CAICT 中国信通院

2020年上半年网络安全态势情况综述

指导：工业和信息化部网络安全管理局

编制：中国信息通信研究院

2020年9月

前　言

在工业和信息化部网络安全管理局的指导下，中国信息通信研究院发布《2020 年上半年网络安全态势情况综述》，通过对电信和互联网行业 2020 年上半年网络安全威胁及事件的监测、汇总、分析认定和处置情况进行梳理和分析，提出上半年十大网络安全态势的突出特点，并对下半年网络安全趋势进行预测。

一、上半年网络安全态势

与 2019 年下半年相比，安全形势依旧严峻，2020 年上半年公共互联网网络安全威胁数量总体呈大幅度上升趋势，但整体安全态势平稳，未发生重大区域性、行业性网络安全突发事件。

（一）DDoS 攻击强度、类型、重点目标基本不变。共监测到针对基础通信网络的 DDoS 攻击 45 万余次，与去年相比无明显变化。攻击类型主要为 TCP SYN Flood 和 UDP Flood，未发现新类型。攻击规模主要以 10Gbps 以下的攻击为主，占比约 70%。攻击源方面，攻击流量中境外流量占比约 50%。攻击对象方面，浙江、江苏、福建、北京、山东等 ICP 资源比较集中的省网依然是主要攻击目标。

（二）安全威胁处置数量大幅增长，处置率显著提高。2020 年上半年，工业和信息化部网络安全威胁信息共享平台（以下简称平台）共完成约 7.6 万个各类威胁处置。一是完成约 1.2 万个安全隐患的处置工作，相比 2019 年下半年上涨约 5 倍，北京市、广东省、上海市和江苏省等地处置完成量约占安全隐患处置总量的 53.76%。二是完成恶意程序传播威胁处置约 4 万个，相比 2019 年下半年增长 13 倍，广东省、北京市、江苏省为处置数量排名前三的省份，在仿冒 APP 治理工作中，累计处置腾讯应用宝、百度手机助手等应用商店仿冒 APP 类事件 72 件。三是协调处置网页篡改问题近 5 千

个、网站仿冒 35 个，相比 2019 年下半年增长 40.11%，北京市、广东省、河南省为处置数量排名前三的省份。四是处置僵尸网络类事件近 7 千起，相比 2019 年下半年增长 36 倍，来自河南省、广东省、浙江省、辽宁省、北京市的 IP 占重复发起攻击 IP 的 33.49%，广东省、江苏省、浙江省、北京市和山东省处置 43.16%的僵尸网络事件。

（三）多个境外 APT 组织利用“新型肺炎”话题为诱饵对我国境内目标和机构实施攻击活动。监测发现 APT 组织蔓灵花、摩诃草、海莲花、透明部落等攻击活动活跃，其中，海莲花是对我境内攻击最频繁的 APT 组织，利用以 COVID-19 为主题的钓鱼邮件，对我目标进行入侵。从攻击手法看，从钓鱼邮件攻击向利用 0day 或 Nday 漏洞实施攻击转变。

（四）医疗行业高危漏洞数量与 Web 攻击事件占比最高，攻击危害不容忽视。从漏洞类型和分布区域看，高危漏洞占比高达 72%，上海、江苏等规模较大省市漏洞数量相对较多。从事件类型与后果看，Web 攻击事件占比高达 96.44%，而僵木蠕攻击危害同样严重，可造成系统不可用、数据丢失等严重后果。多家医疗机构网站遭受漏洞利用等攻击，其中暴力破解达到单日 80 万次高峰。例如，某市中心医院数据上报系统存在未授权访问漏洞，攻击者可获取医护人员敏感信息。

（五）人工智能数据流通存在泄露和滥用风险。目前，多数人工智能初创企业普遍使用开源框架进行应用开发并存在较大依赖性。由于缺乏严格的安全认证，将面临不可预期的系统漏洞、数据泄露和供应链断供等安全风险。例如，2020 年上半年，中国信息通信研究院对我国 14 款 APP 进行传输安全、权限控制等安全项检测，发现 5 款 APP 存在数据泄露风险。

（六）5G 智慧城市加速发展同时仍需防范可用性破坏、数据泄露等风险。5G 与城市现代化的深度融合与迭代演进，推动 5G 智慧城市建设提速发展。5G 新技术新架构加大了网络安全边界泛化的程度，导致线上线下安全问题复杂交织、智能基础设施安全防御难度增大。具体而言，5G 智慧城市网络架构主要包括应用层、数据平台层、网络层、边缘层、终端层等架构层面，可能面临服务中断、数据滥用与隐私信息泄露等风险。

