2019 年

中国政企机构
网络安全形势分析报告

奇安信行业安全研究中心

2020 年 03 月 13 日

摘 要

办公安全

- 2019 年全国共有 2237 家政企单位受到勒索病毒攻击，累计涉及终端 10.6 万台。
- 从被攻击终端类型来看，被攻击的 10.6 万台终端中，83.3%是办公电脑，16.7%是服务器。
- 根据 Coremail 论客与奇安信行业安全研究中心的联合监测，同时综合网易、腾讯、阿里巴巴等主流企业邮箱服务提供商的公开数据进行分析评估，截止 2019 年底，国内注册的企业邮箱独立域名约为 520 万个，相比 2018 年增长 1.96%。活跃的国内企业邮箱用户规模约为 1.4 亿，相比 2018 年用户规模增长了 7.7%。
- 2019 年，在邮件系统收发的邮件中，仅有近 4 成为正常邮件，垃圾邮件及其他各类非法、恶意邮件等非正常邮件的数量，是正常邮件数量的 1.6 倍左右。
- 2019 年，全国企业邮箱用户共收到各类垃圾邮件约占企业级用户邮件收发总量的 47.2%，是企业级用户正常邮件数量的 1.2 倍。相比 2018 年下降了 17.9%。全国企业邮箱用户共收到各类钓鱼邮件约 344.3 亿封，相比 2018 年收到各类钓鱼邮件的 204.3 亿封增长了 68.5%。全国企业级用户共收到约 424.3 亿封带毒邮件，相比 2018 年收到的 203.7 亿封带毒邮件相比，同比增长了 108.36%。

网站安全

- 2019 年，在接受网站安全监测平台检测的 6045405 个网站中，共有 347514 个（单月去重）网站被扫描检测出安全漏洞，占比为 5.7%，被扫描检出 3131473 次安全漏洞。
- 2019 年，奇安信网站卫士共为全国 135600 个网站拦截各类网站漏洞攻击 46.9 亿次，平均每天拦截漏洞攻击 1286.2 万次。
- 2019 年，补天平台共收录全国相关网站的 68521 个安全漏洞。从行业分布来看，来自教育培训行业的漏洞最多，共 5890 个，占全年漏洞的 8.6%；其次是政府及事业单位，共 5369 个，占比约为 7.8%；制造业排名第三，占比 5.5%。
- 从漏洞的危险等级来看，高危漏洞 14650 个，占比为 21.4%；中危漏洞 39237 个，占比为 57.2%；低危漏洞 14634 个，占比为 21.4%。从漏洞的技术类型来看，SQL 注入漏洞最多，占比为 33.4%，其次是信息泄露漏洞，占比为 16.7%，弱口令漏洞，占比为 12.0%。

应急响应

- 2019 年全年，奇安信集团安服团队共参与和处置了 1029 起全国范围内的网络安全应急响应事件，同比 2018 年全年增长 312 起，投入工时为 2018 年同期的 1.24 倍。

- 2019 年全年应急处置事件最多的行业 TOP3 分别为：政府及事业单位（250 起）、医疗卫生行业（153 起）以公检法（84 起），事件处置数分别占应急处置所有行业的 24.3%、14.8%、8.2%。

- 2019 年全年应急事件中，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。

- 通过对 2019 年全年应急响应处理漏洞利用攻击事件进行统计分析，弱口令、永恒之蓝漏洞是政企机构、大中型企业被攻陷的重要原因。

专题研究

- 根据中国国家信息安全漏洞共享平台最新统计，截止到 2019 年 12 月，CNVD 收录的与工业控制系统相关的漏洞高达 2306 个，2019 年新增的工业控制系统漏洞数量达到 413 个。

- 在四大漏洞平台收录的工业控系统漏洞中，高危漏洞占比 57.3%，中危漏洞占比为 35.5%，中高危漏洞占比高达 92.8%。

- 奇安信威胁情报中心在 2019 年监测到的高级持续性威胁相关公开报告总共 596 篇。从公开披露的高级威胁活动中涉及目标行业情况来看（摘录自公开报告中提到的攻击目标所属行业标签），政府（包括外交、政党、选举相关）和军事（包括军事、军工、国防相关）依然是 APT 威胁的主要目标，能源（包括石油、天然气、电力、民用核工业等）、通信行业也是 APT 攻击的重点威胁对象。

- 2019 年上半年，网络安全人才需求规模指数为 117.2，较 2018 年下半年环比增长了 104.9%，较 2018 年上半年同比增长 173.2%。

- 对网络安全人才需求量最大的行业是 IT 信息技术，其发布的网络安全人才招聘数量占所有网络安全人才招聘总人数的 42.4%，其次为互联网，占 13.7%。

- 高校分布进一步亲民化，不再是重点高校学生占据排行榜首，大量的省/市地方院校也加入培养网络安全人才的大军。95 后的毕业生或求职者开始崭露头角。

- 69%的新晋网络安全人才更感兴趣的网络安全领域或技术方向是大数据安全，62.1%的网络安全人才更感兴趣人工智能安全，其次是 5G/物联网安全。

目 录

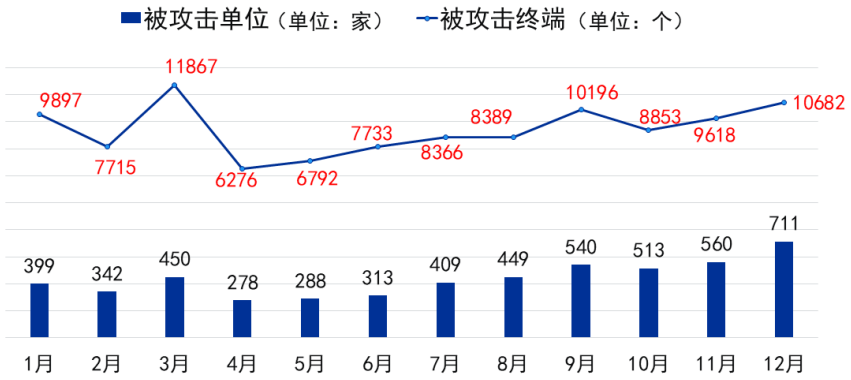
第一篇 办公安全

第一章　勒索病毒分析

一、　全年攻击态势

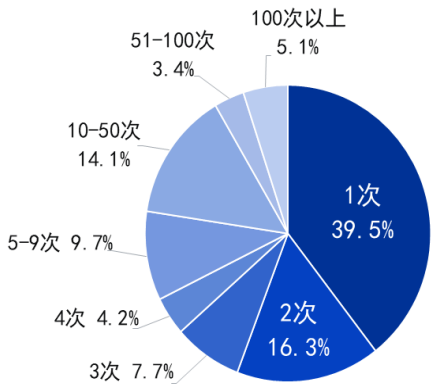
2019 年 1-12 月奇安信病毒响应中心数据显示，2019 年全国共有 2237 家政企单位受到勒索病毒攻击，累计涉及终端 10.6 万台。从被攻击单位来看，12 月被攻击情况最严重，累计约有 711 家企业被勒索病毒攻击。从被攻击终端数量来看，3 月涉及终端最多，全国共有 11867 个终端遭受到勒索攻击。具体每月被攻击情况分布如下图所示。

2019年政企单位遭遇勒索攻击整体攻击态势



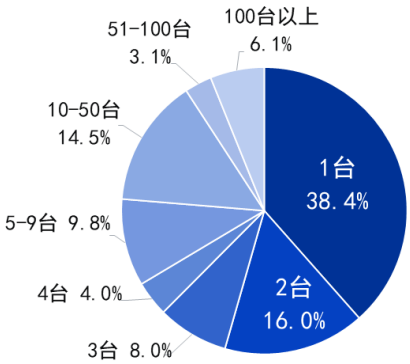
在被攻击政企单位中，39.5%的单位仅受到一次勒索攻击，5.1%的政企单位全年遭到 100 次以上勒索病毒攻击。

2019年政企单位被勒索病毒攻击频率



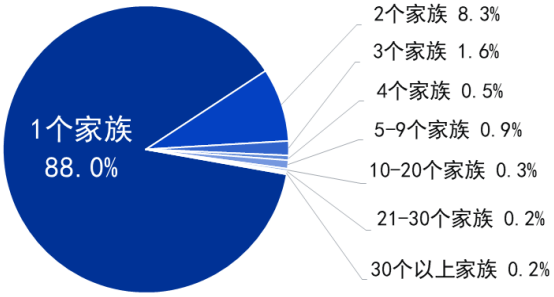
在政企单位所遭受的勒索病毒攻击事件中，就单个单位全年累计被攻击量来看，38.4%政企单位仅一台终端受到勒索病毒攻击，6.1%政企单位累计有 100 台以上终端被勒索病毒攻击。

2019年政企单位被勒索病毒攻击终端数量



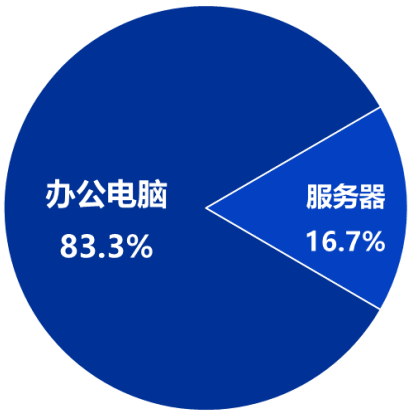
在政企单位所遭受的勒索病毒攻击事件中，88.0%政企单位全年仅被一个勒索病毒家族攻击过，0.2%政企单位全年累计遭到 30 个以上勒索家族攻击。

2019年政企单位被勒索病毒攻击遭遇勒索家族数量



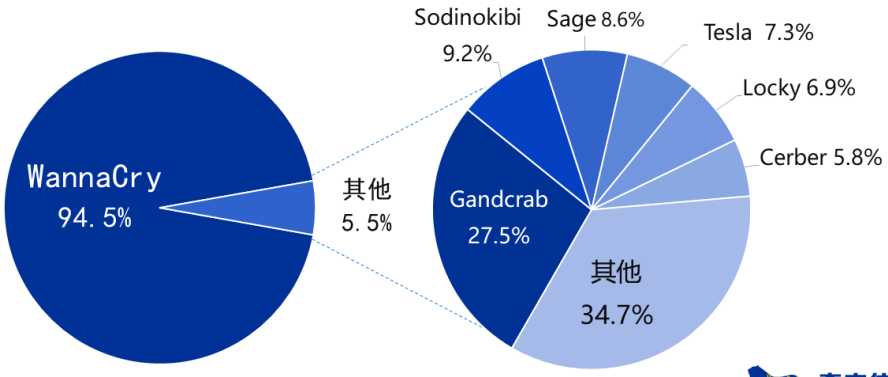
从被攻击终端类型来看，被攻击的 10.6 万台终端中，83.3%是办公电脑，16.7%是服务器。

2019年政企单位遭遇勒索攻击终端类型



2019 年遭到攻击的所有勒索攻击中，94.5%为 WannaCry 类勒索攻击。其他类勒索攻击中，Gandcrab、Sondinokibi、Sage 这三大家族勒索病毒的受害者最多，其中，来自 Gandcrab 勒索家族占其他攻击终端总数的 27.5%；其次为 Sodinokibi 家族，占比 9.2%。具体分布如下图所示：

2019年政企机构终端遭遇勒索家族攻击分布

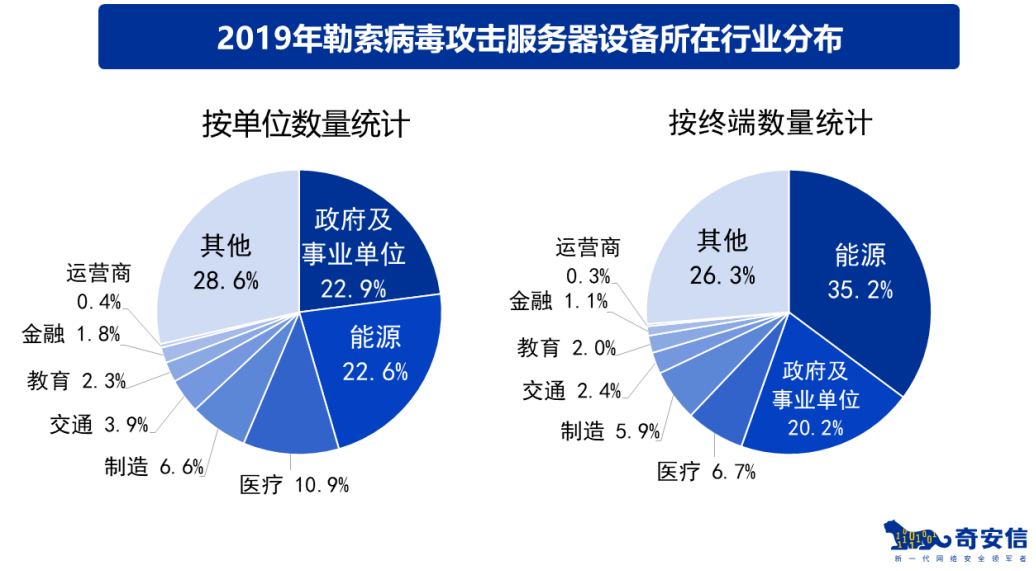


二、 行业分布情况

从被攻击单位来看，2019 年，被勒索病毒攻击的服务器所在行业中，政府及事业单位占比最多，占 22.9%；能源行业排名第二，占 22.6%；医疗排名第三，占 10.9%。

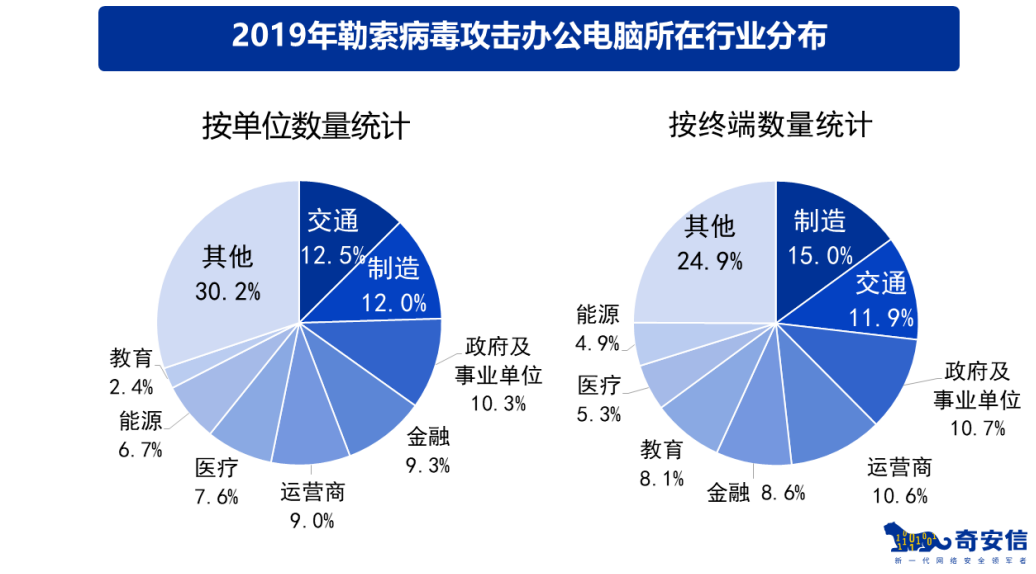
从被攻击终端分布来看，2019 年勒索病毒攻击的服务器所在行业中，能源行业遭到攻击的终端最多，占 35.2%；其次是政府及事业单位占 20.2%，医疗行业排名第三，占 6.7%。

具体分布如下图所示：



从单位分布来看，2019 年勒索病毒攻击办公电脑中，分布在交通行业的最多，占 12.5%，其次是制造业，占 12.0%，政府及事业单位排名第三，占 10.3%。

从终端分布来看，2019 年勒索病毒攻击的办公电脑中，排名前三的行业分别是制造业（15.0%）、交通（11.9%）以及政府及事业单位（10.7%）。



从不同行业单位被勒索病毒攻击频率来看，在服务器被勒索病毒攻击的单位中，能源行业是被攻击次数最多的行业，平均每单位被攻击 40.8 次；在办公电脑被勒索攻击的单位中，运营商行业是被攻击次数最多的行业，平均每单位被攻击 185.1 次。

2019年被攻击单位遭受勒索病毒攻击频率行业分布

服务器

行业	平均被攻击次数	每次攻击端数
能源	40.8	1.5
制造	9.8	2.6
其他	8.5	1.0
政府及事业单位	6.3	1.5
交通	5.7	1.0
运营商	4.6	1.4
医疗	3.7	1.0
金融	3.6	1.0
教育	2.9	1.5

办公电脑

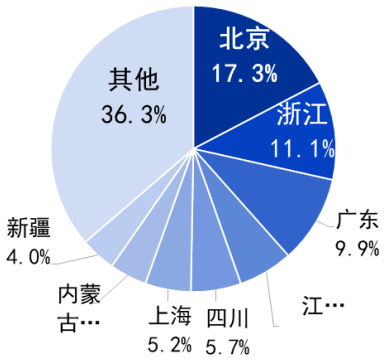
行业	平均被攻击次数	每次攻击端数
运营商	185.1	1.9
交通	73.8	2.4
制造	67.4	2.0
金融	66.2	1.8
能源	44.7	2.3
企业	44.5	1.4
教育	25.2	1.4
政府及事业单位	20.6	6.6
医疗	12.6	1.6

三、 地域分布情况

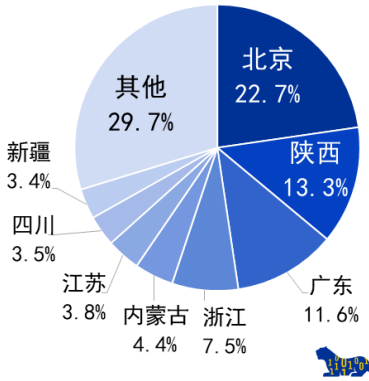
从勒索病毒攻击服务器设备地域分布来看，在服务器被勒索病毒攻击的单位中，北京是数量最多的地区，占比为 17.3%，从被攻击终端开看，在服务器被勒索病毒攻击的单位中，北京同样是数量最多的地区，占比为 22.7%。

2019年勒索病毒攻击服务器设备地域分布

按单位数量统计



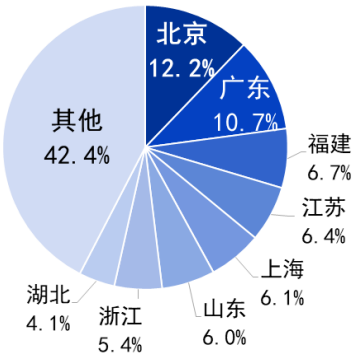
按终端数量统计



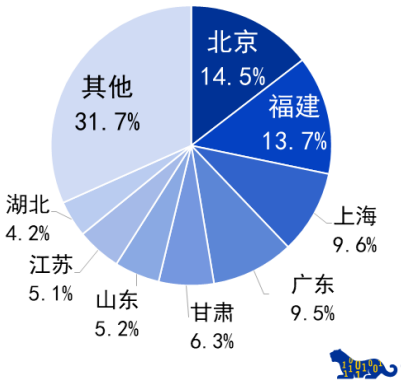
从勒索病毒攻击办公电脑地域分布来看，无论是按被攻击单位统计，还是按被攻击终端数量统计，北京均排名第一。分别占比 12.2%与 14.5%。具体分布如下图所示。

