2018年

网络安全应急响应分析报告



2019年01月16日

主要观点

* 凡事预则立，不预则废。网络安全应急响应是为了对网络安全有所认识、有所准备，以便在遇到突发网络安全事件时做到有序应对、妥善处理。
* 2018年全年，全国应急响应服务需求呈逐步上升趋势，自2017年“永恒之蓝”勒索病毒爆发以来，针对政府、金融等行业的攻击层出不穷，我国网络安全态势严峻。
* 政府、医疗、金融和教育培训行业是2018年黑客攻击的主要目标，传媒、银行、科研等关键基础设施行业也面临着越来越多的安全威胁风险。网络安全防护存在短板、人员缺乏安全意识是网络攻击有机可乘的重要原因，应大力倡导各行各业，通过宣传教育、攻防演练等方式，加强网络安全意识培训。
* 2018年，应急响应处理安全事件中，勒索病毒攻击是政府机构、大中型企业服务器、终端失陷的重要原因之一，面对勒索病毒的频繁变种，政府机构、大中型企业应打破传统安全防护观念，多角度看待安全问题，实现安全能力的大幅提升与技术体系的全面升级。
* 网络安全应急响应工作应成为政府机构、大中型企业日常管理的一部分。勒索病毒等影响广泛的网络安全事件可能扩大为全行业、全国甚至全球性问题，网络安全应急响应需要政府机构、安全厂商、企业加强合作、取长补短，必要时进行跨国协作。
* 网络安全厂商提供的网络安全应急服务已经成为政府机构、大中型企业有效应对网络安全突发事件的重要手段。网络安全应急服务应该基于数据驱动、安全能力服务化的安全服务运营理念，结合云端大数据和专家诊断，为客户提供安全运维、预警检测、持续响应、数据分析、咨询规划等一系列的安全保障服务。

摘 要

* 2018年全年360安服团队共参与和处置了717起网络安全应急响应事件.
* 行业应急处置排在前三位的分别为公检法（66起）、政府部门（63起）、医疗机构（56起），占到所有行业应急处置的9.0%、8.0%、8.0%，三者之和约占应急处置事件总量的25%。
* 在2018年360安服团队参与处置的所有政府机构和企业的网络安全应急响应事件中，由行业单位自己发现的安全攻击事件占92%，而另有8%的安全攻击事件政府机构和企业实际上是不自知的，他们是在得到了监管机构或主管单位的通报才得知已被攻击。
* 安全事件的影响范围主要集中在外部网站和内部网站（25.3%）、内部服务器和数据库（18.7%）。除此之外，还占有一定比例的还有办公终端（17.5%）、业务专网（6.3%）。
* 黑产活动、敲诈勒索仍然是攻击者攻击政府机构、大中型企业的主要原因。攻击者通过黑词暗链、钓鱼页面、挖矿程序等攻击手段开展黑产活动谋取暴利；利用勒索病毒感染政府机构、大中型企业终端、服务器，对其实施敲诈勒索。
* 从上述数据可以看出，攻击者对系统的攻击所产生现象主要表现为导致生产效率低下、破坏性攻击、声誉影响、系统不可用。其中，导致生产效率低下占比20%，数据丢失占比13%，破坏性攻击占比10%。

**关键词：**应急响应、安全服务、敲诈勒索、黑产活动、木马病毒

目 录

[第一章 研究背景 1](#_Toc535600851)

[第二章 应急响应监测分析 2](#_Toc535600852)

[一、 月度报告趋势分析 2](#_Toc535600853)

[二、 行业报告排名分析 2](#_Toc535600854)

[三、 攻击事件发现分析 3](#_Toc535600855)

[四、 影响范围分布分析 5](#_Toc535600856)

[五、 攻击意图分布分析 5](#_Toc535600857)

[六、 攻击现象统计分析 6](#_Toc535600858)

[七、 事件类型分布分析 7](#_Toc535600859)

[第三章 应急响应服务分析 9](#_Toc535600860)

[一、 网站安全 9](#_Toc535600861)

[（一） 网页被篡改 9](#_Toc535600862)

[（二） 非法子页面 9](#_Toc535600863)

[（三） 网站DDoS攻击 9](#_Toc535600864)

[（四） CC攻击 9](#_Toc535600865)

[（五） 网站流量异常 10](#_Toc535600866)

[（六） 异常进程与异常外联 10](#_Toc535600867)

[（七） 网站安全总结及防护建议 10](#_Toc535600868)

[二、 终端安全 11](#_Toc535600869)

[（一） 运行异常 11](#_Toc535600870)

[（二） 勒索病毒 11](#_Toc535600871)

[（三） 终端DDoS攻击 12](#_Toc535600872)

[（四） 终端安全总结及防护建议 12](#_Toc535600873)

[三、 服务器安全 12](#_Toc535600874)

[（一） 运行异常 12](#_Toc535600875)

[（二） 木马病毒 13](#_Toc535600876)

[（三） 勒索病毒 13](#_Toc535600877)

[（四） 服务器DDoS攻击 13](#_Toc535600878)

[（五） 服务器安全总结及防护建议 13](#_Toc535600879)

[四、 邮箱安全 14](#_Toc535600880)

[（一） 邮箱异常 14](#_Toc535600881)

[（二） 邮箱DDoS攻击 15](#_Toc535600882)

[（三） 邮箱安全总结及防护建议 15](#_Toc535600883)

[第四章 应急响应典型案例 16](#_Toc535600884)

[一、 某医院服务器勒索软件事件应急响应 16](#_Toc535600885)

[（一） 事件概述 16](#_Toc535600886)

[（二） 防护建议 16](#_Toc535600887)

[二、 某电网公司终端勒索软件事件应急响应 16](#_Toc535600888)

[（一） 事件概述 16](#_Toc535600889)

[（二） 防护建议 17](#_Toc535600890)

[三、 某汽车公司挖矿木马事件应急响应 17](#_Toc535600891)

[（一） 事件概述 17](#_Toc535600892)

[（二） 防护建议 17](#_Toc535600893)

[四、 某部委CC事件应急响应 18](#_Toc535600894)

[（一） 事件概述 18](#_Toc535600895)

[（二） 防护建议 18](#_Toc535600896)

[五、 某证券公司DDoS事件应急响应 18](#_Toc535600897)

[（一） 事件概述 18](#_Toc535600898)

[（二） 防护建议 18](#_Toc535600899)

[六、 某集团网站挂马事件应急响应 19](#_Toc535600900)

[（一） 事件概述 19](#_Toc535600901)

[（二） 防护建议 19](#_Toc535600902)

[七、 某大学网站非法页面应急响应 19](#_Toc535600903)

[（一） 事件概述 19](#_Toc535600904)

[（二） 防护建议 20](#_Toc535600905)

[八、 某部委蠕虫病毒事件应急响应 20](#_Toc535600906)

[（一） 事件概述 20](#_Toc535600907)

[（二） 防护建议 20](#_Toc535600908)

[九、 某地法院遭到APT攻击事件应急响应 21](#_Toc535600909)

[（一） 事件概述 21](#_Toc535600910)

[（二） 防护建议 21](#_Toc535600911)

[第五章 附录 360安服团队 23](#_Toc535600912)

1. 研究背景

当前，网络空间安全形势日益严峻，国内政府机构、大中型企业的门户网站和重要核心业务系统成为攻击者的首要攻击目标，安全事件层出不穷、逐年增加，给各单位造成严重的影响。为妥善处置和应对政府机构、大中型企业关键信息基础设施发生的突发事件，确保关键信息基础设施的安全、稳定、持续运行，防止造成重大声誉影响和经济损失，需进一步加强网络安全与信息化应急保障能力。

2018年，360安全服务团队/360安服团队共为全国各地600余家政府机构、大中型企业提供了网络安全应急响应服务，参与和协助处置各类网络安全应急响应事件717次，第一时间恢复系统运行，最大限度减少突发安全事件对政府机构、大中型企业的门户网站和业务系统造成的损失和对公众的不良影响，提高了公众服务满足度。同时，为政府机构、大中型企业建立完善的应急响应体系提供技术支撑。

