数字产业：
2019年度网络安全威胁情报分析

联合出品

中国信息通信研究院安全研究所
腾讯科技（深圳）有限公司

CAICT 中国信通院 | 腾讯安全

版权声明

目录

前言

2020 年 3 月 4 日，中共中央政治局常务委员会召开会议，强调要加快 5G 基建、特高压、城际高速铁路和城市轨道交通、新能源汽车充电桩、大数据中心、人工智能、工业互联网等“新型基础设施建设”的建设进度。新型基础设施建设，是我国立足当前、着眼未来的重大战略部署，对构建数字经济时代的关键基础设施、支撑经济社会数字化转型具有重大意义。

在新基建的七大领域中，工业互联网、大数据、人工智能（以及 5G 网络的应用）可以称之为“数字新基建”，重点是通过数字技术的投入、积累与发展，激发传统行业通过数字化改造升级实现价值的跃升。“新基建”的提出，打破了传统的产业边界，加速了产业间的融合创新，为众多企业提供了数字化转型抢先加速、弯道超车的窗口期。但是，“新基建”在助力产业新秩序重新建立的同时，也将面临网络安全带来的新挑战。网络安全将成为提升企业数字化转型核心竞争力的关键因素。为充分应对数字化转型过程中面临的网络安全威胁，数字化转型企业需要从战略角度切入，改变过去被动防御的传统思维，做好主动规划和安全管理，从“情报—攻防—管理—规划”四个维度构建企业安全免疫系统。

而威胁情报作为企业网络安全防护能力的重要差异化因素之一，对企业优化风险应对策略，强化应急处置能力，完善企业纵深防御体系、提升企业整体安全防御能力，助推企业数字化转型具有重要意义。为提升数字化转型企业的网络安全意识，鼓励企业充分利用威胁情报应对层出不穷的网络安全风险，督促数字化转型企业履行网络安全主体责任，中国信息通信研究院安全研究所产业互联网安全实验室联合腾讯安全威胁情报中心从网络安全、终端安

全、云安全等维度对 2019 年的威胁情报现状进行监测汇总，同时对重点网络安全威胁事件进行复盘说明，详细分析威胁成因并给出了针对性的对策建议，供相关机构人员参考。

一、2019 年威胁情报态势总览

就 2019 年全年网络安全态势而言，网络安全事件数量仍然呈现上升趋势。DDoS 攻击凭借其极低的技术门槛和成本位居网络攻击之首，大量 DDoS 黑产通过恶意流量挤占网络带宽，扰乱正常运营，尤其给企业服务（如通信服务、常用软件工具等）、游戏、电商等领域带来了不小困扰。

其次，2019 年度针对企业终端的攻击依然未有放缓。一方面，攻击者通过漏洞利用、爆破攻击、社工钓鱼等主流攻击方式攻陷企业服务器，进而通过内网横向渗透进一步攻陷更多办公机器。另一方面，企业员工的不良上网习惯也同样会给企业带来一定的威胁，包括使用盗版系统、破解补丁、游戏外挂等。值得注意的是，近年来针对 Linux 平台的攻击活动也呈现逐渐上升趋势，企业安全运营者需引起关注。

此外，针对云平台传统网络架构的入侵、病毒等安全问题也逐渐呈常态化趋势，针对云平台架构的虚拟机逃逸、资源滥用、横向穿透等新的安全问题层出不穷。而且由于云服务具有成本低、便捷性高、扩展性好的特点，利用云平台提供服务或资源去攻击其他目标也成为一种新的安全问题。

除了上述提到的网络安全威胁，勒索病毒、挖矿木马已成为近年主流的 PC 端恶意软件，并形成了完整的产业链。通过垃圾邮件、钓鱼邮件实现勒索病毒、挖矿木马定向传播，利用 Office 高危漏洞构造攻击文件、在 Office 文档中嵌入恶意攻击宏代码、结合社会工程欺骗等手法成为常用技巧。

暗流涌动的网络黑产、重新崛起的 DDoS 攻击、层出不穷的各类木马、趋于常态的病毒勒索，影响深远的数据泄露都为企业的数字化转型带来了巨大的挑战。频发的网络安全事

件，加重了企业在数字化转型过程中关于网络安全的思考。

二、企业面临的网络安全威胁现状

2.1 网络安全威胁

根据 2019 年威胁情报监测数据显示，在网络攻击方面，主要的网络侧攻击为 DDoS 攻击和 BGP 劫持。

2.1.1 DDoS 攻击

在信息技术高速革新的背景下，网络空间面临的安全威胁不断升级，越来越多的服务器、个人电脑以及 IoT 设备沦为黑客的攻击目标。在企业面临的网络安全威胁中，DDoS 攻击凭借其技术门槛低、攻击速度快等特点，成为了大量黑产的“核武器”，通过恶意流量挤占网络资源，扰乱正常运营，给企业发展带来极大威胁。

DDoS 攻击的历史由来已久，同时在云生态环境下愈演愈烈。一方面，随着云计算和物联网技术的发展，越来越多的可利用设备暴露在公共网络中；另一方面，某些国外用户甚至以个人名义申请成为通信服务运营商，以此来获取更多的带宽资源以及自行配置路由器选项的权限。这都导致攻击者对 DDoS 资源的获取变得更加容易。同时，随着云服务提供商对网络外部资源的使用增加，DDoS 攻击对云服务提供商网络级别上的威胁也同步增强。

在攻击目标方面，根据 2019 年威胁情报监测数据显示，约三分之二的 DDoS 攻击事件以云平台上的 IP 作为攻击目标，云平台已成为 DDoS 攻击事件发生的重灾区；超过四分之一的目标 IP 是专门的 IDC 机房 IP 或高防机房 IP，针对个人或单独组织的相对较少。

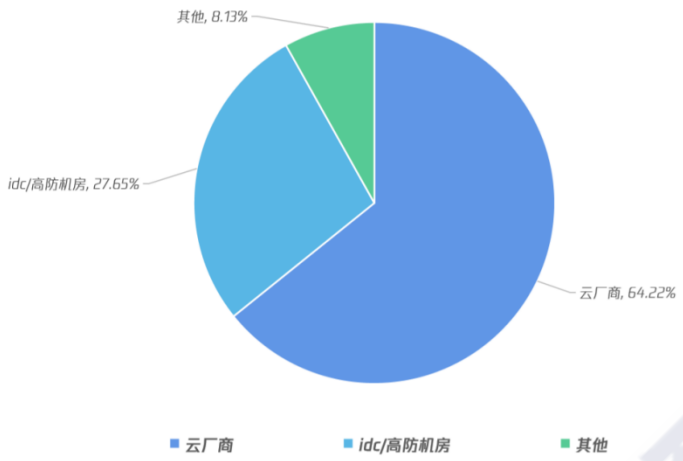

图 1 DDoS 攻击目标分布

当前 DDoS 的攻击趋势整体呈现攻击目标所属行业分布广泛、超大流量规模性攻击次数上升、整体攻击次数降低、目标攻击越发精准等趋势。在攻击目标所属行业分布方面，DDoS 对包含互联网、游戏、电商、金融等多个行业都造成了极大的威胁，其中遭受 DDoS 攻击最多的行业分别是行业工具、游戏、电商。

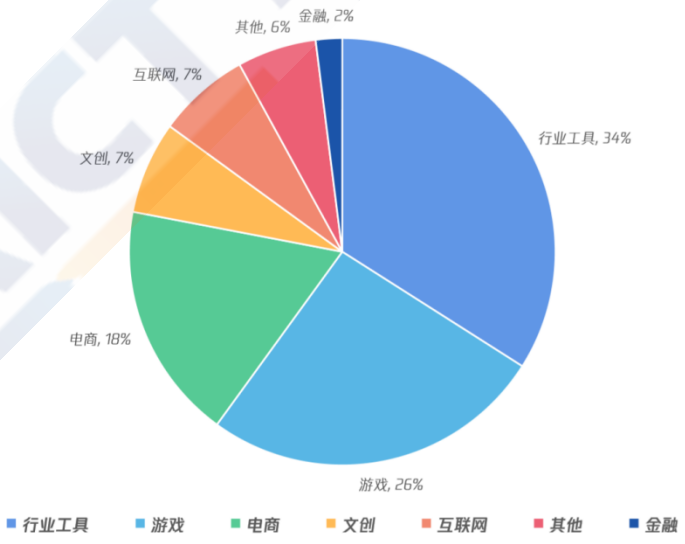

图 2 DDoS 攻击行业分布情况

从全年的攻击流量分布情况上看，98.8%以上的攻击流量为小于 100G 的流量，99.6%以上的攻击为小于 200G 流量。2019 年度 300-400G 梯度的大流量攻击与往年相比基本持