2019年勒索病毒攻击办公电脑地域分布

按单位设备统计



按终端数量统计



第二章　企业邮件安全分析

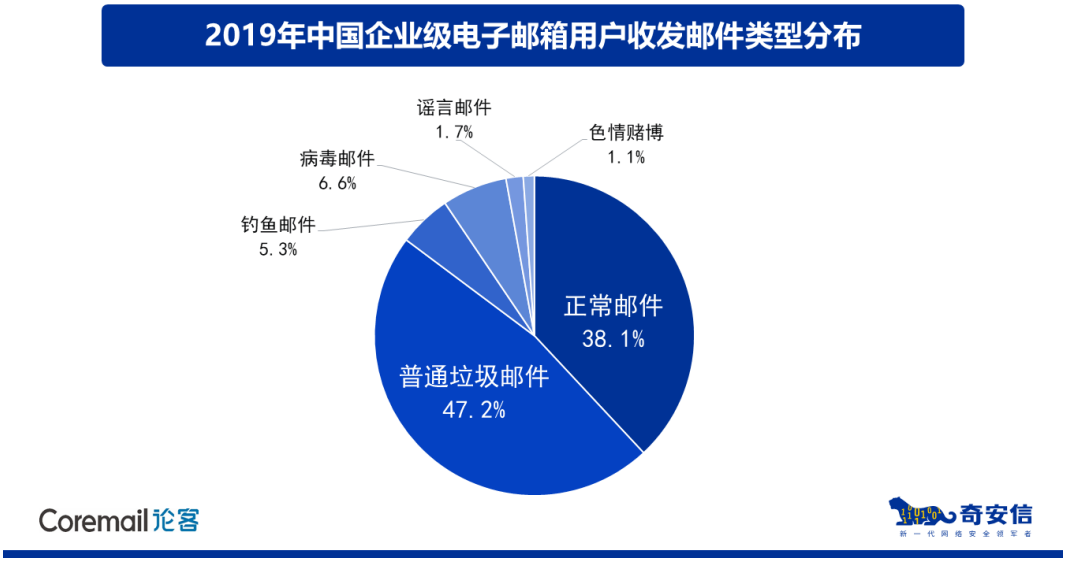
本章数据主要来自 Coremail 论客与奇安信集团联合监测，以电子邮箱的使用、垃圾邮件、钓鱼邮件、带毒邮件为主体，从规模、行业分布及地域分布等方面分析中国企业邮箱安全性。结合了 Coremail 论客与奇安信集团多年在企业邮箱领域的丰富实践经验及研究经验，相关研究成果具有很强的代表性。希望能够对各个行业、单位，开展以邮件防护为基础，增强完善整体网络安全建设，提供一定参考。

《2019 年中国企业邮箱安全性研究报告》完整版可点击下方链接，通过奇安信官网下载查阅。下载链接：https://www.qianxin.com/threat/reportdetail?report_id=41

一、　电子邮箱的使用规模

根据 Coremail 论客与奇安信行业安全研究中心的联合监测，同时综合网易、腾讯、阿里巴巴等主流企业邮箱服务提供商的公开数据进行分析评估，截止 2019 年底，国内注册的企业邮箱独立域名约为 520 万个，相比 2018 年增长 1.96%。活跃的国内企业邮箱用户规模约为 1.4 亿，相比 2018 年用户规模增长了 7.7%。

从电子邮箱的使用情况来看，2019 年，全国企业邮箱用户共收发各类电子邮件约 6448.1 亿封，相比 2018 年企业及电子邮箱用户收发邮件数量增长 4.8%。平均每天收发电子邮件约 17.7 亿封。其中，正常邮件占比约为 38.1%，普通垃圾邮件占比为 47.2%、钓鱼邮件 5.3%、病毒邮件 6.6%、谣言邮件 1.7%，色情、赌博等违法信息推广邮件约 1.1%。也就是说，2019 年，在邮件系统收发的邮件中，仅有近 4 成为正常邮件，垃圾邮件及其他各类非法、恶意邮件等非正常邮件的数量，是正常邮件数量的 1.6 倍左右。

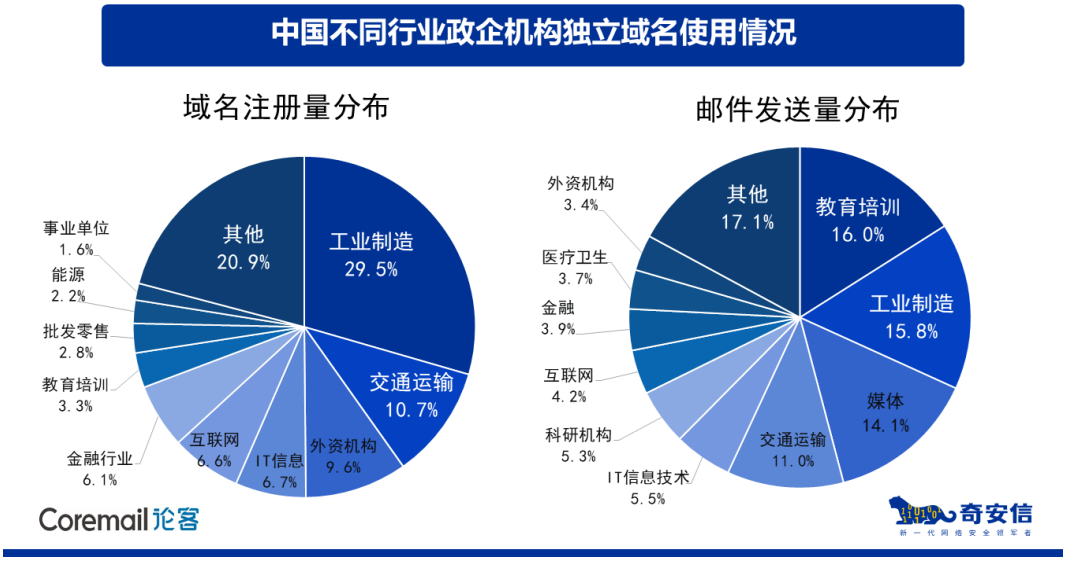


仅就正常邮件而言，统计显示，全国企业邮箱用户在 2019 年共收发正常电子邮件约 2454.1 亿封，比 2018 年增长 25.4%，平均每天发送正常电子邮件约 6.7 亿封，人均每天发送电子邮件约 4.8 封。相比 2018 年人均每天发送 4.1 封邮件，增长了 0.7 封。企业信息化办公程度的逐年提高，很大程度上促进了员工企业邮箱的使用。同时，随着国际化趋势，企业组织间交流合作逐步增多，对于跨国交流而言，相比于其他通讯软件，电子邮件更为通用。

二、 电子邮箱用户行业分布

对中国政企机构独立邮箱域名的抽样分析显示，从域名注册量来看，工业制造类企业注册的邮箱域名最多，占比为 29.5%，其次是交通运输行业占比 10.7%，外资机构占比 9.6%；还有 IT 信息技术占比 6.7%，互联网企业占比 6.6%，金融行业占比 6.1%等，这些都属于电子邮箱使用独立域名较多的行业。

如果从正常邮件的发送量上来看，教育培训和工业制造行业发送的邮件数量最多，教育培训找 16.0%，排名第一；工业制造占比 15.8%，排名第二；其次是媒体占比为 14.1%，交通运输行业占比 11.0%；还有 IT 信息技术占比 5.5%，科研机构、互联网、金融行业等也都是邮件发送量较多的行业。具体占比如下图所示：

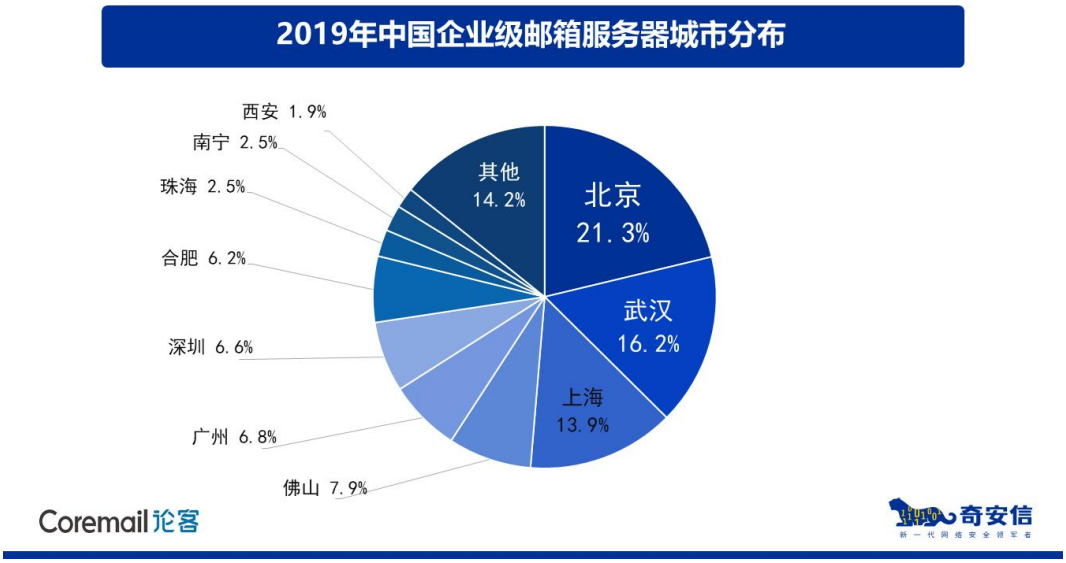


三、 电子邮件的服务器地域分布

统计显示，全国企业邮箱用户收发的邮件以境内收发为主。国内收发占 65.6%；海外收发 34.4%。

从服务器的所在地来看，2019 年，国内企业邮箱服务器设在北京的数量排名第一，占比为 21.3%；武汉排第二，占比为 16.2%；上海排名第三，占比 13.9%。值得注

意的是，在 2017 年的相关统计中，国内有半数以上的企业邮箱服务器是设在杭州市的。这表明，针对政企机构的邮箱服务正在从局部地区高度集中，向全国各地分散开来。这也是全国各地信息化建设水平普遍显著提升的必然结果。

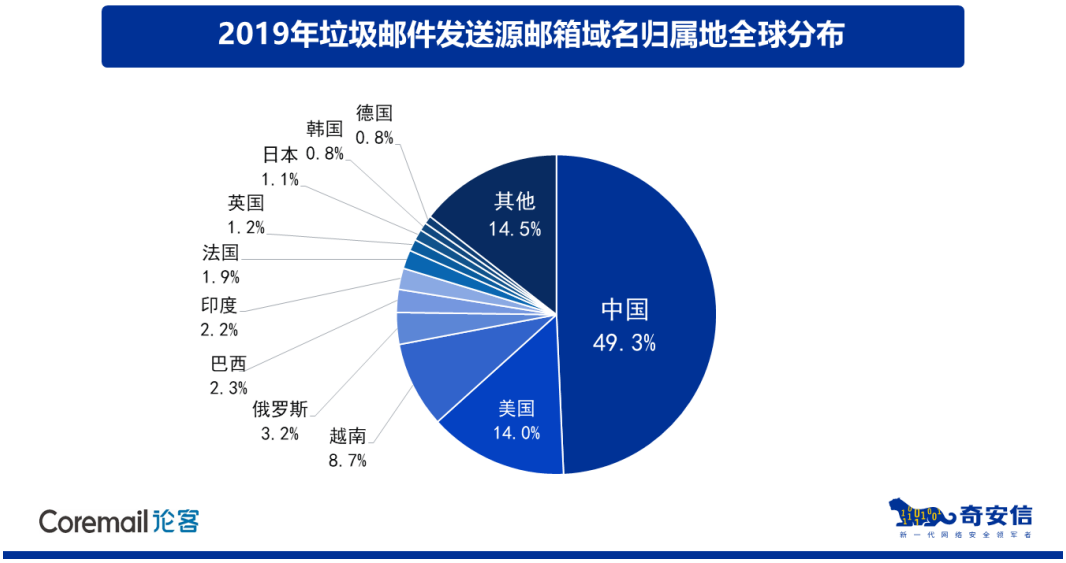


四、 非正常邮件规模

（一） 垃圾邮件

根据 Coremail 论客与奇安信行业安全研究中心的联合监测评估，2019 年，全国企业邮箱用户共收到各类垃圾邮件约占企业级用户邮件收发总量的 47.2%，是企业级用户正常邮件数量的 1.2 倍。相比 2018 年下降了 17.9%。

从发送者邮箱域名归属情况来看，来自国内的垃圾邮件最多，占总数的 49.3%，来自美国的垃圾邮件次之，占总量约 14.0%，第三是越南，约占 8.7%。具体占比如下图所示：



与 2017 年垃圾邮件发送源邮箱域名归属地分布情况对比，来自境外的垃圾邮件占比由近 7 成减少至 5 成左右，2019 年，更多的垃圾邮件来自境内。

（二） 钓鱼邮件的规模

在本小节内容中，钓鱼邮件是指含有恶意欺诈信息的邮件，包括 OA 钓鱼邮件、鱼叉邮件、钓鲸邮件、CEO 仿冒邮件和其他各类钓鱼欺诈邮件，但不包括带毒邮件、非法邮件等。

根据 Coremail 论客与奇安信行业安全研究中心的联合监测评估，2019 年，全国企业邮箱用户共收到各类钓鱼邮件约 344.3 亿封，相比 2018 年收到各类钓鱼邮件的 204.3 亿封增长了 68.5%。

2019 年全国企业邮箱用户收到的钓鱼邮件数量约占企业级用户邮件收发总量的 5.3%，平均每天约有 0.9 亿封钓鱼邮件被发出和接收。

（三） 带毒邮件的规模

根据 Coremail 论客与奇安信行业安全研究中心联合监测评估，2019 年，全国企业级用户共收到约 424.3 亿封带毒邮件，相比 2018 年收到的 203.7 亿封带毒邮件相比，同比增长了 108.36%。越来越多的带毒邮件正在被发送给企业邮箱。2019 年企业级用户收到的带毒邮件量约占用户收发邮件总量的 6.6%。平均每天约有 1.2 亿封带毒邮件被发出和接收。

第二篇 网站安全

第三章　网站漏洞监测分析

网站漏洞整体形势可以从两个角度分析：一是网站安全检测分析，二是网站漏洞攻击分析。本章将以奇安信网站安全检测与防护相关产品的统计结果为依据，分析 2019 年 1-12 月中国网站漏洞情况。

一、　网站安全检测

本节主要以奇安信网站安全监测平台数据为基础，对全国网站漏洞情况进行统计分析。

2019 年 1-12 月，在接受网站安全监测平台检测的 6045405 个网站中，共有 347514 个（单月去重）网站被扫描检测出安全漏洞，占比为 5.7%，被扫描检出 3131473 次安全漏洞。

对奇安信网站安全监测平台扫描出漏洞次数最多的 10 个漏洞类型进行分析，我们发现 2019 年 1-12 月前 10 的漏洞类型之和占到了总量的 70.1%。具体占比如下表所示。

排名	漏洞类型	占比
1	跨站脚本攻击漏洞	37.3%
2	SQL 注入漏洞（盲注）	8.5%
3	发现目录启用了自动目录列表功能	8.2%
4	SQL 注入漏洞	5.7%
5	X-Frame-Options 头未设置	3.3%
6	Flash 配置不当漏洞	2.8%
7	发现目录开启了可执行文件运行权限	1.6%
8	发现 install.php 文件	1.1%
9	WEB 服务器启用了 OPTIONS 方法	0.8%
10	.htaccess 文件可读	0.8%

表 1　扫出漏洞最多的漏洞类型及漏洞次数占比

对奇安信网站安全监测平台扫描出漏洞次数最多的高危漏洞类型进行分析，我们发现2019 年 1-12 月排名前 5 的高危漏洞类型之和占到了高危漏洞总数的 49.3%。具体占比如下表所示。

排名	高危漏洞类型	占比
1	跨站脚本攻击漏洞	26.9%
2	SQL 注入漏洞（盲注）	12.8%
3	SQL 注入漏洞	8.6%
4	发现 SVN 版本控制信息文件	0.6%
5	SQL 注入漏洞（path）	0.4%

表 2　高危漏洞扫出漏洞最多的漏洞类型及漏洞次数占比

二、　网站漏洞攻击分析

本节将主要以奇安信网站卫士数据，对网站漏洞攻击的情况进行分析。

2019 年 1-12 月，奇安信网站卫士共为全国 135600 个网站拦截各类网站漏洞攻击 46.9 亿次，平均每天拦截漏洞攻击 1286.2 万次。

2019 年 1-12 月，全国漏洞攻击次数最多的 10 个类型拦截量占到了漏洞拦截总量的 95.8%，其中，protocol invalidation 类漏洞最多，占 34.0%。具体情况如下表所示。

排名	漏洞类型	占比
1	protocol invalidation	34.0%
2	SQL 注入	19.7%
3	webshell	13.5%
4	通用漏洞	12.5%
5	XSS	5.3%
6	扫描器	4.6%
7	本地文件包含	2.1%
8	RFI	1.6%
9	文件备份探测	1.3%
10	nginx 攻击	1.2%

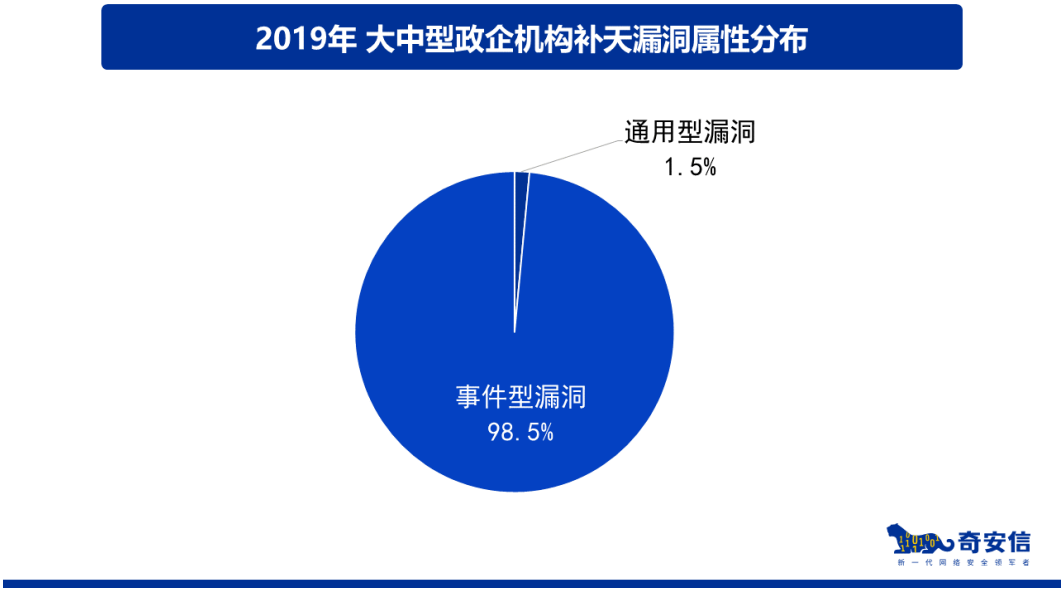
表 3　漏洞类型及攻击次数占比

第四章　人工挖掘漏洞分析

开放的第三方漏洞报告平台收录的某个地区的网站漏洞数量，也是考察该地区网络安全状况的参考指标。本章主要以补天平台数据为基础，对人工报告的网站漏洞情况进行分析。

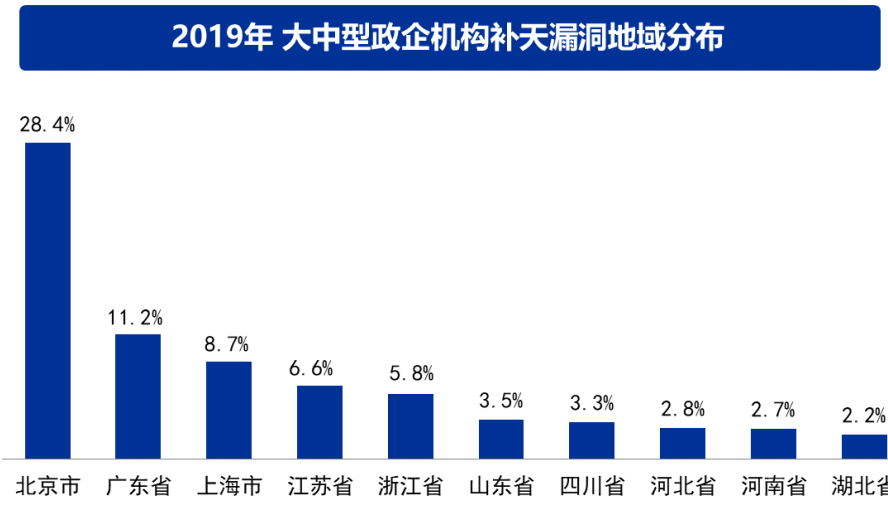
一、　漏洞报告数量

2019 年 1-12 月，补天平台共收录全国相关网站的 68521 个安全漏洞，其中 67471 个为事件型漏洞，占全年漏洞的 98.5%；1050 个为通用型漏洞，占 1.5%。