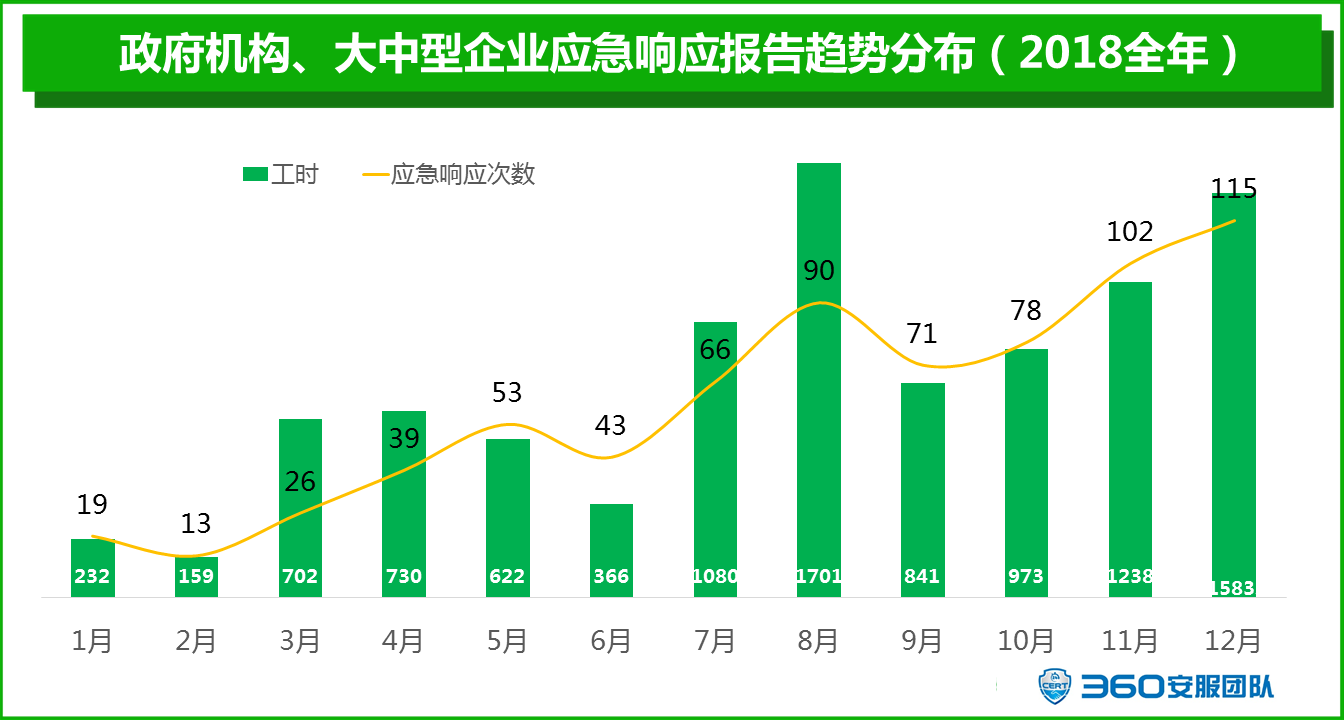
网络安全应急响应服务是安全防护的最后一道防线，巩固应急防线对安全能力建设至关重要。360构建了全流程的应急响应服务体系，为政府机构、大中型企业提供高效、实时、全生命周期的应急服务。

1. 应急响应监测分析

2018年360安服团队共参与和处置了717起全国范围内的网络安全应急响应事件，第一时间协助用户处理安全事故，确保了用户门户网站和重要业务系统的持续安全稳定运行。为进一步提高政府机构、大中型企业对突发安全事件的认识，增强安全防护意识，同时强化第三方安全服务商的应急响应能力，对2018年全年处置的所有应急响应事件从不同维度进行统计分析，反映全年的应急响应情况和攻击者的攻击目的及意图。

1. 月度报告趋势分析

2018年全年360安服团队共参与和处置了717起网络安全应急响应事件，月度报告趋势分布如下图所示：

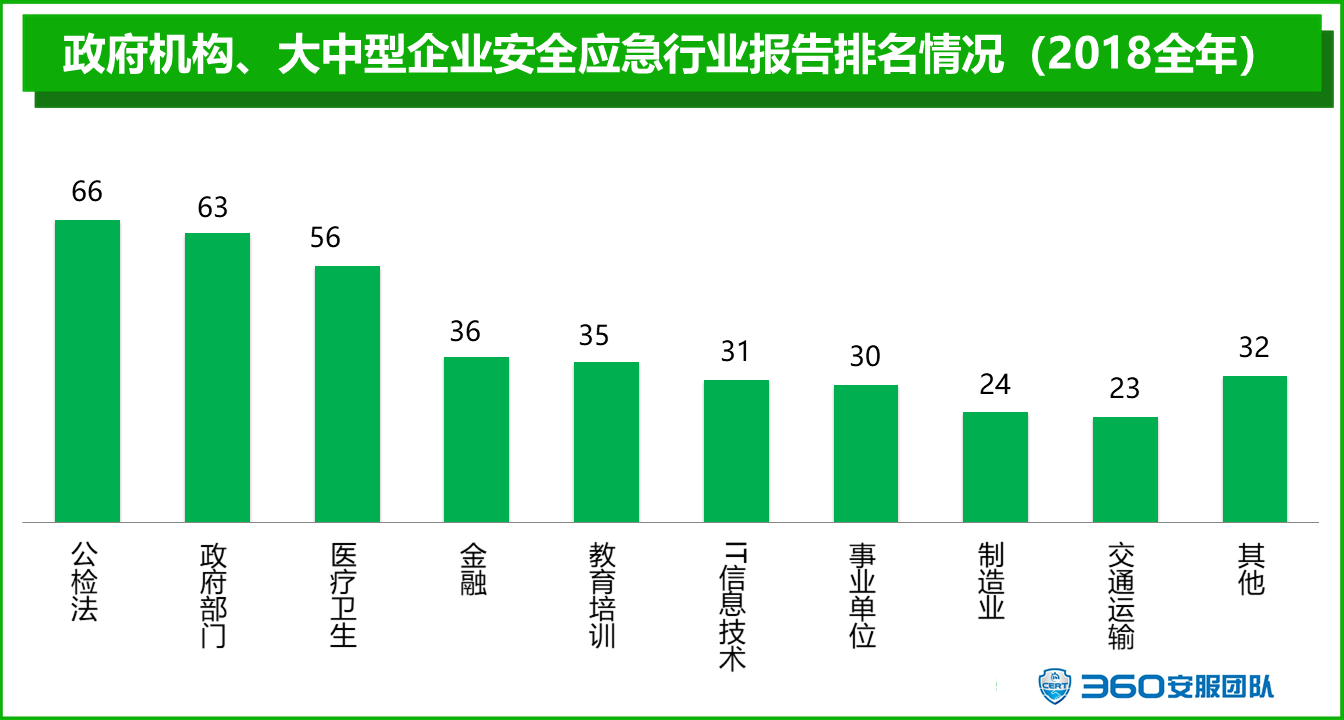
****

从上述数据中可以看到，每年年初和年底发生的应急响应事件请求存在较大反差，年初处置的安全应急请求较少，年底相对较多，8月份应急请求达全年最高，全年整体上处置的安全应急请求趋于上升趋势。

对政府机构、大中型企业的攻击从未间断过，在重要时期的攻击更加频繁。所以，政府机构、大中型企业应做好全年的安全防护工作，特别是重要时期的安全保障工作，同时建立完善的应急响应机制。

1. 行业报告排名分析

通过对2018年全年应急响应事件行业分类分析，汇总出行业应急处置数量排名，如下图所示：



需要说明的是，应急响应次数多，并不意味着这个行业的整体安全状况差。这与机构本身的数量和性质有关，与360的客户覆盖也有关。

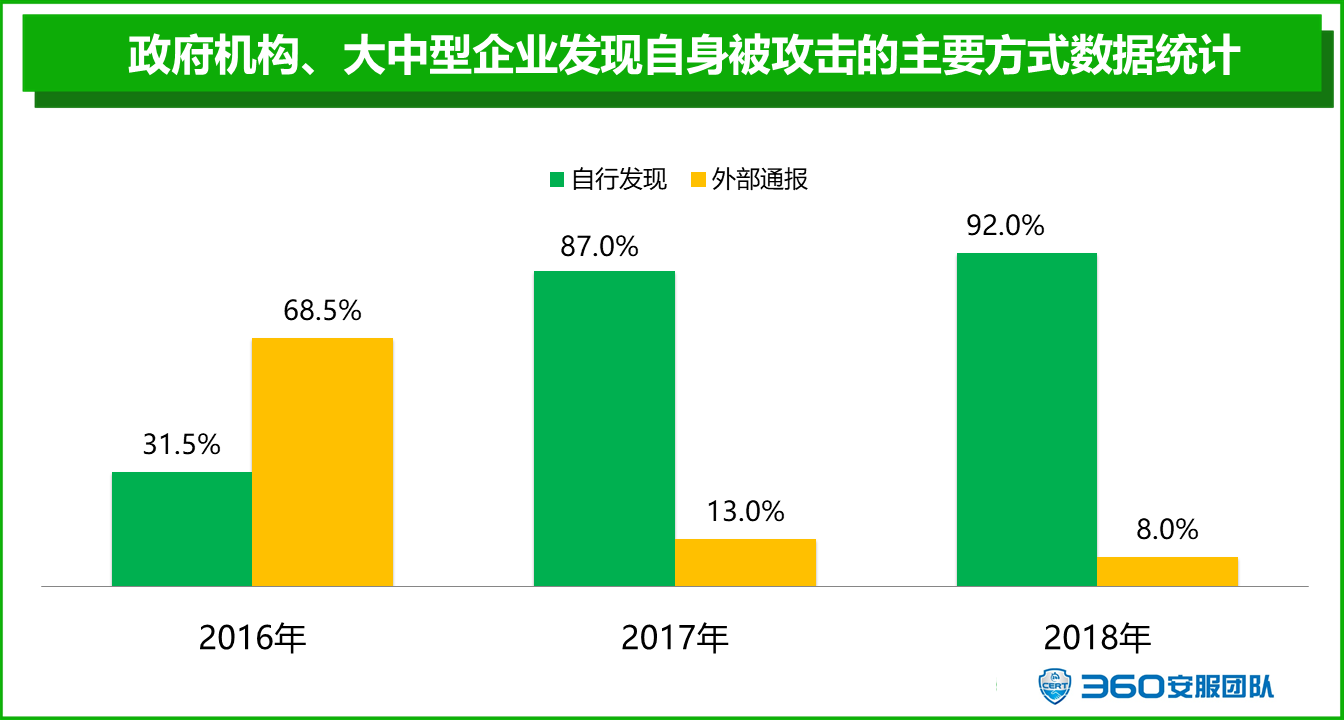
从上述数据中可以看出，行业应急处置排在前三位的分别为公检法（66起）、政府部门（63起）、医疗机构（56起），占到所有行业应急处置的9.0%、8.0%、8.0%，三者之和约占应急处置事件总量的25%，即全年应急响应事件四分之一是出在政府部门、事业单位、金融机构。而金融、教育培训、事业单位、IT信息技术、制造业所产生的应急响应事件也占到了所有行业的18%。

