，占比为 12.2%，被攻击单位的绝对数量比 2 月增加 50.0%。



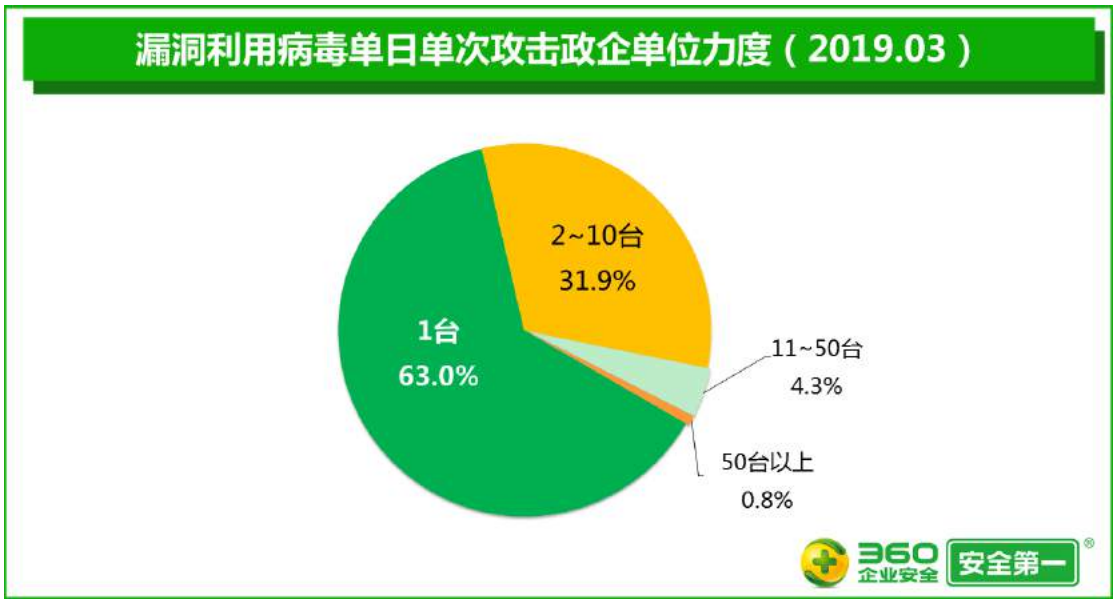
第三章　漏洞利用病毒攻击政企分析

360 终端安全实验室监测数据显示，2019 年 3 月，政企单位被漏洞利用病毒攻击的事件数量比 2 月**增加 92.9%**，被漏洞利用病毒攻击的政企终端的累计数量比 2 月**增加 124.4%**，被漏洞利用病毒攻击的政企单位的绝对数量比 2 月**增加 73.8%**。

