2017 年

网络安全应急响应分析报告

360安服团队

2018 年 08 月 13 日

360安服团队

摘　　要

- 2017 年全年 360 安服团队共参与和处置了 199 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政府部门（59 起）、事业单位（24 起）、金融机构（16 起），占到所有行业应急处置的 29.6%、12.1%、8.0%，三者之和约占应急处置事件总量的 49.6%。
- 在 2017 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 88%，而另有 12%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（42%）、内部服务器和数据库（39%）。除此之外，还占有一定比例的还有办公终端（9%）、重要业务系统（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 29.1%，破坏性攻击占比 18%，声誉影响占比 16%。

关键词：应急响应、安全服务、敲诈勒索、黑产活动、木马病毒

360安服团队

目　　录

第一章　前言

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。

2017 年，360 安全服务团队/360 安服团队共为全国各地 100 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 199 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。

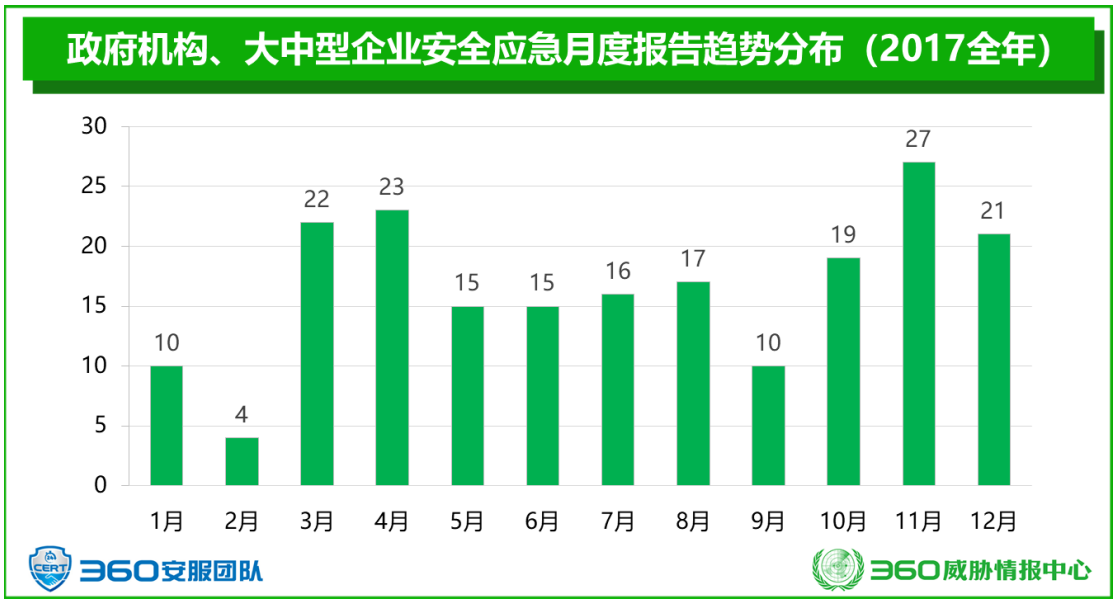
网络安全应急响应服务是安全防护的最后一道防线，巩固应急防线对安全能力建设至关重要。360 构建了全流程的应急响应服务体系，为政府机构、大中型企业提供高效、实时、全生命周期的应急服务。

第二章　应急响应监测分析

2017 年 360 安服团队共参与和处置了 199 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 2017 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。