从行业报告排名可知，攻击者的主要攻击对象为公检法、各级政府部门以及医疗卫生，其次为金融、教育培训、IT信息技术和事业单位，从中窃取数据、敲诈勒索。上述机构在原有安全防护基础上，应进一步强化安全技术和管理建设，同时应与第三方安全服务商建立良好的应急响应沟通和处置机制。

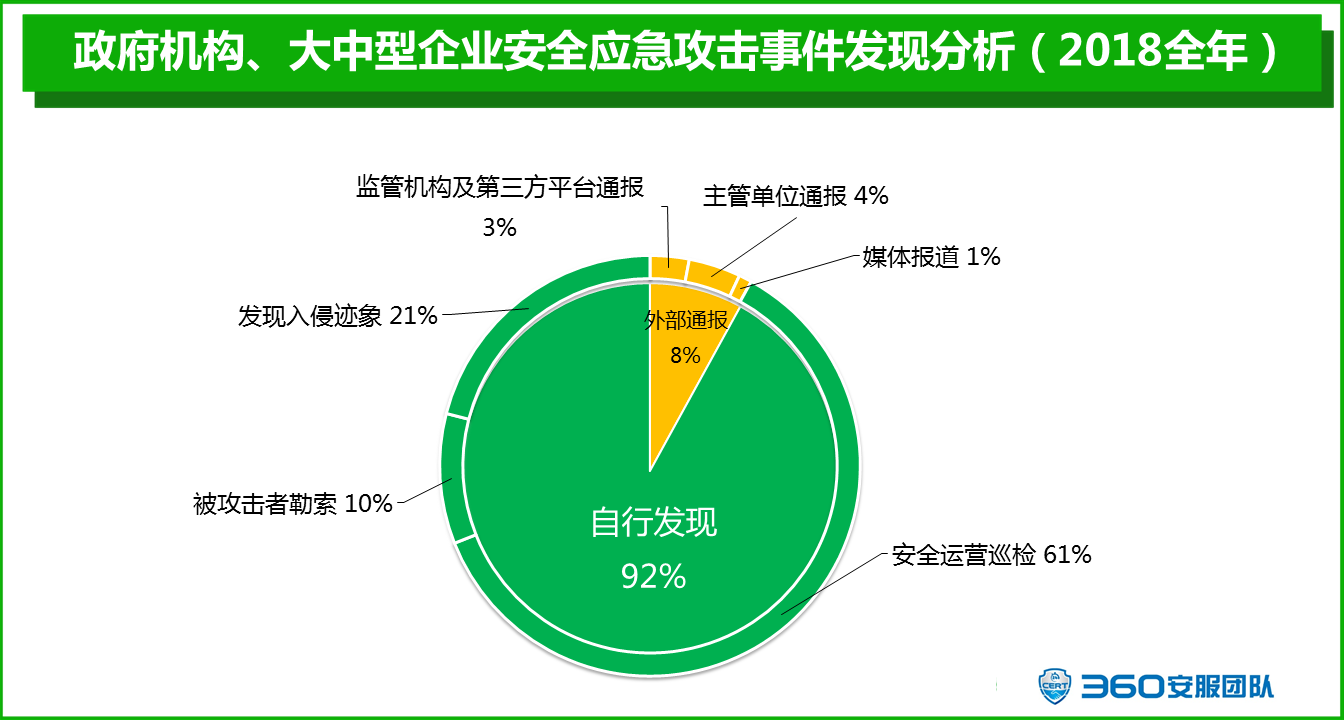
1. 攻击事件发现分析

政企机构对网络攻击的重视程度、发现能力和主动响应的能力正在显著上升。2016年，在360安服团队参与处置的网络安全应急响应事件中，仅有31.5%的攻击事件是政企机构自行发现的，其他68.5%均为接到了第三方机构通报。这些第三方机构包括网络安全监管机构，行业主管机构和媒体等。

但是，2017年和2018年的统计数据显示，近九成的攻击事件都是政企机构自行发现并请求援助的。分析认为，这可能主要是由于2017年6月《网络安全法》的实施，大中型政企机构对安全事件的应急响应重视程度大幅提高，尽早发现，尽早处置，自行响应渐成主流。但是，仍有近一成的安全事件，企业实际上是不自知的，他们是在得到了监管机构的通报或看到了媒体的公开报道后，才得知自己已经被攻击了。



通过对2018年全年应急响应事件攻击发现类型分析，汇总出攻击事件发现情况，如下图所示：



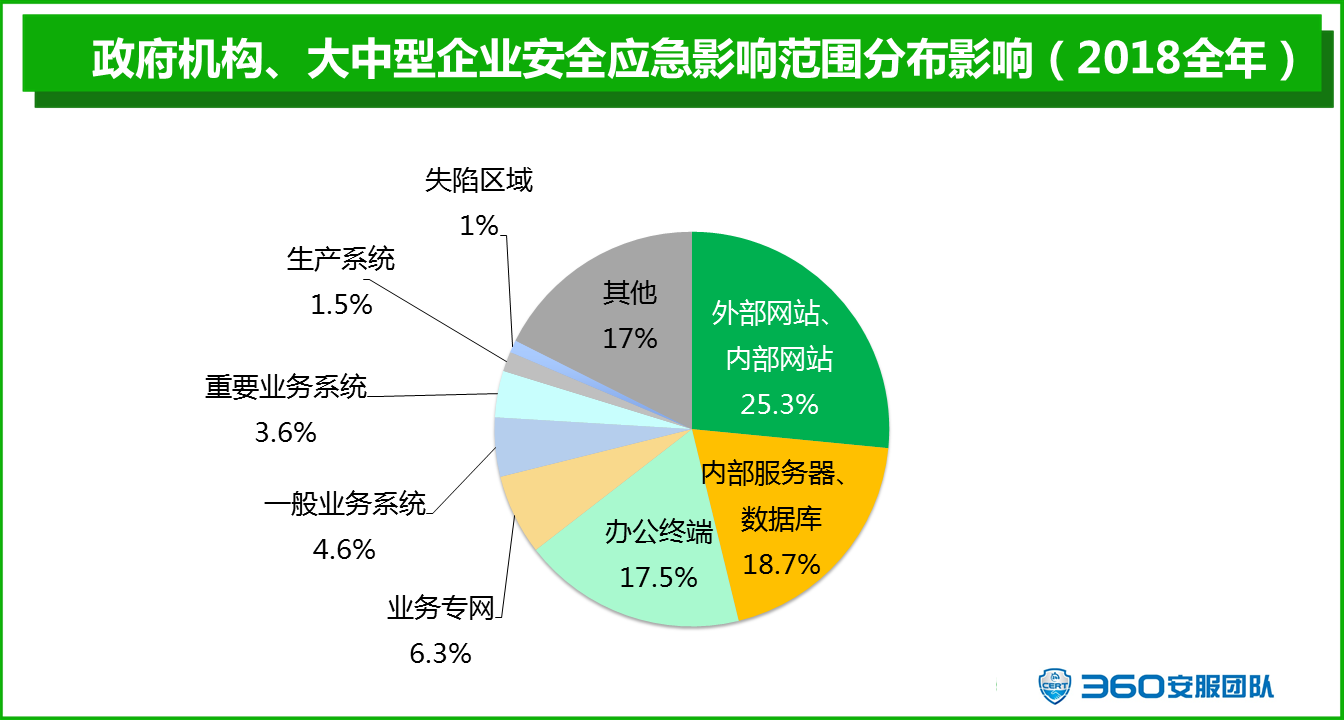
在2018年360安服团队参与处置的所有政府机构和企业的网络安全应急响应事件中，由行业单位自己发现的安全攻击事件占92%，而另有8%的安全攻击事件政府机构和企业实际上是不自知的，他们是在得到了监管机构或主管单位的通报才得知已被攻击。

虽然政府机构和企业自行发现的安全攻击事件占到了92%，但并不代表其具备了潜在威胁的发现能力。其中，占安全攻击事件总量61%的事件是政府机构和企业通过内部安全运营巡检的方式自主查出的，而其余31%的安全攻击事件能够被发现，则完全是因为其网络系统已经出现了显著的入侵迹象，或者是已经遭到了攻击者的敲诈勒索。更有甚者，某些单位实际上是在已经遭遇了巨大的财产损失后才发现自己的网络系统遭到了攻击。