（七）部分远程办公软件存在安全漏洞，我国成为重要攻击目标。随着远程办公方式兴起，一定程度上增加了暴露面，2020 年上半年出现多起围绕 VPN 漏洞的 APT 攻击活动。4 月，APT 组织 DarkHotel 利用 VPN 零日漏洞入侵多家我国政府单位及驻外机构，两百余台 VPN 服务器被入侵。此外，DarkHotel 和 Wellmess 组织利用 VPN 漏洞进行攻击，前者主要针对我基层单位，后者主要针对我多家科研机构。

（八）远程桌面协议访问点仍是最常见的勒索病毒攻击媒介，攻击目标正向关键基础设施渗透。与恶意程序关联的勒索病毒中，占比排名前三的依次是 phobos、GlobeImposter 和 Crysis，安全性较差的远程桌面协议访问点仍是最常用攻击媒介。同时，攻击目标正逐渐渗透至能源、制造等行业。例如，2020 年 4 月，葡萄牙能源公司 EDP 遭到勒索攻击，赎金 1 千余万美元。

（九）僵木蠕攻击中以僵尸网络为主，针对大中型政企机构的攻击事件中挖矿木马占比较多。上半年僵木蠕事件共 2.8 亿起，其中，僵尸网络事件 1.9 亿条，木马事件 8 千余万条，蠕虫事件 77 万条。北京受到僵尸网络的侵害最为严重，江苏受到木马侵害最为严重，陕西省受到蠕虫侵害最为严重。此外，在上半年大中型政企机构遭受恶意程序攻击事件中，挖矿木马占比仅次于勒索病毒。

（十）诱骗欺诈和流氓行为成为移动恶意程序最主要攻击手段。上半年移动恶意程序事件近 1.3 亿条。其中，诱骗欺诈事件 1.1 亿条，流氓行为事件近两千万条，隐私窃取事件三百余万条，远程控制事件一百余万条，资费消耗事件 23 万条，恶意扣费事件 16 万条，系统破坏类事件 6 万条，恶意传播事件 2 万条，诱骗欺诈事件和流氓行为事件数量远超其他六类事件数量总和。

二、下半年网络安全趋势

（一）后疫情时代的网络安全形势更加严峻。随着在线办公、在线教育等线上生产和生活方式日趋成为主流，现实和数字世界边界逐渐模糊，网络攻击、勒索病毒、安全漏洞等网络安全风险将进一步向现实世界渗透，网络安全成为事关经济社会稳定、生产安全、人民群众生命财产安全的问题。

（二）APT 攻击中仍会大量利用已知漏洞。APT 组织在网络攻击中更倾向于使用包括 1-day[1]在内的漏洞，将漏洞披露后的空窗期视为攻击的黄金时间。特别是对于防御方存在已知漏洞的系统，如果未及时进行有效的安全加固，仍将面临极大的安全风险。

（三）勒索病毒攻击方式将持续增多。利用漏洞和弱口令植入勒索病毒事件将逐渐增多，攻击者将以此类漏洞为跳板，植入病毒并攻击其它设备以提升攻击效率。定向攻击方式增多，相对于传统“广撒网”的攻击方式，攻击者将会选择医院、学校、大型企业等高价值的目标进行定向攻击。

（四）针对供应链的攻击将成为网络定向攻击重要手段。攻击者利用机器学习等技术对供应链发起攻击，供应链安全形势愈发严峻。供应链安全风险主要包括源码、库篡改或污染，开发工具污染以及违规操作等，攻击者通过寻找相关漏洞等方式等进行攻击。供应链中的每个环节都可能成为网络

1 1-day 漏洞与尚未披露的 0-day 漏洞不同，是指刚刚披露且尚没有足够时间进行修复或缺乏有效修复手段的漏洞

攻击的对象。

（五）“新基建”安全将成为行业关注热点。“新基建”以 5G 等通信网络基础设施为承载，推动构建全连接的新型网络物理世界，网络安全的战略性、全局性和基础性地位尤为凸显。“新基建”技术架构加速革新、应用生态深度融合、多元场景不断涌现等新特征给行业网络安全工作提出新挑战，同时，安全同步建设的战略保障需求也将为网络安全产业注入新动能，带动网络安全技术产品创新发展。工信部以引领网络安全新产业、建设安全“新基建”为主题，面向全行业征集 2020 年网络安全技术应用试点示范项目，挖掘新一代信息技术与网络安全技术融合创新的典型应用和最佳实践，将有力提升新型信息基础设施安全保障能力，推动网络安全生态协同共治。