一、　攻击整体态势

2019 年 3 月，漏洞利用病毒攻击的最高峰出现在 **3 月 25 日（星期一）**，最低谷则出现在 **3 月 10 日（星期日）**。

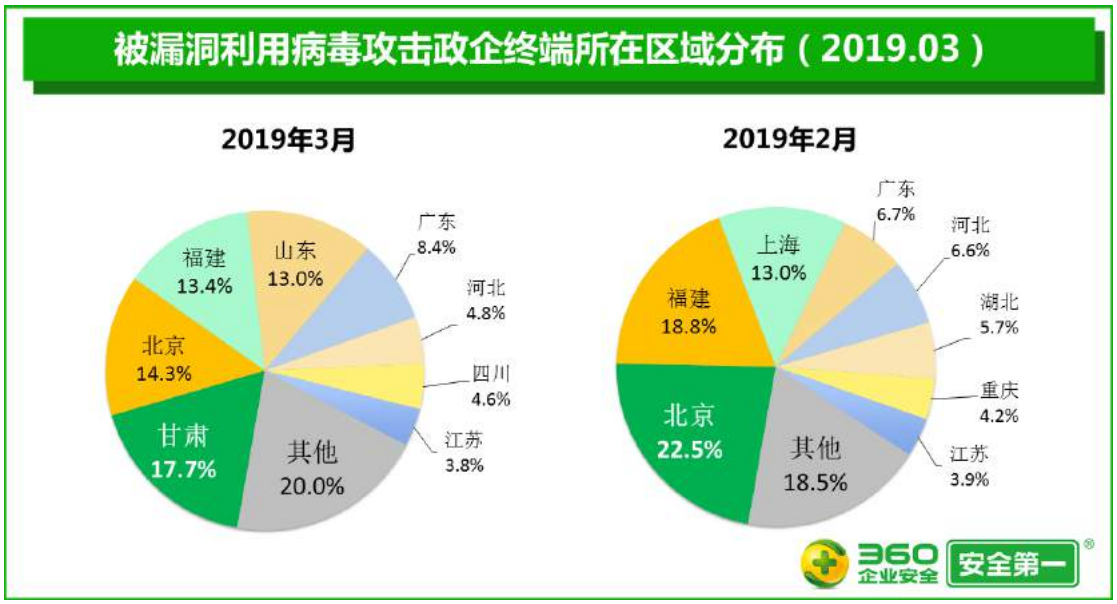
2019 年 3 月，被漏洞利用病毒攻击的事件数量比 2 月增加 92.9%。其中，单日单次攻击政企单位的终端数仅为 1 台的事件比 2 月增加 91.4%，占 3 月漏洞利用病毒攻击事件总数的 63.0%；单日单次攻击终端数为 2~10 台的事件比 2 月增加 98.1%，占 3 月漏洞利用病毒攻击事件总数的 31.9%；单日单次攻击终端数为 11~50 台的事件比 2 月增加 78.3%，占 3 月漏洞利用病毒攻击事件总数的 4.3%；单日单次攻击 50 台以上终端的事件比 2 月增加 100.0%，占 3 月漏洞利用病毒攻击事件总数的 0.8%。



二、 被攻击终端分析

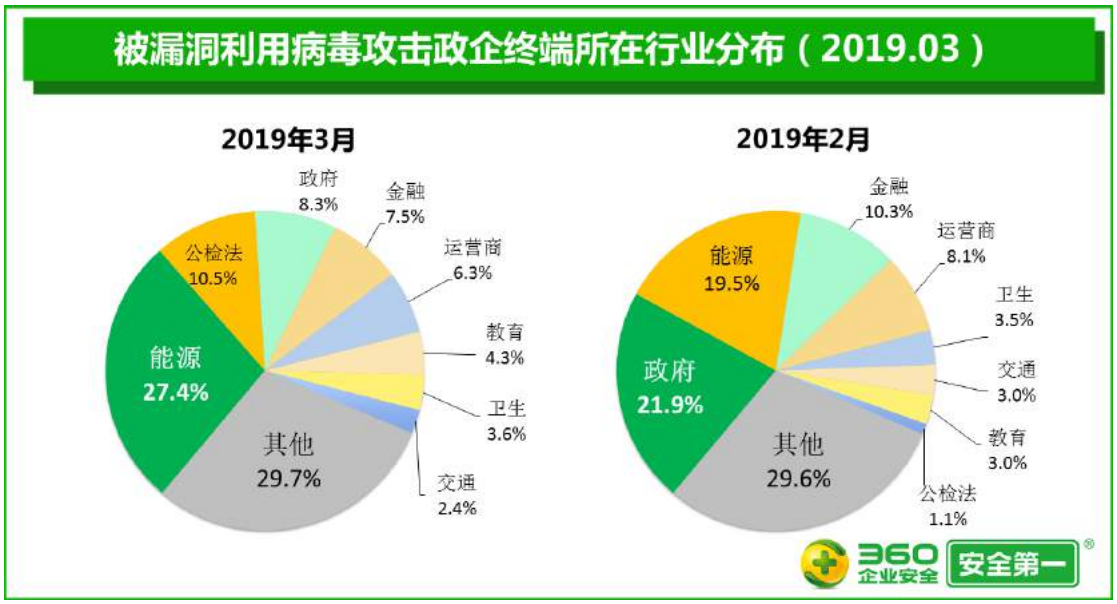
2019 年 3 月，被漏洞利用病毒攻击的政企终端的累计数量比 2 月增加 73.8%。

在被漏洞利用病毒攻击的政企终端中，甘肃地区最多，占比高达 17.7%，被攻击终端的累计数量比 2 月**增加 139 倍**；其次是北京，占比为 14.3%，被攻击终端的累计数量比 2 月增加 40.9%；福建排在第三位，占比为 13.4%，被攻击终端的累计数量比 2 月增加 58.8%。