从上述数据中可以看出，政府机构、大中型企业仍然普遍缺乏足够的安全监测能力，缺乏主动发现隐蔽性较好地入侵威胁的能力。

1. 影响范围分布分析

通过对2017年全年应急响应事件处置报告分析，汇总出安全事件的影响范围分布即失陷区域分布，如下图所示：



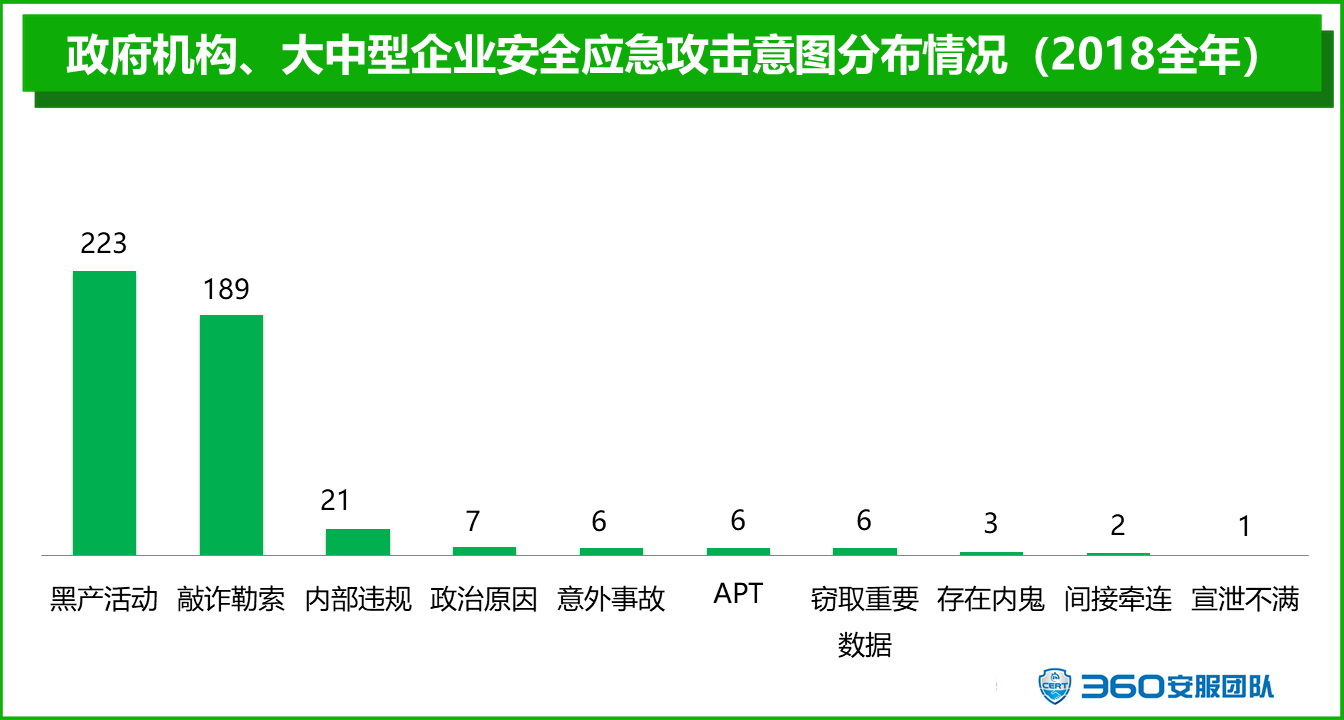
从上述数据中可以看出，安全事件的影响范围主要集中在外部网站和内部网站（25.3%）、内部服务器和数据库（18.7%）。除此之外，还占有一定比例的还有办公终端（17.5%）、业务专网（6.3%）。

从影响范围分布可知，攻击者的主要攻击对象为政府机构、大中型企业的互联网门户网站、内部网站、内部业务系统服务器以及数据库，其主要原因是门户网站暴露在互联网上受到多重安全威胁，攻击者通过对网站的攻击，实现敲诈勒索、满足个人利益需求；而内部网站、内部服务器和数据库运行核心业务系统、存放重要数据，也成为攻击者进行黑产活动、敲诈勒索等违法行为的主要攻击目标。

基于此，政府机构、大中型企业应强化对互联网门户网站的安全防护建设，加强对内网中内部网站、内部服务器和数据库、终端以及业务系统的安全防护保障和数据安全管理。

1. 攻击意图分布分析

通过对2018年全年应急响应事件处置报告分析，汇总出攻击者攻击政府机构、大中型企业的攻击意图分布，如下图所示：



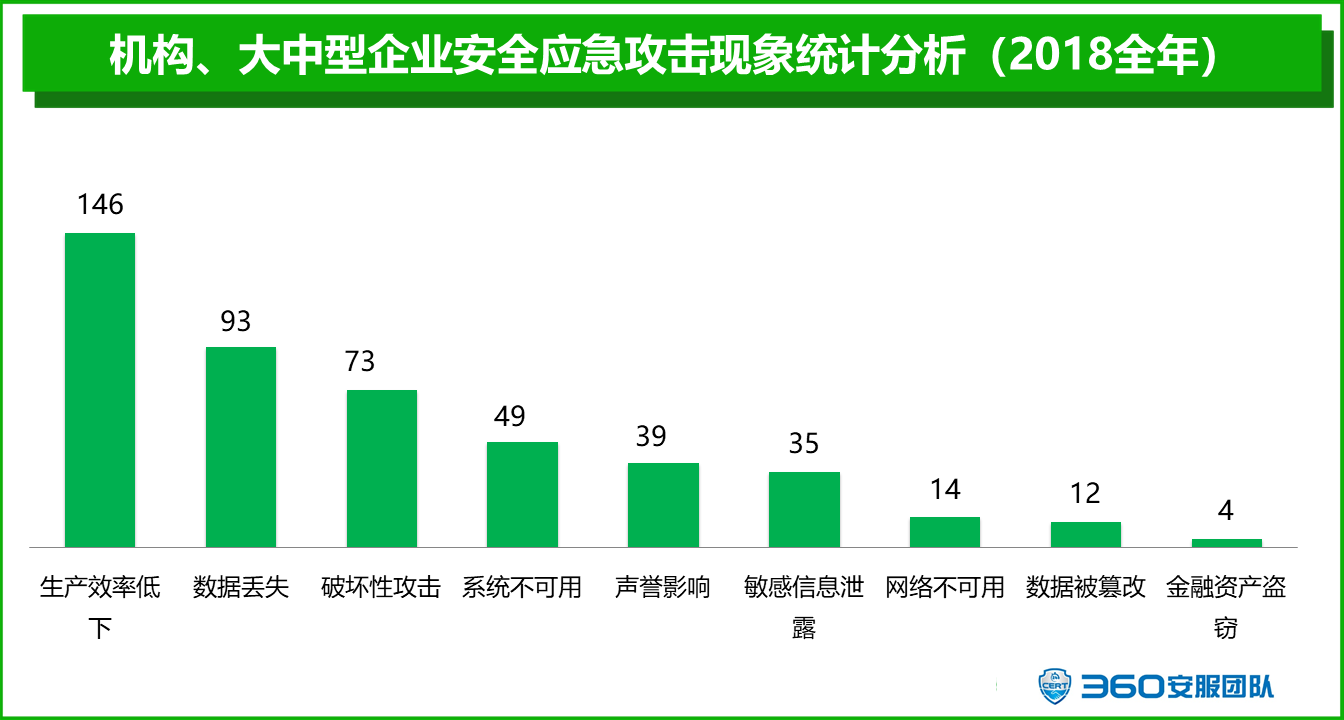
从上述数据中可以看出，黑产活动、敲诈勒索仍然是攻击者攻击政府机构、大中型企业的主要原因。攻击者通过黑词暗链、钓鱼页面、挖矿程序等攻击手段开展黑产活动谋取暴利；利用勒索病毒感染政府机构、大中型企业终端、服务器，对其实施敲诈勒索。对于大部分攻击者而言，其进行攻击的主要原因是为获取暴利，实现自身最大利益。

其次是内部违规响应事件，表明政府机构、大中型企业业务人员、运维人员的安全意识有待提升。

APT攻击和出于政治原因攻击意图的存在，说明具有组织性、针对性的攻击团队对政府机构、大中型企业的攻击目的不单单是为钱财，而有可能出于政治意图，窃取国家层面、重点领域的数据。虽然APT攻击和出于政治原因的攻击数量相对较少，但其危害性较重，所以政府机构、大中型企业，特别是政府机构，应强化整体安全防护体系建设。