（六）公共服务平台将助力产业良性发展。疫情期间，中国电信监测发现各类攻击亿余次，启动防护措施 3 千余万次，有力护航 5 千余家客户。中国移动流量清洗服务平台为近 50 余家企业提供了抗 DDoS、APT 分析防护等服务，协助企业开展应急演练 20 余次，累计发现防护攻击 1 千余次。“联通云盾”面向中国联通全网用户，具备全国近 3T 的流量清洗、DNS 解析监测与处置等多项重要网络安全技术手段。基础电信企业通过公共服务平台输出安全能力已获得初步成效。随着产业公共服务平台建设的不断加快，网络安全相关机构、

企业的能力和研究成果不断推出，我国网络安全产业环境将持续优化。

（七）网络安全市场投融资仍将持续活跃。截至 2020 年 7 月，已有超过 20 家网络安全企业获得资本青睐。从投融资轮次来看，目前网络安全相关投融资仍集中在早期阶段，B 轮及之前的融资事件占比超过 60%。从投融资金额来看，数亿元大融资频现，1 亿元人民币及以上的融资事件为 10 件，占比达到 43.5%。在国家新型基础设施相关政策驱动下，网络安全产业仍将成为资本市场投融资的热点方向。

（注：上述态势分析及监测处置数据主要来自中国电信、中国移动、中国联通、奇安信、上海观安、恒安嘉新、安恒信息、安天、微步在线、绿盟科技等电信和互联网行业信息报送单位。）

附件

2020 年上半年十大网络安全事件

2020 年上半年，正值疫情全球爆发的特殊时期，网络空间安全也面临巨大挑战。安全漏洞、APT 攻击、数据泄露等网络安全事件频发，政府单位、医疗机构、科技企业等成为攻击重点目标，数据泄露后果日趋严重。

一、境外黑客组织攻击我国视频监控系统

2 月，有境外黑客组织发布推文宣布将于 2 月 13 日对我国实施网络攻击。本次攻击的主要目的是对视频监控系统实施破坏，攻击目标包括科大讯飞、中集集团、网智天元、浩瀚深度等国内企业以及政府网站。黑客同时声称已掌握我国境内大量摄像头控制权限，并在 pastebin 网站上公开了部分受控目标。经核实，这些受控目标均为我国某视频监控设备制造企业生产的视频监控设备。工信部网络安全威胁信息共享平台针对此次事件，及时发布处置建议，提醒部署该产品的用户及时部署安全防护措施。

二、APT 组织“绿斑”（GreenSpot）借“新型肺炎”话题为诱饵对我国发起网络攻击，意图窃取用户邮箱账号密码

2 月，疑似 APT 组织“绿斑”持续以“新型肺炎”话题为诱饵，利用仿冒 QQ 和 163 邮箱的域名对我国有关政府部门、

医疗机构发起钓鱼攻击。该黑客组织通过邮件等方式发送“疫情防控日报表”、“《南部杜氏中医》献方”等文档下载链接，一旦受害者点击该链接，则会弹出要求验证邮箱账号的页面，诱导输入账号与密码，并将输入的信息回传到攻击者的服务器。工信部网络安全威胁信息共享平台针对此次事件，及时发布处置建议，提醒相关单位提高警惕、加强防范。

三、APT 组织“蔓灵花”对我国境内主机发起攻击，非法控制主机并窃取敏感信息

3 月 1 日至 4 月 19 日，APT 组织“蔓灵花”对我国 17 台主机植入木马，窃取并对外传输主机敏感信息。攻击者 IP 主要分布在美国，受控流量主要流向保加利亚和美国。6 个攻击者控制端域名中，有一半的控制域名注册商为美国域名注册机构。工信部网络安全威胁信息共享平台及时处置威胁信息，督促地方主管部门排查安全风险并完成整改。

四、南亚 APT 组织“肚脑虫”（Donot）针对我及周边国家政府系统开展新一轮攻击窃密

南亚 APT 组织“肚脑虫”（Donot）表现活跃，利用新型冠状病毒疫情（COVID-19），以中国等周边国家的政府机构为目标进行网络攻击活动，窃取机密敏感信息。据调查，2017 年起该组织开始针对中国等周边国家和地区发起针对性的网络攻击，该组织目前具备针对 Windows 与 Android 双平台的攻击能力。

五、国外黑客组织针对多国外贸行业发起攻击，可能导致敏感信息泄漏

4 月，有国外黑客组织针对外贸行业进行钓鱼邮件投放攻击。攻击成功后会自动释放后门程序，将计算机中 Office 文档、台账资料、邮箱和浏览器账号密码等敏感信息回传至该组织的匿名邮箱中。攻击目标遍布全球多个国家，国内也有部分企业遭受此类攻击。工信部网络安全威胁信息共享平台及时预警处置活跃恶意攻击 IP、URL 信息，并通报遭受攻击企业采取相应防范措施。