在被漏洞利用病毒攻击的政企终端中，能源行业最多，占比高达 27.4%，被攻击终端的累计数量比 2 月增加 212.4%；其次是公检法行业，占比为 10.5%，被攻击终端的累计数量比 2 月**增加 20.8 倍**；政府行业排在第三位，占比为 8.3%，被攻击终端的累计数量比 2 月**减**

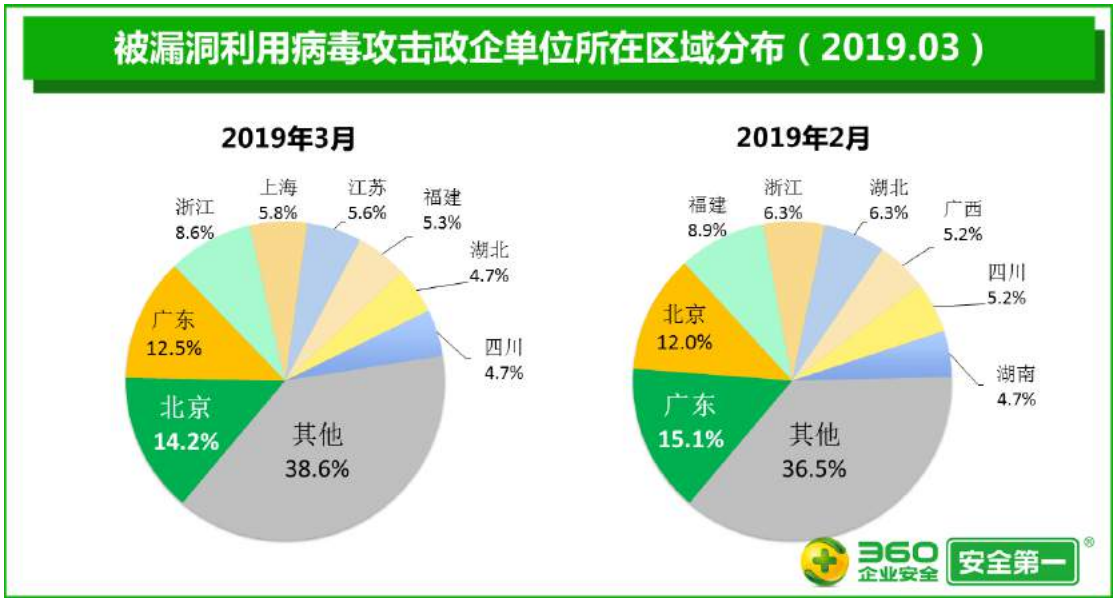
少 15.9%。



三、 被攻击单位分析

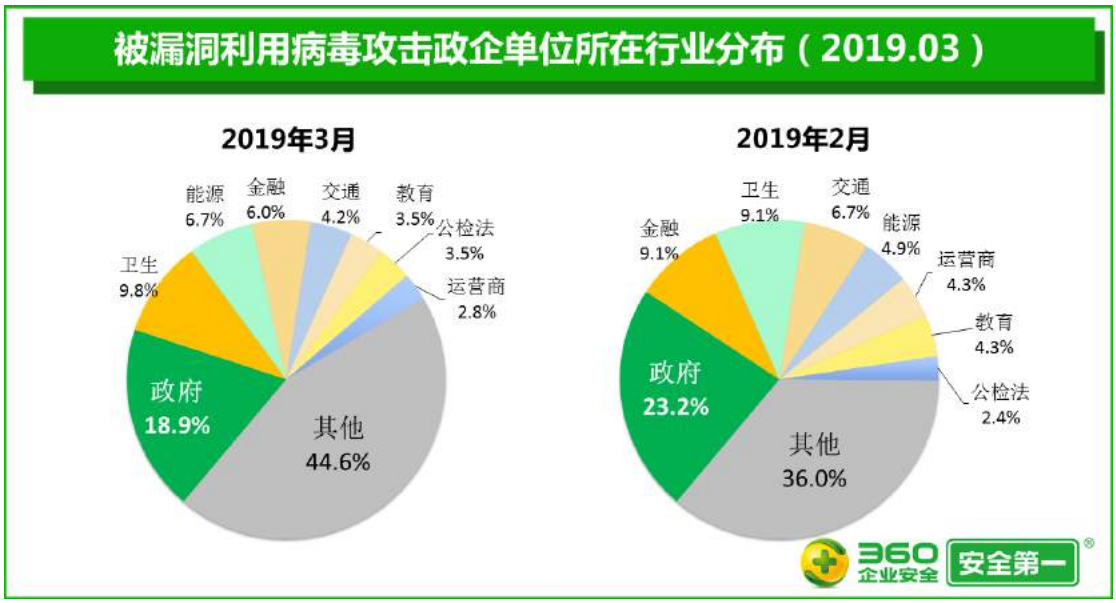
2019 年 3 月，被漏洞利用病毒攻击的政企单位的绝对数量比 2 月增加 73.8%。