一、　月度报告趋势分析

2017 年全年 360 安服团队共参与和处置了 199 起网络安全应急响应事件，月度报告趋势分布如下图所示：

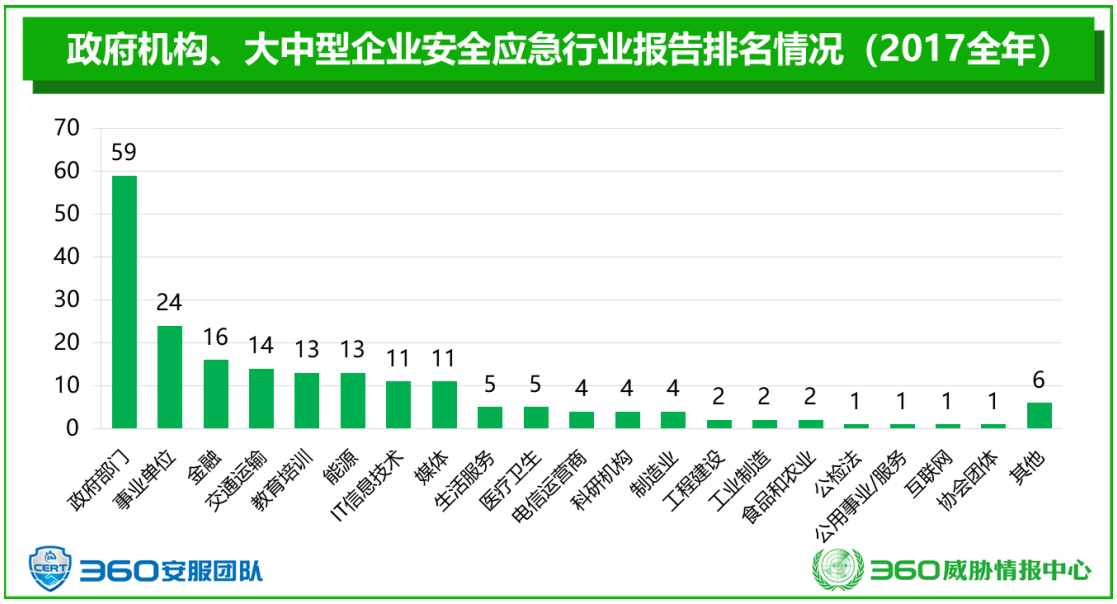


从上述数据中可以看到，每年年初和年底发生的应急响应事件请求存在较大反差，年初处置的安全应急请求较少，年底相对较多，3 月份到 10 月份整体上处置的安全应急请求趋于平稳。

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。

二、　行业报告排名分析

通过对 2017 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：

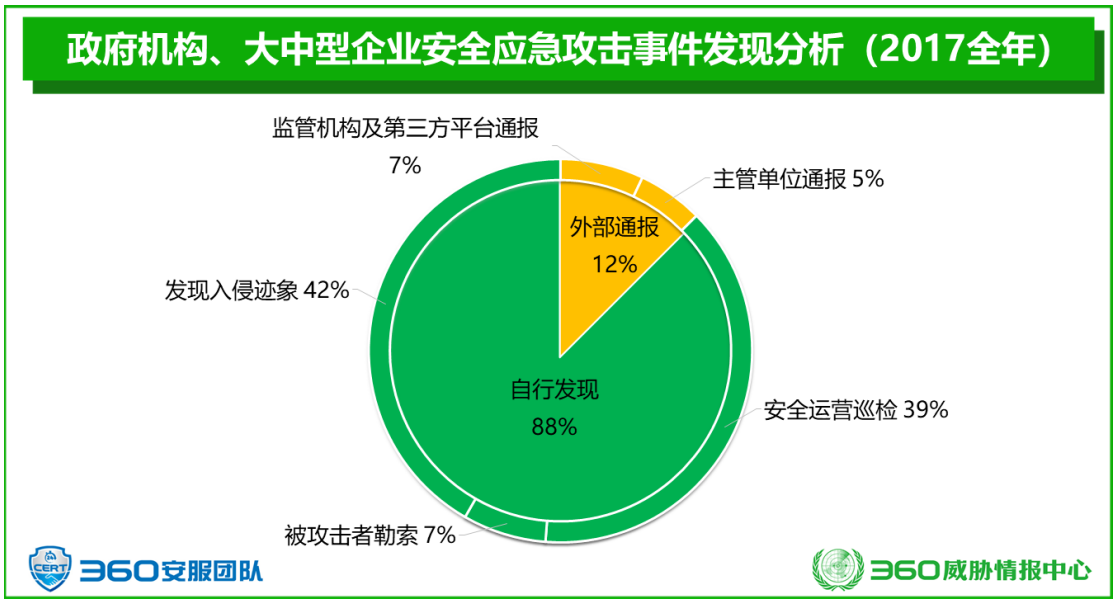


从上述数据中可以看出，行业应急处置排在前三位的分别为政府部门（59 起）、事业单位（24 起）、金融机构（16 起），占到所有行业应急处置的 29.6%、12.1%、8.0%，三者之和约占应急处置事件总量的 49.6%，即全年应急响应事件一半是出在政府部门、事业单位、金融机构。而交通运输、教育培训、能源、IT 信息技术、媒体所产生的应急响应事件也占到了各行业的 33%。