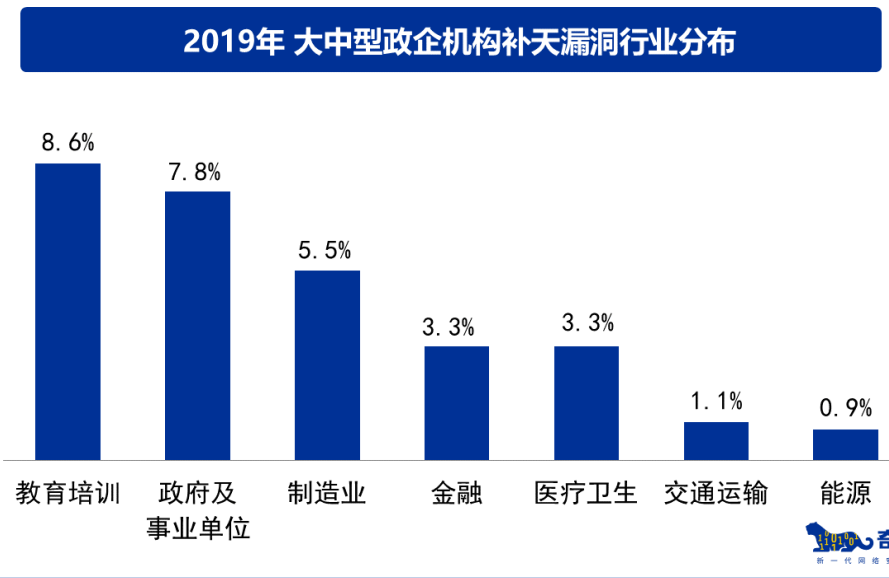
二、　漏洞地域分析

从网站的 IP 归属地（省级）来看,来自北京市的网站被报告漏洞数量最多，共 19437 个，占比约为 28.4%；其次是广东省，共 7703 个，占比为 11.2%；上海市排第三，占比 8.7%。



三、 漏洞行业分布

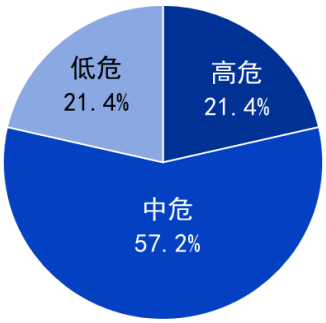
从行业分布来看，2019 年，来自教育培训行业的漏洞最多，共 5890 个，占全年漏洞的 8.6%；其次是政府及事业单位，共 5369 个，占比约为 7.8%；制造业排名第三，占比 5.5%。具体分布如下图所示：



四、 漏洞类型分析

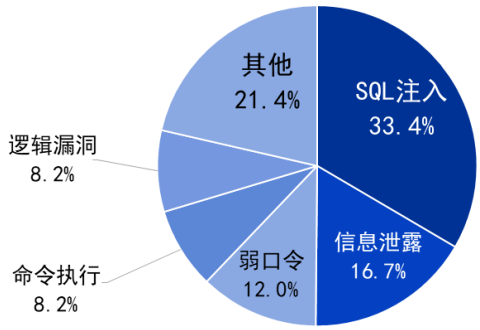
从漏洞的危险等级来看，高危漏洞 14650 个，占比为 21.4%；中危漏洞 39237 个，占比为 57.2%；低危漏洞 14634 个，占比为 21.4%。

2019年 大中型政企机构补天漏洞等级分布



从漏洞的技术类型来看，SQL 注入漏洞最多，占比为 33.4%，其次是信息泄露漏洞，占比为 16.7%，弱口令漏洞，占比为 12.0%。具体漏洞类型分布请见下图。

2019年 大中型政企机构补天漏洞类型分布



第三篇 应急响应

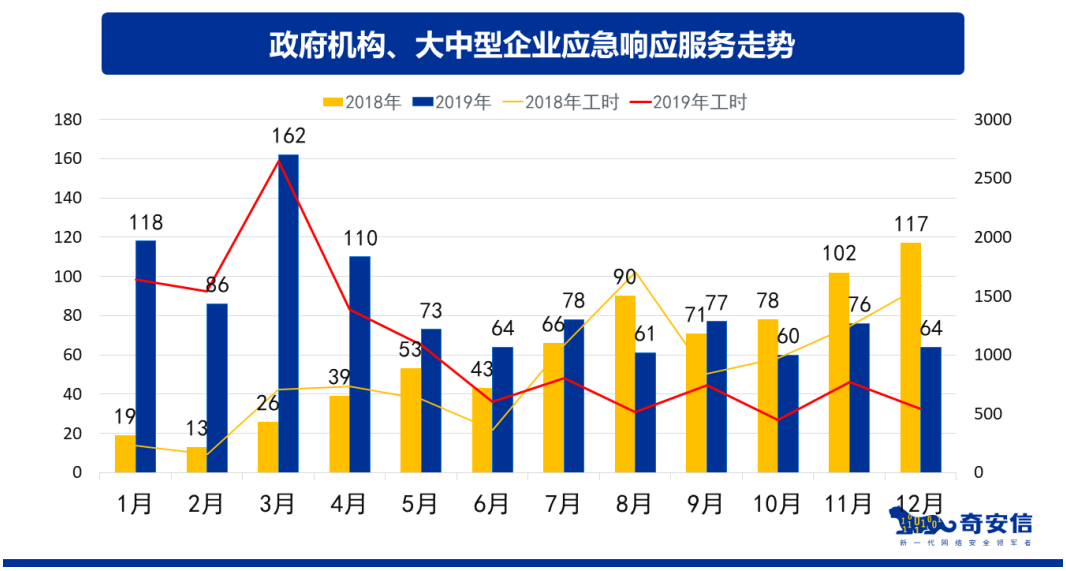
第五章　网络安全应急响应分析

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。本章将以奇安信安服团队应急响应情况为依据，分析 2019 年中国网络安全重大事故处置情况。

《2019 年网络安全应急响应分析报告》完整版可点击下方链接，通过奇安信官网下载查阅。下载链接：https://www.qianxin.com/threat/reportdetail?report_id=43

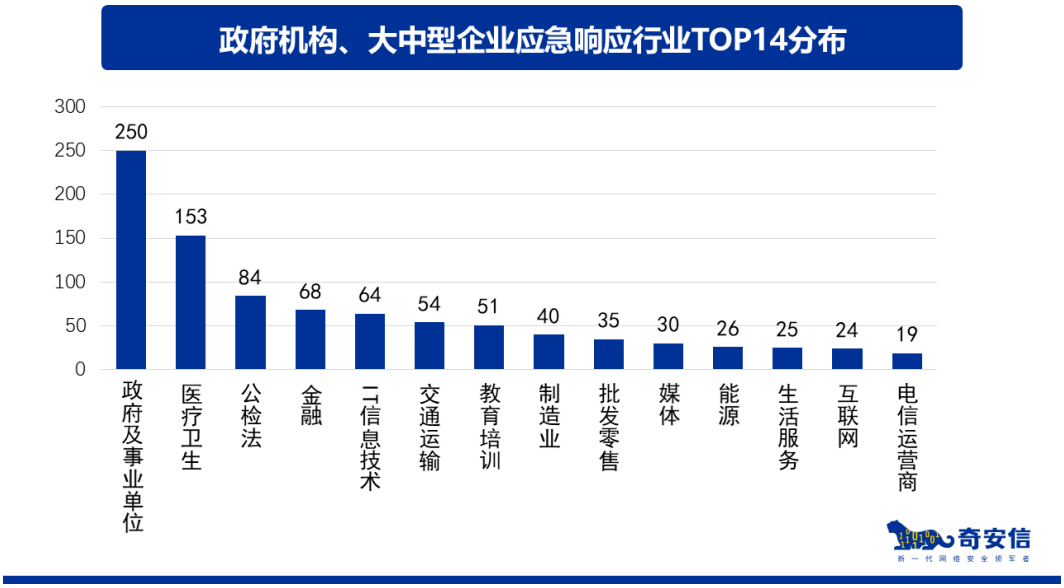
一、　全年应急情况统计

2019 年全年，奇安信集团安服团队共参与和处置了 1029 起全国范围内的网络安全应急响应事件，同比 2018 年全年增长 312 起，投入工时为 2018 年同期的 1.24 倍。通过对 2019 年全年数据分析，19 年 1 月至 3 月，应急请求逐月上升，于 3 月份达到全年最高，4 月份之后应急请求逐渐趋于平稳。

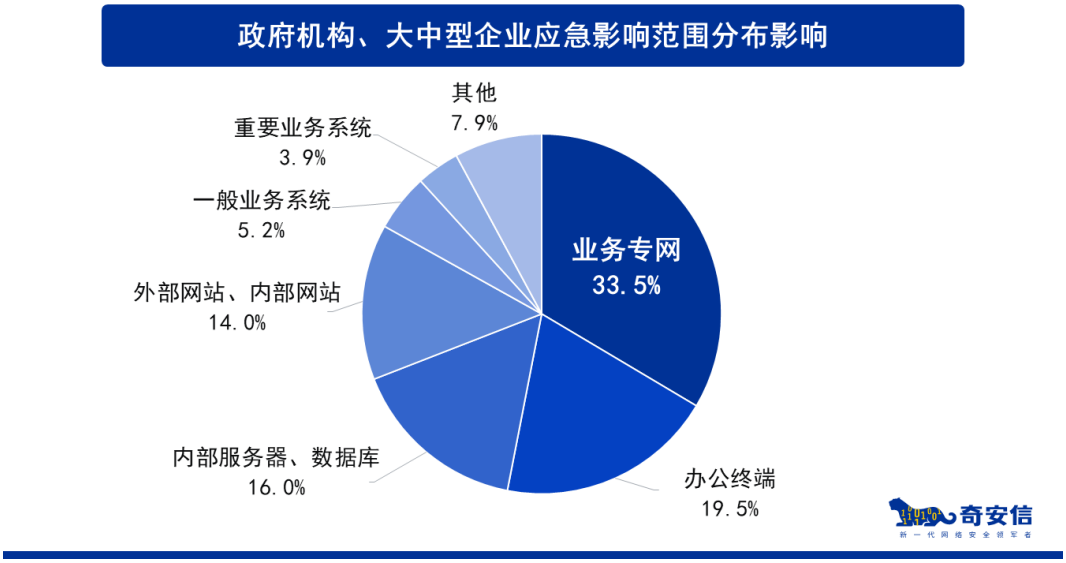


二、　应急事件受害者分析

2019 年全年应急处置事件最多的行业 TOP3 分别为：政府及事业单位（250 起）、医疗卫生行业（153 起）以公检法（84 起），事件处置数分别占应急处置所有行业的 24.3%、14.8%、8.2%。三者之和约占应急处置事件总量的 39.2%，即全年近半数的应急处置事件发生于政府及事业单位、医疗卫生以及公检法行业。政企机构、大中型企业应急行业分布 TOP14 详见下图：

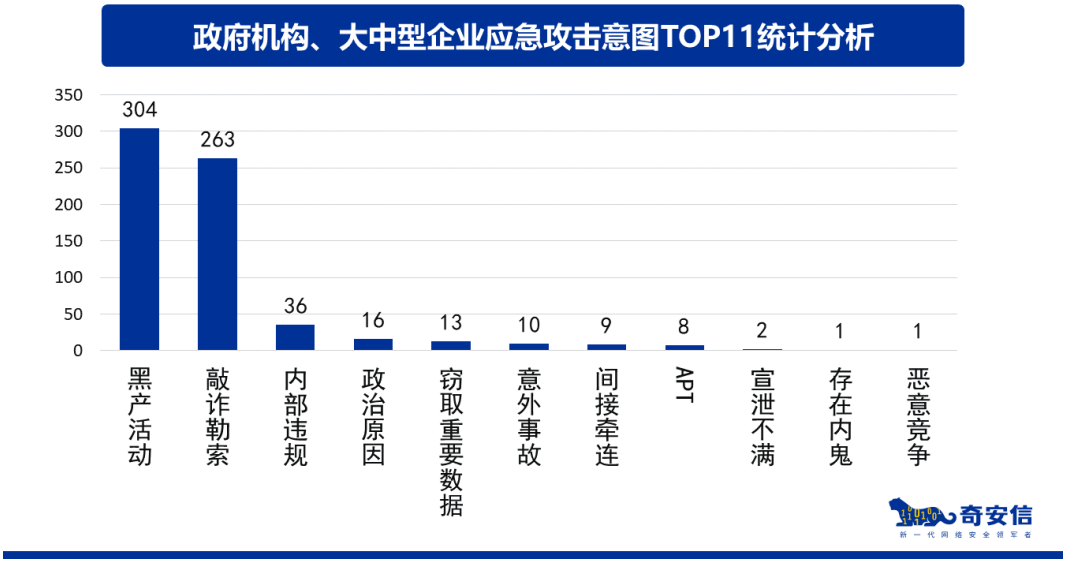


2019 年全年应急安全事件的影响范围主要集中在业务专网，占比 33.5%；办公终端，占比为 19.5%。其次为内部服务器和数据库，16.0%；外部网站和内部网站，14.0%。

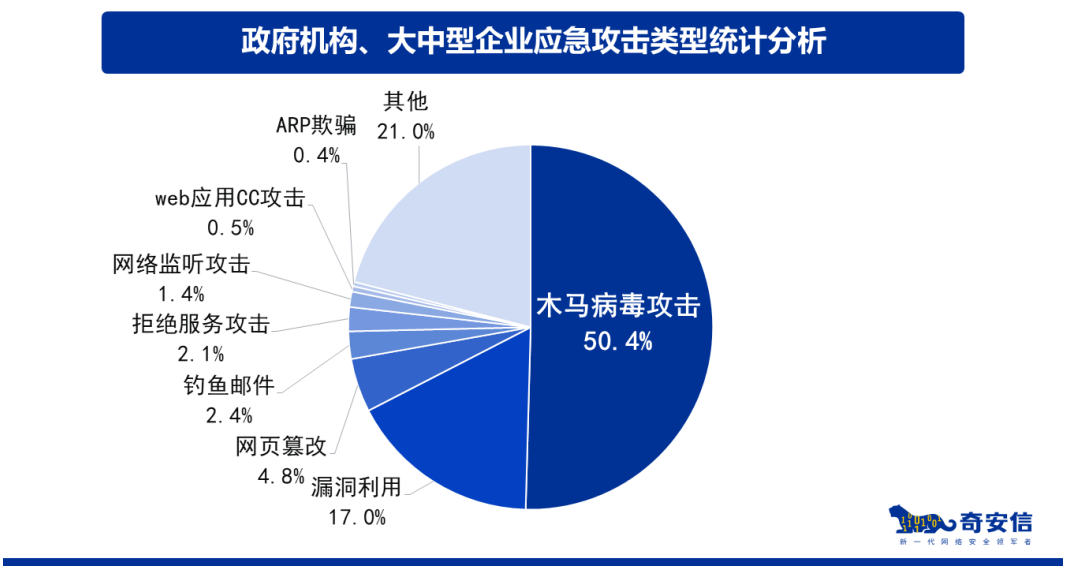


三、 应急事件攻击者分析

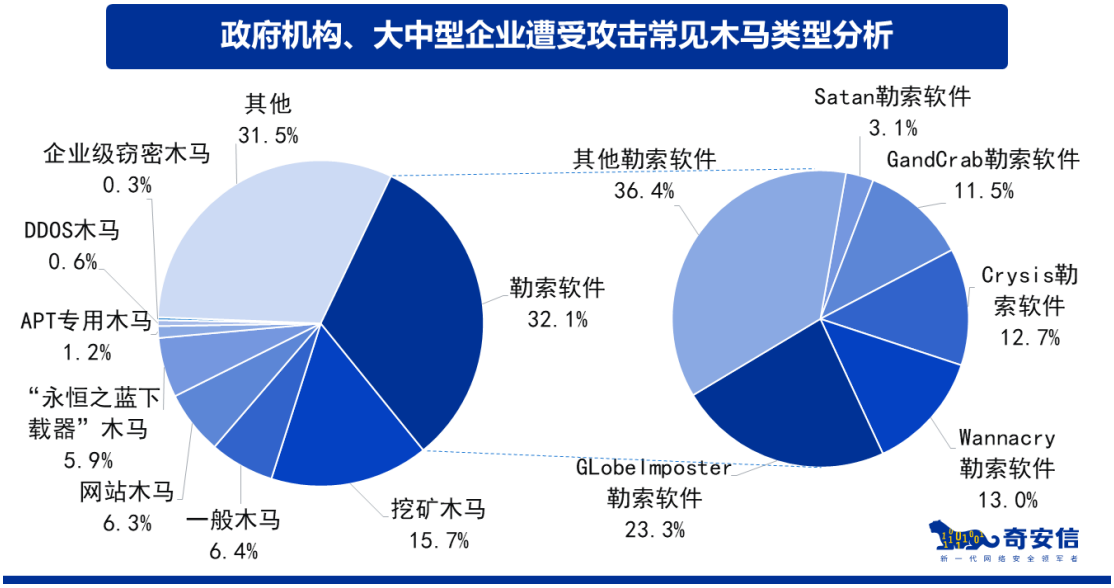
2019 年全年应急事件中，黑产活动、敲诈勒索仍然是攻击者攻击政府机构、大中型企业的主要原因。



通过对 2019 年全年政府机构、大中型企业安全事件攻击类型进行分析，排名前三的类型分别是：木马病毒攻击，占比 50.4%；漏洞利用，占比，17.0%；网页篡改，占比，4.8%。具体分布如下图所示：

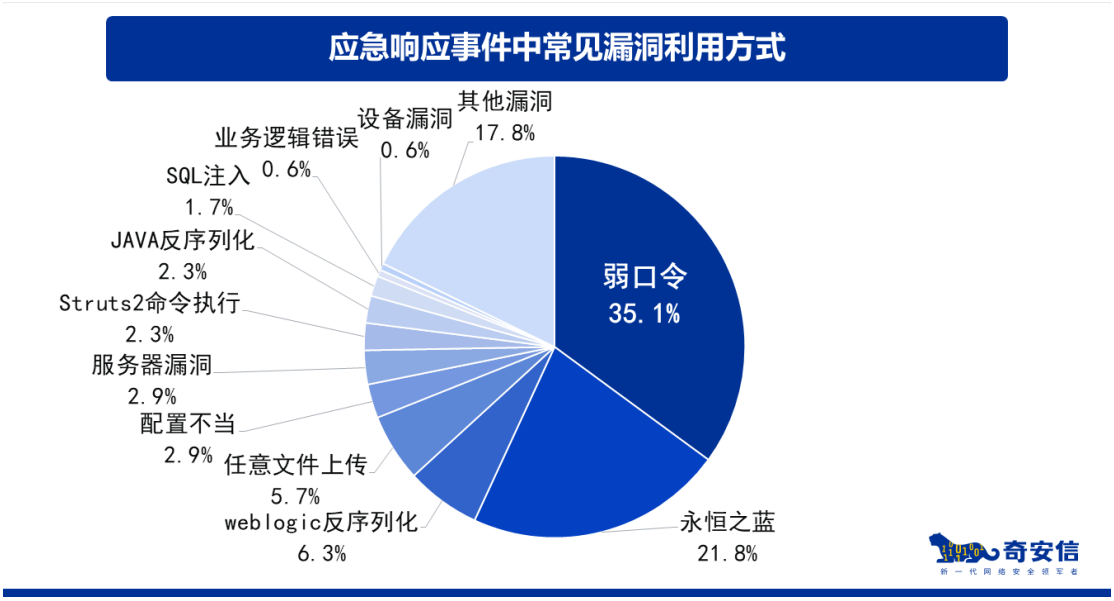


2019 年全年政府机构、大中型企业安全事件遭受攻击常见木马排名前三的为勒索病毒、挖矿木马以及一般木马，分别占比 32.1%、15.7%、6.4%。



从以上数据可以看出，勒索病毒、挖矿木马仍为攻击者攻击政府机构、大中型企业的常见木马类型。其中，勒索病毒常见于 GlobeImposter 勒索软件、Wannacry 勒索软件、Crysis 勒索软件、GandCrab 勒索软件等。

通过对 2019 年全年应急响应处理漏洞利用攻击事件进行统计分析，弱口令、永恒之蓝漏洞是政企机构、大中型企业被攻陷的重要原因，其次，weblogic 反序列化也经常作为黑客日常利用的攻击手段。