在被漏洞利用病毒攻击的政企单位中，北京地区最多，占比高达 14.2%，被攻击单位的绝对数量比 2 月增加 121.7%；其次是广东，占比为 12.5%，被攻击单位的绝对数量比 2 月增加 55.2%；浙江排在第三位，占比为 8.6%，被攻击单位的绝对数量比 2 月**增加 158.3%**。



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 18.9%，被攻击单位的

绝对数量比 2 月增加 42.1%；其次是卫生行业，占比为 9.8%，被攻击单位的绝对数量比 2 月增加86.7%；能源行业排在第三位，占比为6.7%，被攻击单位的绝对数量比2月**增加137.5%**。

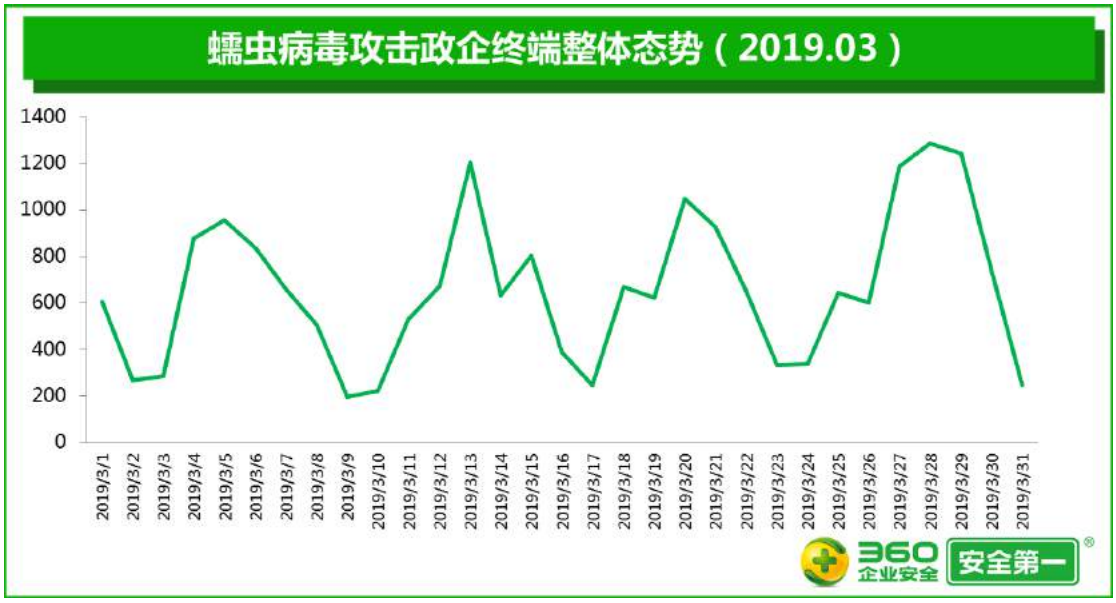


第四章　蠕虫病毒攻击政企分析

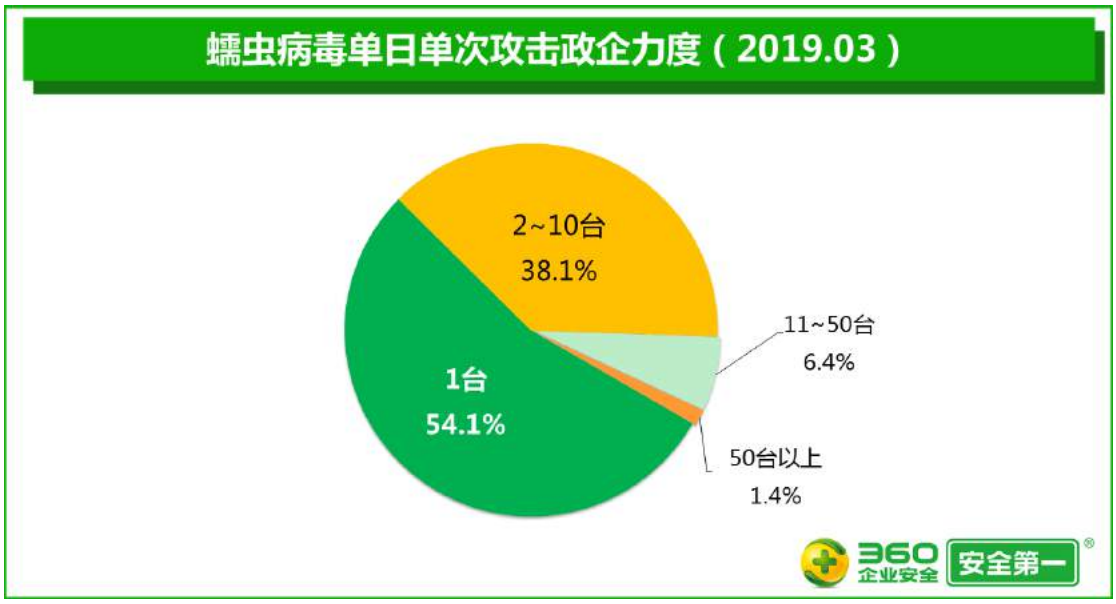