从行业报告排名可知，攻击者的主要攻击对象为各级政府部门、事业单位以及金融机构，其次为交通运输、教育培训、能源、IT 信息技术和媒体，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。

三、 攻击事件发现分析

通过对 2017 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：



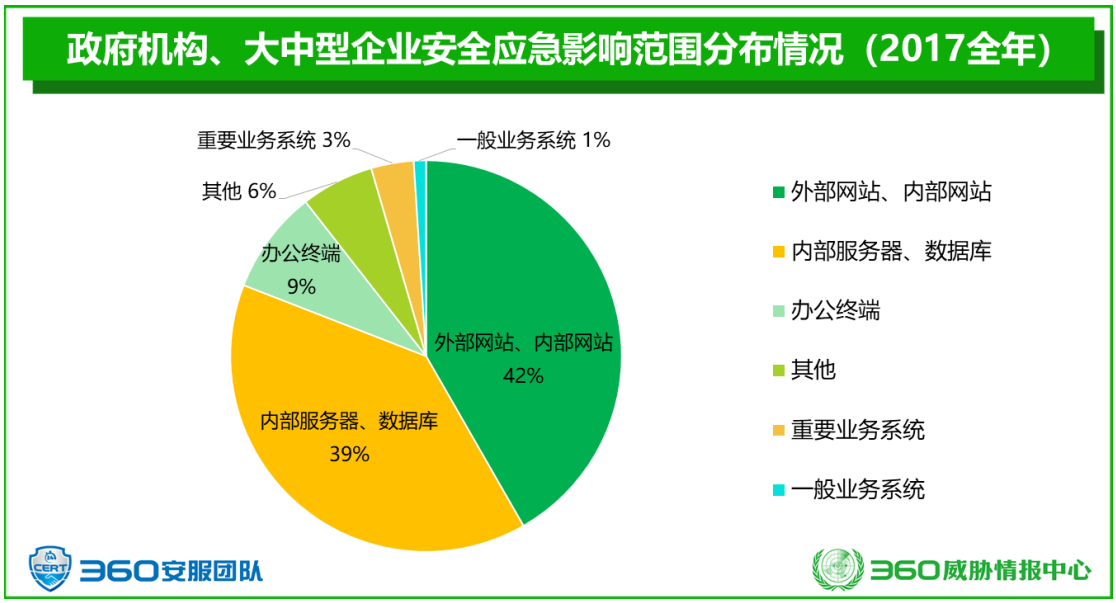
在 2017 年 360 安服团队参与处置的所有政府机构和企业的网络安全应急响应事件中，由行业单位自己发现的安全攻击事件占 88%，而另有 12%的安全攻击事件政府机构和企业实际上是不自知的，他们是在得到了监管机构或主管单位的通报才得知已被攻击。

虽然政府机构和企业自行发现的安全攻击事件占到了 88%，但并不代表其具备了潜在威胁的发现能力。实际上，仅有占安全攻击事件总量 39%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 49%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。