第四篇 专题研究

第六章　IT/OT 一体化工业信息安全态势

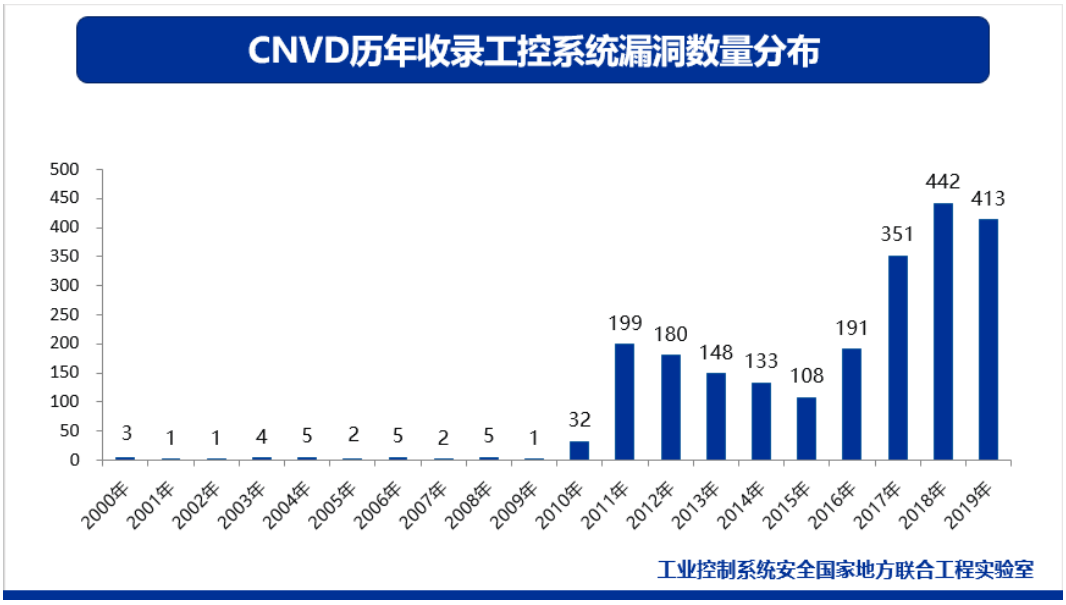
本章主要以工业控制系统安全国家地方联合工程实验室（简称：工业安全国家联合实验室）漏洞库收录的工业控制系统相关的漏洞信息为基础，综合参考了 Common Vulnerabilities & Exposures（CVE）、National Vulnerability Database（NVD）、中国国家信息安全漏洞共享平台（CNVD）及国家信息安全漏洞库（CNNVD）所发布的漏洞信息，从工控漏洞的年度变化趋势、等级危害、漏洞类型、漏洞涉及行业、漏洞设备类型等方面分析工业控制系统的安全威胁态势及脆弱性。

本章中的工控漏洞风险评估方法，基于通用漏洞评分系统，将可见性、可控性、漏洞利用目标服役情况等体现工控安全特性的指标纳入量化评估范围。该方法使用改进的工控漏洞风险评估算法，既可以生成工控漏洞的基础评分、生命周期评分，也可以用于安全人员结合实际工控安全场景的具体需求以生成环境评分。

《ITOT 一体化工业信息安全态势报告》完整版可点击下方链接，通过奇安信官网下载查阅。下载链接：https://www.qianxin.com/threat/reportdetail?report_id=46

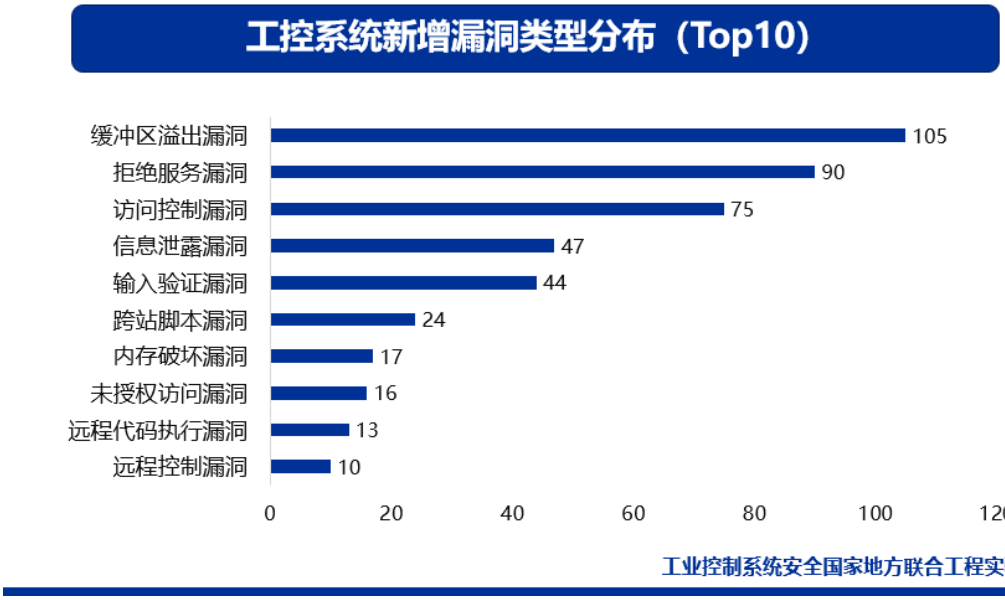
一、　工业互联网安全漏洞分析

根据中国国家信息安全漏洞共享平台最新统计，截止到 2019 年 12 月，CNVD 收录的与工业控制系统相关的漏洞高达 2306 个，2019 年新增的工业控制系统漏洞数量达到 413 个，基本和 2018 年持平，工业控制系统漏洞数据居高不下，形势依然比较严峻。CNVD 工控新增漏洞年度分布如下所示：



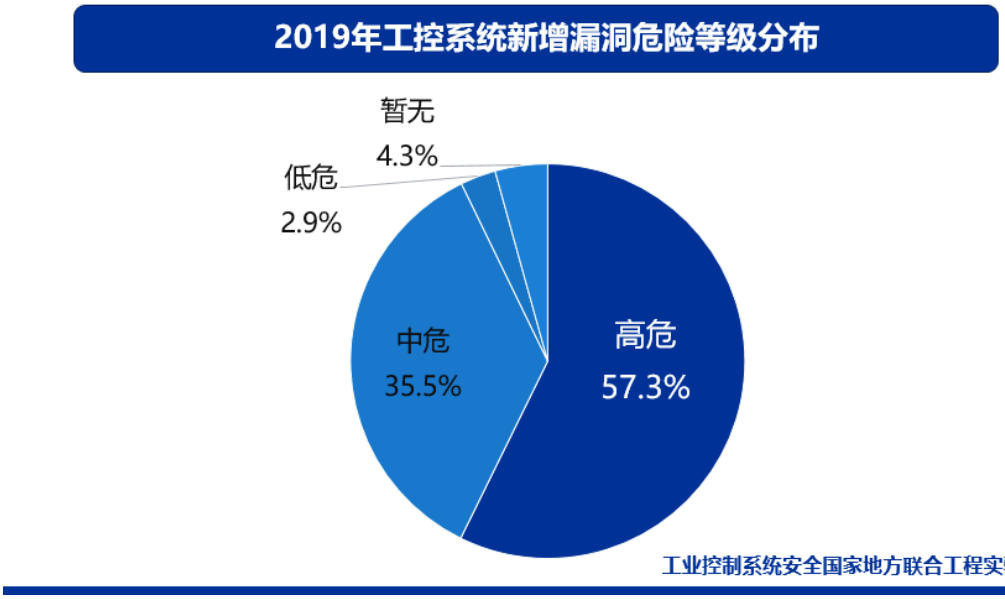
在 2019 年，Common Vulnerabilities & Exposures（CVE）、National Vulnerability Database（NVD）、中国国家信息安全漏洞共享平台（CNVD）及国家信息安全漏洞库（CNNVD）四大漏洞平台收录的漏洞信息共达到了 690 条漏洞，漏洞成因多样化特征明显，技术类型多达

30 种以上。其中，缓冲区溢出漏洞（105 条）、拒绝服务漏洞（90 条）和访问控制漏洞(75 条)数量最为常见。2019 年工控系统新增漏洞类型分布如下：



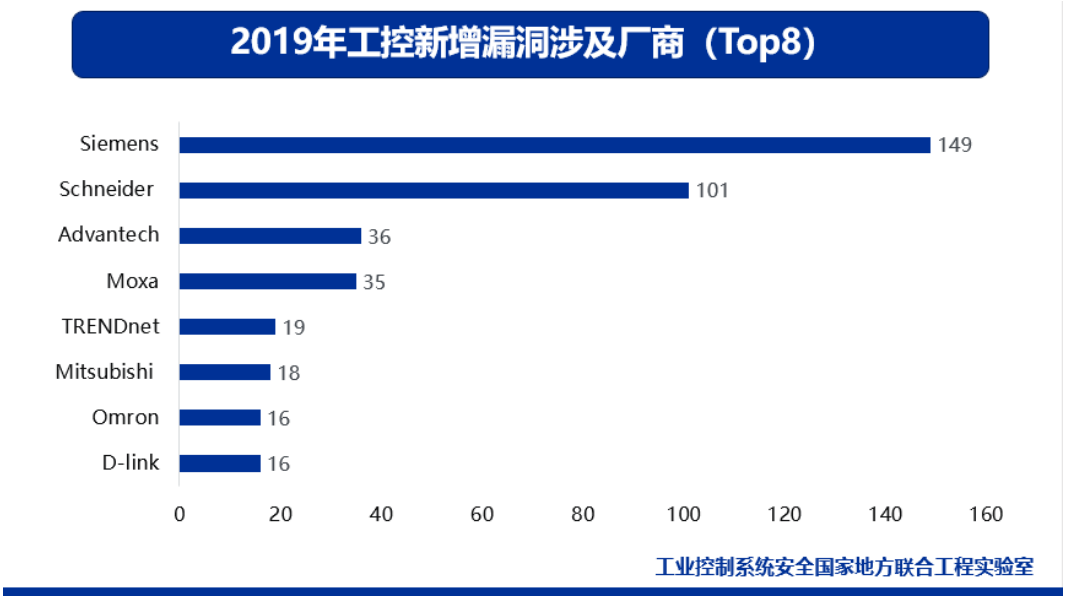
攻击者可以利用多样化的漏洞获取非法控制权、通过遍历的方式绕过验证机制、发送大量请求造成资源过载等安全事故。实际上，无论攻击者利用何种漏洞造成生产厂区的异常运行，均会影响工控系统组件及设备的可用性和可靠性。

在四大漏洞平台收录的工业控系统漏洞中，高危漏洞占比 57.3%，中危漏洞占比为 35.5%，中高危漏洞占比高达 92.8%。在信息安全技术 标准中定义：漏洞可以容易地对目标对象造成严重后果为高危漏洞，工业控制系统又多应用于国家重要信息系统，一旦遭受网络攻击，会造成较为严重的损失。



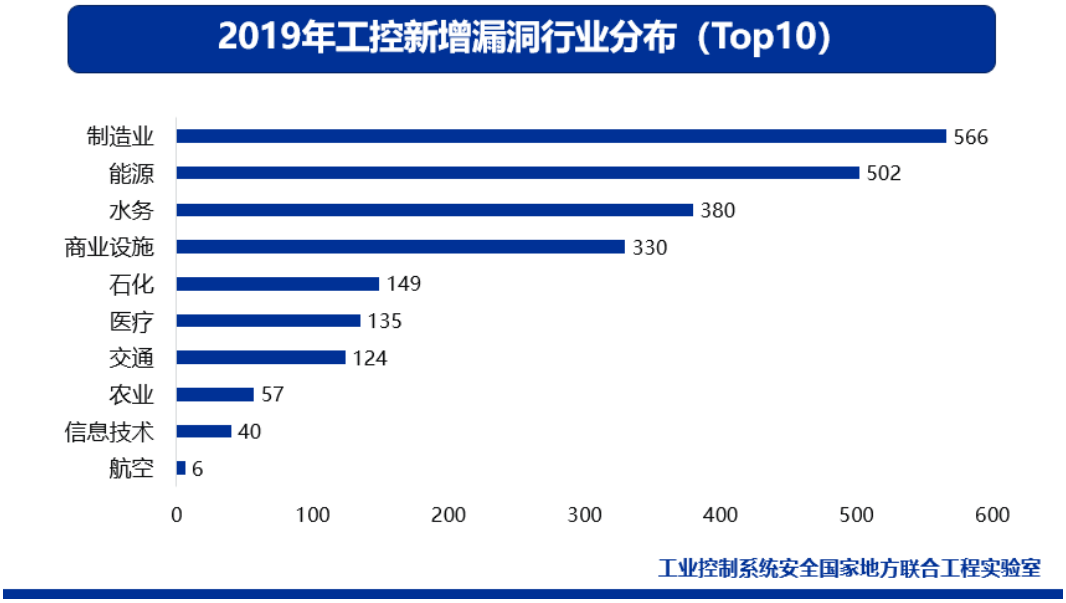
在收录的工业控制系统漏洞中，涉及到的前八大工控厂商分别为西门子（Siemens）、施

耐德（Schneider）、研华（Advantech）、摩莎（Moxa）、趋势科技（TRENDnet）、三菱（Mitsubishi）、欧姆龙（Omron）、和友讯（D-Link）。漏洞涉及主要厂商情况如下图所示：



需要说明的事，虽然安全漏洞在一定程度上反映了工控系统的脆弱性，但不能仅通过被报告的厂商安全漏洞数量来片面判断比较厂商产品的安全性。因为一般来说，一个厂商的产品越是使用广泛，越会受到更多安全研究者的关注，因此被发现安全漏洞的可能性也越大。某种程度上来说，安全漏洞报告的厂商分布，更多程度上反映的是研究者的关注度。

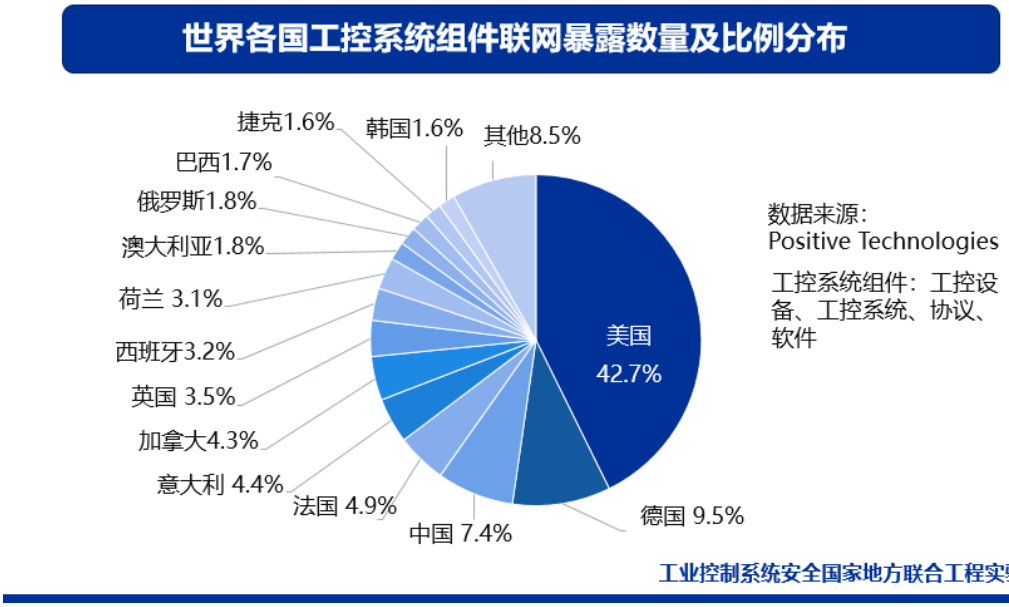
在收录的工业控制系统安全漏洞中，多数分布在制造业、能源、水务、商业设施、石化、医疗、交通、农业、信息技术、航空等重要信息系统。一个漏洞可能涉及多个行业，在 690 个漏洞中，有 566 个漏洞涉及到制造业，也是占比最高的行业。涉及到的能源行业漏洞数量高达 502 个。制造业和能源行业工控漏洞较多，应加强这两个行业工业安全建设。漏洞行业分布图如下：



二、 工控系统互联网暴露风险

为了收集在互联网上具有可访问性的工业控制系统组件，美国安全公司 Positive Technologies 采用被动方式，使用可公开访问的引擎： Shodan（shodan. io）、 Google、Censys（censys. io）对全球工业系统进行了搜索。其中，Shodan 和 Censys 可搜索工业服务器、路由器、专用摄像头等设备的联网情况。

根据 Positive Technologies 研究数据显示：当前全球工控系统联网暴露组件总数量约为 22.4 万个，同比去年增长 27%。将可通过互联网访问的工业控制系统组件（工控设备、协议、软件、工控系统等）数量按照国家进行分类，美国联网的工控设备暴露情况最为严重，达到 95661 个，其次为德国，联网工控组件达到 21449 个，相比去年而言，中国工控系统互联网暴露数量呈现明显增长趋势，由 6223 个增长到 16843 个，增长比例高达 2.7 倍，排名第三。全球各国工控系统联网组件暴露数量及分布情况如下图。



美国和德国联网设备在全球排名前两位，美国遥遥领先，同时也证实了美国工业突飞猛进的发展。德国联网的工控设备排名全球第二，工业发展迅速。2015 年，中国国务院颁布了印发《中国制造 2025》、《关于积极推进“互联网+”行动的指导意见》；2016 年，印发《关于深化制造业与互联网融合发展的指导意见》；推进信息化与工业化的深度融合，促进在工业互联网综合集成应用；2017 年，印发《关于深化“互联网+先进制造业”发展工业互联网的指导意见》；2019 年，印发《加强工业互联网安全工作的指导意见的通知》，中国布局工业互联网，工业得到进一步发展，这也是中国工控系统组件联网暴露数量攀升到全球第三的原因。

三、 工业互联网安全保障建议

结合工业互联网安全风险和威胁，我们发现传统的“围墙式”网络安全建设、业务和安全“两张皮”、IT 安全管理和 OT 安全管理“两张皮”式的安全防护体系已经不能满足越来越复杂的网络安全环境。因此，规划建设“工业互联网安全技术保障平台”有利于全面提高工业互联网安全建设水平。

三级协同的“工业互联网安全技术保障平台”建设将全面提升工业互联网安全保障水平。平台基于“监测-响应”的技术路线进行建设实施，有利于工业生产的长期可靠、稳定运行。因此，旁路的、非侵入式的平台建设结合关键节点串接、阻断式的安全防护是工业互联网安全建设的发展趋势。

通过近年来不断的宣传教育，大多数工业企业开始重视工业网络安全工作，但是很多企业存在着重建设、轻运营的问题。一方面，这些企业对安全运营的重要性缺乏必要的认识。另一方面，工业企业也普遍缺乏合格的安全人才。这些现状导致已部署的平台长期处于一种无运营或者有限运营的状态，不能充分发挥平台的安全防护能力。

我们认为工业企业可以利用外部资源，特别是安全公司提供的远程、驻场或托管式安全运营服务开展工作。工业企业也可以把安全运营工作上移到集团、行业等平台，通过委托方式用专业安全团队来提供安全保障。这些平台通常都具备本地化的应急响应团队，可以对工业安全事件进行及时响应。

采用以上方案，不仅可以在威胁发现、风险预测、处置响应、追踪溯源等方面大幅度提高工业企业网络安全防护能力，还可以减少人力资源投入、降低工业企业安全运营成本。省级或行业级平台在和企业数据对接过程中，要重点做好数据采集、数据传输、数据存储、数据处理等方面的安全防护工作，构建全生命周期的工业大数据安全防护体系。省级或行业级工业互联网安全技术保障平台要以服务工业用户为主要目的，为接入企业提供有价值的安全运营服务。数据上报后帮助工业企业定期分析安全风险，及时发现安全威胁，第一时间应急响应，事后实现追踪溯源，减少企业安全损失，提供安全咨询，让工业企业看到数据上报后给企业所带来的价值。

目前工业互联网安全技术保障平台建设还在起步阶段，特别是企业侧平台的建设机会巨大。平台建设应处理好与等保建设之间的关系，加强平台的运营和管理，吸引更多的工业企业接入上级平台。平台的建设必将推动我国工业互联网快速、健康发展。

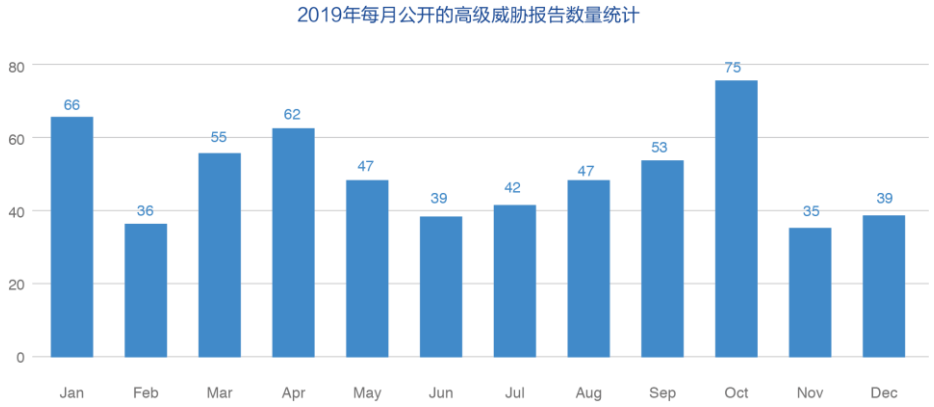
第七章　全球高级持续性威胁分析

本章内容是基于奇安信威胁情报中心对 200 多个 APT 类情报来源或渠道的数据，进行收集、统计和分析的结果。同时，结合自身收集渠道获取的公开内容进行分析，总结形成 2019 年全球高级持续性威胁的态势情况，并对 2020 年 APT 威胁趋势进行了预测。