平，而大于 400G 的超大型流量攻击的次数明显超过往年。

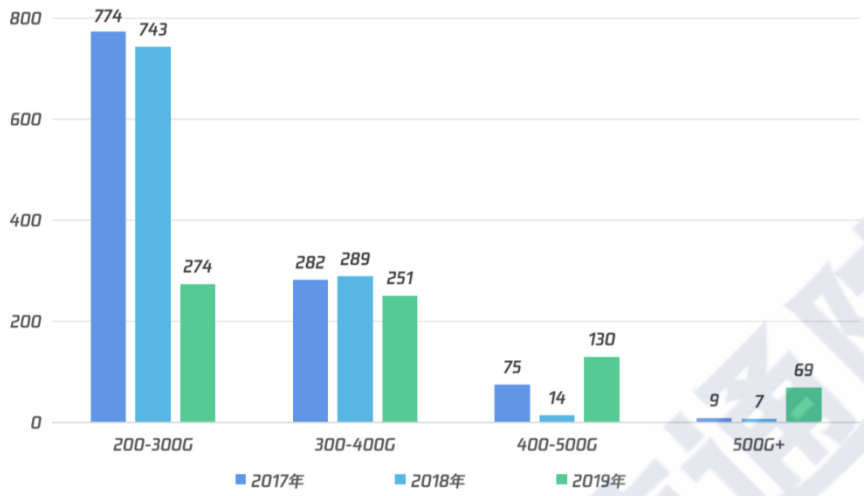

图 3 DDoS 攻击流量分布

结合数据分析发现，虽然基于超大流量的规模性攻击次数有所上升，但全年对云平台的流量攻击总次数有所减少。目前的 DDoS 攻击呈现出高度集成管理的态势，攻击者通过不断优化手段，试图以最小的攻击成本达到最优的攻击效果。从结果来看，攻击者的尝试也确实取得了一定效果，全年总体的攻击次数虽有所回落，但攻击成效大大提升。据此可推断，随着云平台的广泛使用，攻击者对云服务平台防御手段和防御策略的研究投入了大量的精力。为实现以最小攻击成本达到最佳效果，通过对 DDoS 攻击策略实现个性化定制提升攻击精准化水平将是今后 DDoS 攻击的一大趋势。

2.1.2 BGP 劫持

BGP 劫持即伪造网络层可达性信息，云服务提供商为了实现快速网络查找目标，使得路由尽可能高效查找到目标 IP 并进行通信，会使用 BGP 协议，即边界网关协议。在 BGP 劫持的情况下，某个独立运营的网络或自治系统（AS）公告实际上不属于其控制的自治系统地址空间，而此公告未被过滤，传播到正常的 BGP 路由表中，从而引发全球性的路由查找错误。这种错误通常是由于配置错误而发生的，但一旦发生有很大可能影响云资源的可用

性。

2.2 终端安全威胁

2019 年威胁情报监测数据显示,2019 年针对企业网络终端的攻击依然未有放缓。企业的终端安全威胁主要来源于三方面，一是攻击者通过漏洞利用、爆破攻击、社工钓鱼等方式攻陷企业服务器，通过内网横向渗透进一步攻陷更多办公机器；二是企业员工不良的上网习惯也给企业带来了巨大的安全威胁，比如使用盗版系统、破解补丁、游戏外挂等；三是针对 Linux 平台的攻击活动逐渐增加。

2.2.1 终端安全性

根据 2019 年威胁情报监测数据显示，在平均每周都拦截到病毒木马的终端中，约 12%的机器为企业终端。全年内拦截过病毒木马攻击的企业终端中，40%的机器平均每周拦截至少一次病毒木马攻击。在企业终端染毒类型分布方面，占比前两位的分别是风险类软件和后门远控类木马，占比分别为 44%和 21%。

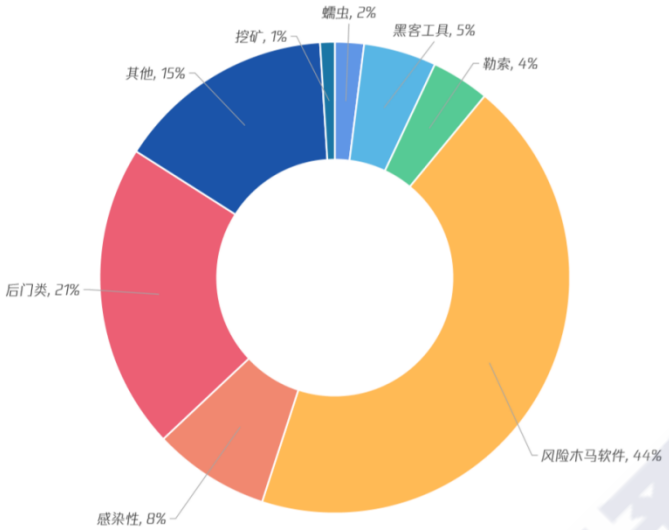

图 4 企业终端染毒类型分布

从各行业的感染病毒类型分布情况来看，风险木马类软件在各行业的染毒事件中占比最高，均在 40%以上。风险木马软件感染主要是由不良的上网习惯及缺乏安全意识引起，如使用盗版软件或外挂工具等。因此，相较于政府、金融、医疗和教育行业，科技行业感染风险木马软件的比例更小。后门远控类木马是除了风险软件之外感染量最大的染毒类型，占比在 20%左右。后门远控类木马有着极高的隐蔽性，可接受远程指令执行信息窃取、截屏、文件上传等操作，造成信息泄露等严重后果。

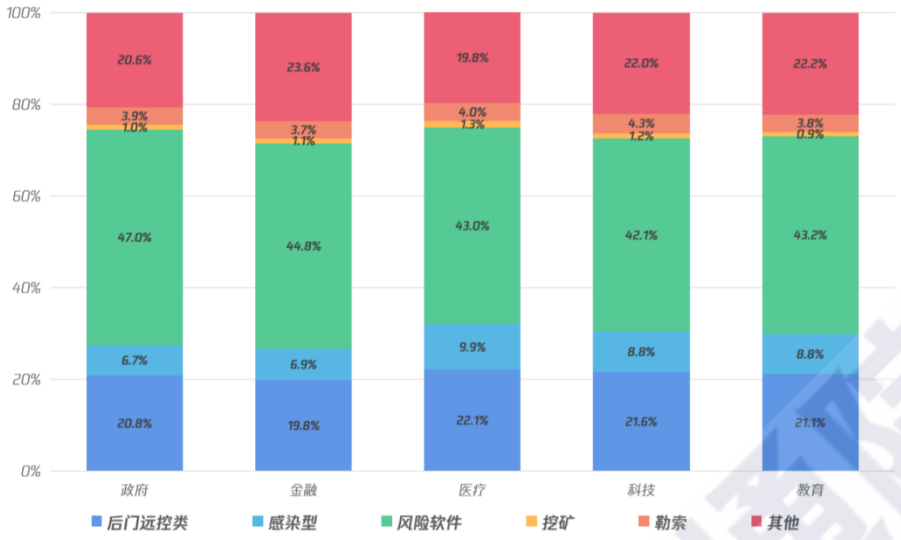

图 5 不同行业感染病毒的类型分布

2.2.2 终端脆弱性

当前，数量庞大且安全性薄弱的智能终端设备已然成为攻击者的新目标。漏洞利用及端口爆破是攻陷终端设备的重要手段，攻击者通过漏洞利用或爆破攻击公网环境下的服务器，随后进行内网横向渗透。

从企业终端漏洞修复角度来看，根据 2019 年威胁情报监测数据显示，截至 2019 年 12 月底，有 79%的企业终端上至少存在一个未修复的高危漏洞。在主要的高危漏洞中，LNK 漏洞（CVE-2017-8464）补丁安装比例最高，RTF 漏洞（CVE-2017-0199）补丁安装比例最低，仍有 74%的机器未安装该补丁。而 RTF 漏洞文档常被攻击者通过邮件钓鱼的方式利用，进而发起 APT 攻击，一旦机器失陷将会给企业造成极大的损失。