360 终端安全实验室监测数据显示，2019 年 3 月，政企单位被蠕虫病毒攻击的事件数量比 2 月增加 57.3%，被蠕虫病毒攻击的政企终端的累计数量比 2 月增加 34.9%，被蠕虫病毒攻击的政企单位的绝对数量比 2 月增加 44.5%。

一、　攻击整体态势

2019 年 3 月，蠕虫病毒攻击的最高峰出现在 **3 月 28 日（星期四）**，最低谷则出现在 **2 月 3 日（星期六）**。



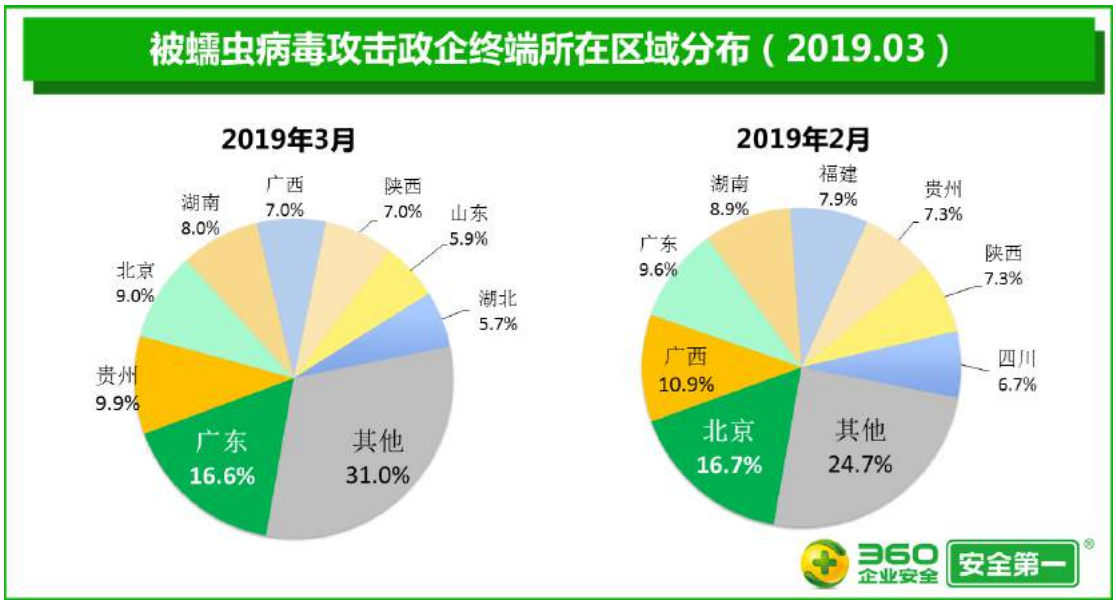
2019 年 3 月，被蠕虫病毒攻击的事件数量比 2 月增加 57.3%。其中，单日单次攻击政企单位的终端数仅为 1 台的事件比 2 月增加 52.9%，占 3 月攻击事件总数的 54.1%；单日单次攻击终端数为 2~10 台的事件比 2 月增加 61.5%，占 3 月攻击事件总数的 38.1%；单日单次攻击终端数为 11~50 台的事件比 2 月**增加 92.3%**，占 3 月攻击事件总数的 6.4%；单日单次攻击 50 台以上终端的事件比 2 月增加 11.3%，占 3 月攻击事件总数的 1.4%。