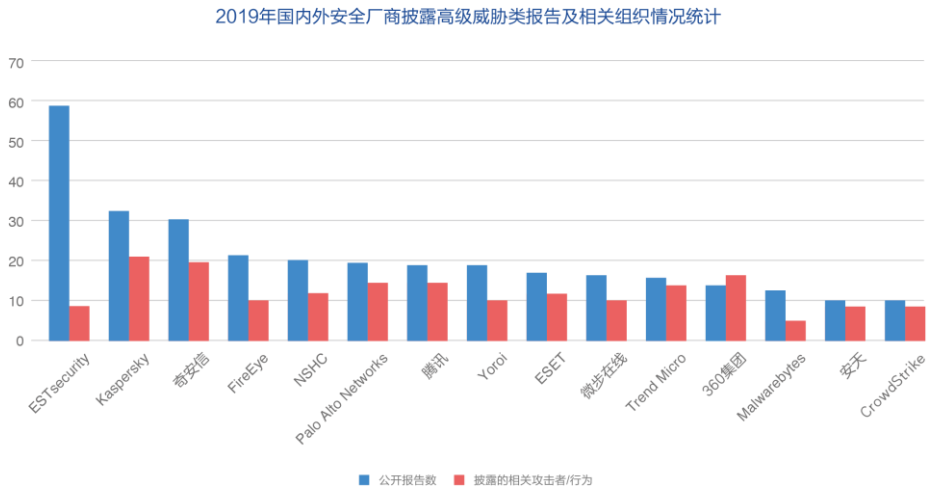
《全球高级持续性威胁（APT）2019 年报告》完整版可点击下方链接，通过奇安信官网下载查阅。下载链接：https://www.qianxin.com/threat/reportdetail?report_id=44

一、　全球 APT 活动公开报告状况

奇安信威胁情报中心在 2019 年监测到的高级持续性威胁相关公开报告总共 596 篇。



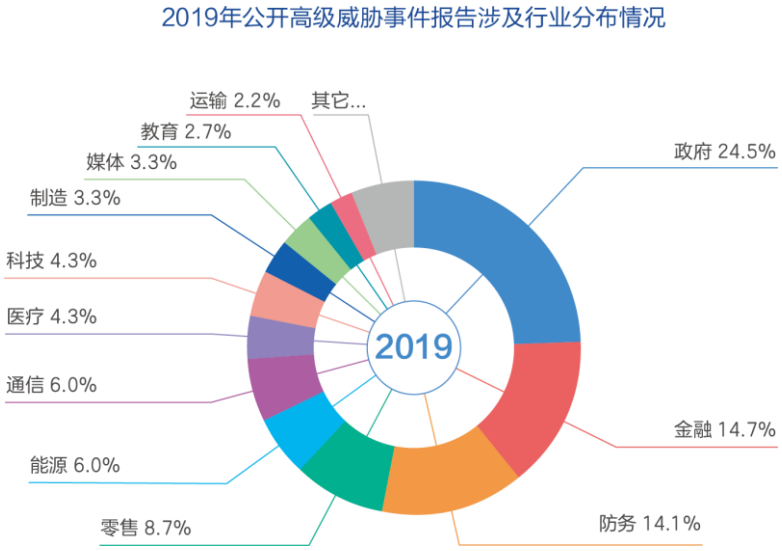
从公开报告的发布渠道统计来看，韩国安全厂商 ESTsecurity 发布了最多的高级威胁类报告，不过其披露的主要为针对韩国本土目标的攻击组织和攻击行动。除此以外，像奇安信、Kaspersky、FireEye、Palo Alto Networks 和腾讯等依然保持着较高的高级威胁的跟踪、分析和披露，并且跟踪和披露全球范围内的多个 APT 组织和攻击行动。



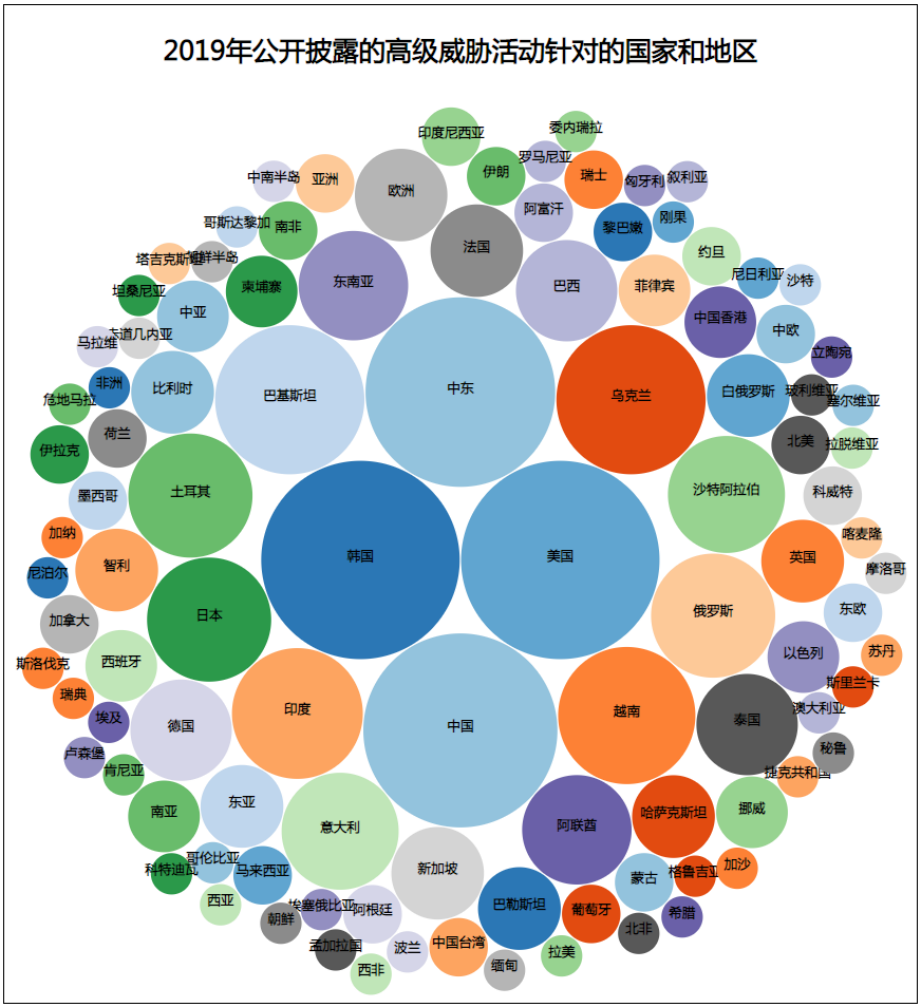
二、　受害目标的行业与地域

从公开披露的高级威胁活动中涉及目标行业情况来看（摘录自公开报告中提到的攻击目标所属行业标签），政府（包括外交、政党、选举相关）和军事（包括军事、军工、国防相关）依然是 APT 威胁的主要目标，能源（包括石油、天然气、电力、民用核工业等）、通信行业也是 APT 攻击的重点威胁对象。

由于更加组织化的网络犯罪团伙的活跃活动，导致金融（包括银行、证券、数字货币等）和零售（电子商务、餐饮等）行业所面临的高级威胁现象越发严峻

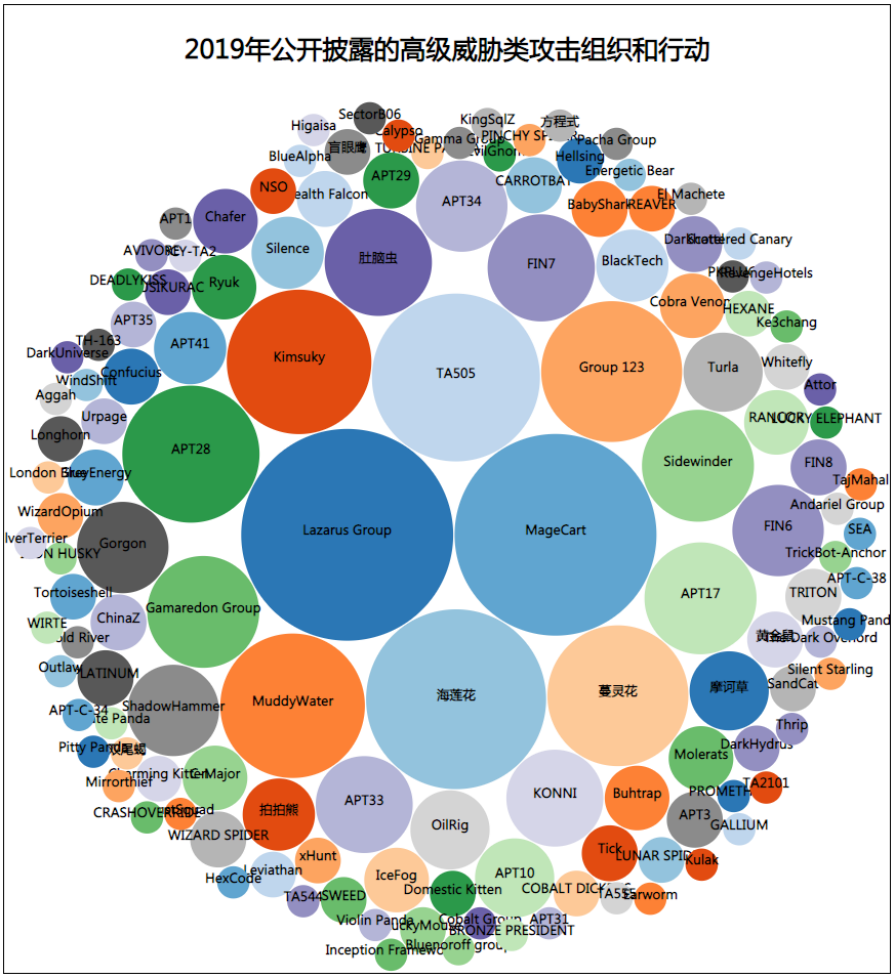


高级威胁活动涉及目标的国家和地域分布情况统计如下图（摘录自公开报告中提到的受害目标所属国家或地域），可以看到高级威胁攻击活动几乎覆盖了全球绝大部分国家和区域。

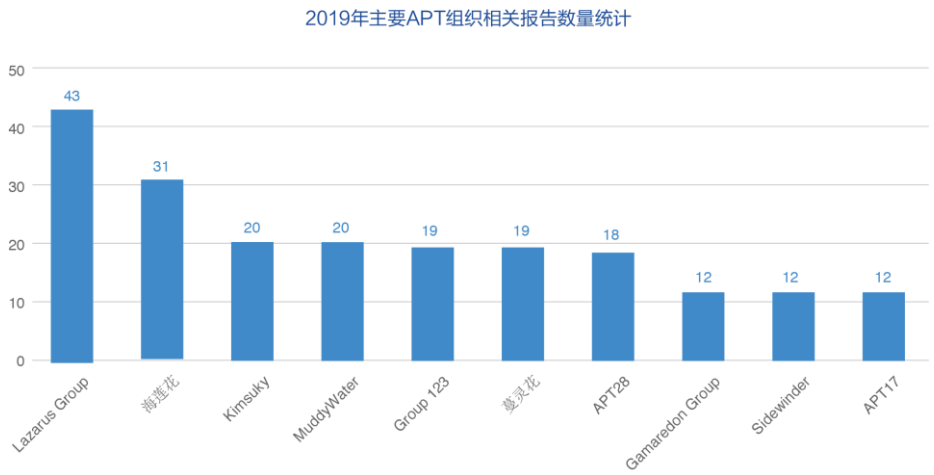


三、 活跃的威胁攻击者

进一步对公开报告中高级威胁活动中命名的攻击行动名称、攻击者名称，并对同一背景来源进行归类处理后的统计情况如下，总共涉及 136 个命名的威胁来源命名，较 2018 年数量有所增长。



我们也统计了 2019 年公开披露最多的 APT 组织，跟 2018 年相比，疑似来自东北亚某地的 Lazarus Group、Kimsuky 和 Group 123 三个 APT 组织被频繁曝光。



四、 典型行业高级威胁活动分析

APT 威胁是定向性的，其会选择攻击的行业、地域、目标以及要达到的目的，这些是由

APT 组织在实施行动前制定的需要达到的阶段性目标和动机所决定的。从过去的 APT 威胁来看，APT 组织在一段时间内会保持其攻击目标行业的专注程度，这可能也与攻击组织在针对新的行业实施攻击时，需要时间收集和熟悉目标，并弥补自身能力与目标行业的缺失部分，以及构建相应的攻击武器库。

我们在 2019 年的威胁报告中首次加入从行业视角的 APT 威胁分析和研究，并且重点关注当年内针对特定行业的活跃攻击组织和攻击活动情况。除了政府、军事相关行业外，金融、能源和电信是 APT 威胁的主要行业目标，所以本报告对这 3 个行业在 2019 年的 APT 威胁情况进行总结。

（一） 金融行业

这里，我们将金融行业包括了传统的银行、证券行业以及新兴的数字货币交易所，以及像电子商务，在线的零售商家这些在线交易机构。针对金融行业的攻击主要以牟利为目的，除了像 Emotet 这样极为流行的银行木马外，也活跃着不少组织化的网络犯罪团伙，其通常拥有自己独立的攻击 TTP 和定制化的攻击武器集合。少数 APT 组织同样也针对金融行业目标实施攻击，我们列举了 2019 年公开披露的主要活跃的针对金融行业的攻击组织。

Lazarus Group 最早被发现针对金融银行的攻击是 2016 年 2 月，其针对孟加拉国银行 SWIFT 系统的 APT 攻击，并试图窃取 9.51 亿美金[61]。之后该组织就一直针对全球范围的金融银行机构实施攻击活动。由于其牟利的攻击动机和过去实施网络间谍活动和情报窃取不一致，所以一些安全厂商也将其攻击金融银行机构的活动以独立的子组织命名进行跟踪，例如卡巴作为 Bluenoroff，FireEye 作为 APT38。

我们在上表中也列举了多个 2019 年公开披露过并且持续活跃的网络犯罪团伙。我们总结了网络犯罪团伙在 2019 年的主要攻击活动。

组织化的网络犯罪团伙和 APT 组织类似，其会定制化自有的攻击工具集，并且拥有自己的 TTP 模式。其通常会利用 BEC 攻击，垃圾邮件，钓鱼等方式活动初始的攻击立足，其也会结合公开或开源的渗透工具，包括 Meterpreter，Cobalt Strike 和 Empire 之类，并用于横向移动阶段。我们列举了数个网络犯罪团伙常用的攻击工具。

如 FIN6 组织的攻击工具集：

攻击工具名称	主要别名	功能说明
FrameworkPOS	Trinity	FIN6常用的针对PoS系统的后门
More_eggs	Terra Loader，SpicyOmelette	JScript后门
Meterpreter	-	公开工具
Cobalt Strike beacon	-	公开工具
TrickBot-Anchor	-	TrickBot变种

FIN7 组织的攻击工具集，安全厂商也披露 FIN7 组织和新的僵尸网络 AveMaria 的运营有关。

攻击工具名称	主要别名	功能说明
CARBANAK	-	FIN7常用木马
SQLRat	-	一个以SQL Server为控制基础设施的RAT
DNSbot	-	支持DNS，HTTPS和SSL多种通信方式
TinyMet	-	开源的meterpreter stager
GRIFFON	-	轻量级JS植入程序
BOOSTWRITE	-	新的加载器
RDFSNIFFER	-	新的RAT，由BOOSTWRITE加载

TA505 网络犯罪组织会频繁新增和变更其攻击工具集，下表也列举了其在 2019 年活动

中使用的攻击木马程序。

攻击工具名称	主要别名	功能说明
ServHelper	–	后门程序
FlawedGrace	–	RAT，由ServHelper下载
FlawedAmmyy	–	常用的远控木马
tRat	–	RAT后门
LOLbins	–	开源工具
AndroMut	Gelup	下载器
FlowerPippi	–	后门
Get2	–	下载器
Snatch	–	RAT，由Get2下载
SDBbot	–	RAT，由Get2下载

而 MageCart 组织似乎与上述组织有所不同，其主要以攻击目标网站和 Web 应用的供应链并在失陷的网站和 Web 程序中植入 Javascript 实现的 skimmer 脚本，从而窃取受害用户的信用卡信息。该组织的活动非常频繁，并针对全球化的电子商务平台，在线零售等等。

与 APT 组织不同的是，网络犯罪组织的主要目的在于牟利，其更换其攻击工具或使用其他的网络犯罪程序更加容易，在网络犯罪的地下市场充斥着商业工具提供者或制作者，服务提供商，运营团伙等多类角色，所以更容易出现工具和恶意程序的重叠。并且由于角色的划分，攻击活动的归属和背后实施攻击活动的运营团伙可能出现变更。例如 2018 年 8 月 1 日，美国 DoJ 宣布逮捕了涉及 FIN7 相关的黑客人员，但 FIN7 的活动并未因此而停止，其极有可能是有新的运营人员接管了相关的攻击工具和网络犯罪平台以持续运营[62]。

从 2019 年主要的网络犯罪组织和 APT 组织针对金融行业目标的攻击活动来看，金融银行机构的 PoS 系统，ATM 终端，SWIFT 交易系统，以及与电子商务和在线支付相关的网站都是攻击组织的主要攻击对象，并且通过非授权的资金交易转账，获取和售卖支付卡和信用卡数据，以及地下市场交易来进行非法牟利。

（二） 能源行业

能源行业包括了如石油、天然气、电力、核能、矿业等等领域，无论是从国家经济层面还是社会民生层面都和能源行业息息相关。随着能源行业这些传统行业的组织和机构如今也向着信息化程度的建设，也必然带来了其可能作为网络攻击和网络利用的重要目标之一。

从网络攻击的动机来看，能源行业可能主要面临着 APT 威胁，其用于在必要时对目标进行破坏和影响，导致目标产线异常甚至出现生产错误。由于能源行业部分也涉及了敏感的信息和数据，其也是 APT 威胁中的重要目标。

而对于能源行业来说，甚至是扩展到工业控制领域，其主要可以划分为 IT 和 OT 两个部分，其网络通常与互联网隔离，重要的工业产线控制甚至是在隔离网络下，并可能由专用的系统和软件加以控制，然而其依然会存在被攻击的风险。在今年，一份外媒报道也披露了当年的 Stuxnet 事件中，由欧洲某国情报人员招募的一名工程师，由其携带了带有病毒的 USB

设备并插入到内部系统，从而获得了访问权。

对能源行业目标的攻击和破坏对于国家、社会和民生安定来说影响是巨大的，例如 2015 年乌克兰的两次停电事件，2019 年南美地区包括委内瑞拉、阿根廷和乌拉圭地区的停电事件都对当地人名的生活造成了巨大的影响。虽然今年上半年南美地区的大规模停电事件并没有明确的证据显示和网络攻击有确凿的联系，但结合当年乌克兰的停电事件我们依然可以评估网络攻击针对电力系统的攻击破坏所造成的影响会是巨大的。

我们在这里也列举出 2019 年公开披露的针对能源行业的 APT 攻击活动和主要的 APT 组织。

从公开披露的 APT 威胁报告来看，中东是针对能源攻击活动的重点活跃地域之一，这也与中东地区复杂的地缘政治因素和已有的丰富能源产业有关。

像 OilRig 组织，后续国外安全厂商常和 APT34 进行合并跟踪，能源行业是其主要的目标之一，如知名的 Shamoon 恶意程序就被公开认为与其相关，并曾经用于攻击和破坏沙特阿拉伯的石油公司造成了其服务停止。

HEXANE，又称 LYCEUM，其是由国外安全公司 Dragos 披露的主要针对工业控制领域攻击的团伙，其最早可能从 2018 年 4 月开始活动。其攻击手法被认为和 APT33、APT34 存在相似，但并未出现明确的线索重叠。

另一个值得关注的是，疑似 Lazarus Group 在 9 月-10 月期间被发现针对印度 Kudankulam 核电厂的网络攻击，虽然主要攻击的是核电厂的 IT 网络，并未进入到 OT 网络中。该事件中似乎使用了一个 Dtrack 样本，其用于横向移动阶段，并且硬编码了疑似核电厂相关的登录名称。