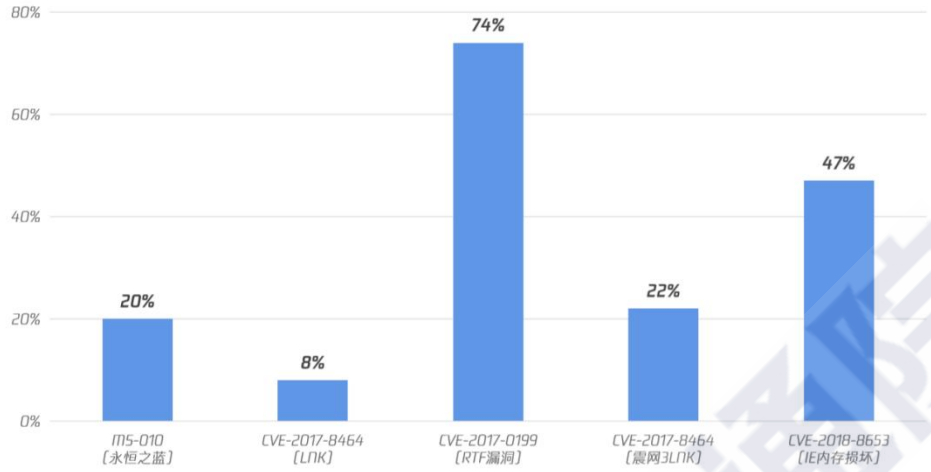

图 6 指定漏洞修复情况

从常见服务器漏洞攻击类型来看，如果企业、政府开放的服务器存在高危漏洞，可能导致灾难性的后果，其实许多黑客攻击和恶意软件入侵是可以预防的。通过对暴露在公网的服务器做抽样分析发现，常见的攻击类型中，远程代码执行（RCE）、SQL 注入、XSS 攻击类型比例较高，探测性扫描（Probe Scan）发生的频率也较高。

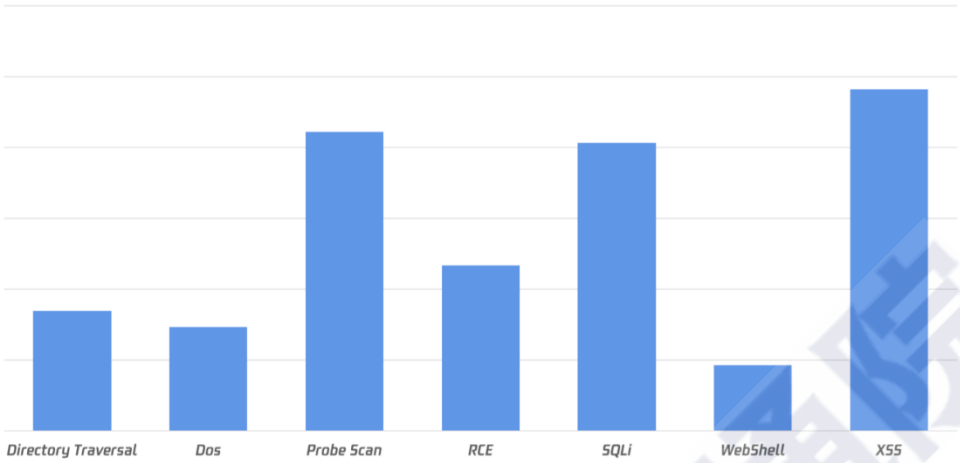

图 7 常见攻击类型

从高危端口开放情况来看，我们将黑客攻击频次较高且较为常见的端口（如 21、22、53 等端口）定义为高危端口，并对 Web 服务器等互联网空间资产做抽样空间测绘，发现有大量网络资产开放了高危端口，存在较高的安全隐患。除了 22、1900 等端口之外，还有较大比例的邮件服务、数据库服务等端口暴露在公共互联网上。

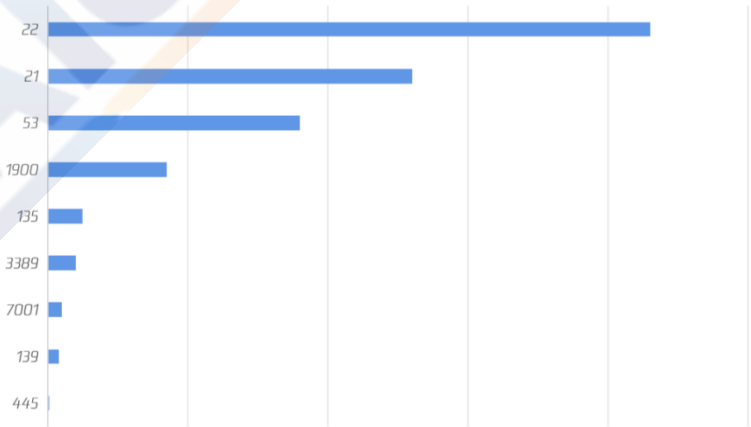

图 8 常见高危端口开放情况

2.2.3 终端失陷后的横向扩散

迄今为止，绝大多数企业都还是通过部署防火墙进行内外网隔离构建安全体系。企业内网被认为是可信区间，为了便于日常工作的开展，通常不会严格限制员工对内网资源的访问。因此，当病毒突破外围防火墙进入内网环境之后，将会在内网肆意扩散。病毒为了让其自身恶意行为实现效益最大化，首先会通过开机启动实现用户系统常驻，进而尝试内网横向传播。常见的攻击形式主要包括漏洞利用传播、弱口令爆破以及文件共享传播等。

- 常见攻击形式

(1) 漏洞利用传播

从针对系统组件的漏洞攻击情况来看，2019 年发生频率最高的内网病毒传播事件仍然是利用内网 SMB 共享服务漏洞进行传播的“永恒之蓝”木马下载器，该木马通过多种方式在企业内网攻击传播，以组建僵尸网络挖矿为主要目的。有多个企业因未及时修补“永恒之蓝漏洞”而被反复攻陷。

(2) 弱口令爆破攻击

弱密码爆破攻击在入侵内网以及作为横向扩散的手段上效果显著。对部分已检测的服务器做抽样分析发现，弱密码爆破攻击集中发生在凌晨 12 点到 6 点之间的非工作时段。实际上，黑客成功入侵局域网之后对内网的爆破攻击，使用的协议与外网有较大不同，SMB 攻击最为常见，其次是远程桌面连接爆破和 SSH 爆破。

(3) 文件共享传播

根据企业的应急处置经验发现，文件共享目录、可移动介质是蠕虫病毒、感染型病毒、

Office 文档病毒在内网的感染重灾区。这三类病毒一般都以窃取敏感信息为主要目的。

➢ 企业终端失陷的后果

(1) 敲诈勒索

勒索病毒通过恐吓、绑架用户文件或破坏用户计算机等方式，向用户勒索数字货币。通过加密用户系统内的重要资料文档，再结合虚拟货币交易实施犯罪依然为当前勒索病毒使用的最主要勒索形式。

(2) 挖矿木马

根据监测数据发现，2019 年 3 月份挖矿木马感染处于峰值，随后逐步下降，感染量基本稳定持平。感染了挖矿木马的机器会被消耗掉大量的系统资源，造成系统卡慢，此外还存在信息窃取、植入后门等潜在风险。

(3) 信息窃密

信息窃密类木马其主要目的是获取机器上的机密敏感信息，科研机构、高校、高科技企业及政府机关等最易受到这类木马攻击，窃取的信息包括失陷机器相关信息（MAC 及 IP 地址、操作系统版本等），个人或企业信息（如企业员工联系方式，企业邮箱等），重要机密文件等。

(4) 肉鸡后门

攻击者攻陷一台主机获得其控制权后，往往会在主机上植入后门，安装木马程序，以便下一次入侵时使用。后门木马会长期驻留在受害机器上，接受远控指令执行定期更新、远程下载执行、键盘监控、文件窃取上传等功能。此外，随着 IoT 物联网设备的增加，针对 IoT