1. 攻击现象统计分析

通过对2018年全年应急响应事件处置报告分析，汇总出攻击现象排名，如下图所示：



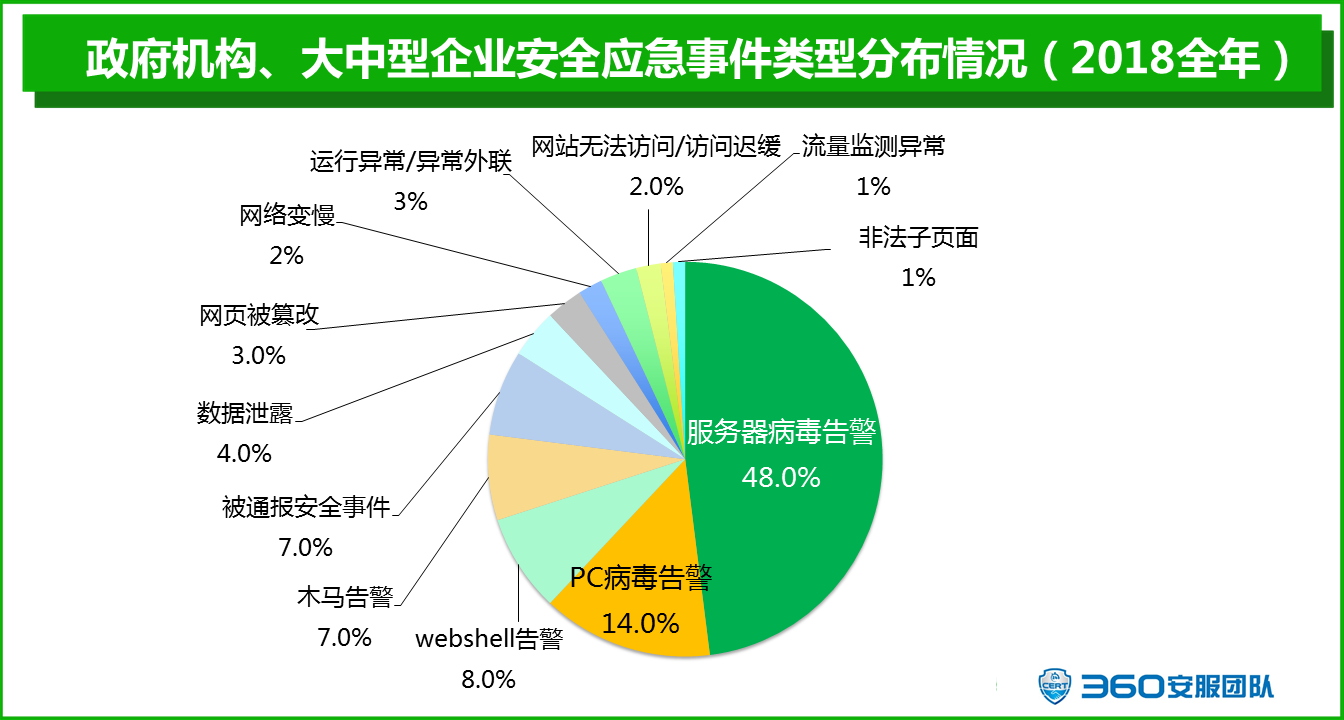
从上述数据可以看出，攻击者对系统的攻击所产生现象主要表现为导致生产效率低下、破坏性攻击、声誉影响、系统不可用。

其中，导致生产效率低下占比20%，攻击者通过挖矿、拒绝服务等攻击手段使服务器CPU占用率异常高，从而造成生产效率低下；数据丢失占比13%；破坏性攻击占比10%，攻击者通过利用服务器漏洞、配置不当、弱口令、Web漏洞等系统安全缺陷，对系统实施破坏性攻击；系统不可用占比7%，主要表现为攻击者通过对系统的攻击，直接造成业务系统宕机；声誉影响占比5%，主要体现在对政府机构、大中型企业门户网站进行的网页篡改、黑词暗链、钓鱼网站、非法子页面等攻击，对政府和企业造成严重的声誉影响，特别是政府机构。同时，敏感信息泄露、数据被篡改、网络不可用也是攻击产生的现象，对政府机构、大中型企业造成严重后果。

从攻击现象统计看，攻击者对系统的攻击具备破坏性、针对性，严重影响系统正常运行。

1. 事件类型分布分析

通过对2018年全年应急响应事件处置报告分析，汇总出事件类型分布，如下图所示：



从上述数据可以看出，安全事件类型主要表现在服务器病毒告警、网页被篡改、运行异常/异常外联、PC病毒告警等方面。

其中，服务器病毒告警是攻击者利用病毒感染对服务器进行的攻击，占48%，成为攻击者主要的攻击手段；PC病毒告警是攻击者利用病毒感染对办公终端进行攻击，占14%，是对攻击终端的主要手段；webshell告警、木马告警是攻击者对互联网门户网站进行的常见攻击，占8%，可能会导致政府机构、大中型企业数据外泄；运行异常/异常外联是攻击者利用不同的攻击手段造成服务器、系统运行异常或异常外联，降低生产效率；。

除此之外，还有流量监测异常、被通报安全事件、网站无法访问/访问迟缓、网站被篡改等安全事件类型。所以，作为政府机构、大中型企业的安全负责人和安全主管，应清楚地认识到攻击者可通过不同的攻击手段、攻击方式，对我们的服务器或系统进行攻击，单一、被动的安全防护措施已无法满足安全防护需要。

1. 应急响应服务分析

根据2018年360安服团队的现场处置情况，政府机构、大中型企业在自行发现或被通告攻击事件，并主动寻求应急响应服务时，绝大多数情况是因为互联网网站（DMZ区）、办公区终端、核心重要业务服务器以及邮件服务器等遭到了网络攻击，影响了系统运行和服务质量。

下面将分别对这四类对象从主要现象、主要危害、攻击方法，以及攻击者的主要目的进行分类分析。

1. 网站安全
2. 网页被篡改

**主要现象**：首页或关键页面被篡改，出现各种不良信息，甚至反动信息。

**主要危害**：散步各类不良或反动信息，影响政府机构、企业声誉，特别是政府机构，降低其公信力。

**攻击方法**：黑客利用webshell等木马后门，对网页实施篡改。

**攻击目的**：宣泄对社会或政府的不满；炫技或挑衅中招企业；对企业进行敲诈勒索。

1. 非法子页面

**主要现象**：网站存在赌博、色情、钓鱼等非法子页面。

**主要危害**：通过搜索引擎搜索相关网站，将出现赌博、色情等信息；通过搜索引擎搜索赌博、色情信息，也会出现相关网站；对于被植入钓鱼网页的情况，当用户访问相关钓鱼网站页面时，安全软件可能不会给出风险提示。

对于政府网站而言，该现象的出现将严重降低政府的权威性及在民众中的公信力，挽回难度相对较大。

**攻击方法**：黑客利用webshell等木马后门，对网站进行子页面的植入。

**攻击目的**：恶意网站的SEO优化；为网络诈骗提供“相对安全”钓鱼页面。

1. 网站DDoS攻击

**主要现象**：政府机构或企业网站无法访问、访问迟缓。

**主要危害**：网站业务中断，用户无法访问网站。特别是对于政府官网，影响民众网上办事，降低政府公信力。

**攻击方法**：黑客利用多类型DDoS技术对网站进行分布式抗拒绝服务攻击。

**攻击目的**：敲诈勒索政府或企业；企业间的恶意竞争；宣泄对网站的不满。

1. CC攻击

**主要现象**：网站无法访问、网页访问缓慢、业务异常。

**主要危害**：网站业务中断，用户无法访问网站、网页访问缓慢。

**攻击方法**：主要采用发起遍历数据攻击行为、发起SQL注入攻击行为、发起频繁恶意请求攻击行为等攻击方式进行攻击。

**攻击目的**：敲诈勒索；恶意竞争；宣泄对网站的不满。

1. 网站流量异常

**主要现象**：异常现象不明显，偶发性流量异常偏高，且非业务繁忙时段也会出现流量异常偏高。

**主要危害**：尽管从表面上看，网站受到的影响不大。但实际上，网站已经处于被黑客控制的高度危险状态，各种有重大危害的后果都有可能发生。

**攻击方法**：黑客利用webshell等木马后门，控制网站；某些攻击者甚至会以网站为跳板，对企业的内部网络实施渗透。

**攻击目的**：对网站进行挂马、篡改、暗链植入、恶意页面植入、数据窃取等。

1. 异常进程与异常外联

**主要现象**：操作系统响应缓慢、非繁忙时段流量异常、存在异常系统进程以及服务，存在异常的外连现象。

**主要危害**：系统异常，系统资源耗尽，业务无法正常运作；同时，网站也可能会成为攻击者的跳板，或者是对其他网站发动DDoS攻击的攻击源。

**攻击方法**：使用网站系统资源对外发起DDoS攻击；将网站作为IP代理，隐藏攻击者，实施攻击。

**攻击目的**：长期潜伏，窃取重要数据信息。

1. 网站安全总结及防护建议
2. 常见攻击手段

以上六类网站安全威胁，是政府机构、大中型企业门户网站所面临的主要威胁，也是网站安全应急响应服务所要解决的主要问题。

通过对现场处置情况的汇总和分析得知，黑客主要采用以下攻击手段对网站实施攻击：

* 1. 黑客利用门户网站Tomcat、IIS等中间件已有漏洞、网站各类应用上传漏洞、弱口令以及第三方组件或服务配置不当等，将webshell上传至门户web服务器，利用该webshell对服务器进行恶意操作；
  2. 黑客利用已有漏洞上传恶意脚本，如挖矿木马等，造成网站运行异常；
  3. 黑客利用多类型DDoS攻击技术（SYN Flood、ACK Flood、UDP Flood、ICMP Flood等），对网站实施DDoS攻击；
  4. 黑客发起遍历数据攻击、SQL注入攻击、频繁恶意请求攻击等攻击方式进行攻击。