（三） 电信行业

电信行业是另一个 APT 威胁中的重要目标行业之一，由于电信行业承担着互联网骨干网络和核心基础设施的运营，以及包括电信网、蜂窝网、移动通信和有线电视等。

针对电信行业目标实施 APT 攻击往往能够建立在更高维度的信息系统控制能力下实现包括劫持、监听、篡改等目的。

我们总结了 2019 年公开披露的针对电信行业的攻击活动和活跃组织如下：

五、 2020 年高级持续性威胁预测

我们基于 2019 年 APT 威胁的趋势以及近年来 APT 威胁组织和活动的变化情况对 2020 年高级持续性威胁进行预测。

（一） APT 威胁归因困难导致攻击归属命名更加碎片化

奇安信威胁情报中心一直在收集、分析和研判全球范围 APT 类威胁的归属命名和公开披露情报，但我们发现 APT 威胁的归因问题变得更加复杂和困难。

APT 攻击组织在实施攻击活动的操作安全上变得更加谨慎，并且利用多种方式避免其行为特征被发现和关联，在过去我们看到了攻击组织使用如下的方法：

1） 频繁更换攻击程序的形态，避免代码重用；

2） 利用和定制化公开的或开源的攻击工具，利用脚本语言和商业工具；

3） 利用无文件攻击技术尽量避免攻击载荷的留存；

4） 利用本地命令，也称为 live off the land 攻击；

5） 故意留下假旗标志误导安全分析人员；

6） 劫持其他攻击组织的控制基础设施。

归因的问题最终导致了归属命名的碎片化，从而依赖于更丰富维度的元数据和线索证据来佐证最终的归因判定。

另外，一些高价值目标可能会同时作为不同 APT 组织的攻击目标，造成攻击活动重叠的冲突，也可能给归属分析判定带来影响。

（二） 出现更多的在野 0day 攻击案例

在 2018 年的全球高级持续性威胁报告中，我们总结了在 2018 年公开披露的在野攻击活动中利用的 0day 漏洞总共有 14 个，涉及明确的攻击组织 6 个。在 2019 年的报告中，我们总结了 2019 年内公开披露的在野攻击活动中利用的 0day 漏洞总共有 17 个，涉及明确的攻击组织至少 7 个，相对于 2018 年来说略有增长。然而 2019 年的 0day 攻击案例中，似乎并未出现新的文档型漏洞的利用，并且随着 Adobe Flash 生命的完结，未来利用 Flash 的漏洞可能会越来越少。

在 2019 年中，针对浏览器的完整利用链在被曝光的在野攻击活动中出现的越来越多，不光是针对 PC，还有针对 Android、iOS 移动设备，其漏洞利用往往需要更少的用户交互即可完成。从趋势上来看，我们也认为未来会出现更多的在野 0day 攻击案例。

（三） 针对行业性的 APT 威胁越发凸现

我们预测在未来针对行业性的 APT 威胁活动会越来越多，也就是说 APT 威胁活动不光局限于政府、国防、军工、外交等领域的目标，金融、能源和电信也可能作为未来 APT 威胁中的重点攻击目标。

从今年的威胁活动来看，网络犯罪团伙正向着高度组织化，高度武器化和高度战术化的趋势发展，其大多拥有一套自定义的攻击工具集和战术技术过程。以牟利为动机的针对金融银行行业的攻击活动，不光是针对受害用户自身的在线资金的攻击（包括银行卡信息盗窃），

还会针对金融机构本身的系统、终端、网络实施攻击活动，并尝试获得更大的战果。

从 APT 攻击的动机来看，金融、能源和电信是高度符合攻击组织需要的，通过攻击金融银行机构实现所需资金的补充，攻击能源行业会对目标国家发展和社会安定的破坏，甚至获取重要的情报，例如针对核能领域的攻击，以及攻击电信通信行业能够获取到骨干网或核心网络基础设施的控制权。

由于 APT 威胁可能针对特定行业实施，攻击组织在筹备攻击活动以前会更多的尝试对目标行业情况进行情报收集，并积极弥补和目标的技术差距，并针对性构建攻击工具集。因此，攻击组织需要准备更加针对性的攻击能力和攻击战技术。

（四） 5G 商业化和物联网或为 APT 威胁提供新的控制基础设施

今年，5G 正在向商业化的趋势发展，5G 网络提供的高质量和高速率的网络通信能力必将为物联网带来进一步的发展空间。物联网设备，家用智能设备，路由器，甚至智能手机等在未来都可能以某种形式连接在一起，然而其中的终端设备安全良莠不齐必然导致存在诸多的安全风险。

从过去的 VPNFilter 事件，名为 Inception Framework APT 组织利用路由器 UPnP 功能最为代理隐藏自身，可以看出基于物联网设备的攻击活动不再是网络黑客的专属，其同样会被应用到 APT 威胁攻击中。并且从 2016 年 Mirai 造成美国东海岸断网事件来看，其同样可以用于网络攻击破坏中，以瘫痪目标网络和基础设施服务。

（五） 更加频繁和隐蔽的网络攻击破坏活动

2019 年从公开报道和披露，有不少疑似与网络攻击或者疑似网络攻击造成的破坏活动，其主要和电力系统，政府机构，核电厂，炼油厂相关。网络攻击所造成的破坏活动能够瘫痪目标系统或者造成目标运转的异常，最终导致国家发展、社会民生造成不安定的影响。

网络攻击破坏活动相对于军事行动来说，更加具有隐蔽性和溯源难的特点，从而攻击源头可以进行否认。由此可以预见未来网络攻击破坏活动可能更加频繁。

第八章　网络安全人才市场状况

本章以智联招聘多年来形成的丰富的招聘、求职信息大数据为基础，结合了奇安信集团在网络安全领域多年来的专业研究经验，相关研究成果具有很强的代表性。对涉及安全人才的全平台招聘需求与求职简历进行分析（注：本章中的需求指数采用的是全量数据统计，其他维度的分析一般采用的是抽样数据统计），在需求变化，供需结构，用人单位特点以及人才自身特征等多个方面对网络安全人才市场现状展开了全面、深入的研究，

《网络安全人才市场状况研究报告》完整版可点击下方链接，通过奇安信官网下载查阅。下载链接：https://www.qianxin.com/threat/reportdetail?report_id=27

一、　网络安全人才市场供需趋势

我们以智联招聘平台 2016 年 1 月收到的政企机构网络安全人才招聘需求总数为基准，即设 2016 年 1 月智联招聘平台收到的政企机构网络安全人才招聘需求总量为 A，并假设此时网络安全人才需求规模指数为

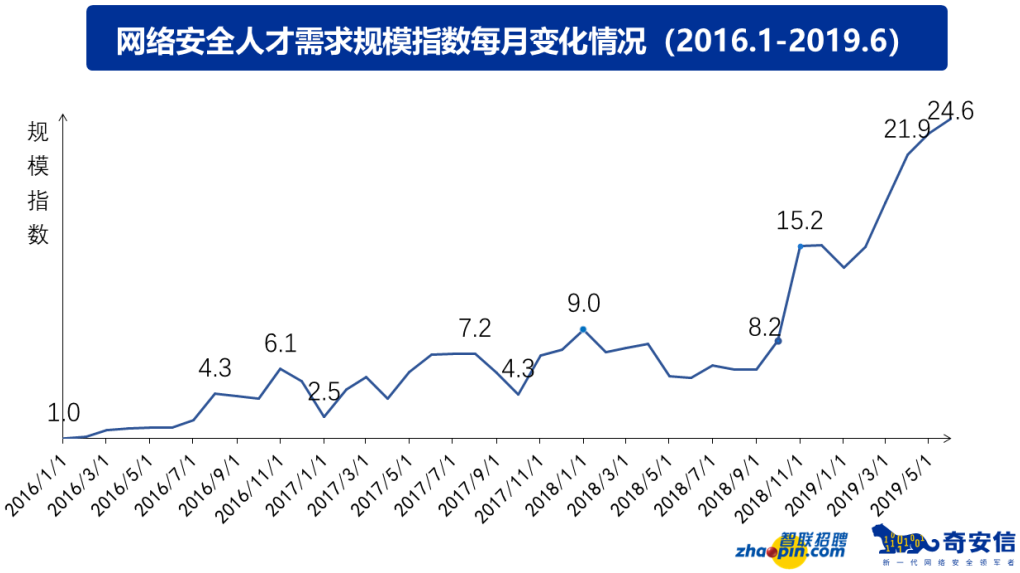
指数（2016.1）＝1

则，若在某一时间段 x 内（注：一般是指某一个月，或者若干个月，或者半年、全年），智联招聘平台收到政企机构的网络安全人才招聘需求总量为 B，则在这一时间段内，网络安全人才需求规模指数为

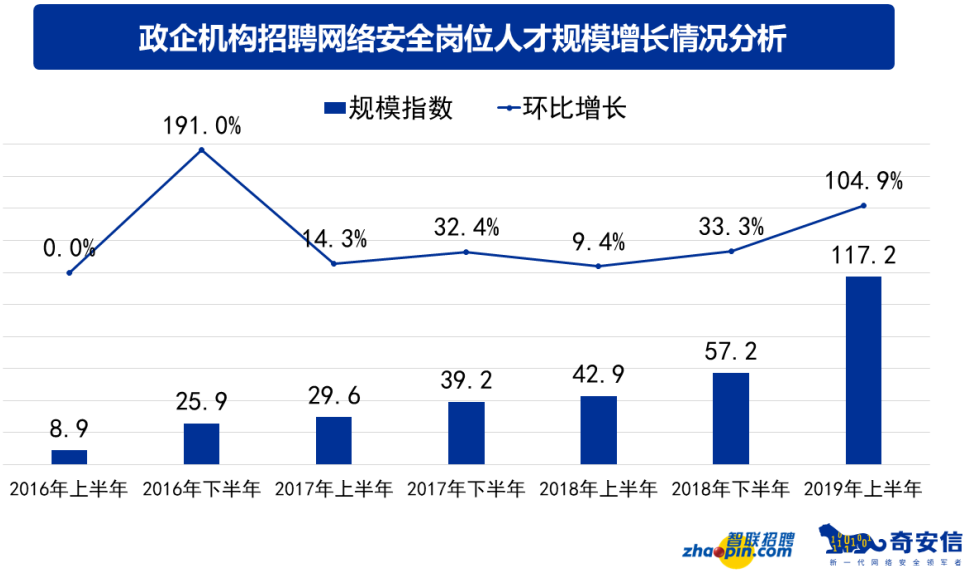
指数（x）＝B/A×指数（2016.1）＝B/A

下图给出 2016 年 1 月至 2019 年 6 月，国内网络安全人才需求规模指数（简称规模指数）的每月变化情况。

很明显看到，2018 年 10 月以来，需求指数呈高速增长趋势，11 月份首次突破个位数，达到两位数的规模。即人才市场的需求在三年的时间内，扩大了 2016 年初的 10 倍以上。2019 年 6 月，指数达到三年来最高值 24.6，增长速度堪称惊人！



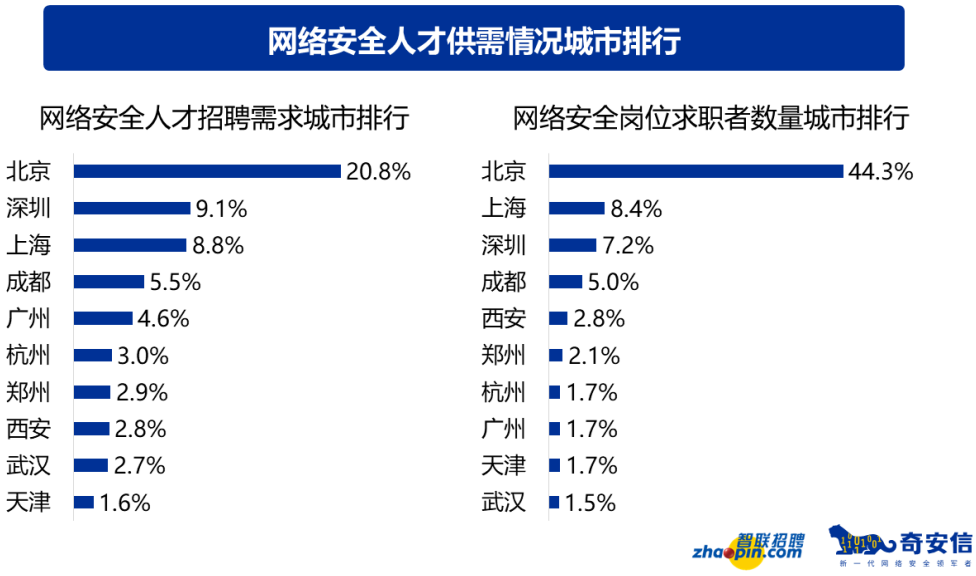
由于政企单位的人才招聘需求跟季节周期有一定关系，下面我们统计了以半年为周期的人才需求规模指数。其中，半年指数的值为其间 6 个月指数之和。从下图中可以看出，2019 年上半年，网络安全人才需求规模指数较 2018 年下半年环比增长了 104.9%。历史上再次超过 100%的增长率，较 2018 年上半年同比增长 173.2%，说明 2019 年上半年政企机构对安全人才“广开大门”、“求贤若渴”，同时某种程度上也预示着网络安全岗位成为十分热门的职位之一！



从地域范围来看，网络安全人才，不论是需求还是供给，都多集中于北京、上海、深圳等一线城市。抽样统计显示：北京、深圳、上海、成都、广州是网络安全人才需求量最大的城市，这五个城市对网络安全人才需求的总量占全国需求总量的 48.8%。相较于 2018 年需求量前五的城市占全国的 60.7%，今年的需求占比总和降低了约 16 个百分点，更多地区加大了对网络安全的投入，增加了对网络安全人才的需求。

2019 年度网络安全人才市场呈现需求进一步增长、用人单位的地域分布进一步下沉、人才需求更加多样化、基础化、体系化（常态化）等特点。

而从人才供给情况来看，位于北京的求职者占比从去年的 59.4%下降至 44.3%，其他城市的求职者正在稳步上升。正在慢慢的由“只有去北上广深才能找到工作”向“各个地区都需要网络安全人才”转变。



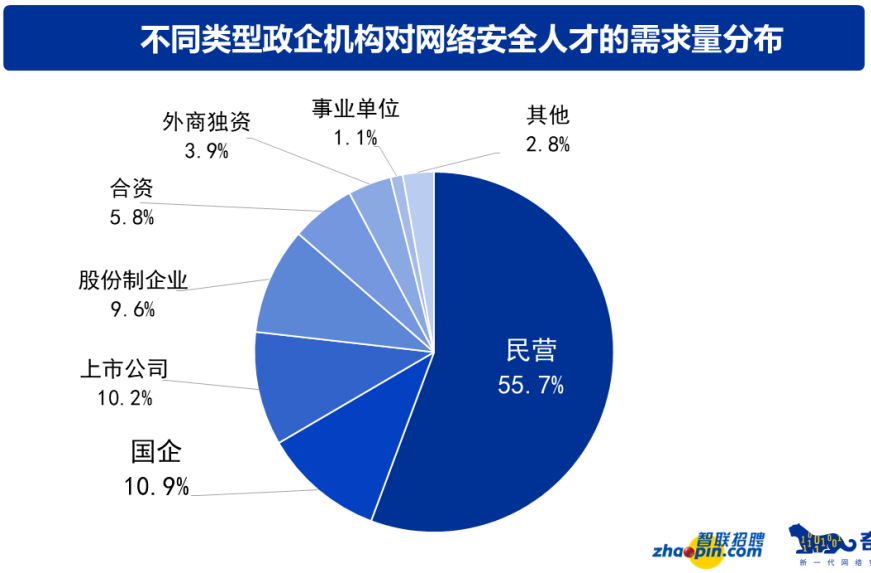
相比于 2018 年，在招聘需求排行榜上，排名前五的城市为：北京、深圳、上海、广州、杭州。到 2019 年，成都网络安全人才招聘需求回升至前五名，由 2018 年的 2.5%（排名第七）增长到 2019 年的 5.5%（排名第四）需求量直线升高。

统计显示，2017 年求职者期望的平均薪资约为 7533.5 元/月，2018 年为 8587.5 元/月，2019 年为 11263.9 元/月，相比 2018 年增长了 2676.4 元/月，求职者渴望的平均薪资在逐年增长。而政企机构提供的网络安全相关岗位的平均薪酬约为 11728.9 元/月。另外，安全企业提供给网络安全相关岗位的平均薪酬约为 12004.8 元/月。

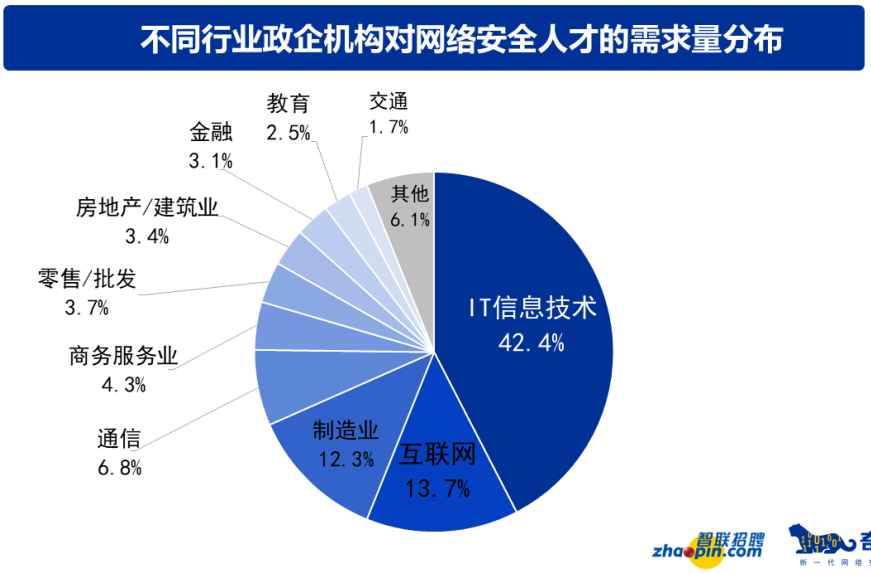
总体而言，用人单位提供给安全人员的薪酬大大高于求职者的预期，政企机构网络安全相关岗位平均薪酬比 2018 年略有减少，可能是由于更多政企机构增加了网络安全相关基础岗位的设置，而这些岗位并不需要从业人员拥有很强的高级防护能力，需要的是具有维护日常运维和基础服务的能力。

二、 网络安全人才用人单位分析

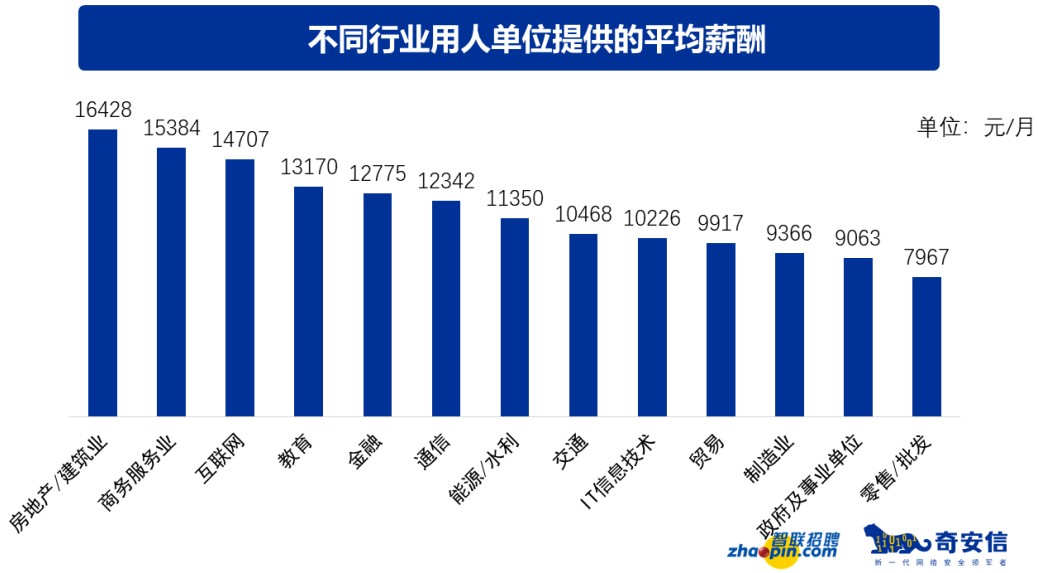
从招聘单位（注：招聘单位即“政企机构”，后文同）的机构性质来看，在网络安全人才招聘需求的政企机构中，招聘需求最多的是民营企业，用人需求占网络安全人才招聘总量的 55.7%；其次是国企，占比 10.9%；上市公司排第三，占 10.2%。（上述各类型政企机构用人数量独立统计，互不交叉）。