设备的攻击也越来越频繁，攻击成功后通过植入后门、组建僵尸网络、开展挖矿、DDoS攻击等进行获利。

(5) 刷量推广

刷量推广类病毒木马主要是通过下载器、盗版 ghost 系统、流氓软件推装、游戏外挂等传播，还会通过搜索引擎竞价排名推广以获得更大的受众面。为了诱导用户下载，此类病毒木马往往会伪装成知名的第三方软件，如 flashplayer、photoshop 等。其获利渠道主要是主页锁定、软件推装、暗刷流量、广告弹窗等。

2.3 云安全威胁

随着云计算解决方案优势逐渐显现，越来越多的企业机构选择将其业务上云，为云计算服务提供商提供了更为广阔的市场。但与此同时，由于云技术本身共享的特性，内部各层次有相互关联，暴露在公共互联网的资产、服务、接口更多，影响的用户也更多，“云”的安全问题被提升到至关重要的位置。

2.3.1 云安全威胁全景

在云平台上，除了 DDoS、入侵、病毒等传统安全问题，针对云平台架构的虚拟机逃逸、资源滥用、横向穿透等新安全问题也层出不穷。此外，由于云服务具有成本低、便捷性高、扩展性好的特点，利用云提供的服务或资源去攻击其他目标的也成为一种新的安全问题。

根据 2019 年威胁情报监测数据显示，云资源作为攻击源的比例在所有国内攻击源中已接近一半。在云计算生态环境下，暴露给攻击者的信息表面看与传统架构中基本一致，但是由于云生态环境下虚拟化技术、共享资源、复杂的架构以及逻辑层次的增加，导致可利用的攻击面增加，攻击者可使用的攻击路径和复杂度也大大增加。

恶意攻击者从互联网环境下攻击云租户和平台（包括云平台的底层资源、管理软件、管

理界面、服务器集群等）的攻击路径包括如下几类：

- 裸金属服务器管理接口：潜在攻击者利用裸金属服务开放的 IPMI 等管理接口存在的漏洞和缺陷，控制服务器底层硬件，并进一步利用带外管理网络横向扩展，作为跳板访问云管理和控制平台的内部接口，尝试对平台和其他租户发起攻击；
- 租户虚拟机逃逸：潜在攻击者通过租户应用的数据库、Web 等应用程序漏洞，进入云服务使用者（IaaS 平台的租户所拥有的虚拟机实例）的操作系统，并进一步通过潜在的虚拟化逃逸漏洞进入云资源底层的 Hypervisor，进而控制云平台底层资源并进行横向扩展；
- 独立租户 VPC 实例模式的容器和微服务网络攻击：潜在攻击者通过微服务管理系统的脆弱性或容器安全漏洞，进入云服务提供商所使用的虚拟机实例操作系统，随后进一步通过潜在的虚拟化逃逸漏洞进入云资源底层的 Hypervisor，进而控制云平台底层资源并进行横向扩展；
- 共享集群模式容器和微服务网络攻击：潜在攻击者通过容器逃逸或微服务组件漏洞，直接控制物理服务器执行恶意操作或进行横向扩展；
- SaaS 服务共享集群模式攻击：潜在攻击者通过云服务提供商所提供的 SaaS 类服务能够使用的 API、中间件、数据库等漏洞，直接逃逸或越权访问进入提供服务的底层服务器集群，执行恶意操作，窃取数据或进行横向扩展；
- 恶意攻击者针对云服务平台业务互联网络的旁路攻击：恶意攻击者通过对于云平台业务连接的相关企业内部网络进行 APT 攻击，并进一步迂回横向扩展返回攻击云平台业务、运维或管理网络；
- 恶意攻击者针对云服务平台开发/运营网络的旁路攻击：恶意攻击者通过对于云平台连接的运维或管理内部网络进行 APT 攻击，并进一步迂回横向扩展返回攻击云平台业

务、运维或管理网络；

- 针对云用户控制台界面或开放式 API 的攻击：潜在攻击者通过云服务提供商提供的控制台或开放式 API，利用控制台应用漏洞或 API 漏洞访问，对租户资源或平台进行攻击。

此外，在攻击路径图中还存在一系列横向扩展路径。横向扩展指当攻击者成功获取到租户或平台系统的一定权限后，利用网络或共享资源进行横向迁移，进一步扩大攻击范围，获取其他租户和系统的资源、数据或访问权限的情况，具体路径包括：

- 利用租户资源和访问权限，在 VPC 内进行横向迁移攻击，或作为跳板攻击其他用户；
- 利用微服务不同功能组件间共享资源或权限的横向迁移；
- 利用共享数据库集群间的资源或数据进行横向迁移；
- 当成功实现虚拟机逃逸后，利用 Hypervisor 和硬件层面的控制面网络和接口进行横向迁移；
- 利用网络虚拟化的共享资源、威胁接触面和控制面网络进行横向迁移；
- 利用存储虚拟化的共享资源、威胁接触面和控制面网络进行横向迁移；
- 利用云平台管理面/控制面和业务面间的接口进行横向迁移；
- BMC 等固件破坏后获取进行物理机层面的潜伏，或利用底层硬件权限反向获取 Hypervisor OS 或租户虚拟机 OS 的数据和系统访问权限。

2.3.2 基础攻击面

➢ 云主机安全

云主机是云服务提供商为客户提供的海量虚拟化服务器，企业可根据实际业务需求在云主机实现资源的灵活配置。企业租用的云主机与企业自有终端在管理维护上具有一定的

相似性，因此云主机同样会面临传统终端可能遭遇的威胁。

为了在黑客入侵前发现系统风险点，安全管理人员通常通过专业的风险评估工具，对网络风险进行检测、移除和控制，以此来减小攻击面。

(1) 风险来源

常见的云主机安全风险主要源自安全补丁、漏洞、弱密码、应用风险、账号风险等。

- 云主机高危端口开放

在对 Web 服务器等互联网空间资产做空间测绘后发现，有大量的资产开放了高危端口，存在较高的安全隐患。除了 22、1900 等端口之外，还有较大比重的邮件服务、数据库服务等端口暴露在公网上。

- 云主机软件弱密码

不同服务都具有各自服务特色的弱口令，比如 MySQL 数据库的默认密码为空。通过分析发现，主机软件弱密码主要集中在 MySQL、SSH、SVN、Redis、vsftpd 这五类应用上，其中 MySQL 和 SSH 超过云主机弱密码风险总数的 30%。

- 高风险主机账号普遍存在

主机系统账号普遍存在各类风险，尤其是那些拥有 Root 权限的高风险账号，更需要实时进行监控。根据风险账号检测结果，删除主机中无用的账号，按照权限最小化原则限制主机中可疑账号的权限。通过对主机账号分析发现，超过 95%的账号都属于高危账号，这些高危账号通常都存在不合规的配置问题。

- 中高危漏洞修复不及时

各种软件的漏洞修复不及时已经成为大规模网络与信息安全事件、重大信息泄露事件发生的主要原因之一。从漏洞等级上来说，漏洞可分为高危、中危、低危三大类。根据样本数据分析发现，未修复的漏洞大部分是高危或者中危的，其中未修复的高危漏洞比例更是高达45.77%。在 2019 年基于漏洞所影响的主机数量排名 TOP10 漏洞数据中，这些漏洞均已在 2016 年至 2018 年爆出，漏洞的不及时修复为企业带来了严重的安全威胁。

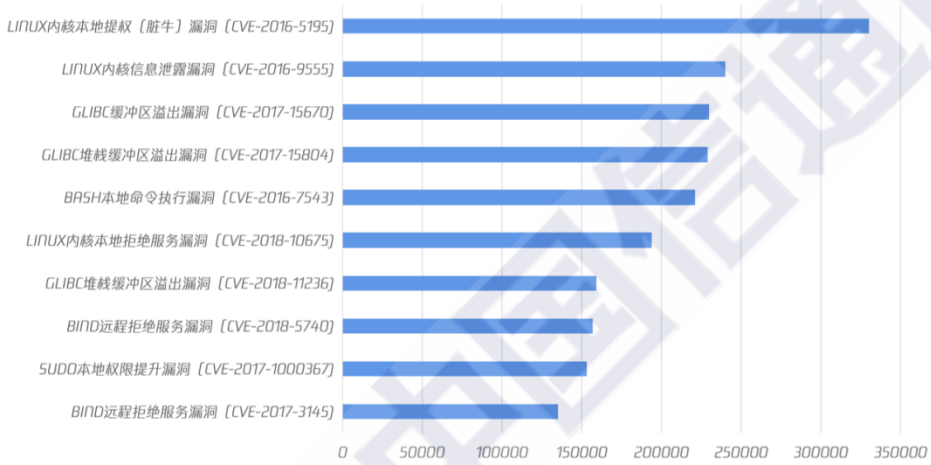

图 9 2019 年影响主机 TOP10 的漏洞

(2) 入侵分析

通过对暴露在公网的服务器做抽样分析发现，在常见的攻击类型中，远程代码执行（RCE）、SQL 注入、XSS 攻击类型比例较高，同时黑客为了获取服务器、网站的基本信息，常见的探测性扫描(Probe Scan)量同样非常高。