1. 安全防护建议

针对网站所面临的安全威胁以及可能造成的安全损失，政府机构、大中型企业应采取以下安全防护措施：

1. 针对网站，建立完善的监测预警机制，及时发现攻击行为，启动应急预案并对攻击行为进行防护；
2. 有效加强访问控制ACL策略，细化策略粒度，按区域按业务严格限制各网络区域以及服务器之间的访问，采用白名单机制只允许开放特定的业务必要端口，其他端口一律禁止访问，仅管理员IP可对管理端口进行访问，如FTP、数据库服务、远程桌面等管理端口；
3. 配置并开启网站应用日志，对应用日志进行定期异地归档、备份，避免在攻击行为发生时，导致无法对攻击途径、行为进行溯源等，加强安全溯源能力；
4. 加强入侵防御能力，建议在网站服务器上安装相应的防病毒软件或部署防病毒网关，即时对病毒库进行更新，并且定期进行全面扫描，加强入侵防御能力；
5. 定期开展对网站系统、应用以及网络层面的安全评估、渗透测试以及代码审计工作，主动发现目前存在的安全隐患；
6. 建议部署全流量监测设备，及时发现恶意网络流量，同时可进一步加强追踪溯源能力，对安全事件发生时可提供可靠的追溯依据；
7. 加强日常安全巡检制度，定期对系统配置、网络设备配合、安全日志以及安全策略落实情况进行检查，常态化信息安全工作。
8. 终端安全
9. 运行异常

**主要现象**：操作系统响应缓慢、非繁忙时段流量异常、存在异常系统进程以及服务、存在异常的外连现象。

**主要危害**：被攻击的终端被攻击者远程控制；政府机构和企业的敏感、机密数据可能被窃取。个别情况下，会造成比较严重的系统数据破坏。

**攻击方法**：针对政府机构、企业办公区终端的攻击，很多情况下是由高级攻击者发动的，而高级攻击者的攻击行动往往动作很小，技术也更隐蔽，所以通常情况下，并没有太多的异常现象，被攻击者往往很难发觉。

**攻击目的**：长期潜伏，收集信息，以便于进一步渗透；窃取重要数据并外传；使用终端资源对外发起DDoS攻击。

1. 勒索病毒

**主要现象**：内网终端出现蓝屏、反复重启和文档被加密的现象。

**主要危害**：政府机构、企业向攻击者付勒索费用；造成内网终端无法正常运行；数据可能泄露。

**攻击方法**：通过弱口令探测、软件和系统漏洞、传播感染等攻击方式，使内网终端感染勒索病毒。

**攻击目的**：向政府机构、企业勒索钱财，以到达自身盈利目的。

1. 终端DDoS攻击

**主要现象**：内网终端不断进行外网恶意域名的请求。

**主要危害**：造成内网终端资源的浪费；攻击者可能对内网进行攻击，造成业务中止、数据泄露等。

**攻击方法**：可通过网络连接、异常进程、系统进程注入可疑DLL模块以及异常启动项等多种方式进行攻击。

**攻击目的**：使用政府机构、企业的内网终端资源对外发起DDoS攻击，以达到敲诈、勒索以及恶意竞争等目的。

1. 终端安全总结及防护建议
2. 常见攻击手段

以上三类终端安全威胁，是政府机构、大中型企业内网终端所面临的主要威胁，也是终端安全应急响应所要解决的主要问题。

通过对现场处置情况的汇总和分析得知，黑客主要采用以下攻击手段对终端实施攻击：

1. 通过弱口令爆破、软件和系统漏洞、社会人工学以及其他等攻击手段，使内网终端感染病毒；
2. 通过网络连接、异常进程、系统进程注入可疑DLL模块以及异常启动项等多种方式进行攻击。
3. 安全防护建议

针对内网终端所面临的安全威胁以及可能造成的安全损失，政府机构、大中型企业应采取以下安全防护措施：

1. 定期给终端系统及软件安装最新补丁，防止因为漏洞利用带来的攻击；
2. 采用统一的防病毒软件，并定时更新，抵御常见木马病毒；
3. 在网络层面采用能够对全流量进行持续存储和分析的设备，对已知安全事件进行定位溯源，对未知的高级攻击进行发现和捕获；
4. 完善政府机构和企业内部的IP和终端位置信息关联，并记录到日志中，方便根据IP直接定位机器位置；
5. 加强员工对终端安全操作和管理培训，提高员工安全意识。
6. 服务器安全
7. 运行异常

**主要现象**：操作系统响应缓慢、非繁忙时段流量异常、存在异常系统进程以及服务、存在异常的外连现象。

**主要危害**：被攻击的服务器被攻击者远程控制；政府机构和企业的敏感、机密数据可能被窃取。个别情况下，会造成比较严重的系统数据破坏。

**攻击方法**：针对政府机构、企业服务器的攻击，很多情况下是由高级攻击者发动的，攻击过程往往更加隐蔽，更加难以被发现，技术也更隐蔽。通常情况下，并没有太多的异常现象。

**攻击目的**：长期潜伏，收集信息，以便于进一步渗透；窃取重要数据并外传；使用服务器资源对外发起DDoS攻击。

1. 木马病毒

**主要现象**：服务器无法正常运行或异常重启、管理员无法正常登陆进行管理、重要业务中断、服务器响应缓慢等。

**主要危害**：被攻击的服务器被攻击者远程控制；政府机构和企业的敏感、机密数据可能被窃取。个别情况下，会造成比较严重的系统数据破坏。

**攻击方法**：黑客通过利用弱口令探测、系统漏洞、应用漏洞等攻击方式，种植恶意病毒进行攻击。

**攻击目的**：利用内网服务器资源进行虚拟币的挖掘，从而赚取相应的虚拟币，以到达获利目的。

1. 勒索病毒

**主要现象**：内网服务器文件被勒索软件加密，无法打开，索要天价赎金。

**主要危害**：用户无法打开文件，政府机构、企业向攻击者付勒索费用；造成内网服务器无法正常运行；数据可能泄露。

**攻击方法**：通过利用弱口令探测、共享文件夹加密、软件和系统漏洞、数据库爆破等攻击方式，使内网服务器感染勒索病毒。

**攻击目的**：通过使服务器感染勒索病毒，向政府机构、企业勒索钱财，以到达自身盈利目的。

1. 服务器DDoS攻击

**主要现象**：向外网发起大量异常网络请求、恶意域名请求等。

**主要危害**：严重影响内网服务器性能，如服务器CPU以及带宽等，导致服务器上的业务无法正常运行；攻击者可能窃取内网数据，造成数据泄露等。

**攻击方法**：黑客可能利用弱口令、系统漏洞、应用漏洞等系统缺陷，通过种马的方式，让服务器感染DDoS木马，以此发起DDoS攻击。

**攻击目的**：使用政府机构、企业的内网服务器对外发起DDoS攻击，以达到敲诈、勒索以及恶意竞争等目的。

1. 服务器安全总结及防护建议
2. 常见攻击手段

以上四类服务器安全威胁，是政府机构、大中型企业内网服务器所面临的主要威胁，也是服务器安全应急响应服务所要解决的主要问题。

通过对现场处置情况的汇总和分析得知，黑客主要采用以下攻击手段对服务器实施攻击：

1. 通过弱口令探测、共享文件夹加密、软件和系统漏洞、数据库爆破以及Webshell等多种攻击方式，感染内网服务器勒索病毒；
2. 黑客利用弱口令、系统漏洞、应用漏洞等系统缺陷，通过种马的方式，让服务器感染各类木马（如挖矿木马、DDoS木马等），以此实现攻击目的。
3. 安全防护建议

针对内网服务器所面临的安全威胁以及可能造成的安全损失，政府机构、大中型企业应采取以下安全防护措施：

1. 及时清除发现的webshell后门、恶意木马文件、挖矿程序。在不影响系统正常运行的前提下，建议重新安装操作系统，并重新部署应用，以保证恶意程序被彻底清理；
2. 对受害内网机器进行全盘查杀，可进行全盘重装系统更好，同时该机器所属使用者的相关账号密码信息应及时更改；
3. 系统相关用户杜绝使用弱口令，设置高复杂强度的密码，尽量包含大小写字母、数字、特殊符号等的混合密码，加强运维人员安全意识，禁止密码重用的情况出现；
4. 有效加强访问控制ACL策略，细化策略粒度，按区域按业务严格限制各个网络区域以及服务器之间的访问，采用白名单机制只允许开放特定的业务必要端口，其他端口一律禁止访问，仅管理员IP可对管理端口进行访问，如远程桌面等管理端口；
5. 禁止服务器主动发起外部连接请求，对于需要向外部服务器推送共享数据的，应使用白名单的方式，在出口防火墙加入相关策略，对主动连接IP范围进行限制；
6. 加强入侵防御能力，建议在服务器上安装相应的防病毒软件或部署防病毒网关，即时对病毒库进行更新，并且定期进行全面扫描，加强入侵防御能力；
7. 建议增加流量监测设备的日志存储周期，定期对流量日志进行分析，及时发现恶意网络流量，同时可进一步加强追踪溯源能力，对安全事件发生时可提供可靠的追溯依据；
8. 定期开展对服务器系统、应用以及网络层面的安全评估、渗透测试以及代码审计工作，主动发现目前系统、应用存在的安全隐患；
9. 加强日常安全巡检制度，定期对系统配置、网络设备配合、安全日志以及安全策略落实情况进行检查，常态化信息安全工作。
10. 邮箱安全
11. 邮箱异常