四、 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：



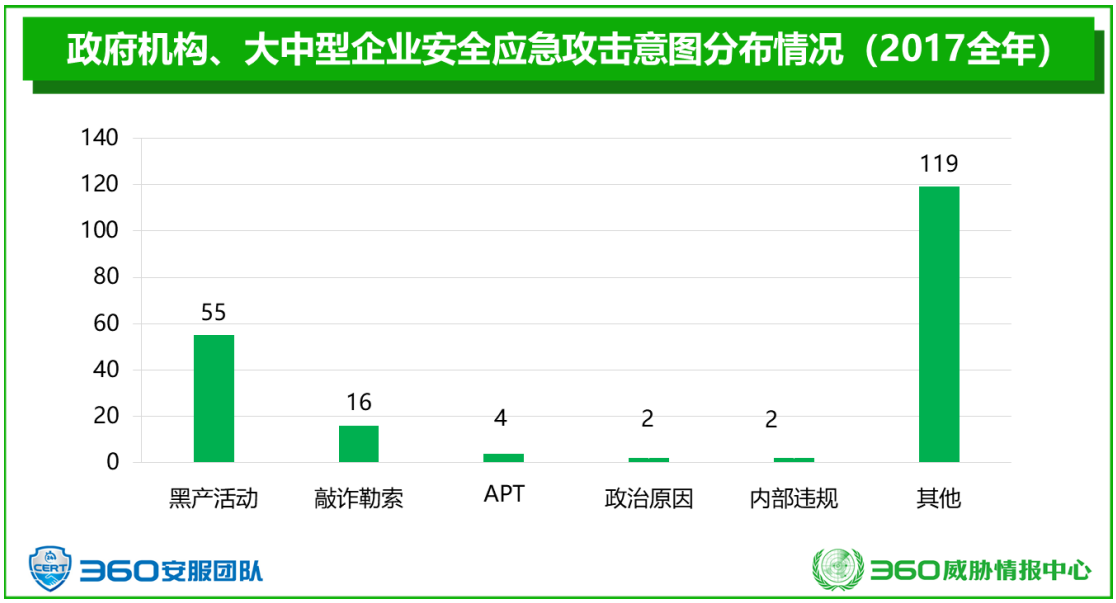
从上述数据中可以看出，安全事件的影响范围主要集中在外部网站和内部网站（42%）、内部服务器和数据库（39%）。除此之外，还占有一定比例的还有办公终端（9%）、重要业务系统（3%）。

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。

五、 攻击意图分布分析

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：

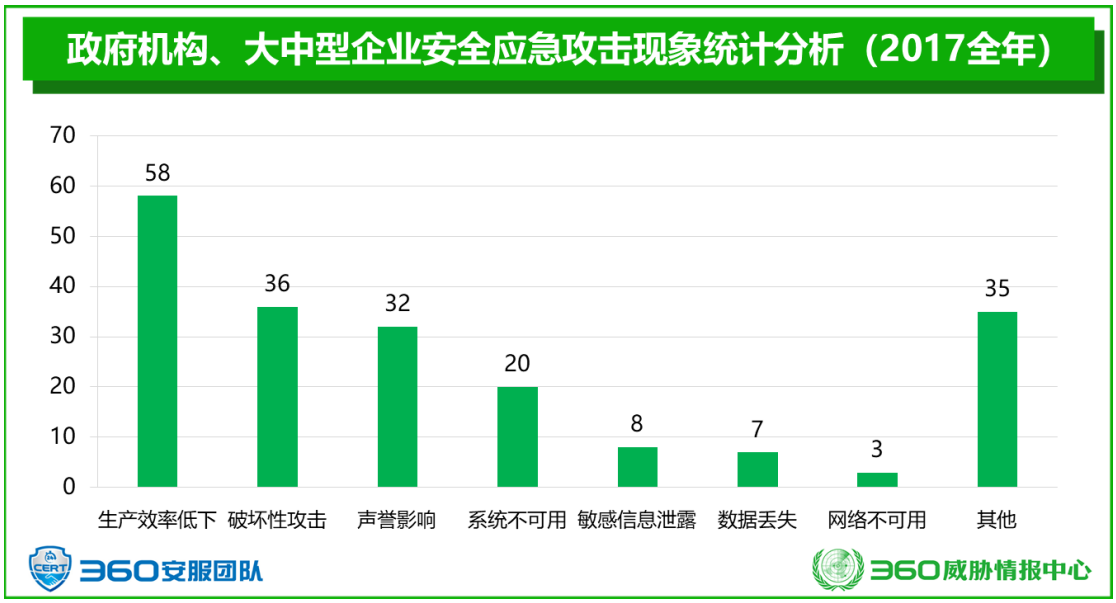


从上述数据中可以看出，黑产活动、敲诈勒索仍然是攻击者攻击政府机构、大中型企业的主要原因。攻击者通过黑词暗链、钓鱼页面、挖矿程序等攻击手段开展黑产活动谋取暴利；利用勒索病毒感染政府机构、大中型企业终端、服务器，对其实施敲诈勒索。对于大部分攻击者而言，其进行攻击的主要原因是为获取暴利，实现自身最大利益。

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。内部违规响应事件的减少，表明业务人员、运维人员的安全意识有所提升。