- 全国主机感染病毒木马的情况

2019 年，全国企业用户服务器病毒木马感染事件超百万起。其中，Webshell 恶意程序感染事件近 80 万起，占 73.27%；Windows 恶意程序感染事件占 18.05%；Linux 恶意

程序感染事件占 8.68。可见 Webshell 是攻击者针对服务器攻击的重要手段。

从感染主机中共发现超 1 万种木马病毒，其中 Webshel 木马病毒 l 约占 27%，Windows 木马病毒约占 61%，Linux 木马病毒约占 12%。Webshell 是一类专门针对服务器攻击的恶意程序，随着云服务器的大量增长，Webshell 的种类也在快速增加。值得注意的是，Linux 平台的木马病毒也随着云时代的到来而快速增长。

单从感染 Webshell 的服务器操作系统看，约 44%的 Windows 服务器曾经感染过 Webshell，而 Linux 服务器感染过 Webshell 的仅 0.2%。从感染的 Webshell 语言类型来看，PHP 类型的 Webshell 最多，其次是 ASP 语言。

- 暴力破解目标

攻击者利用软件对那些暴露在公网上的 RDP、SSH、Telnet、FTP 等服务进行扫描，然后进行暴力破解，进而以存在弱口令的主机为基本立足点，借此攻陷整个系统。互联网中存在大量的扫描系统会对云主机是否存在弱密码进行扫描。据有关报告显示，端口暴露的单个 Linux 系统，平均遭受超过 40000 次/天的网络攻击，攻击频率约 5 次/秒。存在弱口令的 Linux 系统，每月约有 17000 次被入侵成功。

- 云上挖矿

根据不同操作系统样本数据进行分析，总共发现超过 3000 台 Windows 服务器感染了挖矿木马，超 2000 台 Linux 服务器感染了挖矿木马。通过对被感染的主机进行分析，发现挖矿木马主要挖比特币与门罗币。Windows 平台挖矿事件主要发生在夜晚 23 点以及 3 点到 8 点之间，Linux 平台挖矿事件主要发生在凌晨 2 点到 6 点之间。

(3) 合规分析

所有企事业单位的网络安全建设都需要满足国家或监管单位的安全标准，如等保 2.0、CIS 安全标准等，网络安全管理的合规化建设是企事业单位需首要履行的义务。

- 主机账号的合规分析

在样本分析过程中，我们发现很多账号存在不合规情况，例如未设置密码尝试次数锁定、未设置密码复杂度限制等，这不符合国家等级保护相关要求。

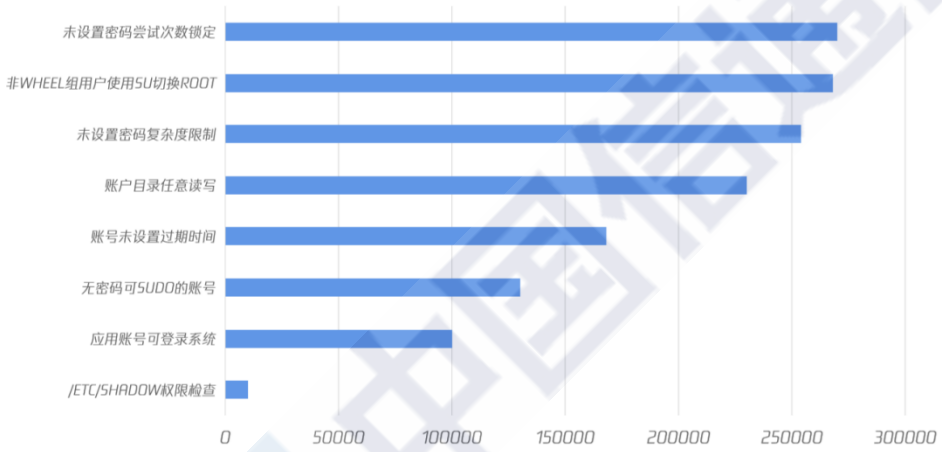

图 10 主机账号的不合规情况

- 主机系统配置合规分析

缺乏对主机底层的操作系统的适当配置，可能引发许多安全问题。通过研究分析样本数据，发现 GRUB 密码设置、UMASK 值异常、未开启 SYN COOKIE 这三类问题是所有主机系统风险中所占比例最多的三类。

- 主机应用合规分析

主机服务器承载了非常多的应用，如果应用中存在不合规的情况，例如配置错误、安全

漏洞未及时修复等。黑客就可能通过主机中的非合规应用进入主机系统内部，进而产生安全风险。

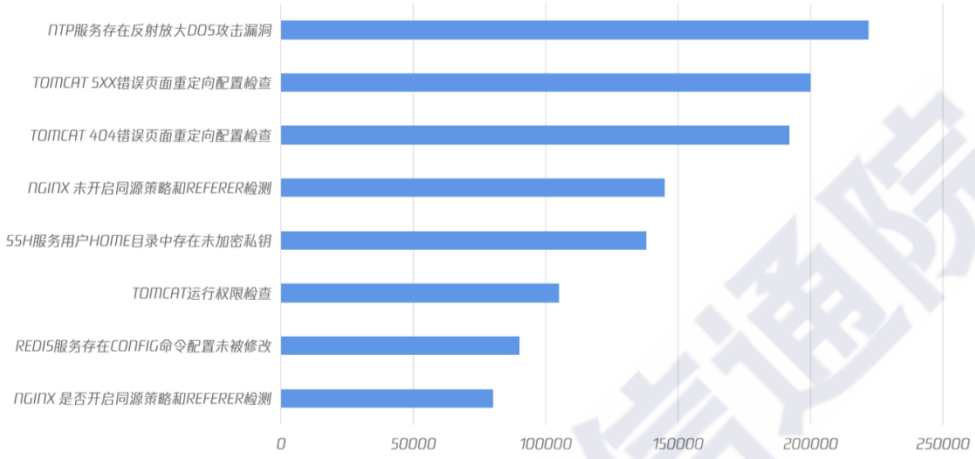

图 11 常见应用的配置风险

➢ 云上数据安全

对于任何企业而言，数据都是最宝贵的资产，尤其是业务数据和用户数据，更是关乎其企业存亡的关键信息，企业上云后的数据安全一直是在云存储数据的主要问题之一。随着越来越多的企业将业务迁移到云上，部分敏感数据也将存储在云上，数据安全已经成为所有企业在产业互联网时代必须直面的挑战。

(1) 数据泄露

云服务使用方可以在数据库使用之初进行完善的配置和良好的身份验证访问和管理机制，使用云服务提供商提供的多重身份认证以及密钥管理服务进行数据库访问的相关操作，对流程中的数据使用加密传输和加密存储；同时加强内部员工的安全意识培训，防止在内部出现数据泄露。