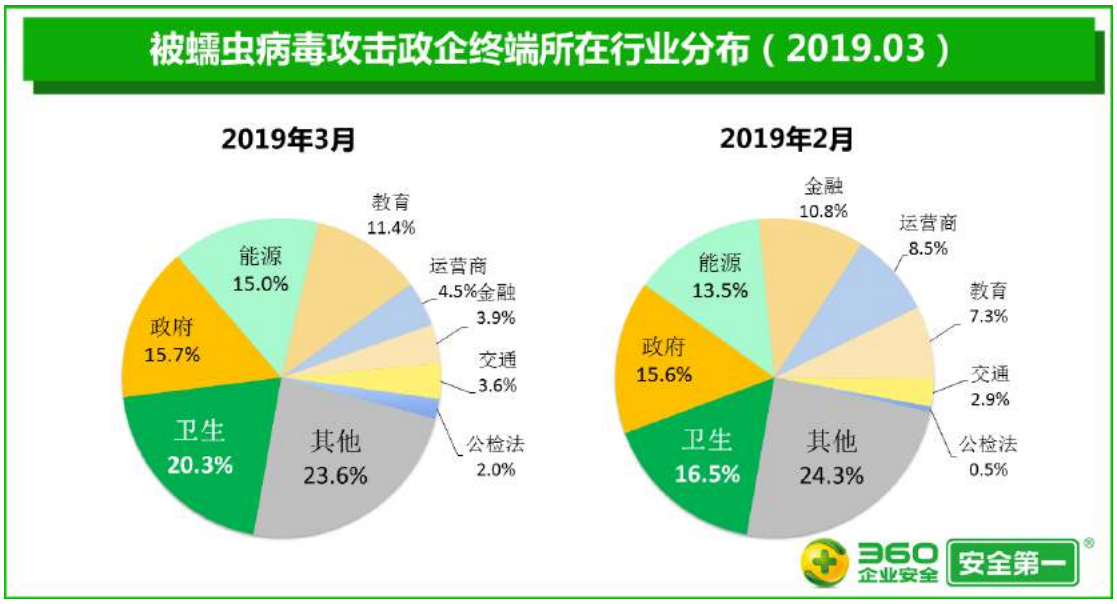
二、 被攻击终端分析

2019 年 3 月，被蠕虫病毒攻击的政企终端数量比 2 月增加 34.9%。

在被蠕虫病毒攻击的政企终端中，广东地区最多，占比高达 16.6%，被攻击终端的累计数量比 2 月**增加 131.7%**；其次是贵州，占比为 9.9%，被攻击终端的累计数量比 2 月增加 82.4%；北京排在第三位，占比为 9.0%，被攻击终端的累计数量比 2 月**减少 27.6%**。