六、 攻击现象统计分析

通过对 2017 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：



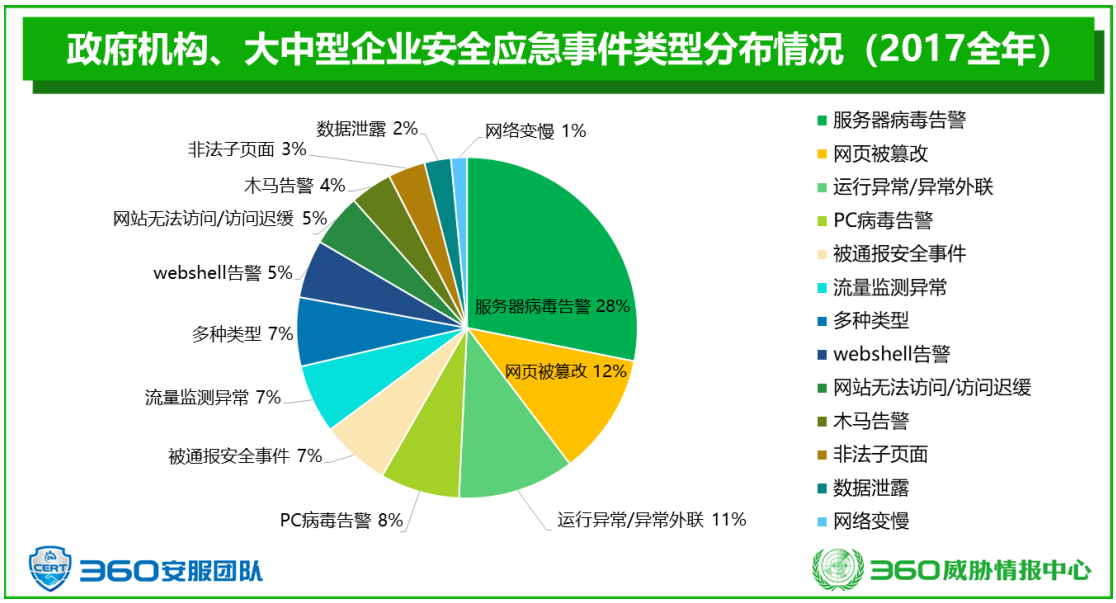
从上述数据可以看出，攻击者对系统的攻击所产生现象主要表现为导致生产效率低下、破坏性攻击、声誉影响、系统不可用。

其中，导致生产效率低下占比 29.1%，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；破坏性攻击占比 18%，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；声誉影响占比 16%，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；系统不可用占比 10%，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。同时，敏感信息泄露、数据丢失、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。

七、 事件类型分布分析

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 28%，成为攻击者主要的攻击手段；网页被篡改是攻击者对互联网门户网站进行的常见攻击，占 12%，严重损害政府机构、大中型企业的声誉；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；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 8%，是对攻击终端的主要手段。

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、webshell 告警等安全事件类型。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。

第三章　应急响应服务分析

根据 2017 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。

一、　网站安全

（一） 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。

（二） 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。

（三） 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。

（四） 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。

（五） 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。

（六） 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。

（七） 网站安全总结及防护建议

1） 安全攻击手段

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：

第一、 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；

第二、 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；

第三、 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；

第四、 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。

2） 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：

第一、 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；

第二、 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；

第三、 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；

第四、 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；

第五、 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；

第六、 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；

第七、 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。

二、 终端安全

（一） 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。

（二） 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。

（三） 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。

（四） 终端安全总结及防护建议

1） 安全攻击手段

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：

第一、 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；

第二、 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。

2） 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：

第一、 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；

第二、 采用统一的防病毒软件，并定时更新，抵御常见木马病毒；

第三、 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；

第四、 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；

第五、 加强员工对终端安全操作和管理培训，提高员工安全意识。

三、 服务器安全

（一） 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。

（二） 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。

（三） 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。

（四） 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。

（五） 服务器安全总结及防护建议

1） 安全攻击手段

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：

第一、 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；

第二、 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。

2） 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：

第一、 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；

第二、 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；

第三、 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；

第四、 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；

第五、 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；

第六、 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；

第七、 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；

第八、 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；

第九、 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。

四、 邮箱安全

（一） 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。

（二） 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。

（三） 邮箱安全总结及防护建议

1） 安全攻击手段

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：

第一、 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；

第二、 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。

2） 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：

第一、 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；

第二、 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；

第三、 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；

第四、 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；

第五、 部署安全邮件网关进一步加强邮件系统安全。

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 60 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。