(2) 数据丢失

数据丢失的可能原因包括：文件意外删除、恶意软件（勒索软件）、硬盘故障、电源故障、账号劫持/入侵等情况。

三、重点网络安全威胁说明

根据 2019 年威胁情报监测数据显示，2019 年勒索病毒主要呈现出传统勒索家族转向精准化、勒索病毒定制个性化、勒索病毒与僵尸网络融合化、中文定制化等趋势。

表 1 勒索病毒演进趋势

勒索病毒演进趋势	具体特征
传统勒索家族转向精准化	老牌勒索家族已经从广撒网、无差别模式的攻击，转变为精准化、高质量的行动，该转变使攻击者每次攻击行动后的收益转化过程更有效。当企业服务器被攻陷，攻击者会将该机器作为跳板机，继续尝试攻击其它局域网内的重要资产，在部分勒索感染现场我们也看到攻击者留下的大量相关对抗、扫描工具，个别失陷环境中攻击者使用的密码抓取工具就有数十款之多。
勒索病毒定制个性化	2019 年，勒索病毒团伙开始偏向于赎金定制化，对不同目标要价各不相同，往往根据被加密数据的潜在价值定价（通常在 5 千-10 万人民币），勒索病毒运营者的这种手法大幅提高了单笔勒索收益。当企业有完善的数据备份方案，拒绝缴纳赎金时，勒索团伙则采取另一种手段——威胁泄露受害者的机密文件来勒索。
勒索病毒与僵尸网络融合化	僵尸网络是一种通过多重传播手段，将大量主机感染 bot 程序，从而在控制者和感染僵尸网络程序之间所形成的一对多控制的网络，僵尸网络拥有丰富的资源（肉鸡），勒索病毒团伙与其合作可迅速提升其勒索规模，进而直接有效增加勒索收益。
中文定制化	中国网民或企业已成为勒索病毒的重要目标，一部分勒索病毒运营者开始在勒索信、暗网服务页面提供中文语言界面。

3.1 勒索病毒攻击情况

从 2019 年的勒索病毒攻击事件来看，勒索病毒的主要攻击方式是通过加密用户系统内的重要资料文档、数据，来进行虚拟货币勒索。当加密数据勒索不成功时，再以泄露数据胁

迫企业进行盈利（Maze 和 Sodinokibi 已使用）。此外，使用群发勒索恐吓邮件，命中收件人隐私信息后，再利用收件人的恐慌心理，实施欺诈勒索的方式也较为流行。

2019 年国内遭受勒索病毒攻击最为严重的省市分别为广东、北京、江苏、上海、河北、山东，其它省份也遭受到不同程度攻击。从勒索病毒入侵行业方面看，传统企业、教育、政府机构遭受攻击最为严重，互联网、医疗、金融、能源紧随其后。而在勒索病毒攻击方式方面，以弱口令爆破为主，其次为通过海量的垃圾邮件传播以及借助僵尸网络传播。

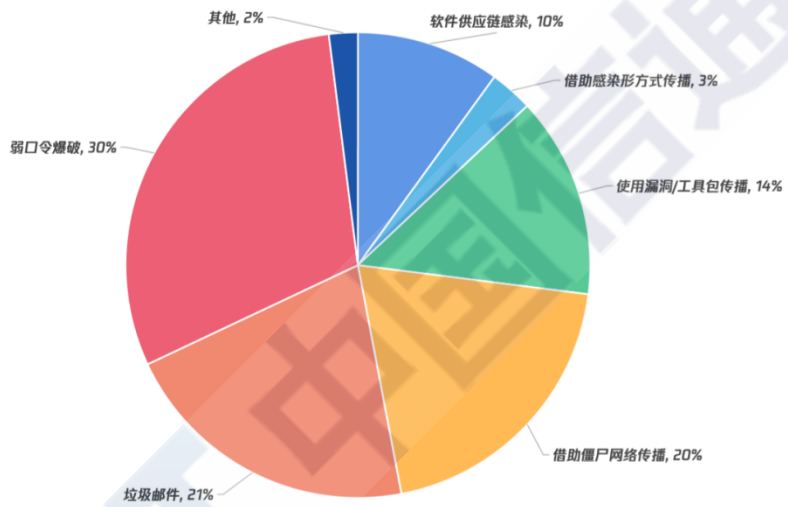

图 12 2019 年勒索病毒入侵方式占比

3.2 挖矿木马活动情况

黑客入侵控制大量计算机并植入矿机程序后，利用计算机的 CPU 或 GPU 资源完成大量运算，从而获得数字加密货币。同时，黑产在暗网进行非法数据或数字武器售卖时大部分采用比特币作为交易货币，数字加密货币成为黑灰产业的流通媒介，进而推动了挖矿产业的持续繁荣。从 2017 年爆发之后，挖矿木马逐渐成为网络世界主要的威胁之一。

2019 年威胁情报监测数据显示，2019 年挖矿木马攻击呈“上升—下降—保持平稳”

的趋势。2019 年上半年挖矿木马非常活跃，高峰时检出攻击样本超过 10 万个/日；5 月之后攻击趋势有所减缓，下降到了 6 万个/日。从地区分布情况上来看，2019 年挖矿木马在全国各地均有分布，其中感染最严重的省市分别为广东、浙江、北京以及江苏。受到挖矿木马影响最为严重的行业分别为互联网、制造业、科研和技术服务以及房地产业。

3.2.1 挖矿木马活跃家族

根据 2019 年威胁情报监测数据显示，2019 年挖矿木马最活跃的三个家族分别为 WannaMiner、MyKings、DTLMiner（永恒之蓝下载器木马）。其中 MyKings 是老牌的僵尸网络家族，而 WannaMiner 和 DTLMiner 分别在 2018 年初和年底出现。在 2019 年这几个家族都有超过 2 万用户的感染量，他们的共同特点为利用“永恒之蓝”漏洞进行蠕虫式传播，使用多种类的持久化攻击技术，难以被彻底清除。

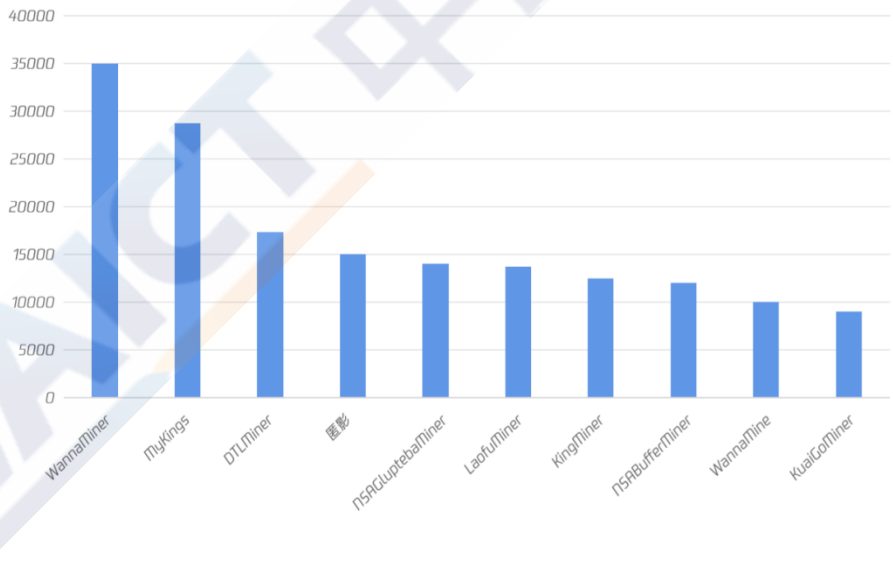

图 13 2019 年挖矿木马活跃 TOP 榜

3.2.2 主要入侵方式

2019 年排名前三的挖矿木马入侵方式分别是漏洞攻击、弱口令爆破和借助僵尸网络。

由于挖矿木马需要获取更多的计算资源，所以利用普遍存在的漏洞和弱口令，或者是控制大量机器的僵尸网络进行大规模传播成为挖矿木马的主要手段。

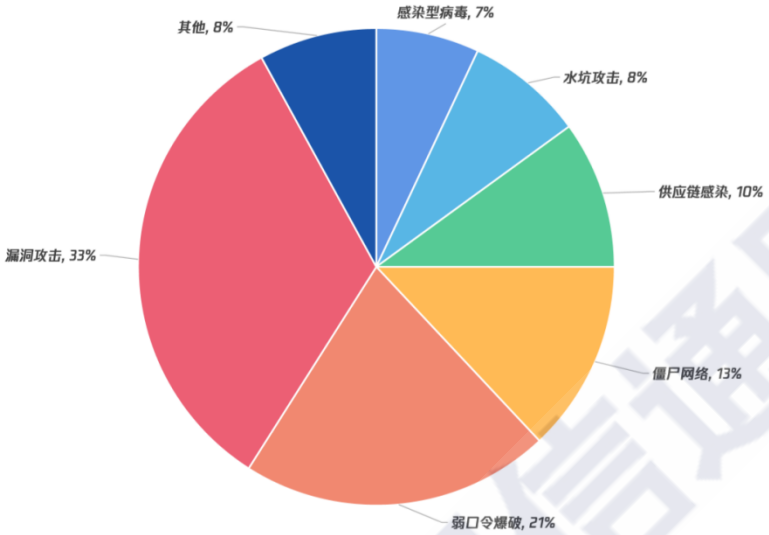

图 14 挖矿木马主要入侵方式

表 2 挖矿木马入侵方式

挖矿木马入侵方式	实施方法
漏洞攻击	利用的漏洞最主要类型为 Windows 系统漏洞（“永恒之蓝”），其次是 WebLogic 相关组件漏洞，Apache 相关组件漏洞。常用于攻击的包括以下 CVE 编号的漏洞：MS17-010“永恒之蓝”CVE-2017-0143；Weblogic 反序列化任意代码执行漏洞 CVE-2017-10271，CVE-2018-2628，CVE-2019-2725；Apache Struts2 远程代码执行漏洞 CVE-2017-5638；Apache Solr 远程代码执行漏洞 CVE-2019-0193；Apache Tomcat 远程代码执行漏洞 CVE-2017-12615。
弱口令爆破	挖矿木马主要的爆破攻击类型为 SQL 爆破(包括 MsSQL、MySQL)，其次是 IPC$和 SSH。由于部分 IT 管理人员缺乏安全意识，许多数据