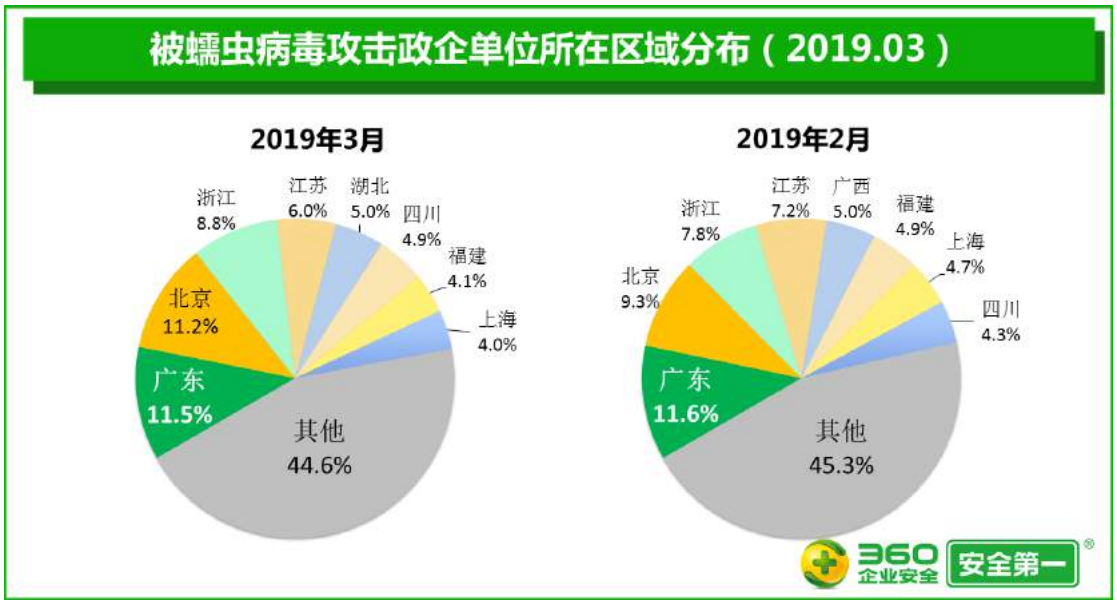
在被蠕虫病毒攻击的政企终端中，卫生行业最多，占比高达 20.3%，被攻击终端的累计数量比 2 月**增加 65.1%**；其次是政府行业，占比为 15.7%，被攻击终端的累计数量比 2 月增加 36.1%；能源行业排在第三位，占比为 15.0%，被攻击终端的累计数量比 2 月增加 49.9%。



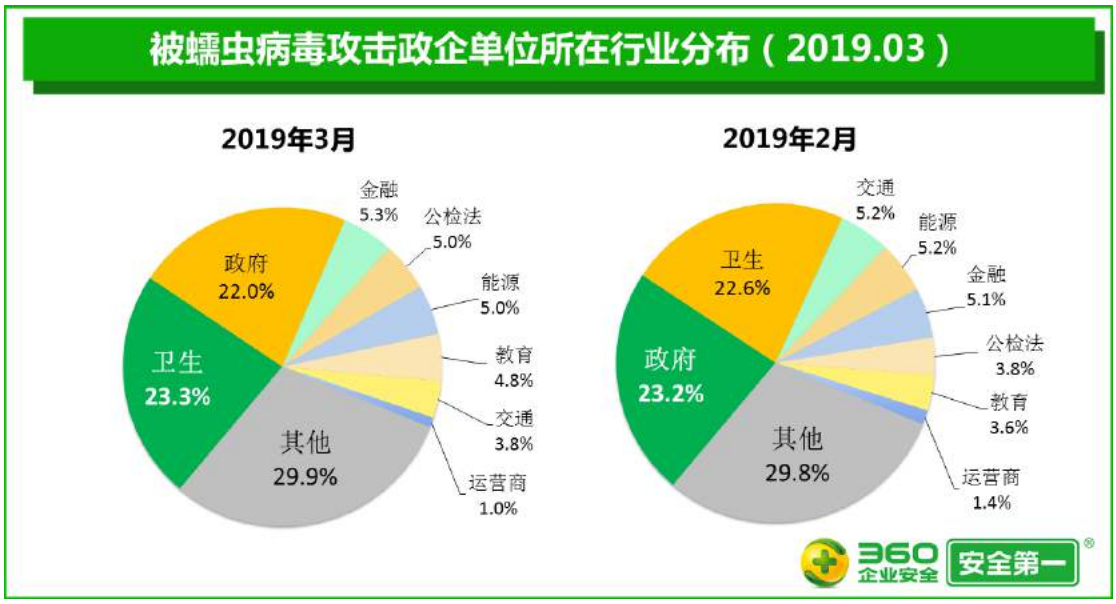
三、 被攻击单位分析

2019 年 3 月，被蠕虫病毒攻击的政企单位的绝对数量比 2 月增加 44.7%。

在被蠕虫病毒攻击的政企单位中，广东地区最多，占比高达 11.5%，被攻击单位的绝对数量比 2 月增加 43.0%；其次是北京，占比为 11.2%，被攻击单位的绝对数量比 2 月**增加 74.6%**；浙江排在第三位，占比为 8.8%，被攻击单位的绝对数量比 2 月增加 64.2%。