**主要现象**：邮箱异常、邮件服务器发送垃圾邮件。

**主要危害**：严重影响邮件服务器性能、邮箱运行异常。

**攻击方法**：黑客通过多渠道获取员工邮箱密码，进而登录到邮箱系统进行垃圾邮件发送操作。

**攻击目的**：炫技或挑衅中招单位；向政府机构、企业勒索钱财，以到达自身盈利目的。

1. 邮箱DDoS攻击

**主要现象**：无法正常发送邮件、服务器宕机。

**主要危害**：邮件服务器业务中断，用户无法正常发送邮件。

**攻击方法**：黑客对邮件服务器进行邮箱爆破、发送大量垃圾数据包、投递大量恶意邮件等。

**攻击目的**：通过DDoS攻击导致邮件服务器资源耗尽并拒绝服务，以达到敲诈、勒索以及恶意竞争等目的。

1. 邮箱安全总结及防护建议
2. 常见攻击手段

以上两类邮件服务器安全威胁，是政府机构、大中型企业邮件服务器所面临的主要威胁，也是邮件服务器安全应急响应服务所要解决的主要问题。

通过对现场处置情况的汇总和分析得知，黑客主要采用以下攻击手段对邮件服务器实施攻击：

1. 通过弱口令探测、社会人工学等多种攻击方式控制邮件服务器，从而发送垃圾邮件；
2. 对邮件服务器进行邮箱爆破、发送垃圾数据包、投递恶意邮件等。
3. 安全防护建议

针对邮件服务器所面临的安全威胁以及可能造成的安全损失，政府机构、大中型企业应采取以下安全防护措施：

1. 邮箱系统使用高复杂强度的密码，尽量包含大小写字母、数字、特殊符号等的混合密码，禁止密码重用的情况出现；
2. 邮箱系统建议开启短信验证功能，采用双因子身份验证识别措施，将有效提高邮箱账号的安全性；
3. 邮箱系统开启HTTPS协议，通过加密传输的方式防止旁路数据窃听攻击；
4. 加强日常攻击监测预警、巡检、安全检查等工作，及时阻断攻击行为；
5. 部署安全邮件网关进一步加强邮件系统安全。
6. 应急响应典型案例

根据2018年应急响应数据分析，18年应急响应共涉及全国26个省市，近30个行业，其中包括医疗卫生，大中型企业、政府机构，高等院校等多个行业。发生安全事件类型10余种，其中不乏各种变种勒索病毒，蠕虫病毒以及会导致CPU运行过高的挖矿木马。长生了较为恶劣的社会负面影响，也给客户带来严重损失。

下面将对部分行业从事件概述以及防护建议方面对突发大规模典型应急事件进行分析说明。

1. 某医院服务器勒索软件事件应急响应
2. 事件概述

2018年1月，360安服团队接到某医院的服务器安全应急响应请求。客户反馈有几台服务器出现重启/蓝屏现象，应急响应人员初步判定为感染了勒索软件。

应急响应人员对重启/蓝屏服务器分析后，判定均遭受永恒之蓝勒索软件，同时遭受感染的服务器中部分文件被加密。通过对服务器进行漏洞检查发现服务器存在MS17-010漏洞，同时发现服务器开放了445端口。

通过本次安全事件，医院信息系统暴露了诸多安全隐患，包括未定期开展安全评估工作，导致内部服务器存在严重高危漏洞；安全域划分不明确，较为混乱；安全意识仍需加强等。

1. 防护建议
2. 周期性对全网进行安全评估工作，及时发现网络主机存在的安全缺陷，修复高风险漏洞，避免类似事件发生；
3. 系统、应用相关的用户杜绝使用弱口令；
4. 有效加强访问控制ACL策略，细化策略粒度，采用白名单机制只允许开放特定的业务必要端口，其他端口一律禁止访问，仅管理员IP可对管理端口进行访问；
5. 加强日常安全巡检制度，定期对系统配置、网络设备配合、安全日志以及安全策略落实情况进行检查，常态化信息安全工作；
6. 加强安全意识，提高对网络安全的认识，关注重要漏洞与网络安全事件。
7. 某电网公司终端勒索软件事件应急响应
8. 事件概述

2018年4月，360安服团队接到某电网公司的终端安全应急响应请求，有几台办公终端出现部分Office文档、图片文档、pdf文档多sage后缀，修改后变成乱码。

应急响应人员接到请求后，通过对感染勒索软件的机器样机进行分析得知，此次感染的勒索软件的类型为sage2.2勒索软件。对于感染过程，响应人员分析该勒索软件可能使用了包含欺骗性消息的恶意电子邮件，消息可以是各种类型，皆在使潜在受害者打开这些电子邮件的恶意.zip。

1. 防护建议
2. 对受感染的机器第一时间进行物理隔离处理;
3. 部署终端安全管控软件，实时对终端进行查杀和防护；
4. 对个人PC中比较重要的稳定资料进行随时备份，备份应离线存储；
5. 继续加强网络与信息安全意识培训教育。意外收到的或来自未知发件人的电子邮件，不要按照文字中的说明进行操作，不要打开任何附件，也不要点击任何链接；
6. 操作系统以及安装在计算机上的所有应用程序（例如Adobe Reader，Adobe Flash，Sun Java等）必须始终如一地更新。
7. 某汽车公司挖矿木马事件应急响应
8. 事件概述

2018年11月，360安服团队接到某汽车公司的挖矿木马事件应急响应请求，其内网多台终端被挖矿木马攻击，服务器卡顿、进程缓慢，无法正常运行。

应急人员到达现场后，对内网服务器、终端进程、日志等多方面进行分析，发现内网服务器、终端CPU被powershell进程占满，服务器、终端均开放135、139、445等服务端口，且均未安装“永恒之蓝”补丁。

经过分析排查，应急人员成功找到问题根源，并对病毒进行抑制、根除。本次事件主要是由于内部工作人员安全意识较低，点击恶意链接感染终端，然后通过被感染终端对服务器SMB弱口令进行爆破获取服务器账号和密码，并利用服务器作为突破口，对内网中有“永恒之蓝”漏洞的主机进行攻击，种植挖矿木马，并横向传播，意图感染内网其他终端。

1. 防护建议
2. 系统、应用相关的用户杜绝使用弱口令，同时，应该使用高复杂强度的密码，尽量包含大小写字母、数字、特殊符号等的混合密码，加强管理员安全意识，禁止密码重用的情况出现，尽量避免一密多用的情况；
3. 禁止服务器主动发起外部连接请求，对于需要向外部服务器推送共享数据的，应使用白名单的方式，在出口防火墙加入相关策略，对主动连接IP范围进行限制；
4. 关闭内网远程服务、共享等危险性服务端口；
5. 定期更新电脑补丁，使用正确渠道，如微软官网，下载对应漏洞补丁；
6. 服务器上部署安全加固软件，通过限制异常登录行为、开启防爆破功能、禁用或限用危险端口、防范漏洞利用等方式，提高系统安全基线，防范黑客入侵；
7. 部署高级威胁监测设备，及时发现恶意网络流量，同时可进一步加强追踪溯源能力，对安全事件发生时可提供可靠的追溯依据；
8. 定期开展对系统、应用以及网络层面的安全评估、渗透测试以及代码审计工作，主动发现目前系统、应用存在的安全隐患；
9. 加强人员安全意识培养，不要点击来源不明的邮件附件，不从不明网站下载软件。
10. 某部委CC事件应急响应
11. 事件概述

2018年3月，360安服团队接到某部委的网站安全应急响应请求，网站存在动态页面访问异常缓慢现象，但静态页面访问正常，同时WAF、DDoS设备出现告警信息。

应急响应人员通过对现场技术人员所提供WAF告警日志、DDoS设备日志、Web访问日志等数据进行分析，发现外部对网站的某个动态页面全天的访问量多达12万次，从而导致动态页面访问缓慢。

根据本次攻击事件的分析，造成网站动态页面访问缓慢的原因主要是攻击者频繁请求“XXX页面”的功能，同时该页面查询过程中并未要求输入验证码信息，大量频繁的HTTP请求以及数据库查询请求导致CC攻击，从而使服务器处理压力过大，最终导致页面访问缓慢。

1. 防护建议
2. 对动态页面添加有效且复杂的验证码功能，确保验证码输入正确后才进入查询流程，并每次进行验证码刷新；
3. 检查动态页面是否存在SQL注入漏洞；
4. 加强日常监测运营，开启安全设备上的拦截功能，特别对同一IP的频繁请求进行拦截封锁；
5. 建议部署全流量的监测设备，从而弥补访问日志上无法记录POST具体数据内容的不足，有效加强溯源能力；
6. 相关负载设备或反向代理上应重新进行配置，使Web访问日志可记录原始请求IP，有助于提高溯源分析效率；
7. 开启源站保护功能，确保只允许CDN节点访问源站；
8. 定期开展渗透测试工作以及源代码安全审计工作。
9. 某证券公司DDoS事件应急响应
10. 事件概述

2018年6月，360安服团队接到某省网安的应急响应请求，本地证券公司在10日7:00-8:00遭受1G流量的DDoS攻击，整个攻击过程持续了1个小时，造成证券公司网站无法正常访问。同时，多个邮箱收到勒索邮件，并宣称如不尽快交钱会把攻击流量增加到1T。

应急响应人员通过利用360大数据平台对网站域名进行分析，发现了Top10 IP地址对被攻击地址进行了DDoS攻击，并发现其攻击类型为NTP反射放大攻击。通过后端大数据综合分析，准确定位了攻击者的真实IP地址。