六、自动化运维工具 SaltStack 被曝存在两个远程命令执行漏洞

5 月 3 日，国外安全团队披露自动化运维工具 SaltStack 存在两个高危远程命令执行漏洞，允许攻击者以 root 身份劫持使用该框架的数据中心和云服务,执行任意代码。受此漏洞影响的版本为 SaltStack 3000.2 之前的版本。目前，SaltStack 已发布最新更新，修复了以上漏洞。据互联网公开数据显示，目前全球共有 5933 个 IP 开放了 SaltStack 服务，其中国内数量为 1086 个，占全球总量的 18.3%。针对该事件，工业和信息化部网络安全威胁信息共享平台迅速组织行业力量，对境内 SaltStack 资产信息开展了检测和研判，确认存在漏洞的用户，并指导涉事单位按照相关安全建议修复漏洞及整改系统。

七、以色列研究人员发现新 DNS 协议漏洞 NXNSAttack，

可导致大型分布式拒绝服务攻击

5 月 21 日，以色列特拉维夫大学和以色列跨学科中心披露 DNS 协议漏洞 NXNSAttack，可导致大型分布式拒绝服务攻击。研究人员表示，该漏洞主要存在于 Unbound 和 BIND 中，会影响所有递归 DNS 解析器，已被证实会影响由谷歌、微软、亚马逊、甲骨文和 IBM 等提供的 DNS 服务。目前，受影响的组织已修复了其软件和服务器，防止被攻击。Unbound 是一个具有验证、递归和缓存等功能的 DNS 解析器。据互联网公开数据显示，目前全国共有一百余个 IP 使用了 Unbound 程序。BIND 是一款实现 DNS 服务器的开放源码软件，提供双向解析、转发、子域授权等功能，是世界上使用最为广泛的 DNS 服务器软件。据互联网公开数据显示，目前全国共有一千余个 IP 使用了 BIND 程序。针对该漏洞，工信部网络安全威胁信息共享平台迅速组织行业力量，确认境内存在对应漏洞的 Unbound 用户 IP，并组织涉事单位按照相关安全防护建议进行漏洞修复及系统整改。

八、美国 Treck 公司开发的 TCP/IP 协议实现产品存在严重安全漏洞，影响全球数亿台物联网设备安全

6 月 18 日，美国国土安全部发布了一项重要的安全建议，警告称有十九个新发现的安全漏洞影响到全球多家供应商生产的数亿台物联网设备。这组被称为“Ripple20”的漏洞位于 Treck 公司开发的专用于嵌入式系统的低级 TCP/IP 软件库

中，这些漏洞可以用于远程代码执行、DoS 攻击和获取潜在的敏感信息。据统计，受影响的设备目前已应用于各个行业。针对该事件，Treck 公司已发布了 TCP/IP 协议栈 6.0.1.67 或更高版本，修复了大部分漏洞。工信部网络安全威胁信息共享平台及时收录该漏洞，并通过平台和官方门户网站发布了风险提示，给出技术防范措施与建议。

九、甲骨文云数据平台泄露数十亿条网络数据记录

6 月 22 日，据国外媒体报道，美国科技巨头甲骨文公司（Oracle）的云数据平台 BlueKai 被曝出泄漏了数十亿条记录的 Web 跟踪数据。由于平台服务器处于不安全状态且没有密码，这些数据正在被泄漏到互联网中，可被任何人查找。BlueKai 是一个基于云的大数据平台，支持甲骨文公司进行个性化的在线、离线和移动营销活动。目前，甲骨文公司已表示将采取其他措施以避免此类问题再次发生。除此以外，该公司拒绝透露更多细节，并拒绝透露是否就此事件向美国或国际监管机构发出警告。

十、Netgear 路由器曝出严重漏洞，影响 79 种不同设备

2020 年上半年，安全研究人员发现 Netgear 路由器存在栈缓存溢出远程代码执行漏洞，该漏洞影响 79 种不同型号 Netgear 路由器的七百余种固件版本，受影响的固件版本最早于 2007 年发布。远程攻击者可利用该漏洞以 root 权限执行代码并接管设备。通过监测，发现境内受该漏洞影响的用户

IP 四百余个，工信部网络安全威胁信息共享平台迅速组织人员，通过平台进行预警提示，通知涉事单位及时修复。

中国信息通信研究院

地址：北京市海淀区花园北路52号

邮政编码：100191

联系电话：010-62300261

传真：010-62300264

网址：www.caict.ac.cn