	库和远程登录服务被设置为弱口令。SplashData 公布的 2019 排名前五位的最差密码分别是“123456”、“123456789”、“qwerty”、“password”和“1234567”，这些密码也是黑客在爆破攻击时的首选。挖矿木马通过内置的包含大量简单密码的字典进行自动匹配，很容易破解此类弱口令并入侵系统。

3.2.3 挖矿木马技术特点

(1) 供应链感染

2018 年底出现的 DTLMiner 是利用现有软件的升级功能进行木马分发，属于供应链感染的典型案例。黑客在后台配置文件中插入木马下载链接，导致软件在升级时下载木马文件。由于软件本身拥有巨大的用户量，导致木马在短时间内感染了大量的机器。

(2) 跨平台攻击和多种手段混合攻击

挖矿木马经历了从以控制普通电脑为主到以控制企业主机为主，从只控制 Windows 挖矿到混合感染多个平台的变化。我们监测发现了“Agwl”、“萝莉帮”、WannaMine、Satan 等多个针对 linux 的挖矿木马。黑产为了实现的利益最大化，还会将挖矿木马与勒索软件、远控后门、剪贴板大盗、DDoS 等木马打包进行混合攻击。

(3) 社交网络

根据监测，研究团队在 2019 年 12 月发现了通过社会工程骗术传播的“老虎”挖矿木马（LaofuMiner）。攻击者将远控木马程序伪装成“火爆新闻”、“色情内容”、“隐私资料”、“诈骗技巧”等文件名，通过社交网络发送到目标电脑，当受害者双击查看文件，会立刻被安装“大灰狼”远控木马。然后，攻击者通过远控木马控制中毒电脑下载挖矿木马，中毒电脑随即沦为矿工。

(4) VNC 爆破

2019 年 3 月，Phorpiex 僵尸网络针对被广泛使用的远程管理工具“VNC”默认端口 5900 进行爆破攻击，在高价值服务器上下载运行 GandCrab 5.2 勒索病毒，加密重要系统资料实施敲诈勒索；若攻破有数字货币交易的电脑，则运行数字货币钱包劫持木马抢钱；若被攻击的只是普通电脑，则植入门罗币挖矿木马，将之变成 Phorpiex 控制的矿工电脑。

(5) 恶意代码检测难度提升

- “无文件”攻击

2019 年 4 月 3 日，DTLMiner 在 Powershell 中反射加载 PE 映像，达到“无文件”形式执行挖矿程序。这种方法直接在 Powershell.exe 进程中运行恶意代码，注入“白进程”执行的方式可能造成难以检测和清除挖矿代码的后果。这也是被首次发现的大规模利用“无文件”形式执行的挖矿木马。

- DLL 侧加载

为逃避杀软检测，KingMiner 启动挖矿木马时采用 DLL 侧加载(DLL Side-Loading)技术，也就是“白+黑”技术，利用正常的有数字签名的白文件来调用恶意 DLL。其使用到的有微软系统文件“Credential Backup and Restore Wizard(凭据备份和还原向导)”和多个知名公司的数字签名的文件。

(6) 阻断其他木马入侵，独占挖矿资源

挖矿木马会修改设置禁止其他机器通过远程桌面服务访问本机，以此来阻止其他木马进入系统，从而达到独占挖矿资源的目的。

3.3 邮件安全威胁

本节我们将通过监测到的实际案例总结 2019 年恶意邮件的影响情况。

3.3.1 垃圾邮件

根据 2019 年威胁情报监测数据，每天有大量垃圾邮件通过掺杂成语释义、敏感词混淆等手段与各类邮箱反过滤机制的对抗。

3.3.2 恶意邮件

从恶意行为的角度来看，恶意邮件可以分为如下几种：诱导回复敏感信息、诱导打开钓鱼页面链接、诱导打开带毒附件。企业用户日常容易遇到后两种案例，典型代表如带恶意附件的鱼叉邮件。鱼叉邮件是一种针对特定人员或特定公司的员工进行定向传播攻击的恶意邮件。网络犯罪分子首先会精心收集目标对象的信息，使“诱饵”更具诱惑力。然后结合目标对象信息，制作相应主题的邮件和内容，骗取目标运行恶意附件。

如下图与“订单”相关的邮件，通过将带有精心构造的“CVE-2017-8570”漏洞利用代码的 word 文档伪装为附件“订单列表”，诱使用户打开文档以触发漏洞代码逻辑，最终实现投放“NetWiredRC”远控木马。在 2017 年爆发了 WannaCry（永恒之蓝）勒索病毒后，很多变形后的勒索软件通过空白主题的邮件进行广泛传播。

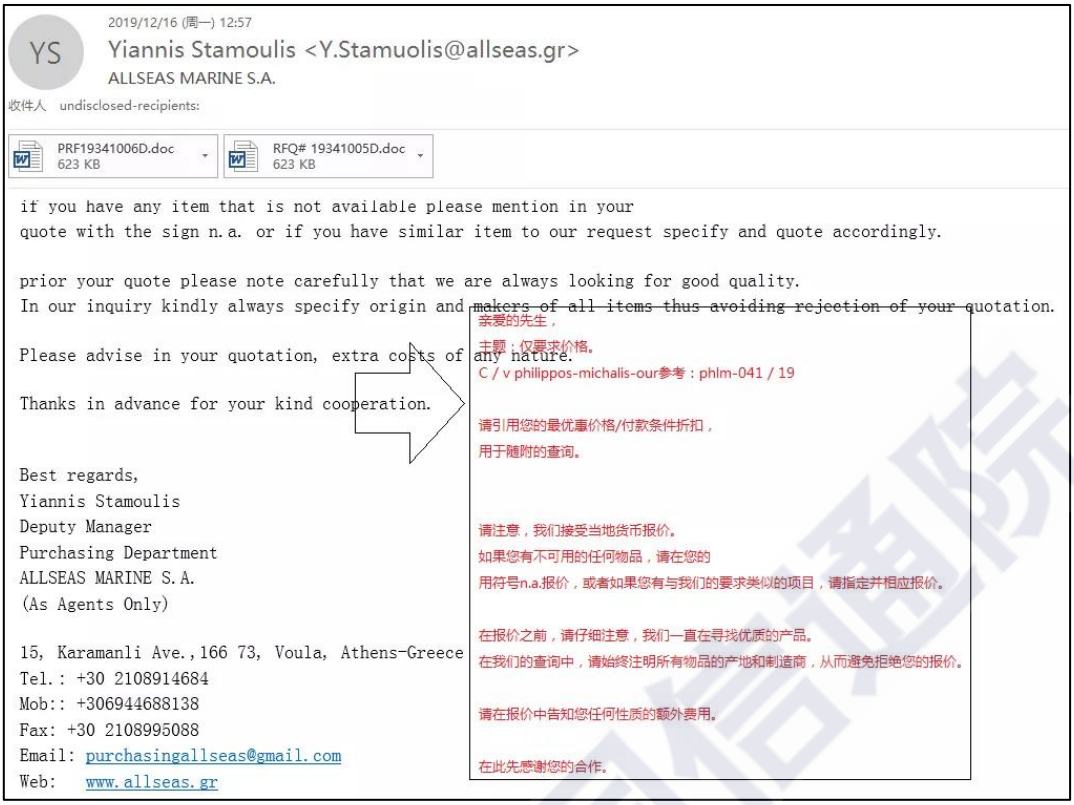

图 15 勒索病毒邮件内容

3.3.3 邮件安全案例

鱼叉邮件主要以投递“窃密”、“远控”、“勒索”木马为目的。近年来，为了快速变现，投递勒索病毒的趋势日益加剧。其中，最受攻击者青睐的是 Office 漏洞 CVE-2017-11882。利用 Office 软件的公式编辑器漏洞 CVE-2017-11882 实现隐秘远程下载的恶意邮件是十分常见的。由于邮件来源和内容被高度伪装，用户很容易放下防备心打开文档，进而释放病毒。虽然该漏洞的补丁早在 2017 年 11 月已被公布以供修复，但实际上 Office 安全漏洞的修复率比系统补丁修复率要低得多，导致该漏洞被广泛利用。