1. 防护建议
2. 针对重要业务系统、重要网站等，建立完善的监测预警机制，及时发现攻击行为，并启动应急预案及时对攻击行为进行防护；
3. 建议部署类似于360安域等的云安全防护产品，云端安全防护产品对常见的DDoS、Web行为攻击等进行有效防护。
4. 某集团网站挂马事件应急响应
5. 事件概述

2018年5月，360安服团队接到某集团网站挂马事件应急响应请求，客户门户网站被挂马，非域名或IP直接访问跳转色情网站。

应急人员到达现场后，对网站系统、服务器文件、账号、网络链接、日志等多方面进行分析，网站网页被植入恶意JS脚本代码，同时网站系统存在DOTNETCMS 1.0 版本漏洞。

经过分析排查，本次事件中黑客主要通过对网站进行扫描，发现网站系统存在SQL注入、登陆绕过、任意文件上传等漏洞，黑客通过利用漏洞获取系统权限，并在网页中加入恶意JS脚本，并为了不被内部管理维护人员发现，以达到更长时间的黑帽SEO流量，黑客使用只从百度等搜索引擎跳转，其他则不跳转。

1. 防护建议
2. 平时运维过程中应当及时备份重要文件，且文件备份应与主机隔离，规避通过共享磁盘等方式进行备份；
3. 尽量避免打开来源不明的链接，给信任网站添加书签并通过书签访问；
4. 对非可信来源的邮件保持警惕，避免打开附件或点击邮件中的链接；
5. 定期用专业反病毒软件扫描系统.及时对服务器的补丁进行更新；
6. 定期开展对系统、应用以及网络层面的安全评估、渗透测试以及代码审计工作，主动发现目前系统、应用存在的安全隐患；
7. 加强日常安全巡检制度，定期对系统配置、网络设备配合、安全日志以及安全策略落实情况进行检查，常态化信息安全工作。
8. 某大学网站非法页面应急响应
9. 事件概述

2018年5月，360安服团队接到某大学信息中心的网站安全应急响应请求，其官网上出现大量黑链、赌博、游戏外挂等违规关键词。

应急响应人员到达现场后，对网站服务器文件、服务器账号、网络连接、进程信息、服务信息、日志信息等多方面进行分析，发现文件中包含大量aspx木马及gif图片伪装成木马，发现存在多个无效账号，以及向外连接的可疑IP地址。

经过分析排查发现，本次事件中所使用的黑链手法为黑产行业惯用手法，利用搜索引擎对大学院校网站发表内容收录快、排名高等优势，利用网站后台程序漏洞对网站进行攻击，上传webshell木马文件至服务器，获取网站管理权限并篡改服务器原有文件，插入黑链恶意脚本，达到控制搜索引擎网页访问跳转，实现搜索引擎“黑帽SEO”。在获取权限后克隆服务器管理员账号以达到长期控制服务器的目的。

1. 防护建议
2. 建议部署操作系统及相关应用并生成快照，进一步落实口令管理；
3. 建议使用独立的、随机生成的满足强度要求的口令，严禁使用弱口令、统一口令管理服务器，及时销毁临时、测试账户；
4. 修改后台管理员密码为复杂密码，修改后台管理目录为复杂路径防止被攻击者猜到，禁用或删除后台模板功能；
5. 服务器运行环境部署需要进行加固处理，关注各个应用系统所使用程序、组件、第三方插件等安全现状，及时更新相应的补丁版本；
6. 加强对敏感服务器、配置文件、目录的访问控制，以免敏感配置信息泄露；加强信息系统安全配置检查工作。
7. 某部委蠕虫病毒事件应急响应
8. 事件概述

2018年11月，360安服团队接到某部委蠕虫病毒事件应急响应请求，内网多台终端外联外部恶意域名下载恶意软件。

应急人员到达现场后，对内网服务器文件、服务器账号、网络链接等、日志等多方面进行分析，发现内网主机用户浏览带有恶意链接的Web页面，并于内嵌链接中触发对该异常域名的访问，导致服务器被感染飞客蠕虫病毒，并外联下载恶意软件。该病毒会对随机生成的IP地址发起攻击，攻击成功后会下载一个木马病毒，通过修改注册表键值来使某免费安全工具功能失效。病毒会修改hosts文件，使用户无法正常访问安全厂商网站及服务器。

1. 防护建议
2. 配置并开启操作系统、关键应用等自动更新功能，对最新系统、应用安全补丁进行订阅、更新。避免攻击者通过相关系统、应用安全漏洞对系统实施攻击，或在获取系统访问权限后，对系统用户权限进行提升；
3. 限制服务器及其他业务服务网可进行访问的网络、主机范围。有效加强访问控制ACL策略，细化策略粒度，按区域按业务严格限制各个网络区域以及服务器之间的访问，采用白名单机制只允许开放特定的业务必要端口，其他端口一律禁止访问，仅管理员IP可对管理端口进行访问，如FTP、数据库服务、远程桌面等管理端口，限制公网主机对139、445端口等访问；
4. 部署高级威胁监测设备，及时发现恶意网络流量，同时可进一步加强追踪溯源能力，对安全事件发生时可提供可靠的追溯依据；
5. 定期开展对系统、应用以及网络层面的安全评估、渗透测试以及代码审计工作，主动发现目前系统、应用存在的安全隐患；
6. 加强日常安全巡检制度，定期对系统配置、网络设备配合、安全日志以及安全策略落实情况进行检查，常态化信息安全工作；
7. 服务器上部署安全加固软件，通过限制异常登录行为、开启防爆破功能、禁用或限用危险端口、防范漏洞利用等方式，提高系统安全基线，防范黑客入侵；
8. 加强人员安全意识培养，不要点击来源不明的邮件附件，不从不明网站下载软件。对来源不明的文件包括邮件附件、上传文件等要先杀毒处理。
9. 某地法院遭到APT攻击事件应急响应
10. 事件概述

2018年12月，360安服团队接到某法院遭到APT攻击事件应急响应请求，客户天眼存在APT告警行为，服务器存在失陷迹象，要求对服务器进行排查，同时对攻击影响进行分析。

应急人员到达现场后，对内网服务器文件、服务器账号、网络链接、日志等多方面进行分析，发现内网主机和大量服务器遭到APT组织lazarus的恶意攻击，并被植入恶意Brambul 蠕虫病毒和Joanap 后门程序。

经过分析排查，本次事件中APT组织所使用的是通过植入恶意Brambul 蠕虫病毒和Joanap 后门程序，进行长期潜伏，盗取重要信息数据。黑客通过服务器ssh弱口令爆破以及利用服务器“永恒之蓝”漏洞对服务器进行攻击，获取服务器权限，并通过主机设备漏洞对大量主机进行攻击，进而植入蠕虫病毒以及后门程序，进行长期的数据盗取。

1. 防护建议
2. 内网主机存在入侵痕迹，并存在可疑横向传播迹象，建议对内网主机做全面排查，部署终端查杀工具做全面查杀；
3. 内网服务器存在未安装补丁现象，建议定期做补丁安装，做好服务器加固；
4. 整个专网可任意访问，未做隔离，建议做好边界控制，对各区域法院间的访问做好访问控制；
5. 服务器运行业务不清晰，存在一台服务器存在其它未知业务的现象，建议梳理系统业务，做好独立系统运行独立业务，并做好责任划分；
6. 失陷服务器存在异常克隆账号风险，建议全面排查清理不必要的系统账号；
7. 需严格排查内外网资产，做好资产梳理，尤其是外网出口做好严格限制；
8. 应用服务器需做好日志存留，对于操作系统日志，应定期进行备份，并进行双机热备，防止日志被攻击者恶意清除，增大溯源难度；
9. 系统、应用相关的用户杜绝使用弱口令，同时，应该使用高复杂强度的密码，尽量包含大小写字母、数字、特殊符号等的混合密码，加强管理员安全意识，禁止密码重用的情况出现；
10. 禁止服务器主动发起外部连接请求，对于需要向外部服务器推送共享数据的，应使用白名单的方式，在出口防火墙加入相关策略，对主动连接IP范围进行限制；
11. 重点建议在服务器上部署安全加固软件，通过限制异常登录行为、开启防爆破功能、禁用或限用危险端口、防范漏洞利用等方式，提高系统安全基线，防范黑客入侵；
12. 部署全流量监测设备，及时发现恶意网络流量，同时可进一步加强追踪溯源能力，对安全事件发生时可提供可靠的追溯依据。
13. 附录 360安服团队



360安服团队汇集国内知名安全专家，在网络攻防、数据分析、应急响应及攻击溯源等方面有着丰富的经验。

360安服团队创新性地提出基于数据驱动的安全服务运营理念，结合云端数据及专家诊断，为客户提供咨询规划、数据分析、预警检测、持续响应、安全运维等一系列的安全保障服务。

360安服团队参与了多次知名APT事件的分析溯源工作，参与的国内重大活动安全保障工作超过75次，参与上合峰会、博鳌论坛、全国两会、十九大、金砖国家峰会、达沃斯论坛、一带一路等重大活动安全保障工作，并屡获客户认可及感谢信。

360企业安全集团提供7\*24小时全天候应急响应服务，大家如遇网络安全事件可随时拨打：4008 136 360 转2 转4