在被蠕虫病毒攻击的政企单位中，卫生行业最多，占比高达 23.3%，被攻击单位的绝对数量比 2 月增加 48.8%；其次是政府行业，占比为 22.0%，被攻击单位的绝对数量比 2 月增加 37.5%；金融行业排在第三位，占比为 5.3%，被攻击单位的绝对数量比 2 月增加 50.0%。


被蠕虫病毒攻击政企单位所在行业分布（2019.03）
2019年3月
金融 5.3%
公检法 5.0%
能源 5.0%
教育 4.8%
交通 3.8%
运营商 1.0%
其他 29.9%
卫生 23.3%
政府 22.0%
2019年2月
交通 5.2%
能源 5.2%
金融 5.1%
公检法 3.8%
教育 3.6%
运营商 1.4%
其他 29.8%
政府 23.2%
卫生 22.6%
360 企业安全 安全第一

第五章　3 月热点病毒事件关注

GandCrab V5.2 利用恐吓主题钓鱼邮件传播

近期，360 威胁情报中心捕获到一起针对中文使用者的钓鱼邮件。该邮件带有一个压缩包，压缩包内是最新的 GandCrab 5.2 勒索软件。

由于 Gandcrab5.2 版本会通过垃圾电子邮件分发，因此建议用户不要打开任何未知来源的电子邮件，尤其是不要打开附件。即使附件来自常用联系人，也建议您在打开之前使用 360 天擎对其进行扫描，以确保不包含任何恶意文档或文件。

多家医院服务器受到 GlobeImposter 勒索病毒攻击

3 月 10 日，360 安全服务应急响应团队接到某省多家医院服务器遭受攻击的应急救援，该省同一卫生专网遭到 GlobeImposter V3 勒索病毒攻击，多台业务服务器遭黑客加密勒索，影响该省近 60 家市县医院。

从截获的样本和勒索攻击溯源分析来看，GlobeImposter V3 的攻击手段和加密方式和以往版本相比并没有新的变化：攻击手段依然是定向爆破和投递勒索，通过 RDP 远程桌面弱密码攻击服务器。

首个利用 WinRAR 漏洞传播的未知勒索软件出现

3 月 17 日，360 威胁情报中心截获了首个利用 WinRAR 漏洞（CVE-2018-20250）传播未知恶意勒索软件的 ACE 文件。该恶意压缩文件名为 vk_4221345.rar，当受害者在本地计算机上通过 WinRAR 解压该文件后便会触发漏洞，漏洞利用成功后会将内置的勒索软件写入到用户计算机启动项目录中，当用户重启或登录系统都会执行该勒索软件从而导致重要资料被加密。

由于该勒索软件执行后并没有保存生成的 RSA 公私钥，也没有通过其他渠道将公私钥信息发送给攻击者，所以即便受害者向勒索软件作者支付相应的赎金也不可能解密文件。360 威胁情报中心提醒用户，如遇到类似的勒索软件攻击，切忌支付赎金，并再次提醒广大用户务必对此高危漏洞做好十足的防护措施。

海德鲁公司多个工厂遭遇 LockerGoga 勒索病毒攻击

3 月 18 日，世界最大的综合性铝业集团之一的挪威海德鲁公司（Norsk Hydro）在美国

和欧洲的多个工厂遭受勒索软件攻击，导致 IT 系统无法使用，造成多个工厂关闭和部分工厂切换为手动运营模式。该公司临时关闭多个工厂，并将挪威、卡塔尔和巴西等国家的工厂运营模式部分改为“可以使用的”手动模式，以缓解对生产的影响。该勒索病毒似乎还攻击了美国的化工企业 Hexion 和 Momentive，以至于部分员工无法正常登陆系统。

360 威胁情报中心对该勒索病毒（LockerGoga）进行了进一步的详细分析，发现该勒索病毒极可能为定向攻击的破坏性勒索病毒，会加密各种类型的文件，包括 PE 文件、系统目录以及启动目录下的文件，因此具有很强的破坏性。

第六章　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 4000 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。