从用人单位的所属行业来看，对网络安全人才需求量最大的行业是 IT 信息技术，其发布的网络安全人才招聘数量占所有网络安全人才招聘总人数的 42.4%，其次为互联网，占 13.7%。实际上，IT 信息技术和互联网行业由于其本身行业性质，对网络安全相关岗位需求量要明显高于其他行业。排名第三的是制造业，招聘数量占比 12.3%。通信行业（6.8%）商务服务业（4.3%）等排在其后。



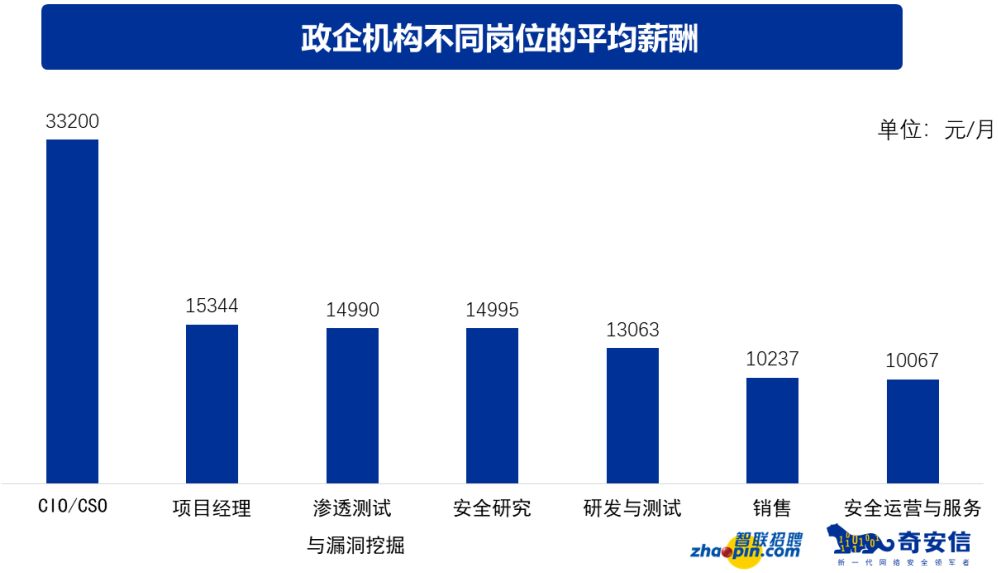
不同行业用人单位提供的薪酬也有所差别。从不同行业用人单位提供的平均薪酬来看，房地产/建筑行业相关用人单位给网络安全人才提供的薪酬最多，平均约为 16428 元/月，其次为商务服务业，平均薪酬为 15384 元/月，互联网行业平均薪酬为 14707 元/月。具体分布如下图所示。



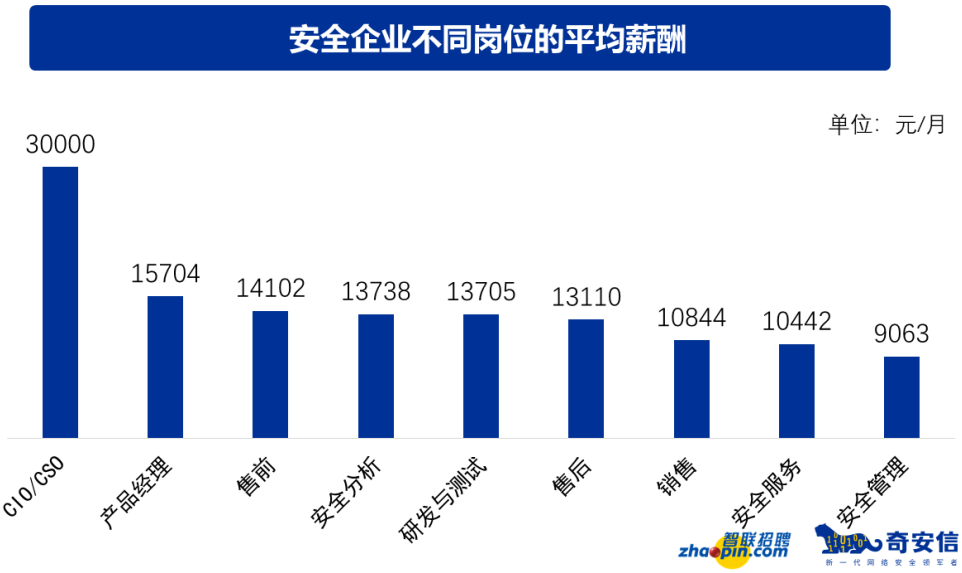
需要说明的是：不能通过各行业用人单位平均薪酬的差别，简单的认为不同行业的薪资待遇不同。据统计，往往薪酬高的行业，相对应的岗位对网络安全人才的经验、能力等要求也更高。

因此不能单纯通过各行业平均薪酬待遇来判断同一人在不同行业的薪资待遇不同。

网络安全人才的薪酬也会随着岗位的不同，有所差别。综合一般企业对不同岗位平均薪酬进行分析，排名第一的是 CIO/CSO（首席信息官，Chief Information Officer/首席安全官，Chief Security Officer）平均薪酬为 33200 元/月，其次为项目经理类相关岗位，平均薪酬 15344 元/月，渗透测试与漏洞挖掘类岗位排名第三，平均薪酬为 14990 元/月。



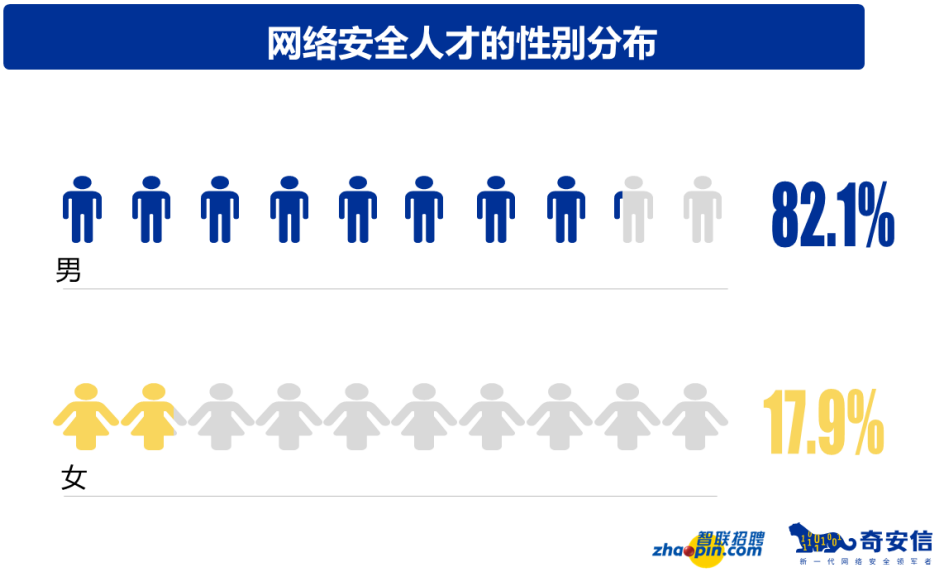
从安全企业各岗位平均薪酬来看，CIO/CSO 依旧最高，为 30000 元/月，与政企机构 CSO 岗位平均薪酬水平基本相似。其次为产品经理类岗位，平均薪酬 15704 元/月，售前类岗位，平均薪酬为 14102 元/月。



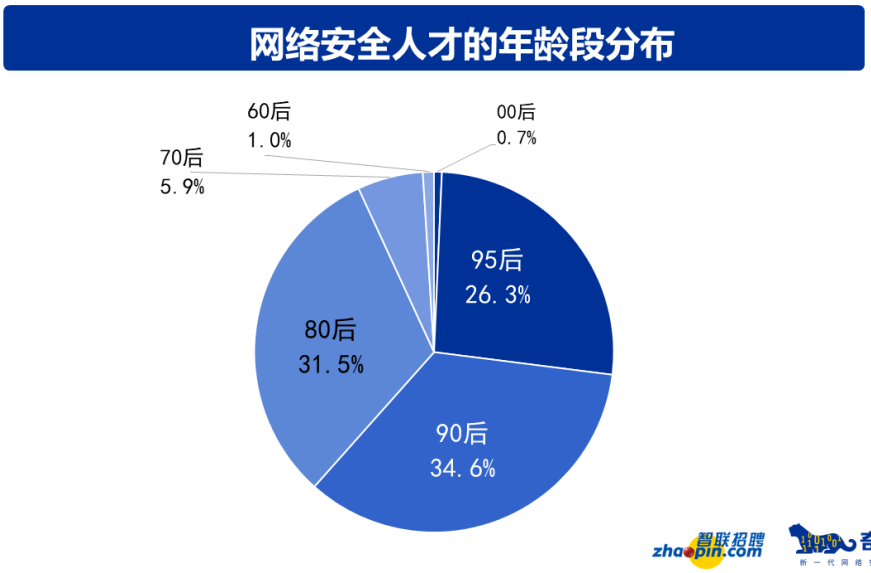
预计未来 3-5 年内，具备实战技能的安全运维人员与高水平的网络安全专家，将成为网络安全人才市场中最为稀缺和抢手的资源。

三、 网络安全人才的特征分析

通过对应聘网络安全岗位的求职者简历分析，我们发现，男性是网络安全人才构成的绝对主体，占比高达 82.1%，而女性占比仅为 17.9%。由此可见，网络安全领域，基本上还是以男性为主。



从年龄段来看，网络安全岗位的求职者中，90 后最多（包含 95 后人群和 90 后人群），总占比为 60.9%，其次是 80 后，占比为 31.5%。这两个年龄段的人数占比之和超过 90%。



值得注意的是，2019 年 00 后网络安全人才进入网络安全产业，预计在未来的 2-3 年会有更多的 00 后进入网络安全产业。

在智联招聘平台上，求职网络安全岗位的人才中，毕业于河北科技学院、山西工商学院、郑州科技学院、中国石油大学的人才最多。下表给出了智联招聘平台上，投递网络安全岗位的求职者毕业的前 20 所国内大学。来自这 20 所大学的网络安全岗位求职者占到了所有求职者总数的 9.56%。特别是河北科技学院和山西工商学院，来自这两所高校的网络安全岗位求职者，占了求职者总数的 1.49%。

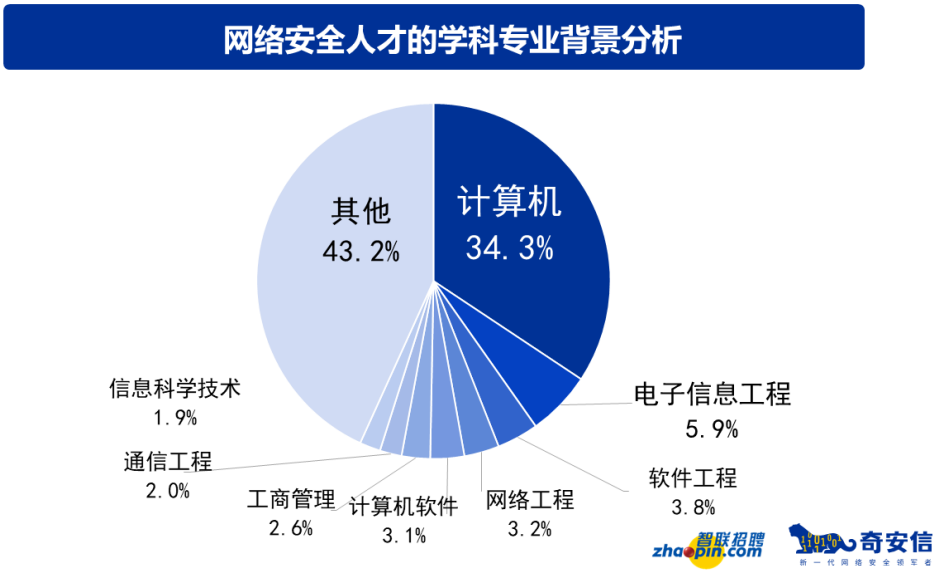
序号	学校	占比
1	河北科技学院	0.75%
2	山西工商学院	0.74%
3	郑州科技学院	0.66%
4	中国石油大学	0.60%
5	北京理工大学	0.60%
6	国家开放大学	0.57%
7	北京城市学院	0.56%
8	河北传媒学院	0.55%
9	吉林大学	0.47%
10	黄河科技学院	0.44%
11	北京航空航天大学	0.44%
12	中国人民大学	0.41%
13	北京大学	0.38%
14	郑州大学	0.37%
15	北京交通大学	0.37%
16	北京联合大学	0.36%
17	北京邮电大学	0.36%
18	北京科技大学	0.33%

19	电子科技大学	0.30%
20	北京工业大学	0.30%

表 5 求职者毕业学校占比 Top20 的高校

通过上表可以发现，高校分布进一步亲民化，不再是重点高校的学生占据排行榜首，更多的省/市地方院校也加入培养网络安全人才的大军。但从毕业院校占比 TOP20 来看，网络安全人才还是重点高校居多。优秀的网络安全人才不止取决于毕业院校，更取决于他们的能力是否符合用人单位需求。这些普通高校的网络安全人才质量是未来我们需要更加关注的。

从网络安全人才的学科专业背景来看，仅有极少数求职者有网络安全或信息安全的学科教育背景，而更多的网络安全岗位求职者实际上是来自于计算机、电子信息工程、软件工程和网络工程等兄弟专业。这也再次说明了，网络安全专业向市场输出的人才数量非常有限。

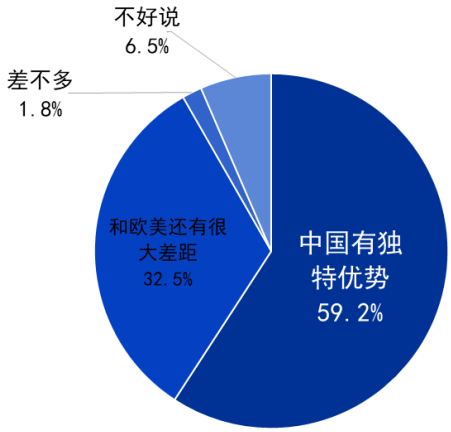


四、 新晋网络安全人才专项调研分析

更好了解新晋网络安全人才的特点和发展状况，我们采用问卷调研方式，对全国范围内超过 600 名新晋网安人才做专项调研分析。接下来将具体论述相关研究数据与分析结论。

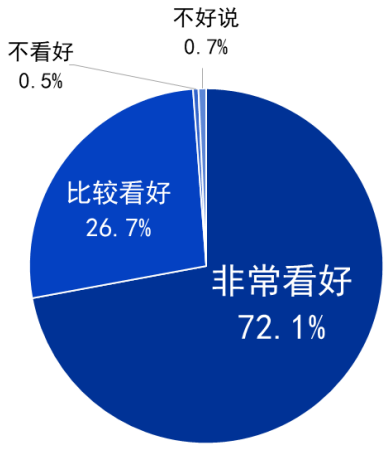
当前信息化建设与网络安全成为各国竞争新高地，新晋网络安全人才对全球网络安全产业的竞争有不同的看法，59.2%的新晋网络安全人才认为中国有独特优势；32.5%的新晋网络安全人才认为和欧美还有很大差距，国内安全产业起步晚。具体情况如下图所示：

网络安全人才对未来我国与欧美发达国家之间的看法

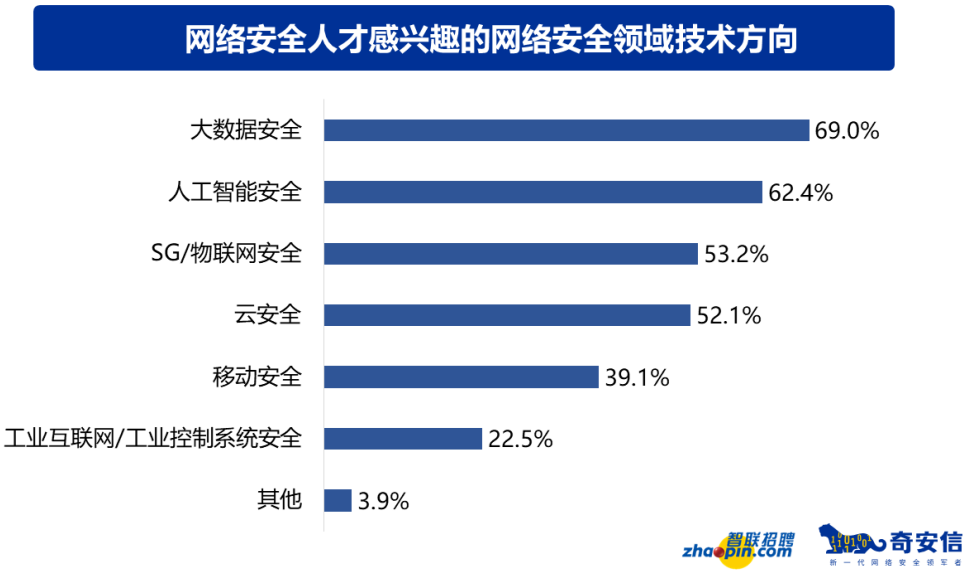


近年来，勒索软件、信息泄露等网络安全事件频发，全社会越来越重视加强网络安全建设。在这种背景下，新晋网络安全人才对于网络安全行业的发展前景也有不同的看法：72.1%的人非常看好网络安全行业的发展，认为有需求，有法律支撑，肯定会成为下一个新的风口；26.7%的人才认为网络安全行业还是有很大的市场空间，比较看好其发展前景；还有 0.5%的人才不看好网络安全产业，他们认为本行业竞争太激烈，而当前市场空间有限。

网络安全人才对行业发展前景的看法



调研显示，69%的新晋网络安全人才感兴趣的网络安全领域或技术方向是大数据安全，62.1%的新晋网络安全人才对人工智能安全最感兴趣，其次是 5G/物联网安全。大家更感兴趣的多是实际接触较多，宣传力度较大的领域。



五、 网络安全人才市场发展趋势

结合智联招聘网络安全人才大数据及奇安信行业安全研究中心对教育机构、大型政企机构和安全企业的调查研究成果，我们总结了网络安全人才市场发展的几大趋势。

1） 网络安全人才岗位从选配到标配

从 2018-2019 年度的网络安全人才需求指数的增长趋势可以看出，即社会整体对网络安全人才需求数量的暴增，说明社会层面开始重视网络安全的保障工作，积极引入专业安全人才，建立网络安全团队，应对网络空间各方面威胁与风险。

结合当前我国在网络安全领域的立法和监管力度、深度，持续增加，广大政企单位招聘使用网络安全人才，不仅仅是自身的需要，更是国家和政府的要求。

随着法律制度进一步完善，安全团队逐步成为政企单位组织的标配。政企机构必将更加重视和更多招用安全人才，按照国家相关合规标准与要求，逐步提升技术和管理手段，建立完善网络安全专门的机构职能体系。

2） 基础性网络安全人才需求更显迫切

根据对一些政企机构的调研，了解到他们招聘的网络安全人员结构正发生一些变化，不再仅关注网络安全高水平攻防的人才，而是更注重使用基础性网安人才，从全面构建安全防御能力的角度，逐步吸纳所需人才，组建网络安全专业队伍。

基础性安全人才与高学历、高智商挖洞人才的需求量，形成一个人才需求的“金字塔”结构。底座是基础性的实践应用型人才，塔尖是高学历、能力超长的研究型、创新型人才。

未来，随着各个行业所需基础性人才数量增大，尤其既熟悉用人单位经营业务，又熟悉安全业务，同时还能熟练使用市场上各种安全产品的人才会会更紧俏，需求也更迫切。

3） 安全需求推动人才培养持续创新

近年来，面对网络安全人才近百万的市场缺口，高等学校、安全企业、社会培训机构、相关科研机构和协会联盟等，都积极探索、实践多元化、协同联动的网络安全人才培养模式，尤其是 2018-2019 年出现一些创新的人才培养新特点值得关注。

a）基地模式打通人才输送最后一公里

b）高校与安全企业，挖掘潜力，联合持续创新

在高校和企业持续加大创新力度的同时，国家教育部也于 2018 年底和 2019 年初分别发布了《教育部高等教育司关于公布有关企业支持的产学合作协同育人项目申报指南(第一批/第二批)的函》，从而极大鼓舞安全企业和高校合作的创造力，未来我们将会看到更多校企深度合作的新模式、新路径。