四、网络安全威胁成因分析

随着“新基建”的持续推进，企业的数字化转型步伐将逐步加快，未知的网络安全风险持续攀升，面临的网络安全形势日趋严峻。当前，企业在数字化转型过程中面临的网络安全问题主要包括安全意识淡薄、管理制度不健全、教育培训缺失、防护体系不完善等。加快提升企业网络安全防护水平，助推企业数字化转型迫在眉睫。

4.1 安全意识淡薄，重视程度不足

当攻击者无法通过传统技术手段对企业资产进行攻击时，由于企业员工的网络安全意识淡薄，使得人员管理上的漏洞成为攻击者的突破口。例如源代码不小心上传到了开源的网站、应用设置了简单的密码口令、个人密码企业密码共用、随意设置共享目录、防毒软件更新不及时等问题，降低了企业的网络安全防护水平。企业需充分认识到提高员工网络安全意识的重要性，对内部员工进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施，帮助企业内部员工成为企业数据安全的优秀屏障。

4.2 管理制度不健全，责任落实不到位

健全的网络安全管理制度是落实网络安全主体责任的重要前提。网络安全管理是一项系统化的工作，当前大部分企业均在管理制度规范建设、安全岗位人员配备、网络技术力量投入等方面做了大量基础工作，但整体还存在一些不容忽视的共性问题，如管理制度不健全，缺乏配套的考核和奖惩机制，网络安全责任人、安全管理人员职责分工不明确，未建立企业内部跨部门的网络安全联动机制，未制定企业网络安全应急处置预案等。这使得企业内部的网络安全管理工作无法做到有章可循，网络安全主体责任落实不到位，企业整体网络安全管

理水平不高。

4.3 教育培训缺失，实战能力不足

网络安全是企业实现数字化转型的重要保障和前提，而网络安全人才作为网络安全的根本，是提升企业数字化转型核心竞争力的关键。随着网络安全人才需求迅速增长，人才供应缺口巨大是各国各行业亟待解决的重要问题。当前企业网络安全人才主要来源是高等教育院校毕业生和非科班人员转化。高等教育院校毕业生存在着重理论、轻实践，与企业实际需求脱节等问题，短期内无法满足企业实际的网络安全人才需求。而职业教育培训周期短、针对性强是提升网络安全从业人员专业技能的理想方式。但是目前大多企业都未对网络安全从业人员和准从业人员开展专业培训，导致网络安全从业人员的实战能力不强，企业的网络安全防护能力出现“木桶效应”。

4.4 防护体系不完善，威胁应对不足

为充分应对企业数字化转型过程中层出不穷的网络安全威胁，做好企业的网络安全防护部署，需充分发挥先进网络安全技术优势，利用专业网络安全解决方案，为企业的数字化转型保驾护航。但是，通过上述的分析可见，当前仍有部分企业的网络安全防护体系并不完善，仍然存在网络安全产品和技术支撑不足，专业技术解决方案的缺失；安全操作配置不当；安全漏洞未及时修复等问题，无法建立从“专业设备安全配置—边界安全防护—网络安全态势感知”的闭环管控，成为企业实现业务数字化、智能化升级的关键风险点。

五、建议举措

5.1 强化网络安全意识，筑牢网络安全防线

安全意识是落实网络安全主体责任的基本保障。没有网络安全就没有国家安全，维护网络安全是全社会共同的责任。党的十八大以来，以习近平同志为核心的党中央高度重视网络安全和信息化工作，高瞻远瞩、高屋建瓴、把握大势，将马克思主义基本原理与我国互联网发展治理实践相结合，形成了具有鲜明时代特色的网络强国战略思想。在习近平总书记网络强国战略思想的指引下，我国相继出台《中华人民共和国国家安全法》《中华人民共和国反恐怖主义法》《中华人民共和国网络安全法》《中华人民共和国密码法》等法律法规。随着网络安全法律的不断完善，全面规范网络空间安全管理已迈入法治化轨道。“网络安全为人民，网络安全靠人民”维护网络安全既是我们的权利也是我们的义务。构建网络安全网，是全社会共同的愿景，也是全社会的共同责任。相关企业从全面贯彻落实总体国家安全观的高度，深刻把握信息化发展大势，强化网络风险意识，践行网络安全主体责任和义务，以高度的责任感和历史使命感构筑网络安全防线，捍卫国家网络安全。

5.2 健全安全管理制度，强化主体责任担当

企业应充分认识网络安全工作的极端重要性，以国家网络安全部署、行业网络安全发展规划为指导，结合企业实际建立和完善相应的管理制度和工作流程，制定网络安全责任制实施方案，从制度层面体现网络安全工作人人有责、人人尽责的工作要求，认真落实网络安全工作责任制。将网络安全责任明确细化落实到具体部门、具体岗位、具体人员，不断强化全体职工网络安全责任意识。此外，不断强化企业网络安全责任监督考核制度，完善健全考核机制，明确考核内容、方法、程序并将考核结果作为对相关领导干部及相关共工作人员综合考核评价的重要内容，不断推进网络安全责任制落实，确保国家网络安全法律法规和党中央、国务院等决策部署不打折扣地落实到位。严肃网络安全监督考核，强化制度执行，细化考核内容，把网络安全责任考核严起来。

5.3 加强人才能力建设，激发人才资源活力

网络安全人才是网络安全建设的核心资源，网络安全人才队伍建设情况直接影响到企业网络安全保障能力的强弱。为提高企业的网络安全实战能力，建设具有攻防实战技能的网络安全人才队伍相关企业应注重强化网络安全教育培训工作，充分发挥网络安全教育培训的重大作用。面向企业网络安全负责人、安全管理人员及相关人员开展网络安全教育培训，让企业员工深入了解国家网络安全面临的严峻形势，并通过剖析国内外网络安全事件，提升公司员工网络安全意识，普及网络安全基础知识和基本技能，巩固公司网络空间安全构筑，让“网络安全为人民、网络安全靠人民”的思想深入人心，切实提升网络安全教育培训质量。在培训模式方面，不断探索新思路、新方法，积极探索培训内容的时效性、针对性和可操作性，补齐企业网络安全教育培训短板，实现网络安全培训规范化和常态化发展。此外，要严格落实网络安全教育培训管理，将企业网络安全教育培训纳入企业网络安全从业人员的日常考评中。

5.4 强化技术防护措施，提升安全防护能力

强化网络安全技术防护是提升企业网络安全防护能力的重要途径。相关企业应不断贯彻落实网络安全等级保护、关键信息基础设施保护等相关制度，定期开展网络安全风险评估工作，通过引进先进产品及技术对网络安全防护体系不断修正，打造涵盖威胁情报、态势感知、动态防御、体系联动、安全闭环等能力在内的多层次立体防御体系。此外，需不断建立健全常态化的网络安全事件应急演练工作机制，积极探索企业内部跨部门上下贯通、左右协同的网络安全应急指挥调度和多方协同配合机制。不断强化网络安全事件应急演练，通过开展跨部门的网络安全应急演练模拟网络安全事件应急处置流程，不断完善应急响应预案，持续优化网络安全技术防护措施，提高网络安全突发事件应急处置能力。

中国信息通信研究院 安全研究所

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：17600344689 15201279481

电子邮箱：jiangding@caict.ac.cn wangrong1@caict.ac.cn

传真：010-62300264

网址：www.caict.ac.cn