4） 新型安全竞赛促进专项人才选拔培养

近些年，各大高校、团体等举办各种类型的安全类夺旗、攻防等竞技比赛，一方面可以以赛促学，培养选拔网络安全的专业能手；另一方面可以促进全社会更加关注重视网络安全。2018-2019 年度的网络安全比赛依然很多，但出现一些细分安全领域的专项比赛，以及某些特定行业的安全竞技比赛，促进了网络安全专项人才的培养，对其他领域和行业的网安人才培训选拔具有示范意义。

附录1　2019 年国内外重大网站安全事件

一、 武汉四人利用快递系统漏洞盗卖 1100 万公民信息被判刑

2019 年 1 月，陈某、蒋某、胡某、孙某等四人因利用快递公司大客户发货系统漏洞，盗取客户发货账号，获取大量公民个人信息出售并从中获益，被武汉江汉区法院以侵犯公民个人信息罪，一审分别判处三年至四年不等的有期徒刑。

根据该快递公司向公安机关的报告，有多个 IP、MAC 地址在其企业大客户发货系统上盗取客户发货账号 500 多个，并利用系统漏洞非法窃取这些大客户的快递单页。后经司法鉴定中心检验，该犯罪团伙的涉案电脑及 U 盘中，分别检测出公民个人信息超过 1100 万条。

二、 1600 多名酒店房客被非法偷拍，甚至被海外色情网站直播

2019 年 11 月，公安部网安局通报了一起非法生产、销售、使用联网型针孔摄像头大案。这种针孔摄像头利用配套的手机 App 等客户端，通过互联网远程控制摄像头，偷拍偷窥侵犯他人隐私。2019 年三月，韩国警方抓获了一个犯罪团伙，他们涉嫌在韩国 10 个城市的 30 家酒店里安装了 1 毫米超微型摄像头，对 1600 多名房客进行非法偷拍，并在海外色情网站上直播获取暴利。

2019 年，国内影响最大物联网安全事件非酒店偷拍莫属。过去两年间酒店偷拍事件层出不穷，从单体民宿、自如、Airbnb 到威斯汀酒店和皇冠假日酒店都不能幸免。

三、 OEM 摄像头严重漏洞使 200 万物联网摄像头“裸奔”

2019 年 4 月，安全研究者披露了可能是迄今最为严重的物联网摄像头安全漏洞，受影响监控摄像头数量超过 200 万个，来自包括 HiChip、TENVIS、SV3C、VStarcam、Wanscam、NEO Coolcam、Sricam、Eye Sight 和 HVCAM 等多个摄像头厂商。

这些产品都使用了某国内厂商开发的名为 iLnkP2P 的 P2P 通讯组件。该组件包含两个漏洞，可能使远程黑客能够找到并接管设备中使用的易受攻击的摄像机并监视其所有者。

此外，7 月物联网摄像头制造商 Swann 修补了其联网摄像头中的一个漏洞，该漏洞使远程攻击者可以访问其视频源。9 月，多达 80 万个基于 IP 的闭路电视摄像机暴露在零日漏洞攻击之下，该漏洞可能使黑客能够访问监视摄像机，监视和操纵视频源或植入恶意软件。

四、 美国在线辅导网站 Wyzant 被黑，200 万用户数据泄露

2019 年 5 月，总部位于美国芝加哥、提供超 250 个科目的在线辅导网站“Wyzant”遭遇了数据泄露。Wyzant 数据库中有超 200 万注册用户和超 76,000 名活跃辅导员。Wyzant 发送给受影响客户的电子邮件通知副本显示，攻击者获得了其中一个数据库的访问权，包括名字、姓氏、电子邮件地址、邮政编码及某些客户的 Facebook 个人资料图片、使用 Facebook 登录平台的人等个人识别信息等均已被窃。

五、 马印航空、泰国狮航数千万条旅客记录泄露

2019 年 9 月，研究人员发现有两个数据包在多个数据交换论坛中流通。两个数据库中，一个包含 2100 万条记录，另一个包含 1400 万条记录。这些数据属于马印航空 Malindo Air 和泰国狮航 Thai Lion Air，以及巴迪航空 Batik Air（该公司的母公司也是泰国狮航）。

泄露的详细信息包括旅客和预订 ID，实际地址，电话号码，电子邮件地址，姓名，出生日期，电话号码，护照号码和护照到期日期等。

六、 日本加密币交易所遭黑客攻击，损失资产 3200 万美元

2019 年 7 月，日本持牌加密货币交易所 Bitpoint 在周四发现不正常的取款行为后，于周五上午停止了所有服务，包括交易、存款和提取任意类别的加密资产。

Bitpoint 的运营母公司 Remixpoint 发布公告称，7 月 11 日晚，BitpointJapan 的虚拟货币交易系统检测出汇款相关的错误。调查结果显示，BitpointJapan 管理的加密货币遭窃，被盗币种目前可确定包括瑞波币-XRP，初步损失预估在 35 亿日(约合 3200 万美元)元左右。其中，大约 25 亿日元的被盗资金属于客户，剩余 10 亿日元属于交易所。

七、 委内瑞拉古里水电站遭网络攻击

2019 年 3 月，委内瑞拉最大的电力设施古里水电站计算机系统控制中枢遭受到网络攻击，引发全国性大面积停电，约 3000 万人口受到影响；7 月，委内瑞拉古里水电站再次遭到攻击，导致包括委内瑞拉首都加拉加斯在内的 16 个州发生大范围停电。

八、 日本制造企业 Hoya 感染挖矿病毒被迫停产三天

2019 年 4 月，日本最大的光学产品生产商 Hoya 公司称，他们位于泰国的工厂曾在 2 月底遭受了一次严重的网络攻击，工厂生产线因此停摆三天。网络攻击发生后，一台负责生产控制的主机服务器被病毒入侵后首先宕机，导致工厂用来管理订单和生产的软件无法正常运行，随后病毒在厂区继续蔓延，相继感染网络中的 100 余台终端设备，导致 Hoya 公司大量系统登录 ID 和密码被黑客窃取。据悉，网络攻击持续三天后，才逐步恢复，期间黑客还曾尝试劫持厂区所有主机用以挖掘加密货币，但均未成功。

九、 Facebook 被爆明文存储 6 亿用户密码，已被查看 900 万次

2019 年 3 月 22 日，据网络安全记者布莱恩-克雷布斯(BrianKrebs)的一份报告表明，Facebook 在没有加密的情况下存储了数亿用户的密码，并且以明文的方式展示给数万名公司职员。据调查，此事件直接影响可能多达 6 亿用户。

消息人士称，Facebook 访问日志显示，大约 2000 名 Facebook 工程师和开发人员对包含纯文本用户密码的内容进行了大约 900 万次内部查询。

Facebook 也在声明中承认了此事：“在 1 月的例行安全审查中，我们发现一些用户密码以可读格式存储在我们的内部数据存储系统中，”Facebook 撰文称，“这引起了我们的注意，因为我们的登录系统本应通过技术来屏蔽密码，使其不可读。我们已经修复了这些问题。为

了提早预防，我们将通知相关用户。“

十、 印度最大的核电站遭到网络攻击

2019 年 9 月，新闻社 IANS 报道称，印度最大的核电站 Kudankulam 核电站的两个反应堆之一已中止运行，而一名 Twitter 用户将该停止与来自朝鲜的 DTrack 网络攻击关联在一起。

10 月 30 日，印度核电公司(NPCIL)证实，Kudankulam 核电站今年 9 月曾遭到网络攻击。根据一份声明，NCPIL 于 2019 年 9 月 4 日接到印度计算机应急响应小组的通知。NCPIL 说，原子能部门(DAE)的专家立即对此事进行了调查。

调查显示，受感染的个人电脑属于一名连接互联网的用户，该网络用于行政用途。这是与关键的内部网络隔离的。这些网络正在被持续监控。另一方面，核电厂系统并未受到影响。

11 月 20 日，印度政府澄清，Kudankulam 核电站计算机系统与管理网络是隔离的，任何企图都无法破坏核电站计算机系统。

十一、 全球 27 亿电子邮件地址和 10 亿密码数据暴露

2019 年 12 月，研究人员发现了一个 Elasticsearch 数据库遭泄露，而此次数据泄露的体量之大令人咋舌，其中包括有 27 亿个电子邮件地址，10 亿个电子邮件账户密码以及一个装载了近 80 万份出生证明副本的应用程序。

根据资料显示，本次被盗的 27 亿个电子邮箱地址中，有 10 亿个密码都是简单明文进行存储。

据报道，大多数电子邮件地址来自中国，包括 qq.com，139.com，126.com，gfan.com 和 game.sohu.com，均来自腾讯，新浪，搜狐和网易等知名互联网公司。一些电子邮件地址具有 Yahoo 和 Gmail 域，还有一些俄语域，例如 rambler.ru 和 mail.ru。

十二、 佛罗里达州遭勒索攻击，政府工作停摆两周

2019 年 6 月 10 日，佛罗里达州莱克城(LakeCity)遭到灾难性的勒索软件攻击，各项市政工作已停摆两周。市政紧急会议投票决定支付价值将近 50 万美元的赎金

尽管该城市的 IT 人员在发现攻击后的十分钟内将受影响的系统断开连接，但是除了在独立网络中运行的警察和消防部分，该市政的几乎所有计算机系统都感染了勒索软件。

此前，佛罗里达州 Riviera City 也遭黑客攻击，支付了 60 万美元赎金。两起袭击有一个共同点，一名政府工作人员点击了一封电子邮件中的恶意附件，使得勒索软件传播至整个网络。

附录2　奇安信网神终端安全管理系统

奇安信网神终端安全管理系统（简称天擎）是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，奇安信还面向所有天擎政企用户免费推出敲诈先赔服务：如果用户在开启了天擎敲诈先赔功能后，仍感染了勒索软件，奇安信将负责赔付赎金，为政企用户提供百万先赔保障，帮政企客户免除后顾之忧。

附录3　奇安信补天漏洞响应平台

补天漏洞响应平台，成立于 2013 年 3 月，是国内专注于漏洞响应的第三方平台。2014 年 12 月更名为“补天漏洞响应平台”，简称“补天平台”。补天平台以守护企业网络安全为使命，是一个致力于企业网络漏洞检测与响应的安全平台。从解决企业网络安全中的漏洞入手，助力保护企业网络安全，建立在漏洞响应领域内的公信力和权威性，成为企业关于漏洞响应的首席知识官。补天平台的职责在于更好的消除漏洞隐患，更好的保护企业安全，是一个公正的、中立的第三方平台，旨在集聚民间优秀白帽子的力量，为企业网络安全提供实时的、高效的安全助力。

该平台于 2013 年 3 月份推出时，是一项针对开源建站系统漏洞征集项目。该项目通过现金奖励的方式，公开征集建站工具软件/系统存在的漏洞，以帮助软件公司和开发者及时修复漏洞，加强国内数百万家网站对黑客攻击的防范能力，并加强奇安信网站安全产品的漏洞检测能力和攻击防御能力。该项目目前已陆续协助 ShopEx、Discuz!、ECShop、ShopEX、PHPWind、PHPCMS 等上百个知名建站和 IT 系统修复了安全漏洞。

从 2014 年 6 月开始，除了通用型漏洞外，补天平台也开始陆续收到事件型漏洞的报告。事件型漏洞主要是指网站或应用的一个具体漏洞，只对该网站自身有影响。如某政府网站后台存在弱口令可进后台 GETSHELL，某企业门户网站存在重要信息泄露等。

面对复杂多变的网络安全态势和层出不穷的攻击手段，补天平台通过 SRC、众测等方式服务广大企业，以安全众包的形式让白帽子从模拟攻击者的角度发现问题，解决问题，帮助企业树立动态、综合的防护理念，维护企业的网络安全。

补天平台通过帮助企业建立 SRC（Security Response Center，安全应急响应中心），一方面，可以最大程度避免企业由于安全漏洞遭受损失；另一方面，尊重白帽子的劳动产出，让白帽子获得一定的收益。

继 2014 年下半年提供专属 SRC 服务之后，2016 年 4 月补天平台又推出众测服务。补天众测是补天漏洞响应平台基于众包模式打造的互联网专项安全测试服务，通过集结国内顶尖的安全专家，采取生产环境或者测试环境进行安全渗透测试，帮助企业发现系统和业务中的潜在漏洞及风险，为企业提供深度定制化的安全测试服务方案。

2017 年 9 月推出的漏洞情报服务，主要向企业提供第一手的面向不同行业精准的行业漏洞情报。补天平台 4 万余名白帽子及补天安全专家获取的漏洞数据，经过联合分析研判、协同挖掘和脱敏加工，最终形成深层次的行业漏洞情报。通过补天平台行业标签算法，第一时间向行业客户进行精准推送。补天平台希望将多种安全服务有机的整合起来，进一步提升企业的漏洞响应能力和积极防御能力。

2019 年 3 月补天平台推出数据泄露监控服务，旨在通过补天平台积累多年的数据挖掘经验和信息采集、智能处理技术，帮助企业及时发现在 Github 上泄露的源代码和主流网盘上泄露的敏感文件，减少因源代码、敏感文件泄露对企业的损害。

补天平台将多种安全服务有机的整合起来，进一步提升企业的漏洞响应能力、积极防御能力和常态化安全运营能力。

2019 年 5 月，基于补天众测的漏洞治理与风险管理平台入选工业和信息化部公布网络安全技术应用试点示范项目名单，在网络安全漏洞领域唯一以安全厂商身份入选。作为奇安信集团独立开发运营的 SaaS 平台，通过标准化的工作流程驱动企业高效处置精英可信白帽发现的漏洞。持续生产和运营的安全风险线索能保障用户及时、精准的获知和处置。本平台聚焦为企业解决漏洞发现不全面、漏洞修复不彻底的难题以及威胁无法提前预知和防范的风险管理问题，帮助企业完善漏洞治理架构和风险管理机制，助力企业构建管理闭环、关口前移、源头治理的积极防御体系。

截止 2020 年 3 月，平台注册白帽子已达 64000 余名，累计为 10 万 6 千多家企业报告的漏洞超过 44 万个。其中，公益 SRC 服务（安全应急响应中心）累计为 5700 余家企业免费收集和报告漏洞，平均每天报告经过验证有效的漏洞 160 余个，每天帮助企业防控数千万条潜在的数据泄露风险。

补天漏洞响应平台先后被公安部、国家信息安全漏洞共享平台（CNVD）、国家信息安全漏洞库（CNNVD）分别评定为技术支持先进单位、漏洞信息报送突出贡献单位和一级技术支撑单位。

网聚安全力量，为社会提供准确、详实的安全情报，让全中国网络都实现漏洞的及时发现与快速响应是补天平台始终坚持并不断履行的社会使命。

附录4　奇安信集团安服团队

奇安信是北京 2022 年冬奥会和冬残奥会官方网络安全服务和杀毒软件赞助商，作为中国领先的网络安全品牌，奇安信多次承担国家级的重大活动网络安全保障工作，创建了稳定可靠的网络安全服务体系——全维度管控、全网络防护、全天候运行、全领域覆盖、全兵种协同、全线索闭环。

奇安信安全服务以攻防技术为核心，聚焦威胁检测和响应，通过提供咨询规划、威胁检测、攻防演习、持续响应、预警通告、安全运营等一系列实战化的服务，在云端安全大数据的支撑下，为客户提供全周期的安全保障服务。

应急响应服务致力于成为“网络安全 120”。2016 年以来，奇安信已具备了丰富的应急响应实践经验，应急响应业务覆盖了全国 30 个省份，处置政企机构网络安全应急事件超过两千起，累计投入工时 25000 多个小时，为全国超千家政企机构解决网络安全问题。

推出应急响应训练营服务，将一线积累的丰富应急响应实践经验面向广大政企机构进行网络安全培训和赋能，帮助政企机构的安全管理者、安全运营人员、工程师等不同层级的人群提高网络安全应急响应的能力和技术水平。奇安信正在用专业的技术能力保障着企业用户的网络安全，最大程度的减少了安全事件所带来的经济损失以及恶劣的社会负面影响。

应急响应 7*24 小时热线电话：4008 136 360 – 6

附录5　工业控制系统安全国家地方联合工程实验室

工业控制系统安全国家地方联合工程实验室（简称：工业安全国家联合实验室）是由国家发展与改革委员会批准授牌成立，由奇安信集团承建的对外开放的工业控制安全技术方面的公共研究平台。

工业安全国家联合实验室以对工业控制系统安全领域有重大影响的前沿性、战略性技术作为研究目标，建立以工程实验室为主，联合高等院校、科研院所和国家需求部门、企业共同参加的，产、学、研、用相结合的合作机制，发挥高等院校、科研院所在基础理论研究方面的力量和优势，发挥国家需求部门、企业在技术创新和应用方面的主体作用，共享科研成果。

工业安全国家联合实验室积极吸纳国内外优秀的科技人才，建立高水平专业人才培养基地。目前实验室已与北京大学、西安电子科技大学、吉林大学、武汉大学、北京理工大学、信息工程大学等均建立了人才联合培养机制。

工业安全国家联合实验室拥有软件著作权 7 项，专利 16 项，创新地提出了工业互联网自适应防护架构（PC4R），推出了工业主机安全防护系统、工业防火墙/网关、工业安全监测系统、工业安全监测控制平台、工业互联网安全监测服务平台等工业安全领域完整解决方案及产品，并已经在众多央企和工业企业中进行应用。未来，工业安全国家联合实验室将充分利用科技资源，发挥产学研联盟作用，打造产业链合作，与产业链企业实现互利共赢，在合作中共同壮大，努力成为工业互联网安全产业创新的龙头。

附录6　奇安信威胁情报中心

奇安信威胁情报中心是奇安信集团旗下的威胁情报专业机构。该中心以业界领先的安全大数据资源为基础，基于长期积累的核心安全技术，依托亚太地区顶级的安全人才团队，结合强大的数据分析能力，实现全网威胁情报的实时、深入、全面综合分析，为企业和机构提供网络空间威胁防护的情报预警及分析能力。

奇安信 ALPHA 威胁分析平台（https://ti.qianxin.com），是奇安信集团面向安全分析师和应急响应团队提供的一站式云端服务平台，该平台拥有海量互联网基础数据和威胁研判分析结果，为安全分析人员及各类企业用户提供基础数据的查询、攻击线索拓展、事件背景研判、攻击组织解析、研究报告下载等多种维度的威胁情报数据与威胁情报服务，提供全方位的威胁情报能力。

微信公众号：

奇安信威胁情报中心：

奇安信病毒响应中心：

附录7　红雨滴团队（Red Drip Team）

奇安信旗下的高级威胁研究团队红雨滴（RedDrip Team，@RedDrip7）,成立于 2015 年（前身为天眼实验室），持续运营奇安信威胁情报中心至今，专注于 APT 攻击类高级威胁的研究，是国内首个发布并命名“海莲花”（APT-C-00，OceanLotus）APT 攻击团伙的安全研究团队，也是当前奇安信威胁情报中心的主力威胁分析技术支持团队。

目前，红雨滴团队拥有数十人的专业分析师和相应的数据运营和平台开发人员，覆盖威胁情报运营的各个环节：公开情报收集、自有数据处理、恶意代码分析、网络流量解析、线索发现挖掘拓展、追踪溯源，实现安全事件分析的全流程运营。团队对外输出机读威胁情报数据支持奇安信自有和第三方的检测类安全产品，实现高效的威胁发现、损失评估及处置建议提供，同时也为公众和监管方输出事件和团伙层面的全面高级威胁分析报告。

依托全球领先的安全大数据能力、多维度多来源的安全数据和专业分析师的丰富经验，红雨滴团队自 2015 年持续发现多个包括海莲花在内的 APT 团伙在中国境内的长期活动，并发布国内首个团伙层面的 APT 事件揭露报告，开创了国内 APT 攻击类高级威胁体系化揭露的先河，已经成为国家级网络攻防的焦点。

红雨滴团队 LOGO：

“红雨滴”背后的故事——“从 100 亿个雨滴中找一个红雨滴”

2006 年 11 月 20 日，因发现 J 粒子而获得诺贝尔奖的著名华裔物理学家丁肇中教授来到中国驻瑞士大使馆，做了一场精彩的讲座。丁肇中教授形容自己发现构成物质的第四种基本粒子-J 粒子的高精度实验时说到：“相当于在北京下雨时，每秒钟有 100 亿个雨滴，如果有一个雨滴是红色的，我们就要从这 100 亿个里找出它来。”

而奇安信威胁情报中心高级威胁分析团队同样需要在海量数据中精准找寻那些红色威胁。最终，我们选择了“红雨滴”作为团队的名称。